SOME GALOIS EXTENSIONS OF QUADRATIC EXTENSIONS ASSOCIATED WITH WITT RINGS

WENFENG GAO AND JÁN MINÁČ

Abstract. A Galois field extension E/F whose Galois group is a pro-2-group of an exponent of at most 8, with a nilpotency class of at most 4, is determined, such that it contains essential information about the Witt rings of all quadratic extensions of F.

Let F be a field of characteristic not 2 and F_q the quadratic closure of F. Let G_F be the Galois group of F_q/F. Then G_F is a pro-2-group. Let $F = F^{(1)} \subset F^{(2)} \subset \cdots \subset F_q$ be a tower of fields such that $F^{(n+1)}$ is the compositum of all of the quadratic extensions of $F^{(n)}$ which are Galois over F. Observe that $F^{(n)}$ is a Galois extension of F. We denote $Gal(F^{(n)}/F)$ by $G_F^{[n]}$. It is a quotient of G_F and we denote $G_F^{(n)}$ the kernel of the natural projection of G_F onto $G_F^{[n]}$. We have $G_F^{(n+1)} = (G_F^{(n)})^2[G_F^{(n)}, G_F]$. This means that $G_F^{(n+1)}$ is the smallest closed subgroup of G_F which contains all squares of elements in $G_F^{(n)}$ and all commutators $[\sigma, \tau]$, where $\sigma \in G_F^{(n)}$ and $\tau \in G_F$. We denote by WF the Witt ring of a quadratic form over F. For the basic theory of Galois pro-2-extensions see [Ko], [N-S-W], [Rib], or [Sh]. For basic information on the Witt rings of quadratic forms see [La] or [Sch]. We also use Kummer theory which describes abelian field extensions of a given exponent with enough roots of unity in the base field. (See e.g. [A-T], Chapter 6.)

We use freely some well-known and easily derived conditions for the existence of an embedding of quadratic extensions in Galois extensions with a Galois group isomorphic to a cyclic group of order 4, and also conditions for an embedding of biquadratic extensions in Galois extensions with a Galois group isomorphic to a dihedral group of order 8, which we denote as D_4. (See e.g. [G-M], pages 101 and 102.)

In [M-Sp] it was proved:

The second author's research is partially supported by NSERC. This author also gratefully acknowledges the special Dean of Science fund at The University of Western Ontario, along with the hospitality of the Mathematical Sciences Research Institute in Berkeley, California during the Fall of 1999.

Theorem 1 (M-Sp). *Let F, F' be two fields. Then*

(1) $WF \cong WF'$ *implies that* $G_F^{[3]} \cong G_{F'}^{[3]}$,
(2) *If* $\langle 1,1\rangle_F$ *is universal, assume that* $\sqrt{-1} \in F$ *iff* $\sqrt{-1} \in F'$. *Then* $G_F^{[3]} \cong G_{F'}^{[3]}$ *implies that* $WF \cong WF'$.

This theorem shows that the theory of Witt rings can be thought of as part of Galois theory. In particular the classification of Witt rings can be reduced to the classification of Galois groups $G_F^{[3]}$ and specifying whether $\sqrt{-1} \in F$ or $\sqrt{-1} \notin F$.

One of the major unsolved probems in the theory of quadratic forms is the precise relationship between WF and $WF(\sqrt{a})$, where

$$a \in F^*:\ = F - \{0\} \text{ and } F(\sqrt{a}) \text{ is a quadratic extension of } F.$$

However some interesting progress has been done on some special cases, and there is partial information related to progress with a general case. (See e.g., [E-L], [L-Sm], [M-Sm], [M-W], [P-S-C-L] and [Szy].) Closely related to this problem are the cohomology rings of $G_F^{[3]}$ which can be viewed as invariants of Witt rings. (See [A-K-M].)

We set $L = F(\sqrt{a})$ such that $a \in F^*$ and $[L : F] = 2$. Then we have $F \subset L \subset F^{(2)}$. Also for any pro-2-extension K/F we denote by $\bar{K}/F$ or simply by $\bar{K}$ the Galois closure of K/F. In our paper we clarify "how much Galois theory" is needed to understand WL. More precisely we prove

Theorem 2. $\overline{L^{(3)}} \subset F^{(5)}$.

