ACTA ARITHMETICA
123.1 (2006)

Self-dual normal bases for infinite odd abelian Galois ring extensions

by

Patrik Lundström (Trollhättan)

1. Introduction. Let S/R be an extension of commutative rings always assumed to be associative and possessing identity elements. Let G be a finite group of R-algebra automorphisms of S such that $R = S^G := \{s \in S \mid g.s = s, g \in G\}$.

Recall that an R-basis for S is called *normal*, with respect to G, if it is the G-orbit of some element s in S. In that case s is called a *normal basis generator*. Normal bases do not always exist. In fact, by a result of Noether [18], if S/R is a finite extension of Dedekind domains, $G = \mathrm{Aut}_R(S)$ and R is a discrete valuation ring, then the extension has a normal basis precisely when it is tamely ramified. On the other hand, if R is semilocal and S/R is a Galois ring extension with finite group G, that is, if S/R is a separable ring extension and for all $g, g' \in G$, $g \neq g'$, and all nonzero idempotents $e \in S$, there is $s \in S$ such that $(g.s)e \neq (g'.s)e$, then the extension always has a normal basis (see [5]). In particular, a finite Galois field extension always has a normal basis. A Galois ring extension S/R with finite group G is called *odd* if the order of G is odd.

The trace function $\mathrm{tr}_{S/R} : S \to R$, defined by $\mathrm{tr}_{S/R}(s) = \sum_{g \in G} g.s$ for all $s \in S$, induces a symmetric bilinear form $q_S : S \times S \to R$ by the relation $q_S(s, s') = \mathrm{tr}_{S/R}(ss')$ for all $s, s' \in S$. The bilinear form q_S is also a *G-form*, that is, it is invariant under the action of G. If a normal basis $\{g.s \mid g \in G\}$ is self-dual with respect to q_S, that is, if $q_S(g.s, g.s) = 1$ and $q_S(g.s, g'.s) = 0$ if $g \neq g'$ for all $g, g' \in G$, then it is called a *self-dual normal basis* and s is called a *self-dual normal basis generator*. Note that the existence of such a basis can alternatively be formulated by saying that (S, q_S) and $(R[G], q_0)$ are isomorphic as G-forms, where q_0 is the unit G-form, that is, the R-bilinear map $R[G] \times R[G] \to R$ defined by $q_0(g, g) = 1$ and $q_0(g, g') = 0$ if $g \neq g'$ for all $g, g' \in G$. The problem of when a self-dual

2000 *Mathematics Subject Classification*: 13B05, 11S20, 11R04, 11R32, 11R33.

normal basis exists has only been solved in particular cases. Bayer-Fluckiger [1] has shown that if S/R is an odd Galois field extension, then a self-dual normal basis always exists. For more results on self-dual normal bases for field extensions, see the paper [2] by Bayer-Fluckiger and Lenstra and the extensive paper [3] by Bayer-Fluckiger and Serre. By adapting an idea from Kersten and Michaliček [8], Mazur [16] has shown the following result for general Galois ring extensions.

THEOREM 1 (Mazur). *Let S/R be a finite odd abelian Galois ring extension with Galois group G. If S and $R[G]$ are isomorphic as left $R[G]$-modules, then (S, q_S) and $(R[G], q_0)$ are isomorphic as G-forms.*

If G is infinite, the definition of a normal basis makes no sense. However, if we let (G, R) denote the set of functions $f : G \to R$ and we let G operate on (G, R) by $(g.f)(g') = f(g^{-1}g')$, $g, g' \in G$, then the existence of a normal basis can be formulated by saying that there is a left R-module isomorphism $F : (G, R) \to S$ that respects the action of G. Namely, if s is a normal basis generator, then we can define F by $F(f) = \sum_{g\in G} f(g)g.s$ for all $f \in (G, R)$. Conversely, if $F : (G, R) \to S$ is an isomorphism as above and $f \in (G, R)$ is defined by $f(1) = 1$ and $f(g) = 0$ for all $g \in G \setminus \{1\}$, then $s := F(f)$ is a normal basis generator. Lenstra [9] has shown that this version of the normal basis theorem is valid for infinite Galois field extensions S/R provided we only consider the continuous functions $G \to R$. In fact, he shows that if G is equipped with the Krull topology, R with the discrete topology and we let $C(G, R)$ denote the set of continuous functions from G to R, then there is an R-vector space isomorphism from $C(G, R)$ to S respecting the action of G.

