PACIFIC JOURNAL OF MATHEMATICS
Vol. 158, No. 1, 1993

WITT RINGS UNDER ODD DEGREE EXTENSIONS

ROBERT W. FITZGERALD

For a separable odd degree field extension K/F the kernel of a Scharlau transfer of Witt rings $s_*: WK \to WF$ is a WF-module. We compute the prime ideals attached to ker s_* and deduce that WK is not a projective WF-module if an ordering on F extends uniquely to K. An example shows WK may be a free WF-module if F is real and no ordering extends uniquely. For non-real, non-rigid F we show that K/F Galois and WK noetherian implies WK is not a projective WF-module.

If K/F is a finite extension of fields (characteristic not 2) then each non-trivial linear functional $s: K \to F$ induces a Scharlau transfer $s_*: WK \to WF$ on the Witt rings. When $K = F(\sqrt{d})$ the kernel and image of s_* are well known. We restrict our attention to separable odd degree extensions, where s_* is surjective but little is known of ker s_*. The map induced by inclusion $r_*: WF \to WK$ is injective and we view WF as a subring of WK. Then WK and ker s_* are WF-modules and our approach is module theoretic.

WF need not be noetherian and ker s_* need not be finitely generated over WF. So the usual theory of prime ideals associated to modules must be replaced by the notion of attached primes (in the sense of Dutton). We show no $P(\alpha, p)$ is attached to ker s_*, $P(\alpha)$ is attached iff α has more than one extension to K and IF is attached iff $W_tK \cap$ ker $s_* \neq 0$. As a consequence, $WK = WF$ iff each ordering on F extends uniquely to K and $W_tK \cap \ker s_* = 0$. Another consequence is that WK is finitely generated over WF if F has only finitely many orderings and IF is not attached to ker s_*.

The main result deduced from the work on attached primes is that WK is not a projective WF-module if some ordering on F extends uniquely to K. WK may be projective, however, if F is real and no ordering extends uniquely. We present an example where K/F is Galois, F is real, both WK and WF noetherian rings and WK is a free WF-module. When F is non-real and non-rigid we show the same conditions (K/F Galois, WK and WF noetherian) implies WK is not a free WF-module. Weaker results hold under fewer restrictions on K/F.

The first section gives basic results and several examples. The last section concerns the possible values of $[G(K) : G(F)]$ when this is finite (here $G(E) = E^{\cdot}/E^{\cdot 2}$). Two sample results: If K/F is Galois and $[K : F] = p$ a prime then p divides $[G(K) : G(F)] - 1$. If K/F has a real normal closure then $[K : F] \leq [G(K) : G(F)]$.

$\operatorname{Hom}(K, F)^{\cdot}$ denotes the non-trivial linear functionals $s : K \to F$. The set of orderings on a field E is denoted X_E. If $\alpha \in X_F$ then $X(\alpha) = \{\beta \in X_K | \beta|F = \alpha\}$. For $\alpha \in X_F$ and an odd prime p we write $P(\alpha, p)$ for $\{r \in WF | \operatorname{sgn}_\alpha r \equiv 0 \pmod p\}$ and $P(\alpha) = \{r \in WF | \operatorname{sgn}_\alpha r = 0\}$. These ideals, with $IF = \{r \in WF | \dim r \equiv 0 \pmod 2\}$, are the prime ideals of WF.

W_tF denotes the torsion part of WF. The height of F, $h(F)$, is the least positive k such that $2^k \cdot W_tF = 0$ (or infinity if no such k exists). If R_1 and R_2 are Witt rings then the fiber product $R_1 \sqcap R_2 = \{(r_1, r_2) | r_i \in R_i, \dim r_1 \equiv \dim r_2 \pmod 2\}$ is again a Witt ring. If C is a group of exponent two then the group ring $R_1[C]$ is again a Witt ring.

1. Basic facts.

DEFINITION. (i) $m(K/F) = \bigcap \ker s_*$, over all $s \in \operatorname{Hom}(K, F)^{\cdot}$.
(ii) $M(K/F) = \sum \ker s_*$, over all $s \in \operatorname{Hom}(K, F)^{\cdot}$.

LEMMA 1.1. *Let* $s \in \operatorname{Hom}(K, F)^{\cdot}$.

(1) $\ker s_*$ *is a* WF*-submodule of* WK.
(2) *If* $t \in \operatorname{Hom}(K, F)^{\cdot}$ *then* $\ker s_* = \langle z \rangle \ker t_*$ *for some* $z \in K^{\cdot}$.
(3) $m(K/F) = [\ker s_* : WK]$ *is an ideal of* WK.
(4) $M(K/F)$ *is the ideal generated by* $\ker s_*$.
(5) *There exists* $t \in \operatorname{Hom}(K, F)^{\cdot}$ *with* $t_*\langle 1 \rangle = \langle 1 \rangle$.
(6) *If* $s_*\langle 1 \rangle = \langle 1 \rangle$ *then* $WK \approx WF \oplus \ker s_*$.
(7) *If* $s_*\langle 1 \rangle = \langle 1 \rangle$ *then* $\ker s_*$ *is generated* (*over* WF) *by* $\{\langle x \rangle - s_*\langle x \rangle | x \in K^{\cdot}\}$.

Proof. (1) s_* is additive and if $\phi \in \ker s_*$ and $r \in R$ then $s_*(r\phi) = rs_*(\phi) = 0$. Thus $\ker s_*$ is a WF-submodule of WK.

(2) There exists $z \in K^{\cdot}$ such that $s(x) = t(zx)$ for all $x \in K$. Then $s_*(\phi) = t_*(\langle z \rangle \phi)$ for all $\phi \in WK$ and so $\ker s_* = \langle z \rangle \ker t_*$.

(3) Let $\phi \in m(K/F)$ and $z \in K^{\cdot}$. Define $t(x)$ to be $s(zx)$ for all $x \in K$. Then $\phi \in \ker t_* = \langle z \rangle \ker s_*$. Since z was arbitrary, we have $\phi \in [\ker s_* : WK]$. Conversely, if $\phi \in [\ker s_* : WK]$ then for every $z \in K^{\cdot}$, $\langle z \rangle \phi \in \ker s_*$ and $\phi \in \langle z \rangle \ker s_* = \ker t_*$, for some

$t \in \mathrm{Hom}(K/F)^{\cdot}$. Thus $\phi \in m(K/F)$. Clearly $[\ker s_* : WK]$ is an ideal.

(4) $M(K/F) = \sum \ker t_* = \sum \langle z\rangle \ker s_*$ is the ideal generated by $\ker s_*$.

(5) We may write $K = F(x)$ since K is separable over F. Take $t \in \mathrm{Hom}(K, F)^{\cdot}$ with $t(1) = 1$ and $t(x) = \cdots = t(x^{n-1}) = 0$ $(n = [K:F])$. Then $t_*\langle 1\rangle = \langle 1\rangle$ by [**15**, II 5.8].

(6) If $s_*\langle 1\rangle = \langle 1\rangle$ then the exact sequence $0 \to \ker s_* \to WK \to WF \to 0$ splits. This also proves (7). □

There are few examples of Witt rings under odd degree extensions in the literature. We present several to illustrate the range of possible $m(K/F)$ and $M(K/F)$.

EXAMPLES. (1) The definitions of $m(K/F)$ and $M(K/F)$ make sense for any finite extension $F \subset K$. Consider $K = F(\sqrt{d})$ and define $s : K \to F$ by $s(1) = 0$, $s(\sqrt{d}) = 1$. Then $\ker s_* = r_*(WF)$. Since $\langle 1\rangle \in \ker s_*$ we have $M(K/F) = WK$. Also, $m(K/F) = \mathrm{ann}_{WF}(\mathrm{ann}_{WF}\langle 1, -d\rangle) \otimes K$ by [**5**, 2.12]. Note that if WF is Gorenstein (e.g., a group ring extension of a Witt ring of local type) then $\mathrm{ann}_{WF}(\mathrm{ann}_{WF}\langle 1, -d\rangle) = (\langle 1, -d\rangle)$ and hence $m(K/F) = 0$ (cf. [**9**]).

(2) Let $F = \mathbf{Q}_2$ and $K = \mathbf{Q}_2(e)$ where e is a root of $x^3 + 2$. Then $K^{\cdot}/K^{\cdot 2}$ may be represented by the group generated by $\langle 2\rangle$, $\langle 3\rangle$, $\langle 5\rangle$, $\langle\alpha\rangle$, $\langle\beta\rangle$ where $\alpha = 2 + e^2$ and $\beta = 1 + e^2$. Define $s : K \to F$ by $s(1) = 1$, $s(e) = 0$ and $s(e^2) = 0$. Then $s_*\langle 1\rangle = \langle 1\rangle$, $s_*\langle\alpha\rangle = \langle 3\rangle$, $s_*\langle\beta\rangle = \langle 5\rangle$ and $s_*\langle\alpha\beta\rangle = \langle 2\rangle\langle 1, -7, -14\rangle \simeq \langle 2\rangle\langle 1, 1, 2\rangle \simeq \langle 1, 1, 1\rangle$ (see [**15**, p. 188]). Set $\rho = 4\cdot\langle 1\rangle$ and $\chi = 3\cdot\langle 1\rangle$.

We verify that $m(K/F) = 0$. Let $\phi = r_1 + r_2\langle\alpha\rangle + r_3\langle\beta\rangle + r_4\langle\alpha\beta\rangle \in m(K/F)$ with $r_i \in WF$. From $s_*\phi = 0$, $s_*\langle\alpha\rangle\phi = 0$ and $s_*\langle\beta\rangle\phi = 0$ we obtain:

$$\begin{aligned} r_1 + \langle 3\rangle r_2 + \langle 5\rangle r_3 + \chi r_4 &= 0, \\ \rho r_3 + \rho r_4 &= 0, \\ \rho r_2 + \rho r_4 &= 0. \end{aligned}$$

The last two equations imply $\dim r_2 \equiv \dim r_3 \equiv \dim r_4 \pmod 2$. The first equation yields $\phi = \langle\alpha, -3\rangle r_2 + \langle\beta, -5\rangle r_3 + (\langle\alpha\beta\rangle - \chi) r_4$. When all r_i $(2 \le i \le 4)$ are even dimensional then $\phi \in I^2K$. When all r_i are odd dimensional then $d(\phi) = 1$ and again $\phi \in I^2K$. But $I^2K = \{0, \rho\}$ and $s_*(\rho) = \rho \neq 0$. Thus $\phi = 0$.

