Homology, Homotopy and Applications, vol.6(1), 2004, pp.351–362

CLASS 2 GALOIS REPRESENTATIONS OF KUMMER TYPE

HANS OPOLKA

(*communicated by Hvedri Inassaridze*)

Abstract

The purpose of this note is to give a description of class 2 representations of the absolute Galois group of a field k of characteristic 0 which satisfy a certain condition of Kummer type. This description is based on Galois cohomology and on the theory of projective representations of finite abelian groups.

1. Central pairs and twisted group algebras

In this section we recall some well known basic facts from the theory of projective representations and twisted group algebras over fields of characteristic 0, see e.g. [**11**], Kap.V; [**12**]; [**26**]; [**27**].

Let k be a field of characteristic 0 and let $\overline{k}$ be an algebraic closure of k. A *central pair* over k consists of a finite group A and of a central 2-cocycle f on A with values in k^*, i.e. $f : A \times A \to k^*$ is a mapping which satisfies $f(x,y)f(xy,z) = f(x,yz)f(y,z)$ for all $x,y,z \in A$. Two central pairs (A,f), (B,g) are said to be isomorphic if there is an isomorphism $\alpha : A \to B$ such that the cocycle $g_\alpha : A \times A \to k^*$ defined by $g_\alpha(x,y) := g(\alpha(x),\alpha(y))$, $x,y \in A$, is cohomologous to the cocycle f. Every central pair (A,f) over k determines the so called twisted group algebra

$$(k,A,f) = \bigoplus_{x \in A} ke_x, ae_x = e_x a, e_x e_y = f(x,y)e_{xy}$$

for all $a \in k$ and all $x,y \in A$. Since $char(k) = 0$ this k-algebra (k,A,f) is semisimple, see [**26**], Theorem 4.1, p.171.

Examples. (a) We mention the central pair which is constructed by E. Artin in [**1**], p.10 ff, from a nondegenerate quadratic form over k. In this case the corresponding twisted group algebra is isomorphic to the Clifford algebra of the quadratic form.

(b) Assume that the field k contains a primitive root of unity ω of order m, let $a,b \in k^*$ and denote by $A_\omega(a,b)$ the corresponding symbol algebra, i.e. $A_\omega(a,b) = \langle X,Y : XY = \omega YX,\ X^m = a,\ Y^m = b\rangle$. Then there is a central pair $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}, f)$ over k such that $A_\omega(a,b) \cong (k, \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}, f)$. Moreover every tensor product of symbol algebras is isomorphic to (k,A,f) for some central pair (A,f) over k with an abelian group A; see e.g. [**13**], 1.3.21.

Received December 1, 2003, revised July 28, 2004; published on September 25, 2004.
2000 Mathematics Subject Classification: 11R34, 20C25.
Key words and phrases: Galois cohomology, projective representations.
© 2004, Hans Opolka. Permission to copy for private use granted.

There is a bijective correspondence $R \mapsto T$ between the set of (irreducible) representations of the twisted group algebra (k, A, f) and the set of (irreducible) f-cocycle representations of A over k which is given by $R(e_x) = T(x)$, $x \in A$. Moreover, the group $Hom(A, k^*)$ of linear characters of A with values in k^* acts by multiplication on the set of irreducible representations of the twisted group algebra (k, A, f) and therefore on the set of irreducible f-cocycle representations of A over k, see [**12**], §4; [**26**], §5. If $A \cong A_1 \times A_2$ is isomorphic to the direct product of the groups A_1 and A_2 then every central 2-cocycle f on A is cohomologous to the 2-cocycle $g : A \times A \to k^*$ given by

$g((a_1, a_2), (b_1, b_2)) = f(a_1, b_1)f(a_2, b_2)\beta(a_1, b_2)$, $a_1, b_1 \in A_1$, $a_2, b_2 \in A_2$.

$\beta(a_1, b_2) = f(a_1, b_2)/f(b_2, a_1)$

It turns out that $\beta : A_1 \times A_2 \to k^*$, $\beta((a_1, a_2)) = f(a_1, a_2)/f(a_2, a_1)$, is a bimultiplicative pairing, see e.g. [**26**], 2.2. The direct product $A_1 \times A_2$ is said to be *orthogonal* with respect to the central 2-cocycle f if the pairing β is trivial; in this case we write $(A, f) \cong (A_1, f_1) \perp (A_2, f_2)$. The next proposition is obvious.

Proposition 1.1. *If* $(A, f) \cong (A_1, f_1) \perp (A_2, f_2)$ *then there is an isomorphism of* k*-algebras*

$$(k, A, f) \cong (k, A_1, f_1) \otimes_k (k, A_2, f_2)$$

given by $e_{(a_1,a_2)} \mapsto e_{a_1} \otimes e_{a_2}$.

