MATH. SCAND. 94 (2004), 185–190

GENERALIZATIONS OF THE NORMAL BASIS THEOREM

ELISE BJÖRKHOLDT and PATRIK LUNDSTRÖM

Abstract

We give several generalizations of the normal basis and primitive element theorems for a finite Galois field extension, with an infinite base field. These generalizations are obtained by considering polynomial expressions of conjugates of a fixed element.

1. Introduction

Given a finite Galois field extension L/K of degree n with Galois group $G = \{g_1, \ldots, g_n\}$, there are two classical results on the existence of certain types of bases for this extension. One result (which in fact holds for general separable field extensions – see e.g. [3]), where the basis consists of powers of a fixed element:

THEOREM 1.1 (The Primitive Element Theorem). *There exists an $x \in L$, such that, $x^0, \ldots, x^{n-1}$ form a basis for L over K.*

The conjugates of an element are used for the other result:

THEOREM 1.2 (The Normal Basis Theorem). *There exists an $x \in L$, such that, $g_1(x), \ldots, g_n(x)$ form a basis for L over K.*

A proof can be found in [2]. In this article, we consider the following question: *Given $f_1, \ldots, f_n \in K[X_{g_1}, \ldots, X_{g_n}]$ (the ring of polynomials over K, in the variables $X_{g_1}, \ldots, X_{g_n}$), does there exist an $x \in L$ such that $f_i(g_1(x), \ldots, g_n(x))$, $i = 1, \ldots, n$, form a basis for L over K?*

When K is infinite, this question can be answered using an argument concerning the non-vanishing of a certain determinant over $K[X_{g_1}, \ldots, X_{g_n}]$ (see Lemma 2.1). In Section 2, we use this argument to establish several generalizations (see Theorems 2.2–2.5) of the primitive element and the normal basis theorems. In Section 3, we calculate some examples.

Received June 19, 2002.

2. Existence of Bases

We continue to use the same notation as in the introduction, and we also assume that K is infinite. Let $R = K[X_{g_1}, \dots, X_{g_n}]$. We define an action of G on R by

$$(g \cdot f)(X_{g_1}, \dots, X_{g_n}) = f(X_{gg_1}, \dots, X_{gg_n}),$$

$g \in G$ and $f \in R$. For $f_1, \dots, f_n \in R$, we use the above action to define the matrix

$$M(g_i \cdot f_j) = \begin{bmatrix} g_1 \cdot f_1 & \dots & g_1 \cdot f_n \\ \vdots & \ddots & \vdots \\ g_n \cdot f_1 & \dots & g_n \cdot f_n \end{bmatrix}$$

Furthermore, we let $D(M(g_i \cdot f_j))$ denote the determinant of this matrix. For $f \in R$ and $x \in L$, we let $f(x) = f(g_1(x), \dots, g_n(x))$, and we use the standard notation $\deg(f)$ to denote the degree of f.

We will repeatedly make use of the following (more or less well-known) result:

Lemma 2.1. *There exists an $x \in L$, such that, $f_1(x), \dots, f_n(x)$ form a basis for L over K, if and only if, $D(M(g_i \cdot f_j)) \neq 0$.*

Proof. First, note that, if $x \in L$, then $D(M(g_i \cdot f_j))(x)$ is the discriminant of $f_1(x), \dots, f_n(x)$. Hence, the "only if" statement follows immediately. The "if" statement follows directly from the fact that since K is infinite, the elements of G are algebraically independent over K (see e.g. [3]), and therefore there exists an $x \in L$, such that, $D(M(g_i \cdot f_j))(x) \neq 0$.

We are now ready to state our first generalization of the theorems mentioned in the introduction.

Theorem 2.2. *Let $f_i \in K[X_{\sigma_i}]$, $\sigma_i \in G$ and $i = 1, \dots, n$, be non-zero polynomials, such that, at most one of them is constant, and let all pairs $(\sigma_i, \deg(f_i))$ be distinct. Then there exists an element $x \in L$, such that, $f_i(\sigma_i(x))$, $i = 1, \dots, n$, form a basis for L over K.*

Proof. By Lemma 2.1, we need to establish that $D(M(g_i \cdot f_j))(x) \neq 0$. We observe, that it is enough (by the multi-linearity of the determinant) to check that the determinant of $(X^{r_j}_{g_i \sigma j})_{i,j}$, where $r_j = \deg(f_j)$, is non-zero. This determinant is non-zero by Thm. 2 in [4].

We need the following notation: for a subgroup H of G, let $L^H = \{x \in L \mid g(x) = x, g \in H\}$.