Lastly, $M(K/F) = (\langle 1, -3\alpha\rangle, \langle 1, -5\beta\rangle)$. Namely, $M(K/F)$ is generated by $\langle 1, -3\alpha\rangle$, $\langle 1, -5\beta\rangle$ and $\chi - \langle\alpha\beta\rangle$. Now $\rho \in \langle 1, -3\alpha\rangle IK$ and $\chi - \langle\alpha\beta\rangle = \rho - \langle 1, \alpha\beta\rangle = \rho - \langle 15\rangle(\langle 1, -3\alpha\rangle + \langle 3\alpha\rangle\langle 1, -5\beta\rangle)$.

(3) Let $F = \mathbf{C}(x)$. It is easy to see $t^3 + xt + x$ is irreducible over F. Let α be a root and let $K = F(\alpha)$. Pick $s \in \operatorname{Hom}(K, F)^{\cdot}$ with $s_*\langle 1\rangle = \langle 1\rangle$. Now for all $u \in K$, $s_*\langle u\rangle = \langle N_{K/F}(u)\rangle + \phi$, for some $\phi \in I^2K = 0$. We are using here that K is a C_1-field for every finite extension [**15**, II 15.2]. So $s_*\langle u\rangle = \langle N_{K/F}(u)\rangle$, and s_* is a ring homomorphism. Thus $m(K/F) = \ker s_* = M(K/F) = \{\langle 1, -u\rangle | N_{K/F}(u) = 1\}$.

This is the only example (of the three) for which $m(K/F) \neq 0$. To verify this it is enough to show $-x\alpha \notin K^2$ as $N_{K/F}(-x\alpha) \in F^2$. But if $-x\alpha = (a+b\alpha+c\alpha^2)^2$ then $b = a^2/2cx$ and $(a/c)^4 + 8(a/c)x^2 = 4x^3$. However $t^4 + 8x^2t - 4x^3$ has no roots in F.

(4) In §3 an extension $F \subset K$ will be constructed with $WF \approx \mathbf{Z}$ and $WK \approx \mathbf{Z}^3$. Here $\dot{F}/\dot{F}^2 = \{\pm 1\}$ and $\dot{K}/\dot{K}^2 = \{\pm 1, \pm\alpha, \pm\beta, \pm\alpha\beta\}$. Here α corresponds to $(1, -1, -1) \in \mathbf{Z}^3$ and β corresponds to $(-1, 1, -1)$. There is, by a later result (1.4), an $s \in \operatorname{Hom}(K, F)^{\cdot}$ with $s_*\langle 1\rangle = \langle 1\rangle$, $s_*\langle\alpha\rangle = \langle 1\rangle$, $s_*\langle\beta\rangle = \langle 1\rangle$ and $s_*\langle\alpha\beta\rangle = -3\langle 1\rangle$. Thus ker s_* is generated by $\langle 1, -\alpha\rangle$, $\langle 1, -\beta\rangle$, $\langle 1, 1, 1, \alpha\beta\rangle$. Using $\langle 1, \alpha, \beta, \alpha\beta\rangle = 0$ it is straightforward to show $m(K/F) = 0$ and $M(K/F) = (\langle 1, -\alpha\rangle, \langle 1, -\beta\rangle)$.

For any field E let $G(E) = E^{\cdot}/E^{\cdot 2}$. Set $U = \{\langle x\rangle \in G(K) | N_{K/F}(x) \in \dot{F}^2\}$.

LEMMA 1.2. $G(K) \approx U \times G(F)$.

Proof. The sequence $1 \to U \to G(K) \to G(F) \to 1$ is exact and splits since for $a \in F^{\cdot}$ we have $N_{K/F}(a) = a^m$ where $m = [K : F]$ is odd and so $N_{K/F}(a) \in a\dot{F}^2$. □

LEMMA 1.3. *If $s_*\langle 1\rangle = \langle 1\rangle$ and $\dim(s_*\langle x\rangle)_{an} = 1$ for some $x \in K^{\cdot}$ then $s_*\langle x\rangle = \langle N_{K/F}(x)\rangle$.*

Proof. Suppose $[K : F] = 2k + 1$. Then $s_*\langle 1\rangle \simeq k \cdot \langle 1, -1\rangle + \langle 1\rangle$ so that $\det(s_*\langle 1\rangle) = (-1)^k$. Hence $\det(s_*\langle x\rangle) = (-1)^k N_{K/F}(x)$ [**15**, II 5.12] and so $s_*\langle x\rangle = \langle N_{K/F}(x)\rangle$. □

PROPOSITION 1.4. *Let $s \in \operatorname{Hom}(K, F)^{\cdot}$ with $s_*\langle 1\rangle = \langle 1\rangle$. Set $L(s) = \{\langle y\rangle \in G(K) \mid N_{K/F}(y) \in F^2$ and $s_*\langle y\rangle = \langle 1\rangle\}$. Then:*

(1) *$\{\langle 1, -y\rangle | y \in L(s)\} \subset \ker s_*$, and*

(2) *$L(s)L(s) = U$.*

Proof. (1) is clear as is the inclusion $L(s)L(s) \subset U$. Suppose then that $\beta \in U$ and set $E = F(\beta)$. Define $v: E \to F$ by $v(1) = 1$ and $v(\beta^i) = 0$, $1 \le i < [E : F]$. Then $v_*\langle 1\rangle = \langle 1\rangle$ and $v_*\langle\beta\rangle = \langle 1\rangle$ **[15**, II 5.8] (note $N_{E/F}(\beta) = 1$ as $1 = N_{K/F}(\beta) = N_{E/F}(N_{K/E}(\beta)) = N_{E/F}(\beta)$, modulo squares). Pick any $u \in \mathrm{Hom}(K, E)^{\cdot}$ with $u_*\langle 1\rangle = \langle 1\rangle$. Then $(vu)_*\langle 1\rangle = \langle 1\rangle$ and $(vu)_*\langle\beta\rangle = v_*(u_*\langle\beta\rangle) = v_*\langle\beta\rangle = \langle 1\rangle$, as $\beta \in E$. Thus $\{1, \beta\} \subset L(vu)$. Now there exists $z \in K^{\cdot}$ with $vu(x) = s(zx)$ for all $x \in K$. Note $\langle 1\rangle = (vu)_*\langle 1\rangle = s_*\langle z\rangle$ so that $N_{K/F}(z) \in F^2$ by (1.3). Also $zL(vu) = L(s)$. Thus $z, z\beta \in L(s)$ and $\beta \in L(s)L(s)$. □

PROPOSITION 1.5. *$m(K/F) \subset W_tK$, the torsion ideal of WK.*

Proof. If $x \in K^{\cdot}$ and $\phi \in m(K/F)$ then $\mathrm{tr}_*(\langle x\rangle\phi) = 0$ where tr is the trace map $\mathrm{tr}_{K/F}$. Let $Q \in X_K$ and let $P = Q \cap F$. Since $X(P)$ is finite, we may find a Pfister form p and integer m with $\mathrm{sgn}_Q(p) = 2^m$ and $\mathrm{sgn}_{Q'}(p) = 0$ for $Q' \in X(P) - \{Q\}$. Then by **[15**, III 4.5]:

$$0 = \mathrm{sgn}_p\, \mathrm{tr}_*(p\phi) = \sum_{Q' \in X(P)} \mathrm{sgn}_{Q'}(p\phi) = 2^m \mathrm{sgn}_Q(\phi).$$

Thus $\mathrm{sgn}_Q(\phi) = 0$ and as Q was arbitrary, we have $\phi \in W_tK$. □

PROPOSITION 1.6. *Suppose $s \in \mathrm{Hom}(K, F)^{\cdot}$ satisfies $s_*\langle 1\rangle = \langle 1\rangle$. Let $m = [K : F]$ and set $k = (m-1)/2$ and $n = m - (-1)^k$. Let $J \subset WK$ be the ideal generated by $\{\langle 1, -y\rangle | y \in U\}$. Then*:

(1) $M(K/F) = J + (\{\langle 1\rangle - s_*\langle y\rangle | y \in U\})$.

(2) *If K/F is Galois then $n \cdot \langle 1\rangle \in M(K/F)$.*

(3) *If K/F is Galois then $M(K/F) = J$.*

Proof. (1) $J \subset M(K/F)$ by (1.4). If $N_{K/F}(y) \in F^2$ then $\langle y\rangle - s_*\langle y\rangle \in \ker s_* \subset M(K/F)$ and $\langle 1\rangle - s_*\langle y\rangle = \langle 1, -y\rangle + \langle y\rangle - s_*\langle y\rangle \in M(K/F)$. Conversely, $M(K/F)$ is generated by $\ker s_*$, by (1.1), which is generated by $\langle y\rangle - s_*\langle y\rangle$, for $y \in U$. And $\langle y\rangle - s_*\langle y\rangle = -\langle 1, -y\rangle + (\langle 1\rangle - s_*\langle y\rangle) \in J + (\{\langle 1\rangle - s_*\langle y\rangle | y \in U\})$.

(2) Let $G = \mathrm{Gal}(K/F)$. Let $\mathrm{tr} = \mathrm{tr}_{K/F} : K \to F$. There exists $z_0 \in K^{\cdot}$ with $\mathrm{tr}_*\langle z_0\rangle = s_*\langle 1\rangle = \langle 1\rangle$. So $(-1)^k = \det \mathrm{tr}_*\langle z_0\rangle = (\det \mathrm{tr}_*\langle 1\rangle)N_{K/F}(z_0) = N_{K/F}(z_0)$, as $\mathrm{tr}_*\langle 1\rangle = m\langle 1\rangle$. Set $z = (-1)^k z_0$. Then $N_{K/F}(z) \in F^2$ and $\mathrm{tr}_*\langle z\rangle = \langle(-1)^k\rangle$. Thus $\langle(-1)^k\rangle = \sum_G \langle g(z)\rangle$ and $\sum_G \langle 1, -g(z)\rangle = |G|\langle 1\rangle - \langle(-1)^k\rangle = n\langle 1\rangle \in J \subset M(K/F)$.

