

## BRAUER GROUP ANALOGUES OF RESULTS RELATING THE WITT RING TO VALUATIONS AND GALOIS THEORY

YOON SUNG HWANG AND BILL JACOB

**ABSTRACT.** Let  $F$  be a field of characteristic different from  $p$  containing a primitive  $p$ -th root of unity. This paper studies the cup product pairing  $H^1(F, p) \times H^1(F, p) \rightarrow H^2(F, p)$  and its relationship to valuation theory and Galois theory. Sufficient conditions on the pairing which guarantee the existence of a valuation on the field are described. In the non  $p$ -adic case these results provide a converse to the well-known structure theory in this situation. In the  $p$ -adic case, the pairing is described using the notion of “relative rigidity”. These results are analogues of results in quadratic form theory developed in the past decade, which cover the special case  $p = 2$ . Applications to the maximal pro- $p$  Galois group of  $F$  are also described.

In recent years, one of the interesting applications of quadratic form theory has been its use in determining the structure of the maximal pro-2 Galois group of a field  $F$  of characteristic different from 2. As examples we cite the papers [B], [W 1], and [JWr 1, 2]. In this paper we develop a theory which extends some of these results to the pro- $p$  Galois group where  $p$  is an odd prime. A first difficulty in trying to generalize the results just cited for odd primes is that there is no usable version of Witt ring for higher degree forms. This difficulty is circumvented in the present work by instead generalizing the notion of a quaternionic pairing. Quaternionic pairings were developed in [MY] as a tool for studying abstract Witt rings. The first section of this paper is devoted to this topic. The main objective of this paper is to illustrate some of the relationships between the higher quaternionic pairings of a field  $F$ , valuations on  $F$ , and the maximal pro- $p$  Galois group of  $F$ . The second section deals with valuation theory. In particular, using an analogue of the notion of rigidity from quadratic form theory, criteria for detecting valuations using the quaternionic pairing are developed. In the third section, the notion of relative rigidity in quadratic form theory is generalized to the Brauer group setting. The main result is the theorem which guarantees the existence of a splitting tower for the maximal pro- $p$  Galois group.

**1. Basic notions.** Throughout the following  $p$  will denote an arbitrary prime. All fields considered will have characteristic different from  $p$  and will always contain a primitive  $p$ -th root of unity. If  $F$  is such a field we denote by  $G_F(p)$  the Galois group of the maximal pro- $p$  Galois group of  $F$ , and will use  $H^i(F, p)$  to denote the Galois cohomology group

---

The first author was supported in part by GARC in Seoul, Korea.

The second author was supported in part by NSF.

Received by the editors September 7, 1994.

AMS subject classification: 12, 16.

© Canadian Mathematical Society 1995.

$H^i(G_F(p), \mathbf{Z}/p\mathbf{Z})$ . We shall utilize the familiar identifications  $H^1(F, p) \cong F^*/F^{*p}$  and  $H^2(F, p) \cong {}_p\text{Br}(F)$ , the elements of order  $p$  in the Brauer group  $\text{Br}(F)$  of  $F$ . The class of the element  $a \in F$  inside  $H^1(F, p)$  under this identification is denoted as usual by  $(a)$ , and we will usually denote the cup-products as  $(a) \cup (b) = (a, b)$  and  $(a) \cup (b) \cup (c) = (a, b, c)$ .

An easy, but important observation in the theory of quadratic forms is that the group  $H^1(F, 2)$ , the cup-product pairing  $H^1(F, 2) \times H^1(F, 2) \rightarrow H^2(F, 2)$ , together with knowledge of the class  $(-1) \in H^1(F, 2)$  completely determines the Witt ring  $WF$ . (This observation, in fact, led to the consideration of abstract quaternionic pairings in the theory of quadratic forms.) The idea in this paper is to apply an analogue of abstract quaternionic pairings to the study of pro- $p$  Galois theory. These objects are defined next.

DEFINITION 1.1. Suppose that  $G$  and  $Q$  are two elementary abelian  $p$ -groups and that

$$\gamma: G \times G \rightarrow Q$$

is a surjective skew-symmetric bilinear pairing. For any  $a \in G$  we denote by  $N_\gamma(a)$  the radical of  $a$  under  $\gamma$ , that is,  $N_\gamma(a) = \{b \in G \mid \gamma(a, b) = 0\}$ . We shall say that the pairing  $\gamma: G \times G \rightarrow Q$  satisfies  $M(n)$  if whenever  $t_1, a_1, t_2, a_2, \dots, t_n, a_n \in G$  and

$$\gamma(t_1, a_1) + \gamma(t_2, a_2) + \dots + \gamma(t_n, a_n) = 0 \in Q$$

then

$$a_1 \in \prod_{\substack{1 \leq i_1 \leq p-1 \\ 0 \leq i_2, \dots, i_n \leq p-1}} N_\gamma(t_1^{i_1} t_2^{i_2} \dots t_n^{i_n}).$$

A  $p$ -quaternionic pairing is a surjective skew-symmetric bilinear pairing  $\gamma: G \times G \rightarrow Q$  which satisfy the conditions  $M(n)$  for all  $n \geq 2$ .

In the sequel we will apply the obvious categorical notions to the class of  $p$ -quaternionic pairings, omitting the definitions when no confusion can arise. We will also use the theory of abstract Witt rings as well as the algebraic theory of quadratic forms. All our notation is standard, and we give the books [L] and [M 1] as references.

FACT 1.2. Whenever  $F$  is a field containing a primitive  $p$ -th root of unity we denote by

$$\gamma_F: H^1(F, p) \times H^1(F, p) \rightarrow H^2(F, p)$$

the cup-product pairing. The conditions  $M(n)$  are all true for this pairing  $\gamma_F$ . This is consequence of [Me, Proposition 4] and the Merkurjev-Suslin theorem. In fact, these conditions are crucial to the proof of the Merkurjev-Suslin theorem.

REMARK 1.3. When  $p = 2$  the condition  $M(2)$  is equivalent to the condition that the pairing  $\gamma: G \times G \rightarrow Q$  be linked in the sense of [MY]. Recall that  $\gamma$  being linked means that whenever  $a, b, c, d \in G$  and  $\gamma(a, b) = \gamma(c, d)$  then there exists some  $\ell \in G$  with  $\gamma(a, b) = \gamma(a, \ell) = \gamma(c, \ell)$ . To see this equivalence, suppose that  $\gamma$  satisfies  $M(2)$ , and assume that  $\gamma(a, b) = \gamma(c, d)$ . Since  $\gamma(a, b) + \gamma(c, d) = 0 \in Q$ ,  $M(2)$  gives that  $b = \alpha\beta$  for some  $\alpha \in N_\gamma(a)$  and  $\beta \in N_\gamma(ac)$ . We find that  $\gamma(a, b) = \gamma(a, \alpha\beta) = \gamma(c, \beta)$  showing that

$\gamma$  is linked. Conversely, if  $\gamma(a, b) + \gamma(c, d) = 0 \in Q$ , then the linkage condition shows there exists some  $\ell$  with  $\gamma(a, b) = \gamma(a, \ell) = \gamma(c, \ell)$ . Expressing  $b = (b\ell)\ell$ , and noting that as  $\gamma(a, b\ell) = 0 = \gamma(ac, \ell)$  we have  $b\ell \in N_\gamma(a)$  and  $\ell \in N_\gamma(ac)$ , which establishes  $M(2)$ .

In the sequel, we shall reserve the phrase “linked quaternionic pairing” for those pairings which satisfy  $M(2)$ , but do not necessarily satisfy  $M(n)$  for  $n > 2$ .

REMARK 1.4. It is possible for any  $n \geq 3$  to construct a skew-symmetric bilinear pairing  $\gamma: G \times G \rightarrow Q$  which satisfies  $M(2)$  through  $M(n-1)$ , but for which  $M(n)$  fails. As an example let  $G$  be the elementary abelian  $p$ -group of rank  $2n$  with basis  $t_1, a_1, t_2, a_2, \dots, t_n, a_n$  and let  $\gamma$  be the composite pairing

$$G \times G \rightarrow G \wedge G \rightarrow [(G \wedge G) / \langle t_1 \wedge a_1 + t_2 \wedge a_2 + \dots + t_n \wedge a_n \rangle] := Q.$$

It is easy to check that  $\gamma_\wedge: G \times G \rightarrow G \wedge G$  is a  $p$ -quaternionic pairing using the fact that  $N_{\gamma_\wedge}(g) = \langle g \rangle$  for all  $g \in G$ . As  $n \geq 3$ , we also have  $N_\gamma(g) = \langle g \rangle$  since the element  $t_1 \wedge a_1 + t_2 \wedge a_2 + \dots + t_n \wedge a_n$  cannot be expressed as a sum of fewer wedges in  $G \wedge G$ . From this it follows that  $M(n-1)$  must hold while  $M(n)$  fails. As a consequence of this, one sees that there are linked quaternionic pairings which are not the quaternionic pairings of any field.

In [MY] it was shown that one can associate an abstract Witt ring to every linked quaternionic pairing in a natural way. However, Remark 1.4 shows that the category of linked quaternionic pairings cannot be embedded as a subcategory of the category of abstract Witt rings. In [M 2], this problem was resolved by considering only the quaternionic set rather than the group  $Q$ , that is only the quaternionic mapping (rather than pairing) is considered. (In a quaternionic mapping the group  $Q$  is dropped and the subset  $S \subseteq Q$  consisting of the elements  $\gamma(a, b)$  for  $a, b \in G$  of  $Q$  is considered.) Marshall proved that the category of *linked quaternionic mappings* (or quaternionic structures) is equivalent to the category of abstract Witt rings. In the next proposition we use Marshall’s result to show that the quaternionic pairings that satisfy all the conditions  $M(n)$  embed in the category of abstract Witt rings. This result is not needed for the latter sections of this paper, but is included to illustrate the power of the properties  $M(n)$ .

