Relations between quadratic forms and certain Galois extensions.

by Fernando Rodriguez Villagas.

The Ohio State University
July, 1988

§1 Introduction.

1.1 Our main concern in this paper is the following embedding problem:

Given beforehand the finite Galois extension $F/K$ construct all extensions $L/K$ containing $F$, with $[L:F] = 2$ and $L/K$ Galois.

Though much of what we will do can be done generally for $[L:F] = \text{any prime } p$, we prefer to deal with the case $p = 2$ only, because of its relation to quadratic forms. Throughout this paper we assume every field has characteristic not equal to two.

In section 2 we find necessary and sufficient conditions for the existence of such extensions in terms of the vanishing of a determined algebra class in $\text{Br}(K)$, the Brauer group of $K$. This is summarized (and precisely defined) in the main exact sequence given in Theorem 2.4. A general criterion like this is known and goes back to Brauer, $[\text{Br}]$. Further references can be found in $[\text{Wi}]$, $[\text{Fr}]$, $[\text{Sh}]$. For convenience of the reader we include a proof in §6.

In section 3 we restrict what was found in §2 to the case where the group $\text{Gal}(F/K)$ is of exponent two and rephrase the main exact sequence in Theorem 3.8. In section 4 we restate the injectivity $k_2(K) \rightarrow \text{Br}_2(K)$ in Merkurjev's Theorem in terms of Galois extensions; this is Proposition 4.2. A purely formal generalization of this restatement is raised as a question in 4.7.

In section 4 we also show some concrete applications of all this to the construction of extensions whose Galois groups are of a special type ($h < 3$, see §3). These include the quaternionic group of order 8 and a group of order 32, built by pasting two dihedral groups of order 8 by their centers.

A generalization of Witt's method of construction using spinor norms ($[\text{Wi}]$) is given in §5.
1.2 Notation:

Given a field $K$, 

$K^*$ is the multiplicative group of non-zero elements.

$K^*/K^{*2}$ is the group of square classes, viewed as a vector space over the field of two elements.

If $a$ is in $K^*$, $<a>$ denotes its square class.

$K[2]$ is the field $K$ with all its square roots adjoined.

$\text{Br}_2(K)$ is the 2-torsion of the Brauer group of $K$, which we will write additively.

Given two square classes $u = <a>$ and $w = <b>$, $\{a, b\}$ or $[u, w]$ will denote the class of the quaternion algebra $(a, b)/K$ in $\text{Br}_2(K)$.

Given a vector space $V$, over the field of two elements, $S^2(V)$ will denote the degree two part of the symmetric algebra $V$.

$k_2(K)$ is Milnor's second $k$-group, see [Mi]. We will use its following definition:

$k_2(K) = S^2(K^*/K^{*2}) / \{ <a>, <b> : \{a, b\} = 0 \}$.

$\mu_2 = \{ +1, -1 \}$ viewed as naturally embedded in $K^*$.
§2 The main exact sequence.

Given a Galois extension $F/K$ with $\text{Gal}(F/K) = G$, we are interested in the following set of extensions of $F$ contained in some fixed algebraic closure.

2.1 Definition:

$$Q(F/K) = \{ L : L \supseteq F, L/K \text{ is Galois and } [L:F] \leq 2 \}$$

In what follows, $F/K$ is assumed to be finite. The standard modifications should be used for the infinite case. This will be tacitly assumed in Theorem 3.6.

$Q(F/K)$ can be interpreted as a cohomology group.

2.2 Lemma: The map $H^0(G,F^*/F^{*2}) \to Q(F/K)$ which sends $<x>$ to $F(\sqrt{x})$ is bijective.

Proof: Let $a$ be in $F^*$ then $F(\sqrt{x})/K$ is normal $\iff F(\sqrt{x}) = F(\sqrt{x^2})$ for all $g$ in $G$ $\iff \frac{g\cdot x}{x}$ is in $F^{*2}$ for all $g$ in $G$ $\iff <x>$ is in $H^0(G,F^*/F^{*2})$.

Using this bijection we can carry the group structure of $H^0(G,F^*/F^{*2})$ over to $Q(F/K)$. Then $F(\sqrt{x}) + F(\sqrt{y}) = F(\sqrt{xy})$. The identity element, of course, is $F$. Also, we will sometimes identify $Q(F/K)$ with its image in $F^*/F^{*2}$.

