

# FINITE FIELDS

KEITH CONRAD

This handout discusses finite fields: how to construct them, properties of elements in a finite field, and relations between different finite fields (including their Galois groups). We write  $\mathbf{Z}/(p)$  and  $\mathbf{F}_p$  interchangeably for the field of size  $p$ .

Here is an executive summary of the main results.

- Every finite field has prime power order.
- For every prime power, there is a finite field of that order.
- For a prime  $p$  and positive integer  $n$ , there is an irreducible  $\pi(x)$  of degree  $n$  in  $\mathbf{F}_p[x]$ , and  $\mathbf{F}_p[x]/(\pi(x))$  is a field of order  $p^n$ .
- Any two finite fields of the same size are isomorphic (usually not in just one way).
- Every finite extension of  $\mathbf{F}_p$  is a Galois extension whose Galois group over  $\mathbf{F}_p$  is generated by the  $p$ th power map.
- If  $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = d$ , the  $\mathbf{F}_p$ -conjugates of  $\alpha$  are  $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$ .

## 1. CONSTRUCTION

**Theorem 1.1.** *For a prime  $p$  and a monic irreducible  $\pi(x)$  in  $\mathbf{F}_p[x]$  of degree  $n$ , the ring  $\mathbf{F}_p[x]/(\pi(x))$  is a field of order  $p^n$ .*

*Proof.* The cosets mod  $\pi(x)$  are represented by remainders

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, \quad c_i \in \mathbf{F}_p,$$

and there are  $p^n$  of these. Since the modulus  $\pi(x)$  is irreducible, the ring  $\mathbf{F}_p[x]/(\pi(x))$  is a field using the same proof that  $\mathbf{Z}/(m)$  is a field when  $m$  is prime.  $\square$

**Example 1.2.** Two fields of order 8 are  $\mathbf{F}_2[x]/(x^3 + x + 1)$  and  $\mathbf{F}_2[x]/(x^3 + x^2 + 1)$ .

**Example 1.3.** Two fields of order 9 are  $\mathbf{F}_3[x]/(x^2 + 1)$  and  $\mathbf{F}_3[x]/(x^2 + x + 2)$ .

**Example 1.4.** The polynomial  $x^3 - 2$  is irreducible in  $\mathbf{F}_7[x]$ , so  $\mathbf{F}_7[x]/(x^3 - 2)$  is a field of order  $7^3 = 343$ .

**Warning.** Do **not** try to create a field of order 8 as  $\mathbf{Z}/(8)$ . That is not a field. Similarly,  $\mathbf{Z}/(9)$  is not a field. The ring  $\mathbf{Z}/(m)$  is a field only when  $m$  is a prime number. In order to create fields of non-prime size we must do something other than look at  $\mathbf{Z}/(m)$ .

We will see that every finite field is isomorphic to a field of the form  $\mathbf{F}_p[x]/(\pi(x))$ , so these polynomial constructions give us working models of any finite field. However, finite fields may not literally have the form  $\mathbf{F}_p[x]/(\pi(x))$ . For instance,  $\mathbf{Z}[\sqrt{2}]/(3)$  is a field of size 9 (which is isomorphic to  $\mathbf{F}_3[x]/(x^2 - 2)$ ).

**Theorem 1.5.** *Any finite field has prime power order.*

*Proof.* For any commutative ring  $R$  there is a unique ring homomorphism  $\mathbf{Z} \rightarrow R$ , given by

$$m \mapsto \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}}, & \text{if } m \geq 0, \\ -(\underbrace{1 + 1 + \cdots + 1}_{|m| \text{ times}}), & \text{if } m < 0. \end{cases}$$

We apply this to the case when  $R = F$  is a finite field. The kernel of  $\mathbf{Z} \rightarrow F$  is nonzero since  $\mathbf{Z}$  is infinite and  $F$  is finite. Write the kernel as  $(m) = m\mathbf{Z}$  for an integer  $m > 0$ , so  $\mathbf{Z}/(m)$  embeds as a subring of  $F$ . Any subring of a field is a domain, so  $m$  has to be a prime number, say  $m = p$ . Therefore there is an embedding  $\mathbf{Z}/(p) \hookrightarrow F$ . Treating  $F$  as a vector space over  $\mathbf{Z}/(p)$ , it is finite-dimensional since  $F$  is in fact a finite set. Letting  $n = \dim_{\mathbf{Z}/(p)}(F)$ , the elements of  $F$  can be written in terms of a basis  $\{e_1, \dots, e_n\}$  over  $\mathbf{Z}/(p)$  as unique linear combinations

$$c_1 e_1 + \cdots + c_n e_n, \quad c_i \in \mathbf{Z}/(p).$$

The number of these linear combinations is  $p^n$ . □

**Lemma 1.6.** *If  $F$  is a finite field, the group  $F^\times$  is cyclic.*

*Proof.* Let  $N$  be the largest order of a number in the group  $F^\times$ , which is abelian. It is a theorem from group theory that in any finite *abelian* group, all orders of elements divide the maximal order of the elements<sup>1</sup>, so every  $t$  in  $F^\times$  satisfies  $t^N = 1$ . Therefore all numbers in  $F^\times$  are roots of  $x^N - 1$ .

