

COHOMOLOGY AND GALOIS THEORY. I. NORMALITY OF ALGEBRAS AND TEICHMÜLLER'S COCYCLE

BY

SAMUEL EILENBERG AND SAUNDERS MACLANE

1. **Introduction.** Throughout this paper, P is a fixed base field, N is a finite, separable, and normal extension of P , Q is the Galois group of N over P , and $\lambda \in Q$ is an automorphism $x \rightarrow \lambda \cdot x$ of N leaving P elementwise fixed.

Among the simple algebras A with center N , the noncommutative Galois theory (cf. [13], [10a]⁽¹⁾) singles out those algebras A for which every automorphism λ of the center N over P can be extended to an automorphism of A . We term such algebras " Q -normal" or normal over P . Teichmüller [13] investigated these algebras and showed that each such algebra leads to a function $t(\lambda, \mu, \nu)$ of three arguments λ, μ, ν in Q , with values in N , and satisfying the identity.

$$(1.1) \quad \lambda \cdot t(\mu, \nu, \pi) t(\lambda, \mu\nu, \pi) t(\lambda, \mu, \nu) = t(\lambda\mu, \nu, \pi) t(\lambda, \mu, \nu\pi).$$

In view of the topological interpretation of functions satisfying analogous identities, we term such a function t a 3-dimensional *cocycle* of Q over N .

The cocycle t of a Q -normal algebra A is not uniquely determined. It may be modified by multiplication with a function $\delta h(\lambda, \mu, \nu)$ obtained from any function $h(\lambda, \mu)$ of two variables in Q with nonzero values in N by the formula

$$(1.2) \quad \delta h(\lambda, \mu, \nu) = \lambda \cdot h(\mu, \nu) [h(\lambda\mu, \nu)]^{-1} h(\lambda, \mu\nu) [h(\lambda, \mu)]^{-1}.$$

Such a function δh of three variables is termed a *coboundary*; it is always a cocycle (that is, $t = \delta h$ satisfies the identity (1.1)).

We study here the characterization of those 3-dimensional cocycles t which can arise as the cocycles of a Q -normal algebra, in the sense of Teichmüller.

To this end, consider any field K containing N , and still finite, separable and normal over P . Each automorphism α of K over P induces an automorphism $\alpha' = \lambda$ of N , and the function $(\Delta t)(\alpha, \beta, \gamma) = t(\alpha', \beta', \gamma')$ is a cocycle of the Galois group of K in K . We say that Δt is obtained by *lifting* t . We prove that t is the cocycle of a Q -normal algebra if and only if t can be lifted to a field K in which it is a coboundary, and that t is the cocycle of a Q -normal algebra split by the field K if and only if t becomes a coboundary when lifted to K .

The proof that such t 's are the only ones which occur is straightforward

Presented to the Society, September 5, 1947; received by the editors May 16, 1947.

(1) Numbers in brackets refer to the references cited at the end of the paper.

(§8). The proof that every such t can occur requires a detailed consideration (Theorem 10.1) of the conditions under which a crossed product algebra is Q -normal.

The proof of this crossed product theorem depends on certain coboundary computations which are manageable chiefly because of the use of a simple normalization condition (cf. (2.3)) which has hitherto been unaccountably neglected in the study of crossed products and related topics. These computations, though apparently formal, could presumably be given a conceptual interpretation in terms of suitable non-associative systems after the model of [7].

The determination of the cocycle t of a Q -normal algebra A is essentially a homomorphism T of the group of algebra classes of such algebras into the three-dimensional cohomology group of Q over N , defined as the group of 3-dimensional cocycles modulo the subgroup of coboundaries. Thus our result determines the exact image of this homomorphism T . Teichmüller has shown that the kernel of T consists of certain classes of algebras embeddable in algebras with the center P ; there is also an alternative characterization of the kernel of T as those algebra classes over N which can be obtained by extension of the field of scalars from P to N . The whole paper can be read without knowledge of Teichmüller's results in [13].

2. Galois cocycles. For each constant $c \neq 0$ in the normal field N we may define a function δc on the Galois group Q of N by setting

$$(2.1) \quad (\delta c)(\lambda) = \lambda \cdot c / c.$$

By a fundamental theorem of Galois theory, δc is the identity function $\delta c = 1$ if and only if c is in P , the base field.

Each function f defined on Q with nonzero values in N yields a function δf of two variables in Q , defined by

$$(2.2) \quad \delta f(\lambda, \mu) = [\lambda \cdot f(\mu)] f(\lambda\mu)^{-1} f(\lambda).$$

The function $f = \delta c$ defined in (2.1) has $\delta f = 1$, by direct computation. Conversely, Speiser's "Principal genus theorem in minimalen" ([12], cf. [2, p. 57]) asserts that every function f with $\delta f = 1$ has the form $f = \delta c$, for some constant c in N .

The equation (1.2) defines for each function h of two variables in Q a new function δh of three variables in Q . The functions h with $\delta h = 1$ are the "factor sets" of Q , and determine (cf. §9 below) the crossed product algebras (h, Q, N) . Conversely, each central simple algebra over P with maximal subfield N can be represented as such a crossed product. A crossed product algebra is a total matrix algebra if and only if its factor set h is a transformation set $h = \delta f$ of the form (2.2).

The Teichmüller formula (1.1) is the analog in the next higher dimension. For completeness, we state the general definition.

An n -dimensional *cochain* f of Q over N is a function $f(\lambda_1, \dots, \lambda_n)$ of n arguments λ_i in Q with nonzero values in N , subject only to the "normalization" condition that

$$(2.3) \quad f(\lambda_1, \dots, \lambda_n) = 1 \quad \text{if any } \lambda_i = 1.$$

In particular, a 0-cochain is simply a constant in N . The product $f_1 f_2$ of two n -cochains is defined as

$$f_1 f_2(\lambda_1, \dots, \lambda_n) = f_1(\lambda_1, \dots, \lambda_n) f_2(\lambda_1, \dots, \lambda_n);$$

under this multiplication the n -cochains form a group $C^n(Q, N)$.

The coboundary δf of an n -cochain f is an $(n+1)$ -cochain defined as

$$(2.4) \quad \delta f(\lambda_1, \dots, \lambda_{n+1}) = \lambda_1 \cdot f(\lambda_2, \dots, \lambda_{n+1}) \\ \cdot \left[\prod_{i=1}^n f(\lambda_1, \dots, \lambda_i \lambda_{i+1}, \dots, \lambda_{n+1})^{(-1)^i} \right] f(\lambda_1, \dots, \lambda_n)^{(-1)^{n+1}}.$$

The operation δ is a homomorphism $\delta: C^n \rightarrow C^{n+1}$, and $\delta\delta=0$. The n -cochains f with $\delta f=0$ are called the *n -cocycles*, and form a subgroup $Z^n(Q, N)$ of C^n ; this subgroup is the kernel of δ . The n -cochains of the form $f=\delta g$ for g an $(n-1)$ -cochain are called the *n -coboundaries* and constitute the subgroup $B^n(Q, N)$ of Z^n which is the image of C^{n-1} under δ . The factor group

$$H^n(Q, N) = Z^n(Q, N)/B^n(Q, N), \quad n = 1, 2, 3, \dots,$$

is the n -dimensional cohomology group of Q over N . Two cocycles f_1, f_2 in the same cohomology class in this group (that is, with $f_1=f_2(\delta g)$ for δg a coboundary) are called *cohomologous*.

In particular, the remarks made above indicate that $H^1(Q, N)=1$ (Speiser's theorem) and that $H^2(Q, N)$ is the group of algebra classes over P split by N (that is, the crossed product algebras with fixed field N).

The definition of $H^n(Q, N)$ depends only on the multiplicative group N^* of the nonzero elements of N and on the action of the automorphisms of Q on N^* ; it is thus a special case of the notion of the cohomology group of a group Q with coefficients in an abelian group on which Q operates. The cohomology theory for such groups has been developed in [5], using additive notation for the coefficient group. In particular, it was shown [5, §6] that the cohomology group H^n is the same with or without the normalization condition (2.3).

