PACIFIC JOURNAL OF MATHEMATICS
Vol. 50, No. 2, 1974

NORMAL BASES FOR QUADRATIC EXTENSIONS

CHARLES SMALL

This note complements the author's paper in Journal of Pure and Applied Algebra, 2 (1972), in which a computation is made of the functor which associates to each commutative ring k its group $Q(k)$ of quadratic extensions, where "quadratic extension of k" means "Galois extension of k with respect to a group of order two". In general, quadratic extensions are rank two projective k-modules; the free ones form a subgroup $Q_F(k)$ of $Q(k)$. Among the free ones are some which admit a *normal* basis (definition recalled below); these form a subgroup $Q_{NB}(k)$. This paper studies the filtration $0 \subseteqq Q_{NB} \subseteqq Q_F \subseteqq Q$.

The starting point for the computation in [5] was the construction of a functor $\mathscr{R}$ and a natural monomorphism $\beta: \mathscr{R}(k) \rightarrow Q(k)$ (definitions recalled below). Our first observation here is that β is an isomorphism $\mathscr{R}(k) \rightarrow Q_F(k)$ and that the subfunctor R of $\mathscr{R}$ which corresponds to Q_{NB} (via β) is one studied by Micali and Villamayor in [3]. These results, which follow without difficulty from the work in [5], allow us to find simple necessary and sufficient conditions for $Q_{NB}(k) = Q_F(k)$, and at the other extreme to produce an infinite family of k for which $0 = Q_{NB}(k) \neq Q_F(k)$.

Now it is known that Q_{NB} is isomorphic to the Harrison cohomology functor $H^2(\ , \Pi)$ where Π is the group of order two. (See [2] and [4] for the following more general result: The group of normal-basis extensions of k with Galois group G is naturally isomorphic to $H^2(k, G)$ for *any* abelian group G.) In § 2 we establish directly, by a series of simple calculations, an isomorphism $\alpha: H^2(\ , \Pi) \rightarrow R$. (In fact $\beta\alpha$ turns out to be the isomorphism $H^2(\ , \Pi) \rightarrow Q_{NB}$ of [2] and [4].) This provides a new proof of the isomorphism $H^2(\ , \Pi) = Q_{NB}$ and also, in our opinion, sheds new light on it by identifying the functor in question with that of Micali-Villamayor. The isomorphism $Q_{NB} = H^2(\ , \Pi)$ generalizes nicely, as indicated above; on the other hand, for quadratic extensions the description in terms of Harrison cohomology is unnecessarily complicated and R is considerably easier to compute with.

Thanks are due to L. N. Childs and M. Orzech for (respectively) raising and discussing the question.

1. Identification of $R \subseteqq \mathscr{R}$ with $Q_{NB} \subseteqq Q_F$. Throughout, k is an arbitrary commutative ring (with 1) and Π is the group of order two. We will associate various groups with k, using the same symbol

$*$ for the operation in each; our results relate the groups in such a way that, among other things, this ambiguity of notation is rendered harmless.

By a *quadratic extension* of k we mean a (commutative) k-algebra which is a Galois extension of k with respect to Π, in the sense of [1]. If A and B are quadratic extensions of k then so is $A * B$, the subring of elements of $A \otimes_k B$ left fixed by $\sigma_A \otimes \sigma_B$ (where σ_A generates the Galois group of A/k, etc.). Indeed, $*$ makes the set of isomorphism classes of quadratic extensions of k into an abelian group of exponent $\leqq 2$ (see [5]). This group we denote $Q(k)$. Q is a functor: $k \to K$ induces $Q(k) \to Q(K)$ by $A \mapsto A \otimes_k K$.

In general, quadratic extensions of k are projective of rank two as k-modules ([1], Lemma 4.1). The free ones form a subgroup $Q_F(k)$ of $Q(k)$. Among the free quadratic extensions are some which admit a normal basis, that is, a basis of the form $\{w, \sigma w\}$ where σ generates the Galois group. These form a subgroup $Q_{NB}(k)$ of $Q_F(k)$.

We now recall the construction of the groups $\mathscr{R}(k)$ and $R(k)$, referring to [5] for the proofs. Let $U(k)$ denote the multiplicative group of units of k. If $f\colon R \to k$ is a homomorphism from a commutative ring R to k and we fix an element $y \in R$, the set

$$k_y = \{x \in k \mid (1 - f(y)x) \in U(k)\}$$

becomes an abelian group under the operation $x_1 * x_2 = x_1 + x_2 - f(y)x_1x_2$[1]. In particular we get a group k_n for each $n \in \boldsymbol{Z}$ from the unique homomorphism $\boldsymbol{Z} \to k$. Write $*$, or $*_n$ where necessary, for the group operation in k_n.

PROPOSITION 1. *$\psi(x) = x(1 - x)$ defines a natural homomorphism $\psi\colon k_2 \to k_4$ whose kernel is the group $I(k)$ of idempotents of k.*

Proof. We have first to show that $x \in k_2$ implies $x(1 - x) \in k_4$ and that $\psi(x_1 *_2 x_2) = (\psi x_1) *_4 (\psi x_2)$. Both are trivial. The statement about the kernel just says $x(1 - x) = 0 \Leftrightarrow x = x^2$.

