Relations between quadratic forms and certain Galois extensions.

by Fernando Rodriguez Villegas .

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 $[L : F] =$ 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 $Br(K)$, 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 , [Br] . Further references can be found in [Wi] , [Fr] , [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 $Gal(F / K)$ is of exponent two and rephrase the main exact sequence in Theorem 3.8 . In section 4 we restate the injectivity $k_2(K) \rightarrow Br_2(K)$ 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 ([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.

$Br_2 (K)$ 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 $Br_2 (K)$.

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 $Gal(F / K) = G$, we are interested in the following set of extensions of F contained in some fixed algebraic closure.

2.1 *Definition* :

$\mathbf{Q}(F / K) = \{ L : L \supseteq F , L / K$ 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 .

$\mathbf{Q}(F / K)$ can be interpreted as a cohomology group .

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

Proof : Let a be in F^* then $F(\sqrt{x}) / K$ is normal $\Leftrightarrow F(\sqrt{x}) = F(\sqrt{x^g})$ for all g in $G \Leftrightarrow \frac{x^g}{x}$ is in F^{*2} for all g in $G \Leftrightarrow < x >$ 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 $\mathbf{Q}(F / K)$. Then $F(\sqrt{x}) * F(\sqrt{y}) = F(\sqrt{x.y})$. The identity element , of course , is F . Also , we will sometimes identify $\mathbf{Q}(F / K)$ with its image in F^* / F^{*2} .

2.3 *Definition*: Given L in $\mathbf{Q}(F / K)$ 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 μ_2 by G. Here we replaced $Gal(L/K)$ by μ_2 since they are isomorphic as G-modules . This induces a map

$$\theta : Q(F/K) \to H^2(G, \mu_2)$$

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

Given $< x >$ in $H^0(G, F^*/F^{*2})$ we have $\frac{x^g}{x} = s_g^2$ for some s_g in F^*, hence $s_g \cdot s_h^g = f(g,h) \cdot s_{hg}$ with $f(g,h)$ in μ_2 . Then $\theta(< x >)$ is the class of the cocycle f . See proof in §6.

2.4 THEOREM : The following sequence is exact

$$K^* \to Q(F/K) \overset{\theta}{\to} H^2(G, \mu_2) \overset{\phi}{\to} Br_2(F/K).$$

Here the first map induced by the natural inclusion and ϕ 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 : (Ware [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 $\mathbf{Q}(F / K)$ have the direct product $G . \mu_2$ as Galois group .

Proof : Let $L = F(\sqrt{x})$ and $Tr_{F/K}(x)$ not zero . Such an element exists by the lemma . Then $\frac{x^g}{x} = s_g^2$ for some s_g in F^* and $\frac{Tr_{F/K}(x)}{x} = \sum_g s_g^2$ 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 *Notation*: 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 $F = K(\sqrt{U})$, that is , F is K with all $\sqrt{a_u}$ adjoined , for u in U , (defined in some fixed algebraic closure) . Then :

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

(ii) Let $V^* = Hom(V, \mu_2)$ be the dual vector space . The following map is an isomorphism .

$$U \rightarrow V^*$$

$$u \rightarrow \left(v \rightarrow \frac{\sqrt{a_u}^{\,v}}{\sqrt{a_u}} \right)$$

Proof: This is standard Kummer theory and can be found for example in [La] . ■

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 . ■

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 θ and ϕ 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 $\phi(u \cdot w) = [u, w]$ in the Brauer group . Here [u , w] is the class of the quaternion algebra in (u , w) / K .

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

The Galois groups of extensions in $\mathbf{Q}(F/K)$, where $Gal(F/K)$ is of exponent two , are the extensions of μ_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 μ_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.

$V' = \{ v \text{ in } V \mid b(v, w) = 0 \text{ for all } w \text{ in } V \}$ be the radical of V .

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

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

$\Delta(q)$ = Arf invariant of q' when non singular and 0 otherwise .

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

h = 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 : $u_1 . u_1 + u_2 . u_2 + u_1 . u_2 + \ldots + u_{n-1} . u_n$ n even

Type 3 : $u_1 . u_1 + u_2 . u_3 + \ldots + u_{n-1} . u_n$ 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 $\quad h = (n + 1) / 2$

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

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

$$(D_4^r \# H_8^{\Delta(q)} \# C_4^t) \times V'' .$$

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} and let $F = K (\sqrt{U})$.

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

$D_4^r \# H_8^{\Delta(q)} \# C_4^t \times V''$ iff there is an independent set $\{ u_1 , \dots , u_n \}$ in U

with $n = 2.r + t$, such that

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

Proof : It follows from considerations above , after some calculation . ■

3.7 *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

$$1 \quad \rightarrow \quad Q(K^{(2)}/K) \quad \overset{\theta}{\rightarrow} \quad S^2(K^*/K^{*2}) \quad \overset{\phi}{\rightarrow} \quad Br_2(K)$$

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 . ■

§4 Relation to the injectivity in Merkurjev's Theorem.