PROPOSITION 1.5. *Suppose that  $G_1, G_2, Q_1$  and  $Q_2$  are elementary abelian 2-groups and that  $\gamma_1: G_1 \times G_1 \rightarrow Q_1$  and  $\gamma_2: G_2 \times G_2 \rightarrow Q_2$  are 2-quaternionic pairings that have the same Marshall-Yucas Witt ring. Then  $\gamma_1$  and  $\gamma_2$  are isomorphic, in other words, the category of 2-quaternionic pairings embeds as a full subcategory of the category of abstract Witt rings.*

PROOF. In view of Marshall’s result just mentioned, it suffices to show that  $\gamma_1$  and  $\gamma_2$  are isomorphic whenever they have the same quaternionic structure. Hence we can assume that  $G_1 = G_2$  and we have the same quaternionic mapping into the same set  $S$  embedded in  $Q_1$  and  $Q_2$  for each pairing. Since each  $Q_i$  is generated by  $S$ , the quaternionic pairings will be the same if we show that whenever  $t_1, a_1, t_2, a_2, \dots, t_r, a_r \in G$ , then

$(t_1, a_1) + (t_2, a_2) + \dots + (t_r, a_r) = 0 \in Q_1$  if and only if  $(t_1, a_1) + (t_2, a_2) + \dots + (t_r, a_r) = 0 \in Q_2$ . We proceed by induction on  $r$ , the case of  $r = 1$  is given by the quaternionic mapping. Observe that if  $(t_1, a_1) + (t_2, a_2) + \dots + (t_r, a_r) = 0 \in Q_1$ , then by  $M(r)$  we can express  $a_1 = \prod_{(i_2, \dots, i_r)} \alpha_{(i_2, \dots, i_r)}$  where  $\alpha_{(i_2, \dots, i_r)} \in N_{\gamma_1}(t_1 t_2^{i_2} \dots t_r^{i_r})$  and  $i_j \in \{0, 1\}$ . Using the fact that  $(t_1, \alpha_{(i_2, \dots, i_r)}) = (t_1^{i_2} \dots t_r^{i_r}, \alpha_{(i_2, \dots, i_r)})$  in  $Q_1$  together with the bilinearity of  $\gamma_1$ , we find that we can express

$$(t_1, a_1) + (t_2, a_2) + \dots + (t_r, a_r) = (t_2, b_2) + \dots + (t_r, b_r) \text{ in } Q_1$$

where the  $b_i \in G$  arise as products of the various  $\alpha_{(i_2, \dots, i_r)}$  and  $a_i$ . However, we know that  $N_{\gamma_1}(g) = N_{\gamma_2}(g)$  for all  $g \in G$ , so the bilinearity of  $\gamma_2$  gives the same expression in  $Q_2$  as well. The result now follows by applying the induction hypothesis to  $(t_2, b_2) + \dots + (t_r, b_r)$ . ■

One can carry out many of the same constructions for  $p$ -quaternionic pairings that one has for abstract Witt rings and linked quaternionic pairings. In the study of finitely generated Witt rings the notion direct product and group extension are crucial. We conclude this section by giving their analogues for  $p$ -quaternionic pairings.

DEFINITION 1.6. (a) Suppose that  $\gamma_1: G_1 \times G_1 \rightarrow Q_1$  and  $\gamma_2: G_2 \times G_2 \rightarrow Q_2$  are  $p$ -quaternionic pairings. Then the *direct product* of  $\gamma_1$  and  $\gamma_2$  is the pairing

$$\gamma_1 \oplus \gamma_2: (G_1 \oplus G_2) \times (G_1 \oplus G_2) \rightarrow Q_1 \oplus Q_2$$

defined in the obvious way.

(b) Suppose that  $\gamma: G \times G \rightarrow Q$  is a  $p$ -quaternionic pairing and let  $H$  be an elementary abelian  $p$ -group. Then the *group extension of  $\gamma$  by  $H$*  is the pairing

$$\gamma \times H: (G \oplus H) \times (G \oplus H) \rightarrow Q \oplus (G \otimes H) \oplus (H \wedge H)$$

defined by  $\gamma \times H((g_1, h_1), (g_2, h_2)) = \gamma(g_1, g_2) \oplus (g_1 \otimes h_2 - g_2 \otimes h_1) \oplus h_1 \wedge h_2$ .

Using a straight-forward calculation one can show that the direct product of  $p$ -quaternionic pairings is also a  $p$ -quaternionic pairing. Whenever  $\gamma$  is the  $p$ -quaternionic pairing of a field  $F$  and  $H \cong (\mathbf{Z}/p\mathbf{Z})^n$ , then it is well-known that  $\gamma \times H$  is the  $p$ -quaternionic pairing of the iterated Laurent series field  $F((t_1)) \dots ((t_n))$ . Therefore these two operations provide a method for obtaining new  $p$ -quaternionic pairings from old ones. Those fields whose  $p$ -quaternionic pairings are nontrivial group extensions carry  $p$ -henselian valuations. This is proved in Section 2.

**2. Rigidity and valuations.** We continue to assume that  $F$  is a field containing a primitive  $p$ -th root of unity. In this section we shall consider subgroups  $T, H \subset F^*/F^{*p}$  with special properties. We will always assume that  $-1 \in F^{*p}$ , which is not a restriction if  $p$  is odd. For analogous results in this section in the case where  $p = 2$  and  $-1 \notin F^{*p}$  we refer the reader to [AEJ]. For convenience we will frequently abuse notation and identify an element  $x \in F$  with its coset  $x F^{*p} \in F^*/F^{*p}$  whenever no confusion may arise. Therefore, at times we will view  $T$  and  $H$  as subgroups of  $F^*$  as well. We denote

by  $(T, F)$  and  $(H, H)$  the subgroups of  ${}_p\text{Br}(F)$  generated by the elements  $(t, f)$  and  $(h_1, h_2)$  respectively where  $t \in T, f \in F^*$  and  $h_1, h_2 \in H$ .

DEFINITION 2.1. We say that  ${}_p\text{Br}(F)$  is  $T$ -rigid if  $F^*/F^{*p} \cong T \oplus H, {}_p\text{Br}(F) = (T, F) \oplus (H, H)$ , and  $(H, H) \cong H \wedge H$  where the wedge denotes the exterior product (as  $\mathbb{Z}/p\mathbb{Z}$ -vector spaces).

Suppose that  $F = \bar{F}((T_1))((T_2)) \cdots ((T_n))$  is an iterated formal Laurent power series field. If we let  $T = \bar{F}^*/\bar{F}^{*p} \subset F^*/F^{*p}$  and  $H = \langle T_1, T_2, \dots, T_n \rangle \subset F^*/F^{*p}$ , then well-known calculations show that  ${}_p\text{Br}(F)$  is  $T$ -rigid. More generally, if  $\nu: F \rightarrow \Gamma$  is a valuation and if one sets  $T = U_F F^{*p} \subset F^*/F^{*p}$  and lets  $H$  denote an inverse image of  $\Gamma/p\Gamma$  in  $F^*/F^{*p}$ , then  ${}_p\text{Br}(F)$  is  $T$ -rigid. Our goal in this section is to show that  ${}_p\text{Br}(F)$  being  $T$ -rigid corresponds to the existence of valuations on  $F$ , thereby providing a partial converse the examples just given.

LEMMA 2.2. If  ${}_p\text{Br}(F)$  is  $T$ -rigid and  $y \in F^* - T$ , then

$$T + Ty \subseteq T \cup Ty \cup Ty^2 \cup \dots \cup Ty^{p-1}.$$

PROOF. As  $Ty = Ty_0$  for some  $y_0 \in H$ , we may assume that  $y \in H$ . For a given element  $t + t'_1y$  of  $T + Ty$  with  $t, t'_1 \in T$  we can express  $t + t'_1y = t'_2h$  for some  $t'_2 \in T$  and  $h \in H$ . Multiplying this expression by  $t^{-1}$  we have  $1 + t_1y = t_2h$  for some  $t_1, t_2 \in T$ . It follows, in  ${}_p\text{Br}(F)$  that

$$0 = (t_1y, 1 + t_1y) = (t_1y, t_2h) = (t_1y, t_2) + (t_1, h) + (y, h).$$

Since  ${}_p\text{Br}(F) = (T, F) \oplus (H \wedge H)$  we have  $(y, h) = 0$  in  $H \wedge H$ . This shows that  $h \in \{1, y, y^2, \dots, y^{p-1}\}$  in  $H$  and  $t + t'_1y \in T \cup Ty \cup Ty^2 \cup \dots \cup Ty^{p-1}$  follows. ■

In the algebraic theory of quadratic forms, rigidity was originally defined for field elements. We give these definitions next.

DEFINITION 2.3. Let  $T$  be a subgroup of  $F^*$  containing  $F^{*p}$ . An element  $x \in F^*$  is called  $T$ -prerigid (in  $F$ ) if  $1 + x \in T \cup xT$  and is called  $T$ -rigid (in  $F$ ) if  $T + xT \subseteq T \cup xT$ . If  $x$  is not  $T$ -rigid, then  $x$  is called  $T$ -basic, and the set of all  $T$ -basic elements in  $F$  is denoted by  $B_F(T)$ .

We will show in the next two propositions that if  ${}_p\text{Br}(F)$  is  $T$ -rigid, then there is at most one element  $a$  lying outside  $T$  such that  $x$  is  $T$ -prerigid for all  $x \notin \langle T, a \rangle$ , where  $\langle T, a \rangle$  denotes the subgroup of  $F^*$  generated by  $T$  and  $a$ .

PROPOSITION 2.4. Suppose that  ${}_p\text{Br}(F)$  is  $T$ -rigid. Assume that there is an element  $a \in F^* - T$  such that  $1 - a \in T$  but  $1 + a \notin T$ . If  $x \in F^* - \langle T, a \rangle$  then

- (a)  $1 - x \in T$  if and only if  $1 + x \in T$ . (So,  $1 - x \in xT$  if and only if  $1 + x \in xT$ .)
- (b)  $x$  is  $T$ -prerigid.

