A normal basis theorem for infinite Galois extensions

by H.W. Lenstra, Jr.

Mathematisch Instituut, University of Amsterdam, Roetersstraat 15, 1018 WB Amsterdam, the Netherlands

Communicated at the meeting of November 26, 1984

ABSTRACT

The normal basis theorem from Galois theory is generalized to infinite Galois extensions.

INTRODUCTION

Let K be a field, L a Galois extension of K, and G the Galois group of L over K. We consider G as a topological group with the topology defined by Krull [4; 1, Chapitre V, Appendice II].

The *normal basis theorem* asserts that if L is finite over K there exists $x \in L$ such that the elements $\sigma(x)$, $\sigma \in G$, form a basis for L as a vector space over K, see [5; 3]. If L is infinite over K then no such basis exists, since for every $x \in L$ the set $\{\sigma(x) : \sigma \in G\}$ is finite. Hence if we wish to generalize the normal basis theorem to infinite Galois extensions we must look for an alternative formulation.

Let L be finite over K, and write (G, K) for the K-vector space of all functions $f : G \to K$. We let G operate on (G, K) by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$, for $\sigma, \tau \in G$. We can now reformulate the normal basis theorem by saying that there is an isomorphism $\varphi : (G, K) \to L$ of K-vector spaces that respects the action of G. Namely, if $(\sigma(x))_{\sigma \in G}$ is a basis of L over K, then we can define φ by $\varphi(f) = \sum_{\sigma \in G} f(\sigma)\sigma(x)$. Conversely, if $\varphi : (G, K) \to L$ is an isomorphism as above, and $h : G \to K$ is defined by $h(1) = 1$, $h(\tau) = 0$ $(\tau \in G, \tau \neq 1)$, then $x = \varphi(h)$ has the property that $(\sigma(x))_{\sigma \in G}$ is a basis of L over K.

It turns out that this version of the normal basis theorem is valid for *infinite*

Galois extensions as well, provided that we only consider *continuous* functions $G \to K$.

THEOREM 1. *Let $K \subset L$ be a Galois extension of fields, with group G, and denote by $C(G,K)$ the K-vector space of all continuous functions $f: G \to K$; here G is provided with the Krull topology and K with the discrete topology. Let G operate on $C(G,K)$ by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$, for $\sigma, \tau \in G$. Then there exists an isomorphism $C(G,K) \to L$ of K-vector spaces that respects the action of G.*

The proof of this theorem is given in Section 3 of this paper.

We can also express the normal basis theorem by saying that, for L finite over K, the additive group of L is free on one generator as a left module over the group ring $K[G]$. This assertion can be generalized to the infinite case as follows.

Denote by U the set of open normal subgroups of G. We order U by letting $N' \leq N$ if and only if $N \subset N'$. For $N, N' \in U$, $N \subset N'$, let the ring homomorphism $\varrho_{N'/N}: K[G/N] \to K[G/N']$ be induced by the natural group homomorphism $G/N \to G/N'$. We write $K[[G]] = \varprojlim_{N \in U} K[G/N]$, the projective limit being taken with respect to the maps $\varrho_{N'/N}$ (see Section 1 for our conventions about projective limits). Observe that $K[[G]]$ contains the group ring $K[G]$ in a natural way, and is equal to it if G is finite.

For $N \in U$, let the subfield L^N of L be defined by $L^N = \{y \in L : \sigma(y) = y$ for all $\sigma \in N\}$; this is a finite Galois extension of K with group G/N. For $N, N' \in U$, $N \subset N'$, the *trace* map $\mathrm{Tr}_{N'/N}: L^N \to L^{N'}$ is defined by $\mathrm{Tr}_{N'/N}(y) = \sum_{\sigma \in N'/N} \sigma(y)$. The projective limit $\varprojlim_{N \in U} L^N$, taken with respect to the maps $\mathrm{Tr}_{N'/N}$, is in a natural way a left module over $K[[G]]$.

THEOREM 2. *For any Galois extension of fields $K \subset L$ with group G, the left $K[[G]]$-module $\varprojlim_{N \in U} L^N$ is free on one generator.*

The proof of this theorem is given in Section 3 of this paper.