Assume that A is abelian. Then the *symplectic pair* associated with the central pair (A, f) is given by (A, ω_f), where $\omega_f : A \times A \to \mu_k$ is the symplectic pairing on A with values in the group of roots of unity μ_k of k given by $\omega_f(x, y) := f(x, y)/f(y, x)$ for all $x, y \in A$; see [**12**], [**26**], [**27**]. Obviously, if f is cohomologous to another central cocycle g on A, then $\omega_f = \omega_g$. The central pair (A, f) is said to be nondegenerate if the symplectic pairing ω_f is nondegenerate. In this case μ_k contains a primitive root of unity of order $e(A) = \exp(A)$. Moreover, it is easily seen that the center of (k, A, f) is (k, R, f), where $R = R(\omega_f)$ is the kernel=radical of the symplectic pairing ω_f. Hence (k, A, f) is central simple if and only if ω_f is nondegenerate.

Assume that the central pair (A, f) over k with abelian A is nondegenerate. Then according to [**27**] the symplectic pair (A, ω_f) is isomorphic to the orthogonal sum of "hyperbolic planes", i.e.

$$(A, \omega_f) \cong (A_1, \omega_{f_1}) \perp ... \perp (A_r, \omega_{f_r})$$

where A_i is isomorphic to a direct product of two isomorphic cyclic groups and f_i is the restriction of f to A_i, $i = 1, ..., r$. Proposition (1.1) yields

$$(k, A, f) \cong \otimes_{i=1}^{r}(k, A_i, f_i),$$

the isomorphism being given by $e_a \mapsto e_{a_1} \otimes ... \otimes e_{a_r}$ for all $a = (a_1, ..., a_r) \in A = A_1 \times ... \times A_r$. For abelian A, which we are assuming, this decomposition follows also from [**3**], corollary, p. 294. Every algebra in this decomposition is isomorphic to a symbol algebra: $(k, A_i, f_i) \cong A_{\omega_i}(a_i, b_i)$, where $A_i = \langle x_i \rangle \times \langle y_i \rangle$, $m_i =$order$(x_i) =$order(y_i), $\omega_i = \omega_f(x_i, y_i)$, $a_i = e_{x_i}^{m_i}$, $b_i = e_{y_i}^{m_i}$. For every $i = 1, ..., r$ let $\alpha_i, \beta_i \in \overline{k}$ be elements such that $\alpha_i^{m_i} = a_i, \beta_i^{m_i} = b_i$ and put $K_i := k(\alpha_i, \beta_i)$. Every extension K_i/k

is a Kummer extension. Denote by $G_i := G(K_ik)$ its Galois group. Every symbol algebra $A_{\omega_i}(a_i, b_i)$ is similar to a crossed product algebra $(K_i/k, c_i)$ with a 2-cocycle $c_i : G_i \times G_i \to \mu_{m_i} \subset \mu_k$, $i = 1, ..., r$. It follows from the multiplication theorem for crossed products, see e.g. [**4**], V, §2, that (k, A, f) is similar to a crossed product of the form $(K/k, c)$, K = compositum of all K_i, $i = 1, ..., r$, with a 2-cocycle $c : G(K/k) \times G(K/k) \to \mu_{\exp(A)}$. So we have

Remark 1.2. *If A is abelian and if the central pair (A, f) over k is nondegenerate then the corresponding twisted group algebra (k, A, f) is a central simple k-algebra which is k-isomorphic to a tensor product of symbol algebras over k. Moreover (k, A, f) is similar to a crossed product algebra of the form $(K/k, c)$ where K is defined as above and c is a 2-cocycle on the Galois group $G(K/k)$ such that all values of c belong to $\mu_{\exp(A)} \subset \mu_k$.*

Crossed product algebras of the type desribed in this remark belong to the class of *regular crossed product* algebras in the sense of [**2**].

We shall also make use of the following result from the cohomology theory of finite groups; for a proof see e.g. [**12**], Lemma 1.2, p.133, and [**26**], Theorem 2.2, p. 160; Proposition 2.1, p. 159.

Lemma 1.3. *Let G be a finite abelian group acting trivially on k^* and $\overline{k}^*$ and assume that k contains a primitive root of unity of order* $\exp(G)$. *Then the embedding $k^* \subset \overline{k}^*$ yields a split exact sequence*

$$1 \to H^2_{sym}(G, k^*) \to H^2(G, k^*) \xrightarrow{\iota} H^2(G, \overline{k}^*) \to 1 \qquad (\circledast)$$

where $H^2_{sym}(G, k^*)$ is the group of cocycle classes which can be represented by a symmetric cocycle t on G, i.e. t satisfies $t(x, y) = t(y, x)$ for all $x, y \in G$. If

$$G \cong \times_{i=1}^r G_i$$

is a decomposition of G as a direct product of cyclic groups G_i of order m_i, $i = 1, ..., r$, then

$$H^2_{sym}(G, k^*) \cong \times_{i=1}^r H^2_{sym}(G_i, k^*)$$

and

$$H^2(G_i, k^*) \cong H^0(G_i, k^*) \cong k^*/{k^*}^{m_i}, i = 1, ..., r;$$

the last isomorphism being induced by mapping a cocycle t on $G_i = \langle x_i \rangle$ to

$$\prod_{j=1}^{m_i} t(x_i, x_i^j) \, mod \, {k^*}^{m_i} \in k^*/{k^*}^{m_i}.$$

2. Central pairs and Galois representations

In this section we explain and state the main results of this note. The proofs will be given in the next sections.

