COLLOQUIUM MATHEMATICUM

VOL. 87 2001 NO. 1

# *REMARKS ON NORMAL BASES*

BY

MARCIN MAZUR (Urbana, IL)

**Abstract.** We prove that any Galois extension of a commutative ring with a normal basis and abelian Galois group of odd order has a self-dual normal basis. We apply this result to get a very simple proof of nonexistence of normal bases for certain extensions which are of interest in number theory.

**1. Introduction.** Let $R \subset S$ be an extension of commutative rings. Suppose that $G$ is a finite group of automorphisms of $S$ and $R = S^G$ (fixed points of $G$). The investigation of $S$ as an $RG$-module is a classical problem with applications to (and motivations from) number theory, algebra and topology. In this note we present a very simple approach to this problem in some special cases of interest in number theory. First, we need to recall several basic notions and facts.

By $S^{(G)}$ we denote the ring $\mathrm{Map}(G, S)$ of all functions from $G$ to $S$. The group $G$ acts on $S^{(G)}$ by $f^g(h) = f(gh)$ and $S$ (= constant functions) is the ring of invariants. There is an obvious ring homomorphism $\phi : S \otimes_R S \to S^{(G)}$ given by $\phi(s_1 \otimes s_2)(g) = s_1 s_2^g$. This map is $G$-equivariant, where $G$ acts on $S \otimes_R S$ via the second component.

Recall that $S$ is called *Galois over* $R$ if $\phi$ is surjective (and then $\phi$ is in fact an isomorphism). Clearly $S^{(G)}/S$ is Galois. If $R$, $S$ are Dedekind domains then the extension $S/R$ is Galois iff the corresponding extension of fields of fractions is Galois with group $G$, $S^G = R$ and $S/R$ is unramified (see [4] for more about Galois extensions of rings).

It is well known that if $S/R$ is Galois then $S$ is a projective, faithfully flat $R$-module of constant rank $|G|$. Moreover, the trace map $\mathrm{tr} : S \to R$, $\mathrm{tr}(s) = \sum s^g$, coincides with the module-theoretic trace and is surjective (for a proof base change to $S$ where the situation is clear and then use f.f. descent).

A first step toward a description of the structure of $S$ as an $RG$-module is the following well known lemma:

2000 *Mathematics Subject Classification*: Primary 11R33.

LEMMA 1. *Let $S/R$ be an extension of commutative rings such that $R = S^G$, $S$ is $R$-projective and the trace map is surjective. Then $S$ is a projective $RG$-module.*

*Proof.* There exists an $RG$-modules epimorphism $p : F \to S$ with $F$ a free $RG$-module. Since $S$ is $R$-projective there exists an $R$-module splitting $f$ of $p$. Let $c \in S$ be such that $\mathrm{tr}(c) = 1$. Define a new map $h : S \to F$ by $h(s) = \sum g^{-1} f(s^g c)$. Clearly $h$ is an $RG$-module map and

$$ph(s) = \sum g^{-1}(s^g c) = s\,\mathrm{tr}(c) = s. \ \blacksquare$$

A natural question to ask is under what circumstances $S$ is a free $RG$-module. For rings of integers in finite extensions of the rationals (we call such rings *number rings*) this is an old and still unsolved problem.

If $S$ is a free $RG$-module then there is an element $s \in S$ such that the orbit of $s$ under $G$ is an $R$-basis of $S$. We call any such basis a *normal basis* of $S$. If, moreover, this basis is self-dual with respect to the trace form then we call it a *self-dual normal basis*. For example, the extension $S^{(G)}/S$ always has a self-dual normal basis generated by $\delta^1_-$ where

$$\delta^1_-(g) = \delta^1_g = \begin{cases} 1 & \text{if } g = 1, \\ 0 & \text{if } g \neq 1. \end{cases}$$

In the present note we discuss some basic properties of self-dual normal bases and use them to give very simple proofs of the following theorems:

THEOREM 1. *Let $R$ be the ring of integers in a totally real number field. If $S/R$ is a non-trivial Galois extension of number rings with Galois group $G$ of odd order then it does not have a normal basis.*

THEOREM 2. *Let $R = \mathbb{Z}[\xi_{p^k} + \xi_{p^k}^{-1}]$, where $p$ is an odd prime and $\xi_n$ is a primitive $n$th root of 1. Let $S$ be the ring of integers in a cyclic extension $L$ of $K = \mathbb{Q}(\xi_{p^k} + \xi_{p^k}^{-1})$ of degree $p^n$. If $S[1/p]/R[1/p]$ is Galois and has a normal basis then it coincides with the cyclotomic $p^n$-extension of $R[1/p]$ (i.e. $L$ is the unique extension of $K$ of degree $p^n$ contained in $\mathbb{Q}(\xi_{p^t})$ for some $t$).*

These results are not new. Theorem 1 and some generalizations have been obtained before by a slightly different method by J. Brinkhuis [3]. We do not know of any explicit reference for Theorem 2, but it can be derived from a much more general result of Cornelius Greither [4] (see Theorem III.3.6 there). Nevertheless, the simplicity of our approach is appealing and we think that it is of some interest.

