Mathematical Research Letters **6**, 335–343 (1999)

CONSTRUCTION OF VALUATIONS FROM K-THEORY

Ido Efrat

Abstract. In this expository paper we describe and simplify results of Arason, Elman, Hwang, Jacob, and Ware on the construction of valuations on a field using K-theoretic data.

Introduction

Several recent developments in arithmetic geometry are based on the construction of valuations on a field just from the knowledge of its absolute Galois group. For instance, this is a main ingredient in Pop's proof of the 0-dimensional case of Grothendieck's "anabelian conjecture", saying that any two fields which are finitely generated over $\mathbb{Q}$ and which have isomorphic absolute Galois groups are necessarily isomorphic; see [P2]–[P4], [S]. Other examples are the characterization of the fields with a p-adic absolute Galois group as the p-adically closed fields ([E], [K]; see also [N], [P1]), and the analogous result for local fields of positive characteristic [EF].

In the earlier approaches to such results, valuations were detected by means of various local-global principles for Brauer groups (or higher cohomology groups) — often in combination with model-theoretic tools (c.f., [N], [P1]–[P3], [S]). A different approach is introduced in [E]: there one uses an explicit and elementary construction of valuations which emerged in the mid-1970's in the theory of quadratic forms. It originates from Bröcker's "trivialization of fans" theorem on strictly-pythagorean fields [Br], i.e., real fields K such that $K^2+aK^2 \subseteq K^2 \cup aK^2$ for all $a \in K \setminus (-K^2)$. By Bröcker's result, such a field has a valuation with very special properties: e.g., its value group is non-2-divisible, its residue field is real, and its principal units are squares. An explicit construction of these valuations was given by Jacob [J] (in the more general context of fans on pythagorean fields). This construction was extended to arbitrary fields by Ware [Wr], and later by Arason, Elman, and Jacob [AEJ]; see [En] for a related result. Roughly speaking, all these results show that if the quadratic forms over the field "behave" as if it possesses a valuation with non-2-divisible value group, residue characteristic $\neq 2$, and such that its principal units are squares, then (apart from a few obvious exceptions) such a valuation actually exists.

Received February 11, 1999.
Mathematics Subject Classification: 12J10

In the case of an odd prime number p and a field K of characteristic $\neq p$ containing a primitive pth root of unity, Hwang and Jacob [HJ] give an analogous construction of valuations with non-p-divisible value group, residue characteristic $\neq p$, and for which the principal units are pth powers. Here the role of quadratic forms is played by certain cohomological structures: the symbolic pairings $K^\times/p \otimes_{\mathbb{Z}} K^\times/p \to {}_p\mathrm{Br}(K)$, where ${}_p\mathrm{Br}(K)$ is the p-torsion part of the Brauer group of K (see also [Bo] and [K] for related constructions).

In this expository paper we give a unified and somewhat simplified presentation of these important constructions. Our approach is completely elementary; in particular, we do not use cohomology, nor non-commutative division rings. Further, we do not assume the existence of primitive pth roots of unity in the field. The cohomological structures above are replaced here by the second Milnor K-group $K_2^M(K)$ of K, i.e., the quotient of the $\mathbb{Z}$-algebra $K^\times \otimes_{\mathbb{Z}} K^\times$ by the ideal generated by all elements of the form $x \otimes (1-x)$, where $0, 1 \neq x \in K$, and the natural projection $K^\times \otimes_{\mathbb{Z}} K^\times \to K_2^M(K)$, $x \otimes y \mapsto \{x, y\}$.

Main Theorem. *Let p be a prime number, let K be a field of characteristic $\neq p$, and let T be a subgroup of $K^\times$ containing $(K^\times)^p$ and -1. Suppose that:*

- (i) *if $x \in K^\times \setminus T$ and $y \in T \setminus K^p$ then $\{x, y\} \neq 0$;*
- (ii) *if the cosets of $x, y \in K^\times$ in $K^\times/T$ are $\mathbb{F}_p$-linearly independent then $\{x, y\} \neq 0$.*

Then there exists a valuation ring O on K with value group Γ, maximal ideal m, and residue field $\bar{K}$ such that $(\Gamma : p\Gamma) \geq (K^\times : T)/p$, $1 - m \subseteq K^p$, and $\mathrm{char}\,\bar{K} \neq p$. Furthermore, if $\bar{K} = \bar{K}^p$ then $(\Gamma : p\Gamma) \geq (K^\times : T)$.

