NORMAL BASIS THEOREM

KIM, SUNGJIN

Theorem 1. Let L/K be a finite Galois extension with Galois group G. Then, there exists $\theta \in L$ such that

$$L = \bigoplus_{\sigma \in G} K\sigma\theta$$

as K-vector spaces.

Proof. Case1 : K is finite.
We have $G = \langle \sigma \rangle = \mathbb{Z}/n\mathbb{Z}$. We regard σ as K-linear endomorphism of vector space L. Then $\{1, \sigma, \cdots, \sigma^{n-1}\}$ is linearly independent, since they are distinct. Thus, the minimal polynomial for σ over K has degree n. The structure theorem for finitely generated module over PID implies the existence of such $\theta \in L$.

Case2 : K is infinite.
Primitive element theorem implies that $L = K(a)$ for some $a \in L$. Let f be the minimal polynomial for a over K. Let $G = \{\sigma_1, \cdots, \sigma_n\}$, and put $\sigma_i(a) = a_i$. Define

$$\sigma_i(g(x)) = g_i(x) = \frac{f(x)}{(x - a_i)f'(a_i)}.$$

Then for $i \neq k$, $g_i(x)g_k(x) \equiv 0 \pmod{f(x)}$.
Since a_i are distinct and degree of g_i are $n-1$, we have

$$g_1(x) + \cdots + g_n(x) - 1 = 0.$$

It follows that $g_i^2(x) \equiv g_i(x) \pmod{f(x)}$.
We next compute the determinant

$$D(x) = |\sigma_i\sigma_k(g(x))|_{\substack{1 \leq i \leq n \\ 1 \leq k \leq n}}.$$

Then we have $D(x)^2 \equiv 1 \pmod{f(x)}$. In particular $D(x) \neq 0$. Since K is infinite, we can find $\alpha \in K$ such that $D(\alpha) \neq 0$. Now, set $\theta = g(\alpha)$. Then the determinant

$$|\sigma_i\sigma_k(\theta)| \neq 0.$$

Consider any linear relation

$$x_1\sigma_1(\theta) + \cdots + x_n\sigma_n(\theta) = 0.$$

for some $x_i \in K$. Applying σ_i would lead to a system of linear equations

$$(\sigma_i\sigma_k(\theta)) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

This forces $x_1 = \cdots = x_n = 0$, and gives the result. ∎