Let  $q = \#F$ . The number of roots of a polynomial over a field is at most the degree of the polynomial, and  $x^N - 1$  has  $q - 1$  roots in  $F$ , so  $q - 1 \leq N$ . Since  $N$  is the order of an element in  $F^\times$ , which is a group with order  $q - 1$ ,  $N \mid (q - 1)$ , so  $N \leq q - 1$ . Therefore  $N = q - 1$ , so there are elements of  $F^\times$  with order  $q - 1$ , which means  $F^\times$  is cyclic. □

**Example 1.7.** In the field  $\mathbf{F}_3[x]/(x^2 + 1)$ , the nonzero numbers are a group of order 8. The powers of  $x$  are

$$x, \quad x^2 = -1 = 2, \quad x^3 = 2x, \quad x^4 = 2x^2 = -2 = 1,$$

so  $x$  is not a generator. But  $x + 1$  is a generator: its successive powers are in the table below.

| $k$   | 1       | 2    | 3        | 4   | 5        | 6   | 7       | 8   |
|-------|---------|------|----------|-----|----------|-----|---------|-----|
| $x^k$ | $x + 1$ | $2x$ | $2x + 1$ | $2$ | $2x + 2$ | $x$ | $x + 2$ | $1$ |

**Example 1.8.** For any prime  $p$ , the group  $(\mathbf{Z}/(p))^\times$  is cyclic: there is an  $a \not\equiv 0 \pmod p$  such that  $\{a, a^2, a^3, \dots, a^{p-1} \pmod p\} = (\mathbf{Z}/(p))^\times$ . The proof of this is not constructive, and in fact there is no simple algorithm for constructing a generator of  $(\mathbf{Z}/(p))^\times$ .

**Theorem 1.9.** *Every finite field is isomorphic to  $\mathbf{F}_p[x]/(\pi(x))$  for some prime  $p$  and some monic irreducible  $\pi(x)$  in  $\mathbf{F}_p[x]$ .*

*Proof.* Let  $F$  be a finite field. By Theorem 1.5,  $F$  has order  $p^n$  for some prime  $p$  and positive integer  $n$ , and there is a field embedding  $\mathbf{F}_p \hookrightarrow F$ .

The group  $F^\times$  is cyclic by Lemma 1.6. Let  $\gamma$  be a generator of  $F^\times$ . Evaluation at  $\gamma$  is a ring homomorphism  $\text{ev}_\gamma: \mathbf{F}_p[x] \rightarrow F$  that fixes  $\mathbf{F}_p$ . Since every number in  $F$  is 0 or a power of  $\gamma$ , the evaluation homomorphism is onto ( $0 \mapsto 0$  and  $x^r \mapsto \gamma^r$  for any  $r \geq 0$ ). Therefore

<sup>1</sup>In a finite nonabelian group, all orders of elements don't have to divide the maximal order, e.g., in  $S_3$  the orders of elements are 1, 2, and 3.

$\mathbf{F}_p[x]/\ker(\text{ev}_\gamma) \cong F$ . The kernel is a maximal ideal in  $\mathbf{F}_p[x]$ , so it must be  $(\pi(x))$  for some monic irreducible  $\pi(x)$  in  $\mathbf{F}_p[x]$ .  $\square$

Theorem 1.9 does not assure us fields of all prime power orders exist. It only tells us that if a field of order  $p^n$  exists then it is isomorphic to  $\mathbf{F}_p[x]/(\pi(x))$  for some irreducible  $\pi(x)$  of degree  $n$  in  $\mathbf{F}_p[x]$ . We aren't even assured yet that there is an irreducible of degree  $n$  in  $\mathbf{F}_p[x]$ . In the next section we will show a field of any prime power order does exist and there is an irreducible in  $\mathbf{F}_p[x]$  of any desired degree.

## 2. FINITE FIELDS AS SPLITTING FIELDS

We can describe any finite field as a splitting field of a polynomial depending only on the size of the field.

**Lemma 2.1.** *A field of prime power order  $p^n$  is a splitting field over  $\mathbf{F}_p$  of  $x^{p^n} - x$ .*

*Proof.* Let  $F$  be a field of order  $p^n$ . From the proof of Theorem 1.5,  $F$  contains a subfield isomorphic to  $\mathbf{Z}/(p) = \mathbf{F}_p$ . Explicitly, the subring of  $F$  generated by 1 is a field of order  $p$ .

