

A NONASSOCIATIVE METHOD FOR ASSOCIATIVE ALGEBRAS

SAUNDERS MacLANE¹

This note exhibits a nonassociative proof for a strictly associative theorem concerned with the "Galois theory" of associative crossed product algebras. The theorem in question has also been established by somewhat more elaborate associative computations: it is perhaps of interest that the nonassociative proof to be given here appears to be both shorter and more conceptual than the associative proof. Practically no technical facts about nonassociative algebras are required for our proof.

Let $K \supset N \supset P$ be fields such that both K and N are finite, separable, and normal extensions of the base field P . The Galois group of K over P , or briefly $\mathcal{G}(K/P)$, will be designated as G , and similarly,

$$(1) \quad \mathcal{G}(K/P) = G, \quad \mathcal{G}(K/N) = S, \quad \mathcal{G}(N/P) = Q.$$

Then $S \subset G$. Each $\alpha \in G$ is an automorphism $\alpha: k \mapsto \alpha \cdot k$ of K , and induces an automorphism $\alpha' \in Q$ of N/P ; this correspondence $\alpha \rightarrow \alpha'$ provides the natural isomorphism $G/S \cong Q$. We consider functions $h(\alpha, \beta)$ with arguments α, β in G and nonzero values in the field K . The coboundary δh is a similar function of three arguments in G , defined as

$$(2) \quad \delta h(\alpha, \beta, \gamma) = [\alpha \cdot h(\beta, \gamma)]h(\alpha, \beta\gamma)[h(\alpha\beta, \gamma)h(\alpha, \beta)]^{-1}.$$

It is convenient to assume that any such function h is "normalized," in the sense that $h(I, \beta) = h(\alpha, I) = 1$, where I denotes the identity automorphism. The coboundary δh is then also normalized, for it follows that $\delta h(I, \beta, \gamma) = \delta h(\alpha, I, \gamma) = \delta h(\alpha, \beta, I) = 1$.

A factor set f of S in the multiplicative group of K is a (normalized) function $f(\sigma, \tau) \in K$ defined for arguments $\sigma, \tau \in S$ and satisfying the identity $\delta f(\rho, \sigma, \tau) = 1$, for all ρ, σ, τ in S . Each factor set f leads to a crossed product (cf. [1, Chap. V]²) $A = (K, f)$, which is a simple algebra with center N , and which may be represented in terms of elements $u(\sigma)$, one for each $\sigma \in S$, as the set of all sums $a = \sum_{\sigma} k(\sigma)u(\sigma)$ with arbitrary coefficients $k(\sigma) \in K$ and with the multiplication table

$$(3) \quad u(\sigma)u(\tau) = f(\sigma, \tau)u(\sigma\tau), \quad u(\sigma)k = [\sigma \cdot k]u(\sigma),$$

Presented to the Society, December 31, 1948; received by the editors November 8, 1947.

¹ John Simon Guggenheim Memorial Fellow.

² Numbers in brackets refer to the bibliography at the end of the paper.

for $\sigma, \tau \in S, k \in K$. The condition $\delta f = 1$ on the factor set assures the associativity of this algebra. In this algebra, the automorphisms σ of K are inner automorphisms $\sigma \cdot k = C[u(\sigma)]k$, where C denotes conjugation; that is, where

$$C[b] \cdot a = bab^{-1}, \quad a \in A,$$

for any regular element b of A . In particular, the elements $u(\sigma)$ are regular.

A factor set f , defined originally for arguments σ, τ in S , can always be extended to a nonzero "normalized" function $h(\alpha, \beta) \in K$, defined for all $\alpha, \beta \in G$, so that

$$(4) \quad f(\sigma, \tau) = h(\sigma, \tau), \quad \sigma, \tau \in S^*$$

THEOREM. *If the factor set f of a crossed product algebra $A = (K, f)$ with center N has an extension h as in (4) such that*

$$(5) \quad \delta h(\alpha, \beta, \gamma) = t(\alpha', \beta', \gamma'), \quad \alpha, \beta, \gamma \in G,$$

where t is a nonzero normalized function $t(\lambda, \mu, \nu) \in K$ defined for $\lambda, \mu, \nu \in Q$, then every automorphism $\lambda \in Q$ can be extended to an automorphism $w(\lambda)$ of the crossed product algebra $A = (K, f)$, in such fashion that there are regular elements $b(\lambda, \mu)$ in A for each pair $\lambda, \mu \in Q$ with

$$(6) \quad w(\lambda)w(\mu) = C[b(\lambda, \mu)]w(\lambda\mu),$$

$$(7) \quad t(\lambda, \mu, \nu)b(\lambda, \mu)b(\lambda\mu, \nu) = [w(\lambda) \cdot b(\mu, \nu)]b(\lambda, \mu\nu).$$

The hypothesis (5) asserts that δh depends only on its arguments α, β, γ modulo SCG . The conclusion shows that the automorphisms of the algebra A over P induce all the automorphisms $\lambda \in Q$ of its normal subfield N over P . As this is analogous to a fundamental property of fields normal over P , such an algebra A may be called *Q-normal*. The conclusion (7) asserts that t is a noncommutative co-boundary δb , where the function b measures the extent to which w is not a homomorphism. In the terminology of Eilenberg and the author [2], this conclusion asserts that the function t of (5) is a "Teichmüller cocycle" of A .