3. The ceilings of cocycles. We frequently have occasion to consider a field $K \supset N$ which is finite, separable and normal over P . We then set

$G =$ the Galois group of K/P , elements α, β, γ ,

$S =$ the Galois group of K/N , elements ρ, σ, τ .

Each automorphism $\alpha \in G$ of K induces an automorphism $\alpha' \in Q$ of N ; by a fundamental theorem of the Galois theory the correspondence $\alpha \rightarrow \alpha'$ is a homomorphism of G onto Q with kernel S . Diagrammatically, we have

$$\begin{aligned} K \supset N \supset P, \\ 1 \subset S \subset G, \\ G/S \cong Q. \end{aligned}$$

Any n -dimensional cochain $f \in Z^n(Q, N)$ can be "lifted" to an n -dimensional cochain $\Lambda_K f$ as

$$\Lambda_K f(\alpha_1, \dots, \alpha_n) = f(\alpha'_1, \dots, \alpha'_n), \quad \alpha_i \in G.$$

Furthermore, $\delta(\Lambda_K f) = \Lambda_K(\delta f)$ so that a lifted cocycle or coboundary is a cocycle or coboundary, respectively. Since $\Lambda_K(f_1 f_2) = (\Lambda_K f_1)(\Lambda_K f_2)$, Λ_K is a homomorphism of $Z^n(Q, N)$ into $Z^n(G, K)$ and of $B^n(Q, N)$ into $B^n(G, K)$ and induces a homomorphism of $H^n(Q, N)$ into $H^n(G, K)$.

A cocycle f which is not a coboundary may be lifted into a coboundary $\Lambda_K f$ in $B^n(G, K)$; we say then that f has the *ceiling* K . If $K' \supset K$ are both finite, separable and normal over P , a cochain f may be lifted to K' either directly or in stages, first to K , then to K' , with the same end result. Hence if K is a ceiling for f , so is K' . If the cocycles f_i have the ceilings K_i , for $i = 1, 2$, then the composite K of the fields K_1 and K_2 is finite, separable, and normal over P , and the product $f_1 f_2$ has ceiling K . Thus the cocycles with a ceiling form a group $Z_0^n(Q, N)$, and determine a subgroup

$$(3.1) \quad H_0^n(Q, N) = Z_0^n(Q, N) / B^n(Q, N)$$

of the cohomology group $H^n(Q, N)$.

This concept is trivial for dimension 2; indeed we have:

THEOREM 3.1. $H_0^2(Q, N) = 1$.

Proof. Suppose that the 2-cocycle f is not a coboundary. We are to show that no $\Lambda_K f$ is a coboundary. Since f is not a coboundary, the crossed product algebra $A = (f, Q, N)$ is not a total matrix algebra. But it is known [11, Theorem 2] that the lifted cocycle $\Lambda_K f$ gives a crossed product algebra $A' = (\Lambda_K f, G, K)$ which is similar to A . Therefore A' is not a total matrix algebra, and $\Lambda_K f$ is not a coboundary.

We give a second proof which depends not on the theory of algebras, but on the Speiser Theorem $H^1(Q, N) = 1$. Suppose $\Lambda_K f = \delta h$ for some $h \in C^1(G, K)$. Define $h_0(\sigma) = h(\sigma)$ for $\sigma \in S$; then, since f is normalized, $\delta h_0 = 0$, and $h_0 \in Z^1(S, K)$. By the Speiser theorem, there is a constant $b \neq 0$ in K such that $h_0(\sigma)b = \sigma \cdot b$. Define h_1 as $h_1(\alpha) = h(\alpha)b/\alpha \cdot b$ for all $\alpha \in G$. Then h_1 is cohomologous to h , and $\delta h_1 = \Lambda_K f$, while h_1 is 1 on the subgroup S . In particular, since f is normalized, $\Lambda_K f(\alpha, \sigma) = \Lambda_K f(\sigma, \alpha) = 1$ for $\sigma \in S$, so

$$h_1(\alpha\sigma) = [\alpha \cdot h_1(\sigma)]h_1(\alpha), \quad h_1(\sigma\alpha) = [\sigma \cdot h_1(\alpha)]h_1(\sigma).$$

Since $h_1(\sigma) = 1$, $h_1(\alpha\sigma) = h_1(\alpha) = h_1(\sigma\alpha)$ is an element invariant under σ . This proves that each value $h_1(\alpha)$ lies in the subfield N of elements of K in-

variant under all σ . By a fundamental theorem of the Galois theory, each automorphism $\lambda \in Q$ of N has an extension $v(\lambda) \in G$ to K ; furthermore $v(\lambda)v(\mu) = \eta v(\lambda\mu)$ for some $\eta = \eta(\lambda, \mu) \in S$. Then

$$\begin{aligned} f(\lambda, \mu) &= \Lambda_K f(v(\lambda), v(\mu)) = \delta h_1(v(\lambda), v(\mu)) \\ &= v(\lambda) \cdot h_1(v(\mu)) [h_1(\eta v(\lambda\mu))]^{-1} h_1(v(\lambda)) \\ &= \lambda \cdot h_1(v(\mu)) [h_1(v(\lambda\mu))]^{-1} h_1(v(\lambda)). \end{aligned}$$

This equation asserts that $f = \delta h_2$, where $h_2(\lambda) = h_1(v(\lambda))$ is a cochain of Q over N . This proves Theorem 3.1 again.

4. Algebras derived by scalar extension. Let B be a simple algebra with center P . Any field K containing the field P determines in the usual fashion [9, p. 89] a scalar extension B_K which is a simple algebra with center K . The correspondence $B \rightarrow B_K$ for fixed K induces a homomorphism $B(P) \rightarrow B(K)$ of the group $B(P)$ of classes of central simple algebras over P into the corresponding group for K . The kernel of this homomorphism consists of the classes of algebras split by K . The image of $B(P)$ under this homomorphism is the subgroup $B(K, P)$ of $B(K)$, consisting of the algebra classes over K derived by scalar extension from P . If K/P is finite, this description of "derived" algebra classes may be related to an equivalent description used by Deuring [4] and by Teichmüller.

THEOREM 4.1. *For a finite extension K of P , the following properties of a central simple algebra A over K are all equivalent.*

- (i) *The algebra class of A can be derived from an algebra class over P by scalar extension;*
- (ii) *There is a simple algebra B with center P such that B_K is a total matrix algebra over A ;*
- (iii) *There is a central simple algebra C over P which contains A (and hence K) in such fashion that every element of C commuting with K lies in A .*

PROOF. If (i) holds, there is a central simple algebra B' over P such that $A \sim B'_K$; that is, such that there are total matrix algebras $M_r(K)$ and $M_s(K)$ of orders r^2, s^2 over K with $A \times_K M_r(K) \cong B'_K \times_K M_s(K)$, the direct products being taken over K . Then $B = B' \times_P M_s(P)$ has $B_K \cong A \times_K M_r(K)$, which gives (ii). Conversely, (ii) immediately implies (i).

It is known (for example [1, Theorem 4.16]) that (iii) implies (ii). Conversely, assume (ii), so that A is similar to $A' = B_K$. Embed K in the total matrix algebra $M_n(P)$, where n is the degree of K over P , and form the simple algebra $C = B \times_P M_n(P)$ with center P . Then C contains $B \times_P K$, which is equivalent to $B_K = A'$; the commutator algebra of K in C clearly contains A' , and is equal to A' in virtue of a well known theorem on the order of such a commutator (for example [1, Theorem 4.13]). Thus A' has property (iii); a standard argument shows that the similar algebra A also has property (iii).

The property (iii) is used in Deuring [4] to obtain the homomorphism $B \rightarrow B_K$ for algebra classes. Choose an algebra C similar to B and containing K as a subfield; for example, one may choose $C = B \times_P M_n(P)$. The commutator C^K of K in C is a simple algebra with center K , and the algebra class of C^K over K does not depend on the choice of C in the class of B . By [1, Theorem 4.16], C^K is similar to the algebra C_K over K . Hence the correspondence $B \rightarrow C^K$ determines the same homomorphism $B(P) \rightarrow B(K, P)$ of algebra classes as does the correspondence $B \rightarrow B_K$. In [4], Deuring proves directly that the correspondence $B \rightarrow C^K$ is a homomorphism, in the case when K/P is separable, by a suitable use of crossed products. He remarks that the result should hold without assumption of separability, and indeed the proof that $B \rightarrow B_K$ is a homomorphism is immediate without this assumption.

