THE FROBENIUS AUTOMORPHISM

The purpose of these notes is to introduce the Frobenius automorphism and its action on roots of polynomials. This will help us justify the assertion in Chapter 3 of Rosen that for a monic irreducible polynomial $P(x) \in \mathbb{F}_q[x]$, we can write

$$P(x) = \prod_{j=0}^{n-1} (x - \alpha^{q^j})$$

where α is any root of $P(x)$ in an extension of $\mathbb{F}_q$.

0.1. Let $\mathbb{F}_q$ be a finite field of q elements, and $\mathbb{E}$ an finite extension of $\mathbb{F}_q$, that is a finite field containing $\mathbb{F}_q$ as a subfield. We define a map

$$\begin{aligned} \mathrm{Frob} = \mathrm{Frob}_{\mathbb{E}/\mathbb{F}_q} : \mathbb{E} &\to \mathbb{E} \\ \alpha &\mapsto \alpha^q \end{aligned}$$

Lemma 1. *The fixed points of* Frob *are precisely* $\mathbb{F}_q$*.*

Proof. If $c \in \mathbb{F}_q$ then $c^q = c$, which follows from the Euler-Fermat theorem. Moreover there cannot be any other fixed points, because the solutions of the equation $\alpha^q = \alpha$ are the roots of a polynomial $x^q - x \in \mathbb{F}_q[x]$ of degree q, hence there cannot be more that q such solutions in $\mathbb{E}$, and since we have found q such solutions, namely the elements of $\mathbb{F}_q$, we have found all solutions. $\square$

We note the following claim, which follows from Euler-Fermat:

Lemma 2. *If* $[\mathbb{E} : \mathbb{F}_q] = n$ *then* $\mathrm{Frob}^n_{\mathbb{E}/\mathbb{F}_q} = \mathrm{Id}_{\mathbb{E}}$ *is the identity map.*

Here $[\mathbb{E} : \mathbb{F}_q]$ is the degree of the extension, which is the dimension of $\mathbb{E}$ as a vector space over $\mathbb{F}_q$; and hence $\#\mathbb{E} = q^{[\mathbb{E}:\mathbb{F}_q]}$.

Proposition 3. *The Frobenius map is an* automorphism *of* $\mathbb{E}$ *over* $\mathbb{F}_q$*, that is it is a field isomorphism* $\mathbb{E} \to \mathbb{E}$ *restricting to the identity on* $\mathbb{F}_q$*.*

Proof. The Frobenius clearly maps $\mathbb{E}$ to itself. That the restriction of Frob to the base field $\mathbb{F}_q$ is the identity means that if $c \in \mathbb{F}_q$ then $c^q = c$, which is precisely Lemma 1.

To show that Frob is a field isomorphism, we need to show that it preserves addition and multiplication, and is $1-1$ and onto.

That it preserves multiplication $\mathrm{Frob}(\alpha\beta) = \mathrm{Frob}(\alpha)\,\mathrm{Frob}(\beta)$ is clear from the definition.

To see that it preserves addition, i.e. that

$$(\alpha+\beta)^q = \alpha^q + \beta^q$$

requires an idea: By the binomial theorem,

$$(\alpha+\beta)^q = \alpha^q + \beta^q + \sum_{j=1}^{q-1} \binom{q}{j} \alpha^j \beta^{q-j}$$

and so we need to show that the binomial coefficients vanish in $\mathbb{F}_q$:

$$\binom{q}{j} = 0 \text{ in } \mathbb{F}_q, \quad 1 \le j \le q-1$$

Of course this is not true in $\mathbb{Z}$; what it means that, if the prime p is the characteristic of the field $\mathbb{F}_q$ (so that $q = p^m$), then we need to show that p divides $\binom{p^m}{j}$ for $1 \le j \le p^m - 1$. That is left as an exercise.

To show that Frob is $1-1$, we first note that $\mathrm{Frob} : \mathbb{E} \to \mathbb{E}$ being a field homomorphism over $\mathbb{F}_q$, it is in particular a linear map of $\mathbb{E}$ as vector space over $\mathbb{F}_q$. Hence it suffices to show that its *kernel* is $\{0\}$. But if $\alpha^q = 0$ then certainly $\alpha = 0$ because $\mathbb{E}$ being a field, has no zero divisors.