Let (A, f) be a central pair over k with a finite abelian group A. Let $\overline{k}$ denote an algebraic closure of k and for every subextension K/k of $\overline{k}/k$ let $G_K = G(\overline{k}/K)$ denote the profinite Galois group of the extension $\overline{k}/K$. For every $x \in A$ define

$$d_f(x) := f(x,x)f(x,x^2)...f(x,x^{m(x)}), \text{ where } m(x) = \text{order of } x,$$

and for every $x \in A$ let $\alpha_f(x)$ denote an $m(x)$-th root of $d_f(x)$ in $\overline{k}$. Denote by k_f the field which is obtained from k by adjoining to k all $\alpha_f(x)$, $x \in A$. If (A,f) is isomorphic to (B,g) then $k_f = k_g$.

Assume that (A,f) is nondegenerate. Then k contains a primitive root of unity of order $e = e(A) = \exp(A)$. Hence $Hom(A,k^*) \cong Hom(A,\overline{k}^*) \cong \widehat{A}$. Moreover, k_f/k is a Kummer extension. It coincides with the field K defined in (1.2). The nondegenerate central pair (A,f) is said to be *full* if $\alpha_f(x)$ has degree $m(x)$ over k for all $x \in A$ and if $(k_f : k) = |A|$.

Example. Let a, b be squarefree integers and assume $ab = a_0a^2$ where a_0 is squarefree and $\neq 1$. Then any central pair $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, f)$ over $\mathbf{Q}$ such that $d_f(x) = a$, $d_f(y) = b$, where $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} = \langle x \rangle \times \langle y \rangle$, is full.

Assume that (A,f) is nondegenerate and full. For every $\lambda \in \widehat{A}$ and every $x \in A$ put $\sigma_\lambda(\alpha_f(x)) := \lambda(x)\alpha_f(x)$. σ_λ induces a k-automorphism of k_f in an obvious way. In this way we get an isomorphism $\widehat{A} \to G(k_f/k)$, $\lambda \mapsto \sigma_\lambda$. Composing this isomorphism with the isomorphism $A \to \widehat{A}$ given by $x \mapsto \omega_f(x,-)$ we get an isomorphism

$$\gamma_f : A \to G(k_f/k). \tag{2.1}$$

Denote by $G_k = G(\overline{k}/k)$ the absolute Galois group of k. A linear resp. projective Galois representation of degree n of G_k is a continuous homomorphism $G_k \to GL(n,\overline{k})$ resp. $G_k \to PGL(n,\overline{k})$, where G_k is regarded as a topological group with respect to the profinite topology, and $GL(n,\overline{k})$ resp. $PGL(n,\overline{k})$ are regarded as discrete groups; so the kernel of every linear resp. projective Galois representation of G_k is a closed subgroup of finite index in G_k which by Galois theory corresponds to a finite Galois extension L resp. K of k contained in $\overline{k}$; L resp. K is called the *kernel field* of the corresponding Galois representation. Many familiar concepts for linear and projective representations of finite groups, e.g. irreducibility or rationality, carry over to Galois representations. A projective Galois representation P of G_k is said to be of *Kummer type* if P is absolutely irreducible of degree greater than 1, if the image $P(G_k)$ is abelian and if k contains a primitive root of unity of order $\exp(P(G_k))$.

The first observation which will be proved in §3 is as follows.

Proposition 2.2. *The isomorphism in (2.1) induces a bijective correspondence between the set of isomorphism classes of nondegenerate full central pairs (A,f) over k (with an abelian group A) and the set of isomorphism classes of irreducible projective Galois representations P of G_k of Kummer type with kernel field k_f; under this correspondence the degree of P is $\sqrt[2]{|A|}$.*

Let e be a natural number such that the group μ_e of e-th roots of unity in $\overline{k}$ is contained in k. As is well known, the exact sequence

$$1 \to \mu_e \to \overline{k} \xrightarrow{\kappa} \overline{k}^* \to 1, \kappa(a) := a^e, \tag{*}$$

of discrete G_k-modules with respect to the natural G_k-Galois action induces an isomorphism

$$H^2(G_k, \mu_e) \cong Br(k)_e, \qquad (**)$$

where $Br(k)_e$ is the subgroup of the Brauer group of k of elements of order dividing e. And the exact sequence of discrete G_k-modules (*) with respect to the trivial G_k-action induces an exact sequence of cohomology groups

$$... \to Hom(G_k, \overline{k}^*) \xrightarrow{\delta_e} H^2(G_k, \mu_e) \to H^2_{tr}(G_k, \overline{k}^*) \to ... \qquad (***)$$