2.3 Lemma: Given $L$ in $Q(F/K)$ with $[L:F] = 2$ the exact sequence of Galois groups

$$1 \to \mu_2 \to G(L/K) \to G \to 1$$
determines an element in the second cohomology group, since it is an extension of $\mu_2$ by $G$. Here we replaced $\text{Gal}(L/K)$ by $\mu_2$ since they are isomorphic as $G$-modules. This induces a map

$$\theta : \mathcal{O}(F/K) \to H^2(G, \mu_2)$$

where $\theta(F)$ is defined as the trivial class. We will show later that $\theta$ is in fact a homomorphism. An explicit formula can be given as follows.

Given $< x >$ in $H^0(G, F^* \times F^* 2)$ we have $\frac{x^g}{x} = s_g^2$ for some $s_g$ in $F^*$, hence

$$s_g \cdot s_h^2 = f(g, h) \cdot s_{gh}$$

with $f(g, h)$ in $\mu_2$. Then $\theta(<x>)$ is the class of the cocycle $f$.

See proof in §6.

2.4 THEOREM: The following sequence is exact

$$\mathcal{O}(F/K) \rightarrow H^2(G, \mu_2) \rightarrow \text{Br}_2(F/K).$$

Here the first map induced by the natural inclusion and $\phi$ is induced in cohomology by the inclusion $\mu_2 \to F^*$, followed by the crossed product map.

Proof: See §6. □

2.5 Remark: The exactness at $H^2$ gives a known criterion for an embedding problem: there is an extension with cocycle $f$, i.e.: there is an $L$ such that $\theta(L) = f$ iff $\phi(f)$ is trivial in the Brauer group. See for example [Br], [Fr], [Wi].

In order to get a first corollary we need the following:
2.6 Lemma: Let $F / K$ be a finite extension and $x$ an element in $F^*$ then there is a $y$ in $F^*$ such that $< x > = < y >$ and $Tr_{F/K}(y)$ is not zero.

Proof: Suppose $Tr_{F/K}(x, z^2) = 0$ for all $z$ in $F$ then replacing $z$ by $z + 1$ and expanding under the assumption char is not 2, we get $Tr_{F/K}(x, z) = 0$ for all and so $x = 0$. ■

2.7 Corollary: (Warr [Wr, Lemma 2.1]) If $F$ is pythagorean (i.e., all sums of squares in $F$ are squares in $F$) then the image of $θ$ is trivial, hence all extensions $L / K$ in $Q(F / K)$ have the direct product $G. μ_2$ as Galois group.

Proof: Let $L = F(√x)$ and $Tr_{F/K}(x)$ not zero. Such an element exists by the lemma. Then $\frac{x^2}{x} = s^2$ for some $s$ in $F^*$ and $\frac{Tr_{F/K}(x)}{x} = \sum_2 s^2$ is a square in $F$ since $F$ is pythagorean. So $< x > = < Tr_{F/K}(x) >$ and the result follows. ■

§3 The exponent two case.

3.1 Motivation: We now restrict ourselves to the case where $Gal(F / K)$ has exponent two.

Because we would like to view this Galois group as a vector space over the field of two elements, we will denote it by $V$. Also $U$ will stand for a finite dimensional subspace of $K^* / K^{*2}$ (here again viewed as vector spaces over the field of two elements). Given $u$ in $U$, $a_u$ will denote a representative in $K^*$.

3.2 Proposition: Given $U$ as above let $F = K(√U)$, that is, $F$ is $K$ with all $\sqrt{a_u}$ adjoining, for $u$ in $U$, (defined in some fixed algebraic closure). Then:

(i) $F / K$ is Galois. Let $V = Gal(F / K)$

(ii) Let $V^* = Hom(V, μ_2)$ be the dual vector space. The following map is an isomorphism.

$$
\begin{align*}
U & \to V^* \\
U & \to (v \to \frac{\sqrt{a_u}v}{\sqrt{a_u}})
\end{align*}
$$
Proof: This is standard Kummer theory and can be found for example in [La]. \[ \blacksquare \]

3.3 PROPOSITION: Let $S^2(V^*)$ be the degree two symmetric algebra on $V^*$. Then the identity map on the group of functions $V \times V \to \mu_2$ yields an isomorphism:

$$H^2(V, \mu_2) \cong S^2(V^*)$$

Proof: This is a consequence of the Künneth formula, see for example [HS, VI 15]. It can also be proven directly. In fact there is a ring isomorphism between the cohomology ring and the symmetric algebra, but we will not need this. \[ \blacksquare \]

3.4 Remark: Note that the degree two algebra on the dual space can be viewed as the group, with pointwise addition, of quadratic forms on $V$.