**2. Self-dual normal bases.** The following observation describes a very useful relation between Galois extensions of rings and some units of the group ring of the Galois group:

PROPOSITION 1. *Let $S$ be a commutative ring, $G$ a finite group of automorphisms of $S$ and $R = S^G$. For $u \in S$ the following are equivalent*:

(1) $\sum u^g g^{-1}$ *is a unit in* $SG$;
(2) $S/R$ *is Galois with normal basis generated by* $u$.

*Proof.* Let $(\sum u^g g^{-1})(\sum w_g g) = 1$. In other words, for any $h \in G$ we have $\sum u^g w_{gh} = \delta^1_h$, i.e. $\sum u^{gh^{-1}} w_g = \delta^1_h$, so also $\sum u^g w^h_g = \delta^1_h$. Since $\phi(\sum u^g \otimes w_g)(h) = \sum u^g w^h_g = \delta^1_h$, the natural map $\phi : S \otimes_R S \to S^{(G)}$ is surjective and $S/R$ is Galois. In particular, $\phi$ is an isomorphism of $SG$-modules. Now $\phi(1 \otimes u) = (\sum u^g g^{-1})\delta^1_-$ is a free generator of the $SG$-module $S^{(G)}$, so $1 \otimes u$ is a free generator of $S \otimes_R S$. Since $RGu \subseteq S$ and after tensoring with $S$ we get equality, $u$ is a free generator of $S$ (note that $S/R$ is faithfully flat). This shows that (1) implies (2).

For the converse observe that the $SG$-module isomorphism $\phi$ maps the element $1 \otimes u$ to a free generator $f : g \mapsto u^g$. But $\delta^1_-$ is also a free generator and $(\sum u^g g^{-1})\delta^1_- = f$ so $\sum u^g g^{-1}$ is a unit. ∎

COROLLARY 1. *If $S/R$ is a Galois extension of commutative rings with group $G$ having a normal basis, then for any normal subgroup $H$ of $G$ the extension $S^H/R$ is Galois and has a normal basis.*

*Proof.* If $\sum u^g g^{-1}$ is a unit of $SG$ then under the natural surjection $SG \to SG/H$ it maps to a unit $\sum v^h h^{-1}$ of $SG/H$, where $v = \mathrm{tr}_{S/S^H} u$. But this is a unit in $S^H G/H$ so the result follows by Proposition 1. ∎

Now we can prove the following very useful proposition, which is the heart of our approach:

PROPOSITION 2. *If $S/R$ is a Galois extension of commutative rings with abelian Galois group of odd order and if it has a normal basis then it has a self-dual normal basis.*

For cyclic groups of odd order this result has been obtained by Kersten and Michaliček [5]. We were informed that some form of Proposition 2 was pointed out to L. McCulloh by Miyamoto many years ago, but we do not know of any written reference. Note also that Bayer and Lenstra ([2], [1]) proved that for odd degree Galois extensions of fields a self-dual normal basis always exists.

QUESTION. Does Proposition 2 remain true without the assumption that the Galois group is abelian?

*Proof of Proposition 2.* Suppose that $u$ generates a normal basis of $S$. By Proposition 1, $U = \sum u^g g^{-1}$ is a unit in $SG$. Note that $G$ acts on $SG$ via its action on $S$ (i.e. $(\sum a_g g)^h = \sum a^h_g g$). Observe that $U^h = hU$ for every $h \in G$.

Recall that in the group ring $SG$ we have an $S$-involution $*$ which acts on $G$ as an inverse (i.e. $(\sum a_g g)^* = \sum a_g g^{-1}$). Clearly, $*$ commutes with the $G$-action. Since $G$ is abelian of odd order, it has an automorphism $\psi$ which maps $g^2$ to $g$ for all $g \in G$. The automorphism $\psi$ extends to a ring automorphism of $SG$ which we also denote by $\psi$. Note that $\psi$ commutes with $*$ and with the $G$-action.

