Note di Matematica **27,** n. 1, 2007, 5–10.

On the normal basis theorem

Dieter Blessenohl
Mathematisches Seminar, Christian-Albrechts-Universität Kiel,
Ludewig-Meyn-Str. 4, 24098 Kiel, Germany
blessenohl@math.uni-kiel.de

Received: 19/10/2005; accepted: 20/12/2005.

Abstract. The normal basis theorem is a fundamental result in Galois theory. For infinite fields, textbooks and monographs usually refer to a proof given by Artin in 1948. For finite fields, a completely different argument is commonly used.

We give two short proofs of the normal basis theorem which work without this distinction. They build on Dedekind's theorem on the linear independence of Galois automorphisms, and on the Krull–Schmidt theorem. The rest is elementary linear algebra. Both proofs are inspired by but simpler than the one given by Deuring in 1932.

Keywords: field theory, Galois theory, normal basis theorem

MSC 2000 classification: 12F10, 01A60, 12-03

Dedicated to Prof. Wolfgang Gaschütz on the occasion of his 85th birthday

In what follows, L/K is a finite Galois extension, G is the Galois group of L/K and $n := |G| = \dim_K L$. Hence L is a KG-module in a natural way.

Normal Basis Theorem. *L is a regular KG-module.*

More explicitly, there exists an element $x \in L$ such that $\{x^\alpha \,|\, \alpha \in G\}$ is a K-basis of L. Any such element x is called *normal* in L/K.

Eisenstein, in 1850, was the first to state this result [6] for a *finite* field L with prime field K. In the same year, Schönemann gave a proof of Eisenstein's "Lehrsatz" under the assumption that the degree of the extension be prime [10]. Hensel established the result for finite fields in full generality in 1888, apparently without knowledge of the work of his predecessors [8].

For certain *infinite* fields E. Noether showed the existence of a normal basis in 1932 [9]. Her work was extended to arbitrary finite Galois extensions of infinite fields by Artin [1]; see also [2]. E. Noether was actually interested in normal bases which are also integral bases of the ring of algebraic integers — a much more difficult problem. Dedekind considered such bases as to be very useful in algebraic number fields in 1880 already[1].

[1] Letter to Frobenius from July 8, 1896; printed in Dedekind, Coll. Papers. Vieweg 1931, Vol. 2, p. 433.

In his proof of 1932, Deuring did not need to distinguish between the finite and the infinite case [4]; see also [5]. This is the only proof of that kind, as far as we know. We present here two proofs of the normal basis theorem which also work equally well for finite and for infinite fields. The first one is a simpler version of Deuring's approach.

First Proof. The field L is an (L, K) bimodule and a (K, KG) bimodule. Hence $L \otimes_K L$ is an (L, KG)-bimodule, with the action of L and KG given by

$$\begin{aligned} l(a \otimes b) &= la \otimes b, \\ (a \otimes b)^{\varphi} &= (a \otimes b)(\mathrm{id} \otimes \varphi) \\ &= a \otimes b^{\varphi} \end{aligned}$$

for all $l, a, b \in L$ and $\varphi \in KG$. In particular, $L \otimes_K L$ is an LG-module. Note that $\dim_L(L \otimes_K L) = n$.

Let $\mu : L \otimes_K L \to L\ ,\ \ a \otimes b \mapsto ab$ denote the linearization of the multiplication in L. We define

$$\lambda_\alpha := (\mathrm{id} \otimes \alpha)\mu : L \otimes_K L \to L$$

for all $\alpha \in G$. It is clear that λ_α is K-linear. In fact, for all $l, a, b \in L$ and $\alpha \in G$, we have

$$[l(a \otimes b)]\lambda_\alpha = (la)b^\alpha = l(ab^\alpha) = l[(a \otimes b)\lambda_\alpha],$$

hence λ_α is L-linear, that is, an element of the dual space $(L \otimes_K L)^*$. It is an immediate consequence of Dedekind's independence theorem that

$$\{\lambda_\alpha \,|\, \alpha \in G\} \text{ is an } L\text{-basis of } (L \otimes_K L)^*. \tag{1}$$

To see this, it is enough to show that $\{\lambda_\alpha \,|\, \alpha \in G\}$ is L-linearly independent since $\dim_L(L \otimes_K L)^* = n$.