From now on we will identify these two groups and keep the names for the maps $\theta$ and $\phi$ as in Theorem 2.4 above. Also according to 3.2 (ii) every element in $S^2(V^*)$ can be written as

$$\sum_{i < j} u_i \cdot u_j$$

for some $u_i$ in $U$.

3.5 PROPOSITION: If $u, w$ are in $U$ then $\phi(u, w) = [u, w]$ in the Brauer group. Here $[u, w]$ is the class of the quaternion algebra $\langle u, w \rangle / K$.

Proof: See for example [Sp, §4], [Se] \[ \blacksquare \]

The Galois groups of extensions in $Q(F/K)$, where $Gal(F/K)$ is of exponent two, are the extensions of $\mu_2$ by some finite vector space $V$ (over the field of two elements). These groups are called 2-extra-special groups (see [Hu]). From 3.3 and 3.5 we deduce that the criterion 2.5 applied to these groups can be expressed in terms of a vanishing product of quaternion algebras. This is summarized in 3.7.
We now calculate properties of these groups in more detail. They can be classified by the quadratic forms over $V$ as 3.3 and 3.4 indicate. Denote by $\#$ the product of two such groups where we identify their copies of $\mu_2$. Also for such a group $G$ let $G^r = G \# \ldots \# G$ ($r$ times). Then this amalgamated product corresponds to the orthogonal sums of the corresponding quadratic forms.

For a quadratic form $q$ on $V$ let:

$$b(v, w) = q(v + w) - q(v) - q(w)$$

be the associated bilinear form.

$$V' = \{ v \in V \mid b(v, w) = 0 \text{ for all } w \in V \}$$

be the radical of $V$.

$$V'' = \{ v \in V' \mid q(v) = 0 \}$$

$q'$ be $q$ projected on $V / V''$, so that $q'$ is nonsingular iff $V' = V''$.

$$\Delta(q) = \text{Arf invariant of } q' \text{ when nonsingular and } 0 \text{ otherwise.}$$

$$n = \dim(V / V'').$$

$h = \text{codimension of a maximal totally isotropic subspace of } V.$ (This does not depend on the subspace chosen.)

Using the standard classification of these quadratic forms, we see that there are essentially three types of groups ($[Hu]$). They correspond to the following cocycles:

**Type 1:** $u_1 u_2 + \ldots + u_{n-1} u_n$ $n$ even

**Type 2:** $u_1 u_2 u_3 + u_1 u_2 + \ldots + u_{n-1} u_n$ $n$ even

**Type 3:** $u_1 u_2 u_3 + \ldots + u_{n-1} u_n$ $n$ odd

for some independent set $u_1, \ldots, u_n$ in $U = V^*$, the dual vector space.

Types 1 and 2 correspond to nonsingular quadratic forms of dimension $n$ and Arf invariant 0 and 1, respectively. Type 3, $n = 1$ is $C_4$, cyclic of order 4. Type 1, $n = 2$ is $D_4$, the dihedral group of order 8. Type 2, $n = 2$ is $H_8$, the quaternionic group of order 8.

It is not hard to see that

for type 1 $h = n/2$

for type 2 $h = n/2 + 1$
for type 3 \( h = \frac{n+1}{2} \)

So, after some simplification, \( h \) is seen to be the minimum number of symbols \( u, w \) needed to define \( q \).