PROOF. (a) As  $x = -x \in F^*/T$ , it suffices to show that if  $1 - x \in T$ , then  $1 + x \in T$ . Suppose not, that is,  $1 + x \notin T$ . By Lemma 2.2 we can express  $1 + a \in a^e T$  and  $1 + x \in x^f T$

for  $1 \leq e, f \leq p - 1$ . So, multiplying by  $a$ , we find  $a - ax \in aT$  and  $a + ax \in ax^fT$ . Since  $1 - a \in T$  and  $1 + a \in a^eT$ , Lemma 2.2 gives further that  $1 - ax = (1 - a) + (a - ax) \in a^iT$  and  $1 - ax = (1 + a) - (a + ax) \in a^{e+j(1-e)}x^{jf}T$  for  $0 \leq i, j \leq p - 1$ . But, since  $x \notin \langle T, a \rangle$ , we have  $j = 0$  and  $1 - ax \in a^eT$ . However, Lemma 2.2 shows that  $1 - ax \in (ax)^kT$  for some  $k$ , a contradiction, establishing (a).

For (b), applying Lemma 2.2,  $1 - x \in x^mT$  and  $1 + x \in x^nT$  for  $0 \leq m, n \leq p - 1$ . This shows that  $a - ax \in ax^mT$  and  $a + ax \in ax^nT$ . Since  $1 - a \in T$  and  $1 + a \in a^eT$  we find again applying Lemma 2.2 that  $1 - ax = (1 - a) + (a - ax) \in (ax^m)^iT$ ,  $1 - ax = (1 + a) - (a + ax) \in a^e(a^{1-e}x^n)^jT$ , and  $1 - ax \in (ax)^kT$  for some  $i, j$ , and  $k$ . So  $im \equiv i \equiv e + (1 - e)j \equiv jn \pmod{p}$ . If  $i \not\equiv 0 \pmod{p}$ , then  $m \equiv 1 \pmod{p}$ , and consequently  $1 - x \in xT$ . In this case  $1 + x \in xT$  follows by (a). If  $i \equiv 0 \pmod{p}$ , then  $jn \equiv e + (1 - e)j \equiv 0 \pmod{p}$ , and since  $e \not\equiv 0 \pmod{p}$ , we have  $j \not\equiv 0 \pmod{p}$ . This shows that  $n \equiv 0 \pmod{p}$  and we have  $1 + x \in T$ , establishing (b). ■

**PROPOSITION 2.5.** *Suppose that  ${}_p\text{Br}(F)$  is  $T$ -rigid. Assume for all  $x \in F^* - T$ ,  $1 - x \in T$  if and only if  $1 + x \in T$ . If there is an element  $a \in F^* - T$  such that  $1 - a \in a^\alpha T$  where  $1 < \alpha < p$ , then every element  $y \in F^* - \langle T, a \rangle$  is  $T$ -prerigid.*

**PROOF.** By assumption it suffices to show that  $1 - y \in T$  or  $1 - y \in yT$ . Suppose not, then there is some  $b \in F^* - \langle T, a \rangle$  such that  $1 - b \in b^\beta T$  with  $1 < \beta < p$ . So,  $a - ab \in ab^\beta T$ . Since  $1 - a \in a^\alpha T$  we find by Lemma 2.2 that  $1 - ab = (1 - a) + (a - ab) \in a^\alpha(a^{1-\alpha}b^\beta)^iT$  and  $1 - ab \in (ab)^jT$  for some  $i, j$ . So,  $\alpha + i(1 - \alpha) \equiv i\beta \pmod{p}$ . Hence  $i(\alpha - 1 + \beta) \equiv \alpha \pmod{p}$ . Since  $\alpha \not\equiv 0 \pmod{p}$ ,  $\alpha - 1 + \beta \not\equiv 0 \pmod{p}$ , we find  $1 - ab \in (ab)^{\alpha_1}T$  where  $\alpha_1 \equiv \alpha\beta/(\alpha - 1 + \beta) \pmod{p}$ .

We denote by  $[\alpha, \beta] = \alpha\beta/(\alpha - 1 + \beta)$ . By applying the same argument as above to the equations  $1 - a \in a^\alpha T$  and  $1 - ab \in (ab)^{\alpha_1}T$ , we find that  $1 - a^2b \in (a^2b)^{\alpha_2}T$  where  $\alpha_2 \equiv [\alpha, \alpha_1] = \alpha^2\beta/((\alpha - 1)^2 + \beta[\alpha^2 - (\alpha - 1)^2]) \pmod{p}$ , and  $(\alpha - 1)^2 + \beta[\alpha^2 - (\alpha - 1)^2] \not\equiv 0 \pmod{p}$ . Applying this same argument repeatedly, we find that  $1 - a^m b \in (a^m b)^{\alpha_m}T$  for  $1 \leq m \leq p - 1$ , where  $\alpha_m \equiv \alpha^m\beta/((\alpha - 1)^m + \beta[\alpha^m - (\alpha - 1)^m]) \pmod{p}$ , and  $(\alpha - 1)^m + \beta[\alpha^m - (\alpha - 1)^m] \not\equiv 0 \pmod{p}$ .

We now claim that  $(\beta - 1)/\beta \notin \langle (\alpha - 1)/\alpha \rangle$ , the subgroup of  $(\mathbf{Z}/p\mathbf{Z})^*$  generated by  $(\alpha - 1)/\alpha$ , from which we will find  $\alpha \not\equiv \beta \pmod{p}$ , as desired. Suppose that  $(\beta - 1)/\beta \equiv [\alpha/(\alpha - 1)]^{m_0} \pmod{p}$  for  $m_0$  with  $0 < m_0 \leq p - 1$ . Then  $\alpha^{m_0}\beta - (\alpha - 1)^{m_0}(\beta - 1) \equiv (\alpha - 1)^{m_0} + \beta[\alpha^{m_0} - (\alpha - 1)^{m_0}] \equiv 0 \pmod{p}$ , which contradicts what we just proved.

Let  $n$  be the order of  $(\alpha - 1)/\alpha$  in  $(\mathbf{Z}/p\mathbf{Z})^*$ . Then  $\alpha^n \equiv (\alpha - 1)^n \pmod{p}$  and  $\alpha_n \equiv \beta \pmod{p}$ . Note that  $1 - a^n b \in (a^n b)^{\alpha_n}T$  and  $1 - b \in b^\beta T$ . Since  $b \notin \langle T, a \rangle$  and  $p$  does not divide  $n$ ,  $b \notin \langle T, a^n b \rangle$ . So by the same argument used in proving that  $\alpha \not\equiv \beta \pmod{p}$  above, we have  $\alpha_n \not\equiv \beta \pmod{p}$ . This contradiction completes the proof. ■

Suppose  ${}_p\text{Br}(F)$  is  $T$ -rigid. Let  $R = \langle T, a \rangle$  be a subgroup of  $F^*$  generated by  $T$  and  $a$  where  $a \in F^* - T$  satisfies either  $1 - a \in T$  but  $1 + a \notin T$  or  $1 - a \in a^\alpha T$  for some  $\alpha$  with  $1 < \alpha < p$  if such an element exists, and let  $R = T$  otherwise. With this notation, Propositions 2.4 and 2.5 give the following.

COROLLARY 2.6. *If  ${}_p\text{Br}(F)$  is  $T$ -rigid and if  $R$  is as just described, then  $B_F(T) \subseteq R$ .*

PROOF. According to Propositions 2.4 and 2.5, if  $x \in F^* - R$ , then  $x$  is prerigid. Now consider any  $t_1, t_2 \in T$ . Since  $xt_1^{-1}t_2$  is prerigid, we know that  $1 + xt_1^{-1}t_2 \in T \cup xT$ . Multiplying by  $t_1$  we find that  $t_1 + xt_2 \in T \cup xT$  and consequently  $x$  is  $T$ -rigid. From this,  $B_F(T) \subseteq R$  follows. ■

Corollary 2.6 shows that  $T$  and  $R$  satisfy the conditions given in Notation 2.1 of [AEJ] (except we use  $R$  where [AEJ] used  $H$ ), and therefore all the results of [AEJ] apply. We next recall some of the key definitions from [AEJ] (also see [W 2]).

DEFINITION 2.7 ([AEJ]). We define

$$\begin{aligned} O_F^-(R, T) &:= \{x \in F \mid x \notin R \text{ and } 1 + x \in T\} \\ O_F^+(R, T) &:= \{x \in F^* \mid x \in R \text{ and } xO_F^-(R, T) \subseteq O_F^-(R, T)\} \\ O_F(R, T) &:= O_F^-(R, T) \cup O_F^+(R, T). \end{aligned}$$

$O_F(R, T)$  is called *preadditive* if  $O_F^-(R, T) \cdot O_F^-(R, T) \subseteq 1 - T$ , that is, if  $x, y \in O_F^-(R, T)$ , then  $1 - xy \in T$ . (See [AEJ, Lemma 2.6.] )

We next give the main theorem of this section.

THEOREM 2.8. *Suppose that  $p$  is an odd prime,  ${}_p\text{Br}(F)$  is  $T$ -rigid and  $R$  is as above. Then  $O_F(R, T)$  is preadditive. Consequently,  $A := O_F(R, T)$  is a valuation ring of  $F$  such that  $U_A \cdot T \subseteq R$  and  $1 + M_A \subseteq T$  where  $U_A$  and  $M_A$  denote the units and maximal ideal of  $A$  respectively.*

PROOF. Let  $x$  and  $y$  be elements of  $O_F^-(R, T)$ . Then  $1 + x = t_1$  and  $1 + y = t_2$  for  $t_1, t_2 \in T$ . Hence,  $x + xy = xt_2$  and  $1 - xy = (1 + x) - (x + xy) = t_1 - xt_2 \in (1 + x)T$  for some  $t \in T$ . As  $x \notin R$  and  $t \in T \subseteq R$ , we have  $xt \notin R$  and consequently  $xt$  is  $T$ -prerigid by Propositions 2.4 and 2.5. This shows that  $1 - xy \in T$  or  $xT$ .

We first suppose that  $yT \neq xT$ . In this case, since  $1 - y \in T$  and  $y - xy \in yT$  we have  $1 - xy = (1 - y) + (y - xy) \in T$  or  $yT$ . As  $yT \neq xT$  we find that  $1 - xy \in T$  as required.

