9. Finite fields

1. *Uniqueness*

Among other things, the following result justifies speaking of *the* field with p^n elements (for prime p and integer n), since, we prove, these parameters completely determine the isomorphism class.

[1.0.1] **Theorem:** Given a prime p and an integer n, there is exactly one (up to isomorphism) finite field $\mathbb{F}_{p^n}$ with p^n elements. Inside a fixed algebraic closure of $\mathbb{F}_p$, the field $\mathbb{F}_{p^m}$ lies inside $\mathbb{F}_{p^n}$ if and only if $m|n$. In particular, $\mathbb{F}_{p^n}$ is the set of solutions of

$$x^{p^n} - x = 0$$

inside an algebraic closure of $\mathbb{F}_p$.

Proof: Let E be an algebraic closure of $\mathbb{F}_p$. Let $F(x) = x^{p^n} - x$ in $\mathbb{F}_p[x]$. The algebraic derivative of F is -1, so $\gcd(F, F') = 1$, and F has no repeated factors. Let $K = \mathbb{F}_p(\alpha_1, \ldots, \alpha_{p^n})$ be the subfield of E generated over $\mathbb{F}_p$ by the roots of $F(x) = 0$, which we know are exactly the p^n distinct α_is occuring as linear factors $x - \alpha_i$ in $F(x)$. [1]

Perhaps unsurprisingly, we claim that K is exactly the set of all the roots of $F(x) = 0$. Naturally we use the fact [2] that binomial coefficients $\binom{p}{i}$ are 0 in characteristic p, for $0 < i < p$. Thus,

$$(\alpha + \beta)^{p^n} = (\ldots((\alpha + \beta)^p)^p \ldots)^p = \alpha^{p^n} + \beta^{p^n}$$

In particular, if $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, then $\alpha + \beta$ has the same property. And even more obviously

$$(\alpha \cdot \beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha \cdot \beta$$

[1] Later we would say that K is a **splitting field** for F since F factors into linear factors in K.

[2] As in the most pedestrian proof of Fermat's Little Theorem.

Additive inverses of roots of $F(x) = 0$ are present in the collection of roots, because $\alpha + \beta = 0$ implies $\alpha^{p^n} + \beta^{p^n} = 0$. Far more simply, certainly non-zero roots have multiplicative inverses among the roots. And 0 is among the roots. Finally, because $\alpha^p = \alpha$ for $\alpha \in \mathbb{F}_p$, certainly $\mathbb{F}_p$ is a subset of the set of roots.

In summary, the smallest subfield K (of some algebraic closure E of $\mathbb{F}_p$) containing the roots of $x^{p^n} - x = 0$ is exactly the set of all roots, and K contains $\mathbb{F}_p$. Thus, K has exactly p^n elements. This proves *existence* of a field with p^n elements.

For *uniqueness* (up to isomorphism) of a field with p^n elements, it suffices to prove that inside a given algebraic closure E of $\mathbb{F}_p$ there is exactly one such field, since [3] any algebraic extension L of $\mathbb{F}_p$ can be mapped injectively to E (by an injection that is the identity on $\mathbb{F}_p$). For L of degree n over $\mathbb{F}_p$, necessarily $L^\times$ is of order $p^n - 1$. That is, the non-zero elements of $L^\times$ all satisfy $x^{p^n-1} - 1 = 0$. [4] Thus, adding a factor of x, all elements of L are roots of $x^{p^n} - x = 0$. Thus, with L sitting inside the fixed algebraic closure E of $\mathbb{F}_p$, since a degree p^n equation has at most p^n roots in E, the elements of L must be just the field K constructed earlier. [5] This proves uniqueness (up to isomorphism). [6]

Inside a fixed algebraic closure of $\mathbb{F}_p$, if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ then the larger field is a vector space over the smaller. Given a basis $e_1, \ldots, e_t$, every element of the larger field is uniquely expressible as $\sum_i c_i e_i$ with c_i in the smaller field, so there are $(p^m)^t$ elements in the larger field. That is, $n = mt$, so $m|n$. Conversely, if $m|n$, then the roots of $x^{p^m-1} - 1 = 0$ are among those of $x^{p^n-1} - 1 = 0$. We have identified $\mathbb{F}_{p^m}^\times$ as the set of roots of $x^{p^m-1} - 1 = 0$ inside a fixed algebraic closure, and similarly for $\mathbb{F}_{p^n}^\times$, so $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. ///

[3] By part of the main theorem on algebraic closures.