We see then that any such group can be written as follows:

\[
(D_4^r \# H_8^{q_1} \# C_4^t) \times V^n.
\]

Here \( r > 0 \) and \( t = 0 \) or 1. This decomposition is not unique but the only relations are:

\( H_8 \# H_8 = D_4 \# D_4 \) and \( H_8 \# C_4 = D_4 \# C_4 \)

3.6 THEOREM: Let \( U \) be a subspace of \( K^+ / K_{2 \times 2} \) and let \( F = K(\sqrt{U}) \).

Then there exists an extension \( L / K \) containing \( K \) with Galois group isomorphic to

\[
D_4^r \# H_8^{q_1} \# C_4^t \times V^n
\]

iff there is an independent set \( \{ u_1, \ldots, u_n \} \) in \( U \)

with \( n = 2r + t \), such that

\[
\Delta(q) \cdot ([u_1, u_1] + [u_2, u_2] + [u_n, u_n] + [u_1, u_2] + \ldots + [u_{2r-1}, u_{2r}] = 0.
\]

\textit{Proof:} It follows from considerations above, after some calculation. $\blacksquare$

3.7 \textit{Remark:} We can handle the groups with \( h < 3 \) in an elementary way (see 4.5); for example the conditions above can be given in terms of quadratic forms instead of quaternion symbols. This follows in the standard way from the fact that only two such symbols are involved. Here is a list of those groups.

(i) \( C_4 \), (ii) \( D_4 \), (iii) \( H_8 \), (iv) \( C_4 \# D_4 \) and (v) \( D_4 \# D_4 \).

The cases (i), (ii) and (iii) are classical, see [Wi], [Lm, ex: VII.8] and [Le]. The general case is given in [Le]. See also [Fr] and [Ms].
We can now give the exponent two version of the main exact sequence

3.8 Theorem: The following sequence is exact

\[ 1 \to Q(\sqrt{2}/K) \xrightarrow{\Theta} S^2(K^*/K^{*2}) \xrightarrow{\phi} \text{Br}_2(K) \]

Here, \( K^{(2)} \) denotes the field \( K \) with all its square roots adjoined (as usual, in some fixed algebraic closure).

Proof: It follows easily from Thm. 2.4 and the considerations above by taking the limit on all finite dimensional subspaces \( U \). \( \blacksquare \)
§4 Relation to the injectivity in Merkurjev's Theorem.

Merkurjev's theorem states that the natural map \( k_2(K) \to \text{Br}_2(K) \) is an isomorphism, for any field of characteristic not two. (See [Me], [Wa],[Ar].) We will now show how the injectivity in this theorem can be restated in terms of Galois extensions.

4.1 PROPOSITION: Let \( F = K(\sqrt{a}) \) for \( a \) in \( K^* \) then the natural map

\[
\psi: F^* \to Q(K^{[2]}|K)
\]
\[
x \mapsto K^{[2]}(\sqrt{x})
\]

satisfies \( \theta \psi(x) = <a> \cdot <N(x)> \). (Here \( N = N_{F/K} \))

(This relates to a construction formula given, for example, in [Ta, 3.2].)

Proof: For any \( \nu \) in \( \text{Gal}(K^{[2]}|K) \) we have

\[
\frac{x^\nu}{x} = 1 \text{ or } \frac{N(x)}{x^2}
\]

so the map is well defined, since \( N(x) \) is in \( K \) and hence is a square in \( K^{[2]} \). After some calculation the claim follows from the formula for \( \theta \) given in 2.3.  

4.2 PROPOSITION: The injectivity in Merkurjev's theorem \( k_2(K) \to \text{Br}_2(K) \) is equivalent to the following:

Every Galois extension \( L/K \) containing \( K^{[2]} \) with \( [L:K^{[2]}] = 2 \) is of the form

\( K^{[2]}(\sqrt{x}) \) with \( x = x_1 \ldots x_n \) for some \( x_i \) in \( K(\sqrt{a_i}) \), \( a_i \) in \( K \).
**Proof:** From the definition given in §1: $k_2(K)$ is $S^2(K^* / K^{*2})$ divided by the subgroup generated by all $<a>, <b>$ with $[a, b] = 0$ or equivalently, with $b = N(x)$ for some $x$ in $K(\sqrt{a})$. The result now follows from 4.1. •

4.3 Remark: In general the statement in Prop. 4.2 does not hold if $K^{(2)}$ is replaced by some intermediate field. Precisely, if $F = K(\sqrt{U})$ and $L = F(\sqrt{x})$ is Galois over $K$, then $K^{(2)}(\sqrt{x}) / K$ is Galois. Hence 4.2 applies and $x = x_1 \ldots x_n$ modulo squares in $K^{(2)}$ for some $x_i$ in $K(\sqrt{a_i})$, $a_i$ in $K$. Now, there is no way to assure that in general $<a_i>$ will belong to $U$.