However, in part (ii) of the theorem above we *cannot* assert that $B_K = A$; a counter example appears in §14.

5. Q -normal algebras. For the given field N with automorphism group Q , a Q -normal algebra A is any central simple algebra over N to which every automorphism λ of Q may be extended. If A and B are both Q -normal, so is the direct product $A \times_N B$, in virtue of the following lemma:

LEMMA 5.1. *Let A and B be algebras over N , each with a unity element, such that the automorphism λ of N can be extended to automorphisms v and w of A and B respectively. There is then one and only one automorphism $v \times w$ of the direct product $A \times_N B$ which agrees with v and w on the factors A and B respectively.*

Proof. The direct product $A \times_N B$ is best regarded [3, p. 48] as the set of all sums of formal products $a \times b$, for $a \in A$, $b \in B$, with the identifications $(a_1 + a_2) \times b = a_1 \times b + a_2 \times b$, $a \times (b_1 + b_2) = a \times b_1 + a \times b_2$ and $(ca) \times b = a \times (cb)$ for any scalar $c \in N$, and with the multiplication rule $(a_1 \times b_1)(a_2 \times b_2) = a_1 a_2 \times b_1 b_2$. A is identified with the subalgebra of elements $a \times 1$, where 1 is the identity of B , and B is similarly identified. If u is any extension of v and w , one must have

$$u \cdot \left(\sum_{i=1}^k a_i \times b_i \right) = \sum_{i=1}^k (v \cdot a_i) \times (w \cdot b_i).$$

Conversely, the above identifications show that this correspondence u is uniquely defined, and the multiplication rule shows that it is the desired automorphism $v \times w$.

For later use we note the following lemma.

LEMMA 5.2. *If in Lemma 5.1 the v_i, w_i are automorphisms of A, B , respectively, extending the automorphisms λ_i of N , for $i = 1, 2$, then*

$$(v_1 \times w_1)(v_2 \times w_2) = v_1 v_2 \times w_1 w_2.$$

Proof. The product $(v_1 \times w_2)(v_2 \times w_2)$ is an automorphism of $A \times_N B$ which extends the automorphism $\lambda_1 \lambda_2$ of N and which agrees on A with $v_1 v_2$, on B with $w_1 w_2$. It must therefore equal the unique such extension $v_1 v_2 \times w_1 w_2$.

The property of Q -normality depends only on the algebra class, in the following sense.

LEMMA 5.3. *If D is a central (simple) division algebra over N , $M = M(N)$ a total matrix algebra over N , then $D \times_N M$ is Q -normal if and only if D is Q -normal.*

Proof. Since a total matrix algebra M is trivially Q -normal, the normality of D implies that of $D \times_N M$ by Lemma 5.1. Conversely, if λ has an extension w to $D \times_N M$, then because of the uniqueness of the representation $A = D \times_N M$ of a central simple algebra, one can follow w by a suitable inner automorphism of A to obtain an automorphism w' of A which maps D on D and extends λ , as required.

One may also show that the reciprocal algebra A^{-1} to any Q -normal algebra A is Q -normal. If B is any central simple algebra over P , the scalar extension B_N is Q -normal, by an argument like that for Lemma 5.1. These observations combine to give the following theorem.

THEOREM 5.4. *If a central simple algebra A over N is Q -normal, so are all similar algebras. The similarity classes of Q -normal algebras over N form a subgroup $B_Q(N)$ of the group of algebra classes over N . The group $B(N, P)$ of algebra classes derived from algebra classes over P by scalar extension is a subgroup of $B_Q(N)$.*

6. The Teichmüller cocycle. If A is Q -normal, select for each $\lambda \in Q$ an extension $w(\lambda)$ which is an automorphism of A , and, in particular, choose $w(1) = 1$. The product $w(\lambda)w(\mu)w(\lambda\mu)^{-1}$ is an automorphism of A which induces on the center N the identity $1 = \lambda\mu(\lambda\mu)^{-1}$; it is therefore an inner automorphism [9, Theorem 5.16] induced by an element $b = b(\lambda, \mu)$ of A which has an inverse b^{-1} . For any such (regular) b we let

$$(6.1) \quad C[b] \cdot a \rightarrow bab^{-1}, \quad a \in A,$$

denote the induced inner automorphism of A . We then have

$$(6.2) \quad w(\lambda)w(\mu) = C[b(\lambda, \mu)]w(\lambda\mu), \quad b(\lambda, \mu) \in A.$$

In particular, we may and do choose $b(1, \mu) = b(\lambda, 1) = 1$.

Using this equation and the identities $C[b_1 b_2] = C[b_1]C[b_2]$ and $wC[b] = C[w \cdot b]w$, we may calculate the triple product $w(\lambda)w(\mu)w(\nu)$ in two ways as

$$\begin{aligned} [w(\lambda)w(\mu)]w(\nu) &= C[b(\lambda, \mu)b(\lambda\mu, \nu)]w(\lambda\mu\nu), \\ w(\lambda)[w(\mu)w(\nu)] &= C[\{w(\lambda) \cdot b(\mu, \nu)\}b(\lambda, \mu\nu)]w(\lambda\mu\nu). \end{aligned}$$

These results must be identical; hence if we write b_1, b_2 for the two arguments of C on the right, we have $C[b_1] = C[b_2]$ or $C[b_1 b_2^{-1}] = 1$, which means that

$b_2 b_1^{-1} = t$ is an element in the center N of A . Thus each triple λ, μ, ν of automorphisms in Q yields an element $t(\lambda, \mu, \nu)$ of N such that

$$(6.3) \quad [w(\lambda) \cdot b(\mu, \nu)]b(\lambda, \mu\nu) = t(\lambda, \mu, \nu)b(\lambda, \mu)b(\lambda\mu, \nu).$$

This equation asserts in effect that t is the non-commutative coboundary of b . The special choices made above show that $t(\lambda, \mu, \nu) = 1$ when one of the arguments λ, μ , or ν is 1. Hence we may regard t as a 3-cochain of Q over N .

Teichmüller (op. cit., p. 147) has proved the following properties of this cochain.

LEMMA 6.1. *The cochain t is a 3-cocycle of Q over N . For fixed choices $w(\lambda)$, a different choice of the regular elements $b(\lambda, \mu)$ of (6.2) replaces t by a cohomologous cocycle, and a suitable different choice of $b(\lambda, \mu)$ replaces t by any specified cohomologous cocycle. If the choice of the extensions $w(\lambda)$ of λ to automorphisms of A is altered, and if suitable new values of $b(\lambda, \mu)$ are chosen, the cocycle t is unaltered.*

The proofs will be omitted, as they are formally identical with the proofs of corresponding statements about the 3-cocycle associated in similar manner with the "kernel" of a group homomorphism (cf. [6; §7]). Indeed, we show in §15 below that the algebra case above is a special instance of the group case.

We call t a *Teichmüller cocycle* of the Q -normal algebra A .

LEMMA 6.2. *If the Q -normal algebras A_1, A_2 have the respective Teichmüller cocycles t_1, t_2 , then the direct product $A_1 \times_N A_2$ has the Teichmüller cocycle $t_1 t_2$.*

Proof. (Cf. [13, p. 148]). Select extensions $w_i(\lambda)$ and elements $b_i(\lambda, \mu)$ in A_i to satisfy (6.2) and (6.3) for $i=1, 2$. Then $w(\lambda) = w_1(\lambda) \times w_2(\lambda)$ is by Lemma 5.1 an extension of the automorphism λ to $A_1 \times_N A_2$. Furthermore $b(\lambda, \mu) = b_1(\lambda, \mu) \times b_2(\lambda, \mu)$ is a regular element of $A_1 \times_N A_2$, and $C[b(\lambda, \mu)] = C[b_1(\lambda, \mu)] \times C[b_2(\lambda, \mu)]$. One proves that w and b are related by (6.2) by using repeatedly the rule of Lemma 5.2, while on calculating (6.2) it appears that the (non-commutative) coboundary of b is indeed $t = t_1 t_2$, as asserted.