Now define $R(k) = \operatorname{coker}(\psi)$, so that the sequence

$$0 \longrightarrow I(k) \longrightarrow k_2 \xrightarrow{\psi} k_4 \longrightarrow R(k) \longrightarrow 0$$

is exact. Note that $x \in k_4$ implies that $x *_4 x = 2x(1 - 2x)$ is in $\psi(k_2)$. This shows that $R(k)$, with the operation $*$ induced by $*_4$, is a group of exponent $\leqq 2$. The functor R was first considered in [3, § 7], where it is called G.

To construct $\mathscr{R}(k)$ we consider first the set $\mathscr{T}(k)$ of triples

[1] The reader will have no trouble completing the definition to make $k \mapsto k_y$ a functor.

(u, a, x) where $u \in U(k)$ and $a, x \in k$ satisfy $a^2u + 4x = 1$. If (u, a, x) and (u', a', x') are in $\mathscr{T}(k)$ then so is $(u, a, x) * (u', a', x') = (uu', aa', x + x' - 4xx')$, and $*$ is commutative and associative and has $(1, 1, 0)$ as neutral element. Define "$(u, a, x) \sim (u', a', x')$ by v, b" to mean: $v \in U(k)$, $b \in k$, $u' = v^2u$, $a'v = a - 2b$, $x' = x + b(a-b)u$. Write $(u, a, x) \sim (u', a', x')$ iff $(u, a, x) \sim (u', a', x')$ by v, b for some $v, b \in k$. Then $\sim$ is an equivalence relation on $\mathscr{T}(k)$, and is compatible with $*$. (Again, for complete proofs see [5].) Hence $*$ induces an operation, again denoted $*$, on the set $\mathscr{T}(k)/\sim$ of equivalence classes. In fact $\mathscr{T}(k)/\sim$ with this operation is a group of exponent $\leqq 2$, since $(1, 1, 0) \sim (u^2, a^2, 2x - 4x^2)$ by $v = u$, $b = 2x$, for any $(u, a, x) \in \mathscr{T}(k)$. This group we call $\mathscr{R}(k)$. $\mathscr{R}$ is, in the obvious way, a functor.

PROPOSITION 2. *The map from k_4 to $\mathscr{T}(k)$ given by $x \mapsto (1 - 4x, 1, x)$ induces a natural injective homomorphism $R(k) \to \mathscr{R}(k)$.*

Proof. Immediate from the definitions.

We will identify $R(k)$ with its image in $\mathscr{R}(k)$; thus an element of $\mathscr{R}(k)$ is in $R(k)$ iff it has a representative (u, a, x) with $a = 1$. It should be noted that when $2 \in U(k)$, $R(k) = \mathscr{R}(k) \cong U(k)/U(k)^2$, and when k has characteristic two, $R(k) = \mathscr{R}(k) \cong k^+/\mathscr{P}(k^+)$, where k^+ is the additive group of k and $\mathscr{P}: k^+ \to k^+$ is the homomorphism $\mathscr{P}(x) = x^2 + x$. See example (1) below for the equality of R and $\mathscr{R}$ in these extreme cases, and see [5] for the identification with the group of square classes (resp. $\mathscr{P}$-classes) of k.

Now, given $(u, a, x) \in \mathscr{T}(k)$, let $k\{u, a, x\}$ denote a free k-module $ks \oplus kt$ with elements $l, st, ts, s^2, t^2, \sigma s, \sigma t$ defined by

$$(*)\begin{cases} l = as + 2t \\ st = ts = 2xs - aut \\ s^2 = ul \\ t^2 = t - xl \\ \sigma s = -s \\ \sigma t = l - t\,. \end{cases}$$

THEOREM 3. *The first four equations of $(*)$ (extended linearly) give $k\{u, a, x\}$ a well-defined structure of k-algebra with $l = 1$, whose isomorphism class depends only on the class of (u, a, x) in $\mathscr{R}(k)$. The map σ given by the remaining two equations (extended linearly) is an algebra automorphism of order two, and $k\{u, a, x\}$ is a quadratic extension of k with Galois group generated by σ. The map β: $\mathscr{R}(k) \to Q(k)$ induced in this way is an injective homomorphism, natural in k. The image of β is precisely $Q_F(k)$; the image of the restriction of β to $R(k)$ is precisely $Q_{NB}(k)$.*

REMARK. When $2 \in U(k)$, any $(u, a, x) \in \mathscr{T}(k)$ is equivalent to $(u', 1, x')$ with $u' = 1 - 4x'$ (see below, Example (1)) and $k\{u', 1, x'\}$ is just $k[X]/(X^2 - u')$ with the expected Galois automorphism "$\sigma(X) = -X$". When k has characteristic two, any $(u, a, x) \in \mathscr{T}(k)$ is equivalent to $(1, 1, x')$ (again, see Example (1) below) and $k\{1, 1, x'\}$ is $k[X]/(X^2 + X + x')$ with the expected Galois automorphism "$\sigma(X) = X + 1$". See [5] for the proofs.

