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. 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.
- All finite fields of the same size are isomorphic (usually not in just one way).
- If $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = d$, the $\mathbf{F}_p$-conjugates of α are $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$.
- 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.

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

$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}, \quad c_i \in \mathbf{F}_p,$$

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. □

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 fields of order 8 or 9 as $\mathbf{Z}/(8)$ or $\mathbf{Z}/(9)$. Those are not fields! 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 look at something other than the rings $\mathbf{Z}/(m)$.

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 every finite field. However, not every finite field is literally of the form $\mathbf{F}_p[x]/(\pi(x))$. For instance, $\mathbf{Z}[\sqrt{2}]/(3)$ is another field of size 9 (which is isomorphic to $\mathbf{F}_3[x]/(x^2 - 2) = \mathbf{F}_3[x]/(x^2 + 1)$).

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

Proof. For each commutative ring R there is a unique ring homomorphism $\mathbf{Z} \to R$, where

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

We apply this to the case when $R = F$ is a finite field. The kernel of $\mathbf{Z} \to F$ 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. A subring of a field is a domain, so m has to be a prime number, say $m = p$. Therefore there is an embedding $\mathbf{Z}/(p) \hookrightarrow F$. Viewing F as a vector space over $\mathbf{Z}/(p)$, it is finite-dimensional since F is finite. Letting $n = \dim_{\mathbf{Z}/(p)}(F)$ and picking a basis $\{e_1, \ldots, e_n\}$ for F over $\mathbf{Z}/(p)$, elements of F can be written uniquely as

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

Each coefficient has p choices, so $|F| = p^n$. □

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

Proof. Let $q = |F|$, so $|F^\times| = q - 1$. Let m be the maximal order of the elements of the group $F^\times$, so $m \mid (q-1)$ by Lagrange's theorem. We will show $m = q - 1$.

It is a theorem from group theory (see the appendix) that in a finite *abelian* group, all orders of elements divide the maximal order of the elements[1], so every t in $F^\times$ satisfies $t^m = 1$. Therefore all elements of $F^\times$ are roots of the polynomial $x^m - 1$. The number of roots of a polynomial over a field is at most the degree of the polynomial, so $q - 1 \leq m$.

Since m is the order of some element in $F^\times$, we have $m \mid (q-1)$, so $m \leq q-1$. Therefore $m = q - 1$, so some element of $F^\times$ has order $q - 1$. □

Example 1.7. In $F := \mathbf{F}_3[x]/(x^2+1)$, there are 8 nonzero elements. The powers of x are

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

so x does not generate $F^\times$. But $x+1$ does: its powers are in the table below.

k	1	2	3	4	5	6	7	8
$(x+1)^k$	$x+1$	$2x$	$2x+1$	2	$2x+2$	x	$x+2$	1

Example 1.8. For prime p, $(\mathbf{Z}/(p))^\times$ is cyclic: $(\mathbf{Z}/(p))^\times = \{a, a^2, \ldots, a^{p-1} \bmod p\}$ for some $a \not\equiv 0 \bmod p$. A constructive proof of this, using the prime factorization of $p-1$, is in Section 6 of https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf.

Remark 1.9. For a finite field F, the multiplicative group $F^\times$ is cyclic but the additive group of F is usually *not* cyclic. When F contains $\mathbf{F}_p$, since $p = 0$ in $\mathbf{F}_p$ every nonzero element of F has additive order p, so F is not additively cyclic unless $|F|$ is prime.

Theorem 1.10. *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 γ be a generator of $F^\times$. Evaluation at γ, namely $f(x) \mapsto f(\gamma)$, is a ring homomorphism $\mathrm{ev}_\gamma \colon \mathbf{F}_p[x] \to F$ that fixes $\mathbf{F}_p$. Since every

[1]In a nonabelian finite 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.

element of F is 0 or a power of γ, ev_γ is onto ($0 = \mathrm{ev}_\gamma(0)$ and $\gamma^r = \mathrm{ev}_\gamma(x^r)$ for all $r \geq 0$). Therefore $\mathbf{F}_p[x]/\ker \mathrm{ev}_\gamma \cong F$. Since F is a field, the kernel of ev_γ is a maximal ideal in $\mathbf{F}_p[x]$, so $\ker \mathrm{ev}_\gamma = (\pi(x))$ for a monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$. □

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

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

x does not generate the nonzero elements in the first field but it generates the nonzero elements in the second and third fields. So although $\mathbf{F}_3[x]/(x^2 + 1)$ is the simplest choice among these three examples, it's *not* the one that would come out of the proof of Theorem 1.10 when we look for a model of fields of order 9 as $\mathbf{F}_3[x]/(\pi(x))$.