We now suppose that  $y = xt$  for some  $t \in T$ . Since  $p$  is odd, we know  $x^2 \notin R$  and we have  $1 - xy = 1 - x^2t \in T$  or  $x^2T$  by Propositions 2.4 and 2.5. Since  $xT \neq x^2T$  we conclude that  $1 - xy \in T$  as required.

The remaining assertions of the theorem follow from Theorem 2.10 of [AEJ]. This concludes the proof. ■

In the sequel we shall use  $v: F \rightarrow \Gamma_A$  to denote the valuation associated with the valuation ring  $A = O_F(R, T)$ . The condition that  $1 + M_A \subseteq T$  means that  $A$  is a  $T$ -compatible valuation ring (see [AEJ, Definition 1.7]). A key property of  $T$ -compatible valuation rings of the form  $O_F(R, T)$  is that  $v(R)$  does not contain any non-trivial convex subgroups of the value group  $\Gamma_A$  (see [AEJ, Lemma 3.1]). The next lemma is a result about  $p$ -adic valued fields.

LEMMA 2.9. *Suppose that  $v: F \rightarrow \Gamma$  is a valuation on a field  $F$  containing a primitive  $p$ -th root of unity and  $\text{char}(\bar{F}) = p$ . Assume that  $x, y \in F$  satisfy  $0 < v(y) \leq v(p)$ , and*

either  $v(x)$  and  $v(y)$  are linearly independent in  $\Gamma/p\Gamma$  or we may assume that  $v(y) \notin p\Gamma$  and  $x \in U_A$  with  $\bar{x} \notin \bar{F}^{*p}$ . Then  $(1 - y, x) \neq 0 \in {}_p\text{Br}(F)$ .

PROOF. We observe that the extension  $L_1 = F(\sqrt[p]{x})$  is either ramified with value group  $\Gamma_{L_1} = \Gamma(\frac{1}{p}v(x))$ , or else is unramified with residue class field the purely inseparable extension  $\bar{F}(\sqrt[p]{\bar{x}})$ . We next observe that the extension  $L_2 = F(\sqrt[p]{1-y})$  is ramified with value group  $\Gamma_{L_2} = \Gamma(\frac{1}{p}v(y))$ . To see this, for  $z \in L_2$  we express  $1 - y = (1 - z)^p = 1 - pz + \dots + pz^{p-1} - z^p$ . Since  $v(-pz + \dots + pz^{p-1}) > v(p) \geq v(y)$  we find that  $v(y) = v(z^p)$  as required. We now apply [JWd, Corollary 2.6] in case  $v(x) \notin p\Gamma$  or [JWd, Corollary 2.9] in case  $x \in U_A$  to the symbol algebra  $D = (1 - y, x)$  to see that the valuation on  $F$  extends to  $D$ . Consequently,  $D$  is a division algebra and the lemma is proved. ■

In the next lemma we refine our knowledge of the valuation  $O_F(R, T)$  in some special cases.

LEMMA 2.10. *Suppose that  $R \neq F^*$  and  $A = O_F(R, T)$  is a  $T$ -compatible valuation ring and that  $T_0 \subset T$  is a subgroup containing  $F^{*p}$  with the property that whenever  $x \in T - T_0$  and  $y \in F^* - R$ , one has  $(x, y) \neq 0 \in {}_p\text{Br}(F)$ . Then,  $(1 + M_A) \subset T_0$ . Furthermore, if for every  $t \in T_0$  there exists some  $x \in T - T_0$  with  $(t, x) = 0 \in {}_p\text{Br}(F)$ , then  $A = O_F(R, T)$  is non  $p$ -adic, that is,  $\text{char}(\bar{F}) \neq p$ .*

PROOF. We begin by observing that whenever  $y \in F^* - R$ , as  $p\Gamma_A = v(U_A F^{*p})$ , the fact that  $U_A T \subseteq R$  shows that  $v(y) \notin p\Gamma_A$ . Further, suppose that  $x \in T$ . Then either  $v(x) \in p\Gamma$  or else  $v(x)$  and  $v(y)$  are linearly independent in  $\Gamma/p\Gamma$ . (For if  $x = y^s z^p u$  where  $0 < s < p$  and  $u \in U_A$ , we find as  $U_A \cdot F^{*p} \subseteq R$  that  $x \notin R$ .)

For the first statement we let  $m \in M_A$ . If  $m \in F^* - R$ , then as  $1 + m \in T$  and as  $(1 + m, -m) = 0$  we conclude by our hypothesis on  $T_0$  that  $1 + m \in T_0$ . Next, we suppose that  $m \in R$ . Then, since  $v(R)$  cannot contain any nontrivial convex subgroup of  $\Gamma_A$  we know there exists  $y \in F^* - R$  with  $0 < v(y) < v(m)$ . (For, the convex subgroup generated by  $v(m)$  cannot be contained in  $v(R)$  and hence there exists some  $z \in F^* - R$  and  $n \in \mathbb{N}$  with  $nv(m) < v(z) < (n + 1)v(m)$ . We may then set  $y = zm^{-n}$ .) We also know that both  $1 + my^{-1} + m \in T$  and  $1 + m + y + my \in T$  since  $v(my^{-1} + m) > 0$  and  $v(m + y + my) > 0$ . We find that  $-y(1 + my^{-1} + m) = -(m + y + my) \in F^* - R$  and that  $(1 + m + y + my, -(m + y + my)) = 0 \in {}_p\text{Br}(F)$ . Again, our hypothesis on  $T_0$  shows that  $(1 + m + y + my) = (1 + m)(1 + y) \in T_0$ . Since we already know that  $1 + y \in T_0$ , we conclude that  $1 + m \in T_0$  as required.

Now suppose that  $\text{char}(\bar{F}) = p$ . Then  $p \in M_A$  and as above there exists  $y \in F^* - R$  with  $0 < v(y) \leq v(p)$ . We know that  $1 - y \in T_0$ . Suppose that  $x \in T - T_0$  is chosen with  $(1 - y, x) = 0 \in {}_p\text{Br}(F)$ . By the above, either  $v(x)$  and  $v(y)$  are linearly independent in  $\Gamma/p\Gamma$  or we may assume that  $x \in U_A$ . In the latter case, as  $x \notin T_0$  and as  $(1 + M_A)F^{*p} \subseteq T_0$ , we conclude that  $\bar{x} \notin \bar{F}^{*p}$ . Applying Lemma 2.9 we find that  $(1 - y, x) \neq 0 \in {}_p\text{Br}(F)$ , a contradiction. This proves the lemma. ■

Recall that a valuation on a field  $F$  is called  $p$ -henselian if Hensel's lemma holds for  $p$ -extensions. When  $F$  has a primitive  $p$ -th root of unity and the valuation is non  $p$ -adic,



this is equivalent to  $1 + M_A \subseteq F^{*p}$ . The next theorem characterizes the case when  $O_F(R, T)$  is non  $p$ -adic and  $p$ -henselian.

**THEOREM 2.11.** *Suppose that  $p$  is an odd prime and the  $p$ -quaternionic pairing of the field  $F$  is a nontrivial group extension, that is, we can decompose  $H^1(F, p) \cong G \oplus H$  so that the cup-product pairing becomes*

$$(G \oplus H) \times (G \oplus H) \rightarrow Q \oplus (G \otimes H) \oplus (H \wedge H)$$

where  $Q$  is the subgroup  $(G, G) \subset {}_p\text{Br}(F)$ . If we set  $T = G$ , then  ${}_p\text{Br}(F)$  is  $T$ -rigid and the valuation ring  $O_F(R, T)$  is non  $p$ -adic and  $p$ -henselian.

**PROOF.** The  $T$ -rigidity of  ${}_p\text{Br}(F)$  is clear. Since  $G = T \subseteq R$ , the condition that  $T \otimes H$  embeds in  ${}_p\text{Br}(F)$  shows that the hypotheses of Lemma 2.10 are satisfied with  $T_0 = F^{*p}$ . Consequently,  $O_F(R, T)$  is non  $p$ -adic and  $1 + M_A \subseteq F^{*p}$ . The proof is complete. ■

In the study of pro-2 Galois groups, whenever  $WF \cong R_1 \times R_2$  in the category of abstract Witt rings, a crucial problem is to find realizations of the factors  $R_1$  and  $R_2$ . This means that one tries to find (usually infinite) 2-extensions  $L_1$  and  $L_2$  of  $F$  with  $WL_i \cong R_i$  such that the projection maps  $WF \rightarrow R_i$  correspond to the maps  $WF \rightarrow WL_i$  induced by field inclusion. We have the analogous notion for  $p$ -quaternionic pairings. Suppose that  $\gamma_F$  decomposes as a direct sum  $\gamma_F = \gamma_1 \oplus \gamma_2: (G_1 \oplus G_2) \times (G_1 \oplus G_2) \rightarrow Q_1 \oplus Q_2$ . We say that a field extension  $L$  realizes the factor  $\gamma_1$  of  $\gamma$  if  $F^*/F^{*p} \rightarrow L^*/L^{*p}$  is surjective with kernel  $G_2$  and if the identification  $G_1 \cong L^*/L^{*p}$  arising from the field inclusion  $F \subset L$  induces an isomorphism  $Q_1 \cong {}_p\text{Br}(L)$ . We note in particular that this means  $\gamma_L$  coincides with  $\gamma_1$  under these identifications. This next result is the analogue of the Realization Theorem [AEJ, Theorem 4.8] for decomposition of  $p$ -quaternionic pairings.

