EXISTENCE OF FROBENIUS ELEMENTS (D'APRÈS FROBENIUS)

KEITH CONRAD

We lift residue field automorphisms by the proof of Frobenius [1, p. 699] that Frobenius elements exist. Dedekind and Hilbert independently proved the same result [2, p. 561].

Let A be a Dedekind domain with fraction field K, L/K be a finite Galois extension and B be the integral closure of A in E. Let $G = \mathrm{Gal}(L/K)$, $\mathfrak{P}$ be a prime in B, $\mathfrak{p} = \mathfrak{P} \cap A$, and $\mathrm{D}(\mathfrak{P}|\mathfrak{p})$ be the decomposition group at $\mathfrak{P}$ in G. We will show the natural homomorphism $\mathrm{D}(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$ is onto: for each $\tau \in \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$, some $\sigma \in G$ satisfies

$$\overline{\sigma(x)} = \tau(\overline{x}) \tag{1}$$

for all $x \in B$, where $\overline{t}$ means $t \bmod \mathfrak{P}$. Then $\sigma(\mathfrak{P}) = \mathfrak{P}$, so σ is in $\mathrm{D}(\mathfrak{P}|\mathfrak{p})$ and reduces to τ.

Since L/K is separable, B is a finitely generated A-module. Therefore we can write

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

for an $n \geq 1$. (Since A may not be a PID, the ω_j's may not be an A-basis and n may not be $[L : K]$.) We seek $\sigma \in G$ such that (1) holds for $x = \omega_1, \ldots, \omega_n$. Then (1) holds for all $x \in B$ by A-linearity. Consider the multivariable polynomial

$$\varphi(Y, X_1, \ldots, X_n) = \prod_{\sigma \in G} (Y - \sigma(\omega_1)X_1 - \cdots - \sigma(\omega_n)X_n) \tag{2}$$

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

Substituting $\omega_1 X_1 + \cdots + \omega_n X_n$ for Y in (2) 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 $\mathfrak{P}$,

$$\overline{\varphi}(\overline{\omega_1} X_1 + \cdots + \overline{\omega_n} X_n, X_1, \ldots, X_n) = \overline{0} \tag{3}$$

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

Make τ a ring automorphism of $(B/\mathfrak{P})[X_1, \ldots, X_n]$ by acting on coefficients. Then

$$\overline{\varphi}(\tau(\overline{\omega}_1) X_1 + \cdots + \tau(\overline{\omega_n}) X_n, X_1, \ldots, X_n) = \overline{0} \tag{4}$$

in $(B/\mathfrak{P})[X_1, \ldots, X_n]$ by applying τ to both sides of (3), since the coefficients of $\overline{\varphi}$ (as a polynomial in $Y, X_1, \ldots, X_n$) are in $A/\mathfrak{p}$ and thus are fixed by τ.

Recalling the definition of φ in (2), equation (4) says that

$$\prod_{\sigma \in G} ((\tau(\overline{\omega_1}) - \overline{\sigma(\omega_1)})X_1 + \cdots + (\tau(\overline{\omega_n}) - \overline{\sigma(\omega_n)})X_n) = \overline{0} \tag{5}$$

in the domain $(B/\mathfrak{P})[X_1, \ldots, X_n]$. Some σ-factor in (5) is $\overline{0}$, so $\overline{\sigma(\omega_j)} = \tau(\overline{\omega_j})$ for all j and we're done.

Here is a second proof of the theorem in the special case that the residue field extension is separable (*e.g.*, finite residue fields).[1] It is similar to the first proof but uses only single-variable polynomials. I learned the argument from Benjamin Steinberg.

[1] There are Galois L/K with an inseparable residue field extension. See the second example in `https://kconrad.math.uconn.edu/blurbs/gradnumthy/sepfield-and-insep-resfield.pdf`.