In particular, a total matrix algebra $M(N)$ has $t=1$ as a Teichmüller cocycle. Hence any two similar Q -normal algebras A and $A \times M$ have the same Teichmüller cocycles. We may thus define a homomorphism T of algebra classes to cohomology classes by assigning to the algebra class of A the cohomology class $T[A]$ of any Teichmüller cocycle of A .

7. The main theorem.

THEOREM 7.1. *The mapping of each Q -normal algebra over N into its Teichmüller cocycle induces a homomorphism T of the group $B_Q(N)$ of Q -normal algebra classes over N into the 3-dimensional cohomology group $H^3(Q, N)$. The kernel of this homomorphism is the group $B(N, P)$ of algebra classes obtained by scalar extension from P . The image under T is the group $H_0^3(Q, N)$ of those*

cohomology classes which have a ceiling; that is, the group of classes of those cocycles which become coboundaries upon being lifted to some field K separable, finite, and normal over P . Hence

$$(7.1) \quad B_Q(N)/B(N, P) \cong H_0^3(Q, N).$$

To prove this theorem, it remains only to establish the statements made as to the kernel and the image of T . To prove that T has the indicated kernel requires:

(i) If A is obtained by scalar extension from P , it has a Teichmüller cocycle 1;

(ii) A Q -normal algebra class with Teichmüller cocycle 1 can be obtained by scalar extension from P .

For completeness, we reproduce the proofs given by Teichmüller. The proof of (i) is immediate. To prove (ii), consider A with $t=1$, and use the quantities b of (6.3) to construct an algebra C with elements uniquely represented as sums $\sum a(\lambda)u(\lambda)$ for coefficients $a(\lambda) \in A$ and symbols $u(\lambda)$ for each $\lambda \in Q$, with the multiplication table determined by the distributive law and the rules

$$(7.2) \quad u(\lambda)a = (\lambda \cdot a)u(\lambda), \quad \lambda \in Q, a \in A;$$

$$(7.3) \quad u(\lambda)u(\mu) = b(\lambda, \mu)u(\lambda\mu), \quad \lambda, \mu \in Q.$$

These formulas are exactly analogous to the construction of a crossed product algebra over a field. Because the (non-commutative) coboundary t of b is 1, the usual computation shows that the algebra C is associative. The element $u(1)$ acts as the identity element of C , hence A is isomorphically embedded in C as the subalgebra of elements $au(1)$, for $a \in A$. The usual argument for crossed products [3, p. 82] proves C simple. A straightforward computation shows that the elements of C commuting with the subfield N of A are simply the elements of A ; hence by (7.2) the center of C is P . Thus A, C satisfy the condition of (iii), Theorem 4.1, which proves (ii) above.

The assertions of the main theorem as to the image of T (this is the only part of the theorem not proved by Teichmüller) are consequences of the following two statements (K is normal over P).

(iii) If the Q -normal algebra A is split by $K \supset N$, any Teichmüller cocycle of A has ceiling K ;

(iv) Every 3-cocycle with ceiling $K \supset N$ is the Teichmüller cocycle of some Q -normal algebra split by K .

Statement (iii) is proved in the next section. The critical point is the proof of (iv), which is given in §12 and which requires appeal to a criterion for the normality of crossed products, as given in §10. This crossed product theorem is also used in §§12 and 13 to give alternative proofs of parts (i), (ii), and (iii) of the main theorem.

In order to see that (iii) and (iv) indeed suffice to give the assertions of the main theorem as to the image of T , one need only observe that every algebra class over N has a splitting field K which is normal over P ; indeed such a K may be constructed as the normal hull of a suitable splitting field K_0 which is finite and separable over N [1, p. 62, Corollary]. Furthermore, the specific form of (iii) and (iv) above will give the following corollary.

COROLLARY 7.2. *If $K \supset N$ is normal over P , the mapping T carries the Q -normal algebra classes over N which are split by K onto the 3-dimensional cohomology classes of Q with ceiling K .*

We note also a consequence of the main theorem in the case when Q is cyclic. The general reduction theory for cohomology groups [5, §16] proves then that $H^3(Q, N) \cong H^1(Q, N)$. Hence H^3 and H_0^3 are both 1, and by the main theorem one has the following corollary.

COROLLARY 7.3. *If Q is cyclic, any Q -normal algebra class over N can be obtained by scalar extension from P .*

This has also been proved by Teichmüller (op. cit. p. 149) by a different method.

8. Normality of scalar extensions. The property (i) above is the special case $K=N$, $N=P$ of the following theorem.

THEOREM 8.1. *If A is Q -normal over N with Teichmüller cocycle t , while $K \supset N$ has Galois group G over P , then A_K is a G -normal algebra over K with a Teichmüller cocycle Λ_{Kt} obtained by lifting t to K .*

Part (iii) of the main theorem is a consequence of this result, for if K splits A , A_K is a total matrix algebra and every Teichmüller cocycle for A_K (with arguments in G) is a coboundary, and this result, applied to Λ_{Kt} , shows that t has ceiling K , as asserted in (iii).

Proof. Regard A_K as the direct product $A \times_N K$, and select $w(\lambda)$, $b(\lambda, \mu)$ and t for A as in §6. Each automorphism $\alpha \in G$ induces an automorphism $\alpha' = \lambda$ of Q , and the extension $w(\alpha')$ agrees with α on the field N of scalars in the product $A \times_N K$. Hence by Lemma 5.1 there is an automorphism $w^*(\alpha) = w(\alpha') \times \alpha$ of $A \times_N K$ which agrees on the respective factors with $w(\alpha')$ and α and which has $w^*(1) = 1$. This provides an extension of any $\alpha \in G$ to A_K ; hence A_K is G -normal.

Two applications of Lemma 5.2 prove

$$\begin{aligned} w^*(\alpha)w^*(\beta) &= [w(\alpha') \times \alpha][w(\beta') \times \beta] = w(\alpha')w(\beta') \times \alpha\beta \\ &= C[b(\alpha', \beta')]w(\alpha'\beta') \times \alpha\beta \\ &= \{C[b(\alpha', \beta')] \times 1\} \{w((\alpha\beta)') \times \alpha\beta\}. \end{aligned}$$

The automorphism in the second set of braces is $w^*(\alpha\beta)$, that in the first is

conjugation in A_K by the element $b^*(\alpha, \beta) = b(\alpha', \beta') \times 1$; hence

$$w^*(\alpha)w^*(\beta) = C[b^*(\alpha, \beta)]w^*(\alpha\beta),$$

as in the general definition (6.2) of the function b . The corresponding Teichmüller cocycle t^* of A_K may thus be derived from b^* by formula (6.3) as $t^*(\alpha, \beta, \gamma) = t(\alpha', \beta', \gamma) \times 1$. This formula states that t^* is obtained by lifting t to K , as asserted in the theorem.

9. Normality of crossed products. Let $K \supset N$ be a finite separable normal extension of P , and S the Galois group of K over N . Any 2-cocycle $f \in Z^2(S, K)$ determines a "crossed product" algebra $A = (f, S, K)$ consisting of all formal sums $\sum a(\sigma)u(\sigma)$ with each $a(\sigma) \in K$ and with symbols $u(\sigma)$ for $\sigma \in S$ which multiply according to the rules

$$(9.1) \quad u(\sigma)u(\tau) = f(\sigma, \tau)u(\sigma\tau), \quad \sigma, \tau \in S,$$

$$(9.2) \quad u(\sigma)a = (\sigma \cdot a)u(\sigma), \quad a \in K.$$

Such an algebra is central simple over N , the subfield of elements of K fixed under all automorphisms of S . The element $u(1)$ is the identity; all elements of A which commute with every element of K lie in K .