Theorem 2.3. *Let the non-zero polynomials $f_i \in K[X_{g_i}]$, $i = 1, \dots, n$, be such that at most one of them is constant. Then there exists an $x \in L$, such* *that, for each subgroup H of G, the collection $f_i(g_i(x))$, $g_i \in H$, is a basis for L over L^H.*

PROOF. For a subgroup H of G, let $I_H = \{i \mid g_i \in H\}$, and $D(H) = D(M(g_i \cdot f_j))$, where $i, j \in I_H$. Since the pairs $(g_i, \deg(f_i))$, $i \in I_H$, are distinct, we get, by Lemma 2.1 and Thm. 2.2, that each $D(H) \neq 0$. Hence, the product $P(X_{g_1}, \dots, X_{g_n})$ of all the determinants $D(H)$ is nonzero. Then there exists an $x \in L$ such that $P(x) \neq 0$, since the elements of G are algebraically independent. Hence, $D(H)(x) \neq 0$ for all subgroups H of G, which (by the proof of Lemma 2.1) implies that $f_i(x)$, $i \in I_H$, is a basis for L over L^H.

Before we state the next theorem, we need to introduce some more notations. For positive integers m and n, let S_n denote the permutation group of $\{1, \dots, n\}$, and (m, n) the greatest common divisor of m and n. For a set I, let $|I|$ denote the cardinality of this set. If $I \subseteq G$ and $g \in G$, then we let $gI = \{gh \mid h \in I\}$.

We conclude this section with two results concerning general monomials.

THEOREM 2.4. *Let $I \subseteq G$, be a fixed subset, such that,* $(|I|, |G|) = 1$. *If*

$$f_i = \prod_{g \in g_i I} X_g^{r_{ig}},$$

for $i = 1, \dots, n$, where the r_{ij} are positive integers, then there exists an $x \in L$, such that, the collection $f_i(x)$, $i = 1, \dots, n$, is a basis for L over K.

PROOF. We claim that the property

$$gI = I \Rightarrow g = 1$$

holds for all $g \in G$. If we assume that the claim holds, then a monomial depending exactly on the elements in I occurs precisely one time in each row and each column of $D(M(g_i \cdot f_j))$. Hence, $D(M(g_i \cdot f_j)) \neq 0$, which (by Lemma 2.1) implies that there exists an $x \in L$, such that, $f_i(x)$, $i = 1, \dots, n$, form a basis for L as a vector space over K.

Now we show the claim. If $gI = I$, then I is a union of right cosets of $\langle g \rangle$. Therefore $|\langle g \rangle|$ is a divisor of $|I|$ and of course of $|G|$ too. Hence $g = 1$.

Recall that the sign function sgn : $S_n \to \{\pm 1\}$ is defined by

$$\operatorname{sgn}(p) = \begin{cases} 1 & \text{if } p \text{ is even,} \\ -1 & \text{if } p \text{ is odd,} \end{cases}$$

for all $p \in S_n$.

THEOREM 2.5. *Let $p \in S_n$ and $f_i = X_{g_1}^{r_{i1}} \dots X_{g_n}^{r_{in}}$, $i = 1, \dots, n$, where the r_{ij} are nonnegative integers. For $p \in S_n$ and $i = 1, \dots, n$, let*

$$r_{pl} = r_{1j_l} + \dots + r_{nj_l},$$

where r_{ij_l} is the exponent of $X_{g_{p(i)}g_j}$, with $g_{p(i)}g_j = g_l$, in $g_i \cdot f_i$. Put

$$r_p = (r_{p1}, \dots, r_{pn}).$$

If there is an even $p \in S_n$ such that $r_p \neq r_{p'}$, for all odd $p' \in S_n$, then there exists an $x \in L$, such that, $f_i(x)$, $i = 1, \dots, n$, is a basis for L over K.

PROOF. Define a structure of a graph on S_n in the following way: $p, p' \in S_n$ are connected by an edge precisely when $\operatorname{sgn}(p) \neq \operatorname{sgn}(p')$ and $r_p = r_{p'}$. Then, by the definition of the r_p, the determinant

$$D(M(g_i \cdot f_j)) = \sum_{p \in S_n} \operatorname{sgn}(p)(X_{g_{p(1)}g_1}^{r_{11}} \dots X_{g_{p(1)}g_n}^{r_{1n}}) \dots (X_{g_{p(n)}g_1}^{r_{n1}} \dots X_{g_{p(n)}g_n}^{r_{nn}})$$

is equal to zero if and only if this bipartite graph possesses a complete matching. Now the theorem follows from Lemma 2.1.

REMARK 2.6. A straightforward calculation shows that the reversed statement in Theorem 2.5 holds for the groups of order one, two and three. The situation for general groups is not clear to the authors at present.

3. Examples

In this section, we exemplify some of the results that we have obtained in Section 2.