A counterexample for $h = 3$, though in a different setting, can be found in [Ti, Ch 4] and [STW]. However, it is true for $h < 3$, i.e. for all cases listed in 3.7, where the following lemma can be used instead of Merkurjev's Theorem.

4.4 Lemma: Given two quaternion symbols $[a, b]$ and $[c, d]$ then the following are equivalent:

(i) There is an element $e$ such that $[a, b, e] = [c, d, e] = [a, c, e] = 0$

(ii) $[a, b] = [c, d]$

**Proof:** See for example [LM, p.69 Ex 12]. •

4.5 Proposition: Let $L/K$ be a Galois extension with group isomorphic to some of the groups listed in 3.7 (groups with $h < 3$). Let $F = K(\sqrt{U})$ be the extension of index two contained in $L$. Then $L$ can be written in the following form:

$L = F(\sqrt{x, y, z})$ where $x \in K(\sqrt{a})$, $y \in K(\sqrt{b})$,

$z \in K(\sqrt{a, b})$ and $<a>, <b>$ are some independent classes in $U$.

**Proof:** It follows from 3.6, 4.1 and 4.4. •
4.6 Remark: The elements $x$, $y$ and $z$ can be worked out quite explicitly in any specific example. Also in the quaternion case, if at least one among $a$, $b$ or $ab$ is a sum of two squares in $K$, then only two of $x$, $y$ and $z$ are needed. For example: when $a = 2$ and $b = 3$ we get $x = 2 + \sqrt{2}$, $y = 3 + \sqrt{3}$ and $z = 1$, hence

$$Q(\sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}) \subset Q$$

has quaternion Galois group. (Here $Q$ is the field of rational numbers).

Another interesting feature of the quaternion case is the fact that there is an unique cocycle associated to it; i.e. up to isomorphisms $H_3$ can satisfy only one exact sequence of the form

$$1 \to \mu_2 \to H_3 \to V \to 1.$$ 

This implies that if $L = F(\sqrt{x}) \subset K$ has quaternion Galois group then all other such extensions are of the form $L' = F(\sqrt{ax})$ with $a \in K^*$. In the form given in 4.5 is how quaternion extensions are usually constructed (e.g. [De], [Ja]). I have not found in the literature that it yields all possible ones. Witt's original approach using spinor norms ([Wi]) will be considered in §5.

We now restate slightly the condition given in Prop. 4.2 so that it becomes the case $n = 1$ of the more general question below. We do not know of any possible interest in this question, apart from its appealing symmetry.

4.7 Question: Does the following hold for $n > 0$? (The case $n = 1$ is injectivity in Merkurjev's thm.)

Given $x$ in $K[2]$

$N_{K(2)}(x)$ is a square in $K[2]$ for all subfields $K$ of index $2^n$.
\[ x = x_1 \ldots x_n \mod K^{(2)} \] for some \( x_i \) in \( K_i \) with \( [K_i : K] = 2^n \)

\section*{5 Using spinor norms.}

Let \( \langle a_1, \ldots, a_n \rangle \) and \( \langle b_1, \ldots, b_n \rangle \) be two equivalent quadratic forms over \( K \). For simplicity, in what follows \( n \) is assumed to be even. The other case can be handled in much the same way (we will use \( n = 3 \) in the corollary below).

Say \( M \) in \( K^{n \times n} \) gives the change of basis, i.e:

\[ M \cdot \text{diag}(a_1, \ldots, a_n) \cdot M^t = \text{diag}(b_1, \ldots, b_n) \]

(Here \( \text{diag}(a, b, c, \ldots) \) stands for the diagonal matrix with entries \( a, b, c \ldots \) along the diagonal.)

Consider the matrix:

\[ M' = \text{diag}(\sqrt{b_1^{-1}}, \ldots, \sqrt{b_n^{-1}}) \cdot M \cdot \text{diag}(\sqrt{a_1}, \ldots, \sqrt{a_n}) \]

Then it is clear that \( M' \) belongs to the orthogonal group \( O(n) \), over the field \( F \) obtained by adjoining to \( K \) \( \sqrt{a_1}, \ldots, \sqrt{a_n}, \sqrt{b_1}, \ldots, \sqrt{b_n} \). Denote by \( V \) the Galois group of \( F/K \). Then for any \( \nu \in V \), \( (M')^\nu = R_\nu \cdot M' \cdot S_\nu \) where \( R_\nu \) and \( S_\nu \) are diagonal matrices with signs.