Every  $t \in F$  satisfies  $t^{p^n} = t$ : if  $t \neq 0$  then  $t^{p^n-1} = 1$  since  $F^\times = F - \{0\}$  is a multiplicative group of order  $p^n - 1$ , and then multiplying through by  $t$  gives us  $t^{p^n} = t$ , which is also true when  $t = 0$ . The polynomial  $x^{p^n} - x$  has every element of  $F$  as a root, so  $F$  is a splitting field of  $x^{p^n} - x$  over the field  $\mathbf{F}_p$ .  $\square$

Using the construction of splitting fields, we can now show a finite field of any prime power order does exist.

**Theorem 2.2.** *For any prime power  $p^n$ , a field of order  $p^n$  exists.*

*Proof.* Taking our cue from the statement of Lemma 2.1, let  $F$  be a field extension of  $\mathbf{F}_p$  over which  $x^{p^n} - x$  splits completely. General theorems from field theory guarantee there is such a field.

Inside  $F$ , the roots of  $x^{p^n} - x$  form the set

$$S = \{t \in F : t^{p^n} = t\}.$$

This set has size  $p^n$  since the polynomial  $x^{p^n} - x$  is separable:  $(x^{p^n} - x)' = p^n x^{p^n-1} - 1 = -1$  since  $p = 0$  in  $F$ , so  $x^{p^n} - x$  has no roots in common with its derivative. It splits completely over  $F$  and has degree  $p^n$ , so it has  $p^n$  roots in  $F$ .

We will show  $S$  is a field. It is easily closed under multiplication and (for nonzero solutions) inversion. It remains to show  $S$  is an additive group. Since  $p = 0$  in  $F$ ,  $(a + b)^p = a^p + b^p$  for all  $a$  and  $b$  in  $F$  (the intermediate terms in  $(a + b)^p$  coming from the binomial theorem have integral coefficients  $\binom{p}{k}$ , which are all multiples of  $p$ ). Therefore  $t \mapsto t^p$  on  $F$  is additive, so its  $n$ -th iterate  $t \mapsto t^{p^n}$  is also additive. The fixed points of an additive map are a group under addition, so  $S$  is a group under addition.  $\square$

**Corollary 2.3.** *For any prime  $p$  and positive integer  $n$ , there is a monic irreducible of degree  $n$  in  $\mathbf{F}_p[x]$ .*

*Proof.* By Theorem 2.2, an abstract field of order  $p^n$  exists. By Theorem 1.9, the existence of an abstract field of order  $p^n$  implies the existence of a monic irreducible  $\pi(x)$  in  $\mathbf{F}_p[x]$  of degree  $n$ .  $\square$

**Theorem 2.4.** *Every irreducible  $\pi(x)$  in  $\mathbf{F}_p[x]$  is separable.*

*Proof.* Let  $n = \deg \pi(x)$ , so  $\mathbf{F}_p[x]/(\pi(x))$  has size  $p^n$  and therefore  $t^{p^n} = t$  for all  $t$  in  $\mathbf{F}_p[x]/(\pi(x))$ . In particular,  $x^{p^n} \equiv x \pmod{\pi(x)}$ , so  $\pi(x) \mid (x^{p^n} - x)$  in  $\mathbf{F}_p[x]$ . We saw in the proof of Theorem 2.2 that the polynomial  $x^{p^n} - x$  is separable in  $\mathbf{F}_p[x]$ , so its factor  $\pi(x)$  is separable.  $\square$

We write  $\mathbf{F}_{p^n}$  for a finite field of order  $p^n$ . By the proof of Theorem 1.5,  $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$ . Each finite field of  $p$ -power order contains a copy of  $\mathbf{F}_p$  in a unique way (as the subfield generated by 1).

Theorems 1.9 and 2.2 tell us there is a monic irreducible  $\pi(x)$  such that  $x \pmod{\pi(x)}$  is a generator of the nonzero numbers in  $\mathbf{F}_p[x]/(\pi(x))$ . For instance, fields of size 9 that are of the form  $\mathbf{F}_p[x]/(\pi(x))$  need  $p = 3$  and  $\deg \pi(x) = 2$ . The monic irreducible quadratics in  $\mathbf{F}_3[x]$  are  $x^2 + 1$ ,  $x^2 + x + 2$ , and  $x^2 + 2x + 2$ . In the fields

$$\mathbf{F}_3[x]/(x^2 + 1), \quad \mathbf{F}_3[x]/(x^2 + x + 2), \quad \mathbf{F}_3[x]/(x^2 + 2x + 2),$$

$x$  is not a generator of the nonzero numbers in the first field but is a generator of the nonzero numbers in the second and third fields. So although the field  $\mathbf{F}_3[x]/(x^2 + 1)$  is the simplest choice among these three examples, it's not the one that would come out of the proof of Theorem 1.9 when we look for a polynomial quotient ring model of fields of order 9.