[4] By Lagrange. In fact, we know that the multiplicative group is cyclic, but this is not used.

[5] For non-finite fields, we will not be able to so simply or completely identify all the extensions of the prime field.

[6] Note that we do not at all assert any uniqueness of the isomorphism between any two such fields. To the contrary, there will be several different isomorphisms. This is clarified just below, in discussion of the Frobenius automorphisms.

2. *Frobenius automorphisms*

Let q be a power of a prime p, and let E be an algebraic closure of $\mathbb{F}_q$. [7] For $\alpha \in E$, the **Frobenius automorphism** (depending on q) is

$$F(\alpha) = \alpha^q$$

[2.0.1] **Proposition:** For fixed prime power q and algebraic closure E of finite field $\mathbb{F}_q$, the Frobenius map $F : \alpha \longrightarrow \alpha^q$ is the identity map on $\mathbb{F}_q$, and stabilizes any overfield K of $\mathbb{F}_q$ inside E. Further, if $\beta \in E$ has the property that $F\beta = \beta$, then $\beta \in \mathbb{F}_q$. Generally, the fixed points of $\alpha \longrightarrow \alpha^{q^n}$ make up the field $\mathbb{F}_{q^n}$ inside E.

Proof: Certainly $F(\alpha\beta) = F(\alpha)F(\beta)$. Since the characteristic is P, also $(\alpha+\beta)^p = \alpha^p + \beta^p$, and F truly is a field homomorphism of E to itself.

Since any subfield K of E is stable under taking powers, certainly F maps K to itself.

By now we know that $\mathbb{F}_{q^n}^\times$ is cyclic, and consists exactly of the roots of $x^{q^n-1} - 1 = 0$ in E. That is, $\mathbb{F}_{q^n}$ is exactly the roots of $x^{q^n} - x = 0$. That is, the fixed points of F^n are exactly $\mathbb{F}_{q^n}$, as claimed. ///

[2.0.2] **Proposition:** Let $f(x)$ be a polynomial with coefficients in $\mathbb{F}_q$. Let $\alpha \in K$ be a root (in a fixed algebraic closure E of $\mathbb{F}_q$) of the equation $f(x) = 0$. Then $F(\alpha) = \alpha^q$, $F^2(\alpha) = F(F(\alpha)) = \alpha^{q^2}$, ... are also roots of the equation.

Proof: Let f have coefficients

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$$

with all the c_i's in $\mathbb{F}_q$. Apply the Frobenius map to both sides of the equation

$$0 = c_n\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_2\alpha^2 + c_1\alpha + c_0$$

to obtain

$$F(0) = F(c_n)F(\alpha)^n + F(c_{n-1})F(\alpha)^{n-1} + \ldots + F(c_2)F(\alpha)^2 + F(c_1)F(\alpha) + F(c_0)$$

since F is a field homomorphism. The coefficients c_i are in $\mathbb{F}_q$, as is the 0 on the left-hand side, so F does not change them. Thus,

$$0 = c_n F(\alpha)^n + c_{n-1}F(\alpha)^{n-1} + \ldots + c_2 F(\alpha)^2 + c_1 F(\alpha) + c_0$$

That is,

$$0 = f(F(\alpha))$$

and $F(\alpha)$ is a root of $P(x) = 0$ if α is. ///

[2.0.3] **Proposition:** Let

$$A = \{\alpha_1, \ldots, \alpha_t\}$$

be a set of (t distinct) elements of and algebraic closure E of $\mathbb{F}_q$, with the property that for any α in A, $F(\alpha)$ is again in A. Then the polynomial

$$(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_t)$$

[7] We take the liberty of considering not only $\mathbb{F}_p$ but any finite field $\mathbb{F}_q$ to be at the *bottom* of whatever towers of fields we consider. This is a simple case of *Galois theory*, which studies automorphisms of general fields.

(when multiplied out) has coefficients in k.