Therefore the Galois closure of the compositum of all extensions $L^{(3)}$ is a subfield of $F^{(5)}$. We also show that in general the Galois closure of the compositum of all extensions $L^{(3)}$ is not a subfield of $F^{(4)}$. (See Example 1 below.) Hence we see that this $F^{(5)}$ in Theorem 2 above cannot be replaced by $F^{(4)}$. Finally we shall observe in Proposition 1 below that $L^{(3)}$ is Galois over F and therefore the bar over $L^{(3)}$ in Theorem 2 may be omitted. We conclude our paper with the observation that the Galois group of the compositum of all $L^{(3)}$ where L runs over quadratic extensions of F, has an exponent of at most 8. Therefore this compositum is in general not equal to $F^{(5)}$. (See Proposition 2.)

We denote $H^1(G_F^{(2)}, \mathbb{F}_2)^{G_F^{[2]}}$ by $J_1(G_F^{(2)})$. Thus $J_1(G_F^{(2)})$ denotes the fixed elements of $H^1(G_F^{(2)}, \mathbb{F}_2)$ under the natural action of $G_F^{[2]}$. Here

$H^1(G_F^{(2)}, \mathbb{F}_2)$ is the first cohomology group of $G_F^{(2)}$ with coefficients in $\mathbb{F}_2$. Thus by Kummer theory $J_1(G_F^{(2)}) \cong ((F^{(2)})^*/((F^{(2)})^*)^2)^{G_F^{[2]}}$, where again the latter group denotes the fixed elements of the square class group of the multiplicative group of $F^{(2)}$. (See [A-T], Chapter 6, Section 2 for details on Kummer theory, and [G-M], page 100, for a more detailed justification of the isomorphism above. In the rest of the paper we identify the two isomorphic groups mentioned above.) Observe that $F^{(3)} := F^{(2)}(\sqrt{J_1(G_F^{(2)})})$ where the latter field means a compositum of all fields $F^{(2)}(\sqrt{\gamma}), \gamma \in J_1(G_F^{(2)})$. Similarly we have $F^{(n+1)} = F^{(n)}(\sqrt{J_1(G_F^{(n)})})$ where $J_1(G_F^{(n)})$ denotes the fixed elements of $H^1(G_F^{(n)}, \mathbb{F}_2)$ under the action of $G_F^{[n]}$ for each $n \geq 2$.

We also frequently use the following well-known fact. (See e.g. [War].)

Statement. *Suppose that K/F is a Galois extension, $G = Gal(K/F)$ is its Galois group and $a \in K^*$. Then $K(\sqrt{a})/F$ is Galois iff $\sigma(a)/a$ is a square in K^* for each $\sigma \in G$.*

We begin with recalling some of the basic inclusions between the fields that we are dealing with. We shall use the notation σ/K to mean a restriction of an automorphism σ of an overfield of K to K. We also use the symbol $[b]_K$ to denote a class of K^*/K^{*2} represented by b. Sometimes when there is no danger of confusion we simply write $[b]$ to denote $[b]_K$.

Lemma 1. *$L^{(2)} \subset F^{(3)}$.*

Proof. By the definition of $L^{(2)}$, it is enough to show that for each quadratic extension $L(\sqrt{b})/L$, $b \in L^*$, we have $L(\sqrt{b}) \subset F^{(3)}$. Consider any element $\sigma \in G_F^{[2]}$, we have $\sigma|_L \in Gal(L/F) = \{1, \tau\} \cong \mathbb{Z}/2$. If $\sigma|_L = 1$, then $\sigma(b) = b$ and $\sigma(b)/b = 1 \in (F^{(2)^*})^2$. If $\sigma|_L = \tau$, then $\sigma(b)/b = \sigma(b)b/b^2 = N_{L/F}(b)/b^2 \in (F^{(2)^*})^2$. Therefore $\sigma(b)/b \in (F^{(2)^*})^2$ in each case and consequently $[b] \in J_1(G_F^{(2)})$. This means that $F^{(2)}(\sqrt{b}) \subset F^{(3)}$. Because $L(\sqrt{b}) \subset F^{(2)}(\sqrt{b}) \subset F^{(3)}$, we have our desired inclusion. $\square$