**Theorem 2.5.** *Any two finite fields of the same size are isomorphic.*

*Proof.* The size of a finite field must be a prime power, say  $p^n$ . By Lemma 2.1, any field of order  $p^n$  is a splitting field of  $x^{p^n} - x$  over  $\mathbf{F}_p$ .

By field theory, any two splitting fields of a fixed polynomial over  $\mathbf{F}_p$  are isomorphic, so any two fields of order  $p^n$  are isomorphic.  $\square$

The analogous theorem for finite groups and finite rings is false: having the same size in general does not imply isomorphism. For instance,  $\mathbf{Z}/(4)$  and  $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$  both have order 4 and they are nonisomorphic as additive groups and nonisomorphic as rings.

**Theorem 2.6.** *The subfields of  $\mathbf{F}_{p^n}$  have order  $p^d$  where  $d \mid n$ , and there is one such field for each  $d$ .*

*Proof.* Let  $F$  be a field with  $\mathbf{F}_p \subset F \subset \mathbf{F}_{p^n}$ . Set  $d = [F : \mathbf{F}_p]$ , so  $\#F = p^d$  and  $d$  divides  $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$ . We will describe  $F$  in a way that only depends on  $\#F$ , so  $F$  is the only subfield of its size in  $\mathbf{F}_{p^n}$ .

Since  $F^\times$  has order  $p^d - 1$ , for any  $t \in F^\times$  we have  $t^{p^d - 1} = 1$ , so  $t^{p^d} = t$ , and that holds even for  $t = 0$ . The polynomial  $x^{p^d} - x$  has at most  $p^d$  roots in  $\mathbf{F}_{p^n}$ , and since  $F$  is a set of  $p^d$  different roots,

$$F = \{t \in \mathbf{F}_{p^n} : t^{p^d} = t\}.$$

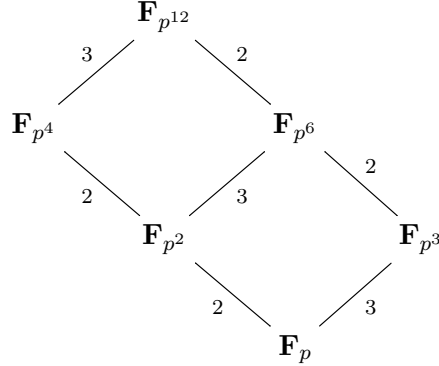
This shows there is at most one field of order  $p^d$  in  $\mathbf{F}_{p^n}$ , since the right side is completely determined as a subset of  $\mathbf{F}_{p^n}$  from knowing  $p^d$ .

To prove for each  $d \mid n$  that there really is a subfield of  $\mathbf{F}_{p^n}$  with order  $p^d$ , we turn things around and take the formula for  $F$  above as a definition. Consider the set

$$\{t \in \mathbf{F}_{p^n} : t^{p^d} = t\}.$$

This is a field by the same proof that  $S$  is a field in the proof of Theorem 2.2. To show its size is  $p^d$  we find  $p^d - 1$  nonzero numbers in  $\mathbf{F}_{p^n}$  satisfying the condition  $t^{p^d - 1} = 1$ . Let  $\gamma$  be a generator of  $\mathbf{F}_{p^n}^\times$ , so  $\gamma$  has multiplicative order  $p^n - 1$ . Since  $d \mid n$ ,  $(p^d - 1) \mid (p^n - 1)$ , so  $\alpha := \gamma^{(p^n - 1)/(p^d - 1)}$  has order  $p^d - 1$ . The powers  $\alpha^k$  ( $1 \leq k \leq p^d - 1$ ) all satisfy  $t^{p^d - 1} = 1$ .  $\square$

In the diagram below are the subfields of  $\mathbf{F}_{p^{12}}$ . It resembles the lattice of divisors of 12.



### 3. GALOIS GROUPS

The numbers in  $\mathbf{F}_{p^n}$  are a full set of roots of  $x^{p^n} - x$ , so  $\mathbf{F}_{p^n}$  is a splitting field over  $\mathbf{F}_p$  of this separable polynomial. Therefore  $\mathbf{F}_{p^n}/\mathbf{F}_p$  is a Galois extension: *every finite extension of  $\mathbf{F}_p$  is a Galois extension*. It is a fundamental feature of finite fields that the Galois group is cyclic, with a canonical generator.