(Here and in the following the index "tr" means "cohomology with respect to the trivial group action".) Motivated by arguments in [**16**], p. 233/234, we denote by $C(k, e)$ the subgroup of the Brauer group $Br(k)_e$ which corresponds to the image of δ_e under the isomorphism (**). Obviously every element of $C(k, e)$ can be represented by a *regular cyclic* crossed product algebra $(k'/k, c)$, i.e. k'/k is a cyclic extension and all values of the 2-cocycle c on its Galois group $G(k'/k)$ belong to μ_e. A nondegenerate central pair (A, f) with abelian A is said to be *regular cyclic* if the Brauer class of the central simple k-algebra (k, A, f) is contained in $C(k, e(A))$, $e(A) = \exp(A)$. (The name "regular cyclic" is suggested by a similar terminology in [**2**].)

From the exact sequence (***) the following proposition is obvious.

Proposition 2.3. *If $M(k) := H^2_{tr}(G_k, \overline{k}^*)$ is trivial then every nondegenerate central pair (A, f) over k with abelian A is regular cyclic.*

For instance, $M(k)$, which is sometimes called the *Schur multiplier* of G_k or of k, is trivial in the following cases: k a local or global number field; see [**22**], and for a proof [**16**], §6. k a field (of characteristic 0) such that its cohomological dimension is 1, e.g. $k = \mathbf{C}(t)$, the rational function field in one variable over the complex number field $\mathbf{C}$, according to Tsen's result [**24**]. For a discussion of fields of cohomological dimension 1 see e.g. [**17**], chapitre II, §3.

Proposition 2.4. *If a nondegenerate central pair (A, f) over k with an abelian group A is regular cyclic then there is a multiple m of $e(A) = \exp(A)$ such that the central simple k-algebra (k, A, f) splits over μ_m, i.e. the cocycle class $(t) \in H^2(G_k, \mu_{e(A)})$ corresponding to the Brauer class of (k, A, f) belongs to the kernel of the homomorphism $H^2(G_k, \mu_{e(A)}) \to H^2_{tr}(G_k, \mu_m)$ which is induced by the embedding $\mu_{e(A)} \hookrightarrow \mu_m$. Especially the cyclotomic extension $k(\mu_m)$ is a splitting field for the central simple k-algebra (k, A, f).*

On the basis of this proposition we call for a regular cyclic central pair (A, f) with abelian A the smallest multiple $m = m(A, f)$ of $e(A)$ such that (k, A, f) splits over μ_m the *regularity index* of (A, f).

Proof of proposition (2.4). By assumption (k, A, f) is similar to a regular cyclic crossed product algebra $(k'/k, c)$. Since $G(k'/k)$ is cyclic the homomorphism $H^2(G(k'/k), \mu_e) \to H^2_{tr}(G(k'/k), \overline{k}^*)$ induced by the embedding $\mu_e \hookrightarrow \overline{k}^*$ is trivial. This implies that there is a function $\alpha : G(k'/k) \to \overline{k}^*$ such that $c(\sigma, \tau) =$

$\alpha(\sigma)\alpha(\tau)/\alpha(\sigma\tau)$ for all $\sigma, \tau \in G(k'/k)$. Hence $\alpha^{e(A)}$ is a character of $G(k'/k)$, and it follows that $\alpha^{e(A)(k':k)}$ is the trivial character. So (k, A, f) splits over $\mu_{e(A)(k':k)}$ and $k(\mu_{e(A)(k':k)})$ is a splitting field of (k, A, f). □

Two linear Galois representations D_1, D_2 of G_k are said to belong to the same *genus* if there is a linear character λ of G_k, i.e. a Galois representation of G_k of degree 1, such that D_2 is isomorphic to λD_1. In this way an equivalence relation is defined on the set of all linear Galois representations of G_k which is compatible with irreducibility. For a linear Galois representation D of G_k we denote by (D) the corresponding equivalence class which is sometimes called the *genus* of D. Let D be an irreducible linear Galois representation of G_k and let $\overline{D}$ be the corresponding projective representation of G_k which is obtained by composing D with the natural epimorphism $GL(n, \overline{k}) \to PGL(n, \overline{k})$. Let K be the kernel field of $\overline{D}$. The restriction of D to the subgroup G_K is a multiple of a linear character $\chi = \chi_D$ of G_K , the so called *central character* of D. The *index* $g((D))$ of the genus (D) of an irreducible Galois representation D of G_k is defined to be the minimal order of a central character χ_F for all $F \in (D)$. An absolutely irreducible linear Galois representation is said to be of *class 2* if its image is a nonabelian nilpotent group of class 2, and it is said to be of *Kummer type* if the corresponding projective representation is of Kummer type. Our main result is as follows.