(3) If $N_{K/F}(y) = 1$ then we need to show $\langle 1\rangle - s_*\langle y\rangle \in J$. Pick z_0 and $z = (-1)^k z_0$ as in (2). Then $\langle 1\rangle - s_*\langle y\rangle = \langle 1\rangle - \mathrm{tr}_*\langle yz_0\rangle = \langle 1\rangle - \sum_G \langle g(yz_0)\rangle = \langle 1\rangle - (-1)^k \sum \langle g(yz)\rangle = \langle 1\rangle + (-1)^k \sum \langle 1, -g(yz)\rangle - (-1)^k m\langle 1\rangle$. As $N_{K/F}(yz) = 1$ we have each $\langle 1, -g(yz)\rangle \in J$. Also $(1-(-1)^k m)\langle 1\rangle \in J$ by the proof of (2) and so $\langle 1\rangle - s_*\langle y\rangle \in J$. □

COROLLARY 1.7. *Suppose K/F is Galois and $s_* : WK \to WF$ is a ring homomorphism. Let $m = [K : F]$ and $k = (m-1)/2$. Then $(m-(-1)^k)\langle 1\rangle = 0$. In particular, F is non-real.*

Proof. Here $(m-(-1)^k)\langle 1\rangle \in M(K/F) = \ker s_*$, using (1.6). Yet $s_*\langle 1\rangle = \langle 1\rangle$, so that $(m-(-1)^k)\langle 1\rangle = 0$. □

COROLLARY 1.8. *Suppose K/F is Galois. Let $m = [K : F]$, $k = (m-1)/2$ and $n = m-(-1)^k$. Let 2^a be the largest 2-power dividing n. If $|X_K| < \infty$ and the height $h(K)$ is finite then $2^a \in M(K/F)$.*

Proof. Write $n = 2^a \cdot b$, where b is odd. If K is non-real then $b\langle 1\rangle$ is a unit in WK and so $2^a \in M(K/F)$ by (1.6)(2). Suppose then that K is real. Let $Q \in X_K$. We Claim $U \not\subset \mathrm{pc}(Q)$, the positive cone of Q. Namely, suppose $U \subset \mathrm{pc}(Q)$. Then $\mathrm{pc}(Q) = U \cdot \mathrm{pc}(P)$ where $P = Q \cap F$. If $S \in X(P) - \{Q\}$ (and such an S exists as $|X(P)| = [K : F]$) then $\mathrm{pc}(S) = g(\mathrm{pc}(Q))$ for some $g \in \mathrm{Gal}(K/F)$. But $g(U) = U$ and g fixes F so that $\mathrm{pc}(S) = g(U\cdot \mathrm{pc}(P)) = U \cdot \mathrm{pc}(P) = \mathrm{pc}(Q)$, a contradiction.

The Claim shows that the only prime ideal to contain $M(K/F) = (\{\langle 1, -y\rangle | y \in U\})$ is IF. By primary decomposition [**8**, 2.3], $M(K/F)$ is IF-primary. Since no power of b is in $M(K/F) \subset IF$ we have $2^a \in M(K/F)$. □

2. Attached primes. For modules M over non-noetherian rings R there are several notions of associated primes (cf. [**10**]). We will use three:

$$\mathrm{Ass}(M) = \{P \in \mathrm{Spec}(R) \mid P = \mathrm{ann}_R(m),\ \text{some } m \in M\}$$

$$\mathrm{Asf}(M) = \{P \in \mathrm{Spec}(R) \mid P \text{ minimal over some } \mathrm{ann}_R(m)\}$$

$$\mathrm{Att}(M) = \{P \in \mathrm{Spec}(R) \mid \text{for all f.g. ideals } I \subset P,\ \text{there exists } m \in M \text{ with } I \subset \mathrm{ann}_R(m) \subset P\}$$

Ass (M) is given by the usual definition of associated primes in the noetherian case. Asf (M) is denoted by $\mathrm{Ass}_f(M)$ in [**10**] and Att (M)

is denoted by $sK(M)$ there. Primes in $\mathrm{Att}(M)$ are called *primes attached to* M (following Dutton [**3**]).

LEMMA 2.1. *Let R be a commutative ring and M an R-module.*
(1) $\mathrm{Ass}(M) \subset \mathrm{Asf}(M) \subset \mathrm{Att}(M)$, *with equality if R is noetherian.*
(2) $\mathrm{Asf}(M) \neq 0$ *iff* $M \neq 0$.
(3) *If* $s, t \in \mathrm{Hom}(K, F)^{\cdot}$ *then* $\mathscr{A}(\ker s_*) = \mathscr{A}(\ker t_*)$ *for* $\mathscr{A} =$ Ass, Asf *and* Att.

Proof. (1) and (2) are clear cf. [**10**, p. 346]. For (3) note that $\ker s_* = \langle z\rangle \ker t_*$ for some $z \in K^{\cdot}$ by (1.1) and $\mathrm{ann}_{WF}(\langle z\rangle m) = \mathrm{ann}_{WF}(m)$. □

We remark that equality in (2.1)(1) can fail at either place for non-noetherian R, cf. [**10**].

LEMMA 2.2. *Let M be a WF-submodule of WK. No $P(\alpha, p)$ is attached to M (where $\alpha \in X_F$, p an odd prime).*

Proof. WK contains no odd dimensional zero-divisors, hence $pm \neq 0$ for all $0 \neq m \in M$. Thus if $\mathrm{ann}_{WF}(m) \subset P(\alpha, p)$ then $m \neq 0$ and $(p) \not\subset \mathrm{ann}_{WF}(m)$. So $P(\alpha, p) \notin \mathrm{Att}(M)$. □

PROPOSITION 2.3. *Let M be a WF-submodule of WK. The following are equivalent:*
(1) $M \cap W_tK \neq 0$.
(2) $IF \in \mathrm{Att}(M)$.
(3) $IF \in \mathrm{Asf}(M)$.
(4) $zd(M) = IF$.

Proof. (1) → (2). By [**3**, Cor. to Prop. 6], $zd(M) = \bigcup_{P \in \mathrm{Att}(M)} P$. If $M \cap W_tK \neq 0$ then $2^k \in zd(M)$ for some k and so $2^k \in P$, for some prime P attached to M. But then $P = IF$.

(2) → (4). By (2.2) we have that $\mathrm{Att}(M)$ consists of some $P(\alpha)$ and possibly IF. Thus every $P \in \mathrm{Att}(M)$ is contained in IF. If $IF \in \mathrm{Att}(M)$ then $IF = \bigcup_{\mathrm{Att}(M)} P = zd(M)$.

(4) → (1) is clear as then $2 \in zd(M)$. (3) → (2) is clear by (2.1). For (1) → (3) note that we have $2^k m = 0$ for some $m \in M$. IF is minimal over $2^k\langle 1\rangle$ so that $IF \in \mathrm{Asf}(M)$. □

COROLLARY 2.4. *Let M be a WF-submodule of WK. Then* $\mathrm{Asf}(M) = \mathrm{Att}(M)$.

Proof. We need only show $\mathrm{Att}(M) \subset \mathrm{Asf}(M)$ by (2.1). Let $P \in \mathrm{Att}(M)$. P is not any $P(\alpha, p)$ by (2.2) and if $P = IF$ then $P \in \mathrm{Asf}(M)$ by (2.3). So suppose $P = P(\alpha)$ for some $\alpha \in X_F$. Then for some $m \in M$ $\mathrm{ann}_{WF}(m) \subset P(\alpha)$ and clearly $P(\alpha)$ is minimal over $\mathrm{ann}_{WF}(m)$. Thus again $P \in \mathrm{Asf}(M)$. □

THEOREM 2.5. *Let* $s \in \mathrm{Hom}(K, F)^{\cdot}$ *and let* $\alpha \in X_F$. *Then* $P(\alpha)$ *is attached to* $\ker s_*$ *iff* $|X(\alpha)| > 1$.

Proof. Suppose first that $|X(\alpha)| > 1$. Let $\beta, \gamma \in X(\alpha)$ be distinct and choose $e \in K^{\cdot}$ with $e >_\beta 0$ and $e <_\gamma 0$. We may assume $s_*\langle 1\rangle = \langle 1\rangle$ by (1.1) and (2.1). Thus $x = \langle 1, e\rangle - s_*\langle 1, e\rangle \in \ker s_*$ and $\mathrm{sgn}_\beta x = 2 - \mathrm{sgn}_\alpha s_*\langle 1, e\rangle$ while $\mathrm{sgn}_\gamma x = -\mathrm{sgn}_\alpha s_*\langle 1, e\rangle$. Hence $x \notin P(\beta) \cap P(\gamma)$. We may assume $x \notin P(\beta)$.

We claim $\mathrm{ann}_{WF}(x) \subset P(\alpha)$. Suppose $r \in WF$ and $rx = 0$. Then $rx \in P(\beta)$ and so $r \in P(\beta) \cap WF = P(\alpha)$. This proves the claim, and since $P(\alpha)$ is a minimal prime, shows $P(\alpha) \in \mathrm{Asf}(\ker s_*) = \mathrm{Att}(\ker s_*)$.

Next, suppose $P(\alpha) \in \mathrm{Att}(\ker s_*)$. Assume, if possible, that $|X(\alpha)| = 1$. Denote by α also its unique extension to K. Suppose $\mathrm{ann}_{WF}(x) \subset P(\alpha)$ for some $x \in \ker s_*$. We may assume $s = \mathrm{tr}_{K/F}$ by (2.1). Thus $0 = \mathrm{sgn}_\alpha s_*(x) = \mathrm{sgn}_\alpha x$ by [**15**, III 4.5]. Hence $x \in P(\alpha)$.

Let $A = \{\delta \in X_K \mid x \in P(\delta)\}$; A is clopen. The complement A' is clopen and so is $B = \varepsilon_{K/F}(A')$, where $\varepsilon_{K/F}(Q) = Q \cap F$, by the Open Mapping Theorem [**6**, 4.9]. By the Normality Theorem [**4**, 3.2], there exists an $r \in WF$ such that $\mathrm{sgn}_\delta r = 0$ if $\delta \in B$ and $\mathrm{sgn}_\delta(r) = 2^n$ if $\delta \notin B$ (some fixed n). We note that $\alpha \notin B$ since $\alpha \in A$, $\alpha \notin A'$ and $\varepsilon_{K/F}^{-1}(\alpha) = \{\alpha\}$ is disjoint from A'.

