ACTA ARITHMETICA
C.1 (2001)

Normal integral bases for infinite abelian extensions

by

PATRIK LUNDSTRÖM (Göteborg)

1. Introduction. Let $K \supseteq \mathbb{Q}$ be a Galois field extension with Galois group G and ring of algebraic integers R. We consider G as a topological group with the Krull topology (see e.g. [L93, p. 329]).

Suppose that $K \supseteq \mathbb{Q}$ is a finite extension. The normal basis theorem asserts that there is $x \in K$ such that $B := \{\sigma(x)\}_{\sigma \in G}$ form a basis for K as a vector space over $\mathbb{Q}$. In fact, such a basis exists for general finite Galois field extensions (see e.g. [J80, p. 283]). B is called a *normal basis* and x is called a *normal basis generator*. If B is a $\mathbb{Z}$-basis for R, then B is called a *normal integral basis* and x is called a *normal integral basis generator*. Normal integral bases do not always exist. In fact, for abelian extensions, Leopoldt [Leo59] proved the following result:

1.1. THEOREM. *Suppose that $K \supseteq \mathbb{Q}$ is a finite Galois field extension with abelian Galois group. Then K has a normal integral basis if and only if K is contained in the nth cyclotomic number field*, K_n, *for some positive square-free integer n.*

For infinite extensions Theorem 1.1 makes no sense. However, if we let $(G, \mathbb{Z})$ denote the set of functions $f : G \to \mathbb{Z}$ and we let G operate on $(G, \mathbb{Z})$ by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$ for $\sigma, \tau \in G$, then Theorem 1.1 can be formulated by saying that there is a left $\mathbb{Z}$-module isomorphism $F : (G, \mathbb{Z}) \to R$ that respects the action of G.

Namely, if B is a $\mathbb{Z}$-basis for R, then we can define F by

$$F(f) = \sum_{\sigma \in G} f(\sigma)\sigma(x).$$

Conversely, if $F : (G, \mathbb{Z}) \to R$ is an isomorphism as above, and $h : G \to \mathbb{Z}$ is defined by $h(1) = 1$ and $h(\sigma) = 0$, $\sigma \neq 1$, then $x := F(h)$ is a normal integral basis generator for K. In this paper we prove, using an idea introduced by Lenstra in [Le85] for the case of normal bases for infinite Galois field

2000 *Mathematics Subject Classification*: 11R04, 11R18, 11R33.

extensions, that this version of Theorem 1.1 is valid for infinite extensions, provided we only consider continuous functions $G \to \mathbb{Z}$:

1.2. THEOREM. *Suppose that $K \supseteq \mathbb{Q}$ is a Galois field extension with abelian Galois group G and ring of algebraic integers R. Denote by $C(G, \mathbb{Z})$ the $\mathbb{Z}$-module of all continuous functions $f : G \to \mathbb{Z}$, where $\mathbb{Z}$ is equipped with the discrete topology. Let G operate on $C(G, \mathbb{Z})$ by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$ for $\sigma, \tau \in G$. Then there is an isomorphism of $\mathbb{Z}$-modules $C(G, \mathbb{Z}) \to R$ that respects the action of G if and only if for every finite extension $K' \supseteq \mathbb{Q}$ such that $K \supseteq K'$ there is a positive square-free integer n such that $K_n \supseteq K'$.*

For some related results concerning normal bases for infinite Galois extensions see [Lu98] and [Lu99].

2. Cofinal countable inverse limits. We recall the following definitions. A set I is *preordered* if it is equipped with a binary relation $\prec$ that is transitive and reflexive. A set I is *directed* if it is preordered 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 sets $(E_\alpha, f_{\alpha\beta})$ relative to a set I consists of a preordered set I, a set E_α for each $\alpha \in I$, and a map $f_{\alpha\beta} : E_\beta \to E_\alpha$ for each pair $\alpha, \beta \in I$ with $\alpha \prec \beta$, such that $f_{\alpha\alpha} = \mathrm{id}_{E_\alpha}$ 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 $\varprojlim_{\alpha \in I} E_\alpha$, is defined to be the set of all $(x_\alpha)_{\alpha \in I}$ in $\prod_{\alpha \in I} E_\alpha$ such that if $\alpha, \beta \in I$ and $\alpha \prec \beta$, then $f_{\alpha\beta}(x_\beta) = x_\alpha$. Recall that a subset J of I is called *cofinal* if for every $\alpha \in I$ there is $\beta \in J$ such that $\alpha \prec \beta$. We use the following result in Section 3:

