

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 L . Let $G = \text{Gal}(L/K)$, \mathfrak{P} be a prime in B , $\mathfrak{p} = \mathfrak{P} \cap A$, and $D(\mathfrak{P}|\mathfrak{p})$ be the decomposition group at \mathfrak{P} in G . We will show the natural homomorphism $D(\mathfrak{P}|\mathfrak{p}) \rightarrow \text{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$ is onto: for each $\tau \in \text{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P})$, some $\sigma \in G$ satisfies

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

for all $x \in B$, where \bar{t} means $t \bmod \mathfrak{P}$. Then $\sigma(\mathfrak{P}) = \mathfrak{P}$, so σ is in $D(\mathfrak{P}|\mathfrak{p})$ 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 $x = \omega_1, \dots, \omega_n$. Then (1) holds for all $x \in B$ by A -linearity. Consider the multivariable polynomial

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

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

Substituting $\omega_1 X_1 + \dots + \omega_n X_n$ for Y in (2) kills the polynomial:

$$\varphi(\omega_1 X_1 + \dots + \omega_n X_n, X_1, \dots, X_n) = 0$$

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

$$(3) \quad \overline{\varphi(\omega_1 X_1 + \dots + \omega_n X_n, X_1, \dots, X_n)} = \bar{0}$$

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

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

$$(4) \quad \overline{\varphi(\tau(\omega_1)X_1 + \dots + \tau(\omega_n)X_n, X_1, \dots, X_n)} = \bar{0}$$

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

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

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

in the domain $(B/\mathfrak{P})[X_1, \dots, X_n]$. Some σ -factor in (5) is $\bar{0}$, 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.

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

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

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

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

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

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

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

$$(7) \quad \beta \equiv \gamma \pmod{\mathfrak{P}} \implies \sigma(\beta) \equiv \sigma(\gamma) \pmod{\mathfrak{P}}$$

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

$$(8) \quad \beta \equiv 0 \pmod{\sigma^{-1}(\mathfrak{P})} \implies \sigma(\beta) \equiv 0 \pmod{\mathfrak{P}}.$$

By (7) and (8),

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

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

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

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

REFERENCES

- [1] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1896), 689–703; *Gesammelte Abhandlungen II*, 719–733. URL <https://www.biodiversitylibrary.org/item/93035#page/719/mode/1up>.
- [2] T. Hawkins, “The Mathematics of Frobenius in Context,” Springer-Verlag, New York, 2013.