Recall that an extension of connected rings S/R is called *infinite Galois* with group G if $G = \mathrm{Aut}_R(S)$, $S^G = R$ and S/R is *locally finitely generated separable*, that is, every finite subset of S belongs to a finitely generated separable ring extension of R in S. In that case, the Krull topology can be defined on G and there is a bijection between the closed subgroups of G and the set of locally finitely generated separable ring extensions in the usual sense of Galois theory (see [17]). We say that such an extension is *odd* if S is the union of finite odd Galois ring extensions of R. The main purpose of this article is to prove the following infinite version of Theorem 1.

THEOREM 2. *Let S/R be an infinite odd abelian Galois ring extension with S connected. If S and $C(G, R)$ are isomorphic as left $R[G]$-modules, then (S, q_S) and $(C(G, R), q_0)$ are isomorphic as coherent G-forms.*

For the proof, see Section 3, and for the definition of coherent G-forms, see Section 2. The secondary purpose is to apply Theorem 2 to infinite odd abelian Galois extensions of fields, connected Galois ring extensions where the base ring is local and compact in the induced topology, and number rings

in local fields where the residue field of the base ring is finite (see Corollaries 1–3 in Section 3).

For related results concerning normal bases for infinite extensions, see [6], [7], [10]–[15].

2. Coherent G-forms. For the rest of the article, unless otherwise stated, we assume that S/R is an infinite Galois extension of connected rings with group G. We also fix the following notation. Let $\mathcal{N}$ denote the set of open normal subgroups of G and for $N, N' \in \mathcal{N}$, put $N' \prec N$ if $N \subseteq N'$. Note that the relation $\prec$ makes $\mathcal{N}$ a directed set.

Let M be a discrete left R-module equipped with a continuous R-linear left action of G. If the group G is infinite, then instead of considering R-bilinear maps $M \times M \to R$, it is more natural to study coherent systems of R-bilinear maps $M^N \times M^N \to R$, $N \in \mathcal{N}$, in the sense defined below.

Definition 1. We say that $q = (q^N)_{N\in\mathcal{N}}$ is a *coherent G-form* on M if each q^N is an R-bilinear G-form on M^N such that $q^{N'}(x, \mathrm{tr}_{N'/N}(y)) = q^N(x, y)$ whenever $N' \prec N$, $x \in M^{N'}$, $y \in M^N$, where $\mathrm{tr}_{N'/N} : M^N \to M^{N'}$ is defined by $\mathrm{tr}_{N'/N}(x) = \sum_{s\in N'/N} s.x$ for all $x \in M^N$. Furthermore, if (M_1, q_1) and (M_2, q_2) are coherent G-forms, then we say that $f = (f^N)_{N\in\mathcal{N}}$ is a *morphism of coherent G-forms* $(M_1, q_1) \to (M_2, q_2)$ if each f^N is a morphism of G-forms $(M_1^N, q_1^N) \to (M_2^N, q_2^N)$ such that if $N' \prec N$, then $f^N|_{M_1^{N'}} = f^{N'}$.

Remark 1. Every coherent G-form (M, q) defines, in a natural way, an R-bilinear map $\overline{q} : M \times \overline{M} \to R$, where $\overline{M} = \varprojlim_{N\in\mathcal{N}} M^N$, the inverse limit taken with respect to the maps $\mathrm{tr}_{N'/N}$, $N' \prec N$. In fact, if $x \in M$ and $y = (y^N)_{N\in\mathcal{N}} \in \overline{M}$, then choose $N' \in \mathcal{N}$ such that $x \in M^{N'}$ and put $\overline{q}(x, y) = q^{N'}(x, y^{N'})$. It is easy to check that $\overline{q}$ is well defined.

We now define the two coherent G-forms mentioned in the introduction.

Example 1. (i) If we put $q_S = (q_{S^N})_{N\in\mathcal{N}}$, then (S, q_S) is a coherent G-form.

(ii) Suppose that $N' \prec N$. The set $C(G, R)^N$ can, in a natural way, be identified with $R[G/N]$. With this identification, the map $\mathrm{tr}_{N'/N} : C(G, R)^N \to C(G, R)^{N'}$ coincides with the canonical map $n_{N'/N} : R[G/N] \to R[G/N']$. If we let q_0^N denote the unit G-form on $R[G/N]$, then it is easy to check that if we put $q_0 = (q_0^N)_{N\in\mathcal{N}}$, then $(C(G, R), q_0)$ is a coherent G-form. Note also that if we use the notation from Remark 1, then we may write $\overline{C(G, R)} = R[[G]] := \varprojlim_{N\in\mathcal{N}} R[G/N]$, where the last inverse limit is taken with respect to the maps $n_{N'/N}$.