LEMMA 9.1. *$A = (f, S, K)$ is Q -normal if and only if every automorphism α of K over P can be extended to an automorphism of A .*

Proof. The condition is sufficient, for each $\lambda \in Q$ can be extended to an automorphism α of the normal extension field K . Suppose conversely that A is Q -normal. For each α , the extension $w(\alpha')$ of $\alpha' = \lambda$ maps the subfield K of A onto an isomorphic subfield K_1 containing $\lambda(N) = N$. The identity automorphism of N can be extended to an isomorphism of K_1 onto K (by a fundamental result in Galois theory) and thence to an automorphism ϕ of A (by a basic theorem on simple algebras; [1, Theorem 4.14]). The product $\phi w(\lambda)$ is an automorphism of A which maps K into K by an automorphism $\alpha_1 \in G$ and which induces the automorphism λ on N . Thus $\alpha\alpha_1^{-1} = \sigma$ is an automorphism of K over N ; by the same theorem on algebras it can be extended to an automorphism ψ of A over N . Finally $\psi\phi w(\lambda)$ is an automorphism of A carrying K into K by the automorphism $\sigma\alpha_1 = \alpha\alpha_1^{-1}\alpha_1 = \alpha$; it is the required extension of α to A .

The Galois group G (cf. §4) may be described as a group extension of Q by S by choosing for each $\lambda \in Q$ an extension $v(\lambda) \in G$, with $v(1) = 1$, and defining the automorphism $\sigma \rightarrow \lambda * \sigma$ of the normal subgroup S as $\lambda * \sigma = v(\lambda)\sigma v(\lambda)^{-1}$. There is then a "factor set" $\eta(\lambda, \mu)$ of elements of S such that

$$(9.3) \quad v(\lambda)v(\mu) = \eta(\lambda, \mu)v(\lambda\mu), \quad \lambda, \mu \in Q,$$

$$(9.4) \quad v(\lambda)\sigma = (\lambda * \sigma)v(\lambda), \quad \lambda \in Q, \sigma \in S.$$

Any elements $\alpha, \beta \in G$ can be expressed uniquely as

$$(9.5) \quad \alpha = \sigma v(\lambda), \quad \beta = \tau v(\mu), \quad \sigma, \tau \in S; \lambda, \mu \in Q.$$

Their product is given by the multiplication table (9.3) and (9.4) as

$$(9.6) \quad [\sigma v(\lambda)][\tau v(\mu)] = \sigma_1 v(\lambda\mu), \quad \sigma_1 = \sigma(\lambda * \tau)\eta(\lambda, \mu).$$

The factor set η satisfies the associativity condition

$$(9.7) \quad [\lambda * \eta(\mu, \nu)]\eta(\lambda, \mu\nu) = \eta(\lambda, \mu)\eta(\lambda\mu, \nu)$$

and is related to the $*$ operation by

$$(9.8) \quad [\lambda * (\mu * \sigma)]\eta(\lambda, \mu) = \eta(\lambda, \mu)[(\lambda\mu) * \sigma].$$

The normality of a crossed product may be formulated in terms of the action of each $w(\lambda)$ on the generators $u(\sigma)$ of the crossed product as follows.

THEOREM 9.2. *The crossed product $A = (f, S, K)$ is Q -normal if and only if there exist for $\lambda \in Q$, $\sigma \in S$ nonzero elements $m(\lambda, \sigma) \in K$ such that $m(1, \sigma) = m(\lambda, 1) = 1$ and*

$$(9.9) \quad m(\lambda, \sigma\tau)[v(\lambda) \cdot f(\sigma, \tau)] = m(\lambda, \sigma)[(\lambda * \sigma) \cdot m(\lambda, \tau)]f(\lambda * \sigma, \lambda * \tau).$$

This relation is observed by Teichmüller (op. cit. p. 142, (2); his β is our m). For a proof, suppose first that A is Q -normal, and that by Lemma 9.1 $w(\lambda)$ is an extension of $v(\lambda)$ to A , with $w(1) = 1$. In (9.2) set $a = v(\lambda)^{-1} \cdot b$ for any $b \in K$ and apply the automorphism $w(\lambda)$ to obtain

$$[w(\lambda) \cdot u(\sigma)]b = [(\lambda * \sigma) \cdot b][w(\lambda) \cdot u(\sigma)].$$

On the other hand (9.2) gives at once

$$u(\lambda * \sigma)b = [(\lambda * \sigma) \cdot b]u(\lambda * \sigma).$$

These two equations assert that $[w(\lambda) \cdot u(\sigma)]u(\lambda * \sigma)^{-1}$ commutes with every $b \in K$, hence lies in K , so we may write

$$(9.10) \quad w(\lambda) \cdot u(\sigma) = m(\lambda, \sigma)u(\lambda * \sigma)$$

for elements $m(\lambda, \sigma)$ in K with $m(\lambda, 1) = m(1, \sigma) = 1$.

The automorphism $w(\lambda)$ of A is determined by its action $v(\lambda)$ on K and by (9.10). It remains to express the fact that $w(\lambda)$, as defined by (9.10) from $m(\lambda, \sigma)$, is indeed an automorphism. Apply $w(\lambda)$ to the multiplication table (9.1) of the algebra to obtain

$$m(\lambda, \sigma)u(\lambda * \sigma)m(\lambda, \tau)u(\lambda * \tau) = [v(\lambda) \cdot f(\sigma, \tau)]m(\lambda, \sigma\tau)u(\lambda * (\sigma\tau)).$$

The left side may be computed by the rules (9.1) and (9.2) to be

$$m(\lambda, \sigma)[(\lambda * \sigma) \cdot m(\lambda, \tau)]f(\lambda * \sigma, \lambda * \tau)u(\lambda * (\sigma\tau)).$$

Comparison with the right side gives the required equation (9.9).

Conversely, given such a function m , use (9.10) to define the effect of

$w(\lambda)$ on $u(\sigma)$, and set $w(\lambda) \cdot [au(\sigma)] = [v(\lambda) \cdot a][w(\lambda) \cdot u(\sigma)]$, and similarly for sums of such elements $au(\sigma)$, $a \in A$. By reversing the above computation, we show that $w(\lambda)$ is indeed an automorphism of A extending the given automorphism λ of N .

10. The main theorem for crossed products. The complete description of the normality of a crossed product and the form of its Teichmüller cocycle may now be stated, where as usual K has the Galois groups G and S over P and over N , respectively, and $Q = G/S$ is the group of N over P .

THEOREM 10.1. *Let $A = (f, S, K)$ be the crossed product algebra determined by a cocycle $f \in Z^2(S, K)$, and let t be a cocycle in $Z^3(Q, N)$. Then A is Q -normal with t as one of its Teichmüller cocycles if and only if there exists a cochain $h \in C^2(G, K)$ such that*

$$(10.1) \quad \delta h = \Lambda_K t,$$

$$(10.2) \quad h(\sigma, \tau) = f(\sigma, \tau), \quad \sigma, \tau \in S.$$

First suppose A Q -normal and extend each automorphism $v(\lambda)$ as in Lemma 9.1 to an automorphism $w(\lambda)$ of A , with $w(1) = 1$. By Lemma 6.1 the given Teichmüller cocycle t of A can be obtained from suitably chosen regular elements $b(\lambda, \mu)$ of A satisfying (6.2). Any automorphism $v(\lambda)$ of G may be extended to A as

$$W(\sigma v(\lambda)) = C[u(\sigma)]w(\lambda),$$

where $C[u(\sigma)]$ again denotes the inner automorphism of A obtained by conjugation with the basis element $u(\sigma)$ in the crossed product A .

For any $\alpha, \beta \in G$ expressed as in (9.5) one then has

$$\begin{aligned} W(\alpha)W(\beta) &= C[u(\sigma)]w(\lambda)C[u(\tau)]w(\mu) \\ &= C[u(\sigma)(w(\lambda) \cdot u(\tau))]w(\lambda)w(\mu) \\ &= C[u(\sigma)(w(\lambda) \cdot u(\tau))b(\lambda, \mu)]w(\lambda\mu). \end{aligned}$$

Define regular elements $h(\alpha, \beta) \in A$, using the notation of (9.6) for the product $\alpha\beta$, by

$$(10.3) \quad h(\alpha, \beta)u(\sigma_1) = u(\sigma)(w(\lambda) \cdot u(\tau))b(\lambda, \mu);$$

the previous equation then becomes

$$(10.4) \quad W(\alpha)W(\beta) = C[h(\alpha, \beta)]W(\alpha\beta).$$

This states that conjugation by $h = h(\alpha, \beta)$ induces on A an automorphism $W(\alpha)W(\beta)W(\alpha\beta)^{-1}$ which is on K the identity $\alpha\beta(\alpha\beta)^{-1}$; in other words $h \in A$ commutes with all elements of the defining subfield K of the crossed product A . But the commutator of K in A is K , whence $h(\alpha, \beta) \in K$. Clearly $h(1, \beta) = h(\alpha, 1) = 1$, so that h is a 2-cochain of G over K .