Proof. For everything except the last sentence, and for a basis-free description of $k\{u, a, x\}$, we refer to [5, Theorem 2]. If A is a quadratic extension of k, the k-linear trace map $\mathrm{tr}\colon A \to k$ given by $\mathrm{tr}(x) = \sigma x + x$ is onto [1, Lemma 1.6] and therefore splits, so that, as k-modules, $A = k \oplus M$ for some rank one projective, viz. $M = \ker(\mathrm{tr})$. Now A is free if and only if M is free, for $M = \Lambda_k^2(A)$. On the other hand, Theorem 3 of [5] shows that M is free if and only if A is in the image of β. Hence β is an isomorphism $\mathscr{R}(k) \to Q_F(k)$ as claimed.[2]

To see that β restricts to an isomorphism $R(k) \to Q_{NB}(k)$, suppose first that the quadratic extension A is in $\beta(R(k))$. According to the first part of the theorem, A has a k-basis $\{s, t\}$ with $\sigma t = 1 - t$ and $1 = s + 2t$. But then clearly t and $\sigma t = s + t$ form a normal basis for A. Conversely, suppose that $A = kw \oplus k(\sigma w)$ is a normal-basis quadratic extension. Choose an element $bw + c(\sigma w)$ of trace one; then $1 = b\,\mathrm{tr}(w) + c\,\mathrm{tr}(\sigma w) = (b + c)\,\mathrm{tr}\, w$. Hence $\mathrm{tr}(w)$ is invertible, and we can replace w by $t = (\mathrm{tr}\, w)^{-1} w$ to get a normal basis $A = kt \oplus k(\sigma t)$ with $\sigma t = 1 - t$. Now let $s = \sigma t - t$. Then $\sigma s = -s$, and moreover, since the trace of an arbitrary element $bt + c(\sigma t)$ is just $b + c$, we have $ks = \ker(\mathrm{tr})$. Clearly $\{s, t\}$ is a basis, and we have $1 = t + \sigma t = s + 2t$. Since $\sigma(s^2) = (\sigma s)^2 = s^2$ we have $s^2 = u.1$ for some $u \in k$, and u is a unit by [5, Lemma 3]. Similarly, σ fixes $t - t^2$, so that $t^2 = t - x.1$ for some $x \in k$. Now solving $x.1 = t - t^2 = (s + t)t$ for st we find $st = 2xs + (4x - 1)t$; on the other hand, given an expression $st = bs + ct (b, c \in k)$, computing the trace of each side shows that $c = -u$. Therefore, $st = 2xs - ut$ and $u + 4x = 1$, and we are done.

Now define $A(k) = \{a \in k \mid \exists b \in k, (a + 2b) \in U(k)\}$ and $B(k) = \{a \in k \mid \exists c \in k, (a^2 + 4c) \in U(k)\}$. Clearly $A(k) \subseteqq B(k)$; if $a + 2b$ is a unit so is $(a + 2b)^2 = a^2 + 4(a + b)b$. As a corollary of the theorem we have

COROLLARY 4. *The following are equivalent*:

(i) $Q_{NB}(k) = Q_F(k)$, i.e., *every free quadratic extension of k admits a normal basis*.

[2] The rule $A \mapsto \ker(\mathrm{tr})$ is a homomorphism $Q(k) \to \mathrm{Pic}(k)$, and $Q(k)/Q_F(k)$ is embedded in this way as a subgroup, usually quite a small one, of the Picard group. See [5, Theorem 4] for the precise statement.

(ii) $A(k) = B(k)$.

Proof. (i) is equivalent to $R(k) = \mathscr{R}(k)$, i.e., to the property that every element (u, a, x) of $\mathscr{T}(k)$ be equivalent to one of the form $(u', 1, x')$. It is immediate from the definition of equivalence ($\sim$) in $\mathscr{T}(k)$ than this is in turn equivalent to (ii).

This arithmetic criterion allows us to list various examples:

(1) If $2 \in U(k)$, or if 2 is in every maximal ideal of k (e.g. if k has characteristic two), then $Q_{NB}(k) = Q_F(k)$. *Proof*: When $2 \in U(k)$, the equation $x + 2b = 1$ can always be solved for b; hence $A(k) = k$ and, *a fortiori*, $A(k) = B(k)$. If 2 is in every maximal ideal, the three conditions $a^2 + 4c \in U(k)$ for some c, $a + 2b \in U(k)$ for some b, $a \in U(k)$ are all equivalent, by Nakayama's lemma. Thus $A(k) = U(k) = B(k)$.

(2) Consequently, when k is local, we have $Q_{NB}(k) = Q_F(k) = Q(k)$, since 2 is either a unit or in the unique maximal ideal. (The same is true for semilocal k, see [1, Theorem 4.2.c].)

(3) Let $k = \{(x, y) \in \boldsymbol{Z} \times \boldsymbol{Z} \mid x \equiv y \bmod n\}$ where $2 < n \equiv 2 \bmod 4$. Then $(1, n + 1)$ is in $B(k)$ but not in $A(k)$, so that k has free quadratic extensions without normal basis. Note that k is connected. This example, with $n = 6$, was found (in a different form) by N. Pullman.

A more shocking example is:

(4) Let k be the ring of integers in $\boldsymbol{Q}(\sqrt{D})$ where D is square-free and $-1 > D \equiv 3 \bmod 4$. Then $2 + \sqrt{D}$ is in $B(k)$ but not in $A(k)$. Moreover, since $U(k) = \{\pm 1\}$, $R(k) = 0$. This shows that $0 = Q_{NB}(k) \neq Q_F(k)$.