Let $\delta \in X_K$. If $\delta \in A'$ then $\beta \equiv \varepsilon_{K/F}(\delta) \in B$ and so $\mathrm{sgn}_\delta(rx) = 0$, as $\mathrm{sgn}_\delta(r) = \mathrm{sgn}_\beta(r) = 0$. If $\delta \in A$ then $\mathrm{sgn}_\delta(rx) = 0$ as $\mathrm{sgn}_\delta(x) = 0$. Hence $rx \in W_tK$ and $2^k rx = 0$ for some k. That is, we have $2^k r \in \mathrm{ann}_{WF}(x) \subset P(\alpha)$. But $\mathrm{sgn}_\alpha(2^k r) = 2^{k+n}$, as $\alpha \notin B$, a contradiction. □

COROLLARY 2.6. *Suppose* $\ker s_* \neq 0$. *The following are equivalent*:
(1) $\ker s_* \subset W_tK$.
(2) $M(K/F) \subset W_tK$.
(3) *Every ordering on* F *extends uniquely to* K.
(4) $\mathrm{tr}_*\langle 1\rangle$ *is a unit.*
(5) $\mathrm{Att}(\ker s_*) = \{IF\}$.

Proof. (1) $\leftrightarrow$ (2) follows as ker s_* generates $M(K/F)$ by (1.1). (3) $\leftrightarrow$ (4) is [**15**, III 4.5] and [**11**, VIII 6.4].

(1) $\rightarrow$ (3). Let $\alpha \in X_F$ and let $\beta_1, \beta_2 \in X(\alpha)$. Choose any $e \in K^\cdot$. We assume $s_*\langle 1\rangle = \langle 1\rangle$. Then $\langle e\rangle - s_*\langle e\rangle \in \ker s_* \subset W_tK$ and so $0 = \operatorname{sgn}_{\beta_i}\langle e\rangle - \operatorname{sgn}_\alpha s_*\langle e\rangle$ for $i = 1, 2$. Thus $\operatorname{sgn}_{\beta_1} e = \operatorname{sgn}_{\beta_2} e$ for all $e \in K^\cdot$. Hence $\beta_1 = \beta_2$.

(3) $\rightarrow$ (1). Let $\alpha \in X_K$ and set $\beta = \alpha \cap F$. Then $\operatorname{sgn}_\beta \operatorname{tr}_*(m) = \operatorname{sgn}_\alpha(m)$ for any $m \in WK$ (tr is the trace $\operatorname{tr}_{K/F}$). Thus if $m \in \ker s_*$ then $\operatorname{sgn}_\alpha m = 0$ and so $m \in W_tK$. Thus $\ker \operatorname{tr}_* \subset W_tK$ and hence $\ker s_* \subset W_tK$.

(3) $\rightarrow$ (5). We have $\operatorname{Att}(\ker s_*) \neq \varnothing$ by (2.1). But (2.2) and (2.5) show only IF could be attached to ker s_*. Lastly, (5) $\rightarrow$ (3) is (2.5). $\square$

For a field E and form $\phi \in WE$ we write $D(\phi)$, or $D_E(\phi)$ if we need more precision, for the elements of E represented by ϕ. For a positive integer m we will write $D(m)$ for $D(m\langle 1\rangle)$. Lastly, $D(\infty) = \bigcup_{n\geq 1} D(m)$.

COROLLARY 2.7. *Let* $s \in \operatorname{Hom}(K, F)^\cdot$ *and suppose* $s_*\langle 1\rangle = \langle 1\rangle$. *Suppose also that* $\dim(s_*\langle x\rangle)_{an} = 1$ *for all* $x \in K^\cdot$. *Then*:

(1) s_* *is a ring homomorphism.*

(2) $m(K/F) = \ker s_* = M(K/F) = (\{\langle 1, -y\rangle | y \in U\})$.

(3) $U \subset D_K(\infty)$.

(4) *Every ordering on* F *extends uniquely to* K.

(5) $\operatorname{Att}(\ker s_*) = \{IF\}$.

(6) *For* $a \in G(F)$, $D_K\langle 1, -a\rangle = D_F\langle 1, -a\rangle(D_K\langle 1, -a\rangle \cap U)$.

Proof. We have $s_*\langle x\rangle = \langle N_{K/F}(x)\rangle$ by (1.3) and so s_* is a ring homomorphism. Then ker s_* is an ideal which gives (2) by (1.1) and (1.6), noting that $\langle 1\rangle - s_*\langle y\rangle \in \ker s_* \cap WF = 0$. By (1.5) $m(K/F) \subset W_tK$ and so if $y \in U$ then $\langle 1, -y\rangle \in W_tK$. Hence $U \subset D_K(\infty)$. Parts (4), (5) follow from (2.6) as $\ker s_* \subset W_tK$.

Lastly, let $bx \in D_K\langle 1, -a\rangle$ where $b \in G(F)$ and $x \in U$. Then $\langle\langle -a, -b\rangle\rangle = \langle\langle -a, -x\rangle\rangle$. Apply s_* to get

$$\langle\langle -a, -b\rangle\rangle = s_*\langle\langle -a, -b\rangle\rangle = \langle\langle -a\rangle\rangle s_*\langle\langle -x\rangle\rangle = 0.$$

Hence $b \in D_K\langle 1, -a\rangle \cap G(F) = D_F\langle 1, -a\rangle$. Then $x \in D\langle 1, -a\rangle \cap U$. $\square$

REMARK. (2.7) applies in the following cases:

(1) $I^2F = 0$ (e.g. $\operatorname{tr.d.}_{\mathbf{C}} F = 1$). Here we may write any $s_*\langle x\rangle = \langle N_{K/F}(x)\rangle + \phi$ where $\phi \in I^2F = 0$.

(2) $G(K) = \{1, a\}G(F)$. This follows from (1.4).

COROLLARY 2.8. *If every ordering on F extends uniquely to K then $G(K)/G(F) \approx D_K(\infty)/D_F(\infty)$.*

Proof. We may assume $WK \neq WF$. $\operatorname{Att}(WK/WF) = \{IF\}$ by (2.6) and so WF is an IF-primary submodule of WK. In particular, multiplication by $2\langle 1\rangle$ is locally nilpotent on WK/WF. That is, if $x \in G(K)$ then $2^m\langle x\rangle \in WF$ for some m. Hence $ax \in D_K(2^m)$ for some $a \in G(F)$. So $G(K) = G(F)D_K(\infty)$ and $G(K)/G(F) \approx D_K(\infty)/D_K(\infty) \cap G(F) = D_K(\infty)/D_F(\infty)$. □

The condition (2.3) telling when IF is attached to $\ker s_*$ is not easy to check. We give some examples. Clearly $IF \in \operatorname{Att}(\ker s_*)$ if F is non-real and $WK \neq WF$. For an example with F real, take $F = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt[3]{2})$. $\mathbf{Q}$ has a unique ordering α which extends uniquely, so $P(\alpha) \notin \operatorname{Att}(\ker s_*)$ by (2.6). Also $\ker s_* \neq 0$ as $\sqrt[3]{2} \notin \mathbf{Q} \cdot K^2$. Thus $\operatorname{Att}(\ker s_*) = \{IF\}$.

For an example with $IF \notin \operatorname{Att}(\ker s_*)$, consider the Pythagorean SAP field K with automorphism σ of odd order n constructed by Ware [16]. If $F = K^\sigma$ then K/F is Galois of degree n. As $|X(P)| > 1$ for $P \in X_F$ we have $WK \neq WF$, while the fact that $W_tK = 0$ implies $IF \notin \operatorname{Att}(\ker s_*)$.

In general, the property $IF \notin \operatorname{Att}(\ker s_*)$ is restrictive. We close this section by examining some of its consequences.

LEMMA 2.9. *Let $[K : F] = 2k + 1$ and choose s such that $s_*\langle 1\rangle = \langle 1\rangle$. Suppose $IF \notin \operatorname{Att}(\ker s_*)$. Then:*

(1) $D_K(\infty) = D_F(\infty)K^2$.

(2) *If $N_{K/F}(w) \in (-1)^k F^{\cdot 2}$ then $D_F(\infty) \subset D_K\langle 1, -w\rangle$.*

(3) $W_tK = W_tF$.

Proof. (1) Let $w \in D_K(\infty)$ so that $\langle 1, -w\rangle \in W_tK$. Now $s_*\langle 1, -w\rangle \in W_tF$. Thus $\langle 1, -w\rangle - s_*\langle 1, -w\rangle \in W_tK \cap \ker s_* = 0$ by (2.3). Then $s_*\langle 1, -w\rangle = \langle 1, -w\rangle$, $w \in F^\cdot K^{\cdot 2}$ and $w \in D_F(\infty)K^{\cdot 2}$.

(2) We have $\det(s_*\langle w\rangle) = N_{K/F}(w) = (-1)^k$. Then

$$\det(\langle w\rangle - s_*\langle w\rangle) = (-1)^{k+1}w \quad \text{and} \quad d(\langle w\rangle - s_*\langle w\rangle) = w.$$

Hence $\langle w\rangle - s_*\langle w\rangle = \langle 1, -w\rangle + \phi$ for some $\phi \in I^2K$. If $x \in D_F(\infty)$

then $\langle 1, -x\rangle(\langle w\rangle - s_*\langle w\rangle) \in \ker s_* \cap W_tK = 0$. By the Arason-Pfister theorem, $\langle 1, -x\rangle\langle 1, -w\rangle = 0$ and $x \in D_K(\langle 1, -w\rangle)$.

(3) W_tK is generated by $\langle 1, -w\rangle$, $w \in D_K(\infty)$. Apply (1). □

COROLLARY 2.10. *If* $IF \notin \mathrm{Att}(\ker s_*)$ *then* $m(K/F) = 0$. *In particular, WK embeds into a fiber product of copies of WF. If $|X_F| < \infty$ then we need only finitely many copies.*

Proof. If $\phi \in m(K/F)$, $\phi \neq 0$ then $\phi \in W_tK$ by (1.5) and $\phi \in \ker s_*$. This contradicts (2.3). Thus $m(K/F) = 0$. Write $G(K) = \mathrm{gr}\{xi | i \in I\} \cdot G(F)$, where $\mathrm{gr}(S)$ is the group generated by S. Set $s_i(y) = \mathrm{tr}_{K/F}(x_i y)$ for all $y \in K$. Then $WK \to \sqcap_I WF$ by $\phi \mapsto (\dots, (s_i)(\phi), \dots)$ is injective.