1. PROJECTIVE LIMITS

A *preordered* set is a set I with a binary relation $\leq$ on I that is transitive and reflexive. A *directed* set is a preordered set I with the property that for any two $\alpha, \beta \in I$ there exists $\gamma \in I$ with $\alpha \leq \gamma$ and $\beta \leq \gamma$. A *projective system* consists of a directed 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 $\alpha \leq \beta$, such that $f_{\alpha\alpha}$ equals the identity on E_α for each $\alpha \in I$, and $f_{\alpha\beta} f_{\beta\gamma} = f_{\alpha\gamma}$ for all $\alpha, \beta, \gamma \in I$ with $\alpha \leq \beta$ and $\beta \leq \gamma$. The *projective limit* of such a system, denoted by $\varprojlim E_\alpha$ or $\varprojlim_{\alpha \in I} E_\alpha$, is defined by

$$\varprojlim E_\alpha = \{(x_\alpha)_{\alpha \in I} \in \prod_{\alpha \in I} E_\alpha : f_{\alpha\beta}(x_\beta) = x_\alpha \text{ for all } \alpha, \beta \in I \text{ with } \alpha \leq \beta\}.$$

The projective limit may be empty, even if all E_α are non-empty and all $f_{\alpha\beta}$ are surjective [6]. We recall from Bourbaki [2, III.7.4] sufficient conditions for a projective system to have a non-empty projective limit.

Let I, $(E_\alpha)_{\alpha\in I}$, $(f_{\alpha\beta})_{\alpha,\beta\in I,\alpha\le\beta}$ be a projective system in which all E_α are *non-empty*. We suppose that for each $\alpha\in I$ we are given a collection $\mathscr{S}_\alpha$ of subsets of E_α, such that the following four conditions are satisfied.

(1.1) If $\alpha\in I$ and $\mathscr{F}\subset\mathscr{S}_\alpha$ then $\bigcap_{M\in\mathscr{F}} M\in\mathscr{S}_\alpha$.

In particular, taking $\mathscr{F}=\emptyset$, we see that $E_\alpha\in\mathscr{S}_\alpha$.

(1.2) If $\alpha\in I$, and $\mathscr{F}\subset\mathscr{S}_\alpha$ is such that $\bigcap_{M\in\mathscr{F}'} M\neq\emptyset$ for all finite subsets $\mathscr{F}'\subset\mathscr{F}$, then $\bigcap_{M\in\mathscr{F}} M\neq\emptyset$.

(1.3) If $\alpha,\beta\in I$, $\alpha\le\beta$ and $x\in E_\alpha$, then $f_{\alpha\beta}^{-1}x\in\mathscr{S}_\beta$.

(1.4) If $\alpha,\beta\in I$, $\alpha\le\beta$ and $M\in\mathscr{S}_\beta$, then $f_{\alpha\beta}[M]\in\mathscr{S}_\alpha$.

In the following proposition we write $E=\varprojlim E_\alpha$. For $\alpha\in I$, we denote the natural map $E\to E_\alpha$ by f_α, and we put $E'_\alpha=\bigcap_{\beta\in I,\alpha\le\beta} f_{\alpha\beta}[E_\beta]$; so $E'_\alpha\subset E_\alpha$, and $E'_\alpha=E_\alpha$ if all $f_{\alpha\beta}$ are surjective.

(1.5) PROPOSITION. *With the above hypotheses and notation, we have:*
(a) $E\neq\emptyset$;
(b) $f_\alpha[E]=E'_\alpha$ *for each* $\alpha\in I$;
(c) *if* $J\subset I$ *is directed with respect to the restriction of* $\le$ *to* J, *then the image of the natural map* $\varprojlim_{\alpha\in I} E_\alpha\to\varprojlim_{\alpha\in J} E_\alpha$ *is* $\varprojlim_{\alpha\in J} E'_\alpha$.