Merkurjev's theorem states that the natural map $k_2(K) \to Br_2(K)$ 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

$$\psi : \quad F^* \to Q(K^{(2)}/K)$$
$$x \to K^{(2)}(\sqrt{x})$$

satisfies $\theta\psi(x) = \langle a \rangle . \langle N(x) \rangle$. (Here, $N = N_{F/K}$)

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

Proof: For any ν in $Gal(K^{[2]}/K)$ 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 θ given in 2.3. ■

4.2 PROPOSITION : The injectivity in Merkurjev's theorem $k_2(K) \to Br_2(K)$ 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 $K^{(2)}$ y 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 *Quaternion slot 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 wich group is 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 a.b 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

$$Q\left(\sqrt{(2 + \sqrt{2}).(3 + \sqrt{3})}\right) / Q$$

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_8 can satisfiy only one exact sequence of the form

$$1 \rightarrow \mu_2 \rightarrow H_8 \rightarrow V \rightarrow 1 .$$

This implies that if $L = F(\sqrt{x})$ / K has quaternion Galois group then all other such extensions are of the form $L' = F(\sqrt{a.x})$ 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 $K^{[2]}$

$N_{K^{(2)}/F}(x)$ is a square in $K^{[2]}$ for all subfields of index 2^n

$\Leftrightarrow$

$x = x_1 \cdot \ldots \cdot x_n$ modulo squares in $K^{(2)}$ for some x_i in K_i with $[K_i : K] = 2^n$

§5 Using spinor norms.

Let $< a_1 , \ldots , a_n >$ and $< b_1 , \ldots , b_n >$ 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:

$$M \cdot \mathrm{diag}(a_1, \ldots , a_n) \cdot M^t = \mathrm{diag}(b_1, \ldots , b_n)$$

(Here diag(a, b, c, ...) stands for the diagonal matrix with entries a, b, c ... along the diagonal).

Consider the matrix :

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

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 $v \in V$, $(M')^v = R_v \cdot M' \cdot S_v$ where R_v and S_v are diagonal matrices with signs. Therefore, the spinor norm of M', sp(M'), is fixed by V (as a square class). I.e: sp(M') belongs to $Q(F / K)$. The natural question is then what is θ sp(M') ? We answer this in the following (compare [Sp])

5.1 PROPOSITION : With M' defined as above we have

$$\theta\, sp(M') = \sum_{i<j} (< a_i >. < a_j >. \quad + \quad < b_i >. < b_j >)$$

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

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

$$1 \rightarrow F^* \xrightarrow{i} \Gamma \xrightarrow{\omega} O(n) \rightarrow 1$$

Here i is the natural inclusion and $\omega : c \rightarrow (e \rightarrow c . e . c^{-1})$, 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 δ, defined by :

$\delta(u_i , u_j) = 1$ if $i < j$ and 0 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 :

$$X_u . X_w = (-1)^{\delta(u,w)} X_{u+w}$$

Here E corresponds to 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 :

$$\bar{X}_u = X_u^{-1} = (-1)^{q(u)} \cdot X_u$$

For c in $C(n)$ define $N(C) = c \cdot \bar{c}$ then we have $sp\,\omega(c) = <N(c)>$.

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

$$c^v = s_v \cdot X_{r(u)} \cdot c \cdot X_{t(u)}$$

where c_v is in F^* and $r, t: V \to U$ are some linear maps .

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

$$\frac{x^v}{x} = s_v^2 \qquad \text{with} \qquad s_v \cdot s_w^v = f(v,w) \cdot s_{v+w} \quad \text{and} \quad f(v,w) \text{ in } \mu_2$$

where f corresponds to

$$\sum_{i<j} (<a_i>.<a_j>. \; + \; <b_i>.<b_j>)$$

The result now follows from the formula for θ given in 2.3 . ■

5.2 COROLLARY : $\theta\, sp(M')$ only depends on the isometry classes of the quadratic forms $<a_1, \ldots, a_n>$ and $<b_1, \ldots, b_n>$

Proof : It is clear . ■

5.3 *Corollary* : 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_8 . (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_8 (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 3×3 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 :

$$sp(M') = < \cos^2 \frac{\alpha}{2} > \quad \text{where } \alpha \text{ is the angle of rotation .}$$

5.5 PROPOSITION : Let x be $sp(M')$ as in 5.1 above then x can be written a $x = x_1 . \ldots . x_n$ modulo squares in $K^{(2)}$ for some x_i in $K (\sqrt{a_i})$, a_i 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 [Lm]) . ■

§6 Proof of Theorem 2.4 .

Consider the short exact sequences

$$1 \to \mu_2 \to F^* \to F^{*2} \to 1$$

$$1 \to F^{*2} \to F^* \to F^*/F^{*2} \to 1$$

where all maps are the natural ones .