**REALIZATION THEOREM 2.12.** *Suppose that  $p$  is an odd prime and the  $p$ -quaternionic pairing  $\gamma$  of the field  $F$  decomposes as a direct sum  $\gamma = \gamma_1 \oplus \gamma_2: (G_1 \oplus G_2) \times (G_1 \oplus G_2) \rightarrow Q_1 \oplus Q_2$  where  $\gamma_1$  is a nontrivial group extension  $\gamma_1 = \overline{\gamma}_1 \times H: (\overline{G}_1 \oplus H) \times (\overline{G}_1 \oplus H) \rightarrow (\overline{G}_1, \overline{G}_1) \oplus (\overline{G}_1 \otimes H) \oplus (H \wedge H)$ . (So, we have  $F^*/F^{*p} \cong (\overline{G}_1 \oplus H) \oplus G_2$ ). Then the factor  $\gamma_1$  is realized by some (possibly infinite)  $p$ -extension  $L$  of  $F$ .*

**PROOF.** We set  $T = \overline{G}_1 \oplus G_2$  and  $T_0 = G_2$  and we let  $R$  be as in Corollary 2.6. We first assume that  $R \neq F^*$ . One readily checks that the fact that  $\gamma_1 = \overline{\gamma}_1 \times H$  guarantees that  ${}_p\text{Br}(F)$  is  $T$ -rigid and since  $R \neq F^*$  all the hypotheses of Lemma 2.10 are satisfied for these  $T_0 \subset T$ . Consequently, the valuation given by  $A = O_F(R, T)$  is non  $p$ -adic and  $1 + M_A \subset T_0$ .

We next claim that  $(1 + M_A)F^{*p} = T_0 = G_2$ . We already know that  $(1 + M_A)F^{*p} \subseteq T_0$ . Conversely, assume  $x \in T_0$ . Let  $y \in (F^* - R) \cap G_1$ . By the first paragraph in the proof of Lemma 2.10, either  $v(x) \in p\Gamma$  or else  $v(x)$  and  $v(y)$  are linearly independent in  $\Gamma/p\Gamma$ . In the latter case, we know by [JWd, Corollary 2.6] that  $D = (x, y)$  is a totally ramified  $F$ -division algebra, contrary to the fact that  $x \in G_2$  and  $y \in G_1$  gives  $(x, y) = 0$ . In the former case, multiplying  $x$  by an element of  $F^{*p}$  we may assume that  $x \in U_A$ . In case  $\bar{x} \notin \bar{F}^{*p}$ , [JWd, Corollary 2.9] gives that  $D = (x, y)$  is a semiramified  $F$ -division algebra (with residue field  $\bar{F}(\sqrt[p]{\bar{x}})$ ). This contradiction shows that  $\bar{x} \in \bar{F}^{*p}$  and  $(1 + M_A)F^{*p} = T_0 = G_2$  has been established. The theorem when  $R \neq F^*$  now follows from the following lemma.

LEMMA 2.13. *Let  $v: F \rightarrow \Gamma$  be a non  $p$ -adic valuation on a field  $F$  containing a primitive  $p$ -th root of unity. Suppose that  $\gamma_F$  decomposes as a direct sum  $\gamma_F = \gamma_1 \oplus \gamma_2: (G_1 \oplus G_2) \times (G_1 \oplus G_2) \rightarrow Q_1 \oplus Q_2$  where  $G_2 = (1 + M_v)F^{*p}$ . If  $L$  is a  $p$ -henselization of  $F$  with respect to  $v$ , then  $L$  realizes the factor  $\gamma_1$ .*

PROOF. When  $L$  is a  $p$ -henselization of  $F$ , it is well-known that  $F^*/F^{*p} \rightarrow L^*/L^{*p}$  is surjective and  $\ker(F^*/F^{*p} \rightarrow L^*/L^{*p}) = (1 + M_A)F^{*p}/F^{*p}$ . Consequently,  $L^*/L^{*p} \cong (F^*/F^{*p})/G_2 \cong G_1$ . It remains to show that  $Q_1 \cong {}_p\text{Br}(L)$  and that  $\gamma_L$  coincides with  $\gamma_1$  with these identifications. The Merkurjev-Suslin theorem shows that  ${}_p\text{Br}(L)$  is generated by the symbols  $(a, b)$  with  $a, b \in G_1 \subset F^*/F^{*p}$ , and consequently the homomorphism  $Q_1 \rightarrow {}_p\text{Br}(L)$  induced by the inclusion  $F \rightarrow L$  is surjective. To prove this map is injective, in view of the Merkurjev-Suslin theorem it suffices to show that whenever  $x \in L^*$  and  $g, g_1 \in G_1 \subset F^*/F^{*p}$  are such that  $g \mapsto [x], g_1 \mapsto [1 - x] \in L^*/L^{*p}$ , then  $(g, g_1) = 0 \in {}_p\text{Br}(F)$ . (For, the Merkurjev-Suslin theorem shows that the kernel of  $L^*/L^{*p} \otimes L^*/L^{*p} \rightarrow {}_p\text{Br}(L)$  is generated by the elements  $(x) \otimes (1 - x)$ , and consequently the kernel of  $Q_1 \rightarrow {}_p\text{Br}(L)$  is generated by symbols which would have been shown to be zero.)

We now note that if  $v(x) > 0$ , then  $1 - x \in L^{*p}$  and consequently  $g_1 = 1 \in G_1$ , so the result is clear in this case. Similarly, if  $v(x) < 0$ , then  $[x] = [1 - x] \in L^*/L^{*p}$  so that  $g = g_1 \in G_1$  and again the result is clear. So we may assume that  $x$  is a unit in  $L$ . Since  $\bar{F} = \bar{L}$  and as  $G_2 = (1 + M_v)F^{*p}$  we may assume (modifying  $g$  by a  $p$ -th power from  $F$  as needed) that  $\bar{g} = \bar{x}$  when viewed as  $L$ -elements. It then follows that  $\overline{1 - g} = \overline{1 - x}$  and consequently  $g_1(1 - g)^{-1} \in (1 + M_v)F^{*p} = G_2$ . In particular,  $g_1 = (1 - g)g_2 \in F^*/F^{*p}$  for some  $g_2 \in G_2$ . We now find,  $(g, g_1) = (g, 1 - g) + (g, g_2) = 0 + 0$  since  $g \in G_1$  and  $g_2 \in G_2$ . The lemma is proved. ■

Returning to proof of the theorem, we next consider the case where  $R = F^*$ . Since  $[R : T] \leq p$  we must be in the situation where  $|H| = p$ . Suppose first that  $\overline{G_1} = \{1\}$ . Then  $(G_1, G_1) = 0$  follows. In this case we let  $L$  be any  $p$ -extension of  $F$  maximal with respect to the property that  $G_1$  embeds in  $L^*/L^{*p}$ , and the desired properties of  $L$  are clear.

So we may now assume that  $|\overline{G_1}| \geq p$  and  $H = \langle h \rangle$  has order  $p$ . In this case we arbitrarily choose some  $\overline{T_1} \subset \overline{G_1}$  with  $[\overline{G_1} : \overline{T_1}] = p$ , and we set  $T' = \overline{T_1} \oplus G_2 \subset T$ . Suppose  $g \in \overline{G_1}$  is chosen so that  $\overline{G_1} = \overline{T_1} \oplus \langle g \rangle$ . We have  $G_1 \cong \overline{T_1} \oplus \langle g, h \rangle$ , and further, since  $(g, h) \neq 0$  we find  $(G_1, G_1) = (\overline{T_1}, G_1) \oplus (\langle g, h \rangle \wedge \langle g, h \rangle)$ . From this it follows that  ${}_p\text{Br}(F)$  is  $T'$ -rigid.

We let  $R'$  be the  $R$  arising in Corollary 2.6 for  $T'$ . Then, as  $[R' : T'] \leq p$  and as  $[F^* : T'] = p^2$ , we know that  $R' \neq F^*$  and by Theorem 2.8  $O_F(R', T')$  is a  $T'$ -compatible valuation subring of  $F$ . In case  $R' = T$ , it follows that  $O_F(R', T') = O_F(T, T') = O_F(T, T)$  is a valuation ring and we are done since we find that our original  $R = T$ . So we may assume that  $R' \neq T$ . We set  $\overline{G'_1} := (R' \cap G_1)/F^{*p}$ . Then  $\overline{G'_1} = \langle \overline{T_1}, hg' \rangle$  for some  $g' \in \overline{G_1}$ . If  $g' \notin \overline{T_1}$ , then  $\overline{G_1} = \overline{T_1} \oplus \langle g' \rangle$  and the homomorphism  $\overline{G'_1} \rightarrow Q_1$  given by  $z \mapsto (z, h)$  is injective since the analogous homomorphism  $\overline{G_1} \rightarrow Q_1$  is injective. We conclude that  $\gamma_1 = \gamma'_1 \times H$  where  $\gamma'_1$  is the pairing  $\gamma'_1 : \overline{G'_1} \times \overline{G'_1} \rightarrow (\overline{G'_1}, \overline{G'_1})$

in this case. If  $g' \in \overline{T_1}$ , then  $\overline{G_1}' = \overline{T_1} \oplus \langle h \rangle$ . We let  $g_1 \in \overline{G_1} - \overline{T_1}$ , and note that the homomorphism  $\overline{G_1}' \rightarrow Q_1$  given by  $z \mapsto (z, hg_1)$  is injective. In this case we conclude that  $\gamma_1 = \gamma_1' \times \langle hg_1 \rangle$ , and we are in the former situation replacing  $H$  by  $\langle hg_1 \rangle$ . But now,  $O_F(R', T') = O_F(R', R')$  is a valuation ring, and we are reduced to the situation above Lemma 2.13 by replacing our original  $T$  with  $R'$ . This concludes the proof. ■

REMARK 2.14. Theorems 2.11 and 2.12 provide all the technicalities necessary to generalize the main results of [JWr 1] to the case of pro- $p$  groups. To describe this, let  $\mathcal{E}_0$  denote the category of finite  $p$ -quaternionic pairings generated from the pairings of non  $p$ -adic local fields using the operations of direct product and group extension. Then the class of pro- $p$  groups  $G_F(p)$  where the  $p$ -quaternionic pairing of  $F$  lies in  $\mathcal{E}_0$  can be described completely by an inductive procedure corresponding to the inductive decomposition of  $\gamma_F$  in  $\mathcal{E}_0$ . The possibilities for  $G_F(p)$  will depend upon the structure of  $\gamma_F$  and the cyclotomic character  $G_F(p) \rightarrow \text{Aut}(\mu_{p^\infty})$  where  $\mu_{p^\infty} \subset F^*$  is the subgroup of all  $p^n$ -th roots of unity for all  $n$ . The details can be obtained by imitating the proofs in [JWr 1] and will not be described here.