In the definition (10.3) of h choose $\alpha = \sigma, \beta = \tau$; then $\sigma_1 = \sigma\tau, \lambda = \mu = 1$, and

$h(\sigma, \tau) u(\sigma\tau) = u(\sigma)u(\tau)$. With (9.1) this shows that h , restricted to the subgroup $S \subset G$, agrees with the factor set f of the crossed product, as asserted in (10.2).

Next we calculate the coboundary δh , for arguments α, β , and $\gamma = \rho\nu$, and with the notation (9.5), (9.6), and

$$\beta\gamma = \tau_1\nu(\mu\nu), \quad \tau_1 = \tau(\mu * \rho)\eta(\mu, \nu).$$

Since multiplication in G is associative $(\alpha\beta)\gamma = \alpha(\beta\gamma) = \epsilon\nu(\lambda\mu\nu)$, where ϵ in S is determined from both products as

$$\epsilon = \sigma_1[(\lambda\mu) * \rho]\eta(\lambda\mu, \nu) = \sigma[\lambda * \tau_1]\eta(\lambda, \mu\nu).$$

Now we calculate, using the definition (10.3) repeatedly, that

$$\begin{aligned} h(\alpha, \beta)h(\alpha\beta, \gamma)u(\epsilon) &= h(\alpha, \beta)h(\alpha\beta, \gamma)u(\sigma_1[(\lambda\mu) * \rho]\eta(\lambda\mu, \nu)) \\ &= h(\alpha, \beta)u(\sigma_1)[w(\lambda\mu) \cdot u(\rho)]b(\lambda\mu, \nu) \\ &= u(\sigma)[w(\lambda) \cdot u(\tau)]b(\lambda, \mu)[w(\lambda\mu) \cdot u(\rho)]b(\lambda\mu, \nu) \\ &= Eb(\lambda, \mu)b(\lambda\mu, \nu), \end{aligned}$$

where

$$\begin{aligned} E &= u(\sigma)[w(\lambda) \cdot u(\tau)]b(\lambda, \mu)[w(\lambda\mu) \cdot u(\rho)]b(\lambda, \mu)^{-1} \\ &= u(\sigma)[w(\lambda) \cdot u(\tau)][w(\lambda) \cdot w(\mu) \cdot u(\rho)]. \end{aligned}$$

On the other hand, using the second expression for ϵ ,

$$\begin{aligned} [\alpha \cdot h(\beta, \gamma)]h(\alpha, \beta\gamma)u(\epsilon) &= [\alpha \cdot h(\beta, \gamma)]u(\sigma)[w(\lambda) \cdot u(\tau_1)]b(\lambda, \mu\nu) \\ &= u(\sigma)[\sigma^{-1} \cdot \alpha \cdot h(\beta, \gamma)][w(\lambda) \cdot u(\tau_1)]b(\lambda, \mu\nu) \\ &= u(\sigma)w(\lambda) \cdot [h(\beta, \gamma)u(\tau_1)]b(\lambda, \mu\nu) \\ &= u(\gamma)w(\lambda) \cdot [u(\tau)(w(\mu) \cdot u(\rho))b(\mu, \nu)]b(\lambda, \mu\nu) \\ &= E[w(\lambda) \cdot b(\mu, \nu)]b(\lambda, \mu\nu). \end{aligned}$$

By the relation (6.3) giving the "coboundary" of b in terms of the Teichmüller cocycle, this becomes

$$Et(\lambda, \mu, \nu)b(\lambda, \mu)b(\lambda\mu, \nu).$$

Comparison with the previous result shows (since t lies in the center N of the algebra A) that

$$i(\lambda, \mu, \nu)h(\alpha, \beta)h(\alpha\beta, \gamma) = [\alpha \cdot h(\beta, \gamma)]h(\alpha, \beta\gamma).$$

But $\alpha' = \lambda$, $\beta' = \mu$, $\gamma' = \nu$, so this equation proves that $\delta h = \Lambda_{\mathcal{K}}t$, which is (10.1) in the theorem.

Note. The values of $h(\alpha, \beta)$ lie in the field K , but the definition (10.3) of these quantities is noncommutative (in the algebra A). This simplifies the manipulations above. One may also give a commutative definition. If the

crossed product $A = (f, S, K)$ is Q -normal, there exist nonzero elements $c(\lambda, \mu)$ in K with $c(1, \mu) = c(\lambda, 1) = 1$ such that

$$w(\lambda)w(\mu) = C[c(\lambda, \mu)u(\eta(\lambda, \mu))]w(\lambda\mu).$$

The crossed product algebra and its normality under the automorphisms $w(\lambda)$ is now described in strictly commutative terms by the functions $f(\sigma, \tau) \in K, m(\lambda, \tau) \in K$ and $c(\lambda, \mu) \in K$. The requisite identities for these functions are $\delta f = 1, (9.9)$ and

$$\begin{aligned} & [\eta(\lambda, \mu) \cdot m(\lambda\mu, \sigma)]f(\eta(\lambda, \mu), (\lambda\mu) * \sigma)c(\lambda, \mu) \\ & = m(\lambda, \mu * \sigma)[v(\lambda) \cdot m(\mu, \sigma)]f(\lambda * \mu * \sigma, \eta(\lambda, \mu))[(\lambda * \mu * \sigma) \cdot c(\lambda, \mu)]. \end{aligned}$$

From the previous definition of h one may show that $h(\alpha, \beta)$ has a commutative expression in terms of $f, m,$ and c as

$$[\sigma \cdot m(\lambda, \tau)]f(\sigma, \lambda * \tau)[(\sigma(\lambda * \tau)) \cdot c(\lambda, \mu)]f(\sigma(\lambda * \tau), \eta(\lambda, \mu)).$$

In particular, if $\lambda = \mu = 1,$ it follows that $h(\sigma, \tau) = f(\sigma, \tau)$ and one may also verify that (10.1) holds. The functions (f, m, c) are the functions α, β and γ^* considered on page 146 by Teichmüller (op. cit.). He remarks that t should be expressible in terms of these three functions. Without proof we state that the expression is

$$\begin{aligned} t(\lambda, \mu, \nu)f(\lambda * \eta(\mu, \nu), \eta(\lambda, \mu\nu))m(\lambda, \eta(\mu, \nu))(\lambda * \eta(\mu, \nu)) \cdot c(\lambda, \mu\nu) \\ = c(\lambda, \mu)[\eta(\lambda, \mu) \cdot c(\lambda\mu, \nu)]f(\eta(\lambda, \mu), \eta(\lambda\mu, \nu)). \end{aligned}$$

In view of its complication, this formula is best avoided by using instead the expression (10.1).

11. The converse proof. To prove the converse part of Theorem 10.1 requires extensive use of the equation $\delta h = \Lambda_K t$ and the consequent fact that $\delta h(\alpha, \beta, \gamma)$ vanishes when any one argument lies in the subgroup S . (This fact is a consequence of the normalization of $t,$ and clearly indicates the great convenience of that innocent assumption.)

