Let $K$ be a finite Galois extension of the field $k$ with Galois group $G = \text{Gal}(K/k)$. We say that $K$ has a normal $k$-basis, if there exists an element $w \in K$, whose conjugates $\sigma(w)$, $\sigma \in G$ form a $k$-basis for $K$. We say also that $w$ generates a normal basis of $K/k$.

A familiar criterion for an element $w$ of $K$ to generate a normal basis of $K/k$ is that the matrix $(\sigma^i(w))$, $\sigma, \tau \in G$ have non zero determinant. [1, p.229] However, in one situation a much simpler criterion is available.

**Theorem.** Let $k$ be a field of characteristic $p \neq 2$ and $K$ a finite Galois extension whose Galois group $G = \text{Gal}(K/k)$ is a dihedral group of order $2p^n$. A nonzero element $w$ of $K$ generates a normal basis of $K/k$ if and only if

$$\text{Tr}(w) = w + \sigma w + \cdots + \sigma^{p^n-1}w + \tau w + \tau \sigma w + \cdots + \tau \sigma^{p^n-1}w \neq 0$$

and

$$w + \sigma w + \cdots + \sigma^{p^n-1}w - \tau w - \tau \sigma w - \cdots - \tau \sigma^{p^n-1} w \neq 0$$

where $G = \text{Gal}(K/k) = \langle \sigma, \tau | \sigma^{p^n} = 1, \, \tau^2 = 1, \, \tau \sigma = \sigma^{-1} \tau \rangle$

**Proof.** Let $H$ be the $p$-Sylow subgroup of $G$. Then the Jacobson's radical of the group ring $kG$ is

$$J(kG) = \sum_{h \in H \setminus \{1\}} kG(h-1)$$

Moreover, we have

$$kG/J(kG) \cong k(G/H) \quad [3, \, \text{p.} \, 68]$$

Assume $w$ generates a normal basis of $K/k$. Then $w, \, \sigma w, \cdots \sigma^{p^n-1}w, \tau w, \sigma \tau w, \cdots, \tau \sigma^{p^n-1}w$ are linearly independent over $k$ and so the result is clear.

Conversely assume that a nonzero element $w$ does not generate normal
basis of $K/k$. Then $\{\xi \in kG : \xi w = 0\}$ is obviously a nonzero ideal of $kG$ and so there exists a minimal ideal $I$ of $kG$ such that if

$$\xi = a_0 + a_1 \sigma + \cdots + a_{p^n-1} \sigma^{p^n-1} + b_0 \tau + b_1 \tau \sigma + \cdots + b_{p^n-1} \tau \sigma^{p^n-1}$$

is a nonzero element of $I$ then we have $\xi w = 0$.

Since $\sigma^i \xi \in I$ for each $i = 1, \ldots, p^n - 1$, and $J(kG) = \sum_{k \in H \setminus \{1\}} kG(h^{-1})$, we have $a_0 = a_1 = \cdots = a_{p^n-1}$ and $b_0 = b_1 \cdots b_{p^n-1}$.

Moreover $kG/J(kG) \cong k(1+\tau) \oplus k(1-\tau)$ implies that

$$\frac{1}{2} (1+\tau) \xi = \xi \quad \text{and} \quad \frac{1}{2} (1-\tau) \xi = 0$$

or

$$\frac{1}{2} (1+\tau) \xi = 0 \quad \text{and} \quad \frac{1}{2} (1-\tau) \xi = \xi$$

Hence

$$Tr(w) = w + \sigma w + \cdots + \sigma^{p^n-1} w + \tau w + \tau \sigma w + \cdots + \tau \sigma^{p^n-1} w = 0$$

or

$$w + \sigma w + \cdots + \sigma^{p^n-1} w - \tau w - \tau \sigma w - \cdots - \tau \sigma^{p^n-1} w = 0$$

This completes the proof.

Finally we give an example.

Let $k$ be a field of 3 elements and let $t_1, t_2, t_3$ be algebraically independent over $k$. Let $G$ be the symmetric group on $t_1, t_2, t_3$. $G$ operates on $K = k(t_1, t_2, t_3)$ by permuting $(t_1, t_2, t_3)$ its fixed field is $F = k(s_1, s_2, s_3)$ where $s_1 = t_1 + t_2 + t_3$, $s_2 = t_1 t_2 + t_1 t_3 + t_2 t_3$ and $s_3 = t_1 t_2 t_3$. Thus $G = \text{Gal}(K/F)$ is a dihedral group of order 6. \[1, p. 201\]

$$G = \langle \sigma, \tau | \sigma^3 = 1, \tau^2 = 1, \tau \sigma = \sigma^2 \tau \rangle$$

Say

$$\sigma = (123), \quad \tau = (12)$$

Let $w = t_1 t_2 \tau \in K = k(t_1, t_2, t_3)$. Then we have

$$Tr(w) = w + \sigma w + \sigma^2 w + \tau w + \tau \sigma w + \tau \sigma^2 w$$

$$= t_1 t_2 \tau^2 + t_2 t_3 \tau^2 + t_3 t_1 \tau^2 + t_1 t_2 + t_2 t_3 + t_3 t_1$$

and

$$w + \sigma w + \sigma^2 w - \tau w - \tau \sigma w - \tau \sigma^2 w = 0$$

Therefore $t_1 t_2 \tau$ generates a normal basis of the Galois extension $k(t_1, t_2, t_3)/k(s_1, s_2, s_3)$.

On the other hand

$$t_1 + \sigma t_1 + \sigma^2 t_1 - \tau t_1 - \tau \sigma t_1 - \tau \sigma^2 t_1 = t_1 + t_2 + t_3 - t_2 - t_1 - t_3 = 0$$
On normal bases

and so \( t_1 \) does not generate a normal basis of the Galois extension.

But \( \text{Tr}(t_1) = 2(t_1 + t_2 + t_3) \) is not zero.

Let \( k \) be a field of characteristic \( p \) and \( E \) a finite Galois extension such that \( \text{Gal}(E/k) \) is a \( p \)-group. Childs & Orzech [2] proved that a nonzero element \( w \) of \( E \) generates a normal basis of \( E/k \) if and only if the trace of \( w \) is not zero.

However, the above example shows that if \( \text{Gal}(E/k) \) is not a \( p \)-group then the converse of the theorem of Childs & Orzech does not hold.

References


Korea University
Seoul 132, Korea