Theorem 2.5. *There is a bijective correspondence between the set of isomorphism classes of nondegenerate full regular cyclic central pairs (A, f) over k with an abelian group A and the set of genera (D) of linear class 2 Galois representations D of G_k of Kummer type; under this correspondence the degree of (D) is $\sqrt[2]{|A|}$, and the index of (D) divides the regularity index of (A, f).*

A nondegenerate central pair (A, f) over k with an abelian group A is said to be *rational* if the central simple k-algebra (k, A, f) splits, i.e. is similar to a matrix algebra over k.

Corollary 2.6. *There is a bijective correspondence between the set of isomorphism classes of nondegenerate full rational central pairs (A, f) over k with an abelian group A and the set of genera (D) of linear class 2 Galois representations D of G_k of Kummer type such that the index of (D) divides $e(A)$.*

3. Duality of central pairs

Assume that A is a finite abelian group and that (A, f) is a nondegenerate full central pair over k. Then, as noted ealier, the symplectic pairing $\omega_f : A \times A \to k^*$ is nondegenerate, hence k contains a root of unity of order $e(A) = \exp(A)$, and the twisted group algebra (k, A, f) is central simple. Let (f_ι) denote the image of the cohomology class $(f) \in H^2(A, k^*)$ under the homomorphism $\iota : H^2(A, k^*) \to H^2_{tr}(A, \overline{k}^*)$, see (1.1). There is up to isomorphism a unique absolutely irreducible projective representation of A over $\overline{k}$ of degree $\sqrt[2]{|A|}$ with cocycle class (f_ι). Composing this representation with the inverse of the isomorphism $\gamma_f : A \to G(k_f/k)$ from (2.1) yields an absolutely irreducible projective Galois representation of G_k

over $\overline{k}$ of Kummer type whose isomorphism class is uniquely determined by the isomorphism class of (A, f).

Now let P be a projective Galois representation of G_k of Kummer type and let K be its kernel field; so $P(G_k) \cong G(K/k)$. It follows that K/k is a Kummer extension. Hence there is a subgroup Δ of k^* containing $k^{*^e}, e = \exp(G(K/k))$, such that $G(K/k)$ is canonically isomorphic to $\widehat{A}$, where $A = \Delta/k^{*^e}$. Assume that $a_1, ..., a_r \in \Delta$ are elements such that $a_1 \, mod \, k^{*^e}, ..., a_r \, mod \, k^{*^e}$ is a basis of A. Denote by m_i the order of $a_i \, mod \, k^{*^e}$, $i = 1, ..., r$. Writing $e = l_i m_i$ we see that $A = \times_{i=1}^r A_i$ where $A_i = \left\langle b_i^{l_i} \, mod \, k^{*^{m_i}} \right\rangle$ for some element $b_i \in k^*$, $i = 1, ..., r$. Let $g : A \times A \to k^*$ denote a symmetric cocycle in the cocycle class which is determined by $(b_1 \, mod \, k^{*^{m_1}}, ..., b_r \, mod \, k^{*^{m_r}})$ under the isomorphism $H^2_{sym}(A, k^*) \cong \times_{i=1}^r k^*/k^{*^{m_i}}$ described in lemma (1.3). Let $(t) \in H^2_{tr}(G(K/k), \overline{k}^*)$ denote the cocycle class of P. Since P is faithful on $G(K/k)$ the symplectic pairing ω_t on $G(K/k)$ is nondegenerate and induces an isomorphism $G(K/k) \to G(K/k)^\wedge \cong A$. Let $(h) \in H^2_{tr}(A, \overline{k}^*)$ denote the cocycle class corresponding to (t) under the induced isomorphism $H^2_{tr}(G(K/k), \overline{k}^*) \cong H^2_{tr}(A, \overline{k}^*)$. Using a splitting of the exact sequence $\circledast$ in lemma (1.3) we see that (g) and (h) uniquely determine a cocycle class $(f) \in H^2(A, k^*)$. By construction the central pair (A, f) is nondegenerate and full, and its isomorphism class is uniquely determined by the isomorphism class of P. Obviously the degree of P is $\sqrt[2]{|A|}$. Moreover, this construction $P \rightsquigarrow (A, f)$ is inverse to the previous one $(A, f) \rightsquigarrow P$.

Altogether we have proved proposition (2.2).

4. Regular cyclic central pairs and Galois representations of class 2

In the proof of theorem (2.5) we make use of the following result, see [**14**].