(5) If k is quadratically closed (every element is a square) then $Q_{NB}(k) = Q_F(k)$. For, suppose $a \in B(k)$: $a^2 + 4c = u \in U(k)$. Choose b so that $b^2 = -c$, then $u = (a + 2b)(a - 2b)$, hence $a + 2b \in U(k)$ and $a \in A(k)$.

REMARK. If $2 \in U(k)$, quadratic closure of k implies $Q_F(k) = U(k)/U(k)^2 = 0$. If $2 \notin U(k)$, $0 \neq Q_F(k)$ is possible even if k is quadratically closed; for example, $k = \boldsymbol{Z}/2\boldsymbol{Z}$. Can this happen with 2 outside some maximal ideal?

(6) Presumably, by a similar argument, $Q_{NB}(k) = Q_F(k)$ whenever k is von-Neumann regular. (Of course the only case of interest is when k is not Noetherian and 2 is a zero-divisor lying outside at least one maximal ideal, for if 2 is in every maximal ideal we have the result by Example (1); if 2 is not a zero-divisor it is a unit, and again we have Example (1); and if k is Noetherian it is a finite direct product of fields, and the result follows because Q, Q_F, and Q_{NB} evidently commute with finite direct products.)

The above results favor bases $\{s, t\}$ with $\operatorname{tr}(s) = 0$, $\operatorname{tr}(t) = 1$. A different view of the gap between Q_{NB} and Q_F is obtained by completing 1 to a basis, as follows:

LEMMA 5. *If A is a free quadratic extension of k then $1 \in A$ can be completed to a k-basis $\{1, d\}$ for A, and writing $d^2 = b_0 + b_1 d$ in this basis yields $b_1 - 2d \in U(A)$, $b_0 = -N(d)$ and $b_1 = \mathrm{tr}\,(d)$. (Here $N(d) = (\sigma d)d$, and $\mathrm{tr}\,(d) = \sigma d + d$ as above.)*

Proof. $k \cdot 1$ is a free k-direct summand of A by [**1**, Lemma 1.6]. Let M be a complement: $A = k \cdot 1 \oplus M$. Then A is free if and only if M is free since $M \cong \Lambda_k^2(A)$. This says that A is free if and only if 1 extends to a basis. Invertibility of $b_1 - 2d$ follows from k-separability of A, since $A \cong k[X]/(f(X))$ where $f(X) = X^2 - (b_0 + b_1 X)$ and $2d - b_1$ is the derivative at $X = d$ of $f(X)$. Finally if $b = \mathrm{tr}\,(d)$ then $N(d) = (b - d)d = -b_0 + (b - b_1)d$ gives the rest.

PROPOSITION 6. *Let A be a free quadratic extension of k and for each basis of the form $\{1, d\}$ use the lemma to define $x_d, y_d \in k$ by $(\mathrm{tr}\,(d) - 2d)(x_d + y_d d) = 1$. Then the following are equivalent:*

(i) *A admits a normal basis.*

(ii) *A admits a basis $\{1, d\}$ with $\mathrm{tr}\,(d)$ invertible.*

(iii) *A admits a basis $\{1, d\}$ with $x_d \in A(k)$.*

Proof. (i) $\Rightarrow$ (ii). If $A = kw \oplus k\sigma(w)$ we have seen that $\mathrm{tr}\,(w)$ is invertible. $\{1, w\}$ generate A as k-module since any element $aw + b(\sigma w)$ can be written as $b(\mathrm{tr}\, w) \cdot 1 + (a - b)w$. It follows that $\{1, w\}$ is a basis, either by checking independence directly using invertibility of $\mathrm{tr}\,(w)$, or by the general fact that any generating set of n elements for a free (or even just projective) module of rank n is a basis.

(ii) $\Rightarrow$ (iii). The relation $(\mathrm{tr}\,(d) - 2d)(x_d + y_d d) = 1$ in $A = k \oplus kd$ implies $\mathrm{tr}\,(d)x_d - 2y_d b_0 = 1$ in k. If $\mathrm{tr}\,(d)$ is invertible we can divide this latter equation by it to see that x_d is in $A(k)$.

(iii) $\Rightarrow$ (i). Choose $b \in k$ so that $v = x_d + 2b \in U(k)$. Put $z = -(y_d b_0 + b b_1) \in k$ (where $d^2 = b_0 + b_1 d$) and put $w = z + vd \in A$. Using $\sigma d = b_1 - d$ and $2z + vb_1 = b_1 x_d - 2y_d b_0 = 1$ we find $w + \sigma w = 1$. Now put $u = v^{-1}$, $\alpha = -uz$, and $\beta = \alpha + u$ (in k). Then $\beta w + \alpha(\sigma w) = \alpha(w + \sigma w) + uw = \alpha + uz + d = d$. Consequently $\{w, \sigma w\}$ generate A as k-module, and therefore form a basis, as before.

2. Comparison with Harrison. In this section we recall (following [2]) the definition of the Harrison cohomology group $H^2(k, \Pi)$ and prove directly that it is naturally isomorphic to $R(k)$. As in § 1, k is any commutative ring and Π is the group of order two.

