EXISTENCE OF FROBENIUS ELEMENTS (D’APRÈS FROBENIUS)

KEITH CONRAD

We show how to lift automorphisms of a residue field extension, using the original proof of Frobenius (Ges. Abh. Vol. II p. 729) that Frobenius elements exist.

Let $A$ be a Dedekind ring with fraction field $F$. Let $E/F$ be a finite Galois extension and $B$ be the integral closure of $A$ in $E$. Set $G = \text{Gal}(E/F)$, choose a prime ideal $\mathfrak{P}$ in $B$, and let $\mathfrak{p} = \mathfrak{P} \cap A$ be the prime below $\mathfrak{P}$ in $A$ and $D(\mathfrak{P}|\mathfrak{p})$ be the decomposition group at $\mathfrak{P}$ in $G$. We want to show the natural homomorphism $D(\mathfrak{P}|\mathfrak{p}) \to \text{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$ is onto. That is, for any $\tau \in \text{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$, we want to show some $\sigma \in G$ satisfies

\[ \sigma(x) = \tau(x) \]

for all $x \in B$, where $\bar{t}$ means $t$ mod $\mathfrak{P}$. (Then $\sigma(\mathfrak{P}) = \mathfrak{P}$, so $\sigma$ is in $D(\mathfrak{P}|\mathfrak{p})$ and reduces to $\tau$.)

Since $B$ is a finitely generated $A$-module, we can write

\[ B = \sum_{j=1}^{n} A\omega_j \]

for some $n \geq 1$. (Note $A$ need not be a PID, so the $\omega_j$’s need not be an $A$-basis and $n$ need not be $[E:F]$.) We will find $\sigma \in G$ such that (1) holds for $x = \omega_1, \ldots, \omega_n$. Then (1) holds for all $x \in B$ by $A$-linearity.

Consider the following multivariable polynomial in $B[Y, X_1, \ldots, X_n]$:

\[ \varphi(Y, X_1, \ldots, X_n) = \prod_{\sigma \in G} (Y - \sigma(\omega_1)X_1 - \cdots - \sigma(\omega_n)X_n) \]

By symmetry, the coefficients of $\varphi(Y, X_1, \ldots, X_n)$ are in $B \cap F = A$.

Substituting $\omega_1 X_1 + \cdots + \omega_n X_n$ for $Y$ kills the polynomial:

\[ \varphi(\omega_1 X_1 + \cdots + \omega_n X_n, X_1, \ldots, X_n) = 0 \]

in $B[X_1, \ldots, X_n]$. Reducing coefficients modulo $\mathfrak{P}$,

\[ \varphi(\mathfrak{P})[X_1, \ldots, X_n] \]

in $(B/\mathfrak{P})[X_1, \ldots, X_n]$, noting $\varphi(Y, X_1, \ldots, X_n)$ lies in $(A/\mathfrak{p})[Y, X_1, \ldots, X_n]$.

Extend $\tau$ from an automorphism of $B/\mathfrak{P}$ to an automorphism of $(B/\mathfrak{P})[X_1, \ldots, X_n]$ by acting on coefficients (fixing the $X_j$’s, that is). Applying this automorphism to both sides of (3) gives

\[ \varphi(\tau(\mathfrak{P})[X_1, \ldots, X_n], X_1, \ldots, X_n) = 0 \]

in $(B/\mathfrak{P})[X_1, \ldots, X_n]$ since the coefficients of $\varphi$ (as a polynomial in $n + 1$ variables) are in $A/\mathfrak{p}$ and thus are fixed by $\tau$.

Recalling the definition of $\varphi$ in (2), equation (4) says that in $(B/\mathfrak{P})[X_1, \ldots, X_n]$,

\[ \prod_{\sigma \in G} ((\tau(\mathfrak{P}) - \sigma(\omega_1))X_1 + \cdots + (\tau(\mathfrak{P}) - \sigma(\omega_n))X_n) = 0. \]

Since $(B/\mathfrak{P})[X_1, \ldots, X_n]$ is a domain, one of the factors must be zero. That means some $\sigma \in G$ satisfies $\sigma(\omega_j) = \tau(\omega_j)$ in $B/\mathfrak{P}$ for all $j$. This $\sigma$ is what we were seeking.