Suppose $|X_F| < \infty$. Then $|X_K| < \infty$ also. Write $X_K = \{Q_1, \dots, Q_n\}$. Now $\bigcap Q_i = D_K(\infty) = D_F(\infty)\dot{K}^2$ by (2.9). Hence

$$[G(K) : G(F)] \leq \left[\dot{K} : \bigcap Q_i\right] \leq 2^n.$$

Thus WK embeds into n copies of WF. □

COROLLARY 2.11. *Suppose* $IF \notin \mathrm{Att}(\ker s_*)$.

(1) *If $|X_F| < \infty$ then WK is a finitely generated WF-module.*

(2) *If WF is noetherian then so is WK.* □

COROLLARY 2.12. *$WF \approx WK$ iff every ordering on F extends uniquely and* $\ker s_* \cap W_tK = 0$.

Proof. By (2.2), (2.3) and (2.5) we have $\mathrm{Att}(\ker s_*) = 0$. Then $\ker s_* = 0$ by (2.1). □

REMARK. There is a partial converse to (2.8). If $W_tK = W_tF$ then $IF \notin \mathrm{Att}(\ker s_*)$. Namely, if $\phi \in W_tK \cap \ker s_*$ then $\phi \in WF$ and so $\phi = s_*(\phi) = 0$. Thus $W_tK \cap \ker s_* = 0$ and $IF \notin \mathrm{Att}(\ker s_*)$.

3. $\ker s_*$ as a projective module.

LEMMA 3.1. (1) $\ker s_*$ *is projective iff WK is projective.*

(2) *If* $\ker s_*$ *is free then WK is free.*

Proof. We may assume $s_*\langle 1\rangle = \langle 1\rangle$ by (1.1). Then both parts follow from $WK \approx WF \oplus \ker s_*$. □

The *trace* of an R-module M is:

$$\mathrm{tr}\, M = \left\{\sum f_i(m_i) | f_i \in \mathrm{Hom}_R(M, R),\ m_i \in M\right\}.$$

We refer to [7] for basic facts about $\operatorname{tr} M$.

PROPOSITION 3.2. *Suppose* $\ker s_*$ *is projective and* $\ker s_* \neq 0$. *Then*:
(1) $\operatorname{tr}(\ker s_*) = WF$,
(2) $ann_{WF}(\ker s_*) = 0$.

Proof. (1) $\operatorname{tr}(\ker s_*)$ is an ideal so if $\operatorname{tr}(\ker s_*) \neq WF$ then $\operatorname{tr}(\ker s_*)$ is contained in a maximal ideal of WF. We check the two cases.

Suppose $\operatorname{tr}(\ker s_*) \subset IF$. Choose $x \in K$ such that $s_*\langle 1\rangle = s_*\langle x\rangle = \langle 1\rangle$. (This is possible by (1.4) since otherwise $L(s) = \{\langle 1\rangle\}$ and $U = \{\langle 1\rangle\}$. But then for any $x \in K^{\cdot}$, $x \in N_{K/F}(x)K^{\cdot 2} \subset F^{\cdot}K^{\cdot 2}$, as $N_{K/F}(xN_{K/F}(x)) \in K^{\cdot 2}$. This implies $WK = WF$ and $\ker s_* = 0$, contrary to the assumption). Then $\langle 1, -x\rangle \in \ker s_*$. We have $IF \cdot \ker s_* = \ker s_*$ by [7, 3.30(a)] while $\langle 1, -x\rangle \in \ker s_* \backslash I^2K$ and $IF \cdot \ker s_* \subset I^2K$. Thus $\operatorname{tr}(\ker s_*) \not\subset IF$.

Next suppose $\operatorname{tr}(\ker s_*) \subset P(\alpha, p)$ for some $\alpha \in X_F$ and odd prime p. Let $m \geq 1$ be the largest integer with $\operatorname{tr}(\ker s_*) \subset P(\alpha, p^m)$; a maximum exists since $\bigcap_m P(\alpha, p^m) \subset P(\alpha) \subset IF$. Now $\operatorname{tr}(\ker s_*) = (tr \ker s_*)^2$ by [7, 3.30(a)]. Hence $\operatorname{tr}(\ker s_*) \subset P(\alpha, p^m)^2 \subset P(\alpha, p^{2m})$, a contradiction. Thus $\operatorname{tr}(\ker s_*) \not\subset P(\alpha, p)$ and so $\operatorname{tr}(\ker s_*) = WF$.

(2) Clearly $\operatorname{tr}(\ker s_*) = WF$ is a finitely generated ideal, so $\operatorname{ann}_{WF}(\ker s_*)$ is generated by an idempotent [7, 3.30(b)]. Only 0 and 1 are idempotent in WF [**11**, VIII 6.8] and clearly $\operatorname{ann}_{WF}(\ker s_*) \neq R$ as $\ker s_* \neq 0$. Thus $\operatorname{ann}_{WF}(\ker s_*) = 0$. □

THEOREM 3.3. *Suppose* F *is real and* $\ker s_* \neq 0$. *If some ordering on* F *extends uniquely to* K *then* $\ker s_*$ *is not projective.*

Proof. Suppose $\ker s_*$ is projective. Then $\operatorname{ann}_{WF}(\ker s_*) = 0$ by (3.2). Let P be a prime ideal attached to $WF \approx WF/\operatorname{ann}_{WF}(\ker s_*)$. Now $(\ker s_*)_P$ is $(WF)_P$-free and so:

$$\operatorname{ann}_{(WF)_P}(\ker s_*)_P = 0 = (\operatorname{ann}_{WF}(\ker s_*))(WF)_P.$$

Then P is attached to $\ker s_*$ [**13**, Lemma 2]. That is, $\operatorname{Att}(WF) \subset \operatorname{Att}(\ker s_*)$.

To complete the proof we need only check that every $P(\alpha)$, $\alpha \in X_F$, is attached to WF, viewed as a WF-module. This would yield a contradiction to (2.5). Let $\alpha \in X_F$ and choose $a >_\alpha 0$ with $a \notin F^2$. Then $0 \neq \langle 1, -a\rangle \in \operatorname{ann}\langle 1, a\rangle$ and $\operatorname{ann}\langle 1, a\rangle \subset P(\alpha)$. Since $P(\alpha)$ is a minimal prime ideal we have $P(\alpha) \in \operatorname{Att}(WF)$. In the case that

$a >_\alpha 0$ implies $a \in F^{\cdot 2}$ we have $X_F = \{\alpha\}$ and $G(F) = \{\pm 1\}$. Thus $WF = \mathbf{Z}$, $P(\alpha) = \{0\} = \operatorname{ann} 2$, so that again $P(\alpha) \in \operatorname{Att}(WF)$. □

COROLLARY 3.4. *Suppose* $\ker s_*$ *is a non-zero projective* WF-*module. If* $W_tF \neq 0$ *then* $\ker s_* \cap W_tK \neq 0$.

Proof. The proof of (3.3) shows $\operatorname{Att}(WF) \subset \operatorname{Att}(\ker s_*)$. If $W_tF \neq 0$ then $IF \in \operatorname{Att}(WF)$ by (2.3) and so $IF \in \operatorname{Att}(\ker s_*)$. This implies $\ker s_* \cap W_tK \neq 0$ by (2.3). □

If no ordering on F extends uniquely to K (for example if K/F is Galois) then it is possible for $\ker s_*$ to be WF-projective—even for WK to be WF-free.

PROPOSITION 3.5. *There is a real field* F *and a Galois extension* K *of* F *of degree* 3 *such that*:

(1) WF *and* WK *are noetherian,*

and

(2) WK *is* WF-*free.*

Proof. Let $\alpha = \alpha_1, \alpha_2, \alpha_3$ be the roots of $x^3 - 3x + 1 \in \mathbf{Q}[x]$. Note that $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois. Let F be a maximal field in $\overline{\mathbf{Q}} \cap \mathbf{R}$ not containing α ($\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$). F is real with the ordering induced by $\mathbf{R}$. Moreover $G(F) = \{\pm 1\}$. Namely, if $a \in F$, $a > 0$ then $F(\sqrt{a}) \subset \overline{\mathbf{Q}} \cap \mathbf{R}$ and $\alpha \notin F(\sqrt{a})$ as deg $\alpha = 3$. Hence, by maximality, $F(\sqrt{a}) = F$ and $a \in F^2$.

Let $K = F(\alpha)$. Since $x^3 - 3x + 1$ is irreducible over F, by construction, K/F is Galois of degree 3. We claim that K is Pythagorean. Suppose not. Let $\beta \in \sum K^2$, $\beta \notin K^2$. Note that $\beta \notin F$, as $\beta \in \sum K^2$ implies $\beta > 0$ and so $\beta \in F$ would yield $\beta \in F^2$. Thus $F(\alpha) = F(\beta) = K$. Let σ generate $\operatorname{Gal}(K/F)$ and set $\beta_i = \sigma^i(\beta)$, $i = 0, 1, 2$ ($\beta_0 = \beta$). We note that each β_i is in $\sum K^2$. If $g(x) = \operatorname{irr}(\beta, F)$ then $g(x^2)) = \operatorname{irr}(\sqrt{\beta}, F)$. Thus $L = F(\sqrt{\beta_0}, \sqrt{\beta_1}, \sqrt{\beta_2})$ is Galois over F, contains $K = F(\beta)$ and is contained in $\overline{\mathbf{Q}} \cap \mathbf{R}$.

Now $[L : F] = 3 \cdot 2^r$ for some $r = 1$, 2 or 3. Let P be a Sylow 3-subgroup and let $F(Q)$ be the fixed field. Then $F(Q) \subset \overline{\mathbf{Q}} \cap \mathbf{R}$ and $\alpha \notin F(Q)$ as deg $\alpha = 3$ while deg $Q = 2^r$. This contradicts the maximality of F.

Hence K is Pythagorean, and SAP since $K \subset \overline{\mathbf{Q}}$ [**4**, Example 1, p. 1177]. F has a unique ordering so K has 3 orderings. Hence $|G(K)| = 8$ and $WK \approx \mathbf{Z} \sqcap \mathbf{Z} \sqcap \mathbf{Z}$ which is free over $\mathbf{Z} \approx WF$. □

The example of (3.5) yields another case where $IF \notin \mathrm{Att}(\ker s_*)$. Indeed $\mathrm{Att}(\ker s_*) = \{P(\alpha)\}$. Also (3.5) is another example of a Pythagorean field with an automorphism of odd order (cf. **[16]**).

We will show that the situation of (3.5), namely, K/F Galois, WK noetherian and WK WF-free, is impossible if F is non-real and non-rigid. Weaker results hold with fewer restrictions on K and F so we begin with no assumptions on K or F.