For a somewhat stronger result see Theorem 4.1.

Needless to say, most ingredients of the proof herein presented already appear in the above-mentioned works. The novelty of this note is mainly in the different organization of the material. We hope that it will make this powerful construction more easily accessible to Galois-theorists. In particular, the construction in this form is already used in [EF].

I thank Ivan Fesenko for the encouragement to publish this manuscript, and for his helpful remarks.

1. The sets O^+, O^-

From now on we fix a field K and a subgroup T of $K^\times$. Let

$$A = \left\{ x \in K^\times \mid T - xT \nsubseteq T \cup -xT \right\},$$

and let $B = \langle -1, A \rangle$ be the subgroup of $K^\times$ generated by -1 and A.

Remark 1.1.

- (i) If $x \in T$ then $0 \in T - xT$ while $0 \notin T \cup -xT$. Thus $T \subseteq A$.
- (ii) For $x \in K^\times$ one has $x \in A$ if and only if $x^{-1} \in A$.
- (iii) If $x \in K^\times \setminus T$ and $1 - x \notin T \cup -xT$ then $1 - x \in A$: indeed, $x \in T - (1-x)T$ but $x \notin T \cup -(1-x)T$.

Given a subgroup S of $K^\times$ we denote $O^-(S) = (1-T) \setminus S$.

Lemma 1.2. *If $z, w \in O^-(B)$ then either $zw \in 1-T$ or $1-zw \in zT = wT$.*

Proof. One has $-z, -w \notin B$, so

$$1 - zw = (1-z) + z(1-w) \in T + zT \subseteq T \cup zT$$
$$1 - zw = (1-w) + w(1-z) \in T + wT \subseteq T \cup wT.$$
□

Proposition 1.3. *Suppose that there exist $a, b \in O^-(B)$ with $1-ab \notin T$. Then:*

(a) $O^-(\langle B, a\rangle)O^-(\langle B, a\rangle) \subseteq 1 - T$;
(b) $A = T$;
(c) $T - a^2T \nsubseteq T \cup a^2T$.

Proof. (a) Let $H = \langle B, a\rangle$. Lemma 1.2 implies that $1 - ab \in aT = bT$, whence $b \in H$. Suppose that $0 \neq x, y \in O^-(H)$ but $xy \notin 1-T$. As $a, b \in H$, $x, y \notin H$, and $T \leq H$, Lemma 1.2 implies that $ax, by \in 1-T$. Furthermore, $ax, by \notin H$, so $ax, by \in O^-(B)$. As $ay^{-1} \notin H$, also $ay^{-1} \notin A$. Hence one of the following cases holds:

Case (i): $ay^{-1} \in 1-T$. Then $ay^{-1} \in O^-(B)$ and $(ay^{-1})(by) = ab \notin 1-T$. By Lemma 1.2, $1 - ab \in ay^{-1}T$, contrary to $1 - ab \in aT$ and $y \notin H$.

Case (ii): $a^{-1}y \in 1-T$. Then $a^{-1}y \in O^-(B)$ and $xy = (ax)(a^{-1}y) \notin 1-T$. By applying Lemma 1.2 twice we obtain $1 - xy \in xT \cap axT$, contrary to $a \notin B$.

(b) By Remark 1.1 (i), $T \subseteq A$. Conversely, take $x \in A$. Suppose $x \notin T$. After replacing x by an appropriate element of xT, we may assume that $1 - x \notin T \cup -xT$.

By Remark 1.1 (iii), $1 - x \in A \subseteq B$. Since $x \in B$ and $a \notin B$ we have $xa, -(1-x)a \notin B$. In particular, $xa, -(1-x)a \notin A$. Therefore

$$1 - xa \in T - xaT \subseteq T \cup -xaT$$
$$1 - xa \in T + (1-x)aT \subseteq T \cup (1-x)aT \quad .$$

By the choice of x, the cosets $-xaT$ and $(1-x)aT$ are disjoint. Hence $1-xa \in T$, so $xa \in O^-(B)$.

