THE EXISTENCE OF FROBENIUS ELEMENTS (APRÉS FROBENIUS)

KEITH CONRAD

We show the Galois group maps onto the decomposition group, using the idea in 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 $K/F$ be finite Galois and $B$ be the integral closure of $A$ in $K$. Set $G = \text{Gal}(K/F)$, choose a prime ideal $\mathfrak{P}$ in $B$, and let $p = \mathfrak{P} \cap A$ be the prime below $\mathfrak{P}$ in $A$. We want to show the natural homomorphism from $D(\mathfrak{P}|p)$ to $\text{Aut}_{A/p}(B/\mathfrak{P})$ is onto.

For any $\tau \in \text{Aut}_{A/p}(B/\mathfrak{P})$, we will show some $\sigma \in G$ satisfies

$$\sigma(x) = \tau(x)$$

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

We can assume $A$ is a PID. Indeed, in the classical setting $A = \mathbb{Z}$. But in general, if $A$ is not a PID at the start, note our problem is unchanged if we localize $A$ (and $B$) at $p$. Then $A$ is a DVR, and in particular a PID. Thus, $B$ is a free $A$-module:

$$B = \bigoplus_{j=1}^{n} A \omega_j,$$

where $n = [K:F]$. To prove $\tau$ lifts to some $\sigma \in G$, it will suffice to find $\sigma \in G$ such that (1) holds just for $x = \omega_1, \ldots, \omega_n$.

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 actually in $A$.

Substituting $\omega_1X_1 + \cdots + \omega_nX_n$ for $Y$ kills the polynomial:

$$\varphi(\omega_1X_1 + \cdots + \omega_nX_n, X_1, \ldots, X_n) = 0$$

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

$$\overline{\varphi}(\overline{\omega_1}X_1 + \cdots + \overline{\omega_n}X_n, X_1, \ldots, X_n) = \overline{0}$$

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

Extend $\tau$ from $\text{Aut}_{A/p}(B/\mathfrak{P})$ 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

$$\overline{\varphi}(\tau(\overline{\omega_1})X_1 + \cdots + \tau(\overline{\omega_n})X_n, X_1, \ldots, X_n) = \overline{0}$$

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

Recalling the definition of $\varphi$ in (2), equation (4) says

$$\prod_{\sigma \in G} ((\tau(\overline{\omega_1}) - \sigma(\overline{\omega_1}))X_1 + \cdots + (\tau(\overline{\omega_n}) - \sigma(\overline{\omega_n}))X_n) = \overline{0}$$

in $(B/\mathfrak{P})[X_1, \ldots, X_n]$.

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.