By the primitive element theorem, $B/\mathfrak{P} = (A/\mathfrak{p})(\overline{\gamma})$ for some $\gamma \in B$, and we can assume $\overline{\gamma} \neq \overline{0}$ since the case $B/\mathfrak{P} = A/\mathfrak{p}$ is trivial. Using the Chinese remainder theorem, there is a $\beta \in B$ such that

$$\beta \equiv \gamma \bmod \mathfrak{P}, \quad \beta \equiv 0 \bmod \sigma^{-1}(\mathfrak{P}) \text{ for all } \sigma \in G - D(\mathfrak{P}|\mathfrak{p}). \tag{6}$$

Set $f(Y) = \prod_{\sigma \in G}(Y - \sigma(\beta))$, which has coefficients in $B \cap K = A$.

In $(B/\mathfrak{P})[Y]$, $\overline{f}(Y)$ has the factor $Y - \overline{\beta} = Y - \overline{\gamma}$, so $\overline{f}(\overline{\gamma}) = \overline{0}$. Let $m(Y)$ be the minimal polynomial of $\overline{\gamma}$ over $A/\mathfrak{p}$, so

$$m(Y) \mid \overline{f}(Y) \text{ in } (A/\mathfrak{p})[Y].$$

We will refine this in $(B/\mathfrak{P})[Y]$ by looking more closely at the factors of $\overline{f}(Y)$ in $(B/\mathfrak{P})[Y]$ using (6). For $\sigma \in D(\mathfrak{P}|\mathfrak{p})$,

$$\beta \equiv \gamma \bmod \mathfrak{P} \Longrightarrow \sigma(\beta) \equiv \sigma(\gamma) \bmod \mathfrak{P} \tag{7}$$

since $\sigma(\mathfrak{P}) = \mathfrak{P}$. For $\sigma \in G - D(\mathfrak{P}|\mathfrak{p})$, $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$, so

$$\beta \equiv 0 \bmod \sigma^{-1}(\mathfrak{P}) \Longrightarrow \sigma(\beta) \equiv 0 \bmod \mathfrak{P}. \tag{8}$$

By (7) and (8),

$$f(Y) \equiv \prod_{\sigma \in D(\mathfrak{P}|\mathfrak{p})} (Y - \sigma(\gamma)) \cdot Y^d \bmod \mathfrak{P}$$

where d is the number of σ in G but not in $D(\mathfrak{P}|\mathfrak{p})$. The polynomial $m(Y)$ is not divisible by Y since $\overline{\gamma} \neq \overline{0}$, so in $(B/\mathfrak{P})[Y]$ we can improve $m(Y) \mid \overline{f}(Y)$ to

$$m(Y) \mid \prod_{\sigma \in D(\mathfrak{P}|\mathfrak{p})} (Y - \overline{\sigma(\gamma)}) \text{ in } (B/\mathfrak{P})[Y].$$

Note this product runs over $D(\mathfrak{P}|\mathfrak{p})$, not G.

For $\tau \in \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$, extend it to a ring automorphism of $(B/\mathfrak{P})[Y]$ by acting on coefficients. We have $(Y - \overline{\gamma}) \mid m(Y)$ in $(B/\mathfrak{P})[Y]$ since $m(\overline{\gamma}) = 0$, and $\tau(m(Y)) = m(Y)$ since $m(Y) \in (A/\mathfrak{p})[Y]$, so $(Y - \tau(\overline{\gamma})) \mid m(Y)$ in $(B/\mathfrak{P})[Y]$. Therefore $Y - \tau(\overline{\gamma}) = Y - \overline{\sigma(\gamma)}$ for some $\sigma \in D(\mathfrak{P}|\mathfrak{p})$, so

$$\tau(\overline{\gamma}) = \overline{\sigma(\gamma)} \tag{9}$$

in $B/\mathfrak{P}$. Since $B/\mathfrak{P} = (A/\mathfrak{p})[\overline{\gamma}]$, taking $(A/\mathfrak{p})$-linear combinations of powers of both sides of (9) implies $\tau(\overline{x}) = \overline{\sigma(x)}$ for all $\overline{x} \in B/\mathfrak{P}$, so we're done.

References

[1] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitzungsberichte der Koniglich Preuisschen Akademie der Wissenschaften zu Berlin* (1896), 689–703; Gesammelte Abhandlungen II, 719–733. Online at https://www.biodiversitylibrary.org/item/93035#page/719/mode/1up.

[2] T. Hawkins, "The Mathematics of Frobenius in Context," Springer-Verlag, New York, 2013.