Theorem 1.10 does not assure us that a field of each prime power order exists. 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 $\mathbf{F}_p[x]$. Why is there an irreducible of each degree in $\mathbf{F}_p[x]$? In the next section we will show a field of each prime power order does exist and there is an irreducible in $\mathbf{F}_p[x]$ of each positive degree.

2. Finite fields as splitting fields

Each finite field is a splitting field of a polynomial depending only on the field's size.

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 $\mathbf{F}_p$. □

Theorem 2.2. *For every 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

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

We will show S is a subfield of F and then $|S| = p^n$.

Since S contains 1 and is easily closed under multiplication and (for nonzero solutions) inversion, for S to be a subfield of F we only need to show it 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 and thus vanish in F). Therefore the p-th power map $t \mapsto t^p$ on F is additive. The map $t \mapsto t^{p^n}$ is also additive since it's the n-fold composite of $t \mapsto t^p$ with itself and the composition of homomorphisms is a homomorphism.[2] The fixed points of an additive map are a group under addition, so S is a group under addition. Therefore S is a field.

[2]Alternatively, additivity of $t \mapsto t^{p^n}$ follows from the binomial coefficients $\binom{p^n}{k}$ being divisible by p for $1 \leq k \leq p^n - 1$. In general $b\binom{a}{b} = a\binom{a-1}{b-1}$ for $1 \leq b \leq a$, so $k\binom{p^n}{k} = p^n\binom{p^n-1}{k-1}$ when $1 \leq k \leq p^n - 1$. Thus $k\binom{p^n}{k}$ is divisible by p^n and the first factor k is not divisible by p^n, so $\binom{p^n}{k}$ is divisible by p.

To show $|S| = p^n$ we show $x^{p^n} - x$ is separable in two ways: (i) $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$ since $p = 0$ in F, so $x^{p^n} - x$ has no roots in common with its derivative, and (ii) if r is a root then by additivity of the p-th power map in $F[x]$ (same reason as its additivity in F),

$$x^{p^n} - x = x^{p^n} - x - (r^{p^n} - r) = (x - r)^{p^n} - (x - r) = (x - r)((x - r)^{p^n} - 1) = (x - r)g(x)$$

and $g(r) = -1 \neq 0$. Since $x^{p^n} - x$ splits completely in $F[x]$ and has degree p^n without repeated roots, $|S| = p^n$. □

Corollary 2.3. *For every prime p and positive integer n, there is a monic irreducible $\pi(x)$ of degree n in $\mathbf{F}_p[x]$, and moreover $\pi(x)$ can be chosen so that $x \bmod \pi(x)$ generates the nonzero elements of $\mathbf{F}_p[x]/(\pi(x))$.*

Proof. By Theorem 2.2, a field F of order p^n exists. By Theorem 1.10, 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, and from the proof of Theorem 1.10 $x \bmod \pi(x)$ generates the nonzero elements of $\mathbf{F}_p[x]/(\pi(x))$ since the isomorphism identifies $x \bmod \pi(x)$ with a generator of $F^\times$. □

Appreciate the order in the logic behind Theorem 2.2 and its corollary: to show we can construct a field of order p^n as $\mathbf{F}_p[x]/(\pi(x))$ where $\deg \pi(x) = n$, the way we showed a $\pi(x)$ of degree n exists is by *first* constructing an abstract field F of order p^n (using a splitting field construction) and then proving F can be made isomorphic to an $\mathbf{F}_p[x]/(\pi(x))$.

Remark 2.4. There is no formula for an irreducible of *each* degree in $\mathbf{F}_p[x]$. Binomial polynomials $x^n - a$ are reducible when $p \mid n$. Trinomials $x^n + ax^k + b$ with $a, b \in \mathbf{F}_p^\times$ and $0 < k < n$ are often irreducible, but in some degrees they are all reducible: that occurs in $\mathbf{F}_2[x]$ in degrees 8 and 13, in $\mathbf{F}_3[x]$ in degrees 49 and 57, in $\mathbf{F}_5[x]$ in degrees 35 and 70, and in $\mathbf{F}_7[x]$ in degrees 124 and 163.