Suppose the coefficients $l_\alpha \in L$ $(\alpha \in G)$ are so chosen that $\sum_\alpha l_\alpha \lambda_\alpha = 0$, then, in particular,

$$0 = \sum_\alpha l_\alpha (1 \otimes b)^{\lambda_\alpha} = \sum_\alpha l_\alpha b^\alpha$$

for all $b \in L$. Thus Dedekind's result yields $l_\alpha = 0$ for all $\alpha \in G$. This implies (1).

Following [7], we define

$$\Phi : L \otimes_K L \to LG\,,\ x \mapsto \sum_{\alpha \in G} x^{\lambda_\alpha} \cdot \alpha^{-1}.$$

This map is L-linear and injective (by (1)), thus an L-isomorphism from $L \otimes_K L$ onto LG since both spaces have the same L-dimension. For all $x \in L \otimes_K L$ and

$\beta \in G$, we have

$$(x^\beta)^\Phi = \left(\sum_{\alpha \in G} x^{\lambda_{\beta\alpha}} \cdot \alpha^{-1}\beta^{-1} \right) \beta = x^\Phi \beta.$$

Therefore Φ is actually an isomorphism of LG-modules. It follows that, on the one hand,

$$L \otimes_K L \;\cong\; LG \;\cong\; \underbrace{KG \oplus \cdots \oplus KG}_{n} \quad \text{as } KG\text{-modules}\,. \tag{2}$$

On the other hand, if $\{a_1, \ldots, a_n\}$ is any K-basis of L, then

$$L \otimes_K L \;=\; (a_1 \otimes L) \oplus \cdots \oplus (a_n \otimes L).$$

This is a KG-direct decomposition of $L \otimes_K L$. Besides, $a_i \otimes L$ is a KG-submodule of $L \otimes_K L$ isomorphic to L, for all i. We conclude:

$$\underbrace{KG \oplus \cdots \oplus KG}_{n} \;\cong\; \underbrace{L \oplus \cdots \oplus L}_{n} \quad \text{as } KG\text{-modules}\,. \tag{3}$$

If M is a module and k is a positive integer, we write

$$k \cdot M := \underbrace{M \oplus \cdots \oplus M}_{k}.$$

Now suppose

$$KG = a_1 \cdot U_1 \oplus a_2 \cdot U_2 \oplus \ldots \quad \text{and} \quad L = b_1 \cdot V_1 \oplus b_2 \cdot V_2 \oplus \ldots$$

are decompositions of KG and L, respectively, into mutually non-isomorphic indecomposable KG-modules $U_1, U_2, \ldots$, respectively $V_1, V_2, \ldots$. Then (3) implies

$$na_1 \cdot U_1 \oplus na_2 \cdot U_2 \oplus \ldots \;\cong\; nb_1 \cdot V_1 \oplus nb_2 \cdot V_2 \oplus \ldots \quad \text{as } KG\text{-modules.}$$

It now follows from the Krull–Schmidt theorem that

$$U_1 \cong V_1,\; U_2 \cong V_2, \ldots \quad \text{and} \quad na_1 = nb_1,\; na_2 = nb_2, \ldots$$

after a suitable relabelling of summands. In particular, we may deduce that $a_1 = b_1,\; a_2 = b_2, \ldots$ and therefore

$$KG \cong L \quad \text{as } KG\text{-modules.}$$

This completes our first proof of the normal basis theorem. $\boxed{QED}$

The maps λ_α, $\alpha \in G$, are algebra epimorphisms from $L \otimes_K L$ onto L. Let $\{d_\alpha \,|\, \alpha \in G\}$ denote the L-Basis of $L \otimes_K L$ dual to $\{\lambda_\alpha \,|\, \alpha \in G\}$, and set $I_\alpha := Ld_\alpha = \bigcap_{\alpha \neq \beta \in G} \ker \lambda_\beta$ for all $\alpha \in G$. Then

$$L \otimes_K L = \bigoplus_{\alpha \in G} I_\alpha \,.$$

This is the decomposition of $L \otimes_K L$ into simple ideals. Deuring's proof takes this decomposition as a starting point. However, his line of reasoning that the Galois group G permutes regularly the direct summands is different from our argument above. Deuring also uses the Krull–Schmidt theorem to conclude his proof. This seems to be a subsequently inserted correction due to E. Noether in [4], and the argument is now usually referred to as the Deuring–Noether theorem (see, for instance, [3]).