Since also $x^{-1} \in A$ (Remark 1.1 (ii)) and since $1 - x^{-1} \notin T \cup -x^{-1}T$, the same argument (with x, a replaced by x^{-1}, b) shows that $x^{-1}b \in O^-(B)$. As $ab = (xa)(x^{-1}b) \notin 1 - T$, Lemma 1.2 implies that $1 - ab \in aT \cap xaT$. This contradicts $x \notin T$.

(c) As already noted, $1 - ab \in aT = bT$ and $a \notin T$. Hence $1 - ab \in T - a^2T$ but $1 - ab \notin T \cup a^2T$. □

Next we define a group H as follows:

- If $O^-(B)O^-(B) \subseteq 1 - T$ then we take $H = B$;
- If $O^-(B)O^-(B) \nsubseteq 1-T$ then we choose $a \in O^-(B)$ such that $aO^-(B) \nsubseteq 1 - T$ and set $H = \langle B, a\rangle$.

Thus $\pm T \le \pm A \le B \le H$. We abbreviate $O^- = O^-(H)$, and let

$$O^+ = \{x \in H \mid xO^- \subseteq O^-\}.$$

Proposition 1.4.

(a) $O^-O^- \subseteq 1 - T$.
(b) $1 - O^- \subseteq O^+$.
(c) $O^-O^- \subseteq 1 - O^+$.
(d) $(1 - O^+) \cap H \subseteq O^+$.
(e) $(1 - O^+) \setminus H \subseteq O^-$.

Proof. (a) follows from Proposition 1.3 (a). For $1 \ne y \in K$ let $\tilde{y} = y/(y-1)$. Then $y \mapsto \tilde{y}$ maps $K \setminus \{0, 1\}$ onto itself. Moreover, $y \in O^-$ if and only if $\tilde{y} \in O^-$. We use the identity

$$1 - xy = (1 - (1 - x)\tilde{y})(1 - y), \qquad (*)$$

for $y \ne 1$.

(b) Take $x \in 1 - O^-$ and $y \in O^-$. By $(*)$ and (a), $1 - xy \in (1 - O^-O^-)T \subseteq TT = T$. Since $x \in T \le H$ and $y \notin H$ this implies $xy \in O^-$. Conclude that $x \in O^+$.

(c) Let $x, y \in O^-$. By $(*)$ and (b),

$$\begin{aligned} 1 - xy \in (1 - (1 - O^-)O^-)(1 - O^-) &\subseteq (1 - O^+O^-)O^+ \\ &\subseteq (1 - O^-)O^+ \subseteq O^+O^+ \subseteq O^+. \end{aligned}$$

(d) Suppose that $x \in (1 - O^+) \cap H$ and $y \in O^-$. By $(*)$,

$$1 - xy \in (1 - O^+O^-)(1 - O^-) \subseteq (1 - O^-)(1 - O^-) \subseteq TT = T.$$

As $xy \notin H$, this shows that $xy \in O^-$, whence $x \in O^+$.

(e) If $x \in (1 - O^+) \setminus H$ then $x \notin A$, so $1 - x \in H \cap (T \cup -xT) = T$. Conlcude that $x \in O^-$. □

2. The valuation O

Let A, H, O^-, O^+ be as in §1, and let $O = O^- \cup O^+$.

Proposition 2.1. *O is a valuation ring on K.*

Proof. We apply (a)–(e) of Proposition 1.4.

By definition, $O^+O^- \subseteq O^-$ and $O^+O^+ \subseteq O^+$. As $O^-O^- \subseteq 1 - T$ also $O^-O^- \setminus H \subseteq O^-$. Finally, $O^-O^- \cap H \subseteq (1 - O^+) \cap H \subseteq O^+$. Conclude that $OO \subseteq O$.

Next we show that for every $0 \neq x \in K$ either $x \in O$ or $x^{-1} \in O$. Indeed, if $x \notin H$ then $x \notin A$, so either $1-x \in T$ or $1-x^{-1} \in T$. Thus either $x \in O^-$ or $x^{-1} \in O^-$ in this case. If $x \in H \setminus \in O^+$ then there exists $y \in O^-$ such that $xy \notin O^-$. By what we have just seen, $(xy)^{-1} \in O^-$. Consequently, $x^{-1} = (xy)^{-1}y \in O^-O^- \subseteq OO \subseteq O$, as desired. In particular, $\pm 1 \in O$.