LEMMA 3.6. *Suppose WK is a free WF-module. Then for some index set I there exists $\phi_i \in WK$ for $i \in I$ such that*:

(1) $WK = \bigoplus_I WF \cdot \phi_i$,

(2) $\phi_i = \langle\alpha_i\rangle + \psi_i$ *where* $\alpha_i \in K$ *and* $\psi_i \in I^2K$, *and*

(3) $G(K) = A \times G(F)$, *where A is the group generated by the α_i, $i \in I$.*

Proof. We have $WK = \bigoplus_I WF \cdot \phi_i$ for some collection $\{\phi_i \in WK | i \in I\}$. Clearly at least one ϕ_i, say ϕ_1, is odd dimensional. For any even dimensional ϕ_j replace ϕ_j by $\phi_j - \phi_1$. We may thus assume (1) and (2) hold.

Now $G(K) = A \cdot G(F)$ since if $x \in G(K)$ then $\langle x\rangle = \sum r_i\phi_i$ and so $x = \det\langle x\rangle = \pm \prod \det(r_i)\alpha_i \in A \cdot G(F)$. We claim that by replacing some ϕ_i by $a\phi_i$, $a \in G(F)$, we may assume $A \cap G(F) = 1$.

This is clearer if we write the $\mathbf{Z}_2$-vector space $G(K)$ additively. We wish to show that there exist a_i $(i \in I)$ in the subspace $G(F)$ such that $\mathrm{span}\{\alpha_i + a_i \mid i \in I\} \cap G(F) = \{0\}$. Choose any complementary subspace $G(F)'$. Then every α_i has a unique expression $\alpha_i = a_i + a_i'$ for some $a_i \in G(F)$ and $a_i' \in G(F)'$. Use these a_i. □

PROPOSITION 3.7. *Suppose F is non-real and WK is a free WF-module. Then for all $f \in G(F)$, $f \neq 1$, we have $D_K\langle 1, -f\rangle = D_F\langle 1, -f\rangle$.*

Proof. Write $WK = \bigoplus_I WF \cdot \phi_i$ as in (3.6). Each odd dimensional form is a unit as F is non-real. Multiplication by ϕ_1^{-1} is an WF-module isomorphism and $\{\phi_1^{-1}\phi_i | i \in I\}$ satisfies (1), (2), (3) of (3.6). We may thus assume $\phi_1 = \langle 1\rangle$. The result is clear if $WK = WF$ so we may assume $|I| \geq 2$. Write $G(K) = A \times G(F)$ as in (3.6) and let $\alpha \in A$.

Claim. $WK = WF \cdot \langle 1\rangle \oplus WF \cdot \langle\alpha\rangle \oplus M$, for some WF-module M.

We have $\langle\alpha\rangle = r_1\langle 1\rangle + \sum_{i\geq 2} r_i\phi_i$. If all r_i $(i \geq 2)$ are even dimensional then by determinants $\alpha \in G(F)$, contradicting (3.6). We may thus assume r_2 is odd dimensional. Since F is non-real, r_2 is a unit in WF. We have:

$$r_2^{-1}\langle\alpha\rangle = r_2^{-1}r_1\langle 1\rangle + \phi_2 + \sum_{i\geq 3} r_2^{-1}r_i\phi_i .$$

Set $M = \bigoplus_{i\geq 3} WF\cdot\phi_i$. Then $\phi_2 \in WF\cdot\langle 1\rangle + WF\cdot\langle\alpha\rangle + M$, hence $WK = WF\cdot\langle 1\rangle + WF\cdot\langle\alpha\rangle + M$. Moreover, if:

$$s_1\langle 1\rangle + s_2\langle\alpha\rangle + m = 0 \qquad (m \in M)$$

then

$$\begin{gathered} s_1\langle 1\rangle + s_2(r_1\langle 1\rangle + r_2\phi_2 + m') + m = 0 \\ (s_1 + s_2r_1)\langle 1\rangle + s_2r_2\phi_2 + s_2m' + m = 0. \end{gathered}$$

But $\langle 1\rangle = \phi_1$ and ϕ_i $(i \geq 2)$ are independent. Thus $s_2r_2 = 0$. Again r_2 is a unit so $s_2 = 0$. Thus $s_1 = 0$ and $m = 0$. This proves the Claim.

Now say $f \in G(F)$, $f \neq 1$. Let $x \in D_K\langle 1, -f\rangle$, $x \notin G(F)$. Then $x = g\alpha$ for some $g \in G(F)$ and $\alpha \in A$, $\alpha \neq 1$. But then $\langle 1, -f\rangle\langle 1\rangle = \langle g\rangle\langle 1, -f\rangle\langle\alpha\rangle$ contradicting the Claim. Thus $D_K\langle 1, -f\rangle \subset G(F)$ and so $D_K\langle 1, -f\rangle = D_F\langle 1, -f\rangle$. □

In the following, $B(F)$ denotes the basic part, namely those $a \in F$ with either $a = \pm 1$, a or $-a$ not rigid (cf. **[12]**).

THEOREM 3.8. *Suppose F is non-real and $G(F)$ is finite. If ker s_* is a finitely generated projective WF-module then either*:

(1) *$WK \approx WF[A]$ where $A = G(K)/G(F)$ or*

(2) *$B(F) = \{\pm 1\}$ and $WF \approx \mathbf{Z}_n[C]$ with $n = 2$ or 4 and C a group or exponent two.*

Proof. WF is a local ring so ker s_*, hence WK, is finitely generated free. Suppose $B(F) \neq \{\pm 1\}$. Choose $f \in B(F)\backslash\{\pm 1\}$. Set $X_1(K) = D_K\langle 1, -f\rangle$. Then $X_1(K) = X_1(F) = D_F\langle 1, -f\rangle$ by (3.7). For $i \geq 2$ and a field E let $X_i(E) = \bigcup D_E\langle 1, -a\rangle$, over $a \in X_{i-1}(E)\backslash\{1\}$. Then by **[2**, 2.4**]**

$$B(K) = \pm(X_1(K)X_2(K)^2 \cup -X_1(K)X_3(K)) = B(F) \subset G(F).$$

The result is then standard, see **[12**, 5.19**]**. And if $B(F) = \{\pm 1\}$ then WF is classified as given **[12**, 5.21**]**. □

REMARK. If $WK = WF[A]$, as in (3.8)(1), then WK is clearly a free WF-module. Suppose $B(F) = \{\pm 1\}$ as in (3.8)(2) *and* $B(K) \cap G(F) = \{\pm 1\}$. We may write $G(K) = B \times C$ where $B(K) \subset B$ and $G(F) = \pm C$. Then any form in WK may be written uniquely as $\sum \langle b_i c_i \rangle = \sum \langle c_{i1} \rangle \cdot \langle b_1 \rangle + \sum \langle c_{i2} \rangle \cdot \langle b_2 \rangle + \dots$. Thus again WK is a free WF-module. However, we know of no example of an odd degree extension K/F with $WK \neq WF$ and either (3.8)(1) or (2) occurring.

We obtain a slightly weaker result if WF is not noetherian.

LEMMA 3.9. *Let* $WK = \bigoplus_I WF \cdot \phi_i$ *as in* (3.6). *Let* $\alpha, \beta \in A \backslash \{1\}$ *be distinct and let* $a, b, c, d \in G(F)$. *If* $b\alpha \in D\langle 1, -a\beta \rangle$ *and* $d\alpha \in D\langle 1, -c\beta \rangle$ *then* $b = d$ *and* $a = c$.

Proof. We have

$$\begin{aligned} 0 = \langle\langle -c\beta, -d\alpha \rangle\rangle &\equiv \langle\langle -ac, -d\alpha \rangle\rangle - \langle\langle -a\beta, -d\alpha \rangle\rangle \\ &\equiv \langle\langle -ac, -d\alpha \rangle\rangle - \langle\langle -a\beta, -bd \rangle\rangle (\operatorname{mod} I^3K). \end{aligned}$$

Thus $\langle\langle -ac, -d\alpha \rangle\rangle = \langle\langle -bd, -a\beta \rangle\rangle$. Apply linkage [**12**, 1.14]:

$$\langle\langle -ac, -d\alpha \rangle\rangle = \langle\langle -ac, -x \rangle\rangle = \langle\langle -bd, -x \rangle\rangle = \langle\langle -bd, -a\beta \rangle\rangle$$

for some $x \in K^{\cdot}$. Now $x \in D\langle 1, -abcd \rangle$. If $ac \neq bd$ then $x \in G(F)$ by (3.7). But $xd\alpha \in D\langle 1, -ac \rangle$ which forces $a = c$, by (3.7) again. Similarly $xa\beta \in D\langle 1, -bd \rangle$ yields $b = d$. Suppose then that $ac = bd$. Now $xd\alpha \in D\langle 1, -ac \rangle$ gives $x \in \alpha G(F)$ (unless $a = c$ and so $b = d$). And $xa\beta \in D\langle 1, -bd \rangle$ gives $x \in \beta G(F)$ (unless $b = d$ and so $a = c$). But $\alpha G(F) \cap \beta G(F) = \varnothing$. Hence $a = c$ and $b = d$. □

THEOREM 3.10. *Suppose* F *is non-real and* $G(F)$ *is infinite. If* $\ker s_*$ *is a finitely generated projective* WF*-module then either*:

(1) $WK \approx WF[A]$, *with* $A = G(K)/G(F)$ *or*

(2) $|B(F)| < \infty$ *and* $R = R_0[C]$ *for some Witt ring* R_0 *and infinite group* C *of exponent* 2.

Proof. If $|B(F)| < \infty$ then R is as described [**12**, 5.19]. Suppose $B(F)$ is infinite. Let $\alpha \in A$, $\alpha \neq 1$. We will show α is bi-rigid.

Suppose α is not rigid (the argument for $-\alpha$ is similar). Then $\alpha \in B(K)$ and for all $f \in B(F)$, $f\alpha$ is not bi-rigid. Hence there exist infinitely many f with $f\alpha$ not rigid (that is, if $f\alpha$ is rigid then $-f\alpha$ is not rigid). But A is finite, as WK is finitely generated over WF, so there exist distinct f, g in F and $\beta \in A \backslash \{1, \alpha\}$ such that $b\beta \in D\langle 1, -f\alpha\rangle$, $d\beta \in D\langle 1, -g\alpha\rangle$ for some $b, d \in F$. This contradicts (4.9). $\square$

LEMMA 3.11. *If* $t_1, \dots, t_n$, *and all* $t_i t_j$ $(i \neq j)$ *are rigid then* $D\langle t_1, \dots, t_n\rangle = \{t_1, \dots, t_n\}$.