Given the crossed product A and $h, t,$ satisfying (10.1) and (10.2), define $m(\lambda, \tau) \in K$ for $\lambda \in Q, \tau \in S$ by

$$(11.1) \quad m(\lambda, \tau)h(\lambda * \tau, v(\lambda)) = h(v(\lambda), \tau).$$

To prove A Q -normal, we must demonstrate that m satisfies (9.9), which in virtue of the definition of m reduces to the identity

$$\begin{aligned} h(v(\lambda), \sigma\tau)[v(\lambda) \cdot h(\sigma, \tau)]h(\lambda * \sigma, v(\lambda))[(\lambda * \sigma) \cdot h(\lambda * \tau, v(\lambda))] \\ = h(v(\lambda), \sigma)[(\lambda * \sigma) \cdot h(v(\lambda), \tau)]h(\lambda * \sigma, \lambda * \tau)h(\lambda * (\sigma\tau), v(\lambda)). \end{aligned}$$

By the principle observed above, $\delta h = \Lambda_K t$ gives

$$1 = \delta h(v(\lambda), \sigma, \tau)[\delta h(\lambda * \sigma, v(\lambda), \tau)]^{-1} \delta h(\lambda * \sigma, \lambda * \tau, v(\lambda)).$$

If these terms are expanded out by the definition of δh , four of the resulting twelve terms cancel, and the remaining eight terms give precisely the desired identity.

It remains to show that t is indeed the Teichmüller cocycle of A . Define the regular element $b(\lambda, \mu)$ of A as

$$(11.2) \quad b(\lambda, \mu) = h(v(\lambda), v(\mu))h(\eta(\lambda, \mu), v(\lambda\mu)^{-1})u(\eta(\lambda, \mu)).$$

To show that b satisfies the usual equation we must demonstrate that, for all $a \in A$,

$$(11.3) \quad [w(\lambda) \cdot w(\mu) \cdot a]b(\lambda, \mu) = b(\lambda, \mu)[w(\lambda\mu) \cdot a],$$

where $w(\lambda)$ is the automorphism of A defined from the function m above as in (9.10). It suffices to prove this for $a \in K$ and $a = u(\sigma)$, since these elements generate the crossed product. For $a \in K$, the commutativity of K reduces (11.3) to

$$[v(\lambda) \cdot v(\mu) \cdot a]u(\eta(\lambda, \mu)) = u(\eta(\lambda, \mu))[v(\lambda\mu) \cdot a],$$

which follows by the rule for commuting u and by the definition (9.3) of the factor set η .

If $a = u(\sigma)$, the desired identity becomes, by the definition (9.10) of $w(\lambda)$,

$$[v(\lambda) \cdot m(\mu, \sigma)]m(\lambda, \mu * \sigma)u(\lambda * \mu * \sigma)b(\lambda, \mu) = b(\lambda, \mu)m(\lambda\mu, \sigma)u((\lambda\mu) * \sigma).$$

Inserting the definitions of m and b and using multiplication rules in the crossed product algebra A to permute and multiply the terms in u , these terms reduce to $u((\lambda * \mu * \sigma)\eta(\lambda, \mu))$ on the left and $u(\eta(\lambda, \mu)[(\lambda\mu) * \sigma])$ on the right. The rule $v(\lambda)v(\mu) = \eta(\lambda, \mu)v(\lambda\mu)$ in the group extension G shows that the arguments of these two terms are equal, so that these u terms may be dropped. There remains an identity involving some twelve factors in the function h with various arguments and operators. Straightforward computation shows that this identity follows from the identity

$$1 = \delta h(v(\lambda), v(\mu), \sigma)\delta h^{-1}(v(\lambda), \mu * \sigma, v(\mu))\delta h(\lambda * \mu * \sigma, v(\lambda), v(\mu)) \\ \delta h^{-1}(\lambda * \mu * \sigma, \eta(\lambda, \mu), v(\lambda\mu))\delta h(\eta(\lambda, \mu), (\lambda\mu) * \sigma, v(\lambda\mu))\delta h^{-1}(\eta(\lambda, \mu), v(\lambda\mu), \sigma)$$

in which each term is 1 because $\delta h = \Lambda_K t$, and at least one of the arguments in each term lies in the subgroup S . The latter identity apparently involves 24 terms, four from each coboundary involved. Each coboundary involves two factors in which products of the arguments occur, and each of these factors cancels with corresponding factors from the next or the preceding coboundary. The remaining 12 factors give precisely the desired identity, and thus complete the proof of (11.3).

The elements $b(\lambda, \mu)$, as defined by (11.2), can now be used to calculate a Teichmüller cocycle t_1 of A as

$$[w(\lambda) \cdot b(\mu, \nu)]b(\lambda, \mu\nu) = t_1(\lambda, \mu, \nu)b(\lambda, \mu)b(\lambda\mu, \nu).$$

We wish to prove that this identity holds with $t_1 = t$. In this identity we may substitute the definition (11.2) for b , use the rule $w(\lambda) \cdot u(\sigma) = m(\lambda, \sigma)u(\lambda * \sigma)$ to apply $w(\lambda)$, replace m by its definition (11.1) in terms of h , and use the multiplication rules of the algebra to move all the terms in u to the right end on each side. The left side gives $u([\lambda * \eta(\mu, \nu)] \eta(\lambda, \mu\nu))$, the right side, $u(\eta(\lambda, \mu)\eta(\lambda\mu, \nu))$. The arguments of these terms are equal, by the associativity condition (9.7) for the factor set η . The terms in u may then be dropped, leaving an identity in t and some 12 factors h , with various arguments. This identity is obtained from the identity

$$\begin{aligned} 1 = & [t(\lambda, \mu, \nu)\delta h^{-1}(v(\lambda), v(\mu), v(\nu))] \delta h(v(\lambda), \eta(\mu, \nu), v(\mu\nu)) \\ & \delta h^{-1}(\lambda * \eta(\mu, \nu), v(\lambda), v(\mu\nu)) \delta h(\lambda * \eta(\mu, \nu), \eta(\lambda, \mu\nu), v(\lambda\mu\nu)) \\ & \delta h^{-1}(\eta(\lambda, \mu), \eta(\lambda\mu, \nu), v(\lambda\mu\nu)) \delta h(\eta(\lambda, \mu), v(\lambda\mu), v(\nu)), \end{aligned}$$

by expanding out each δh by the definition of the coboundary. In this expansion each term involving a product of two arguments of δh cancels with a similar term from a neighboring δh ; the remaining terms give exactly the 12 factors h noted above. The last displayed identity again holds because $\delta h = \Lambda_K t$, for this proves at once that the first term in brackets above is 1, and that the remaining terms are 1 because in each case at least one argument lies in the subgroup S . This proves that t is, as asserted in the theorem, the Teichmüller cocycle of the crossed product A .

Note. A more conceptual proof could presumably be constructed by first using h to construct a suitable nonassociative system (loop or algebra) with factor set h . This construction would explain the choices of the arguments used above in the identities on δh .

12. The image of T . The proof of the main theorem requires only the proof of part (iv) of §7; this we can now give by suitable reference to the crossed product theorem. We also append a similar proof of (iii) of §7, thus showing that the crossed product theorem gives directly a complete description of the possible Teichmüller cocycles of a Q -normal algebra (that is, a complete description of the image under the mapping T).

To prove (iv), suppose that t is any 3-dimensional cocycle of Q in N which has a ceiling K . Then $\Lambda_K t = \delta h$, for some 2-cochain h of Q in N . This equation means in particular that $\delta h(\sigma, \tau, \rho) = 1$ for arguments σ, τ, ρ in the subgroup S , so that the definition $f(\sigma, \tau) = h(\sigma, \tau)$ gives a factor set f of S in K . Construct the crossed product algebra $A = (f, S, K)$ from this set. By the converse part of the main theorem on crossed products, A is Q -normal with Teichmüller cocycle t . This proves (iv).

To prove (iii), observe that any Q -normal algebra A' with the normal splitting field K is similar to a crossed product $A = (f, S, K)$. The main

theorem on crossed products then asserts (10.1) that any Teichmüller cocycle of A (and hence of A') has ceiling K .

13. The kernel of T . The main theorem on crossed products can also be used to prove the assertions (i) and (ii) which characterize the kernel of T in the main theorem of §7. The proof depends on the formalism for the scalar extension of a crossed product. If $h \in Z^2(G, K)$ is a 2-cocycle of a normal field $K \supset N \supset P$, and if $f(\sigma, \tau) = h(\sigma, \tau)$ for σ, τ in the subgroup S corresponding to N , then the crossed product $B = (h, G, K)$ has the scalar extension B_N similar to $A = (f, S, K)$ over N ([1, Theorem 5.8]; [3, Theorem 8.5 D]).