Note that, for $\alpha, \beta \in G$,

$$(d_\alpha d_\alpha)^{\lambda_\beta} = d_\alpha^{\lambda_\beta} d_\alpha^{\lambda_\beta} = \begin{cases} 1 & \text{if } \alpha = \beta, \\ 0 & \text{if } \alpha \neq \beta. \end{cases}$$

Therefore $d_\alpha d_\alpha = d_\alpha$ and d_α is the neutral element of the algebra I_α. Furthermore, $d_\alpha^\Phi = \alpha^{-1}$ and $I_\alpha^\Phi = L\alpha^{-1}$.

In this context, there is a remarkable characterisation of the normal elements in L/K due to Erez [7]. An element $a \in L$ is normal in L/K if and only if the element

$$(1 \otimes a)^\Phi = \sum_{\alpha \in G} a^\alpha \cdot \alpha^{-1}$$

is a unit in the algebra LG. This can be seen as follows. We have

$$\begin{aligned} a \text{ normal in } L/K \quad &\Leftrightarrow \quad L = \bigoplus_\alpha K a^\alpha \\ &\Leftrightarrow \quad L \otimes_K L = \bigoplus_\alpha L \otimes a^\alpha \\ &\Leftrightarrow \quad L \otimes_K L = \langle 1 \otimes a \rangle_{LG} \\ &\Leftrightarrow \quad LG = \langle (1 \otimes a)^\Phi \rangle_{LG}. \end{aligned}$$

The generators of the LG-module LG are exactly the units of the algebra LG, and the proof is complete.

As a K-vector space $L \otimes_K L$ is isomorphic to $\mathrm{End}_K L$. This suggests to employ $\mathrm{End}_K L$ for a proof of the normal basis theorem.

Second Proof. For all $a \in L$, let $\overline{a} : L \to L\,,\ x \mapsto ax$ denote left multiplication by a. The map from L to $\mathrm{End}_K L$ which sends $a \mapsto \overline{a}$ is an embedding of algebras. We denote the image of L under this mapping by $\overline{L}$. From Dedekind's independence theorem we get

$$\mathrm{End}_K L = \bigoplus_{\alpha \in G} \alpha \overline{L} \quad \text{as an } \overline{L}\text{-vector space.} \tag{4}$$

We have $\overline{a}\alpha = \alpha\overline{a^\alpha}$ for all $a \in L$ and $\alpha \in G$, hence

$$\alpha\overline{L} = \overline{L}\alpha$$

for all $\alpha \in G$. Take any K-basis $\{a_1, \ldots, a_n\}$ of L. Then $\{\overline{a_1}, \ldots, \overline{a_n}\}$ is a K-basis of $\overline{L}$. It follows that

$$\alpha\overline{L} \;=\; \overline{L}\alpha \;=\; (\overline{a_1}K \oplus \cdots \oplus \overline{a_n}K)\alpha \;=\; \overline{a_1}\alpha K \oplus \cdots \oplus \overline{a_n}\alpha K.$$

for all $\alpha \in G$. In particular, the set $\{\overline{a_j}\alpha \,|\, 1 \le j \le n,\ \alpha \in G\}$ is a K-basis of $\mathrm{End}_K L$. Furthermore, for each $1 \le j \le n$, $M_j := \langle \overline{a_j}\alpha \,|\, \alpha \in G\rangle_K$ is a regular KG-module since $(\overline{a_j}\alpha)\beta = \overline{a_j}(\alpha\beta)$ for all $\alpha, \beta \in G$. Thus we have shown that

$$\mathrm{End}_K L \;=\; M_1 \oplus \cdots \oplus M_n \;\cong\; \underbrace{KG \oplus \cdots \oplus KG}_{n} \quad \text{as } KG\text{-modules.} \tag{5}$$