Proof. By induction on n. Suppose $n = 2$.

$$D\langle t_1, t_2\rangle = t_1 D\langle 1, t_1 t_2\rangle = t_1\{1, t_1 t_2\} = \{t_1, t_2\}.$$

For $n > 2$ we have by induction:

$$D\langle t_1, \dots, t_n\rangle = \bigcup_{i=1}^{n-1} D\langle t_i, t_n\rangle = \{t_1, \dots, t_n\}. \qquad \square$$

LEMMA 3.12. *Let* K/F *be finite Galois* (*not necessarily of odd degree*). *Let* $t \in K \backslash FK^2$. *Then at least one of* t, tt^g $(g \in \mathrm{Gal}(K/F))$ *is not rigid.*

Proof. Suppose t and all tt^g are rigid. Note t^g is rigid as $D\langle 1, t\rangle^g = D\langle 1, t^g\rangle$. Also if $g, h \in \mathrm{Gal}(K/F)$ are distinct then $t^g t^h = g(tt^{hg^{-1}})$ is rigid. Hence by (3.11) $D(\sum_G \langle t^g\rangle) = \{t^g | g \in \mathrm{Gal}(K/F)\}$. But $\sum \langle t^g\rangle = \mathrm{tr}_*\langle t\rangle \in WF$. Hence some $t^g \in G(F)$. But then $t \in G(F)$, a contradiction. $\square$

THEOREM 3.13. *Let* F *be non-real and suppose that either* (i) $G(F)$ *is finite and* $B(F) \neq \{\pm 1\}$ *or* (ii) $G(F)$ *is infinite and* $B(F)$ *is infinite. Let* K/F *be Galois of odd degree. Then neither* WK *nor* $\ker s_*$ *are finitely generated projective* WF*-modules.*

Proof. If WK is a finitely generated projective WF-module then (3.8), (3.10) imply $B(K) \subset FK^2$ and hence if $t \in K\backslash FK^2$ with $K = F(t)$ then t and all tt^g ($g \in \mathrm{Gal}(K/F)$) are bi-rigid. Namely if $tt^g \in FK^2$, say $t^g = at$, then $g^2(t) = a(at) = t$. Thus t is fixed by g^2. As g has odd order, t is fixed by g. But then $K \neq F(t)$. This contradicts (3.12). $\square$

Ware [**16**, 1.6] shows a rigid field cannot be the Galois odd degree extension. (3.13) improves this slightly: even the case $WK \approx WF[A]$, $A = G(K)/G(F)$ cannot arise.

In a different direction we have:

PROPOSITION 3.14. *Suppose WK is a noetherian, injective WF-module. Then F is non-real and WF is Gorenstein (that is, $|\operatorname{ann} IF| = 2$).*

Proof. WK injective implies its direct summand WF is injective. Thus WF has injective dimension 0 and so Krull dimension 0. Thus F is non-real. Further, WF is Gorenstein (cf. [**1**], [**9**]). □

4. Noetherian extensions. We have given several examples of odd degree extensions K/F where WK is a finitely generated WF-module. This is necessarily the case when X_F is finite and $IF \notin \operatorname{Att}(\ker s_*)$ by (2.11). We collect here several results on the possible values of $[G(K) : G(F)]$.

PROPOSITION 4.1. *Let $[K : F] = p$ be an odd prime and suppose K/F is Galois. If $[G(K) : G(F)] = 2^k$ then $p | 2^k - 1$.*

Proof. Let $G = \operatorname{Gal}(K/F)$ and let σ generate G. G acts on $G(K)/G(F)$. Suppose $xG(F)$ is a fixed point. Then $N_{K/F}(x) \in x^p G(F) = xG(F)$ and so $x \in G(F)$. If $x \notin G(F)$ then the orbit $\{\sigma^i(xG(F)) | i \in \mathbf{Z}\}$ has order p (there is no stabilizer as G is simple). Thus p divides $2^k - 1$. □

EXAMPLE. Let p be an odd prime and set $n = 2^p - 1$. Let K be $\mathbf{Q}_2$ with the nth roots of unity adjoined. Then $K/\mathbf{Q}_2$ is Galois of degree p [**14**, Prop. 16, p. 77]. By [**11**, p. 161] we have $[G(K) : G(\mathbf{Q}_2)] = 2^{p-1}$. This gives the minimal value of $[G(K) : G(F)]$ for p such that the order of 2 mod p is $p - 1$ (thus for $p = 3, 5, 11, 13, 19, 29, 37, 53, 59$ etc.).

COROLLARY 4.2. *Let $[K : F] = p_1 p_2 \cdots p_t$ with the p_i's prime (not necessarily distinct). Let k_i be the least positive integer such that $p_i | 2^{k_i} - 1$. If K/F is Galois and $G(K) \neq G(F)$ then $[G(K) : G(F)] \geq 2^w$, where $w = k_1 + \cdots + k_t$.*

Proof. We use induction on t. The case $t = 1$ is (4.1) and if $t > 1$ then choose an intermediate normal extension L and apply the result to K/L and L/F. □

When p is a Mersenne prime (i.e., $p = 2^k - 1$) then the minimal (non-trivial) square class extension for a Galois extension of degree p is $p + 1$. In this case we may improve (1.5).

Proposition 4.3. *Suppose K/F is Galois and that $[K : F] = p$ where $p = 2^k - 1$ is a prime. If $[G(K) : G(F)] = p+1$ then $m(K/F) \subset \operatorname{ann}(2^k\langle 1\rangle)$.*

Proof. Choose $s \in \operatorname{Hom}(K, F)$ with $s_*\langle 1\rangle = \langle 1\rangle$. There is an $x \in G(K)$ with $\operatorname{tr}_*\langle x\rangle = s_*\langle 1\rangle = \langle 1\rangle$. Now $(-1)^{p-1/2} = \det \operatorname{tr}_*\langle x\rangle = N_{K/F}(x)$. Since $p = 2^k - 1$ $(k \geq 2)$ we have $N_{K/F}(x) = -1$. Write $G(K) = U \times G(F)$ as in §1. There is only one (non-trivial) orbit in $G(K)/G(F)$. Thus $U = \{1, x_1, \dots, x_p\}$ where $\sigma(x_i) = x_{i+1}$ (here σ generates $\operatorname{Gal}(K/F)$ and $x_{p+1} \equiv x_1$). We may assume $x_1 = -x$ and so $\operatorname{tr}_*\langle x_1\rangle = \langle -1\rangle$.

Let $\psi = \phi_0 + \sum_{i=1}^{p}\langle x_i\rangle\phi_i \in m(K/F)$, where $\phi_0, \dots, \phi_p \in WF$. Then:

$$0 = \operatorname{tr}_* \psi = p\phi_0 - \sum_{i=1}^{p} \phi_i,$$

$$0 = \operatorname{tr}_*\langle x_1\rangle \psi = p\phi_1 - \phi_0 - \sum_{i=2}^{p} \phi_i.$$

Subtraction yields $p(\phi_0 - \phi_1) - (\phi_1 - \phi_0) = 0$ and so $2^k(\phi_0 - \phi_1) = 0$. Similarly, $2^k(\phi_i - \phi_j) = 0$ for all i, j.

Now $\langle -1\rangle = \operatorname{tr}_*\langle x_1\rangle = \langle x_1, x_2, \dots, x_p\rangle$. Thus $\langle x_p\rangle = -\langle 1, x_1, \dots, x_{p-1}\rangle$. Then $\psi = \phi_0 + \langle x_1\rangle\phi + \cdots + \langle x_{p-1}\rangle\phi_{p-1} - \langle 1, x_1, \dots, x_{p-1}\rangle\phi_p = (\phi_0 - \phi_p) + \langle x_1\rangle(\phi_1 - \phi_p) + \cdots + \langle x_{p-1}\rangle(\phi_{p-1} - \phi_p)$. Thus $2^k\psi = 0$. □

(4.3) applies when $[K : F] = 3$ and $[G(K) : G(F)] = 4$. See after (4.1) for an example of such an extension. We can improve (4.3) in this case (see the second example after (1.1)).

Corollary 4.4. *Suppose K/F is Galois with $[K : F] = 3$ and $[G(K) : G(F)] = 4$. Write $U = \{1, x, y, xy\}$. Then:*

(1) *$m(K/F) = \{\phi_0\langle x\rangle + \phi_2\langle y\rangle \mid \phi_i \in WF,\ 4\phi_i = 0$ and $\phi_0 + \phi_1 + \phi_2 = 0\}$.*

(2) *$m(K/F) = 0$ iff $D_F(4) \subset D_K\langle 1, -x\rangle \cap D_K\langle 1, -y\rangle$.*

(3) *If F is non-real and $m(K/F) = 0$ then $x, y \in D_K(2)$.*

Proof. (1) Follows from the proof of (4.3). Suppose $m(K/F) = 0$. If $w \in D_F(4)$ then for $\phi = \langle 1, -w\rangle$ we have $4\phi = 0$ and $\langle 1, -x\rangle\phi \in m(K/F) = 0$. Thus $w \in D_K\langle 1, -x\rangle$, and similarly $w \in D_K\langle 1, -y\rangle$.

If $D_F(4) \subset D_K\langle 1, -x\rangle \cap D_K\langle 1, -y\rangle$ and $\psi = \phi_0 + \phi_1\langle x\rangle + \phi_2\langle y\rangle \in m(K/F)$ then

$$\begin{aligned}\psi &= \phi_0 + \phi_1\langle x\rangle - (\phi_0 + \phi_1)\langle y\rangle \\ &= \phi_0\langle 1, -y\rangle + \langle x\rangle\phi_1\langle 1, -xy\rangle = 0 + 0 = 0,\end{aligned}$$

as $\phi_i \in \operatorname{ann}(4)$ which is generated by $\langle 1, -w\rangle$, $w \in D_F(4)$. Thus $m(K/F) = 0$, proving (2).