2.1. PROPOSITION. *Let $(E_\alpha, f_{\alpha\beta})$ be an inverse system of sets relative to a directed set I, which has a countable cofinal subset J. Suppose furthermore that all $f_{\alpha\beta}$, $\alpha, \beta \in J$, are surjective. If all E_α are non-empty, then the inverse limit $\varprojlim_{\alpha \in I} E_\alpha$, taken with respect to the maps $f_{\alpha\beta}$, $\alpha, \beta \in I$, is non-empty.*

Proof. Use the ideas in [B68, III.7.4, Prop. 5]. ■

3. Number fields. In this section, we prove Theorem 1.2. We need three well known results (see Lemmas 3.1–3.3). The multiplicative group of units of a ring S is denoted by S^*.

3.1. LEMMA. *Let $L' \supseteq L$ be finite Galois field extensions of $\mathbb{Q}$. Let* Tr *denote the trace map from L' to L. Suppose that $L \supseteq \mathbb{Q}$ has Galois group H.*

(a) *If L has a normal integral basis, then $\mathbb{Z}[H]^*$ acts transitively on the set of normal integral basis generators for L.*

(b) *If x is a normal integral basis generator for L', then* $\mathrm{Tr}(x)$ *is a normal integral basis generator for L.*

Proof. (a) follows directly from the definition of a normal integral basis generator and (b) is [N90, Theorem 4.10]. ∎

Let $\{p_1, p_2, \ldots\}$ denote the set of all odd primes. For each p_i, let ε_{p_i} denote a primitive p_ith root of unity. For all positive integers m, n such that $m \geq n$, let

$$r_n^m : \mathrm{Gal}(K_{p_1 \ldots p_m}/\mathbb{Q}) \to \mathrm{Gal}(K_{p_1 \ldots p_n}/\mathbb{Q})$$

be the restriction map and let

$$p_n^m : \mathbb{Z}_{p_1 - 1} \times \ldots \times \mathbb{Z}_{p_m - 1} \to \mathbb{Z}_{p_1 - 1} \times \ldots \times \mathbb{Z}_{p_n - 1}$$

be the natural projection. For each positive integer n, let

$$\theta_n : \mathbb{Z}_{p_1 - 1} \times \ldots \times \mathbb{Z}_{p_n - 1} \to \mathrm{Gal}(K_{p_1 \ldots p_n}/\mathbb{Q})$$

be the group isomorphism given by $\theta_n(a_1, \ldots, a_n) = \sigma_{a_1, \ldots, a_n}$, where

$$\sigma_{a_1, \ldots, a_n}(\varepsilon_i) = \varepsilon_i^{a_i}, \qquad i = 1, \ldots, n.$$

With the above notations, we immediately get:

3.2. Lemma. *If m and n are positive integers such that $m \geq n$, then the following diagram is commutative*:

$$\begin{array}{ccc} \mathbb{Z}_{p_1 - 1} \times \ldots \times \mathbb{Z}_{p_m - 1} & \xrightarrow{p_n^m} & \mathbb{Z}_{p_1 - 1} \times \ldots \times \mathbb{Z}_{p_n - 1} \\ \Big\downarrow{\scriptstyle \theta_m} & & \Big\downarrow{\scriptstyle \theta_n} \\ \mathrm{Gal}(K_{p_1 \ldots p_m}/\mathbb{Q}) & \xrightarrow{r_n^m} & \mathrm{Gal}(K_{p_1 \ldots p_n}/\mathbb{Q}). \end{array}$$

We also need the following:

3.3. Lemma. *If G_1 and G_2 are groups, then the map*

$$p : \mathbb{Z}[G_1 \times G_2]^* \to \mathbb{Z}[G_2]^*,$$

induced by the projection $G_1 \times G_2 \to G_2$, is surjective.

Proof. The inclusion $p(\mathbb{Z}[G_1 \times G_2]^*) \subseteq \mathbb{Z}[G_2]^*$ is trivial. For the reverse inclusion, let $i : \mathbb{Z}[G_2]^* \to \mathbb{Z}[G_1 \times G_2]^*$ be the map induced by the canonical injection $G_2 \to G_1 \times G_2$. Then $\mathbb{Z}[G_2]^* = p(i(\mathbb{Z}[G_2]^*)) \subseteq p(\mathbb{Z}[G_1 \times G_2]^*)$. ∎

Proof of Theorem 1.2. Let U denote the set of open subgroups of G. If $N \in U$ let

$$K^N = \{k \in K \mid \sigma(k) = k \text{ for all } \sigma \in N\}.$$

We write $N' \prec N$ when $N, N' \in U$ and $N \subseteq N'$.