Proposition 4.1. *Every absolutely irreducible projective representation of a finite abelian group G over $\overline{k}$ is projectively equivalent to a projective representation such that a corresponding cocycle representation of G is regular, i.e. has all its matrix coefficients in $k(\mu_{\exp(G)})$ and all values of the corresponding cocycle belong to $\mu_{\exp(G)}$.*

Let A be a finite abelian group and let (A, f) be a nondegenerate full central pair over k. Let P denote an absolutely irreducible projective Galois representation of G_k over $\overline{k}$ of Kummer type corresponding to (A, f) in the sense of proposition (2.2). According to (4.1) let

$$W_f : G(k_f/k) \to GL(n, k), n = \sqrt[2]{|A|},$$

be a regular cocycle representation with cocycle

$$c : G(k_f, k) \times G(k_f/k) \to \mu_e \leqslant \mu_k, e = \exp(A),$$

such that $\overline{W}_f$ is isomorphic to P. There is an absolutely irreducible f-cocycle representation $T : A \to GL(n, \overline{k})$ such that $T(x)^{m(x)} = d_f(x) Id_n$ for all $x \in A$, for the definition of d_f see §2. Hence we may and do assume that all matrix coefficients

of T belong to k_f. Recall the isomorphism $\gamma_f : A \to G(k_f/k)$ in (2.1). From the proof of proposition (2.2) we see that the cocycle representations $W_f \circ \gamma_f$ and T of A are projectively equivalent over $\overline{k}$. For every $x \in A$ write $T(x) = (\alpha_{ij}(x))$, $1 \leqslant i, j \leqslant n$. Then w.l.o.g. we get the relation

$$\omega_f(y,x)T(x) = (T(x))^{\gamma_f(y)} = W_f(\gamma_f(y))T(x)W_f(\gamma_f(y))^{-1}$$

for all $x, y \in A$, where

$$(T(x))^{\gamma_f(y)} = (\gamma_f(y)(\alpha_{ij}(x))), 1 \leqslant i, j \leqslant n.$$

It follows that the central simple crossed product k-algebra $(k_f/k, c)$ is similar to the central simple k-algebra (k, A, f); compare the construction of the crossed product e.g. in [**4**], V, §1.

For any multiple m of e let

$$c_m : G(k_f/k) \times G(k_f/k) \to \mu_m$$

denote the cocycle which is obtained by composing c with the embedding $\mu_e \hookrightarrow \mu_m$ and let $G(c_m)$ denote the group extension of $G(k_f/k)$ with kernel μ_m which is defined by c_m. If (A, f) is regular cyclic and if $m = m(A, f)$ is its regularity index, then the inflation $\widetilde{c}_m$ of c_m to G_k splits. In view of [**9**], 1.1, this implies that the underlying embedding problem is solvable, i.e. there is a homomorphism $\psi : G_k \to G(c_m)$ such that the composition of ψ with the natural projection $G(c_m) \to G(k_f/k)$ coincides with the restriction epimorphism of Galois theory $G_k \to G(k_f/k)$. Lifting W_f to a linear representation of $G(c_m)$ and composing this lifting with ψ yields a linear Galois representation $D : G_k \to GL(n, \overline{k})$ such that the corresponding projective representation $\overline{D}$ is isomorphic to $\overline{W_f} =: P$ and such that the central character χ_D has order dividing m. Moreover the construction shows that D is of class 2 and of Kummer type, and that its genus is uniquely determined by the isomorphism class of (A, f).

Conversely assume that there is a linear Galois representation D of G_k of class 2 of Kummer type such that the central character χ_D of D has order equal to the index g of the genus of D. Let (A, f) be a nondegenerate full central pair over k which corresponds to the projective Galois representation $P = \overline{D}$ in the sense of proposition (2.2). Let K denote the kernel field of P and let $c : G(K/k) \times G(K/k) \to \mu_e$, $e = \exp(A)$, denote a 2-cocycle corresponding to P, see (4.1). Let h denote the least common multiple of g and e. Then $(c_h) \in H^2(G(K/k), \mu_h)$ is the image of χ_D under the transgression homomorphism

$$\tau : Hom(G_K, \mu_h)^{G(K/k)} \to H^2(G(K/k), \mu_h)$$

which arises from the exact sequence $1 \to G_K \to G_k \to G(K/k) \to 1$, see [**26**], proposition 1.4, p.155. Therefore by the profinite version of the Hochschild-Serre exact sequence [**10**] in e.g. [**19**] the cocycle $\widetilde{c}_h = \inf(c_h) : G_k \times G_k \to \mu_h$ splits. Hence (A, f) is regular cyclic and its regularity index $m(A, f)$ coincides with h which by definition is divisible by g.

Altogether we have proved theorem (2.5).

A nondegenerate central pair (A, f) over k with an abelian group A is said to be *cyclotomic* if there is a multiple d of $\exp(A)$ such that $k(\mu_d)$ is a splitting field of

(k, A, f); and the smallest such d is called the *cyclotomic index* of (A, f).