**Theorem 3.1.** *The Galois group  $\text{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$  is cyclic and a generator is the  $p$ -th power map  $\varphi_p: t \mapsto t^p$ .*

*Proof.* Any  $a \in \mathbf{F}_p$  satisfies  $a^p = a$ , so the function  $\varphi_p: \mathbf{F}_{p^n} \rightarrow \mathbf{F}_{p^n}$  fixes  $\mathbf{F}_p$  pointwise. Also  $\varphi_p$  is a field homomorphism and it is injective (all field homomorphisms are injective), so  $\varphi_p$  is surjective since  $\mathbf{F}_{p^n}$  is finite. Therefore  $\varphi_p \in \text{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ .

The size of the group  $\text{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$  is  $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$ . We will show  $\varphi_p$  has order  $n$  in this group, so it generates the Galois group.

For  $r \geq 1$  and  $t \in \mathbf{F}_{p^n}$ ,  $\varphi_p^r(t) = t^{p^r}$ . If  $\varphi_p^r$  is the identity on  $\mathbf{F}_{p^n}$  then  $t^{p^r} = t$  for all  $t \in \mathbf{F}_{p^n}$ , which can be rewritten as  $t^{p^r} - t = 0$ . The polynomial  $x^{p^r} - x$  has degree  $p^r$  (since  $r \geq 1$ ) and therefore has at most  $p^r$  roots in a field, so  $p^n \leq p^r$ , so  $n \leq r$ . Thus  $\varphi_p$  has order at least  $n$  in  $\text{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ . Since the Galois group has order  $n$ , the order of  $\varphi_p$  in the Galois group has to be  $n$ , so  $\varphi_p$  generates the Galois group: every element of  $\text{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$  is an iterate of  $\varphi_p$ .  $\square$

**Example 3.2.** On  $\mathbf{F}_p$ ,  $\varphi_p$  is the identity (order 1). On  $\mathbf{F}_{p^2}$ ,  $\varphi_p$  has order 2 (it fixes  $\mathbf{F}_p$  but not  $\mathbf{F}_{p^2}$ , and its iterate  $\varphi_p^2$  fixes  $\mathbf{F}_{p^2}$ ). On  $\mathbf{F}_{p^4}$ ,  $\varphi_p$  has order 4. The same function  $\varphi_p$  has changing orders as an automorphism because the size of the field it acts on is changing.

**Remark 3.3.** Galois theory makes Theorem 2.6 a consequence of Theorem 3.1, since an extension with a cyclic Galois group must have its lattice of intermediate fields resemble the lattice of subgroups of a cyclic group.

**Theorem 3.4.** *If  $\pi(x) \in \mathbf{F}_p[x]$  is irreducible with degree  $d$  and it has a root  $\alpha$  in some extension field of  $\mathbf{F}_p$  then its full set of roots is  $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$ .*

*Proof.* We have seen already that any finite field of  $p$ -power order is Galois over  $\mathbf{F}_p$ . The field  $\mathbf{F}_p(\alpha)$  is finite, so it is Galois over  $\mathbf{F}_p$  and the roots of  $\pi(x)$  can be obtained from  $\alpha$  by applying  $\text{Gal}(\mathbf{F}_p(\alpha)/\mathbf{F}_p)$  to this root. Since the Galois group is generated by the  $p$ -th power map, the roots of  $\pi(x)$  are  $\alpha, \alpha^p, \alpha^{p^2}, \dots$ . Once we reach  $\alpha^{p^d}$  we have cycled back to the

start:  $\alpha^{p^d} = \alpha$  since  $\mathbf{F}_p(\alpha) \cong \mathbf{F}_p[x]/(\pi(x))$  has order  $p^d$ . Therefore the list  $\alpha, \alpha^p, \alpha^{p^2}, \dots$  of all possible roots of  $\pi(x)$  is  $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$ . This list of length  $d$  has to consist of *distinct* roots of  $\pi(x)$  because  $\pi(x)$  has degree  $d$  and is separable (Theorem 2.4).  $\square$

**Example 3.5.** The polynomial  $x^3 + x^2 + 1$  is irreducible in  $\mathbf{F}_2[x]$  since it's a cubic without roots in  $\mathbf{F}_2$ . In the field  $F = \mathbf{F}_2[y]/(y^3 + y^2 + 1)$ , one root of  $x^3 + x^2 + 1$  is  $y$  (we should write this as a coset, like  $\bar{y}$ , but we'll use  $y$ ). The other two roots in  $F$  are  $y^2$  and  $y^4$ .

Since  $y^3 + y^2 + 1 = 0$  in  $F$ , we get  $y^3 = y^2 + 1$  (since  $-1 = 1$ ), so  $y^4 = y^3 + y = (y^2 + 1) + y = y^2 + y + 1$ . Therefore, the roots of  $x^3 + x^2 + 1$  in  $F$  can be written as  $y, y^2$ , and  $y^2 + y + 1$ .