Let Π^i denote the direct product of i copies of Π and let $k\Pi^i$

denote its group-ring. We will construct homomorphisms

$$U(k\Pi) \xrightarrow{d^1} U(k\Pi^2) \xrightarrow{d^2} U(k\Pi^3)\ ,$$

omit (as is traditional) the verification that $d^2d^1 = 0$, and define $H^2(k, \Pi) = \ker d^2/\mathrm{Im}\, d^1$.

First put $\Delta_0(z) = (1, z)$, $\Delta_1(z) = (z, z)$, and $\Delta_2(z) = (z, 1)$ for $z \in \Pi$, and extend $\Delta_i (i = 0, 1, 2)$ to maps $k\Pi \to k\Pi^2$ by linearity. Then, for any $x \in U(k\Pi)$, $d^1x = \prod_{i=0}^{2} (\Delta_i x)^{-1^i}$. Similarly for $(z_1, z_2) \in \Pi^2$ define $\Delta_0(z_1, z_2) = (1, z_1, z_2)$, $\Delta_1(z_1, z_2) = (z_1, z_1, z_2)$, $\Delta_2(z_1, z_2) = (z_1, z_2, z_2)$ and $\Delta_3(z_1, z_2) = (z_1, z_2, 1)$, and extend $\Delta_i(i = 0, 1, 2, 3)$ to maps $k\Pi^2 \to k\Pi^3$ by linearity. Then, for any $x \in U(k\Pi^2)$, $d^2x = \prod_{i=0}^{3} (\Delta_i x)^{-1^i}$. For any i use ε to denote the augmentation on $k\Pi^i$, that is, the ring homomorphism $k\Pi^i \to k$ given by $\varepsilon(\sum a_\sigma \sigma) = \sum a_\sigma$ (both sums over $\sigma \in \Pi^i$). Some additional notation: $Z(k, \Pi) = \ker d^2 =$ group of cocycles; $B(k, \Pi) = \mathrm{Im}\, d^1 =$ group of coboundaries; and $NG = \ker(\varepsilon\colon G \to U(k)) =$ subgroup of normalized elements of G (i.e., elements of augmentation 1), for any subgroup G of $U(k\Pi^i)$ (for example, $NZ(k, \Pi) =$ normalized cocycles, $NB(k, \Pi) =$ normalized coboundaries).

PROPOSITION 7. *Let* $\mu = a_1 + a_\sigma \sigma \in U(k\pi)$, $(a_1, a_\sigma \in k)$. *Then*:

(i) $d^1\mu = (\varepsilon(\mu) - x)(1, 1) + x(1, \sigma) + x(\sigma, 1) - x(\sigma, \sigma)$ *where* $x = a_1a_\sigma/\varepsilon(\mu)$, *and*

(ii) $\varepsilon(d^1\mu) = \varepsilon(\mu)$.

Proof. (ii) follows from (i). By definition we have $d^1\mu = (a_1(1, 1) + a_\sigma(1, \sigma))(a_1(1, 1) + a_\sigma(\sigma, 1))/(a_1(1, 1) + a_\sigma(\sigma, \sigma))$. Letting $\mu^{-1} = b_1 + b_\sigma\sigma$ we have $\varepsilon(\mu^{-1}) = (\varepsilon(\mu))^{-1}$, $a_1b_1 + a_\sigma b_\sigma = 1$, $a_1b_\sigma + a_\sigma b_1 = 0$, and $d^1\mu = (a_1^2(1, 1) + a_1a_\sigma(1, \sigma) + a_\sigma a_1(\sigma, 1) + a_\sigma^2(\sigma, \sigma))(b_1(1, 1) + b_\sigma(\sigma, \sigma))$. Multiplying this out gives $d^1\mu = c_1(1, 1) + c_2(1, \sigma) + c_3(\sigma, 1) + c_4(\sigma, \sigma)$ where $c_1 = a_1^2b_1 + a_\sigma^2b_\sigma$, $c_2 = c_3 = a_1a_\sigma(b_1 + b_\sigma) = x$ and $c_4 = a_\sigma^2b_1 + a_1^2b_\sigma$. Since $a_1^2b_1 + a_\sigma^2b_\sigma = (a_1b_1 + a_\sigma b_\sigma)(a_1 + a_\sigma) - a_1a_\sigma(b_1 + b_\sigma) = \varepsilon(\mu) - x$ and $a_\sigma^2b_1 + a_1^2b_\sigma = (a_1 + a_\sigma)(a_1b_\sigma + a_\sigma b_1) - a_1a_\sigma(b_1 + b_\sigma) = -x$, the proof is complete.

PROPOSITION 8. *Let* $\nu = a_{11}(1, 1) + a_{1\sigma}(1, \sigma) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma) \in U(k\pi^2)$. *Then*:

(i) ν *is a cocycle* $\Leftrightarrow a_{1\sigma} = a_{\sigma 1} = -a_{\sigma\sigma}$, *and*

(ii) ν *is a coboundary* $\Leftrightarrow \nu$ *is a cocycle and* $\exists a_1, a_\sigma \in k$ *such that* $a_1 + a_\sigma\sigma \in U(k\pi)$, $a_{1\sigma} = a_1a_\sigma/(a_1 + a_\sigma)$ *and* $a_{11} = a_1 + a_\sigma - a_{1\sigma}$.