Lemma 2. *$F^{(3)} \subset L^{(3)}$.*

Proof. By the definition of $F^{(3)}$, it is enough to show that for each $[b] \in J_1(G_F^{(2)})$ we have $F^{(2)}(\sqrt{b}) \subset L^{(3)}$. Consider any $\sigma \in Gal(L^{(2)}/L)$. We have $\sigma(b)/b = \sigma|_{F^{(2)}}(b)/b \in (F^{(2)^*})^2 \subset (L^{(2)^*})^2$, the first inclusion follows from the inclusion $[b] \in J_1(G_F^{(2)})$. Therefore $[b]_{L^{(2)}} \in J_1(G_L^{(2)})$ as well. Hence $F^{(2)}(\sqrt{b}) \subset L^{(2)}(\sqrt{b}) \subset L^{(3)}$ for each $[b] \in J_1(G_F^{(2)})$ which proves that $F^{(3)} \subset L^{(3)}$ as we claimed. $\square$

Therefore we have the tower $F \subset L \subset F^{(2)} \subset L^{(2)} \subset F^{(3)} \subset L^{(3)}$.

Let K/F be a Galois 2-extension such that $L \subset K$. This means that the Galois group of K/F is a pro-2-group. Let T/K be a quadratic extension such that T/L is Galois. Let $\overline{T}$ be the Galois closure of T over F.

Lemma 3. *There are only two possibilities:*

(1) *T is Galois over F. Then $T = \overline{T}$.*
(2) *T is not Galois over F. Then $\overline{T} = T(\sqrt{t})$ for some $t \in T^* - T^{*2}$.*

Proof. It is enough to show that if T is not Galois over F then $\overline{T}/F$ is a quadratic extension of T. Assume that T/F is not Galois. Set $T = K(\sqrt{k})$, $G = Gal(K/F)$ and $H = Gal(K/L)$. Because T/F is not Galois we have $\sigma(k)/k \notin (K^*)^2$ for some $\sigma \in G - H$. We set $E = T(\sqrt{\sigma(k)})$. We want to show that E is Galois over F. Consider any $\tau \in G_F$. If we can show that $\tau(E) \subset E$, we shall be done. Because K/F is Galois and $E = K[\sqrt{k},\ \sqrt{\sigma(k)}]$ as a ring, we see that it is enough to show that $\tau(\sqrt{k}))$, $\tau(\sqrt{\sigma(k)}) \in E$.

Consider first $\tau(\sqrt{k})$. We have $\tau(k) = \tau((\sqrt{k})^2) = (\tau(\sqrt{k}))^2$. Therefore $\tau(\sqrt{k})$ must be some square root of $\tau(k)$. If $\tau|_L = 1$, then $\tau|_K \in H$ and $\tau(k)/k \in (K^*)^2$. Therefore $\sqrt{\tau(k)} \in T$. Suppose now that $\tau|_L \neq 1$. Since $(\tau^{-1}\sigma)|_L = 1$, then $[\tau^{-1}\sigma(k)]_K = [k]_K$. Therefore $[\tau(k)]_K = [\sigma(k)]_K$. But this means that $\sqrt{\tau(k)} \in E$.

In a similar fashion, by exploiting the fact that the orbit of the element $[k]$ of $K^*/(K^*)^2$ under the action of G has 2 elements we prove that $\tau(\sqrt{\sigma(k)}) \in E$ for each element $\tau \in G$. Therefore E/F is Galois. Since T/F is not Galois and since $[E : T] = 2$. Therefore we see $E = \bar{T}$. Our proof is complete. $\square$

Lemma 4. $(F^{(4)} \cap L^{(3)})/F$ *is Galois.*

Proof. Both extensions $F^{(4)}$ and $L^{(3)}$ are Kummer extensions of $F^{(3)}$ of exponent at most 2. From our inductive definition of $F^{(4)}$ using $F^{(3)}$ we see that each subextension between $F^{(3)}$ and $F^{(4)}$ is Galois over F. In particular, $L^{(3)} \cap F^{(4)}$ is Galois over F. $\square$