PROOF. We need a few facts from the proof of [2, III.7.4, Théorème 1]. Let $\sum$ denote the set of all families $(A_\alpha)_{\alpha\in I}$ for which

$$A_\alpha\neq\emptyset \text{ and } A_\alpha\in\mathscr{S}_\alpha, \text{ for all } \alpha\in I,$$

$$f_{\alpha\beta}[A_\beta]\subset A_\alpha \text{ for all } \alpha,\beta\in I,\ \alpha\le\beta.$$

Let $(A_\alpha)_{\alpha\in I}\le(A'_\alpha)_{\alpha\in I}$ if and only if $A'_\alpha\subset A_\alpha$ for each $\alpha\in I$. This makes $\sum$ into a partially ordered set. In [2, *loc. cit.*] it is shown that $\sum$ satisfies the conditions of Zorn's lemma, and that the map $E\to\sum$ sending $(x_\alpha)_{\alpha\in I}$ to $(\{x_\alpha\})_{\alpha\in I}$ establishes a bijection between E and the set of maximal elements of $\sum$.

We use this to prove (c). Let $J\subset I$ be directed. It is trivial that the image of E in $\varprojlim_{\alpha\in J} E_\alpha$ is contained in $\varprojlim_{\alpha\in J} E'_\alpha$. To prove the other inclusion, let $(x_\alpha)_{\alpha\in J}\in\varprojlim_{\alpha\in J} E'_\alpha$. For $\beta\in I$, let $A_\beta=\bigcap_{\alpha\in J,\alpha\le\beta} f_{\alpha\beta}^{-1}x_\alpha$. We claim that $A_\beta\neq\emptyset$. To prove this, it suffices by (1.3) and (1.2) to show that $\bigcap_{\alpha\in K,\alpha\le\beta} f_{\alpha\beta}^{-1}x_\alpha\neq\emptyset$ for every *finite* subset $K\subset J$. Let K be such. We may assume that $K\neq\emptyset$. Since J is directed, we can choose $\gamma\in J$ such that $\alpha\le\gamma$ for all $\alpha\in K$, and since I is directed we can choose $\delta\in I$ such that $\beta\le\delta$, $\gamma\le\delta$. We have $x_\gamma\in E'_\gamma\subset f_{\gamma\delta}[E_\delta]$, so $x_\gamma=f_{\gamma\delta}(z)$ for some $z\in E_\delta$, and it is now readily verified that $f_{\beta\delta}(z)\in\in\bigcap_{\alpha\in K,\alpha\le\beta} f_{\alpha\beta}^{-1}x_\alpha$. This proves that $A_\beta\neq\emptyset$. It follows that $(A_\beta)_{\beta\in I}\in\sum$. The results about $\sum$ quoted above imply that $\sum$ has a maximal element $(\{y_\beta\})_{\beta\in I}$ with $(\{y_\beta\})_{\beta\in I}\ge(A_\beta)_{\beta\in I}$. Then $y_\beta\in A_\beta$, and since $A_\alpha=\{x_\alpha\}$ for $\alpha\in J$ this implies that $y_\alpha=x_\alpha$ for all $\alpha\in J$. Hence $(y_\beta)_{\beta\in I}\in E$ maps to $(x_\alpha)_{\alpha\in J}\in\varprojlim_{\alpha\in J} E_\alpha$. This proves (c).

Assertions (b) and (a), which form [2, III.7.4, Théorème 1], follow from (c) by putting $J=\{\alpha\}$ and $J=\emptyset$, respectively. This proves (1.5).

2. ARTIN RINGS

Rings are supposed to have unit elements, and ring homomorphisms are supposed to preserve these. The group of units of a ring R is denoted by R^*. A *projective system of rings* is a projective system I, (R_α), $(g_{\alpha\beta})$ in which each R_α carries the structure of a ring and each $g_{\alpha\beta}$ is a ring homomorphism. The projective limit of such a system carries a natural ring structure.

The following proposition is not needed in the sequel, but its proof motivates the approach taken later.

(2.1) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α satisfies the descending chain condition on two-sided ideals and each $g_{\alpha\beta}$ is surjective. Put $R=\varprojlim R_\alpha$. Then the natural map $R\to R_\alpha$ is surjective for every $\alpha\in I$.*

PROOF. We apply (1.5) with $E_\alpha=R_\alpha$, $f_{\alpha\beta}=g_{\alpha\beta}$ and

$$\mathscr{S}_\alpha=\{\emptyset\}\cup\{x+\mathfrak{a}\colon x\in R_\alpha,\ \mathfrak{a}\subset R_\alpha \text{ is a two-sided ideal}\}.$$

It is clear that $E_\alpha\neq\emptyset$ and that (1.1), (1.3) and (1.4) are satisfied. To prove (1.2), we note that the descending chain condition on two-sided ideals of R_α implies the existence of a minimal element among all finite intersections of sets $M\in\mathscr{F}$; this minimal element must then be $\bigcap_{M\in\mathscr{F}} M$.