3. Resolvents for infinite extensions. In this section, we introduce a resolvent map for infinite Galois ring extensions (Definition 2) and show two results (Propositions 1 and 2) concerning the existence of (self-dual) normal bases and units (norm one elements) in the image of the resolvent. Then we use these results to prove Theorem 2. At the end of this section, we apply Theorem 2 to three different cases of infinite extensions (see Corollaries 1–3).

Recall that in the finite case, the resolvent map $r : S \to S[G]$ is defined by $r(s) = \sum_{g\in G}(g.s)g^{-1}$ for all $s \in S$. The importance of this map stems from the fact that $s \in S$ is a normal basis generator for S/R if and only if $r(s)$ is a unit in $S[G]$, and s is a self-dual normal basis generator for S/R if and only if $r(s)$ is a norm one element in $S[G]$, that is, $r(s)\overline{r(s)} = 1$, where $S[G] \ni x \mapsto \overline{x} \in S[G]$ is the involution defined by the S-linear extension of the relation $\overline{g} = g^{-1}$ for all $g \in G$ (for the details, see e.g. [16]).

Definition 2. The resolvent map $r : \overline{S} \to S[[G]]$ is defined by $r((s_N)_{N\in\mathcal{N}}) = (r_N(s_N))_{N\in\mathcal{N}}$ for all $(s_N)_{N\in\mathcal{N}} \in \overline{S}$ where $r_N : S^N \to S^N[G/N]$ is the usual resolvent map for the extension S^N/R. The involution $S[[G]] \ni x \mapsto \overline{x} \in S[[G]]$ and hence, norm one elements, are defined by the natural extension from the finite case.

We gather some well known results concerning units and norm one elements in group rings in the following lemma (parts of which can be found in e.g. [16]). Recall that the action of G on S induces an action of G on $S[G]$.

Lemma 1. *Let S/R be a finite Galois ring extension with Galois group G.*

(a) *If $x \in R[G] \cap S[G]^*$, then $x^{-1} \in R[G]^*$.*
(b) *Take $x \in S[G]$. Then x is a resolvent if and only if $g.(xg^{-1}) = x$ for all $g \in G$.*
(c) *If $x \in S[G]^*$ is a resolvent, then $\overline{x^{-1}}$ is a resolvent.*

Suppose that G is an odd abelian group and let $\sqrt{\cdot}$ be the unique S-linear extension to $S[G]$ of the group automorphism $\sqrt{g^2} = g$ on G.

(d) *If $x, y \in S[G]$ are resolvents, then $\sqrt{xy}$ is a resolvent.*
(e) *If $x \in S[G]^*$ is a resolvent, then $\sqrt{x\overline{x^{-1}}}$ is a resolvent which is a norm one element.*

Proof. (a) Suppose that $x^{-1} = y \in S[G]$. Applying the action of G on $S[G]$ to the equality $xy = 1$ gives us $x(g.y) = (g.x)(g.y) = g.(xy) = g.1 = 1$ for all $g \in G$. Since the inverse of x is unique this implies that $g.y = y$ for all $g \in G$. Hence $y \in R[G]$.

(b) Take $x \in S[G]$. Suppose that $x = r(s)$ for some $s \in S$. Take $g \in G$. Then

$$g.(xg^{-1}) = g.(r(s)g^{-1}) = g.\Big(\sum_{h\in G} h(s)h^{-1}g\Big) = \sum_{h\in G} gh.(s)(gh)^{-1} = r(s).$$

On the other hand, suppose that $x = \sum_{h\in G} s_h h$ for some $s_h \in S$, $h \in G$, and that $g.(xg^{-1}) = x$ for all $g \in G$. Then $\sum_{h\in G}(g.s_h)hg^{-1} = \sum_{h\in G} s_h h$ for all $g \in G$. Equating coefficients for 1 gives $g.s_g = s_1$ for all $g \in G$ and hence $s_g = g^{-1}.s_1$ for all $g \in G$. Therefore $x = r(s_1)$.

(c) Suppose that x is a resolvent and put $y := x^{-1}$. Then, by (b), $h.(xh^{-1}) = x$ for all $h \in G$. Hence, since G is abelian, we infer for each $h \in G$ that

$$1 = h.1 = h.(xy) = h.(xh^{-1}hy) = (h.(xh^{-1}))(h.(yh)) = x(h.(yh)).$$

Since the inverse of x is unique, $h.(yh) = y$ and hence $h.(\overline{y}h^{-1}) = \overline{y}$ for all $h \in G$. By (b), $\overline{y}$ is a resolvent.