This theorem is the converse part of the main theorem of §10 in [2]; it is this theorem which serves there to characterize those three-dimensional cocycles (t 's with $\delta t = 1$) which may appear as the Teichmüller cocycles of central simple Q -normal algebras over N .

The proof now to be given does not depend on these concepts, as developed in [2]. The proof given there [2, §§9, 11] involves certain long identities in δh ; the present proof was obtained by the observation that these identities may be regarded as resulting from the re-

association of certain products in a suitable nonassociative algebra R constructed from h .

Construct R from symbols $u(\alpha)$, one for each $\alpha \in G$, as the set of all formal sums $\sum_a k(\alpha)u(\alpha)$ with arbitrary coefficients $k(\alpha) \in K$. Addition of such sums (by addition of coefficients) and multiplication of a sum by a scalar in P are defined in the standard way, to make R a vector space of dimension m^2 over P , where m denotes the degree of K over P . Multiplication in R is defined by the rules

$$(8) \quad u(\alpha)k = (\alpha \cdot k)u(\alpha), \quad u(\alpha)u(\beta) = h(\alpha, \beta)u(\alpha\beta),$$

and more generally, for $k, k' \in K, \alpha, \beta \in G$, by

$$(9) \quad [ku(\alpha)][k'u(\beta)] = [k(\alpha \cdot k')h(\alpha, \beta)]u(\alpha\beta).$$

The product of two sums of the form $\sum_a k(\alpha)u(\alpha)$ is then defined by (9) and the distributive law. This multiplication satisfies both distributive laws, so that R becomes a nonassociative algebra over P . The element $u(I)$ is an identity element of R . Comparison of (8) with (3) indicates that R contains the given associative crossed product algebra A ; it is our aim to show that the desired automorphisms of A appear in R as inner automorphisms, much as the automorphisms of a field K become inner automorphisms in an (associative) crossed product algebra.

The deviation from the associative law in R may be measured by using (9) to calculate a triple product in the two possible associations, as

$$\begin{aligned} [ku(\alpha)]\{[k'u(\beta)][k''u(\gamma)]\} \\ &= \{k(\alpha \cdot k')(\alpha \cdot \beta \cdot k'')[\alpha \cdot h(\beta, \gamma)]h(\alpha, \beta\gamma)\}u(\alpha\beta\gamma), \\ \{[ku(\alpha)][k'u(\beta)]\}[k''u(\gamma)] \\ &= \{k(\alpha \cdot k')(\alpha\beta \cdot k'')h(\alpha, \beta)h(\alpha\beta, \gamma)\}u(\alpha\beta\gamma). \end{aligned}$$

Upon comparing the results, using the definition (2) of δh , it appears that

$$(10) \quad [ku(\alpha)]\{[k'u(\beta)][k''u(\gamma)]\} \\ = \delta h(\alpha, \beta, \gamma)(\{[ku(\alpha)][k'u(\beta)]\}[k''u(\gamma)]).$$

In particular, if h were a factor set ($\delta h = 1$), the algebra would be associative. More generally, the equation (10) asserts that δh is the "associator" of the elements of the algebra in question. Such associators are similar to the additive associators used by Zorn [4] in studying alternative algebras and are exactly parallel to the associators used by Eilenberg and the author [3] to interpret cohomology groups of

abstract groups by means of loops. More explicitly, since t is normalized, $t(I, \mu, \nu) = t(\lambda, I, \nu) = t(\lambda, \mu, I) = 1$, and hence, by (5) $\delta h(\sigma, \beta, \gamma) = \delta h(\alpha, \sigma, \gamma) = \delta h(\alpha, \beta, \sigma) = 1$ for $\sigma \in S$. Since the $u(\sigma)$ for $\sigma \in S$ give the algebra A , this proves that every triple product in R with one factor in the subalgebra A is associative.

LEMMA 1. *For $r \in R, \beta \in G$ there is a unique element s in R such that $u(\beta)r = su(\beta)$. If $r \in A$, then $s \in A$ also.*

The uniqueness of s is in effect a cancellation law asserting that $su(\beta) = s'u(\beta)$ for $s, s' \in R$ implies $s = s'$. Indeed, take $s = \sum_{\alpha} k(\alpha)u(\alpha)$; then by the definition of the product

$$su(\beta) = \sum_{\alpha} k(\alpha)h(\alpha, \beta)u(\alpha\beta) = \sum_{\gamma} k(\gamma\beta^{-1})h(\gamma\beta^{-1}, \beta)u(\gamma).$$

On calculating a similar expression for s' and equating like coefficients, one finds that $s = s'$, as asserted. Since the multiplication is distributive, it suffices to prove the existence of s for the case when $r = ku(\alpha)$; in this case $s = (\beta \cdot k)h(\beta, \alpha) [h(\beta\alpha\beta^{-1}, \beta)]^{-1}u(\beta\alpha\beta^{-1})$ has the required property. In particular, since S is a normal subgroup of G , $\beta\sigma\beta^{-1} \in S$ for $\sigma \in S$, so that $s \in A$ whenever $r \in A$.