Degree 2. Let L/K be a quadratic extension with $G = \langle g \mid g^2 = 1 \rangle$. Let

$$\begin{cases} f_1 = \sum_{a,b \geq 0} r_{a,b} X_1^a X_g^b, \\ f_2 = \sum_{c,d \geq 0} s_{c,d} X_1^c X_g^d, \end{cases}$$

where $r_{a,b} = s_{c,d} = 0$ for almost all non-negative integers a, b, c, d. By Lemma 2.1 and a straightforward calculation, there exists an $x \in L$, such that, $f_1(x)$ and $f_2(x)$ form a basis for L over K, if and only if, there are non-negative integers A and B, such that,

$$\sum_{a+d=A, b+c=B} r_{a,b} s_{c,d} \neq \sum_{a+d=B, b+c=A} r_{a,b} s_{c,d}.$$

Note that if $f_1 = X_1^a X_g^b$ and $f_2 = X_1^c X_g^d$, then these conditions simplify to

$$a + b \neq c + d$$

(which, of course, also follows directly from Theorem 2.5 and Remark 2.6).

Degree 3. Let L/K be a cubic extension with $G = \langle g \mid g^3 = 1\rangle$. Assume that

$$f_i = X_1^{r_{i1}} X_g^{r_{i2}} X_{g^2}^{r_{i3}},$$

$i = 1, 2, 3$, where the r_{ij} are nonnegative integers. Consider the following conditions:

$$\begin{array}{lll} r_{11} + r_{23} \neq r_{13} + r_{21} & r_{11} + r_{32} \neq r_{12} + r_{31} & r_{23} + r_{32} \neq r_{22} + r_{33} \\ r_{12} + r_{21} \neq r_{11} + r_{22} & r_{12} + r_{33} \neq r_{13} + r_{32} & r_{21} + r_{33} \neq r_{23} + r_{31} \\ r_{13} + r_{22} \neq r_{12} + r_{23} & r_{13} + r_{31} \neq r_{11} + r_{33} & r_{22} + r_{31} \neq r_{21} + r_{32} \end{array}$$

By Theorem 2.5 and Remark 2.6, there exists an $x \in L$ such that $f_i(x)$, $i = 1, \dots, n$, form a basis for L over K, if and only if, at least one condition in each column holds.

Degree 4. Let L/K be a quartic extension with

$$G = \langle g_1, g_2 \mid g_1^2 = g_2^2 = 1, g_1 g_2 = g_2 g_1\rangle.$$

Let

$$\begin{cases} f_1 = X_1^{r_{11}} X_{g_2}^{r_{12}} X_{g_3}^{r_{13}}, \\ f_2 = X_1^{r_{21}} X_{g_1}^{r_{22}} X_{g_3}^{r_{23}}, \\ f_3 = X_1^{r_{31}} X_{g_1}^{r_{32}} X_{g_2}^{r_{33}}, \\ f_4 = X_{g_1}^{r_{41}} X_{g_2}^{r_{42}} X_{g_3}^{r_{43}}, \end{cases}$$

where the r_{ij} are positive integers and $g_3 = g_1 g_2$. Then, by Theorem 2.4, there exists an x in L, such that, $f_i(x)$, $i = 1, \dots, 4$, form a basis for L over K.

General degree. By Theorem 2.2 and Theorem 2.3, we immediately get the following results from [1] and [4] respectively:

- There exists an $x \in L$, such that, for each subgroup H of G, the collection $g(x)$, $g \in H$, is a basis for L over L^H.
- Let $\sigma_1, \dots, \sigma_n \in G$ and take non-negative integers $r_1, \dots, r_n$. If at most one of the r_i is zero and the pairs $(\sigma_1, r_1), \dots, (\sigma_n, r_n)$ are distinct, then there exists an $x \in L$, such that, $\sigma_i(x)^{r_i}$, $i = 1, \dots, n$, is a basis for L over K.

ACKNOWLEDGEMENT. The authors would like to thank the referee for many helpful comments concerning Theorem 2.4 and Theorem 2.5.

REFERENCES

1. Faith, C., *Extensions of normal bases and completely basic fields*, Trans. Amer. Math. Soc. 85 (1957), 406–427.
2. Jacobson, N. *Basic Algebra I*, Freeman, 1980.
3. Lang, S. *Algebra*, Addison-Wesley, 1993.
4. Waterhouse, W. C., *A unified version of the primitive and normal basis theorem*, Comm. Algebra 22 (1994), 2305–2308.

HÖGSKOLAN I TROLLHÄTTAN/UDDEVALLA
INSTITUTIONEN FÖR INFORMATIK OCH MATEMATIK
GÄRDHEMSVÄGEN 4
BOX 957
461 29 TROLLHÄTTAN
SWEDEN
E-mail: elise.bjorkholdt@htu.se, patrik.lundstrom@htu.se