In  $F$ ,  $y+1$  is a root of  $x^3 + x + 1$ . The other two roots of this polynomial are  $(y+1)^2 = y^2 + 1$  and  $(y+1)^4 = (y^2 + 1)^2 = y^4 + 1 = (y^2 + y + 1) + 1 = y^2 + y$ .

**Example 3.6.** The polynomial  $x^3 - 2$  is irreducible over  $\mathbf{F}_7$  since it's a cubic without roots in  $\mathbf{F}_7$ . In the field  $\mathbf{F}_7[y]/(y^3 - 2)$ ,  $y^2 + y + 2$  has minimal polynomial  $x^3 + x^2 + 6x + 5$  over  $\mathbf{F}_7$ . The other roots of  $x^3 + x^2 + 6x + 5$  are  $(y^2 + y + 2)^7$  and  $(y^2 + y + 2)^{49}$ . Using the relation  $y^3 = 2$  and patience (or a computer), those powers can be simplified:  $(y^2 + y + 2)^7 = 2y^2 + 4y + 2$  and  $(y^2 + y + 2)^{49} = 4y^2 + 2y + 2$ .

#### 4. GENERAL FINITE BASE FIELDS

In addition to looking at finite extensions  $\mathbf{F}_p$ , which includes all fields of  $p$ -power order, we can look at finite extensions of a field  $\mathbf{F}_q$  of possibly non-prime size  $q$ . The number  $q$  is a prime power (e.g.  $q = 4$  or  $q = 27$ ). Every  $a \in \mathbf{F}_q$  satisfies  $a^q = a$ , which will be the substitute for every element  $a$  of  $\mathbf{F}_p$  satisfying  $a^p = a$ . The key change that happens when working over  $\mathbf{F}_q$  compared to working over  $\mathbf{F}_p$  is that the  $p$ -th power map (which fixes the elements of  $\mathbf{F}_p$ ) is replaced with the  $q$ -th power map (which fixes the elements of  $\mathbf{F}_q$ ). Writing  $q$  as the prime power  $p^r$ , say, the  $q$ -th power map on a field  $\mathbf{F}_{q^n} = \mathbf{F}_{p^{rn}}$  is a particular iteration of the  $p$ -th power map, and thus is an isomorphism of  $\mathbf{F}_{q^n}$  to itself. The following theorems are analogues over  $\mathbf{F}_q$  of some results over  $\mathbf{F}_p$ . Proofs are left to the reader.

**Theorem 4.1.** *For any positive integer  $n$ , there is a monic irreducible of degree  $n$  in  $\mathbf{F}_q[x]$ .*

**Theorem 4.2.** *Between  $\mathbf{F}_q$  and  $\mathbf{F}_{q^n}$  there is one field of each order  $q^d$  where  $d|n$ . The field of order  $q^d$  inside  $\mathbf{F}_{q^n}$  can be described as  $\{t \in \mathbf{F}_{q^n} : t^{q^d} = t\}$ .*

**Theorem 4.3.** *For any integer  $n \geq 1$ ,  $\mathbf{F}_{q^n}/\mathbf{F}_q$  is a Galois extension and the Galois group  $\text{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$  is cyclic with generator the  $q$ -th power map  $\varphi_q: t \mapsto t^q$ .*

**Theorem 4.4.** *If  $\pi(x) \in \mathbf{F}_q[x]$  is irreducible with degree  $d$  and it has a root  $\alpha$  in some extension field of  $\mathbf{F}_q$  then its full set of roots is  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$ .*

#### 5. HISTORY

Fields of prime order, namely  $\mathbf{Z}/(p)$ , were the subject of study by many of the early number theorists such as Fermat, Euler, Lagrange, Legendre, and Gauss. The first mathematician to write about other finite fields was Galois, who published a paper on them in 1830. (Gauss had done work on finite fields of nonprime size earlier [1], but this was discovered only after his death in 1855 and published in 1863 without having much influence.) Galois constructed finite fields as  $\mathbf{F}_p(\alpha)$  where  $\alpha$  is the root of an irreducible polynomial

$\pi(x)$  in  $\mathbf{F}_p[x]$ . This is equivalent to working in  $\mathbf{F}_p[x]/(\pi(x))$ . Galois did not show there is an irreducible in  $\mathbf{F}_p[x]$  of every degree.

In 1893, at the International Mathematical Congress in Chicago, E. H. Moore proved that any finite field is isomorphic to a field of the form  $\mathbf{F}_p[x]/(\pi(x))$ , a theorem which he described with the comment [3, p. 211] “This interesting result I have not seen stated elsewhere.” Moore was the first person to use the word field in its algebraic sense, although he treated it as a synonym for the German term *endlicher Körper*, which means finite field [3, p. 208]. So to Moore, field meant what we’d call a finite field. He called any field constructed in the concrete form  $\mathbf{F}_p[x]/(\pi(x))$  a *Galois field*, so for Moore a Galois field is a particular type of concrete model for finite fields. Nowadays in algebra, the word field is not limited to finite fields, and the term Galois field is obsolete. However, in computer science the term Galois field lives on today as a synonym for finite field (even abstract ones) and Moore’s notation  $\text{GF}(q)$  is often used in computer science in place of  $\mathbf{F}_q$ .

