J. Korean Math. Soc. 21 (1984), No. 2, p. 173-175.

ON NORMAL BASES

IN-HO CHO

Let K be a finite Galois extension of the field k with Galois group $G=\mathrm{Gal}\ (K/k)$. 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 $(\sigma\tau(w))$, σ, $\tau\in G$ 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 $G=\mathrm{Gal}\ (K/k)$ 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*

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

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

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

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

Moreover, we have

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

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

Conversely assume that a nonzero element w does not generate normal

Received December 16, 1983.

basis of K/k. Then $\{\xi \in kG \mid \xi w=0\}$ 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 $i=1, \cdots, p^n-1$, and $J(kG)=\sum_{h\in H-\{1\}} kG(h-1)$, 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

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

Hence

$$Tr(w)=w+\sigma w+\cdots\sigma^{p^n-1}w+\tau w+\tau\sigma w\cdots+\tau\sigma^{p^n-1}w=0$$
$$\text{or } w+\sigma w+\cdots\sigma^{p^n-1}w-\tau w-\tau\sigma w-\tau\sigma^2 w\cdots-\tau\sigma^{p^n-1}w=0$$

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 $s_1=t_1+t_2+t_3$, $s_2=t_1t_2+t_1t_3+t_2t_3$ and $s_3=t_1t_2t_3$. Thus $G=\mathrm{Gal}(K/F)$ is a dihedral group of order 6. [1, p. 201]

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

Say

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

Let $w=t_1t_2^2\in K=k(t_1, t_2, t_3)$. Then we have

$$\begin{aligned} Tr(w) &= w+\sigma w+\sigma^2 w+\tau w+\tau\sigma w+\tau\sigma^2 w \\ &= t_1t_2^2+t_2t_3^2+t_3t_1^2+t_1t_3^2+t_3t_2^2 \neq 0 \end{aligned}$$

and

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

Therefore $t_1t_2^2$ 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
$t_1+\sigma t_1+\sigma^2 t_1-\tau t_1-\tau\sigma t_1-\tau\sigma^2 t_1=t_1+t_2+t_3-t_2-t_1--t_3=0$

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

But $Tr(t_1)=2(t_1+t_2+t_3)$ is not zero.

Let k be a field of characteristic p and E a finite Galois extension such that $\mathrm{Gal}(E/k)$ 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 $\mathrm{Gal}(E/k)$ is not a p-group then the converse of the theorem of Child & Orzechs does not hold.

References

1. L. N. Childs and M. Orzech, *On Modular Groups Rings, Normal Basis, and Fixed Points*, Amer. Math. Monthly (1981), 142-145.
2. S. Lang, *Algebra*, Addison-Wesley, 1966.
3. R. S. Pierce, *Associative Algebras*, Springer Verlog, 1982.

Korea University
Seoul 132, Korea