Proof. (ii) is immediate from (i) and part (i) of Proposition 7. For (i), $d^2(\nu)$ is by definition A/B where A is the product of $(a_{11}(1, 1, 1) + a_{1\sigma}(1, 1, \sigma) + a_{\sigma 1}(1, \sigma, 1) + a_{\sigma\sigma}(1, \sigma, \sigma))$ and $(a_{11}(1, 1, 1) +$

$a_{1\sigma}(1, \sigma, \sigma) + a_{\sigma 1}(\sigma, 1, 1) + a_{\sigma\sigma}(\sigma, \sigma, \sigma))$ and B is the product of $(a_{11}(1, 1, 1) + a_{1\sigma}(1, 1, \sigma) + a_{\sigma 1}(\sigma, \sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma, \sigma))$ and $(a_{11}(1, 1, 1) + a_{1\sigma}(1, \sigma, 1) + a_{\sigma 1}(\sigma, 1, 1) + a_{\sigma\sigma}(\sigma, \sigma, 1))$. Multiplying this out, we see that if $a_{1\sigma} = a_{\sigma 1} = -a_{\sigma\sigma}$, then each coefficient in A equals the corresponding coefficient in B, so that ν is a cocycle.

The converse is the key point; the proof that follows is implicit in [2]. Let p_1 (resp. p_2) be the k-algebra homomorphism $k\pi^2 \to k\pi^2$ induced by the map $(x, y) \to (x, 1)$ (resp. $(x, y) \to (1, y)$) from π^2 to π^2, let δ_1 (resp. δ_2) be the k-algebra homomorphism $k\pi^3 \to k\pi^2$ induced by the map $(x, y, z) \to (x, 1)$ (resp. $(x, y, z) \to (1, z)$) from π^3 to π^2, let $\varepsilon: k\pi^2 \to k$ be the augmentation and let $j: k \to k\pi^2$ be the inclusion.

LEMMA 9. *With notation as above, we have the following equalities of maps $k\pi^2 \to k\pi^2$:*

$$\delta_1\Delta_i = \begin{cases} p_1 & \text{if} \quad i = 1, 2, 3 \\ j\varepsilon & \text{if} \quad i = 0 \,, \end{cases}$$

$$\delta_2\Delta_i = \begin{cases} p_2 & \text{if} \quad i = 0, 1, 2 \\ j\varepsilon & \text{if} \quad i = 3 \,. \end{cases}$$

Proof. Let $\nu = a_{11}(1, 1) + a_{1\sigma}(1, \sigma) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma) \in k\pi^2$, then $\delta_1\Delta_1(\nu) = \delta_1(a_{11}(1, 1, 1) + a_{1\sigma}(1, 1, \sigma) + a_{\sigma 1}(\sigma, \sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma, \sigma)) = a_{11}(1, 1) + a_{1\sigma}(1, 1) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, 1) = p_1(\nu)$ and $\delta_1\Delta_0(\nu) = \delta_1(a_{11}(1, 1, 1) + a_{1\sigma}(1, 1, \sigma) + a_{\sigma 1}(1, \sigma, 1) + a_{\sigma\sigma}(1, \sigma, \sigma)) = (a_{11} + a_{1\sigma} + a_{\sigma 1} + a_{\sigma\sigma})(1, 1) = j\varepsilon(\nu)$, etc.

We can now finish the proof of Proposition 8. If ν is a cocycle we have $A = B$ where as above $A = \Delta_0(\nu)\Delta_2(\nu)$ and $B = \Delta_1(\nu)\Delta_3(\nu)$. Hence $\delta_1(A) = \delta_1(B)$ and $\delta_2(A) = \delta_2(B)$. Using the lemma to compute we find $\delta_1(A) = (\delta_1\Delta_0(\nu))(\delta_1\Delta_2(\nu)) = j\varepsilon(\nu)p_1(\nu)$, $\delta_1(B) = (\delta_1\Delta_1(\nu))(\delta_1\Delta_3(\nu)) = (p_1(\nu))^2$, $\delta_2(A) = (\delta_2\Delta_0(\nu))(\delta_2\Delta_2(\nu)) = (p_2(\nu))^2$, $\delta_2(B) = (\delta_2\Delta_1(\nu))(\delta_2\Delta_3(\nu)) = p_2(\nu)(j\varepsilon(\nu))$. Since ν is invertible, $p_1(\nu)$ and $p_2(\nu)$ are also invertible, hence $\delta_1(A) = \delta_1(B)$ yields $j\varepsilon(\nu) = p_1(\nu)$ and $\delta_2(A) = \delta_2(B)$ yields $j\varepsilon(\nu) = p_2(\nu)$. But this means that the three elements $\varepsilon(\nu)(1, 1)$, $(a_{11} + a_{1\sigma})(1, 1) + (a_{\sigma 1} + a_{\sigma\sigma})(\sigma, 1)$ and $(a_{11} + a_{\sigma 1})(1, 1) + (a_{1\sigma} + a_{\sigma\sigma})(1, \sigma)$ of $k\pi^2$ are equal. Hence $a_{\sigma 1} + a_{\sigma\sigma} = 0 = a_{1\sigma} + a_{\sigma\sigma}$, and we are done.