Proof of Theorem 2. By the definition of $L^{(2)}$ and Lemma 1, it is enough to show that for each $\gamma \in L^{(2)^*}$ such that $L^{(2)}(\sqrt{\gamma})/L$ is Galois; hence we have a Galois closure of $(F^{(4)} \cap L^{(3)})(\sqrt{\gamma})$ over F, which is contained in $F^{(5)}$. (Observe that $L^{(2)} \subset F^{(4)} \cap L^{(3)}$ and therefore $L^{(2)}(\sqrt{\gamma}) \subset (F^{(4)} \cap L^{(3)})\sqrt{\gamma}$.) If $\sqrt{\gamma} \in F^{(4)} \cap L^{(3)}$, then $L^{(2)}(\sqrt{\gamma}) \subset F^{(4)} \subset F^{(5)}$. Otherwise, we can apply Lemma 3 to the following situation: $K = F^{(4)} \cap L^{(3)}$ and $T = (F^{(4)} \cap L^{(3)})(\sqrt{\gamma})$. Indeed K/F is Galois by Lemma 4, and since $L^{(2)}(\sqrt{\gamma})$ is Galois over L and $L^{(2)} \subset F^{(4)} \cap L^{(3)}$, we see that T is also Galois over L. We also use notation employed in the proof of Lemma 3; in particular $\sigma \in G := Gal(K/F)$ and $\sigma/L \neq 1_L$. For the sake of ease of notation we denote by σ also its restriction to $F^{(3)}$. Then we obtain $\overline{T} = T(\sqrt{\gamma}, \sqrt{\sigma(\gamma)})$. Moreover we have $\gamma \in L^{(2)} \subset F^{(3)}$, so $\gamma\sigma(\gamma) \in F^{(3)}$. We have $\tau(\gamma)\gamma^{-1} \in (L^{(2)^*})^2$ for each τ which fixes L. Therefore for each $\tau \in Gal(K/L)$ restricted to $F^{(3)}$, we have $\tau\sigma = \sigma\tau'$, $\tau' \in G_F^{[3]}$ and $\tau'|_L = 1$ and

$$\tau(\gamma\sigma(\gamma)) = \tau(\gamma)\sigma(\tau'(\gamma)) \equiv \gamma\sigma(\gamma) \mod (F^{(3)^*})^2 .$$

On the other hand, if $\delta = \sigma\tau'$, where $\tau' \in Gal(F^{(3)}/L)$ we see:

$$\delta(\gamma\sigma(\gamma)) = \sigma(\tau'(\gamma))\sigma\tau'\sigma(\gamma) \equiv \sigma(\gamma)\gamma \mod (F^{(3)^*})^2 .$$

Therefore we see that $F^{(3)}(\sqrt{\gamma\sigma(\gamma)}) \subset F^{(4)}$. But this means that $\gamma \equiv \sigma(\gamma) \mod (F^{(4)^*})^2$ and therefore $\gamma \in J_1(G_F^{(4)})$. Thus we obtain $\overline{L^{(3)}} \subset F^{(5)}$ as we claimed. □

Remark 1. Observe that in the proof above we also showed the following statement:

Let γ be an element of $L^{(2)*}$ such that $L^{(2)}(\sqrt{\gamma})/L$ is a Galois extension. Let also $\sigma \in G_F^{[3]} - Gal(F^{(3)}/L)$. Then the Galois closure of the field extension $L^{(3)} \cap F^{(4)}(\sqrt{\gamma})/F$ is a field $T = L^{(3)} \cap F^{(4)}(\sqrt{\gamma}, \sqrt{\sigma(\gamma)})$ and there is a tower of field extensions which are Galois over F: $L^{(3)} \cap F^{(4)} \subset L^{(3)} \cap F^{(4)}(\sqrt{\gamma\sigma(\gamma)}) \subset T$. Moreover $L^{(3)} \cap F^{(4)}(\sqrt{\gamma\sigma(\gamma)}) \subset F^{(4)}$ and $T \subset F^{(5)}$.

Corollary 1. *The compositum of all W-fields of all quadratic extensions of F is in $F^{(5)}$.*

Observe also the following simple corollary of our discussion.