For $\varphi \in L^*$ and $a \in L$, we define

$$\varphi * a : L \to L, \;\; x \mapsto x^\varphi \cdot a.$$

Then $\varphi * a$ lies in $\mathrm{End}_K L$ and $\varphi * (a+b) = \varphi * a + \varphi * b$ for all $\varphi \in L^*$, $a, b \in L$, and furthermore

$$(\varphi * a)f = \varphi * a^f$$

for all $f \in \mathrm{End}_K L$. In particular, $\varphi * L := \{\varphi * a \,|\, a \in L\}$ is a right ideal of $\mathrm{End}_K L$. If $\varphi \neq 0$, then this right ideal has dimension 1 as an $\overline{L}$-vector space, and it is isomorphic to L as a KG-module.

Let $\{\varphi_1, \ldots, \varphi_n\}$ denote the basis of L^* dual to $\{a_1, \ldots, a_n\}$. If $x = k_1 a_1 + \cdots + k_n a_n \in L$ with $k_1, \ldots, k_n \in K$, then for all $f \in \mathrm{End}_K L$

$$x^f = x^{\varphi_1} a_1^f + \cdots + x^{\varphi_n} a_n^f,$$

hence

$$f = \varphi_1 * a_1^f + \cdots + \varphi_n * a_n^f \in \varphi_1 * L + \cdots + \varphi_n * L.$$

It follows that

$$\mathrm{End}_K L \;=\; \varphi_1 * L \oplus \cdots \oplus \varphi_n * L \;\cong\; \underbrace{L \oplus \cdots \oplus L}_{n} \quad \text{as } KG\text{-modules} \tag{6}$$

since $\dim_{\overline{L}} \mathrm{End}_K L = n$. The claim now follows from (5) and (6) as in the first proof, by means of the Krull–Schmidt theorem. $\boxed{QED}$

Both $L \otimes_K L$ and $\mathrm{End}_K L$ have K-dimension n^2. Hence they are isomorphic as K-vector spaces. But this is not a canonical isomorphism. However, there is a canonical isomorphism ϑ_L from $L^* \otimes_K L$ onto $\mathrm{End}_K L$ which sends

$$\varphi \otimes a \mapsto (x \mapsto x^{\varphi} \cdot a)$$

for all $\varphi \in L^*$ and $a \in L$. The image of $\varphi \otimes a$ under ϑ_L is $\varphi * a$. This is the underlying idea of the isomorphism (6).

We finally remark that $\varphi * L$ is an *irreducible* right ideal of the algebra $\mathrm{End}_K L$ whenever $\varphi \neq 0$. Therefore (6) is in fact a direct decomposition of $\mathrm{End}_K L$ into minimal right ideals.

References

[1] E. Artin: *Linear Mappings and the Existence of a Normal Basis*, Interscience Publ., Volume for Courant's 60th birthday, (1948), 1–5

[2] E. Artin: Galoissche Theorie, Harri Deutsch Verlag, Zürich, Frankfurt, 1973.

[3] R. W. Curtis, I. Reiner: Representation Theory of Finite Groups and Associative Algebras, Interscience Publ., New York, London, 1962.

[4] M. Deuring: *Galoissche Theorie und Darstellungstheorie*, Mathematische Annalen, **107**, (1932), 140–144.

[5] M. Deuring: Algebren. Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer, Berlin, 1935.

[6] G. Eisenstein: *Lehrsätze*, J. reine angew. Math., **39**, (1850), 180–182.

[7] B. Erez: Galois modules and class field theory, Geometry and Topology Monographs, Vol. 3, Invitation to higher local fields, Part II, section 10, 2000.

[8] K. Hensel: *Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*, J. reine angew. Math., **103**, (1888), 230–273.

[9] E. Noether: *Normalbasis bei Körpern ohne höhere Verzweigung.* J. reine angew. Math., **167**, (1932), 147–152.

[10] T. Schönemann: *Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze*, J. reine angew. Math., **40** (1850), 185–187.