#### APPENDIX A. DESCRIBING $\mathbf{F}_p$ -CONJUGATES WITHOUT GALOIS GROUPS

Theorem 2.6 was proved without any mention of Galois theory, and we pointed out in Remark 3.3 that it is an immediate consequence of Galois groups of finite fields being cyclic. In this appendix we will show how Theorem 3.4 can be proved without direct mention of Galois groups either. The argument is somewhat longer.

**Theorem A.1.** *For any  $f(x) \in \mathbf{F}_p[x]$ ,  $f(x)^{p^m} = f(x^{p^m})$  for  $m \geq 0$ .*

*Proof.* The case  $m = 0$  is obvious, and it suffices by induction to do the case  $m = 1$ .

In any ring of characteristic  $p$ , the  $p$ th power map is additive. For a polynomial  $f(x) = c_n x^n + \cdots + c_1 x + c_0$  in the ring  $\mathbf{F}_p[x]$ , we have

$$f(x)^p = (c_n x^n + \cdots + c_1 x + c_0)^p = c_n^p x^{pn} + \cdots + c_1^p x^p + c_0^p.$$

Every  $c \in \mathbf{F}_p$  satisfies  $c^p = c$ , so

$$f(x)^p = c_n x^{pn} + \cdots + c_1 x^p + c_0 = f(x^p).$$

□

**Example A.2.** In  $\mathbf{F}_5[x]$ ,  $(2x^4 + x^2 + 3)^5 = 2x^{20} + x^{10} + 3$ .

**Theorem A.3.** *Let  $\pi(x)$  be irreducible of degree  $d$  in  $\mathbf{F}_p[x]$ .*

- a) *In  $\mathbf{F}_p[x]$ ,  $\pi(x)|(x^{p^d} - x)$ .*
- b) *For  $n \geq 0$ ,  $\pi(x)|(x^{p^n} - x) \iff d|n$ .*

*Proof.* The divisibility in (a) is the same as the congruence  $x^{p^d} \equiv x \pmod{\pi(x)}$ , or equivalently the equation  $x^{p^d} = x$  in  $\mathbf{F}_p[x]/(\pi)$ . Such an equation follows immediately from the fact that  $t^{p^d} = t$  for every element  $t$  of any field of order  $p^d$ .

To prove  $(\Leftarrow)$  in (b), write  $n = kd$ . Starting with  $x^{p^d} \equiv x \pmod{\pi}$  (from (a)) and applying the  $p^d$ -th power to both sides  $k$  times, we obtain

$$x \equiv x^{p^d} \equiv x^{p^{2d}} \equiv \cdots \equiv x^{p^{kd}} \pmod{\pi}.$$

Thus  $\pi(x)|(x^{p^n} - x)$ .

Now we prove  $(\Rightarrow)$  in (b). We assume

$$(A.1) \quad x^{p^n} \equiv x \pmod{\pi}$$

and want to show  $d|n$ . Write  $n = dq + r$  with  $0 \leq r < d$ . We will show  $r = 0$ .

We have  $x^{p^n} = x^{p^{dq}p^r} = (x^{p^{dq}})^{p^r}$ . By  $(\Leftarrow)$ ,  $x^{p^{dq}} \equiv x \pmod{\pi}$ , so  $x^{p^n} \equiv x^{p^r} \pmod{\pi}$ . Thus, by (A.1),

$$(A.2) \quad x^{p^r} \equiv x \pmod{\pi}.$$

This tells us that one particular element of  $\mathbf{F}_p[x]/(\pi)$ , the class of  $x$ , is equal to its own  $p^r$ -th power. Let's extend this property to all elements of  $\mathbf{F}_p[x]/(\pi)$ . For any  $f(x) \in \mathbf{F}_p[x]$ ,  $f(x)^{p^r} = f(x^{p^r})$  by Theorem A.1. Combining with (A.2),

$$f(x)^{p^r} \equiv f(x) \pmod{\pi}.$$

Therefore, in  $\mathbf{F}_p[x]/(\pi)$ , the class of  $f(x)$  is equal to its own  $p^r$ -th power. As  $f(x)$  is a general polynomial in  $\mathbf{F}_p[x]$ , we have proved every  $a \in \mathbf{F}_p[x]/(\pi)$  satisfies  $a^{p^r} = a$  (in  $\mathbf{F}_p[x]/(\pi)$ ). Recall  $r$  is the remainder when  $n$  is divided by  $d$ .

