COLLOQUIUM MATHEMATICUM

VOL. 79 1999 NO. 2

NORMAL BASES FOR INFINITE GALOIS RING EXTENSIONS

BY

PATRIK LUNDSTRÖM (GÖTEBORG)

1. Introduction. Let $L \supseteq K$ be a Galois field extension with Galois group G. We consider G as a topological group with the Krull topology (see e.g. [LS, p. 329]).

The normal basis theorem asserts that if L has finite dimension over K, then there is $x \in L$ such that $\{\sigma(x)\}_{\sigma\in G}$ form a basis for L as a vector space over K (for a proof see e.g. [J, p. 283]). The sequence $\{\sigma(x)\}_{\sigma\in G}$ is called a *normal basis* and x is called a *normal basis generator*. L and $K[G]$ are, in a natural way, left $K[G]$-modules. The normal basis theorem can be formulated by saying that there is a left $K[G]$-module isomorphism

$$K[G] \cong L. \tag{1}$$

The group algebra $K[G]$ can be viewed as the set (G,K) of functions $f : G \to K$ with a $K[G]$-module structure induced by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$ for all $\sigma,\tau \in G$. In this context, (1) is equivalent to the existence of a left $K[G]$-module isomorphism

$$(G,K) \cong L. \tag{2}$$

If L has infinite dimension over K, then the normal basis theorem is, of course, not true any more. However, in [LH] two infinite analogues of (1) and (2) are proved (see (3) and (4) below). The approach taken there is the following: Denote by U the set of open normal subgroups N of G. Taking into account the notations used later, we write $N' \prec N$ when $N \subseteq N'$ are open normal subgroups of G. For $N' \prec N$, let the ring homomorphism $\varrho_{N'/N} : K[G/N] \to K[G/N']$ be induced by the natural group homomorphism $G/N \to G/N'$. If $N \in U$, let $L^N = \{y \in L \mid \sigma(y) = y \text{ for all } \sigma \in N\}$. Then L^N is a finite Galois extension of K with Galois group G/N. When $N' \prec N$, we have the trace map $\mathrm{Tr}_{N'/N} : L^N \to L^{N'}$ given by $\mathrm{Tr}_{N'/N}(y) = \sum_{\sigma\in N'/N} \sigma(y)$. Since U is a pre-ordered set with respect to the relation $\prec$, we can define the inverse limits $K[[G]] = \varprojlim_{N\in U} K[G/N]$

1991 *Mathematics Subject Classification*: Primary 13B05.

and $\overline{L} = \varprojlim_{N\in U} L^N$, taken with respect to the maps $\varrho_{N'/N}$ and $\mathrm{Tr}_{N'/N}$ respectively. $\overline{L}$ is in a natural way a left module over $K[[G]]$.

1.1. Theorem. *Let $L \supseteq K$ be a Galois field extension with Galois group G. Then there is a left $K[[G]]$-module isomorphism*

$$K[[G]] \cong \overline{L}. \tag{3}$$

Note that Mostowski [M] proved an analogous theorem already in 1955 for the case when the characteristic of K is zero.

If we replace (G,K) in (2) by $C(G,K)$, the set of continuous functions $f: G \to K$ (where we let K have the discrete topology), then the following theorem holds:

1.2. Theorem. *Let $L \supseteq K$ be a Galois field extension with Galois group G. Then there is a left $K[G]$-module isomorphism*

$$C(G,K) \cong L. \tag{4}$$

If $S \supseteq R$ is a finite Galois ring extension (see Section 4 for our conventions about Galois ring extensions) of commutative rings, where S is connected (i.e. it has no non-trivial idempotents) and R is local, then a normal basis exists for $S \supseteq R$ (see e.g. [C]).