Proof: For a polynomial

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$$

with coefficients in E, define a new polynomial $F(f)$ by letting the Frobenius F act on the coefficients

$$F(f)(x) = F(c_n)x^n + F(c_{n-1})x^{n-1} + \ldots + F(c_2)x^2 + F(c_1)x + F(c_0)$$

This action gives a $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]$. Applying F to the product

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t)$$

merely permutes the factors, by the hypothesis that F permutes the elements of A. Thus,

$$c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t)$$

$$= (x-F\alpha_1)(x-F\alpha_2)\ldots(x-F\alpha_t) = F(c_n)x^n + F(c_{n-1})x^{n-1} + \ldots + F(c_1)x + F(c_0)$$

Equality of polynomials is coefficient-wise equality, so $F(c_i) = c_i$ for all indices i. ///

[2.0.4] Corollary: Let α be an element of an algebraic closure E of $\mathbb{F}_q$. Suppose that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$. Then the minimal polynomial $M(x)$ of α is

$$M(x) = (x-\alpha)(x-F(\alpha))(x-F^2(\alpha))\ldots(x-F^{n-1}(\alpha))$$

Proof: By definition of the minimal polynomial, M is the unique monic polynomial in $\mathbb{F}_q[x]$ such that any other polynomial in $\mathbb{F}_q[x]$ of which α is a zero is a polynomial multiple of M. Since α generates a degree n extension of $\mathbb{F}_q$, from above $F^n\alpha = \alpha$. Thus, the set α, $F\alpha$, $F^2\alpha$, ..., $F^{n-1}\alpha$ is F-stable, and the right-hand side product (when multiplied out) has coefficients in $\mathbb{F}_q$. Thus, it is a polynomial multiple of M. Since it is monic and has degree n (as does M), it must be M itself. ///

Given ground field $\mathbb{F}_q$ and α in an algebraic extension E of $\mathbb{F}_q$, the images

$$\alpha,\ \alpha^q,\ \alpha^{q^2},\ \ldots$$

of α under the Frobenius are the **(Galois) conjugates** of α **over** $\mathbb{F}_q$. Indeed, the notion of *Frobenius* automorphism is relative to the ground field $\mathbb{F}_q$. Two elements α, β in an algebraic extension E of $\mathbb{F}_q$ are **conjugate** if

$$\beta = \alpha^{q^t}$$

for some power F^t of the Frobenius over $\mathbb{F}_q$.

[2.0.5] Proposition: Inside a given algebraic extension E of $\mathbb{F}_q$, the property of being conjugate is an equivalence relation. ///

[2.0.6] Corollary: Given α in an algebraic field extension E of $\mathbb{F}_q$, the *number* of distinct conjugates of α over $\mathbb{F}_q$ is equal to the degree $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. ///

[2.0.7] Corollary: Let $f(x) \in \mathbb{F}_q[x]$ be irreducible, of degree n. Then $f(x)$ factors into linear factors in $\mathbb{F}_{q^n}$, (up to isomorphism) the unique extension of $\mathbb{F}_q$ of degree n. ///

Fix a prime power q, and an integer n. The set

$$= \mathrm{Aut}_{\mathbb{F}_q}\,\mathbb{F}_{q^n} = \{ \text{ automorphisms } h : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \quad \text{trivial on } \mathbb{F}_q\}$$

is a *group*, with operation *composition*. [8]

[2.0.8] **Theorem:** The group $G = \mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^n}$ of automorphisms of $\mathbb{F}_{q^n}$ trivial on $\mathbb{F}_q$ is cyclic of order n, generated by the Frobenius element $F(\alpha) = \alpha^q$.