Proposition 1. *Suppose that L/F is any quadratic extension of F. Then $L^{(3)}/F$ is a Galois extension.*

Proof. Suppose that $\tau \in G_F$. It is sufficient to prove that $\tau(L^{(3)}) \subset L^{(3)}$. First observe that $\tau(L^{(2)}) \subset L^{(2)}$ as $\sqrt{\tau(l)} \in L^{(2)}$ for each $l \in L^*$.

Now let $\gamma \in L^{(2)*}$ be an element of $L^{(2)*}$ such that $L^{(2)}(\sqrt{\gamma})/L$ is Galois. Then for each $\delta \in Gal(L^{(2)}/L)$ we have $\delta(\gamma)\gamma \in (L^{(2)})^{*2}$. Now let us consider two cases. In the second case we use the fact that G_L is the normal subgroup of G_F of index 2.

Case 1 τ/L is an identity automorphism. Then for each

$$\omega \in Gal(L^{(2)}/L) \text{ we have } [\omega\tau(\gamma)] = [\tau(\gamma)] = [\gamma] \text{ in } (L^{(2)})^*/(L^{(2)*})^2.$$

Case 2 τ/L is a nontrivial automorphism. Then for each $\omega \in Gal(L^{(2)}/L)$ we can find $\omega_1, \omega_2 \in G_L$ such that $\omega_1 \mid L^{(2)} = \omega$ and $\tau\omega_2 = \omega_1\tau$. Therefore $[\omega\tau(\gamma)] = [\omega_1\tau(\gamma)] = [\tau\omega_2(\gamma)] = [\tau(\gamma)]$ in $L^{2*}/(L^{(2)*})^2$.

Hence in both cases we see that $\tau(\gamma) \in J_1(G_L^{(2)})$ and therefore $L^{(2)}(\sqrt{\tau(\gamma)})/L$ is a Galois extension. From the fact that $L^{(3)}$ is the compositum of all fields $L^{(2)}(\sqrt{\gamma}), \gamma \in L^{(2)*}$ such that $L^{(2)}(\sqrt{\gamma})/L$ is Galois, we see that $\tau(L^{(3)}) \subset L^{(3)}$. Our proof is now completed. □

The following is an example of $L^{(3)} \not\subseteq F^{(4)}$. Here we shall employ the usual notation: $\mathbb{R}$ - the field of all real numbers - and $\mathbb{C}$ - the field of all complex numbers.

Example 1. Let $F = \mathbb{R}(t)$. Then $L{:} = F(\sqrt{-1}) = \mathbb{C}(t)$. Since $\mathbb{C}[t]$ is a unique factorization domain, then $[t+2i] \neq [1], [t-i] \neq [1] \in L^*/L^{*2}$. Also $[t+2i]$ and $[t-i]$ are linearly independent in L^*/L^{*2}. It is well-known that $H^2(\mathbb{C}(t), \mathbb{F}_2) = 0$. (See e.g. [Rib], page 70 and page 217.) Then there exists a Galois extension K/L such that $Gal(K/L) \cong D_4$ and $\mathbb{Z}/4\mathbb{Z} \cong Gal(K/L(\sqrt{(t+2i)(t-i)}))$.

We denote this D_4-extension of L by K. We also denote

$$\mathbb{C}(\sqrt{t-i}, \sqrt{t+2i}) \text{ by } E.$$

Observe that

$$F^{(2)} = \mathbb{C}(\sqrt{t-r}, \sqrt{t^2+bt+c}, b^2-4c<0, b, c, r \in \mathbb{R}).$$

Claim 1. $E \cap F^{(2)} = \mathbb{C}(t)$.