Since the $g_{\alpha\beta}$ are surjective we have $E'_\alpha=E_\alpha=R_\alpha$ in (1.5), so (2.1) follows from (1.5)(b). This proves (2.1).

An *Artin ring* is a ring that satisfies the descending chain condition on left ideals.

(2.2) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α is an Artin ring and each $g_{\alpha\beta}$ is surjective. Put $R=\varprojlim R_\alpha$. Then the natural map $R^*\to R_\alpha^*$ is surjective for each $\alpha\in I$.*

The properties of Artin rings needed in the proof are listed in Lemma (2.4). This lemma can easily be derived from the structure of semisimple Artin rings and properties of the Jacobson radical. We give a direct proof, starting from the following well-known lemma. By a *module* we mean a left module on which the unit element acts as the identity, and a module is called *simple* if it is non-zero and has no submodules except itself and $\{0\}$.

(2.3) LEMMA. *Let R be a ring, $(M_v)_{v\in V}$ a collection of simple R-modules, $M=\oplus_{v\in V} M_v$, and $N\subset M$ a submodule. Then there is a subset $W\subset V$ such that $M/N\cong\oplus_{v\in W} M_v$ and $N\cong\oplus_{v\in V-W} M_v$.*

PROOF. With Zorn's lemma, choose $W \subset V$ maximal among all subsets $W' \subset V$ for which the sum $N + \oplus_{w \in W'} M_w$ is direct. Then for $v \in V$ the sum $(N + \oplus_{w \in W} M_w) + M_v$ is not direct, by the maximality of W, so $(N + \oplus_{w \in W} M_w) \cap M_v \neq 0$; but M_v is simple, so $(N + \oplus_{w \in W} M_w) \cap M_v = M_v$, and $M_v \subset N + \oplus_{w \in W} M_w$. This implies that $M = N + \oplus_{w \in W} M_w$, and the lemma follows easily. This proves (2.3).

(2.4) LEMMA. *Let R be an Artin ring, and $x \in R$. Then we have:*
(a) *x is a unit if and only if it is a left unit, and if and only if it is a right unit;*
(b) *R has only finitely many maximal two-sided ideals.*
(c) *$x \in R^*$ if and only if $(x \bmod \mathfrak{m}) \in (R/\mathfrak{m})^*$ for every maximal two-sided ideal $\mathfrak{m}$ of R.*

PROOF. (a) It suffices to show that $yz = 1$ implies $zy = 1$. The descending chain condition implies that $Ry^n = Ry^{n+1}$ for some $n \geq 0$, so $y^n = wy^{n+1}$ for some $w \in R$. Then $1 = y^n z^n = wy^{n+1} z^n = wy$ and $w = wyz = z$.

(b) Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ be distinct maximal two-sided ideals. Then $\mathfrak{m}_i + \mathfrak{m}_j = R$ for $i \neq j$, so the map $R \to \prod_{i=1}^k R/\mathfrak{m}_i$ is surjective with kernel $\bigcap_{i=1}^k \mathfrak{m}_i$. This proves that $\bigcap_{i=1}^k \mathfrak{m}_i$ is properly contained in $\bigcap_{i=1}^{k-1} \mathfrak{m}_i$. The descending chain condition now implies a bound on k.