PROPOSITION 10. *If $\nu = a_{11}(1, 1) + a_{1\sigma}(1, \sigma) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma)$ is a cocycle, $a_{1\sigma}/\varepsilon(\nu)$ is in k_4.*

Proof. We need $1 - (4a_{1\sigma}/\varepsilon(\nu)) \in U(k)$, for which it suffices to show $\varepsilon(\nu) - 4a_{1\sigma} \in U(k)$. Since ν is a cocycle, $\varepsilon(\nu) - 4a_{1\sigma} = a_{11} - 3a_{1\sigma}$. Let $\nu^{-1} = b_{11}(1, 1) + b_{1\sigma}(1, \sigma) + b_{\sigma 1}(\sigma, 1) + b_{\sigma\sigma}(\sigma, \sigma)$. Then, using $1 = a_{11}b_{11} + a_{1\sigma}b_{1\sigma} + a_{\sigma 1}b_{\sigma 1} + a_{\sigma\sigma}b_{\sigma\sigma} = a_{11}b_{11} + 3a_{1\sigma}b_{1\sigma}$ and $0 = a_{11}b_{1\sigma} + a_{1\sigma}b_{11} + a_{\sigma\sigma}b_{\sigma 1} +$

$a_{\sigma 1}b_{\sigma\sigma} = a_{11}b_{1\sigma} + a_{1\sigma}b_{11} - 2a_{1\sigma}b_{1\sigma}$, we have $(a_{11} - 3a_{1\sigma})(b_{11} - 3b_{1\sigma}) = 1 - 3(2a_{1\sigma}b_{1\sigma} - a_{1\sigma}b_{11} - a_{11}b_{1\sigma}) = 1$.

PROPOSITION 11. *If $x \in k_4$ then $\nu = (1-x)(1, 1) + x(1, \sigma) + x(\sigma, 1) - x(\sigma, \sigma)$ is a unit in $k\pi^2$, and therefore is in $Z(k, \pi)$.*

Proof. Let $\nu' = (1 - 3x)(1, 1) - x(1, \sigma) - x(\sigma, 1) + x(\sigma, \sigma)$, then $\nu\nu' = (1 - 4x)(1, 1)$, which is a unit since $x \in k_4$, hence ν is a unit too.

The preceeding propositions show that the rules $\alpha(a_{11}(1, 1) + a_{\sigma 1}(1, \sigma) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma)) = a_{1\sigma}/(a_{11} + a_{1\sigma})$ and $\gamma(x) = (1 - x)(1, 1) + x(1, \sigma) + x(\sigma, 1) - x(\sigma, \sigma)$ define maps $Z(k, \pi) \to k_4$ and $k_4 \to Z(k, \pi)$ respectively. Note that $\alpha\gamma$ is the identity, while $(\gamma\alpha)\nu = \nu/\varepsilon(\nu)$.

PROPOSITION 12. *γ and α are homomorphisms.*

Proof. The computation for γ is routine. For α, we need $(a_{1\sigma}c_{11} + a_{11}c_{1\sigma} + a_{\sigma 1}c_{\sigma\sigma} + a_{\sigma\sigma}c_{\sigma 1}) / \varepsilon(\nu)\varepsilon(\mu) = (a_{1\sigma}/\varepsilon(\nu)) + (c_{1\sigma}/\varepsilon(\mu)) - (4a_{1\sigma}c_{1\sigma}/\varepsilon(\nu)\varepsilon(\mu))$. Putting the right-hand side over the common denominator $\varepsilon(\nu)\varepsilon(\mu)$ and using $\varepsilon(\mu) = c_{11} + c_{1\sigma}$, $\varepsilon(\nu) = a_{11} + a_{1\sigma}$, $a_{1\sigma} = -a_{\sigma\sigma}$, $c_{1\sigma} = -c_{\sigma\sigma}$ to compute the resulting numerator, we arrive at the left-hand side.

COROLLARY 13. *α and γ are inverse isomorphisms, $k_4 \cong NZ(k, \pi)$.*

Proof. $\mathrm{Im}\ \gamma \subseteqq NZ(k, \pi)$ and $\gamma\alpha$ is the identity on $NZ(k, \pi)$.

PROPOSITION 14. *If $x \in \psi(k_2)$, $\gamma(x) \in NB(k, \pi)$.*

Proof. If $x = b(1 - b)$, $(1 - 2b) \in U(k)$, put $c_1 = -b/(1 - 2b)$ and $c_\sigma = (1 - b)/(1 - 2b)$. Then $(c_1 + c_\sigma\sigma)(b + (1 - b)\sigma) = 1$, so $\mu = b + (1 - b)\sigma \in U(k\Pi)$, and $d^1\mu = \gamma x$.

PROPOSITION 15. *If $\nu = a_{11}(1, 1) + a_{1\sigma}(1, \sigma) + a_{\sigma 1}(\sigma, 1) + a_{\sigma\sigma}(\sigma, \sigma)$ is a coboundary then $\alpha(\nu) \in \psi(k_2)$.*

Proof. Choose $\mu = (a_1 + a_\sigma\sigma) \in U(k\pi)$ so that $d^1\mu = \nu$. Then $\alpha(\nu) = a_{1\sigma}/\varepsilon = a_1a_\sigma/\varepsilon^2$ where $\varepsilon = \varepsilon(\mu) = \varepsilon(\nu)$. Now $a_1a_\sigma/\varepsilon^2 = (a_1/\varepsilon)(1 - (a_1/\varepsilon))$, so we have only to check that $1 - (2a_1/\varepsilon) \in U(k)$, or equivalently that $\varepsilon - 2a_1 = a_\sigma - a_1$ is a unit. Mimicking the proof of Proposition 10, let $(b_1 + b_\sigma\sigma) = \mu^{-1}$, then $(a_\sigma - a_1)(b_\sigma - b_1) = 1$.