(d) Assume that $x = \sum_{g\in G} g.(s)g^{-1}$ and $y = \sum_{g\in G} g.(s')g^{-1}$ for some $s, s' \in S$. Then $xy = \sum_{g\in G} c_g g^{-1}$ where $c_g = \sum_{h\in G}(h.s)(gh^{-1}.s')$ for all $g \in G$. Then, since G is abelian, we get $f.c_1 = \sum_{h\in G}(h.s)(f^2h^{-1}.s') = c_{f^2}$ for all $f \in G$. Hence, since the order of G is odd, we find

$$\sqrt{xy} = \sqrt{\sum_{g\in G} c_g g^{-1}} = \sqrt{\sum_{g\in G} c_{g^2} g^{-2}} = \sum_{g\in G} g.(c_1)g^{-1} = r(c_1).$$

(e) Put $y = \overline{x^{-1}}$. A straightforward calculation shows that $\sqrt{xy}$ is a norm one element. The rest follows from (c) and (d). ∎

Proposition 1. *The left $R[G]$-modules S and $C(G,R)$ are isomorphic if and only if there is a unit in the image of the resolvent.*

Proof. Suppose that we have an $R[G]$-module isomorphism $\varphi : C(G,R) \to S$. Take $N \in \mathcal{N}$ and define $\delta_N \in C(G,R)^N$ by $\delta_N(s) = 1$ if $s \in N$ and $\delta_N(s) = 0$ otherwise. Since each δ_N is a free generator for the $R[G/N]$-module $C(G,R)^N$, the same is true for $s_N := \varphi(\delta_N) \in S^N$. From the finite case we know that each $r_N(s_N)$ is a unit in $S^N[G/N]$. Then $s := (s_N)_{N\in\mathcal{N}} \in \overline{S}$. In fact, this follows from the commutativity of the diagram

$$\begin{array}{ccc} C(G,R)^N & \xrightarrow{\varphi_N} & S^N \\ {\scriptstyle \mathrm{tr}_{N'/N}}\downarrow & & \downarrow{\scriptstyle \mathrm{tr}_{N'/N}} \\ C(G,R)^{N'} & \xrightarrow{\varphi_{N'}} & S^{N'} \end{array}$$

for all $N' \prec N$, and the fact that $\mathrm{tr}_{N'/N}(\delta_N) = \delta_{N'}$, where φ_N denotes the restriction of φ to $C(G,R)^N$. Hence, $r(s)$ is a unit in $S[[G]]$.

On the other hand, suppose that there is $s = (s_N)_{N\in\mathcal{N}} \in \overline{S}$ such that $r(s)$ is a unit in $S[[G]]^*$. Then, by Lemma 1(a), each $r_N(s_N)$ is a unit in $S^N[G/N]$ and hence each s_N is a normal basis generator for S^N. Now we define $\varphi : C(G,R) \to S$. Take $f \in C(G,R)$. Since G is compact and R is equipped with the discrete topology, there is $N \in \mathcal{N}$ such that f is constant

on cosets of N in G. Define $\varphi : C(G,R) \to S$ by $\varphi(f) = \sum_{g\in G/N} f(g)(g.s_N)$. It is clear that φ is R-linear and that it respects the action of G. Since $s \in \overline{S}$, φ is well defined, and since each s_N is a normal basis generator for S^N, φ is bijective. ∎

PROPOSITION 2. *The coherent G-forms (S, q_S) and $(C(G,R), q_0)$ are isomorphic if and only if the image of the resolvent contains a norm one element.*

Proof. This follows from the finite case in the same way as in the proof of Proposition 1. ∎

Proof of Theorem 2. Assume that there is an isomorphism of left $R[G]$-modules from $C(G,R)$ to S. Then, by Proposition 1, there is $s=(s_N)_{N\in\mathcal{N}}\in\overline{S}$ such that $r(s)$ is a unit in $S[[G]]$. Since the square root maps and the involutions $\overline{(\cdot)}$ on $S[G/N]$, $N \in \mathcal{N}$, are ring homomorphisms and they commute with the natural maps $S[G/N] \to S[G/N']$, $N' \prec N$, we can use Lemma 1(e) to construct $s' \in \overline{S}$ such that $r(s')$ is a norm one element in $S[[G]]$. Theorem 2 now follows from Proposition 2. ∎

Now we apply Theorem 2 to three different cases. First we consider infinite Galois field extensions.