3. **Relative rigidity.** The notion of relative rigidity in quadratic form theory was introduced in [J] as an axiomatic approach to the structure of the Witt rings of field with dyadic henselian valuations. The main result proved there is the existence of splitting towers for the pro-2 Galois group, providing insight into how the Witt ring determines its structure. In this section we show how to extend these results to the pro- $p$  case. In order to better illustrate the techniques developed we limit the discussion in this section to the case where  $n = 2$ , the general case is indicated in Remark 3.6.

Recall that  $p$  is a fixed (not necessarily odd) prime and that  $F$  is a field containing a primitive  $p$ -th root of unity. For any  $a \in F$  we denote by  $N_F(a) := N_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^*) / F^{*p} \subseteq F^* / F^{*p}$ , the image of the norm map. Whenever  $t \in F^* / F^{*p}$  we use  $\langle t \rangle$  to denote the cyclic subgroup of  $F^* / F^{*p} \cong H^1(F, p)$  generated by  $t$ , and we use  $(t, F)$  to denote the subgroup of  ${}_p \text{Br}(F) (\cong H^2(F, p))$  generated by cyclic algebras (cup products) of the form  $(t, f)$  for all  $f \in F^* / F^{*p}$ . The next definition is the analogue of a Witt ring being 2-relatively rigid given in terms of the cohomology ring  $H^*(F, p)$ .

DEFINITION 3.1. Let  $t_1, t_2 \in F^*$  and let  $H_F$  be a subgroup of  $F^* / F^{*p}$  such that cup product mapping  $H_F \rightarrow H^3(F, p)$  given by  $h \mapsto (t_1, t_2, h)$  is injective. Then the  $p$ -torsion component  ${}_p \text{Br}(F)$  of the Brauer group is called *relatively rigid mod  $H_F$*  for  $t_1, t_2$  if:

- (i)  $F^* / F^{*p} = N_F(t_1)N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1}) \oplus H_F$
- (ii) Whenever  $g_0 g_1 g_2 \cdots g_p = 1 \in F^* / F^{*p}$  where  $g_0 \in N_F(t_1), g_1 \in N_F(t_2), g_2 \in N_F(t_1 t_2), \dots, g_p \in N_F(t_1 t_2^{p-1})$ , then necessarily  $g_0 \in \langle t_1 \rangle, g_1 \in \langle t_2 \rangle, g_2 \in \langle t_1 t_2 \rangle, \dots, g_p \in \langle t_1 t_2^{p-1} \rangle$ .
- (iii)  ${}_p \text{Br}(F) = (t_1, F) + (t_2, F)$ .

The most interesting examples of fields  $F$  for which  ${}_p \text{Br}(F)$  is relatively rigid mod  $H_F$  for  $t_1, t_2$  are the generalized local fields of level 2 considered by Kato in [K]. In this case  $H_F \cong \mathbf{Z}/p\mathbf{Z}$ . More generally, if  $F$  is complete with respect to a discrete valuation

with uniformizing parameter  $t_1$ , and if  $\bar{F}$  has characteristic  $p$  with a  $p$ -basis the single element  $\bar{t}_2$  where  $t_2$  is a unit of  $F$ , then  ${}_p\text{Br}(F)$  is relatively rigid mod  $H_F$  for  $t_1, t_2$  where  $H_F \cong \bar{F}/(\wp(\bar{F}) + \sum_{i=1}^{p-1} \bar{t}_1^i \bar{F}^p)$ . For further discussion in the case  $p = 2$  we refer the reader to Section 6 of [J].

Whenever  $p = 2$  and  $L/F$  is a quadratic extension, one knows that the restriction-corestriction sequence  $H^n(F, 2) \rightarrow H^n(L, 2) \rightarrow H^n(F, 2)$  is exact. However, when  $p > 2$  and  $L/F$  is a cyclic  $p$ -extension, this zero sequence is no longer exact. Because this exactness is a central tool in the theory of quadratic forms, some understanding of the homology of this sequence is crucial in order to generalize results. Hilbert’s Theorem 90 for  $K_2$  gives some useful information about the kernel of corestriction in the relatively rigid case as the next lemma shows.

LEMMA 3.2. *Suppose that  ${}_p\text{Br}(F)$  is relatively rigid mod  $H_F$  for  $t_1, t_2$ . Let  $L = F(\sqrt[p]{t_1})$ . Then  $\ker(\text{cor}_{L/F}: {}_p\text{Br}(L) \rightarrow {}_p\text{Br}(F)) \subseteq (t_2, L)$ .*

PROOF. Let  $A \in \ker(\text{cor}_{L/F})$  and let  $\sigma$  be a generator of the Galois group  $\text{Gal}(L/F)$ . Using Hilbert’s Theorem 90 for  $K_2$ ,  ${}_p\text{Br}(F) \cong K_2(F)/pK_2(F)$  (the Merkurjev-Suslin theorem), and using the fact that  $\text{cor} \circ \text{res}: {}_p\text{Br}(F) \rightarrow {}_p\text{Br}(F)$  is zero, we find that

$$A = {}^\sigma A_1 - A_1 + \text{res}_{L/F}(C) \quad \text{in } {}_p\text{Br}(L)$$

for some  $A_1 \in {}_p\text{Br}(L)$  and  $C \in {}_p\text{Br}(F)$ . Since  ${}_p\text{Br}(F) = (t_1, F) + (t_2, F)$ , we find that  $A \equiv {}^\sigma A_1 - A_1 \pmod{(t_2, L)}$ .

Next, using  ${}_p\text{Br}(F) = (t_1, F) + (t_2, F)$ , we express

$$\text{cor}_{L/F}(A_1) = (t_1, c_1) + (t_2, c_2) \quad \text{for some } c_1, c_2 \in F^*.$$

Using  $F^*/F^{*p} = N_F(t_1)N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1}) \oplus H_F$  together with the fact that  $(t_2, x) \in (t_1, F)$  whenever  $x \in N_F(t_1 t_2^i)$  for  $i = 1, 2, \dots, p - 1$ , we may assume that  $c_2 = N_{L/F}(\alpha)h$  with  $\alpha \in L$  and  $h \in H_F$ . Setting  $B_1 = A_1 - (\sqrt[p]{t_1}, c_1) - (t_2, \alpha)$  we have  $\text{cor}_{L/F}(B_1) = (t_2, h)$ . However, as  $0 = \text{cor}_{L/F}(B_1) \cup (t_1) = (t_1, t_2, h)$ , we find by our hypotheses on  $H_F$  that  $h = 1$  and consequently  $\text{cor}_{L/F}(B_1) = 0$ .

We next observe that  ${}^\sigma(\sqrt[p]{t_1}, c_1) - (\sqrt[p]{t_1}, c_1) = (\xi, c_1) \in \text{res}_{L/F}({}_p\text{Br}(F)) \subseteq (t_2, L)$  ( $\xi$  is some primitive  $p$ -th root of unity), and  ${}^\sigma(t_2, \alpha) - (t_2, \alpha) = (t_2, {}^{(\sigma-1)}\alpha) \in (t_2, L)$ . This shows that  ${}^\sigma A_1 - A_1 \equiv {}^\sigma B_1 - B_1 \pmod{(t_2, L)}$  and consequently  $A \equiv {}^\sigma B_1 - B_1 \pmod{(t_2, L)}$  with  $\text{cor}_{L/F}(B_1) = 0$ . By applying the same arguments to  $B_1$  instead of  $A$ , we can express  $B_1 \equiv {}^\sigma B_2 - B_2 \pmod{(t_2, L)}$  for some  $B_2 \in {}_p\text{Br}(L)$  with  $\text{cor}_{L/F}(B_2) = 0$ . Iterating this argument gives  $\pmod{(t_2, L)}$

$$A \equiv {}^{(\sigma-1)}B_1 \equiv {}^{(\sigma-1)^2}B_2 \equiv {}^{(\sigma-1)^3}B_3 \equiv \dots \equiv {}^{(\sigma-1)^{p-1}}B_{p-1}$$

where  $B_i \in {}_p\text{Br}(L)$  with  $\text{cor}_{L/F}(B_i) = 0$  for  $1 \leq i \leq p - 1$ . Since  $(-1)^k \binom{p-1}{k} \equiv 1 \pmod{p}$  we find that  $\pmod{(t_2, L)}$

$$A \equiv \sum_{i=0}^{p-1} {}^{\sigma^i} B_{p-1} \equiv \text{res}_{L/F}(\text{cor}_{L/F}(B_{p-1})) = 0.$$

This shows that  $A \in (t_2, L)$ , proving the lemma. ■

One of the principal objectives of this section is to show that relative rigidity is inherited under certain cyclic extensions. The next lemma shows how to describe the behavior of norm subgroups under these extensions.