As $1 - O^- \subseteq O^+$, $(1-O^+) \cap H \subseteq O^+$, and $(1-O^+) \setminus H \subseteq O^-$, we have $1 - O \subseteq O$.

For $0 \neq x, y \in O$ we show that $x+y \in O$. By symmetry we may assume that $-x^{-1}y \in O$. Then $1 + x^{-1}y \in 1 - O \subseteq O$. Therefore $x + y = x(1+x^{-1}y) \in OO \subseteq O$.

The assertion follows. □

Proposition 2.2. *$O^\times \leq H$.*

Proof. Otherwise there exists $x \in O^\times \setminus H$. In particular, $x \in O^-$, so $1-x \in T$. Hence $1 - x^{-1} \in -x^{-1}T$, and therefore $1 - x^{-1} \notin T$. Conclude that $x^{-1} \notin O^-$, contrary to $x \in O^\times \setminus H$. □

We denote the maximal ideal of the valuation O by m.

Proposition 2.3. *$1 - m \leq T$.*

Proof. By definition, $1 - O^- \subseteq T$. So let $x \in O^+ \cap m$; we show that $x \in 1 - T$. As $x^{-1} \in H \setminus O^+$ we have $x^{-1}y \notin O^-$ for some $y \in O^-$. Since $x^{-1}y \notin H$ this implies $x^{-1}y \notin O$. Hence $xy^{-1} \in O \setminus H = O^-$. By Proposition 1.4 (a), $x = (xy^{-1})y \in O^-O^- \subseteq 1 - T$. □

Fix a prime number p.

Lemma 2.4. *If $1 - (m \setminus H) \subseteq (K^\times)^p$ then $1 - m \subseteq (K^\times)^p$.*

Proof. Take $m \in m \cap H$. Since $m^{-1} \notin O^+$ there exists $y \in O^-$ such that $m^{-1}y \notin O^-$. As $m^{-1}y \notin H$ this means that $m^{-1}y \notin O$. Then $y, y^{-1}m \in O \setminus H \subseteq m$, by Proposition 2.2. By Proposition 2.3, $1 + y^{-1}m - m \in 1 - m \leq T \leq H$. Since $y \in m \setminus H$ this implies $y + m - ym \in m \setminus H$. By assumption, $(1-y)(1-m) = 1 - (y + m - ym) \in (K^\times)^p$. Also, $1 - y \in 1 - (m \setminus H) \subseteq (K^\times)^p$. Hence $1 - m \in (K^\times)^p$. □

Corollary 2.5. *Suppose that for every $x \in K^\times \setminus H$ and every $y \in T \setminus (K^\times)^p$ one has $\{x, y\} \neq 0$. Then $1 - m \subseteq (K^\times)^p$.*

Proof. Let $x \in m \setminus H$. Then $x \in O^-$, so $1 - x \in T$. As $\{x, 1-x\} = 0$ we have $1 - x \in (K^\times)^p$. Now apply Lemma 2.4. □

Lemma 2.6. *Suppose that $p \in m$ and $1 - m \subseteq (K^\times)^p$. Then $m \setminus pm \subseteq (K^\times)^p$.*

Proof. Given $x \in 1 - m$, we may write $x = y^p$ with $y \in O^\times$. The residues $\bar{x}, \bar{y}$ then satisfy $\bar{1} = \bar{x} = \bar{y}^p$. Since $\operatorname{char} O/m = p$, necessarily $\bar{y} = \bar{1}$, i.e., $y \in 1 - m$. Thus $1 - m = (1-m)^p$.

Now let $a \in m \setminus pm$. By what we have just seen, there exists $b \in m$ such that $1+a=(1+b)^p \in 1+b^p-pm$. Since $a \notin pm$ this implies $a \in b^p(1-m) \subseteq (K^\times)^p$. □

From now on we assume that $(K^\times)^p \leq T$.