COROLLARY 16. *α and γ restrict to inverse isomorphisms $\psi(k_2) \cong NB(k, \pi)$, and they induce inverse isomorphisms $R(k) \cong H^2(k, \pi)$.*

Proof. The first statement follows from Propositions 13, 14, and 15. For the second we need, in addition to the definitions, the fact that $Z(k, \pi)/B(k, \pi) \cong NZ(k, \pi)/NB(k, \pi)$. This follows because units of k are always coboundaries: $d^1u = u(1, 1)$ for any $u \in U(k)$, so that any cocycle ν represents the same element of $H^2(k, \pi)$ as the normalized cocycle $\nu/\varepsilon(\nu)$.

It is worth noting that the proof of Proposition 14 provides an isomorphism between k_2 and the group of normalized units of $k\pi$:

COROLLARY 17. *$\lambda(x) = (1 - x) + x\sigma$ defines a homomorphism $\lambda: k_2 \to U(k\pi)$, and the resulting sequence*

$$0 \longrightarrow k_2 \xrightarrow{\lambda} U(k\pi) \xrightarrow{\varepsilon} U(k) \longrightarrow 1$$

is split exact.

Proof. The argument which proves Proposition 14 shows that λ maps k_2 to $U(k\pi)$. It is obviously a homomorphism, and the exactness is easily checked.

By definition, d^0 is the trivial map $U(k) \to U(k\pi)$, so that $H^1(k, \pi) = \ker d^1/\mathrm{Im}\, d^0 = \ker d^1$. The resulting exact sequence can be normalized (i.e., restricted to the augmentation 1 part) to yield the bottom row of a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & I(k) \arrow[r] \arrow[d] & k_2 \arrow[r, "\psi"] \arrow[d, "\lambda"] & k_4 \arrow[r] \arrow[d, "\gamma"] & R(k) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & NH^1(k, \pi) \arrow[r] & NU(k\pi) \arrow[r, "d^1"'] & NZ(k, \pi) \arrow[r] & Q_{NB}(k) \arrow[r] & 0
\end{tikzcd}$$

in which the rows are exact and the verticals are all isomorphisms. In fact $NH^1(k, \pi) = H^1(k, \pi)$ because d^1 commutes with ε by Proposition 7 (ii), so we have proved:

COROLLARY 18. *λ induces an isomorphism $I(k) \to H^1(k, \pi)$, and in particular k is connected $\Leftrightarrow$ the inclusion of π in $k\pi$ is an isomorphism $\pi \to H^1(k, \pi)$.*

Lifting the description $k_2 \cong NU(k\pi)$ of normalized units to arbitrary ones yields the following criterion, whose proof is left as an easy exercise:

COROLLARY 19. *Let $\mu = (a + b\sigma) \in k\pi$, then $\mu \in U(k\pi) \Leftrightarrow a^2 - b^2 \in U(k)$.*

Finally, it should be pointed out that $\beta\alpha\colon H^2(\ \ ,\pi)\to R\to Q_{NB}$ is the isomorphism of [2], [4]. Thus the cocycle $(\varepsilon(\nu)-x)(1,1)+x(1,\sigma)+x(\sigma,1)-x(\sigma,\sigma)$ corresponds to the quadratic extension $A=kw\oplus kw'$, described by

$$\begin{cases} w^2=(\varepsilon(\nu)-x)w-xw' \\ ww'=xw+xw'=w'w \\ (w')^2=-xw+(\varepsilon(\nu)-x)w' \\ w'=\sigma w,\ w=\sigma w'\ . \end{cases}$$

Note that $(w+w')/\varepsilon(\nu)=1$ in A, and consequently $\operatorname{tr}(w)=\varepsilon(\nu)$. Thus the fact, noted in proving Corollary 16, that every cohomology class can be represented by a normalized cocycle, corresponds precisely to the fact (used in proving the converse part of Theorem 3) that any normal basis $\{w,\sigma w\}$ can be replaced by one with $\operatorname{tr}(w)=1$.

REFERENCES

1. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois Theory and Galois Cohomology of Commutative Rings*, Amer. Math. Soc., Memoir #52, 1965, 15-33.

2. S. U. Chase and A. Rosenberg, *A theorem of Harrison, Kummer theory, and Galois algebras*, Nagoya Math. J., **27** (1966), 663-685.

3. A. Micali and O. Villamayor, *Sur les Algèbres de Clifford*, Ann. Sci. de l'E.N.S. **1** (1968), 271-304.

4. M. Orzech, *A cohomological description of abelian Galois extensions*, Trans. Amer. Math. Soc., **137** (1969), 481-499.

5. C. Small, *The group of quadratic extensions*, J. Pure Appl. Algebra, **2** (1972), 83-105 and 395.

Received September 26, 1972.

QUEEN'S UNIVERSITY