Proof. Set V as the subspace of L^*/L^{*2} generated by $[t-r], [t^2+bt+c], r, b, c \in \mathbb{R}$ such that $b^2-4c<0$. In order to prove our claim, it is enough to show that $[t-i]$ and $[t+2i]$ generate a vector space W of L^*/L^{*2} such that $W \cap V = \{0\}$. Assume that some element; say $[(t-i)(t+2i)] \in W \cap V$. Then

$$(t-i)(t+2i)P(t)^2 = \prod_r (t+r) \prod_{b,c} (t^2+bt+c)Q(t)^2$$

for some $P(t), Q(t) \in \mathbb{C}[t]$ and some finite set of linear factors $t + r$ and a finite set of quadratic factors $(t^2 + bt + c)$ such that $b^2 - 4c < 0$. This implies that $(t - i)$ must divide some $t^2 + bt + c$. However if $t - i \mid t^2 + bt + c$, then $t^2 + bt + c = (t - i)(t + i) = t^2 + 1$. Hence we see that $t + i$ appears on the right hand side of our equation above, in odd power, but $t + i$ appears on the left hand side of our equation above, in even power - a contradiction. Hence $E \cap F^{(2)} = L$. □

Claim 2. $K \cap F^{(2)} = L$.

Proof. Indeed $K \cap F^{(2)} \subset L^{ab}:$ = the maximal abelian subextension of K over L. (Because $F^{(2)}/L$ is an abelian extension.) Hence $K \cap F^{(2)} \subset L^{ab} = E$. By *Claim 1*, we obtain $K \cap F^{(2)} \subset E \cap F^{(2)} = \mathbb{C}(t) = L$.

By Claim 2, $Gal(KF^{(2)}/F^{(2)}) = Gal(K/K \cap F^{(2)}) \cong D_4$. Observe however that $F^{(4)}/F^{(2)}$ is an abelian extension. Indeed one can check easily that $[G_F^{(2)}, G_F^{(2)}] \subset G_F^{(4)}$. (See e.g. Chapter 7.15 in [Ko].) Then $KF^{(2)} \not\subseteq F^{(4)}$. On the other hand, $KF^{(2)} \subset L^{(3)}$. Hence $L^{(3)} \not\subseteq F^{(4)}$. Our Example 1 is completed. □

Set $(\sqrt{/}F)^{(3)}$:= the compositum of all field extensions $L^{(3)}/F$, where L is a quadratic extension of F, and $Gal((\sqrt{/}F)^{(3)}/F):\ = G^{[3]}_{\sqrt{/}F}$. From Proposition 1 we know that $(\sqrt{/}F)^3$ is a Galois extension. We proved that $(\sqrt{/}F)^{(3)} \subset F^{(5)}$. Observe however that in general the exponent of $G_F^{[5]} = Gal(F^{(5)}/F)$ is 16 while the exponent of $Gal((\sqrt{/}F)^{(3)}/F)$ is in general just 8. More precisely, we have the proposition below. Recall that F is quadratically closed if $F_q = F$ and F is a Euclidean field if F_q^{*2} is an ordering of F_q and $F_q^* = F_q^{*2} \cup -F_q^{*2}$. In the proof of the proposition below we consider pythagorean fields. Recall that a field F is pythagorean if each sum of two squares is again a square. It is well known that if F is a pythagorean field then $F(\sqrt{-1})$ contains all of the roots of unity of an order with a power of 2. (See e.g. [Be2], page 83.)

Proposition 2.

1. *If F is quadratically closed, then $(\sqrt{/}F)^{(3)} = F = F^{(n)}$ for each $n \in \mathbb{N}$.*
2. *If F is a Euclidean field then $(\sqrt{/}F)^{(3)} = F^{(2)} = F^{(n)}$ for each $n \in \mathbb{N}$, $n \geq 2$.*
3. *If F is neither a quadratically closed nor a Euclidean field, then $(\sqrt{/}F)^{(3)} \subset F^{(5)}$ and the exponent of $G_F^{[5]}$ is* 16 *while the exponent of $Gal((\sqrt{/}F)^{(3)}/F)$ is 8. In particular $(\sqrt{/}F)^{(3)} \neq F^{(5)}$.*

Proof. If F is a Euclidean field then $F_q = F(\sqrt{-1})$. (See [Be1], Satz 3.) Therefore both cases 1 and 2 are clear. Now consider the case when