Corollary 2.7. *If $1-m \subseteq (K^\times)^p$ and $\mathrm{char}\,K \neq p$ then $p \notin m$.*

Proof. Suppose $p \in m$. Lemma 2.6 then shows that $p \in m \setminus pm \subseteq (K^\times)^p \leq H$. Since $p^{-1} \notin O^+$, there exists $a \in O^-$ such that $p^{-1}a \notin O$. By Proposition 2.2, $O^\times \leq H$, so $a \in m \setminus pm$. Lemma 2.6 once again gives $a \in (K^\times)^p \leq H$, a contradiction. □

3. The size of H

In order to prove the non-triviality of O in various situations one needs an estimate on the size of $(H:T)$. This is obtained in Corollary 3.3 below. For its proof we need two technical facts.

Lemma 3.1. *Let Δ be an elementary abelian p-group and let $\omega\colon \Delta \to \mathbb{Z}/p$ be a map such that:*

(i) *if $a, b \in \Delta$ are $\mathbb{F}_p$-linearly independent and at least one of $\omega(a)$, $\omega(b)$ is non-zero then $\omega(ab)=\omega(a)\omega(b)$;*
(ii) *there exist $\mathbb{F}_p$-linearly independent $a, b \in \Delta$ such that $\omega(a), \omega(b) \neq 0$.*

Then $1 \in Im(\omega)$.

Proof. Take a, b as in (ii). From (i) we obtain inductively that

$$\omega(a^ib)=\omega(a)^i\omega(b) \neq 0,$$

$i=1,\dots,p-1$. Since $(\mathbb{Z}/p)^\times$ has order $p-1$ this gives in particular $\omega(a^{p-1}b)=\omega(b)$. Moreover, $\omega(a^{p-1})\omega(b)=\omega(a^{p-1}b)$ by (i). Hence $\omega(a^{p-1})=1$. □

Proposition 3.2. *Assume that for every $x \in K^\times \setminus T$ one has $1-x \in \bigcup_{i=0}^{p-1} x^iT$. Suppose that the cosets of $a, b \in K^\times$ in $K^\times/T$ are $\mathbb{F}_p$-linearly independent. Then $1-a \in T \cup aT$ or $1-b \in T \cup bT$.*

Proof. For every $x \in K^\times \setminus T$ there exists by assumption a unique $0 \leq i \leq p-1$ such that $1-x \in x^iT$. When $i \neq 0$ let $0 \leq \omega(x) \leq p-1$ be the unique integer such that $w(x) \equiv 1-i^{-1} \pmod p$. When $i=0$ we set $\omega(x)=0$. Note that $\omega(x)=0$ if and only if $1-x \in T \cup xT$. Also, $1 \notin \mathrm{Im}(\omega)$.

We apply Lemma 3.1 with $\Delta = K^\times/T$. It suffices to show that if the cosets of $a, b \in K^\times$ in $K^\times/T$ are $\mathbb{F}_p$-linearly independent and at least one of $\omega(a)$, $\omega(b)$ is non-zero then $\omega(ab) \equiv \omega(a)\omega(b) \pmod p$.

Take $0 \leq i, j, r \leq p-1$ such that $1-a \in a^iT$, $1-b \in b^jT$, $1-ab \in (ab)^rT$. The assumptions imply that $i \neq 1$ or $j \neq 0$. Hence

$$1-ab=(1-a)+a(1-b) \in a^i(T-a^{1-i}b^jT) \subseteq \bigcup_{k=0}^{p-1} a^i(a^{1-i}b^j)^kT.$$

Therefore, $(ab)^r T \cap a^i(a^{1-i}b^j)^k T \neq \emptyset$ for some $0 \leq k \leq p-1$. Since a, b are independent modulo T one has $r \equiv i + (1-i)k \equiv jk \pmod{p}$. Then $r(i+j-1) \equiv jk(i+j-1) \equiv ij \pmod{p}$.

If $r \neq 0$ then also $i, j \neq 0$ and $1 - r^{-1} \equiv (1-i^{-1})(1-j^{-1}) \pmod{p}$; i.e., $\omega(ab) \equiv \omega(a)\omega(b) \pmod{p}$, as required.