COROLLARY 1. *If L/K is an infinite odd abelian Galois field extension, then (L, q_L) and $(C(G,K), q_0)$ are isomorphic as coherent G-forms.*

Proof. In [9] Lenstra shows that the left $K[G]$-modules L and $C(G,K)$ are isomorphic. The result now follows from Theorem 2. ∎

Next, we consider infinite Galois ring extensions. Recall that an ideal I in a ring is called *residually nilpotent* if $\bigcap_{n=1}^{\infty} I^n = \{0\}$. In that case $\{I^n\}_{n\geq 1}$ form a basis of neighborhoods of zero of a Hausdorff topology on the ring called the *I-adic topology* (see e.g. [4]).

COROLLARY 2. *Let S/R be an infinite odd abelian Galois ring extension with S connected. If R is a local ring with a residually nilpotent maximal ideal I such that R is compact in the I-adic topology, then (S, q_S) and $(C(G,R), q_0)$ are isomorphic as coherent G-forms.*

Proof. By Theorem 1.3 in [11], the left $R[G]$-modules S and $C(G,R)$ are isomorphic. The result now follows from Theorem 2. ∎

Finally, we consider infinite extensions of number rings. Recall that extensions are called *unramified* (resp. tamely ramified) if all finite subextensions are unramified (resp. tamely ramified).

COROLLARY 3. *Let S/R be an infinite odd unramified abelian extension of number rings in local fields. If the residue field of R is finite, then (S, q_S) and $(C(G,R), q_0)$ are isomorphic as coherent G-forms.*

Proof. We prove this in two different ways. The extension S/R being unramified, it is a Galois ring extension (see e.g. [5]). The claim now follows from Corollary 2.

On the other hand, the extension S/R being unramified, it is, of course, tamely ramified. Hence, by Theorem 1.5 in [14], the left $R[G]$-modules S and $C(G, R)$ are isomorphic. Now we can again use Theorem 2 to obtain the desired result. ∎

REMARK 2. Corollaries 1 and 3 have already appeared in [13] and [14] in the cases when the characteristic of K is odd and the residue class field of R is of odd order, respectively; they were proved by other means.

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] E. Bayer-Fluckiger et J.-P. Serre, *Torsions quadratiques et bases normales autoduales*, ibid. 116 (1994), 1–64.

[4] N. Bourbaki, *General Topology*, Hermann, 1966.

[5] S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. 52 (1965).

[6] D. Hachenberger, *Primitive normal bases for towers of field extensions*, Finite Fields Appl. 5 (1999), 378–385.

[7] —, *Universal normal bases for the abelian closure of the field of rational numbers*, Acta Arith. 93 (2000), 329–341.

[8] I. Kersten und J. Michaliček, *Kubische Galoiserweiterungen mit Normalbasis*, Comm. Algebra 9 (1981), 1863–1871.

[9] H. W. Lenstra, Jr., *A normal basis theorem for infinite Galois extensions*, Indag. Math. 47 (1985), 221–228.

[10] P. Lundström, *Self-dual normal bases for infinite Galois field extensions*, Comm. Algebra 26 (1998), 4331–4341.

[11] —, *Normal bases for infinite Galois ring extensions*, Colloq. Math. 79 (1999), 235–240.

[12] —, *Normal integral bases for infinite abelian extensions*, Acta Arith. 100 (2001), 79–83.

[13] —, *Cohomology and self-dual normal bases for infinite Galois field extensions*, J. Algebra 256 (2002), 531–541.

[14] —, *Self-dual normal integral bases for infinite unramified extensions*, J. Number Theory 97 (2002), 350–367.

[15] —, *Cohomology and the normal basis theorem*, preprint, Univ. of Trollhättan/ Uddevalla, 2005.

[16] M. Mazur, *Remarks on normal bases*, Colloq. Math. 87 (2001), 79–84.

[17] T. Nagahara, *A note on Galois theory of commutative rings*, Proc. Amer. Math. Soc. 18 (1965), 334–340.

[18] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. 167 (1932), 147–152.

Department of Technology, Mathematics and Computer Science
University West
Gärdshemsvägen 4, Box 957
461 29 Trollhättan, Sweden
E-mail: patrik.lundstrom@hv.se

Received on 21.4.2005
and in revised form on 3.2.2006 (4980)