Therefore, the spinor norm of \( M' \), \( \text{sp}(M') \), is fixed by \( V \)

(as a square class). I.e. \( \text{sp}(M') \) belongs to \( Q(F/K) \). The natural question is then: what is \( \Theta \text{sp}(M') \)?

We answer this in the following (compare [Sp]).

\subsection*{5.1 PROPOSITION:} With \( M' \) defined as above we have
\[ \theta \text{sp}(M) = \sum_{i<j} (\langle a_i, a_j \rangle + \langle b_i, b_j \rangle) \]

**Proof:** Let \( C(n) \) be the Clifford algebra of the form \( \langle 1, \ldots, 1 \rangle \) over the field \( F \), with \( V \) acting in a natural way. Consider the Clifford group: \( \Gamma = \{ c \in C(n) : c \text{ is invertible and } c \cdot E \cdot c^{-1} = E \} \). Here \( E \) denotes the underlying quadratic space in \( C(n) \).

We have then the following exact sequence (recall \( n \) is assumed to be even):

\[
1 \to F^n \to \Gamma \to \text{O}(n) \to 1
\]

Here \( i \) is the natural inclusion and \( \omega : c \to (e \to c \cdot e \cdot c^{-1}) \), for \( e \in E \).

(See for example [Lm]). We will use the following description of the algebra \( C(n) \):

Let \( U \) be an \( n \)-dimensional vector space over the field of two elements. Fix a basis \( u_1, \ldots, u_n \) for \( U \) and consider the bilinear map \( \delta \), defined by:

\[ \delta(u_i, u_j) = 1 \text{ if } i < j \text{ and } 0 \text{ otherwise.} \]

Let also \( q(u) = \delta(u, u) \) be its associated quadratic form on \( U \).

Let \( \{ X_u, u \in U \} \) be an independent set over \( F \), then view \( C(n) \) as span \( \{ X_u \} \) with the product:

\[ X_u \cdot X_w = (-1)^{\delta(u, w)} \cdot X_{u+w} \]

Here \( E \) corresponds to \( \text{span} \{ X_{u_i} \}, i = 1, \ldots, n \).
Also the 'bar' involution, defined as the antiautomorphism of \( C(n) \) which is the identity on \( E \), is described on this basis as:

\[
\bar{X}_u = X_u^{-1} = (-1)^{\mu(u)} X_u .
\]

For \( c \) in \( C(n) \) define \( N(c) = c \cdot \bar{c} \) then we have \( sp \omega(c) = \langle N(c) \rangle \).

Let now \( c \) be such that \( \omega(c) = M' \) then for any \( v \) in \( V \)

\[
c' = s_v \cdot X_{c(u)} \cdot c \cdot X_{u(u)}
\]

where \( c_u \) is in \( P^* \) and \( r, t : V \to U \) are some linear maps.

Let \( x = N(c) \) then after some calculation we see that

\[
\frac{x^v}{x} = s_v^2 \quad \text{with} \quad s_v \cdot s_w^v = f(v, w) \cdot s_{v+w} \quad \text{and} \quad f(v, w) \text{ in } \nu_2
\]

where \( f \) corresponds to

\[
\sum_{1 < j} (\langle a_1 \rangle, \langle a_j \rangle, + \langle b_1 \rangle, \langle b_j \rangle)
\]

The result now follows from the formula for \( \theta \) given in 2.3.

5.2 COROLLARY: \( \theta sp(M') \) only depends on the isometry classes of the quadratic forms

\( \langle a_1, \ldots, a_n \rangle \) and \( \langle b_1, \ldots, b_n \rangle \)

Proof: It is clear.
5.3 Example: Let $<a>$ and $<b>$ be independent classes in $K^*/K^{*2}$ and suppose that the forms $<1,1,1>$ and $<a,b,a.b>$ are equivalent over $K$. Consider

$$x = sp(M')$$

as in the above proposition. Also, let

$$F = K(\sqrt{a}, \sqrt{b})$$

and

$$L = F(\sqrt{x})$$

then $Gal(L/K)$ is isomorphic to the quaternion group $H_3$. (See remark 4.6).