LEMMA 3.3. *Suppose that  $t_1$  and  $t_2$  are elements of  $F^*/F^{*p}$  which are  $\mathbf{Z}/p\mathbf{Z}$ -linearly independent and satisfy condition (ii) of Definition 3.1. Let  $L = F(\sqrt[p]{t_1})$ . Then*

$$N_L(t_2) = i_{L/F}(N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1})).$$

PROOF. We must show the inclusion  $\subseteq$ , the reverse inclusion is clear. Suppose that  $\alpha \in N_L(t_2)$ . Since  $(t_2, \alpha) = 0$  we have that  $(t_2, N_{L/F}(\alpha)) = 0 \in {}_p \text{Br}(F)$ . Thus,  $N_{L/F}(\alpha) \in N_F(t_1) \cap N_F(t_2)$  and consequently by condition (ii) of Definition 3.1 we have  $N_{L/F}(\alpha) = 1$  in  $F^*/F^{*p}$ . Applying Hilbert’s Theorem 90 we can express  $\alpha = c_1 \cdot (\sigma^{-1})\alpha_1$  for some  $c_1 \in F, \alpha_1 \in L$  where  $\sigma$  is a generator for  $\text{Gal}(L/F)$ . Since  $(-1)^k \binom{p-1}{k} \equiv 1 \pmod{p}$  we find  $(\sigma^{-1})^{p-1} \alpha_1 \equiv N_{L/F}(\alpha_1) \pmod{L^{*p}}$ . Therefore in  ${}_p \text{Br}(L)$ , since  $(t_2, \alpha) = 0$

$$0 = (t_2, (\sigma^{-1})^{p-2} \alpha) = (t_2, (\sigma^{-1})^{p-2} c_1 \cdot (\sigma^{-1})^{p-1} \alpha_1) = (t_2, N_{L/F}(\alpha_1)).$$

Since  $\ker(\text{res}_{L/F}: {}_p \text{Br}(F) \rightarrow {}_p \text{Br}(L)) = (t_1, F)$  it follows we can express  $(t_2, N_{L/F}(\alpha_1)) = (t_1, c) \in {}_p \text{Br}(F)$  for some  $c \in F$ . Applying the condition  $M(2)$  together with condition (ii) of Definition 3.1 shows that

$$N_{L/F}(\alpha_1) \in (N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1})) \cap N_F(t_1) = (t_1) \subset F^*/F^{*p}.$$

Applying Hilbert’s Theorem 90,  $\alpha_1 = (\sqrt[p]{t_1})^i c_1 \cdot (\sigma^{-1})\alpha_2$  for some  $c_1 \in F$  and  $\alpha_2 \in L$ . Direct calculation then gives that  $(\sigma^{-1})\alpha_1 = \xi^i \cdot (\sigma^{-1})^2 \alpha_2$  and therefore

$$(*) \quad \alpha = c_1 \cdot (\sigma^{-1})\alpha_1 = c_2 \cdot (\sigma^{-1})^2 \alpha_2$$

where  $c_2 = c_1 \xi^i \in F$ . Repeating the process leading to expression (\*) iteratively  $p - 3$  times and using  $(-1)^k \binom{p-1}{k} \equiv 1 \pmod{p}$  gives

$$\alpha = c_{p-1} \cdot (\sigma^{-1})^{p-1} \alpha_{p-1} = c_{p-1} N_{L/F}(\alpha_{p-1})$$

in  $L^*/L^{*p}$  for some  $c_{p-1} \in F$  and  $\alpha_{p-1} \in L$ . Set  $d = c_{p-1} N_{L/F}(\alpha_{p-1}) \in F$ , noting that  $i_{L/F}(d) = \alpha \in L^*/L^{*p}$ . Then in  ${}_p \text{Br}(L)$  we have  $(t_2, \alpha) = (t_2, d) = 0$ . Consequently in  ${}_p \text{Br}(F)$  we have  $(t_2, d) = (t_1, e) = 0$  for some  $e \in F$ . Applying condition  $M(2)$  we have that  $d \in N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1})$  from which the lemma follows. ■

We are now ready to prove the main result of this section.

**THEOREM 3.4.** *Suppose that  $F$  is relatively rigid mod  $H_F$  for  $t_1, t_2$ . Then  $L = F(\sqrt[p]{t_1})$  is relatively rigid mod  $H_L := i_{L/F}(H_F)$  for  $\sqrt[p]{t_1}, t_2$ .*

**PROOF.** We must verify that conditions (i), (ii) and (iii) of Definition 3.1 hold for  $L$ . We begin with (i). Let  $\alpha \in L^*$ . By condition (iii) for  $F$  we can express  $\text{cor}_{L/F}(\sqrt[p]{t_1}, \alpha) = (t_1, c_1) + (t_2, c_2) \in {}_p\text{Br}(F)$  for some  $c_1, c_2 \in F$ . Applying condition (i) for  $F$  together with the fact that  $(t_2, x) \in (t_1, F)$  whenever  $x \in N_F(t_1 t_2^i)$  for  $i = 1, 2, \dots, p-1$ , we may assume that  $c_1 \in N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1}) \oplus H_F$  and  $c_2 \in N_F(t_1) \oplus H_F$ . We express  $c_2 = N_{L/F}(\delta)h$  (in  $F^*/F^{*p}$ ) where  $\delta \in L$  and  $h \in H_F$ . Then in  ${}_p\text{Br}(F)$  we have

$$\text{cor}_{L/F}(\sqrt[p]{t_1}, \alpha c_1^{-1}) - (t_2, \delta) = (t_2, h).$$

We set  $D = (\sqrt[p]{t_1}, \alpha c_1^{-1}) - (t_2, \delta) \in {}_p\text{Br}(L)$ . Then  $0 = (t_1) \cup \text{cor}_{L/F}(D) = (t_1, t_2, h)$  shows that  $h = 1 \in F^*/F^{*p}$  and consequently  $\text{cor}_{L/F}(D) = 0$ . Applying Lemma 3.2 we know that  $D = (t_2, \gamma)$  for some  $\gamma \in L$ . This shows that  $(\sqrt[p]{t_1}, \alpha c_1^{-1}) = (t_2, \delta\gamma) \in {}_p\text{Br}(L)$ . Applying  $M(2)$  we find that

$$\alpha c_1^{-1} \in N_L(\sqrt[p]{t_1})N_L(\sqrt[p]{t_1}t_2)N_L(\sqrt[p]{t_1}t_2^2) \cdots N_L(\sqrt[p]{t_1}t_2^{p-1}).$$

By construction we have that

$$c_1 \in N_F(t_2)N_F(t_1 t_2)N_F(t_1 t_2^2) \cdots N_F(t_1 t_2^{p-1}) \oplus H_F$$

from which it follows that

$$\alpha = (\alpha c_1^{-1})c_1 \in N_L(\sqrt[p]{t_1})N_L(t_2)N_L(\sqrt[p]{t_1}t_2)N_L(\sqrt[p]{t_1}t_2^2) \cdots N_L(\sqrt[p]{t_1}t_2^{p-1}) \oplus H_L.$$

This proves condition (i) for  $L$ .

We next prove condition (iii) for  $L$ . Let  $A \in {}_p\text{Br}(L)$ . Applying condition (iii) for  $F$  we find that  $\text{cor}_{L/F}(A) = (t_1, c_1) + (t_2, c_2)$  for some  $c_1, c_2 \in F$ , where as above we may assume that  $c_2 = N_{L/F}(\delta)h$  with  $\delta \in L$  and  $h \in H_F$ . We obtain that  $\text{cor}_{L/F}(A - (\sqrt[p]{t_1}, c_1) - (t_2, \delta)) = (t_2, h)$ . As shown for  $D$  above in the proof of (i), we can express  $A - (\sqrt[p]{t_1}, c_1) - (t_2, \delta) = (t_2, \gamma)$  for some  $\gamma \in L$ . It now follows that  $A \in (\sqrt[p]{t_1}, L) + (t_2, L)$ .

We conclude by establishing condition (ii). We suppose that  $g_0 g_1 g_2 \cdots g_p = 1 \in L^*/L^{*p}$  where  $g_0 \in N_L(\sqrt[p]{t_1})$ ,  $g_1 \in N_L(t_2)$ ,  $g_2 \in N_L(\sqrt[p]{t_1}t_2), \dots, g_p \in N_L(\sqrt[p]{t_1}t_2^{p-1})$ . We proceed in two steps.

**STEP 1.** Applying Lemma 3.3 we find that  $g_1 = a_1 a_2 \cdots a_p$  in  $L^*/L^{*p}$  where  $a_1 \in N_F(t_2)$ ,  $a_2 \in N_F(t_1 t_2), \dots, a_p \in N_F(t_1 t_2^{p-1})$ . Since  $g_0 g_1 \cdots g_p = 1$  in  $L^*/L^{*p}$  and  $(\sqrt[p]{t_1}, g_0) = (\sqrt[p]{t_1}t_2, g_2) = \cdots = (\sqrt[p]{t_1}t_2^{p-1}, g_p) = 0 \in {}_p\text{Br}(L)$  we obtain

$$(*) \quad 0 = (\sqrt[p]{t_1}, g_1 g_2 \cdots g_p) = (\sqrt[p]{t_1}, a_1 a_2 \cdots a_p) + (t_2, g_2^{-1} g_3^{-2} \cdots g_{p-1}^{-(p-2)} g_p).$$

Let  $\alpha = g_2^{-1} g_3^{-2} \cdots g_{p-1}^{-(p-2)} g_p$ . Applying the corestriction to  $(*)$  we obtain

$$(t_1, a_1 a_2 \cdots a_p) + (t_2, N_{L/F}(\alpha)) = 0 \in {}_p\text{Br}(F).$$

Applying condition  $M(2)$  together with condition (ii) for  $F$  we find that  $N_{L/F}(\alpha) \in N_F(t_2)N_F(t_1t_2)N_F(t_1t_2^2) \cdots N_F(t_1t_2^{p-1}) \cap N_F(t_1) = \langle t_1 \rangle \subset F^*/F^{*p}$ . We express  $N_{L/F}(\alpha) = t_1^i$  in  $F^*/F^{*p}$ . Replacing  $g_p, g_0$ , and  $g_1$  by  $(\sqrt[p]{t_1}t_2^{-1})^{-i}g_p, (\sqrt[p]{t_1})^i g_0$ , and  $t_2^{-i}g_1$ , respectively, we may assume that  $N_{L/F}(\alpha) = 1 \in F^*/F^{*p}$ . Consequently,  $(t_1, a_1a_2 \cdots a_p) = 0 \in {}_p \text{Br}(F)$  and  $a_1a_2 \cdots a_p \in N_F(t_1)$ . Since  $a_1 \in N_F(t_2), a_2 \in N_F(t_1t_2), \dots, a_p \in N_F(t_1t_2^{p-1})$ , applying condition (ii) for  $F$  we find that  $a_1 \in \langle t_2 \rangle, a_2 \in \langle t_1t_2 \rangle, \dots, a_p \in \langle t_1t_2^{p-1} \rangle$ . This shows that  $g_1 = a_1a_2 \cdots a_p \in \langle t_2 \rangle$  in  $L^*/L^{*p}$ , say  $a_1a_2 \cdots a_p = t_2^k$ . Equation (\*) now becomes

$$(**) \quad (\sqrt[p]{t_1}, t_2^k) + (t_2, \alpha) = 0 \in {}_p \text{Br}(L).$$

Since  $N_{L/F}(\alpha) = 1 \in F^*/F^{*p}$ , applying the corestriction to (\*\*) we have  $(t_1, t_2^k) = 0 \in {}_p \text{Br}(F)$ , so  $k = 0$ , that is,  $g_1 = 1 \in L^*/L^{*p}$ . Now, by (\*) we find that  $(t_2, \alpha) = 0 \in {}_p \text{Br}(L)$  so  $\alpha \in N_L(t_2)$ .