They determine the following long exact sequence of cohomology :

$$\ldots \to H^0(G, F^*) \to H^0(G, F^*/F^{*2}) \to H^1(G, F^{*2}) \to H^1(G, F^*) \to \ldots$$

$$\ldots \to H^1(G, F^*) \to H^1(G, F^{*2}) \to H^2(G, \mu_2) \to H^2(G, F^*) \to \ldots$$

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 inmersed ,via the crossed product construction , into the 2-torsion of the Brauer group of K. Hence we end up with the following exact sequence :

$$K^* \to Q(F/K) \xrightarrow{j} H^2(G, \mu_2) \to Br_2(K).$$

It is not hard to check that the map j here corresponds to the formula for θ given 2.3 . Therefore , it now only remains to prove that they are in fact the same map . Recall that θ 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 $L = F(\sqrt{x})$ and $\frac{x^g}{x} = s_g^2$, for some s_g in F^*. It is easy to see that for each $g \in G$ we can choose $\bar{g} \in Gal(L/K)$ such that $\frac{\sqrt{x}^{\bar{g}}}{\sqrt{x}} = s_g$. Then

$$s_g \cdot s_h^g = f(g,h) \cdot s_{hg} \quad \text{with} \quad f(g,h) \text{ in } \mu_2 \text{ and } \sqrt{x}^{\bar{g}.\bar{h}} = f(g,h) \cdot \sqrt{x}^{\overline{g.h}}$$

Hence the cocycle associated with the Galois groups is also the class of f and the proof is finished ■

References :

[Ar] J . Arason : A proof of Merkurjev's theorem . Quadratic forms and Hermitian K - theory . Canad. Math . Soc. Conf . Proc . No. 4 (1984) .

[Br] R. Brauer : Über die Konstruktion der Schiefkörper , die von endlichen Raug in bezug auf ein gegebenes Zentrum sind . J reine angew Math .Band 168 (1932) 44 - 64 .

[De] R . Dean : A rational polynomial whose group is the quaternions .A M M.Vol .88 No.1 42-45 .

[Fr] A . Frölich : Orthogonal representations of Galois groups , Stiefel - Whitney classes and Hasse - Witt invariants. J . Reine Angew Math , Band 360 (1985) 84 -123 .

[Hu] Huppert : Endliche Gruppen Vol 1 Ch 3 §13 . Springer - Verlag .

[HS] P.J.Hilton , U. Stammbach : A course in homological algebra . Springer - Verlag GTM 4 (1971) .

[Ja] N.Jacobson : Lectures in abstract algebra Vol 3 , (New York 1953).

[La] S.Lang : Algebra .Addison - Wesley Publ. Reading Mass. (1965) .

[Le] D.Leep : Preliminary report . A .M. S. meeting , San Antonio (1987).

[Lm] T.Y.Lam : The algebraic theory of quadratic forms . W. A . Benjamin Publ . Reading. Mass (1965).

[Me] A . Merkurjev : On the norm residue symbol of degree 2 . Dokladi Akad.Nauk.SSSR 26 (1981) 542 - 547 .

[Ms] R.Massy : Constructions de p-extensions galoisiennes d'un corps de characteristique différente de p , to appear .

[Se] J.P.Serre : Local Fields . Springer - Verlag GTM 67 (1979) .

[Sh] I.R.Shafarevitch : On the construction of fields with a given Galois group of order l^a . AMS transl. Ser 2 Vol 4 107 - 142 . Izv Akad. Nauk. SSSR Ser. Mat. 18 216 - 296 (1954) .

[Sp] T.A.Springer : On the equivalence of quadratic forms. Proc. Ned . Acad. Sci. 62 (1959) 241 - 253 . .

[STW] D.Shapiro , J.P.Tignol and A.Wadsworth : Witt rings and Brauer groups under multiquadratic extensions II . Journal of Algebra . Vol 78 No 1 (1982) 58 - 90 .

[Ta] J.Tate : Relations between K_2 and Galois cohomology . Invent. Math. Vol 36 257 - 274 (1976) .

[Ti] J.P.Tignol : Corps à involution de rang fini sur leur centre et de caractéristique différente de 2 . Doctoral dissertation Univ. Catholique de Louvain. Louvain - La - Neuve . Belgium (1979) .

[Wa] A.Wadsworth : Merkurjev's elementary proof of Merkurjev's theorem . Cont.Math. (II) (1986) .

[Wi] E.Witt : Konstruktion von galoisschen Körpern der characteristik p zu vorgegebener gruppe der Ordnung p^f . J.reine angew Math. Band 174 (1936) 237 - 245 .

Fernando Rodriguez Villegas .

Mathematics Department , Ohio State University .

231 W 18 Av. Columbus Ohio 43210 .