Assume that there is an isomorphism of $\mathbb{Z}$-modules $F : C(G, \mathbb{Z}) \to R$ that respects the action of G. Pick a finite field extension $K^N \supseteq \mathbb{Q}$, where $N \in U$. By Theorem 1.1, it is enough to show that K^N has a normal integral basis. Let $C_N(G, \mathbb{Z}) = \{f \in C(G, \mathbb{Z}) \mid \sigma f = f \text{ for all } \sigma \in N\}$. Then

$F(C_N(G,\mathbb{Z})) = R^N$. If we define $h \in C_N(G,\mathbb{Z})$ by $h(\sigma) = 1$ if $\sigma \in N$ and $h(\sigma) = 0$ if $\sigma \notin N$, then $F(h)$ is a normal integral basis generator for K^N.

Now suppose that if $K' \supseteq \mathbb{Q}$ is a finite extension such that $K \supseteq K'$, then there is a positive integer n such that $K_n \supseteq K'$. We can assume that $K \supseteq K_n$ for all positive square-free integers n. By Theorem 1.1, for every $N \in U$ there is a normal integral basis generator y_N for K^N. If $N' \prec N$, then let $\mathrm{Tr}_{N'/N} : K^N \to K^{N'}$ denote the trace function and define $\beta_{N'/N} \in \mathbb{Z}[G/N']^*$ by the relation $\mathrm{Tr}_{N'/N}(y_N) = \beta_{N'/N}(y_{N'})$. This is possible because of Lemma 3.1(a), (b). If $N' \prec N$, then let $\varrho_{N'/N} : \mathbb{Z}[G/N] \to \mathbb{Z}[G/N']$ denote the natural map and define the function $\gamma_{N'/N} : \mathbb{Z}[G/N]^* \to \mathbb{Z}[G/N']^*$ by $\gamma_{N'/N}(\alpha_N) = \varrho_{N'/N}(\alpha_N)\beta_{N'/N}$ for all $\alpha_N \in \mathbb{Z}[G/N]^*$. It is easy to check that $(\mathbb{Z}[G/N]^*, \gamma_{N'/N})$ form an inverse system of sets relative to U. Let

$$V = \{N \in U \mid K^N = K_{p_1 \ldots p_n} \text{ for some } n \geq 1\}.$$

By Lemmas 3.2 and 3.3, the functions $\gamma_{N'/N}$, $N, N' \in V$, are surjective. Since V is a countable cofinal subset of U, we see, by Proposition 2.1, that the inverse limit $\Gamma := \varprojlim_{N \in U} \mathbb{Z}[G/N]^*$ taken with respect to the functions $\gamma_{N'/N}$, is non-empty. Now choose $(\alpha_N)_{N \in U} \in \Gamma$. For every $N \in U$, let $x_N = \alpha_N(y_N)$. Then, by Lemma 3.1(a) and the above construction, we get:

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

Let $f \in C(G,\mathbb{Z})$. Since G is compact and $\mathbb{Z}$ 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 $f_N : G/N \to \mathbb{Z}$ induced by f. We now define $F : C(G,\mathbb{Z}) \to R$ by

$$F(f) = \sum_{\sigma \in G/N} f_N(\sigma)\sigma(x_N).$$

By (ii), F is well defined. It is clear that F is $\mathbb{Z}$-linear. By (i), F is bijective. It is easy to check that F also respects the action of G. ■

References

[B68] N. Bourbaki, *Set Theory*, Hermann, 1968.
[J80] N. Jacobson, *Basic Algebra I*, Freeman, 1980.
[L93] S. Lang, *Algebra*, Addison-Wesley, 1993.
[Le85] H. W. Lenstra, Jr., *A normal basis theorem for infinite Galois extensions*, Indag. Math. 47 (1985), 221–228.
[Leo59] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959), 119–149.
[Lu98] P. Lundström, *Self-dual normal bases for infinite Galois field extensions*, Comm. Algebra 26 (1998), 4331–4341.

[Lu99] P. Lundström, *Normal bases for infinite Galois ring extensions*, Colloq. Math. 79 (1999), 235–240.

[N90] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.

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

Received on 3.7.2000 (3846)