(c) "Only if" is clear. To prove "if", suppose that $x \notin R^*$. Then $Rx \neq R$ by (a), so $Rx \subset L$ for some maximal left ideal $L \subset R$. Let $\mathfrak{m} = \operatorname{Ann}(R/L) \subset R$ be the annihilator of the simple R-module R/L. Then $\mathfrak{m} \subset L$ so $(R/\mathfrak{m})(x \bmod \mathfrak{m}) \subset$ $\subset L/\mathfrak{m} \neq R/\mathfrak{m}$ and consequently $(x \bmod \mathfrak{m}) \notin (R/\mathfrak{m})^*$. Hence to prove (c) it suffices to show that $\mathfrak{m}$ is maximal as a two-sided ideal. We have $\mathfrak{m} = \bigcap_{y \in R-L} L_y$ where $L_y = \{r \in R: ry \in L\}$; considering the map $R \to R/L$ sending 1 to y one finds that $R/L_y \cong R/L$ as R-modules. By the descending chain condition we have $\mathfrak{m} = \bigcap_{y \in T} L_y$ for some *finite* set $T \subset R - L$. Then $R/\mathfrak{m}$ is a submodule of $\prod_{y \in T} R/L_y \cong (R/L)^{\#T}$, so $R/\mathfrak{m} \cong (R/L)^m$ for some $m > 0$, by (2.3). Let now $\mathfrak{n}$ be a two-sided ideal of R containing $\mathfrak{m}$. Then $R/\mathfrak{n} \cong (R/L)^n$ for some $n \geq 0$, by (2.3). If $n = 0$ then $\mathfrak{n} = R$, and if $n > 0$ then $\mathfrak{n} = \operatorname{Ann}(R/\mathfrak{n}) =$ $= \operatorname{Ann}(R/L) = \mathfrak{m}$.

This proves (2.4).

(2.5) LEMMA. *Let $g: R_0 \to R_1$ be a surjective ring homomorphism from an Artin ring R_0 to a ring R_1, and let $\mathfrak{a} \subset R_0$ be a two-sided ideal. Then $g[(1 + \mathfrak{a}) \cap R_0^*] = (1 + g[\mathfrak{a}]) \cap R_1^*$.*

PROOF. The inclusion $\subset$ is obvious. To prove $\supset$ we first suppose that $\mathfrak{a} \subset \mathfrak{m}$ for every maximal two-sided ideal $\mathfrak{m}$ of R_0 that does not contain $\ker g$. Let $x = 1 + g(y) \in (1 + g[\mathfrak{a}]) \cap R_1^*$, with $y \in \mathfrak{a}$. Using (2.4)(c) we prove that $1 + y \in R_0^*$. Let $\mathfrak{m}$ be a maximal two-sided ideal of R_0. If $\ker g \subset \mathfrak{m}$ then the natural map $R_0 \to R_0/\mathfrak{m}$ factors via g, so $x = g(1 + y) \in R_1^*$ implies that $(1 + y \bmod \mathfrak{m}) \in$ $\in (R_0/\mathfrak{m})^*$. If $\ker g \not\subset \mathfrak{m}$ then $y \in \mathfrak{a} \subset \mathfrak{m}$ by hypothesis, so $(1 + y \bmod \mathfrak{m}) =$ $= (1 \bmod \mathfrak{m}) \in (R_0/\mathfrak{m})^*$. This proves that $1 + y \in R_0^*$, so $x = g(1 + y) \in$ $\in g[(1 + \mathfrak{a}) \cap R_0^*]$.

In the general case, let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ be the maximal two-sided ideals of R_0 that do not contain $\ker g$. Then $\mathfrak{m}_i + \ker g = R_0$ for each i, so some $z_i \in \mathfrak{m}_i$ satisfies $z_i \equiv 1 \bmod \ker g$. Then $z = z_1 z_2 \ldots z_k$ satisfies $z \in \mathfrak{m}_1 \mathfrak{m}_2 \ldots \mathfrak{m}_k$ and $g(z) = 1$. Therefore $g[\mathfrak{a}] = g[\mathfrak{b}]$ for $\mathfrak{b} = \mathfrak{a}\mathfrak{m}_1 \mathfrak{m}_2 \ldots \mathfrak{m}_k$. Applying the previous case to $\mathfrak{b}$ we see that $(1 + g[\mathfrak{a}]) \cap R_1^* = g[(1 + \mathfrak{b}) \cap R_0^*] \subset g[(1 + \mathfrak{a}) \cap R_0^*]$.

This proves (2.5).