Recall that an ideal I of a ring R is called *residually nilpotent* if $\bigcap_{n=1}^{\infty} I^n = \{0\}$. In that case $\{I^n\}_{n=1}^{\infty}$ are a basis of neighbourhoods of zero of a Hausdorff topology on R called the *I-adic topology* on R (see e.g. [BN]). Using the same notation as in the field case, we will prove results analogous to (3) and (4) that hold for some infinite Galois ring extensions:

1.3. Theorem. *Let $S \supseteq R$ be a Galois ring extension of commutative rings with Galois group G. If S is connected and R is a local ring with a residually nilpotent maximal ideal $\mathfrak{m}$ such that R is compact in the $\mathfrak{m}$-adic topology*, *then there is a left $R[[G]]$-module isomorphism*

$$R[[G]] \cong \overline{S}, \tag{5}$$

where $\overline{S}$ is defined as in the field case above, *and there is a left $R[G]$-module isomorphism*

$$C(G,R) \cong S. \tag{6}$$

Note that neither (5) nor (6) holds if R is replaced by an arbitrary connected ring, since it is well known that normal bases usually do not exist under such general assumptions. However, it is not clear whether they hold for local rings R, which do not satisfy the assumptions of the last theorem.

For some related results concerning normal bases for infinite Galois field extensions see [LP, Theorem 1.3].

2. Inverse limits of compact Hausdorff spaces. We recall the following definitions. A set I is *pre-ordered* if it is equipped with a binary relation $\prec$ that is transitive and reflexive. A set I is *directed* if it is pre-ordered and has the additional property that for any two $\alpha, \beta \in I$ there is $\gamma \in I$ such that $\alpha \prec \gamma$ and $\beta \prec \gamma$. An *inverse system* of topological spaces $(X_\alpha, f_{\alpha\beta})$ relative to a set I consists of a pre-ordered set I, a topological space X_α for each $\alpha \in I$, and a continuous map $f_{\alpha\beta} : X_\beta \to X_\alpha$ for each pair $\alpha, \beta \in I$ with $\alpha \prec \beta$ such that $f_{\alpha\alpha} = \mathrm{id}_{X_\alpha}$ for each $\alpha \in I$ and $f_{\alpha\beta} f_{\beta\gamma} = f_{\alpha\gamma}$ for all $\alpha, \beta, \gamma \in I$ with $\alpha \prec \beta \prec \gamma$. The *inverse limit* of such a system, denoted by $\varprojlim_{\alpha \in I} X_\alpha$, is defined to be the set of all $(x_\alpha)_{\alpha \in I}$ in $\prod_{\alpha \in I} X_\alpha$ such that if $\alpha, \beta \in I$ and $\alpha \prec \beta$, then $f_{\alpha\beta}(x_\beta) = x_\alpha$.

Using [S, Theorem 3], we immediately get the following result about inverse limits of compact Hausdorff spaces, which we need later:

2.1. Proposition. *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of non-empty compact Hausdorff topological spaces relative to a directed set I. If all $f_{\alpha\beta}$ are surjective, then the inverse limit $\varprojlim_{\alpha \in I} X_\alpha$, taken with respect to the maps $f_{\alpha\beta}$, is non-empty.*

3. Topology on group rings. Let R be a ring. We always assume that R has a multiplicative unit 1_R and that ring homomorphisms $R \to S$ map 1_R to 1_S. The multiplicative group of units of R is denoted by R^*. Recall the following definitions: R is *artinian* (*noetherian*) if every non-empty set of left ideals of R contains a minimal (maximal) element with respect to inclusion. The *Jacobson radical* of R, denoted by $J(R)$, is the intersection of the maximal left (or right) ideals of R and R is *semi-local* if $R/J(R)$ is semi-simple artinian. We mention some well-known results about rings, which we need later:

3.1. Proposition. *Let R and S be rings.*

(a) *If R is semi-local and there is a surjective ring homomorphism $R \to S$, then the induced map $R^* \to S^*$ is surjective.*

(b) *If I is an ideal of S contained in $J(S)$, then $s \in S^*$ if and only if $s + I \in (S/I)^*$.*

(c) *If S is finitely generated, as a left R-module, by elements $s \in S$ such that $sS = Ss$, then $J(R)S \subseteq J(S)$.*

Proof. (a) follows directly from [BH, Proposition (2.8)], (b) is [R, Lemma 2.5.5] and (c) is [R, Corollary 2.5.30]. ■

If R is a topological ring and H is a finite group, then we let the group ring, $R[H]$, of R and H be equipped with the topology induced by the topology on R. If I is an ideal of R, then we always let R/I have the quotient topology. A subset of a topological ring is always assumed to have the relative topology and a finite ring is always assumed to have the discrete topology. We gather some elementary facts about topological rings:

3.2. Lemma. *Let R and S be topological rings. Let H_1 and H_2 be finite groups.*

(a) *If R is compact* (*Hausdorff*), *then $R[H_1]$ is compact* (*Hausdorff*).