Remark 4.2. *Let (A, f) be a nondegenerate cyclotomic central pair over k. If the extension $k(\mu_{d(A,f)})$ is cyclic then (A, f) is regular cyclic and the regularity index of (A, f) coincides with its cyclotomic index $d(A, f)$.*

Indeed, since $k(\mu_d)$ splits (k, A, f) and since $k(\mu_d)$ is cyclic, by (3.8) in [**9**] the embedding problem corresponding to $c_d : G(k_f/k) \times G(k_f/k) \to \mu_d$ is solvable and therefore by a similar reasoning as in the above proof of theorem (2.5) we have $m(A, f) = d(A, f)$.

Combining this result with theorem (2.5) yields corollary (2.6).

Example. Let $k = \mathbf{R}(C)$ be the rational function field of a real algebraic curve C. In this case every k-central division algebra is isomorphic to a symbol algebra of the form $A_{-1}(-1, a)$, $a \in k$, $a \neq 0$; see [**24**]; [**25**], p. 10; [**5**]. As shown in (1.2) such a symbol algebra is similar to a crossed product algebra $(k(\sqrt[2]{a}, \sqrt[2]{-1})/k, c)$ where all values of the cocycle c belong to μ_2. Since $k(\sqrt[2]{-1})/k$ is a cyclic splitting field of this algebra we deduce from remark (4.2) that the regularity index of any central pair $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, f)$ over k whose twisted group algebra is isomorphic to $A_{-1}(-1, a)$ divides 4.

5. The case of number fields

Remark 5.1. *Let k be a number field and let (A, f) be a nondegenerate central pair over k with abelian A. Let $S = S(A, f)$ denote the finite set of places v of k such that the completion k_v of k at v is not a splitting field of (k, A, f). Then the cyclotomic index of (A, f) - which exists by the remarks following proposition (2.3) and by proposition (2.4) - divides the smallest multiple d of $\exp(A)$ such that the local degrees $(k_v(\mu_d) : k_v)$, $v \in S$, are all divisible by the exponent of the central simple k-algebra (k, A, f).*

This can be seen as follows: For every $v \in S$ the local extension $k_v(\mu_d)/k_v$, whose degree by assumption is divisible by the exponent of (k, A, f), is a splitting field of (k_v, A, f), see [**4**], VII, §2. By the local global principle [**4**], VII, §5 $k(\mu_d)$ is therefore a splitting field of (k, A, f). (Compare also the reasoning in the proof of the Lemma on p. 92 in [**23**].) The assertion follows from proposition (4.1).

There is an extensive literature on general class 2 extensions of local and global number fields; see e.g. [**6**], [**7**], [**8**], [**20**], [**21**]. In the number field case a relation between central pairs, Galois representations and automorphic forms has been established in [**15**]. Although the present note is quite diverse from those investigations it seems appropriate to discuss the example from [**8**] in the light of our context.

So let d_1, d_2 be squarefree integers and assume $d_1 d_2 = d_0 d^2$, where d_0 is sqarefree and $\neq 1$. Put $A := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Using (2.3), the fact that $M(\mathbf{Q})$ is trivial and lemma (1.3) we see that the element $(d_1 \, mod(\mathbf{Q}^*)^2, d_2 \, mod(\mathbf{Q}^*)^2) \in (\mathbf{Q}^*/(\mathbf{Q}^*)^2)^2$ together with the unique nontrivial element in $H^2_{tr}(A, \overline{k}^*) \cong \mathbf{Z}/2\mathbf{Z}$ defines a non-degenerate full regular cyclic central pair (A, f) over $\mathbf{Q}$. Using results from [**8**] we derive an upper bound for the index g of the genus of class 2 Galois representations

of $G_{\mathbf{Q}}$ of Kummer type corresponding to (A, f) in the sense of (2.5): Put $l := 4dd_0$. Let $R(l)$ denote the ray class field mod l of $\mathbf{Q}(\sqrt[2]{d_0})$ in the narrow sense, see [**20**], and denote by $K^c(l)$ resp. $K^a(l)$ the central class field resp. the genus class field with respect to $R(l)$, i.e. the maximal subfield of $R(l)$ such that $G(K^c(l)/K)$ is contained in the center of $G(K^c(l)/\mathbf{Q})$ resp. the maximal subfield of $R(l)$ such that $K^a(l)$ is abelian over $\mathbf{Q}$. From [**8**] we quote the following explicit formular

$$K^a(l) = \prod_{q \text{ prime } /d_0} \mathbf{Q}(\sqrt[2]{q^*})\mathbf{Q}(\mu_l)(\text{compositum in } \overline{k}), \qquad (\ddagger)$$

where $D = \prod q^*$ is the discriminant of $\mathbf{Q}(\sqrt[2]{d_0})$, i.e. $q^* = (-1)^{(q-1)/2}q$ resp.$= -4$ resp.$= \pm 8$.