(2.6) LEMMA. *Let $g: R_0 \to R_1$ be a surjective ring homomorphism from an Artin ring R_0 to a ring R_1. Then the map $R_0^* \to R_1^*$ induced by g is surjective.*

PROOF. Put $\mathfrak{a} = R_0$ in (2.5). This proves (2.6).

PROOF OF (2.2). We apply (1.5) with $E_\alpha = R_\alpha^*$ and $f_{\alpha\beta}: R_\beta^* \to R_\alpha^*$ the map induced by $g_{\alpha\beta}$. For $\mathscr{S}_\alpha$ we take

$$\mathscr{S}_\alpha = \{\emptyset\} \cup \{(x + \mathfrak{a}) \cap R_\alpha^* : x \in R_\alpha^*, \ \mathfrak{a} \subset R_\alpha \text{ is a two-sided ideal}\}.$$

It is clear that $E_\alpha \neq \emptyset$. We check conditions (1.1)–(1.4).

(1.1) If $\bigcap_{M \in \mathscr{F}} M \neq \emptyset$ then with $x \in \bigcap_{M \in \mathscr{F}} M$ each $M \in \mathscr{F}$ has the form $(x + \mathfrak{a}_M) \cap R_\alpha^*$ for some two-sided ideal $\mathfrak{a}_M \subset R_\alpha$, and then $\bigcap_{M \in \mathscr{F}} M = (x + \mathfrak{a}) \cap R_\alpha^*$ where $\mathfrak{a} = \bigcap_{M \in \mathscr{F}} \mathfrak{a}_M$.

(1.2) Using (1.1) we may assume that $\mathscr{F}$ is closed under taking finite intersections. For $M \in \mathscr{F}$, let $\mathfrak{b}_M$ be the two-sided ideal of R_α generated by $\{y - z : y, z \in M\}$; then $M = (x + \mathfrak{b}_M) \cap R_\alpha^*$ for each $x \in M$. Choose $M' \in \mathscr{F}$ such that $\mathfrak{b}_{M'}$ is minimal among all ideals $\mathfrak{b}_M$, $M \in \mathscr{F}$. It then follows that $M' = \bigcap_{M \in \mathscr{F}} M$.

(1.3) This is clear.

(1.4) If $M = (x + \mathfrak{a}) \cap R_\beta^* \in \mathscr{S}_\beta$ then by (2.5) we have

$$f_{\alpha\beta}[M] = f_{\alpha\beta}[x((1 + \mathfrak{a}) \cap R_\beta^*)] = f_{\alpha\beta}(x) \cdot ((1 + g_{\alpha\beta}[\mathfrak{a}]) \cap R_\alpha^*) =$$
$$= (f_{\alpha\beta}(x) + g_{\alpha\beta}[\mathfrak{a}]) \cap R_\alpha^* \in \mathscr{S}_\alpha.$$

From (2.6) we see that the maps $f_{\alpha\beta}$ are surjective, so $E'_\alpha = R_\alpha^*$ in (1.5). The proposition now follows from (1.5)(b).

This proves (2.2).

(2.7) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α is an Artin ring and each $g_{\alpha\beta}$ is surjective. Let further I, (M_α), $(h_{\alpha\beta})$ be a projective system in which each M_α is a free R_α-module on one generator and each $h_{\alpha\beta}$ is a surjective R_β-module homomorphism; here M_α is considered as an R_β-module via the map $R_\beta \to R_\alpha$. Put $R = \varprojlim R_\alpha$ and $M = \varprojlim M_\alpha$. Then M is a free R-module on one generator, which can be chosen of the form $(x_\alpha)_{\alpha \in I}$, where each x_α generates M_α as an R_α-module.*

PROOF. Without loss of generality we may assume that $M_\alpha = R_\alpha$, for each $\alpha \in I$. By (2.4)(a) we then have $h_{\alpha\beta}(1) \in R_\alpha^*$, and $h_{\alpha\beta}(x) = g_{\alpha\beta}(x) h_{\alpha\beta}(1)$ for all

$x \in R_\beta$. Let $f_{\alpha\beta}: R_\beta^* \to R_\alpha^*$ be the map induced by $h_{\alpha\beta}$; then the statement of (2.7) is equivalent to the assertion that $\varprojlim R_\alpha^* \neq \emptyset$, the projective limit being taken with respect to the maps $f_{\alpha\beta}$.