F is neither quadratically closed nor a Euclidean field. Then from the definition of $F^{(5)}$ we see that $G_F^{[5]}$ has an exponent of at most 16. If F is not a pythagorean field, then there exists an element $a \in F^* - F^{*2}$ which is a sum of two squares. Then $F(\sqrt{a})$ can be imbedded in a Galois extension L/F such that $Gal(L/F) \cong \mathbb{Z}/4\mathbb{Z}$. Then it is well-known (see e.g. [Ku-Le], Theorem 2) that for each $n \in \mathbb{N}$ a Galois extension K/F exists such that $Gal(K/F)$ is $\mathbb{Z}/2^n\mathbb{Z}$. In particular a Galois extension K/F exists such that $Gal(K/F) = \mathbb{Z}/16\mathbb{Z}$. Then $K \subset F^{(5)}$ and any element $\sigma \in G_F^{[5]}$ which restricts to a generator of $Gal(K/F)$ has an order of 16. Hence the exponent of $G_F^{[5]}$ is 16.

On the other hand if F is a pythagorean field which is neither quadratically closed nor a Euclidean field, we can pick an element $a \in F^*$ such that the set $\{[a], [-a]\}$ is linearly independent over $\mathbb{F}_2$. In particular we see that $[a] \neq [1]$ and $a \notin -4F^{*4}$. Therefore from the well-known theorem (see e.g. [Lan], Theorem 9.1) we see that the polynomial $X^{16} - a$ is irreducible over F. Since F is a pythagorean field we know that $F(\sqrt{-1})$ contains all $2^n - th$ roots of unity, $n \in \mathbb{N}$. Therefore the splitting field of the polynomial $f(X) = X^{16} - a$ is $N = F(\sqrt{-1}, \sqrt[16]{a})$ where $\sqrt[16]{a}$ means any element $b \in F_q^*$ such that $b^{16} = a$.

Observe that from Kummer theory we know that $Gal(N/F(\sqrt{-1})) \cong \mathbb{Z}/16\mathbb{Z}$ and that we can choose as a generator of $Gal(N/F(\sqrt{-1}))$ an element τ such that $\tau(\sqrt[16]{a}) = \zeta_{16}\sqrt[16]{a}$ where ζ_{16} is a primitive 16th root of unity. Observe that $F(\sqrt{-1}, \sqrt[4]{a}) \subset F^{(3)}$ and therefore $F(\sqrt{-1}, \sqrt[16]{a}) \subset F^{(5)}$. Therefore we see that for each $\delta \in G_F^{[5]}$ such that $\delta(\sqrt{-1}) = \sqrt{-1}$ and $\delta/N = \tau$ we have an order of δ that is 16. Thus again we see that the exponent of $G_F^{[5]}$ is 16.

Now consider $L^{(3)}$, for any $L = F(\sqrt{a}), a \in F^* - F^{*2}$ and any $\sigma \in G_F^{[5]}$. Then $\sigma^2 \in Gal(F^{(5)}/L)$ and we can consider the restriction of σ^2 to $L^{(3)}/L$. Since each element of $Gal(L^{(3)}/L)$ has an order of at most 4, we see that $\sigma^8/L^{(3)}$ is the identity automorphism of $L^{(3)}$. Because $(\sqrt{\ }/F)^{(3)}$ is the compositum of all extensions $L^{(3)}/L$ over F we see that the exponent of $Gal((L/F)^{(3)}/F)$ is at most 8.

To show that the exponent of $Gal((\sqrt{\ }/F)^3/F)$ is exactly 8, we shall proceed in the same fashion as in the beginning of our proof.

Namely if F is not a pythagorean field, we see again that a Galois extension K/F exists such that $Gal(K/F) \cong \mathbb{Z}/8\mathbb{Z}$. Let L be the unique quadratic subextension of K/F. Then $Gal(K/L) \cong \mathbb{Z}/4\mathbb{Z}$ and we see that $K \subset L^{(3)}$. Now let σ be any element of $Gal((\sqrt{\ }/F)^3/F)$

such that its restriction to K/F is a generator of $Gal(K/F)$. Then the order of σ is at least 8, and we can conclude that the exponent of our Galois group $Gal((\sqrt{/}F)^3/F)$ is 8.