The transgression homomorphism induces an isomorphism

$$Hom(G(K^c(l)/K^a(l)), \overline{k}^*) \cong H^2_{tr}(G(K/\mathbf{Q}), \overline{k}^*).$$

The last group is cyclic of order 2. Hence there is a character

$$\chi \in Hom(G(K^c(l)/K), \overline{k}^*)$$

which is mapped under the transgression homomorphism

$$Hom(G_K, \overline{k}^*)^{G(K/\mathbf{Q})} \to H^2_{tr}(G(K/\mathbf{Q}), \overline{k}^*)$$

to the unique nontrivial element $(f) \in H^2_{tr}(G(K/\mathbf{Q}), \overline{k}^*)$. Using again [**26**], proposition 1.4, p. 155, we see that χ is a central character χ_D for a linear class 2 Galois representation D of $G_{\mathbf{Q}}$ of Kummer type such that the corresponding projective representation $\overline{D}$ has cocycle class (f). The index of the genus of D is g. The order of χ and therefore also g divides the degree $(K^c(l) : K) = 2(K^a(l) : K)$ which can be computed from (‡).

References

[1] E. Artin: *Geometric algebra*, Interscience Publishers, New York, 1957

[2] R. Brauer: *Über die Konstruktion von Schiefkörpern*, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind, JRAM, 168, 1932, 44-64

[3] F.R. DeMeyer: *Galois theory in separable algebras over commutative rings*, Illinois J. Math., 10, 1966, 287-295

[4] M. Deuring: *Algebren*, Springer Verlag, 1935

[5] D.K. Faddeev: *Simple algebras over function fields of one variable*, AMS translation series 2, vol. 3, 15-38; translation of: Trud. Math. Inst. Steklov, 38, 1951, 321-344

[6] A. Fröhlich: *On fields of class 2*, Proc. London Math. Soc., 4, 1954, 235-256

[7] A. Fröhlich: *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary mathematics, AMS, 24, Providence R.I., 1983

[8] Y. Furuta, T. Kubota: *Central extensions and rational quadratic forms*, Nagoya Math. J., 130, 1993, 177-182

[9] K. Hoechsmann: *Zum Einbettungsproblem*, JRAM, 229, 1968, 81-106

[10] G. Hochschild, J.P. Serre: *Cohomology of group extensions*, Transactions AMS, 74, 1953, 110-134

[11] B. Huppert: *Endliche Gruppen I*, Springer Verlag, Berlin, 1967

[12] N. Iwahori, H. Matsumoto: *Several remarks on projective representations of finite groups*, Journal of the Faculty of Science of the University of Tokyo, Section I, 10, 1963/64, 129-146

[13] L. LeBruyn, F. Van Oystaeyen: *Brauer groups of fields*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, Heft 17, 1988

[14] H. Opolka: *Realisierbarkeit absolut irreduzibler projektiver Darstellungen in Einheitswurzelkörpern*, Archiv der Mathematik, XXIX, 1977, 590-593

[15] H. Opolka: *Central pairs, Galois theory and automorphic forms*, Algebras and Representation Theory, 6, 2003, 449-459

[16] J.P. Serre: *Modular forms of weight 1 and Galois representations*; in: Algebraic number fields (A. Fröhlich, editor), Academic Press, 1977, 193-268

[17] J.P. Serre: *Cohomology Galoisienne*, Lecture Notes in Mathematics, 5, cinquième edition, Springer Verlag, 1994

[18] J.P. Serre: *Local fields*, Springer Verlag, New York, 1979

[19] S.S. Shatz: *Profinite groups*, arithmetic and geometry, Annals of Mathematics Studies, Princeton University Press, 1972

[20] S. Shirai: *On the central class field mod m of Galois extensions of an algebraic number field*, Nagoya Math. J.,71,1978, 61-85

[21] A. Scholz: *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II*, JRAM,182, 1940, 217-234

[22] J. Tate: *Duality theorems in Galois cohomology over number fields*, Proceedings International Congress Math., Stockholm, 1962, 288-295

[23] J. Tate: *Global class field theory*, in: Algebraic number theory (J.W.S. Cassels, A. Fröhlich, editors), Academic Press, 1967, 162-203

[24] Ch.C. Tsen: *Divisionsalgebren über Funktionenkörpern*, Nachr. Ges. Wiss. Göttingen, 1933, 335-339

[25] E. Witt: *Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper*, JRAM, 171, 1934, 4-11

[26] K. Yamazaki: *On projective representations and ring extensions of finite groups*, Journal of the Faculty of Science of the University of Tokyo, Section I, 10, 1964, 147-195

[27] E.M. Zmud: *Symplectic geometries over finite abelian groups*; Math. Sbornik, 86, 1971, 9-34

This article may be accessed via WWW at http://www.rmi.acnet.ge/hha/
or by anonymous ftp at
ftp://ftp.rmi.acnet.ge/pub/hha/volumes/2004/n1a19/v6n1a19.(dvi,ps,pdf)

Hans Opolka `h.opolka@tu-bs.de`

TU Braunschweig
Pockelsstraße 14
D-38106 Braunschweig