Proof: We see that

$$<a>.<b> + <a>.<a.b> + <b>.<a.b>$$

$$= <a>.<a> + <a>.<b> + <b>.<b>$$

and this corresponds to $H_3$ (see 3.6). 

5.4 Remark: The above is Witt's result [Wi], though in a different form. To relate both results is enough to use the fact that for any orthogonal $3 \times 3$ matrix $M'$ with $det = 1$ (i.e., a rotation) and with no -1 eigenvalue $sp(M') = <1 + tr(M')>$

(If $M'$ has $det = -1$ we multiply it by the reflection diag (1, 1, -1). This does not change its spinor norm).

Over the rational numbers, as Witt mentions, we have:

$$sp(M') = <\cos^{2}\alpha>$$

where $\alpha$ is the angle of rotation.

5.5 Proposition: Let $x$ be $sp(M')$ as in 5.1 above then $x$ can be written as

$$x = x_1 \ldots x_n$$

modulo squares in $K(2)$ for some $x_i$ in $K(\sqrt{e_1})$, $e_1$ in $K$. (Compare with 4.2).

Proof: Given three quadratic forms $q_1$, $q_2$, $q_3$ over $K$, suppose $M$ is an equivalence between $q_1$ and $q_2$, and $N$ an equivalence between $q_2$ and $q_3$. It is easy to check that $(M, N)' = M', N'$ so that $sp((M,N)') = sp(M'). sp(N')$. The result now follows, after some calculation, from Witt's chain equivalence theorem that states that any equivalence can be written as a product of equivalences, each modifying at most two slots at a time. (See [Lin]).

§6 Proof of Theorem 2.4.

Consider the short exact sequences
\[ 1 \rightarrow \mu_2 \rightarrow F^* \rightarrow F^{*2} \rightarrow 1 \]

\[ 1 \rightarrow F^{*2} \rightarrow F^* \rightarrow F^*/F^{*2} \rightarrow 1 \]

where all maps are the natural ones.

They determine the following long exact sequence of cohomology:

\[ \cdots \rightarrow H^0(G, F^*) \rightarrow H^0(G, F^*/F^{*2}) \rightarrow H^1(G, F^{*2}) \rightarrow H^1(G, F^*) \rightarrow \cdots \]

\[ \cdots \rightarrow H^1(G, F^*) \rightarrow H^1(G, F^{*2}) \rightarrow H^2(G, \mu_2) \rightarrow H^2(G, F^*) \rightarrow \cdots \]

Recall that by Hilbert's theorem 90 we have: \( H^1(G, F^*) = 1 \). Therefore both sequence can be spliced together into one. Also, \( H^0(G, F^*) = K^* \) by Galois theory.

\( H^0(G, F^*/F^{*2}) \) can be replaced by \( Q(F/K) \), by Lemma 2.2 and \( H^2(G, F^*) \) can be imnersed via the crossed product construction, into the 2-torsion of the Brauer group of \( K \). Hence we end up with the following exact sequence:

\[ K^* \rightarrow Q(F/K) \rightarrow H^2(G, \mu_2) \rightarrow Br_2(K). \]

It is not hard to check that the map \( j \) here corresponds to the formula for \( \Theta \) given 2.3. Therefore, it now only remains to prove that they are in fact the same map. Recall that \( \Theta \) was defined in terms of the sequence of Galois groups and hence it is not immediate that it should equal the map \( j \) obtained from the cohomology sequences.
So let \( L = F(\sqrt[3]{x}) \) and \( \frac{x^2}{x} = z_y^2 \), for some \( z_y \) in \( F^* \). It is easy to see that for each \( g \in G \)

we can choose \( \bar{g} \in \text{Gal}(L/K) \) such that \( \frac{\sqrt[3]{x}}{\sqrt[3]{x}} = z_g \). Then

\[
z_g \cdot z_h = f(g, h) \cdot z_{gh} \quad \text{with} \quad f(g, h) \quad \text{in} \quad \mu_2 \quad \text{and} \quad \sqrt[3]{x} \cdot \bar{g} \cdot \bar{h} = f(g, h) \cdot \sqrt[3]{x} \cdot \bar{h}
\]

Hence the cocycle associated with the Galois groups is also the class of \( f \) and the proof is finished. \( \blacksquare \)

References:


Fernando Rodriguez Villegas.

Mathematics Department, Ohio State University.

231 W 18 Ar. Columbus Ohio 43210.