If F is a pythagorean field which is neither a quadratically closed nor a Euclidean field, we can again find an element $a \in F^*$ such that the polynomial $g(X) = X^8 - a$ is irreducible over F. Then the field extension $N = F(\sqrt{-1}, \sqrt[8]{a})$ is the splitting field of $g(X)$ and $Gal(N/F(\sqrt{-1})) \cong \mathbb{Z}/8\mathbb{Z}$. Also observe that N is the Galois closure of $L(\sqrt[4]{(\sqrt{a})})$ over F where $L = F(\sqrt{a})$. Therefore $N \subset (\sqrt{/}F)^{(3)}$. Thus we can again conclude that the exponent of $Gal((\sqrt{/}F)^{(3)}/F)$ is 8. $\square$

References

[A-K-M] A. Adem, D. Karagueuzian and J. Mináč, *On the cohomology of Galois groups determined by Witt rings,* Advances in Math. **148** (1999), 105–160.

[A-T] E. Artin and J. Tate, *Class Field Theory,* Addison-Wesley Publishing Company (1976), second printing.

[Be1] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern,* J. reine angew. Math. **268/269** (1974), 41–52.

[Be2] E. Becker, *Hereditarily-Pythagorean Fields and Orderings of Higher Level,* Instituto De Matemática Pura E Aplicada, Rio De Janeiro, Monographias De Matemática No. 29, (1978).

[E-L] R. Elman and T.-Y. Lam, *Quadratic forms under algebraic extensions,* Math. Ann. **219** (1976), 21–42.

[G-M] W. Gao and J. Mináč, *Milnor conjecture and Galois theory I,* Fields Institute Communications, AMS **16** (1997), 95–110.

[Ko] H. Koch, *Galoissche Theorie Der p-Erweiterungen,* Grundlehren der mathematische Wissenchaften, Springer-Verlag, 1970.

[Ku-Le] W. Kuyk and H. W. Lenstra, Jr., *Abelian extensions of arbitrary fields,* Math. Ann. **216** (1975), 99–104.

[La] T.-Y. Lam, *The Algebraic Theory of Quadratic Forms,* The Benjamin Cummings Publishing Company, Inc., second printing (1980).

[Lan] S. Lang, *Algebra,* Addison-Wesley Publishing Company, Third Edition, 1993.

[L-Sm] D. B. Leep and T. L. Smith, *Multiquadratic extensions, rigid fields and pythagorean fields,* to appear in Bull. Lon. Math. Soc.

[M-Sm] J. Mináč and T. Smith, *W-groups under quadratic extensions of fields,* Can. J. Math. **52** (2000), 833–848.

[M-Sp] J. Mináč and M. Spira, *Witt rings and Galois groups,* Annals of Math. **144** (1996), 35–60.

[M-W] J. Mináč and A. Wadsworth, *The u-invariant of Algebraic Extensions, K-theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras,* eds. B. Jacob and A. Rosenberg, Proc. Symp. Pure Math. **58,2** (1995), 333–358.

[N-S-W] J. Neukirch, A. Schmidt and K. Winberg, *Cohomology of Number Fields,* Springer-Verlag, vol. **323** (2000).

[P-S-C-L] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witts with global fields,* Contemporary Math. vol. **155** (1994), 365–387. (Recent advances in real algebraic geometry and quadratic forms, edited by B. Jacob, T.-Y. Lam and R. O. Robson.)

[Rib] L. Ribes, *Introduction to profinite groups and Galois cohomology,* Queen's Papers in Pure and Applied Mathematics **24** (1970).

[Sch] W. Scharlau, *Quadratic and Hermitian Forms,* Springer-Verlag, 1985.

[Sh] S. Shatz, *Profinite groups, arithmetic, and geometry,* Ann. of Math. Studies vol. **67**, Princeton University Press and University of Tokyo Press, 1972.

[Szy] K. Szymiczek, *Witt equivalence of global fields, II: relative quadratic extensions,* Trans. of the AMS **343** (1994), 277–303.

[War] R. Ware, *When are Witt rings group rings?,* Pac. J. Math., **76** (1978), 541–564.

537 Bellevue Way SE, Apt. 110, Bellevue, WA 98004
E-mail address: wgao@sprintmail.com

The University of Western Ontario, Department of Mathematics, Middlesex College, London, Ontario, Canada N6A 5B7
E-mail address: minac@uwo.ca