Proof: First, we check that the Frobenius map is a field automorphism. It certainly preserves multiplication. Let p be the prime of which q is a power. Then p divides all the inner binomial coefficients $\binom{q}{i}$ with $0 < i < q$, essentially because p divides all the inner binomial coefficients $\binom{p}{i}$ with $0 < i < p$. Thus, for $\alpha, \beta \in \mathbb{F}_{q^n}$, by the binomial expansion,

$$(\alpha + \beta)^q \;=\; \alpha^q + \sum_{0<i<q} \binom{q}{i} \alpha^i \, \beta^{q-i} + \beta^q \;=\; \alpha^q + \beta^q$$

We should show that Frobenious does fix $\mathbb{F}_q$ pointwise. Since $\mathbb{F}_q^\times$ has order $q-1$, every element has order dividing $q-1$, by Lagrange. Thus, for $\beta \in \mathbb{F}_q$,

$$\beta^q = \beta^{q-1} \cdot \beta = 1 \cdot \beta = \beta$$

Certainly 0 is mapped to itself by Frobenius, so Frobenius fixes $\mathbb{F}_q$ pointwise, and, therefore, is a field automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Last, note that F^n fixes $\mathbb{F}_{q^n}$ pointwise, by the same argument that just showed that F fixes $\mathbb{F}_q$ pointwise. That is, F^n is the identity automorphism of $\mathbb{F}_{q^n}$. We note that F is invertible on $\mathbb{F}_{q^n}$, for any one of several reasons. One argument is that F^n is the identity.

The powers of the Frobenius element clearly form a subgroup of the automorphism group G, so the question is whether *every* automorphism is a power of Frobenius. There are many ways to approach this, but one straightforward way is as follows. We have seen that the multiplicative group $\mathbb{F}_{q^n}^\times$ is *cyclic*. Let α be a generator. Any field automorphism σ of $\mathbb{F}_{q^n}^\times$ is completely determined by $\sigma\alpha$, since a field map preserves multiplication, and, therefore,

$$\sigma(\alpha^n) = \Big(\sigma(\alpha)\Big)^n$$

And we know that the only possible images of $\sigma\alpha$ are the other roots in $\mathbb{F}_{q^n}$ of the monic irreducible $f(x)$ of α in $\mathbb{F}_q[x]$, which is of degree n, since we know that

$$\mathbb{F}_{q^n} \approx \mathbb{F}_q[x]/f$$

That is, there are at most n possible images $\sigma\alpha$ of α, including α itself. Let's count the number of distinct images of α under powers of Frobenious. First, for $i < j$, using the invertibility of F, $F^i\alpha = F^j\alpha$ is equivalent to $\alpha = F^{j-i}\alpha$. Thus, it suffices to determine the smallest positive exponent j such that $F^j\alpha = \alpha$. In fact, being the generator of the cyclic group $\mathbb{F}_{q^n}^\times$, α has order exactly $q^n - 1$. Thus, the positive powers of α of orders less than $q^n - 1$ are distinct. Thus, $\alpha^{q^\ell} = \alpha$ implies $\alpha^{q^\ell - 1} = 1$, and then

$$q^n - 1 \text{ divides } q^\ell - 1$$

Thus, it must be that $\ell = n$. This shows that α, $F\alpha$, $F^2\alpha$, ..., $F^{n-1}\alpha$ are distinct, and therefore are *all* the possible images of α by automorphisms. We noted that the image of α by an automorphism determines that automorphism completely, so $1, F, F^2, \ldots, F^{n-1}$ are all the automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. ///

---

3. *Counting irreducibles*

[8] As usual, an *automorphism* of a thing is an isomorphism of it to itself, of whatever sort is currently under discussion. Here, we are concerned with field isomorphisms of $\mathbb{F}_{q^n}$ to itself which fix $\mathbb{F}_q$ pointwise. In general, with some further hypotheses to avoid various problems, roughly speaking the automorphism group of one field over another is a *Galois group*.

By now we might anticipate that counting irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ of degree n is intimately connected with elements α [9] such that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$, by taking roots α of $f(x) = 0$.

[3.0.1] **Proposition:** The collection of monic irreducible polynomials $f(x)$ of degree n in $\mathbb{F}_q[x]$ is in bijection with sets of n mutually conjugate generators of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, by

$$\alpha,\ \alpha^q,\ \ldots,\ \alpha^{q^{n-1}} \quad \longleftrightarrow \quad (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{n-1}})$$

Proof: On one hand, a degree n monic irreducible f has a root α in $\mathbb{F}_q[x]/\langle f\rangle$, which is a degree n field extension of $\mathbb{F}_q$. In particular, $\mathbb{F}_q(\alpha) = \mathbb{F}_q[\alpha]$ is of degree n over $\mathbb{F}_q$. And (from just above)

$$f(x) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\ldots(x-\alpha^{q^{n-1}})$$

We have noted that the n distinct images α^{q^i} are an equivalence class under the equivalence relation of being conjugate, and any one of these roots generates the same degree n extension as does α.