(b) *If there is a group homomorphism $H_1 \to H_2$ and a continuous ring homomorphism $R \to S$, then the induced ring homomorphism $R[H_1] \to S[H_2]$ is continuous.*

(c) *If there is a continuous ring homomorphism $R \to S$ and S^* is closed*, *then the induced group homomorphism $R^* \to S^*$ is continuous.*

(d) *If I is an ideal of S contained in $J(S)$ such that S/I is a finite ring and the natural map $S \to S/I$ is continuous*, *then S^* is closed.*

Proof. (a) This follows from the fact that a non-empty direct product of compact (Hausdorff) topological spaces is compact (Hausdorff).

(b) This follows directly from the definition of a topological ring.

(c) Denote by f the continuous ring homomorphism $R \to S$. Take a closed subset C of S. Then $(f|_{R^*})^{-1}(C \cap S^*) = R^* \cap f^{-1}(C) \cap f^{-1}(S^*)$, which, since S^* is closed, is a closed subset of R^*.

(d) Denote the natural map $S \to S/I$ by n. By Proposition 3.1(b), $S^* = n^{-1}((S/I)^*)$, which is closed. ■

Combining Proposition 3.1 and Lemma 3.2 gives us the following results, which we need in the sequel:

3.3. Proposition. *Let R be a ring such that $J(R)$ is residually nilpotent and R is compact in the $J(R)$-adic topology. Let H_1 and H_2 be finite groups.*

(a) *$R[H_1]^*$ is a compact and Hausdorff topological space.*

(b) *If there is a surjective group homomorphism $H_1 \to H_2$, then the induced group homomorphism $R[H_1]^* \to R[H_2]^*$ is continuous and surjective.*

Proof. (a) By Lemma 3.2(a), $R[H_1]$ is compact and Hausdorff. The quotient $R/J(R)$, being both compact and discrete, must be finite. Hence $R[H_1]^*$ is, by Proposition 3.1(c) and Lemma 3.2(b),(d) (with $S = R[H_1]$ and $I = J(R)[H_1]$), compact and Hausdorff.

(b) By Proposition 3.1(a) the map $R[H_1]^* \to R[H_2]^*$ is surjective and by Lemma 3.2(b),(c) it is continuous. ■

Note that if R is noetherian, then $J(R)$ is residually nilpotent (see e.g. [NM, Theorem (4.2)]).

4. Galois extensions. In this section, we prove Theorem 1.3.

Let $S \supseteq R$ be a ring extension of commutative rings where S is connected. The extension is called *locally finite separable* if every finite subset of S belongs to a finitely generated separable ring extension of R in S. Let G be the set of R-automorphisms of S. The extension is called *Galois* with Galois group G if it is locally finite separable and $S^G = R$. In that case, a 1-1 dual correspondence between locally finite separable R-sub-algebras of S and closed subgroups of G, in the usual sense of Galois theory, can be developed (see [NT]). The extension is called *finite* if the Galois group is finite and it is called *infinite* otherwise. In the finite case, the trace map $\mathrm{Tr}_{S/R} : S \to R$ is defined by $\mathrm{Tr}_{S/R}(s) = \sum_{\sigma\in G} \sigma(s)$ for all $s \in S$. Due to the lack of appropriate reference, we give a proof of the following well-known facts:

4.1. LEMMA. *Let $R'' \supseteq R'$, $R'' \supseteq R$ and $R' \supseteq R$ be finite Galois ring extensions of commutative rings with R'' connected. Suppose that $R' \supseteq R$ has Galois group H.*

(a) *$R[H]^*$ acts transitively on the set of normal basis generators for $R' \supseteq R$.*

(b) *If x is a normal basis generator for $R'' \supseteq R$, then $\mathrm{Tr}_{R''/R'}(x)$ is a normal basis generator for $R' \supseteq R$.*

Proof. (a) This follows directly from the fact that R' is a free rank one $R[H]$-module generated by any normal basis generator.