Consider the unit $W = \psi(U(U^{-1})^*)$. Easy calculations show that $WW^* = 1$ and that $W^h = hW$ for all $h \in G$. Equivalently, $W = \sum w^g g^{-1}$ for some $w \in S$. In particular, $w$ generates a normal basis of $S$ and the equality $WW^* = 1$ means exactly that this basis is self-dual. ∎

**3. Number rings.** Now we are in a position to prove Theorems 1 and 2. Recall that by a number ring we mean the ring of integers in a finite extension of the rationals.

*Proof of Theorem 1.* Suppose that $S/R$ is a Galois extension of number rings with an abelian Galois group $G$ of odd order and having a normal basis. By Proposition 2, $S$ has a self-dual normal basis generated by $a \in S$. Thus $X = \sum a^g g^{-1}$ is a unit in $SG$ and $XX^* = 1$. In particular, $\mathrm{tr}_{S/R}(a^2) = \sum a^g \cdot a^g = 1$, so $\mathrm{tr}_{S/\mathbb{Z}}(a^2) = [R : \mathbb{Z}]$.

Suppose now that $R$ is totally real (and so is $S$). Then all the conjugates of $a^2$ are positive real numbers, so by the arithmetic-geometric mean inequality we get $\mathrm{tr}_{S/\mathbb{Z}}(a^2) \geq n \sqrt[n]{N_{S/\mathbb{Z}}(a^2)}$, where $n = [S : \mathbb{Z}]$. Since $a^2$ is an algebraic integer, its norm is at least 1. Consequently, $[R : \mathbb{Z}] \geq [S : \mathbb{Z}]$, which is possible only if $R = S$ (alternatively, one could note that all conjugates of $a^2$ have absolute value at most 1, so $a^2$ is a root of unity in $S$, hence 1, by a well known theorem of Kronecker). This proves Theorem 1 for abelian extensions. The general case follows by Corollary 1 and the fact that groups of odd order are solvable. ∎

Remark. Before asking whether $S$ is a free $RG$-module one should check if $S$ is a free $R$-module. In the situation of Theorem 1 this is indeed true. In fact, $S$ is an unramified extension of $R$. The class of $S$ in the class group of $R$ is called the Steinitz class of $S$. An excellent description of Steinitz classes is given in Narkiewicz's book [7]. From the method of computing the Steinitz class described there one can relatively easily deduce that if $L/K$ is an odd degree, unramified Galois extension of number fields then the ring of integers of $L$ is a free module over the integers on $K$.

A more conceptual argument goes as follows. First recall that the square of the Steinitz class coincides with the class of the discriminant ideal. In particular, for unramified extensions the square of the Steinitz class is trivial. On the other hand, the definition of the Galois extensions of rings given in the introduction implies that $S \otimes_R S$ is a free $S$-module (it is even free over

$SG$). In other words, the Steinitz class is in the kernel of the base-change map from the class group of $R$ to the class group of $S$. But the composition of base change and the norm induces multiplication by $[L:K]$ on the class group of $R$. Consequently, the Steinitz class has order dividing both 2 and $[L,K]$. Since $[L:K]$ is odd, the Steinitz class vanishes.

Note that Taylor [8] proved that in the situation of the above theorem $S$ is always a free $\mathbb{Z}G$-module.

*Proof of Theorem 2.* Recall that $R=\mathbb{Z}[\xi_{p^k}+\xi_{p^k}^{-1}]$ and $S$ is the ring of integers in a cyclic extension $L$ of $K=\mathbb{Q}(\xi_{p^k}+\xi_{p^k}^{-1})$ of degree $p^n$ such that $S[1/p]/R[1/p]$ is Galois and has a normal basis, where $p$ is an odd prime. By Proposition 2, $S[1/p]/R[1/p]$ has a self-dual normal basis generated by some $a\in S[1/p]$. In other words, $X=\sum a^g g^{-1}$ is a unit in $S[1/p]G$ and $XX^*=1$.

Consider any ring homomorphism $\psi: LG\to\mathbb{C}$. Clearly $\psi(R)=R$ (we consider $K$ as a subfield of $\mathbb{C}$), $\psi(SG)\subseteq\psi(S)[\xi_{p^n}]$ and $\psi(S)$ is the ring of integers in a cyclic extension $\psi(L)$ of $K$ of degree $p^n$. Since $L$ is totally real, we have $\psi(u^*)=\overline{\psi(u)}$ for any $u\in LG$. In particular, $\psi(X^2)=\psi(X/X^*)=\psi(X)/\overline{\psi(X)}$ has absolute value 1. If $\sigma$ is any embedding of $\psi(L)(\xi_{p^n})$ into $\mathbb{C}$, then $\sigma\psi$ is another homomorhism of $LG$ into $\mathbb{C}$. It follows that all conjugates of $\psi(X^2)$ have absolute value 1.