To prove that $\varprojlim R_\alpha^* \neq \emptyset$ we apply (1.5) with the same E_α and $\mathscr{S}_\alpha$ as in the proof of (2.2); but $f_{\alpha\beta}$ differs from the map $f_{\alpha\beta}$ used for (2.2) by a unit factor $h_{\alpha\beta}(1)$ on the right. Since $\mathscr{S}_\alpha$ is transformed into itself by multiplication by units conditions (1.1)–(1.4) are still satisfied. The proposition now follows from (1.5)(a).

This proves (2.7).

3. GALOIS EXTENSIONS

In this section we use the notation from the Introduction.

PROOF OF THEOREM 2. We apply (2.7) to the projective system U, $(K[G/N])$, $(\varrho_{N'/N})$ of rings and the projective system U, (L^N), $(\mathrm{Tr}_{N'/N})$ of modules. Each $K[G/N]$ is finite dimensional over K and therefore an Artin ring. Each L^N is free over $K[G/N]$ on one generator, by the normal basis theorem. The remaining conditions are easy to check. Theorem 2 now follows from (2.7).

PROOF OF THEOREM 1. From (2.7) we obtain an element $(x_N)_{N \in U} \in \prod_{N \in U} L^N$ such that

(3.1) $(\sigma(x_N))_{\sigma \in G/N}$ is a basis of L^N over K, for each $N \in U$;

(3.2) $\mathrm{Tr}_{N'/N}(x_N) = x_{N'}$ for $N, N' \in U$, $N \subset N'$.

To define $\varphi: C(G, K) \to L$, let $f \in C(G, K)$. Since K is discrete, there is for every $\sigma \in G$ an $N \in U$ such that f is constant on σN. By compactness of G, we can choose the same N for all σ. Let $f_N: G/N \to K$ be the map induced by f. We now put

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

From (3.2) it easily follows that the expression on the right does not depend on the choice of N, so φ is well-defined. It is also K-linear, and it respects the action of G. Finally, (3.1) implies that it is bijective.

This proves Theorem 1.

Let L be finite over K, and let M be an intermediate field that is also Galois over K. Applying the trace from L to M one obtains, from every normal basis of L over K, a normal basis of M over K. In addition, every normal basis of M over K can be obtained in this way, since the natural map $K[G]^* \to K[G/N]^*$ is surjective (Lemma (2.6)); here $M = L^N$.

The extension of these results to the general case is as follows. Let L again be arbitrary, and let M be an intermediate field that is also Galois over K. Then $M = L^N$ for a unique closed normal subgroup N of G. From any isomorphism

$C(G,K)\to L$ as in Theorem 1 one obtains, upon taking invariants under N, an isomorphism $C(G/N,K)\to M$ such that the diagram

$$\begin{array}{ccc} C(G/N,K) & \longrightarrow & M \\ \downarrow & & \downarrow \\ C(G,K) & \longrightarrow & L \end{array}$$

is commutative; here the first vertical arrow is induced by the canonical map $G\to G/N$, and $M\to L$ is the inclusion. Conversely, given an isomorphism $C(G/N,K)\to M$ of K-vector spaces that respects the action of G/N one can find an isomorphism $C(G,K)\to L$ as in Theorem 1 such that the above diagram commutes. This is a consequence of (1.5)(c), with $I=U$ and J equal to the set of open normal subgroups of G that contain N.

REFERENCES

1. Bourbaki, N. – Algèbre, Chapitres 4 et 5, Hermann, Paris, 1959.
2. Bourbaki, N. – Théorie des ensembles, Hermann, Paris, 1970.
3. Deuring, M. – Galoissche Theorie und Darstellungstheorie, Math. Ann. **107**, 140–144 (1933).
4. Krull, W. – Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Ann. **100**, 687–698 (1928).
5. Noether, E. – Normalbasis bei Körpern ohne höhere Verzweigung, J. reine angew. Math. **167**, 147–152 (1932).
6. Waterhouse, W.C. – An empty inverse limit, Proc. Amer. Math. Soc. **36**, 618 (1972).