(b) Suppose that $R'' \supseteq R$ has Galois group H_1. By the Galois correspondence, $R' = {R''}^{H_2}$ for some normal subgroup $H_2 = \{\gamma_j\}$ of H_1. Let $H = \{\alpha_i\}$. Choose $\{\beta_i\} \subseteq H_1$ such that $\beta_i|_{R'} = \alpha_i$ for all i. Then $H_1 = \{\beta_i\gamma_j\}$. Since $\mathrm{Tr}_{R''/R'}$ is surjective (see e.g. [C]), the H-conjugates of $\mathrm{Tr}_{R''/R'}(x)$ span R' over R. Suppose that $\sum_i r_i\alpha_i(\mathrm{Tr}_{R''/R'}(x)) = 0$ for some $\{r_i\} \subseteq R$. Then $\sum_{i,j} r_i\beta_i\gamma_j(x) = 0$, which, since x is a normal basis generator for R''/R, implies that all $r_i = 0$. ■

Proof of Theorem 1.3. We first prove (5). If we use Proposition 3.3, then for every $N \in U$ we can define a compact Hausdorff topology on $R[G/N]^*$ induced by the $\mathfrak{m}$-adic topology in R. Pick a normal basis generator y_N for S^N/R. For $N' \prec N$ define $\beta_{N'/N} \in R[G/N]^*$ by the relation $\mathrm{Tr}_{N'/N}(y_N) = \beta_{N'/N}(y_{N'})$. This is possible because of Lemma 4.1(a),(b). By Proposition 3.3, the functions $\gamma_{N'/N} : R[G/N]^* \to R[G/N']^*$ defined by $\gamma_{N'/N}(\alpha_N) = \varrho_{N'/N}(\alpha_N)\beta_{N'/N}$ for all $\alpha_N \in R[G/N]^*$ are continuous and surjective. It is easy to check that $(R[G/N]^*, \gamma_{N'/N})$ forms an inverse system of topological spaces relative to U. By Proposition 2.1, the inverse limit $\varprojlim_{N\in U} R[G/N]^*$ taken with respect to the functions $\gamma_{N'/N}$ is non-empty. Pick $(\alpha_N)_{N\in U} \in \varprojlim_{N\in U} R[G/N]^*$. For every $N \in U$, let $x_N = \alpha_N(y_N)$. By Lemma 4.1(a), x_N is a normal basis generator for S^N/R. Then $(x_N)_{N\in U}$ is a free generator of the left $R[[G]]$-module $\overline{S}$.

Now we prove (6). We proceed as in [LH]: From the proof of (5), we obtain $(x_N)_{N\in U}$ in $\prod_{N\in U} S^N$ such that

(i) if $N \in U$, then x_N is a normal basis generator for S^N/R, and
(ii) if $N' \prec N$, then $\mathrm{Tr}_{N'/N}(x_N) = x_{N'}$.

Let $f \in C(G, R)$. Since G is compact and R is equipped with the discrete topology, there is $N \in U$ such that f is constant on τN for every choice of $\tau \in G$. We can therefore define a map $f_N : G/N \to R$ induced by f. We now define $\Phi : C(G, R) \to S$ by $\Phi(f) = \sum_{\sigma \in G/N} f_N(\sigma)\sigma(x_N)$. By (ii), Φ is well defined. It is clear that Φ is R-linear. By (i), Φ is bijective. It is easy to check that Φ also respects the action of G. ∎

REFERENCES

[BH] H. Bass, *Algebraic K-theory*, Benjamin, 1968.

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

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

[J] N. Jacobson, *Basic Algebra I*, Freeman, 1980.

[LS] S. Lang, *Algebra*, Addison-Wesley, 1993.

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

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

[M] A. Mostowski, *Eine Verallgemeinerung eines Satzes von M. Deuring*, Acta Sci. Math. (Szeged) 16 (1955), 197–203.

[NT] T. Nagahara, *A note on Galois theory of commutative rings*, Proc. Amer. Math. Soc. 18 (1967), 334–340.

[NM] M. Nagata, *Local Rings*, Wiley, 1962.

[R] L. Rowen, *Ring Theory*, Vol. I, Academic Press, 1988.

[S] A. H. Stone, *Inverse limits of compact spaces*, Gen. Topology Appl. 10 (1988), 203–211.

Department of Mathematics
Chalmers University of Technology and the University of Göteborg
S-412 96 Göteborg, Sweden
E-mail: lund@math.chalmers.se

Received 26 June 1998;
revised 5 September 1998