We show now that $\psi(X^2)$ is an algebraic integer. Note that all primes of $\psi(L)(\xi_{p^n})$ over $p$ are stable under complex conjugation. To show this let $m=\max\{n,k\}$. There is only one prime $\pi$ over $p$ in $\mathbb{Q}(\xi_{p^m}+\xi_{p^m}^{-1})$ and it ramifies in $\mathbb{Q}(\xi_{p^m})$. Thus the ramification index of any prime $\beta$ of $\psi(L)(\xi_{p^m})$ over $\pi$ is even. On the other hand, $\psi(L)(\xi_{p^m}+\xi_{p^m}^{-1})/\mathbb{Q}(\xi_{p^m}+\xi_{p^m}^{-1})$ is Galois of odd degree, so the ramification index of $\beta$ is even iff $\beta$ ramifies in the quadratic extension $L(\xi_{p^m})/L(\xi_{p^m}+\xi_{p^m}^{-1})$. In particular, $\beta$ is stable under complex conjugation. Consequently, the $p$-parts of $\psi(X)$ and $\overline{\psi(X)}$ are the same. Thus $\psi(X)/\overline{\psi(X)}=\psi(X^2)$ is a $p$-unit of $\psi(L)(\xi_{p^m})$. Observe that $\psi(X)$ is a $q$-unit for every prime $q\neq p$, since $X$ is a unit of $S[1/p]G$. Thus $\psi(X^2)$ is a $q$-unit for every prime $q$. In particular, it is an algebraic integer.

We proved so far that $\psi(X^2)$ is an algebraic integer all of whose conjugates have absolute value 1. Thus $\psi(X^2)$ is a root of 1 by a theorem of Kronecker. Consequently, $\psi(X)$ is a root of 1 in $\psi(L)(\xi_{p^n})$. Since $p$ is the only prime ramified in $\psi(L)(\xi_{p^n})$, we conclude that the group of roots of unity in this field has order $2p^s$ for some $m\leq s$. Consequently, $\psi(X)^{2p^s}=1$ for all ring homomorphisms $\psi$, and therefore $X^{2p^s}=1$ (recall that the common kernel of all the homomorphisms of $LG$ into $\mathbb{C}$ is trivial).

Now note that the trace of a regular representation of $LG$ is given by $T(\sum u_g g)=|G|u_1$. But the trace of an element of finite order dividing $2p^s$ is a sum of $2p^s$th roots of 1, so in particular $|G|a=T(X)\in\mathbb{Q}(\xi_{p^s})$. Thus

we showed that $L = K(a) \subseteq K(\xi_{p^s}) = \mathbb{Q}(\xi_{p^s})$. This finishes the proof of Theorem 2. ∎

REMARK. The cyclotomic $p^n$-extension of $R[1/p]$ has a normal basis, as shown in [4].

As a direct consequence we get the following result of Kersten and Michaliček [6]:

COROLLARY 2. *If $k = n = 1$ and $S/R$ is Galois then $S[1/p]/R[1/p]$ does not have a normal basis.*

REMARK. Corollary 2 suggests the following attack on Vandiver's Conjecture: show that any extension as above has to have a normal basis and conclude that there is no such extension. Of course, at present nobody knows how to do that.

*REFERENCES*

[1] E. Bayer-Fluckiger, *Self-dual normal bases*, Indag. Math. 51 (1989), 379–383.
[2] E. Bayer-Fluckiger and H. W. Lenstra, Jr., *Forms in odd degree extensions and self-dual normal bases*, Amer. J. Math. 112 (1990), 359–373.
[3] J. Brinkhuis, *On the Galois module structure over CM-fields*, Manuscripta Math. 75 (1992), 333–347.
[4] C. Greither, *Cyclic Galois Extensions of Commutative Rings*, Lecture Notes in Math. 1534, Springer, Berlin, 1992.
[5] I. Kersten und J. Michaliček, *Kubische Galoiserweiterungen mit Normalbasis*, Comm. Algebra 9 (1981), 1863–1871.
[6] —, —, *A remark about Vandiver's Conjecture*, C. R. Math. Rep. Acad. Sci. Canada 7 (1985), 33–37.
[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, 1990.
[8] M. J. Taylor, *On Fröhlich conjecture for rings of integers of tame extensions*, Invent. Math. 63 (1981), 41–79.

Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL 61801, U.S.A.
E-mail: mazur1@math.uiuc.edu

*Received 20 January 2000* (3871)