STEP 2. Since  $g_p = \alpha g_2 g_3^2 \cdots g_{p-1}^{p-2}, g_1 = 1$  and  $g_0 g_1 \cdots g_p = 1$  in  $L^*/L^{*p}$ , we have that  $g_0 \alpha g_2^2 g_3^3 \cdots g_{p-1}^{p-1} = 1$  in  $L^*/L^{*p}$ , where  $g_0 \in N_L(\sqrt[p]{t_1}), \alpha \in N_L(t_2), g_2^2 \in N_L(\sqrt[p]{t_1}t_2), \dots, g_{p-1}^{p-1} \in N_L(\sqrt[p]{t_1}t_2^{p-2})$ . We relabel  $\alpha, g_2^2, g_3^3, \dots, g_{p-1}^{p-1}$  as  $g_1, g_2, g_3, \dots, g_{p-1}$  again. Then we have

$$(a) \quad g_0 g_1 g_2 \cdots g_{p-1} = 1 \in L^*/L^{*p}.$$

Applying the same arguments in Step 1 to (a), after a suitable modification of  $g_{p-1}, g_0$ , and  $g_1$ , we have  $g_1 = 1$  and  $g_{p-1} = \alpha_1 g_2^{i(2)} g_3^{i(3)} \cdots g_{p-2}^{i(p-2)}$  for some  $\alpha_1 \in N_L(t_2)$ . Applying (a) we have that  $g_0 \alpha_1 g_2^{i(2)+1} g_3^{i(3)+1} \cdots g_{p-2}^{i(p-2)+1} = 1$  in  $L^*/L^{*p}$ . By letting  $\alpha_1, g_2^{i(2)+1}, g_3^{i(3)+1}, \dots, g_{p-2}^{i(p-2)+1}$  be  $g_1, g_2, \dots, g_{p-2}$ , respectively, again we have

$$(b) \quad g_0 g_1 g_2 \cdots g_{p-2} = 1 \in L^*/L^{*p}.$$

By repeating this process again and again (and after modifying), we have finally,

$$(c) \quad g_0 g_1 g_2 g_3 = 1 \in L^*/L^{*p}.$$

By applying the same arguments as in Step 1 to expression (c), after a suitable modification of  $g_3, g_0$  and  $g_1$ , we have  $g_1 = 1$  and  $\alpha'_0 := g_2^{-1} g_3^{-2} \in N_{L/F}(t_2)$ . So,

$$(d) \quad g_3 = \alpha_0 g_2^j \quad \text{and} \quad g_0 \alpha_0 g_2^{j+1} = 1 \in L^*/L^{*p}$$

where  $j = (-2)^{-1}$  in  $(\mathbf{Z}/p\mathbf{Z})^*$  and  $\alpha_0 = (\alpha'_0)^j \in N_{L/F}(t_2)$ . By repeating the same arguments used in Step 1, we may assume that  $\alpha_0 = 1$ . As  $g_2 \in N_L(\sqrt[p]{t_1}t_2)$ , and  $g_0 \in N_L(\sqrt[p]{t_1})$ ,  $0 = (g_0, \sqrt[p]{t_1}t_2) = (g_0, t_2)$  in  ${}_p \text{Br}(L)$ . It follows that  $g_0 \in N_L(t_2)$ . By Lemma 3.3, we find  $g_0 = c$  in  $L^*/L^{*p}$  for some  $c \in N_F(t_2)N_F(t_1t_2)N_F(t_1t_2^2) \cdots N_F(t_1t_2^{p-1})$ . Also, as  $g_0 \in N_L(\sqrt[p]{t_1}), 0 = (g_0, \sqrt[p]{t_1}) = (c, \sqrt[p]{t_1})$  in  ${}_p \text{Br}(L)$ . Applying the corestriction, we find that  $(c, t_1) = 0$  in  ${}_p \text{Br}(F)$ , and  $c \in N_F(t_1)$ . Applying condition (ii) for  $F$  we find  $c \in \langle t_1 \rangle$  in  $F^*/F^{*p}$ . Hence  $g_0 = 1$  in  $L^*/L^{*p}$  and from (d) we have  $g_2^{j+1} = 1$  in  $L^*/L^{*p}$ . It now follows that  $g_2 = 1 = g_3$  in  $L^*/L^{*p}$ , since  $j = (-2)^{-1} \neq -1$  in  $(\mathbf{Z}/p/\mathbf{Z})^*$ .

Going back to the previous stages repeatedly, the same arguments show (with modifications) that  $g_4 = 1 = g_5 = \dots = g_p$  in  $L^*/L^{*p}$ . Throughout the process our modifications have included raising our original  $g_i$ 's to prime to  $p$  exponents, or multiplying by some product of  $\sqrt[p]{t_1}$  with suitable powers of  $t_2$ . The conclusion that condition (ii) holds for  $L$  follows. ■

In the next corollary we apply Theorem 3.4 to show that the pro- $p$  Galois group of a relatively rigid field has a  $\tilde{Z}_p \oplus \tilde{Z}_p$  “splitting tower”. (Here,  $\tilde{Z}_p$  denotes the free rank 1 pro- $p$  group  $\varprojlim Z/p^n Z$ .)

**COROLLARY 3.5.** *Suppose that  $F$  is relatively rigid mod  $H_F$  for  $t_1, t_2$ . Set  $L_1 = F(\sqrt[p]{t_1}, \sqrt[p]{t_2})$ ,  $L_2 = F(\sqrt[p^2]{t_1}, \sqrt[p^2]{t_2}), \dots, L_i = F(\sqrt[p^i]{t_1}, \sqrt[p^i]{t_2})$  and set  $\tilde{L} := \cup_{i \in \mathbb{N}} L_i$ . Then  ${}_p \text{Br}(\tilde{L}) = 0$ . Consequently, one obtains a short exact sequence*

$$0 \rightarrow \mathcal{F} \rightarrow G_F(p) \rightarrow M \rightarrow 0$$

where  $\mathcal{F}$  is a free pro- $p$  group and  $M$  is a metabelian pro- $p$  group. Moreover, if  $F$  contains all  $p^n$ -th roots of unity for all  $n$ , then  $M \cong \tilde{Z}_p \oplus \tilde{Z}_p$ , otherwise  $M$  is a semidirect product  $\tilde{Z}_p \rtimes (\tilde{Z}_p \oplus \tilde{Z}_p)$ .

**PROOF.** Theorem 3.4 shows that  ${}_p \text{Br}(L_i) = (\sqrt[p^i]{t_1}, L_i) + (\sqrt[p^i]{t_2}, L_i)$  and  ${}_p \text{Br}(\tilde{L}) = 0$  follows from this. If we let  $\tilde{L}' = \tilde{L}(\mu_{p^\infty})$  be the field obtained from  $\tilde{L}$  by adjoining all the  $p^n$ -th roots of unity for all  $n$ , then  $\tilde{L}'$  is Galois over  $F$ . The result follows setting  $\mathcal{F} := G_{\tilde{L}'}(p)$  and  $M := \text{Gal}(\tilde{L}'/F)$ . ■

**REMARK 3.6.** It is possible to generalize Definition 3.1 and consider a notion of the Brauer group being relatively rigid mod  $H_F$  for  $t_1, t_2, \dots, t_n$ . For this one needs to reformulate the notion of  $n$ -relative rigidity introduced in [J] for the cohomology ring  $H^*(F, p)$ . It should be possible to generalize Theorem 3.4 to this setting. Details will not be given here.

REFERENCES

[AEJ] J. Arason, R. Elman and B. Jacob, *Rigid Elements, valuations, and realization of Witt rings*, J. Algebra **110**(1987), 449–467.  
 [B] E. Becker, *Formal-reelle Körper mit streng-auflösbarer absoluter Galoisgruppe*, Math. Ann. **238**(1978), 203–206.  
 [J] B. Jacob, *Quadratic forms over Dyadic Valued Fields II, Relative Rigidity and Galois Cohomology*, J. Algebra **148**(1992), 162–202.  
 [JWd] B. Jacob and A. Wadsworth, *A New Construction of Noncrossed Product Algebras*, Trans. Amer. Math. Soc. **293**(1986), 693–721.  
 [JWr 1] B. Jacob and R. Ware, *A Recursive Description of the Maximal Pro-2 Galois Group Via Witt Rings*, Math. Z. **200**(1989), 379–396.  
 [JWr 2] ———, *Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups*, Math. Z. **208**(1991), 193–208.  
 [L] T.-Y. Lam, *Algebraic Theory of Quadratic Forms*, W. A. Benjamin Inc., 1973.  
 [K] K. Kato, *A generalization of local class field theory by using  $K$ -groups, I, II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. (2) **26**(1979), 303–376; (3) **27**(1980), 603–683.  
 [M 1] M. Marshall, *Abstract Witt Rings*, Queen’s Papers in Pure and Appl. Math. **57**, 1980.  
 [M 2] ———, *Classification of finitely generated Witt rings which are strongly representational*, preprint.



- [MY] M. Marshall and J. Yucas, *Linked quaternionic mappings and their associated Witt rings*, Pacific J. Math. **95**(1981), 411–426.
- [Me] A. S. Merkurjev,  *$K_2$  and the Brauer Group*, Contemp. Math. **55**(1986), 529–547.
- [W 1] R. Ware, *Quadratic Forms and Profinite 2-groups*, J. Algebra **58**(1979), 227–237.
- [W 2] ———, *Valuation Rings and rigid elements in fields*, Canad. J. Math. **33**(1981), 1338–1355.

*Korea University*  
*Seoul 136-701*  
*Korea*

*University of California-Santa Barbara*  
*Santa Barbara, California 93106*  
*U.S.A.*