In using this lemma it is convenient to write s as $\theta(\beta) \cdot r$, so that

$$(11) \quad u(\beta)r = [\theta(\beta) \cdot r]u(\beta), \quad r \in R.$$

LEMMA 2. $\theta(\beta)$ is an automorphism of A ,

PROOF. In virtue of the distributive law in R applied to (11), $\theta(\beta)$ is a linear transformation of the vector space R into itself, while the associative law of R valid when one factor lies in A shows that

$$\theta(\beta) \cdot (ar) = [\theta(\beta) \cdot a][\theta(\beta) \cdot r], \quad a \in A, r \in R;$$

in particular, $\theta(\beta)$ is an endomorphism of the algebra A .

For elements $\beta, \gamma \in G$ and $a \in A$ one has

$$u(\beta)u(\gamma)a = u(\beta)[\theta(\gamma) \cdot a]u(\gamma) = [\theta(\beta) \cdot \theta(\gamma \cdot a)]h(\beta, \gamma)u(\beta\gamma),$$

and by a different route

$$u(\beta)u(\gamma)a = h(\beta, \gamma)u(\beta\gamma)a = h(\beta, \gamma)[\theta(\beta\gamma) \cdot a]u(\beta\gamma),$$

hence

$$\theta(\beta) \cdot [\theta(\gamma) \cdot a] = C[h(\beta, \gamma)] \cdot [\theta(\beta\gamma) \cdot a].$$

Setting here $\gamma = \beta^{-1}$, and observing that $C[h(\beta, \beta^{-1})]$ and $\theta(I) = I$ are automorphisms of A , we find that the product $\theta(\beta)\theta(\beta^{-1})$ is an automorphism of A . By the same token $\theta(\beta^{-1})\theta(\beta)$ is an automorphism

of A . The first of these two results shows that $\theta(\beta)$ must map A onto all of A , and the second implies that $\theta(\beta)$ can map no nonzero element of A into zero; together they mean that $\theta(\beta)$ is an automorphism of A , as asserted in the lemma.

For elements k in $K \subset A$, the definition (8) and (11) show that $\theta(\beta)$ is exactly the automorphism β of K . By a theorem in Galois theory, every automorphism $\lambda \in Q$ can be extended to some automorphism $\beta = v(\lambda)$ of K . Therefore λ can be extended to the automorphism $w(\lambda) = \theta(v(\lambda))$ of A , as asserted in the first conclusion of the theorem.

To obtain the remaining conclusions (6) and (7), choose a fixed extension $v(\lambda) \in G$ of each automorphism $\lambda \in Q$, and in particular choose $v(I) = I$. Thus $v(\lambda)' = \lambda$, and there is an η with

$$v(\lambda)v(\mu) = \eta(\lambda, \mu)v(\lambda\mu), \quad \eta(\lambda, \mu) \in S.$$

(Actually, η is a factor set of Q in S , obtained by regarding G as an extension of S by $Q \cong G/S$, with representatives v .) There is then a regular element $b(\lambda, \mu) \in A$ for each pair $\lambda, \mu \in Q$ such that

$$(12) \quad u(v(\lambda))u(v(\mu)) = b(\lambda, \mu)u(v(\lambda\mu)).$$

Indeed, one may define a regular element b with this property by the equation

$$h(\eta(\lambda, \mu), v(\lambda\mu))b(\lambda, \mu) = h(v(\lambda), v(\mu))u(\eta(\lambda, \mu)),$$

for if each side of this equation is multiplied on the right by $u(v(\lambda\mu))$, and if the multiplication rule (8) and the definition of η are used, equation (12) results. Note also that $b(I, \mu) = b(\lambda, I) = 1$.

The rule (12), when interpreted in terms of the automorphisms θ of (11), asserts that

$$(13) \quad \theta(v(\lambda))\theta(v(\mu)) = C[b(\lambda, \mu)]\theta(v(\lambda\mu)).$$

On the other hand, a triple product of u 's may be computed as

$$[u(v(\lambda))u(v(\mu))]u(v(\nu)) = b(\lambda, \mu)b(\lambda\mu, \nu)u(v(\lambda\mu\nu))$$

or, on using the "associator" in (10) and the assumption (7), as

$$\begin{aligned} & [u(v(\lambda))u(v(\mu))]u(v(\nu)) \\ &= [\delta h(v(\lambda), v(\mu), v(\nu))]^{-1}u(v(\lambda))[u(v(\mu))u(v(\nu))] \\ &= [\delta h(v(\lambda), v(\mu), v(\nu))]^{-1}[w(\lambda) \cdot b(\mu, \nu)]b(\lambda, \mu\nu)u(v(\lambda\mu\nu)). \end{aligned}$$

By the hypothesis (5) and the fact that $v(\lambda)' = \lambda$, the first factor here becomes $t(\lambda, \mu, \nu)^{-1}$. Comparison of the coefficients of $u(v(\lambda\mu\nu))$ in