To show that Frob is onto, note that since it is a $1-1$ map of the *finite* set $\mathbb{E}$ to itself, it is necessarily onto. □

0.2. We now examine the effect of the Frobenius map on roots of polynomials.

Lemma 4. *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial and α a root of $f(x)$ in some extension $\mathbb{E}$, that is $f(\alpha) = 0$. Then* $\mathrm{Frob}(\alpha)$ *is also a root of f.*

Proof. Suppose

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_j \in \mathbb{F}_q$$

Then because Frob respects addition and multiplication,

$$\mathrm{Frob}(f(\alpha)) = \mathrm{Frob}(\sum_{j=0}^{n} a_j \alpha_j) = \sum \mathrm{Frob}(a_j)\,\mathrm{Frob}(\alpha)^j$$

Moreover, since Frob is the identity on $\mathbb{F}_q$, and $a_j \in \mathbb{F}_q$, we have $\mathrm{Frob}(a_j) = a_j$. Thus we find

$$\mathrm{Frob}(f(\alpha)) = f(\mathrm{Frob}(\alpha))$$

But we assume $f(\alpha) = 0$ and $\mathrm{Frob}(0) = 0$, hence we find $f(\mathrm{Frob}(\alpha)) = 0$, that is $\mathrm{Frob}(\alpha)$ is also a root of f. □

Thus we see Frob *permutes* these roots.

We next assume that $f(x)$ is *irreducible.* We show that Frob permutes the roots *transitively.*

Lemma 5. *If $P(x) \in \mathbb{F}_q[x]$ is irreducible (over $\mathbb{F}_q$) of degree n and α is a root of f lying in an extension $\mathbb{E}$ of $\mathbb{F}_q$. Then* Frob *acts transitively on the roots: All roots of f are $\alpha_1 = \alpha$, $\alpha_2 =$* Frob(α)*, $\ldots$, $\alpha_n =$* Frob$^{n-1}(\alpha)$*. In particular all roots lie in $\mathbb{F}_q(\alpha)$, the minimal extension of $\mathbb{F}_q$ containing α, which is of degree n. We can write*

$$P(x) = \prod_{j=0}^{n-1}(x - \alpha^{q^j})$$

Proof. We may and will assume that P is monic, hence that $P(x) = \prod_{j=1}^{n}(x - \alpha_j)$.

We show that if the action is not transitive, then P is reducible. Suppose that we can partition the roots into two distinct, nonempty, sets $A = \{\alpha_1 = \alpha, \ldots, \alpha_r\}$ and $B = \{\alpha_{r+1}, \ldots, \alpha_n\}$ $(1 \leq r \leq n-1)$ which are both stable under Frob. Let

$$g(x) = \prod_{j=1}^{r}(x - \alpha_j), \quad h(x) := \prod_{j=r+1}^{n}(x - \alpha_j) \in \mathbb{E}[x]$$

so that $P = gh$ is a factorization in $\mathbb{E}[x]$.

Note that Frob permutes the factor of h and of g, hence Frob$(h) = h$ and Frob$(g) = g$. Hence the coefficients of h and of g are fixed by Frob, and are therefore in the base-field $\mathbb{F}_q$. Thus $h, g \in \mathbb{F}_q[x]$ give a factorization of P in $\mathbb{F}_q[x]$ into polynomials of positive degree, contradicting irreducibility of P.

Since the action is transitive, we may index the roots of $P(x)$ as $\alpha_1 = \alpha$, $\alpha_2 =$ Frob$(\alpha) = \alpha^q$, $\ldots$, $\alpha_n =$ Frob$^{n-1}(\alpha) = \alpha^{q^{n-1}}$, with $n = \deg P$. Then all roots lie in $\mathbb{F}_q(\alpha)$, and $P(x) = \prod_{j=0}^{n-1}(x - \alpha^{q^j})$ as claimed. $\square$