Since a splitting field of a central simple algebra B' over P can always be enlarged to contain N and to be normal over P , any such algebra B' over P is similar to some $B = (h, G, K)$ where $\delta h = 1$. By the converse part of Theorem 10.1, the scalar extension $B_N \sim A = (f, S, K)$ is then Q -normal with a Teichmüller cocycle $\Delta_K t = \delta h = 1$. Hence $t = 1$, giving (i) of §7.

Conversely, suppose that $A = (f, S, K)$ has a Teichmüller cocycle 1. By Theorem 10.1, there is then an h with $\delta h = \Delta_K t = 1$; that is, with h a 2-cocycle of G in K . Then A is similar to the scalar extension to N of the crossed product algebra $B = (h, G, K)$, giving (ii) of §7.

14. An example of scalar extension. By Theorem 4.1 the algebra class of an algebra A over N can be obtained by scalar extension from P if there is a central simple algebra B over P with $B_N = A \times_N M(N)$. Observe however that this does *not* necessarily mean that the algebra A can itself be obtained by scalar extension; in other words, the appearance of the total matrix algebra $M(N)$ in this formula is essential.

To show this we adduce an example suggested to us in another connection by A. A. Albert.

The example depends on the arithmetic theory of algebras over a p -adic field F [1, Chapter IX]. Let F have the prime element π . Construct K , the unique unramified extension of degree mn over F , where m, n are integers greater than 1 and not relatively prime. K is cyclic over F , and its Galois group G is generated by an automorphism α . Furthermore, K contains the unramified extension N of F of degree m . The cyclic algebra $C = (K, \alpha, \pi)$ is central simple of order $m^2 n^2$ over F and has the invariant $1/(mn)$, mod 1, hence it is a division algebra. The commutator of N in C is a central simple algebra A of order n^2 over N .

The algebra A is Q -normal (where Q now denotes the Galois group of N over the base field F). For any automorphism λ of N over F can be extended [1, Theorem 4.14] to an automorphism θ of the enveloping simple algebra C . If $a \in A$ and $x = \lambda \cdot y \in N$, then

$$(\theta a)x = (\theta a)(\theta y) = \theta(ay) = \theta(ya) = (\theta y)(\theta a) = x(\theta a).$$

Thus θa commutes with all $x \in N$, so that $\theta a \in A$, and θ maps A onto A . In other words, each λ has the requisite extension $\theta = w(\lambda)$ to A .

The algebra A cannot be obtained by scalar extension from an algebra over F . For suppose $A = B_N$, B central simple over F . Then B has degree n over F , and is a subalgebra of C with the same identity element as C . By [1, Theorem 4.13], the commutator algebra E of B in C is simple, with center F , and $C = B \times_F E$. Over a p -adic number field, the exponent of an algebra equals its index and is a factor of its degree, so that $B^n \sim 1$, $E^m \sim 1$ and hence $C^k \sim 1$, where k is the least common multiple of m and n . In particular, since m, n are not relatively prime, $k < mn$. But on the other hand C has the p -adic invariant $1/mn$, hence has exponent mn , and $C^k \sim 1$ is impossible [1, Theorem 9.25]. Thus $A \neq B_N$.

On the other hand, since Q is cyclic the Teichmüller cocycle of the Q -normal algebra A must by Corollary 7.3 be a coboundary. Hence by the main theorem the algebra class of A can be obtained by scalar extension from P .

15. Q -normal algebras as kernels. The definition of a Teichmüller cocycle of a Q -normal algebra is a special case of the definition of 3-cocycles associated with a kernel of a group homomorphism. The proof depends on the following theorem.

THEOREM 15.1. *In any central simple algebra A over N , the multiplicative group N^* of nonzero elements of the field N is the center of the multiplicative group A^* of regular elements (that is, elements with inverses) in A .*

Proof. A can be represented as the algebra of all $k \times k$ matrices, with matrix units e_{ij} , over a division algebra D with center N . Then $e = \sum e_{ii}$ is the identity element of A and, for any $r \neq s$, $(e + e_{rs})(e - e_{rs}) = e + e_{rs} - e_{rs} = e$; hence $e + e_{rs}$ is a regular element of A . If $a = \sum d_{ij}e_{ij}$, for $d_{ij} \in D$, is any regular element of A in the center of A^* , then $a(e + e_{rs}) = (e + e_{rs})a$, or $ae_{rs} = e_{rs}a$. Multiplication gives

$$\sum_i d_{ir}e_{is} = ae_{rs} = e_{rs}a = \sum_j d_{sj}e_{rj}.$$

Comparing coefficients, we find $d_{rr} = d_{ss}$ for $r \neq s$ and $d_{ir} = 0$ for $i \neq r$. Hence if $d = d_{rr}$, the element a in the center of A^* is $a = \sum d e_{ii} = de$. Since D is a division algebra with center N , it follows that $d \neq 0$ and $d \in N$; hence the center at A^* is N^* , as asserted.

For each automorphism $\lambda \in Q$ let $w(\lambda)$ be an extension of λ to the Q -normal algebra A . Then $w(\lambda)$ is also an automorphism of the group A^* , and by (6.2) $w(\lambda)w(\mu) = w(\lambda\mu)$, modulo inner automorphisms of A^* . Thus we may set $\theta(\lambda) =$ the automorphism class of $w(\lambda)$, modulo inner automorphisms $I(A^*)$, to obtain a homomorphism θ of Q into automorphism classes of A^* . The pair $K = (A^*, \theta)$ is then exactly a Q -kernel with center N^* in the sense of [6]. Observing that the definition of t in §6 is exactly the definition of the 3-cochain of a kernel K in [6], we have the following theorem.

THEOREM 15.2. *Each Teichmüller 3-cochain t of a Q -normal algebra A is a 3-cochain of the corresponding Q -kernel (A^*, θ) with center N^* .*

This result provides a proof of the Lemma 6.1 by reference to the corresponding proofs of [6]. Observe, however, that an arbitrary automorphism of the group A^* in the automorphism class $\theta(\lambda)$ need not be an automorphism of the algebra A , and that the kernel associated with the direct product of two Q -normal algebras is not the product of the kernels, as the operation was defined in [6].

REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, New York, 1939.
2. E. Artin, *Galois theory*, Notre Dame Mathematical Lectures, no. 2, 2d ed., Notre Dame, 1944.
3. E. Artin, C. J. Nesbitt, and R. M. Thrall, *Rings with minimum condition*, University of Michigan Publications in Mathematics, no. 1, Ann Arbor, 1944.
4. M. Deuring, *Einbettung von Algebren in Algebren mit kleinerem Zentrum*, J. Reine Angew. Math. vol. 175 (1936) pp. 124–128.
5. S. Eilenberg and S. MacLane, *Cohomology theory in abstract groups*. I, Ann. of Math. vol. 48 (1947) pp. 51–78.
6. ——— *Cohomology in abstract groups*. II. *Group extensions with a non-abelian kernel*, Ann. of Math. vol. 48 (1947) pp. 326–341.
7. ——— *Algebraic cohomology theory and loops*, Duke Math. J. vol. 14 (1947) pp. 435–463.
8. H. Fitting, *Beiträge zur Theorie der Gruppen endlicher Ordnung*, Jber. Deutschen Math. Verein. vol. 48 (1938) pp. 77–142.
9. N. Jacobson, *The theory of rings*, Mathematical Surveys, vol. 2, New York, 1943.
10. ——— *A note on division rings*, Amer. J. Math. vol. 69 (1947) pp. 27–36.
11. S. MacLane and O. F. G. Schilling, *A formula for the direct product of crossed product algebras*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 108–114.
12. A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeit. vol. 5 (1919) pp. 1–6.
13. O. Teichmüller, *Über die sogenannte nichtkommutative Galoissche Theorie und die Relation $\xi_{\lambda, \mu, \nu} \xi_{\lambda, \mu, \nu, \pi}^{\lambda} = \xi_{\lambda, \mu, \nu, \pi} \xi_{\lambda, \mu, \nu, \pi}$* , Deutsche Mathematik vol. 5 (1940) pp. 138–149.

INDIANA UNIVERSITY,
BLOOMINGTON, IND.
HARVARD UNIVERSITY,
CAMBRIDGE, MASS.