To prove (3) note that (2) implies $D_F(2^{2+k}) \subset D_K(2^k\langle\langle -x\rangle\rangle) \cap D_K(2^k\langle\langle -y\rangle\rangle)$. If $D_F(4) = G(F)$ then $-1 \in D_K\langle 1, -x\rangle \cap D_K\langle 1, -y\rangle$ and $x, y \in D(2)$. Otherwise, say $D_F(2^{k+1}) \neq G(F)$ and $D_F(2^{k+2}) = G(F)$ for some $k \geq 1$. Then $-1 \in D(2^k\langle\langle -x\rangle\rangle)$ and $2^{k+1}\langle\langle -x\rangle\rangle = 0$. Thus $x \in D(2^{k+1}) \subset D(2^{k-1}\langle\langle -x\rangle\rangle)$. So $-1 \in D(2^{k-1}\langle\langle -x\rangle\rangle)$ and $2^k\langle\langle -x\rangle\rangle = 0$. Continue until $2\langle 1, -x\rangle = 0$. Similarly $2\langle 1, -y\rangle = 0$. □

We have only a few results for non-Galois extensions.

PROPOSITION 4.5. *Let L be the normal closure of K/F. If L is real then* $[K : F] \leq [G(K) : G(F)]$.

Proof. Let $X_E(P)$ denote the set of extensions of an ordering P to a field E. Let $Q \in X_L$ and set $P = Q \cap F$, $V = Q \cap K$. Then $|X_L(p)| = [L : F]$ as L/F is Galois, and $|X_L(V)| = [L : K]$. Then $|X_K(P)| = [L : F]/[L : K] = [K : F]$.

Let $h(S)$ denote the number of subgroups of $G(K)$ of index 2 containing a set S. Let $P \in X_F$. Then $h(P) = |G(K)/P| - 1 = 2[G(K) : G(F)] - 1$. Also $h(P \cup \{-1\}) = [G(K) : G(F)] - 1$. Thus there are $[G(K) : G(F)]$ many subgroups of index 2 in $G(K)$, containing P but missing -1. These are the only possible choices for extensions of P to K. Hence $[K : F] = |X_K(p)| \leq [G(K) : G(F)]$. □

We close with a detailed study of the smallest possible case: $[K : F] = 3$ and $[G(K) : G(F)] = 2$. We know of no such extensions.

LEMMA 4.6. *Suppose $[K : F] = 3$ and K/F is separable but not Galois. Let L be the normal closure of K. Then:*

(1) *There exists a field E such that $F \subset E \subset L$, $[L : E] = 3$ and L/E is Galois.*

(2) $[G(K) : G(F)] = \frac{[G(L) : G(E)]}{[D_K\langle 1, -g\rangle : D_F\langle 1, -g\rangle]}$, *for some* $g \in G(F)$.

(3) $[G(K) : G(F)] \leq [G(L) : G(E)]$.

Proof. We have $[L : F] = 6$. Thus there exists a normal subgroup H of $\mathrm{Gal}(L/F)$ of order 3. Let E be the fixed field of H. Then $[L:E]=3$ and $E = F(\sqrt{g})$ for some $g \in G(F)\backslash\{1\}$. Suppose $K = F(e)$. Then $e \notin E$ and so $L = F(\sqrt{g})$. By [**11**, VII, 3.4]:

$$\begin{aligned}[G(E):G(F)] &= \tfrac{1}{2}|D_F\langle 1, -g\rangle| \\ [G(L):G(K)] &= \tfrac{1}{2}|D_K\langle 1, -g\rangle|.\end{aligned}$$

Hence the formula in (2) holds. (3) follows from (2). □

LEMMA 4.7. *Suppose* $G(K) = \{1, a\}G(F)$. *Set* $H = D\langle 1, -a\rangle \cap G(F)$. *Then for* $f \in G(F)$:

$$D_K\langle 1, -f\rangle = \begin{cases} D_F\langle 1, -f\rangle & \text{if } f \notin H, \\ \{1, a\}D_F\langle 1, -f\rangle & \text{if } f \in H, \end{cases}$$
$$D_K\langle 1, -af\rangle = \{1, -af\}(D_F\langle 1, -f\rangle \cap H).$$

Proof. By (1.4) there is an $s \in \mathrm{Hom}(K/F)$ with $s_*\langle 1\rangle = s_*\langle a\rangle = \langle 1\rangle$. (2.7)(6) then gives the computation of $D_K\langle 1, -f\rangle$. Clearly $D_K\langle 1, -af\rangle = \{1, -af\}(D_K\langle 1, -af\rangle \cap G(F))$. Then $g \in D_K\langle 1, -af\rangle \cap G(F)$ iff $af \in D_K\langle 1, -g\rangle$ iff $g \in D_F\langle 1, -f\rangle$ and $g \in H$. Thus $D_K\langle 1, -af\rangle = \{1, -af\}(D_F\langle 1, -f\rangle \cap H)$. □

PROPOSITION 4.8. *Suppose* $[K : F] = 3$ *and* $G(K) = \{1, a\}G(F)$. *Then*:

(1) $|D\langle 1, -a\rangle \cap G(F)| \neq 1$;

(2) *If* $|D\langle 1, -a\rangle \cap G(F)| = 2$ *then either*:

(i) $\mathrm{rad}(F) \neq 1$, *or*

(ii) WF *and* WK *are group ring extensions, or*

(iii) *There is a non-real Witt ring* R_0 *such that* $WF = \mathbf{Z} \sqcap R_0$ *and* $WK = \mathbf{Z} \sqcap R_0[\{1, a\}]$. *In particular,* $|X_F| = |X_K| = 1$.

Proof. (1) Suppose $|D\langle 1, -a\rangle \cap G(F)| = 1$. Then (4.7) implies a is bi-rigid. Thus $WK = WF[\{1, a\}]$ is a group ring extension. Let L be the normal closure of K. Then $L = K(\sqrt{g})$ for some $g \in G(F)$. Set $E = F(\sqrt{g})$. Now $D_K\langle 1, -g\rangle = D_F\langle 1, -g\rangle$ so that $[G(K) : G(F)] = [G(L) : G(E)]$ by (4.6). But (4.1) implies $[G(L) : G(E)] \geq 4$, a contradiction.

(2) Write $D\langle 1, -a\rangle \cap G(F) = \{1, f\}$ and suppose $\mathrm{rad}(F) = 1$; in particular, $D_F\langle 1, -f\rangle \neq G(F)$. If $x \in G(F) - D_F\langle 1, -f\rangle$ then

$D\langle 1, -ax\rangle = \{1, -ax\}$ by (4.7). Thus if there exists $g, -g \in G(F) - D_F\langle 1, -f\rangle$ then ag is bi-rigid. Now $f \in D\langle 1, -a\rangle$ so a is not bi-rigid and hence $g = a \cdot ag$ is bi-rigid. From $D_K\langle 1, -g\rangle = D_F\langle 1, -g\rangle$ we see that both WF and WK are group rings (with $\{1, g\}$ the group). This gives (ii).

So we may assume for all $g \in G(F)$ that either g or $-g$ is in $D\langle 1, -f\rangle$. Thus $[G(F) : D_F\langle 1, -f\rangle] = 2$ and $-1 \notin D_F\langle 1, -f\rangle$. In particular, $D_F\langle 1, -f\rangle$ is an ordering on F. From $G(F) = \{1, f\} \times D_F\langle 1, -f\rangle$ we get $WF = \mathbf{Z} \sqcap R_0$ for some Witt ring R_0.

We also have that $D_K\langle 1, -f\rangle = \{1, a\}D_F\langle 1, -f\rangle$ has index 2, in $G(K)$, and misses -1. Thus $D_K\langle 1, -f\rangle$ is an ordering. Again, $G(K) = \{1, f\} \times D_K\langle 1, -f\rangle$. Now in $D_K\langle 1, -f\rangle$, $D\langle 1, a\rangle = \{1, a\}$ and $D\langle 1, -af\rangle = \{1, -af\}$. Hence $WK = \mathbf{Z} \sqcap R_0[\{1, a\}]$.

Lastly, (2.7) implies $\mathrm{Att}(\ker s_*) = \{IF\}$. Then (2.7) and (2.8) yield $|D_K(\infty)/D_F(\infty)| = 2$. Now $D_F(\infty) = 1 \times D_L(\infty)$, where $R_0 = WL$, and $D_K(\infty) = 1 \times D_L(\infty)$ unless $a \in D_L(\infty)$. But this only occurs if $-1 \in D_L(\infty)$. Hence R_0 is non-real and $|X_K| = |X_F| = 1$. □

References

[1] H. Bass, *On the ubiquity of Gorenstein rings*, Math. Z., **82** (1963), 8–28.

[2] A. Carson and M. Marshall, *Decomposition of Witt rings*, Canad. J. Math., **34** (1982), 1276–1302.

[3] P. Dutton, *Prime ideals attached to a module*, Quart. J. Math. (2), **29** (1978), 403–413.

[4] R. Elman and T.-Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math., **94** (1972), 1155–1194.

[5] ——, *Quadratic forms under algebraic extensions*, Math. Ann., **219** (1976), 21–42.

[6] R. Elman, T.-Y. Lam, and A. Wadsworth, *Orderings under field extensions*, J. Reine Angew. Math., **306** (1979), 7–27.

[7] C. Faith, *Algebra: Rings, Modules and Categories* I, Grundlehren Math. Wiss., vol. 190, Springer-Verlag, New York/Heidelberg/Berlin, 1973.

[8] R. Fitzgerald, *Primary ideals in Witt rings*, J. Algebra, **96** (1985), 368–385.

[9] ——, *Gorenstein Witt rings*, Canad. J. Math., **60** (1988), 1186–1202.

[10] J. Iroz and D. Rush, *Associated prime ideals in non-noetherian rings*, Canad. J. Math., **36** (1984), 344–360.

[11] T.-Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, Mass., 1980.

[12] M. Marshall, *Abstract Witt rings*, Queen's Papers in Pure and Appl. Math., vol. 57, Kingston, Ont., 1980.

[13] D. G. Northcott, *Remarks on the theory of attached prime ideals*, Quart. J. Math. (2), **33** (1982), 239–245.

[14] J.-P. Serre, *Local Fields*, Graduate Texts in Math., vol. 67, Springer-Verlag, New York/Heidelberg/Berlin, 1979.

[15] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren Math. Wiss., vol. 270, Springer-Verlag, Berlin/Heidelberg/New York/Tokyo, 1985.

[16] R. Ware, *Automorphisms of pythagorean fields and their Witt rings*, Comm. Algebra **17** (4) (1989), 945–969.

Received December 1, 1990 and in revised form July 8, 1991.

SOUTHERN ILLINOIS UNIVERSITY
CARBONDALE, IL 62901-4408