Consider now the polynomial  $X^{p^r} - X$ . When  $r > 0$ , this is a polynomial with degree  $p^r$ . We have found  $p^d$  different roots of this polynomial in the field  $\mathbf{F}_p[x]/(\pi)$ , namely every element. Therefore  $p^d \leq p^r$ , so  $d \leq r$ . But, recalling where  $r$  came from,  $r < d$ . This is a contradiction, so  $r = 0$ . That proves  $d|n$ .  $\square$

**Theorem A.4.** *Let  $\pi(x)$  be irreducible in  $\mathbf{F}_p[x]$  with degree  $d$  and  $E \supset \mathbf{F}_p$  be a field in which  $\pi(x)$  has a root, say  $\alpha$ . Then  $\pi(x)$  has roots  $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$ . These  $d$  roots are distinct; more precisely, when  $i$  and  $j$  are nonnegative,  $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \pmod{d}$ .*

*Proof.* Since  $\pi(x)^p = \pi(x^p)$  by Theorem A.1, we see  $\alpha^p$  is also a root of  $\pi(x)$ , and likewise  $\alpha^{p^2}, \alpha^{p^3}$ , and so on by iteration. Once we reach  $\alpha^{p^d}$  we have cycled back to the start:  $\alpha^{p^d} = \alpha$  by Theorem A.3a. (Write the divisibility in Theorem A.3a as an equation in  $\mathbf{F}_p[x]$  and then substitute  $\alpha$  for  $x$ .)

Now we will show  $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \pmod{d}$ , where  $i, j \geq 0$ . Since  $\alpha^{p^d} = \alpha$ , the implication  $(\Leftarrow)$  is straightforward. To argue in the other direction, we may suppose without loss of generality that  $i \leq j$ , say  $j = i + k$  with  $k \geq 0$ . Then

$$\alpha^{p^i} = \alpha^{p^j} \implies \alpha^{p^i} = (\alpha^{p^k})^{p^i}.$$

We conclude  $\alpha = \alpha^{p^k}$  by Lemma ??b. Therefore  $\pi(x)|(x^{p^k} - x)$  in  $\mathbf{F}_p[x]$  (why?), so  $d|k$  by Theorem A.3b. Thus,  $i \equiv j \pmod{d}$ .  $\square$

Since  $\pi(x)$  has at most  $d = \deg \pi$  roots in any field, Theorem A.4 tells us  $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$  are a complete set of roots of  $\pi(x)$ : in  $E[x]$ ,  $\pi(x)$  decomposes into (distinct!) linear factors.

The results we worked out in this appendix over  $\mathbf{F}_p$  adapt with little change to polynomials with coefficients in a general finite field  $\mathbf{F}_q$ , of possible nonprime order.

**Theorem A.5.** *For any  $f(x) \in \mathbf{F}_q[x]$ ,  $f(x)^{q^m} = f(x^{q^m})$  for  $m \geq 0$ .*

**Theorem A.6.** *Let  $\pi(x)$  be irreducible of degree  $d$  in  $\mathbf{F}_q[x]$ .*

- a) *In  $\mathbf{F}_q[x]$ ,  $\pi(x)|(x^{q^d} - x)$ .*
- b) *For  $n \geq 0$ ,  $\pi(x)|(x^{q^n} - x) \iff d|n$ .*

**Theorem A.7.** *Let  $\pi(x)$  be irreducible in  $\mathbf{F}_q[x]$  with degree  $d$  and  $E \supset \mathbf{F}_q$  be a field in which  $\pi(x)$  has a root, say  $\alpha$ . Then  $\pi(x)$  has roots  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$ . These  $d$  roots are distinct; more precisely, when  $i$  and  $j$  are nonnegative,  $\alpha^{q^i} = \alpha^{q^j} \iff i \equiv j \pmod{d}$ .*

## REFERENCES

- [1] G. Frei, *The Unpublished Section Eight: On the Way to Function Fields over a Finite Field*, pp. 159–198 in “The Shaping of Arithmetic after C. F. Gauss’s *Disquisitiones Arithmeticae*,” ed. C. Goldstein, N. Schappacher, J. Schwermer, Springer-Verlag, Berlin, 2007.
- [2] E. Galois, *Sur la théorie de nombres*, Bulletin des Sciences Mathématiques de Férussac **13** (1830), 428–435. (Also *Collected Works*, 1897, pp. 15–23.)
- [3] E. H. Moore *A Doubly-Infinite System of Simple Groups*, pp. 208–242 in “Mathematical papers read at the International Mathematical Congress held in connection with the World’s Columbian Exposition, Chicago, 1893,” Macmillan & Co., New York, 1896.