If $r = 0$ then either $i = 0$ or $j = 0$, so either $\omega(ab) = \omega(a) = 0$ or $\omega(ab) = \omega(b) = 0$, and we are done again. □

Corollary 3.3. *Suppose that $-1 \in T$ and that for every $x \in K^\times \setminus T$ one has $1 - x \in \bigcup_{i=0}^{p-1} x^i T$. Then $(H : T)|p$.*

Proof. By Proposition 3.2, $(B : T)|p$. Now if $O^-(B)O^-(B) \subseteq 1-T$ then $H = B$, so $(H : T)|p$. If $O^-(B)O^-(B) \not\subseteq 1-T$ then $A = T$, by Proposition 2.2(b); hence $B = T$, so $(H : T) = (H : B) = p$. □

4. The main result

By combining the previous results we now obtain:

Theorem 4.1. *Let K be a field and let $(K^\times)^p \leq T \leq K^\times$ be an intermediate group. Suppose that:*

(i) *if $x \in K^\times \setminus T$ and $y \in T \setminus K^p$ then $\{x, y\} \neq 0$;*
(ii) *if $-1 \in T$ and if the cosets of $x, y \in K^\times$ in $K^\times/T$ are $\mathbb{F}_p$-linearly independent then $\{x, y\} \neq 0$.*

Then O above is a valuation ring. Furthermore, let m, $\bar{K}$, and Γ, be its maximal ideal, residue field, and value group, respectively. Then:

(a) *$1 - m \subseteq (K^\times)^p$;*
(b) *if $\operatorname{char} K \neq p$ then also $\operatorname{char} \bar{K} \neq p$;*
(c) *if $-1 \in T$ then $(O^\times T : T) \leq p$;*
(d) *if $-1 \notin T$ then $(O^\times B : B) \leq 2$;*
(e) *if $-1 \in T$ then $(\Gamma : p\Gamma) \geq (K^\times : T)/p$;*
(f) *if $-1 \notin T$ then $(\Gamma : 2\Gamma) \geq (K^\times : B)/2$;*
(g) *if $\bar{K} = \bar{K}^p$ and $-1 \in T$ then $(\Gamma : p\Gamma) \geq (K^\times : T)$;*
(h) *if $\bar{K} = \bar{K}^p$ and $-1 \notin T$ then $(\Gamma : 2\Gamma) \geq (K^\times : B)$.*

Proof. By Proposition 2.1, O is a valuation ring. Assumption (i) and Corollary 2.5 prove (a). Corollary 2.7 proves (b). By Proposition 2.2, $O^\times \subseteq H$.

Suppose that $-1 \in T$. For every $x \in K^\times \setminus T$ one has $\{x, 1-x\} = 0$, so by (ii), $1 - x \in \bigcup_{i=0}^{p-1} x^i T$. Corollary 3.3 now gives $(H : T)|p$, whence (c). Furthermore,

$$(\Gamma : p\Gamma) = (K^\times : O^\times (K^\times)^p) \geq (K^\times : H) \geq (K^\times : T)/p,$$

proving (e).

To prove (g), suppose that $\bar{K} = \bar{K}^p$. By Lemma 2.3, $O^\times = (1-m)(O^\times)^p \leq T$. If $H = O^\times (K^\times)^p$ then $H \leq T$; hence $H = T$, so $(\Gamma : p\Gamma) = (K^\times : T)$, and we are done in this case. On the other hand, if $H > O^\times(K^\times)^p$ then the inequalities above show that $(\Gamma : p\Gamma) > (K^\times : T)/p$. Thus (g) holds in this case as well.

When $-1 \notin T$ we have $p = 2$ and $(H : B) \leq 2$. Assertions (d),(f), and (h) are then proven similarly to (c), (e), and (g). □

Remark 4.2. If $p = 2$ and $-1 \in T$ then assumption (ii) of Theorem 4.1 implies that for every $x \in K^\times \setminus T$ one has $1 - x \in T \cup xT$. Hence $T = A = B$. This shows that the Main Theorem as stated in the introduction is a special case of Theorem 4.1.

Example 4.3. Let p be a prime number and let K be a field. Suppose that the canonical symbolic map induces an isomorphism $\wedge^2(K^\times/p) \cong K_2^M(K)/p$. Then (i) and (ii) of Theorem 4.1 hold with $T = (K^\times)^p$. Hence K possesses a valuation satisfying (a)–(g) above.