On the other hand, let α generate the unique degree n extension of $\mathbb{F}_q$ inside a fixed algebraic closure. That is, $\mathbb{F}_q(\alpha) = \mathbb{F}_q[\alpha]$ is of degree n over $\mathbb{F}_q$, which implies that the minimal polynomial f of α over $\mathbb{F}_q$ is of degree n. From above, the other roots of $f(x) = 0$ are exactly the conjugates of α over $\mathbb{F}_q$. ///

Let $\mu(n)$ be the Möbius function

$$\mu(n) = \begin{cases} 0 & \text{(if the square of any prime divides } n\text{)} \\ (-1)^t & \text{(otherwise, where distinct primes divide } n\text{, but no square does)} \end{cases}$$

[3.0.2] **Corollary:** The number of irreducible degree n polynomials in $\mathbb{F}_q[x]$ is

$$\text{number irreducibles degree } n \ = \frac{1}{n} \cdot \left(\sum_{d|n} \mu(d)\, q^{n/d} \right)$$

Proof: We want to remove from $\mathbb{F}_{q^n}$ the elements which generate (over $\mathbb{F}_q$) proper subfields of $\mathbb{F}_{q^n}$, and then divide by n, the number of conjugates of a given generator of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Above we showed that $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ if and only if $m|n$. Thus, the maximal proper subfields of $\mathbb{F}_{q^n}$ are the fields $\mathbb{F}_{q^{n/r}}$ with r a prime dividing n. But the attempted count $q^n - \sum_{r|n} q^{n/r}$ over-counts the intersections of subfields $\mathbb{F}_{q^{n/r_1}}$ and $\mathbb{F}_{q^{n/r_2}}$, for primes $r_1 \neq r_2$. Thus, typically, we put back $q^{n/r_1 r_2}$, but we have put back too much, and must subtract the common triple intersections, and so on. After this inclusion-exclusion process, we divide by n so that we count equivalence classes of mutually conjugate generators of the degree n extension, rather than the individual generators. ///

Exercises

9.[3.0.1] Show that any root α of $x^3 + x + 1 = 0$ in an algebraic closure of the finite field $\mathbb{F}_2$ with 2 elements is a generator for the multiplicative group $\mathbb{F}_{2^3}^\times$.

9.[3.0.2] Find the irreducible quartic equation with coefficients in $\mathbb{F}_2$ satisfied by a generator for the cyclic group $\mathbb{F}_{2^4}^\times$.

[9] In a fixed algebraic closure of $\mathbb{F}_q$, for example.

9.[3.0.3] Let f be an irreducible polynomial of degree n in $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a field with q elements. Show that $f(x)$ divides $x^{q^n} - x$ if and only if $\deg f$ divides n.

9.[3.0.4] Show that the *general linear group* $GL_n(\mathbb{F}_q)$ of invertible matrices with entries in the finite field $\mathbb{F}_q$ has an element of order $q^n - 1$.

9.[3.0.5] Let k be a finite field. Show that $k[x]$ contains irreducibles of every positive integer degree.

9.[3.0.6] For a power q of a prime p, find a p-Sylow subgroup of $GL_n(\mathbb{F}_q)$.

9.[3.0.7] For q a power of an odd prime p, find a 2-Sylow subgroup of $GL_2(\mathbb{F}_q)$.

9.[3.0.8] For q a power of an odd prime p, find a 2-Sylow subgroup of $GL_3(\mathbb{F}_q)$.

9.[3.0.9] Find a 3-Sylow subgroup of $GL_3(\mathbb{F}_7)$.

9.[3.0.10] (*Artin-Schreier polynomials*) Let q be a power of a prime p. Take $a \neq 0$ in $\mathbb{F}_q$. Show that if α is a root of $x^p - x + a = 0$ then so is $\alpha + i$ for $i = 1, 2, \ldots, p-1$.

9.[3.0.11] Show that Artin-Schreier polynomials are irreducible in $\mathbb{F}_q[x]$.