In particular, this happens for $K = \mathbb{F}_l((t_1))\cdots((t_n))$, where l is a prime number such that $p|l-1$ and such that $4|l-1$ if $p = 2$ [Wd, §2]. Then $\mathbb{F}_l$ contains a primitive pth root of unity, and $(K^\times : (K^\times)^p) = p^{n+1}$ [Wd, Lemma 1.4]. Moreover, the value group Γ of every valuation on K satisfies $(\Gamma : p\Gamma) \leq p^n$. This shows that condition (e) of Theorem 4.1 cannot be strengthened to $(\Gamma : p\Gamma) \geq (K^\times : T)$.

We conclude by proving a criterion for the existence of valuations having arbitrary residue characteristic:

Theorem 4.4. *Let p be an odd prime and let K be a field. The following conditions are equivalent:*

(a) *There exists a valuation v on K with non-p-divisible value group;*
(b) *There exists an intermediate group $(K^\times)^p \leq T < K^\times$ such that for every $x \in K^\times \setminus T$ one has $1 - x \in T \cup xT$.*

Proof. (a)⇒(b): Let $T = v^{-1}(p\Gamma)$ and take $x \in K^\times$. When $v(x) = 0$ (resp., $v(x) > 0$, $v(x) < 0$) we have $x \in T$ (resp., $1 - x \in T$, $1 - x \in xT$).

(b)⇒(a): We take T as in (b). Since $p \neq 2$ we have $-1 \in T$, so $B = A = T$. Moreover, if $a \notin T$ then $a^2 \notin T$, so $T - a^2T \subseteq T \cup a^2T$. By Proposition 1.3(c), $O^-(T)O^-(T) \subseteq 1 - T$, whence $H = T$. Propositions 2.1 and 2.2 give rise to a valuation ring O such that $O^\times \leq T$. Its value group Γ satisfies $(\Gamma : p\Gamma) = (K^\times : O^\times(K^\times)^p) \geq (K^\times : T) > 1$. □

References

[AEJ] J.K. Arason, R. Elman and B. Jacob, *Rigid elements, valuations, and realization of Witt rings*, J. Algebra **110** (1987), 449–467.

[Bo] F.A. Bogomolov, *Abelian subgroups of Galois groups*, Izv. Akad. Nauk SSSR Ser. Mat. **55** (1991), 32–67 (Russian); translation in Math. USSR Izv. **38** (1992), 27–67.

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

[E] I. Efrat, *A Galois-theoretic characterization of p-adically closed fields*, Isr. J. Math. **91** (1995), 273–284.

[EF] I. Efrat and I. Fesenko, *Fields Galois–equivalent to a local field of positive characteristic*, Math. Res. Lett., to appear.

[En] A.J. Engler, *Totally real rigid elements and F_π-henselian valuation rings*, Comm. Algebra **25** (1997), 3673–3697.

[HJ] 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.

[J] B. Jacob, *On the structure of pythagorean fields*, J. Algebra **68** (1981), 247–267.

[K] J. Koenigsmann, *From p-rigid elements to valuations (with a Galois-characterisation of p-adic fields)*, With an appendix by F. Pop, J. Reine Angew. Math. **465** (1995), 165–182.

[N] J. Neukirch, *Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 269–314.

[P1] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.

[P2] ———, *On Grothendieck's conjecture of birational anabelian geometry*, Ann. Math. **139** (1994), 145–182.

[P3] ———, *On Grothendieck's conjecture of birational anabelian geometry II*, preprint, Heidelberg 1995.

[P4] ———, *Glimpses of Grothedieck's anabelian geometry*, Geometric Galois actions. 1 (L. Schneps et al., ed.), Lond. Math. Soc. Lect. Note Ser., vol. 242, Cambridge University Press, Cambridge, 1997, pp. 113–126.

[S] M. Spiess, *An arithmetic proof of Pop's Theorem concerning Galois groups of function fields over number fields*, J. Reine Angew. Math. **478** (1996), 107–126.

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

[Wr] R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), 1338–1355.

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

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