Theorem 2.5. *Each irreducible $\pi(x)$ in $\mathbf{F}_p[x]$ of degree n divides $x^{p^n} - x$ and is separable.*

Proof. The field $\mathbf{F}_p[x]/(\pi(x))$ has order p^n, so $t^{p^n} = t$ for all t in $\mathbf{F}_p[x]/(\pi(x))$ (see the proof of Lemma 2.1). In particular, $x^{p^n} \equiv x \bmod \pi(x)$, so $\pi(x) \mid (x^{p^n} - x)$ in $\mathbf{F}_p[x]$. We saw in the proof of Theorem 2.2 that $x^{p^n} - x$ is separable in $\mathbf{F}_p[x]$, so its factor $\pi(x)$ is separable. □

Example 2.6. In $\mathbf{F}_2[x]$, the irreducible factorization of $x^{2^n} - x$ for $n = 1, 2, 3, 4$ is as follows.

$$\begin{aligned}
x^2 - x &= x(x-1), \\
x^4 - x &= x(x-1)(x^2 + x + 1), \\
x^8 - x &= x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1), \\
x^{16} - x &= x(x-1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).
\end{aligned}$$

In each case the irreducibles of degree n appear in the factorization of $x^{2^n} - x$, which Theorem 2.5 guarantees must happen. That each factor occurs just once reflects the fact that $x^{p^n} - x$ is separable. There are irreducible factors of $x^{p^n} - x$ with degree less than n, if $n > 1$; the irreducible factors of $x^{p^n} - x$ in $\mathbf{F}_p[x]$ turn out (Theorem 3.3 below) to be the irreducibles in $\mathbf{F}_p[x]$ of degree dividing n and each such factor appears once.

We write $\mathbf{F}_{p^n}$ for a finite field of order p^n. Features to keep in mind are

- it contains a unique subfield isomorphic to $\mathbf{F}_p$ (namely the subfield generated by 1),
- $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$ by the proof of Theorem 1.5,
- it is a splitting field of $x^{p^n} - x$ over $\mathbf{F}_p$ by the proof of Theorem 2.2.

Although $x^{p^n} - x$ has degree p^n, its splitting field over $\mathbf{F}_p$ has degree n, *not* p^n. That is not weird, because $x^{p^n} - x$ is reducible (see Example 2.6). The situation is similar to $x^m - 1$, which for $m > 1$ is reducible and its splitting field over $\mathbf{Q}$ has degree less than m.

Theorem 2.7. *All finite fields of the same size are isomorphic to each other.*

Proof. A finite field has prime power size, say p^n. By Lemma 2.1, it is a splitting field of $x^{p^n} - x$ over $\mathbf{F}_p$. Two splitting fields of a polynomial over $\mathbf{F}_p$ are isomorphic (that is, there is a bijective homomorphism between them), so fields of order p^n are isomorphic. □

For finite groups and finite rings, having the same size does not usually imply isomorphism. For instance, $\mathbf{Z}/(4)$ and $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ have order 4 and they are nonisomorphic as additive groups (one is cyclic and the other is not) and as commutative rings (one has a nonzero element squaring to 0 and other does not).

Theorem 2.8. *A subfield of $\mathbf{F}_{p^n}$ has order p^d where $d \mid n$, and there is one such subfield 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 d divides $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. We will describe F in a way that only depends on $|F| = p^d$.

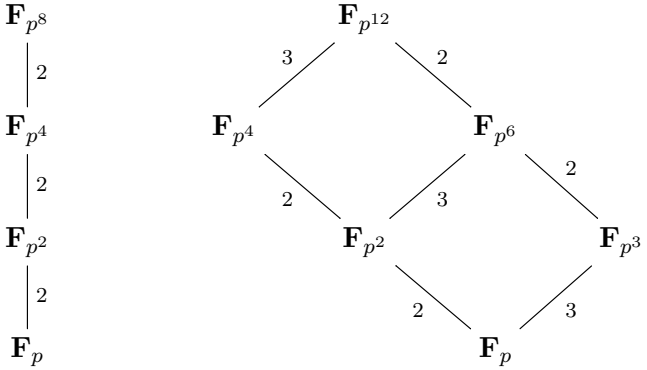
Since $F^\times$ has order $p^d - 1$, for all $t \in F^\times$ we have $t^{p^d-1} = 1$, so $t^{p^d} = t$, and that holds even for $t = 0$. The polynomial $x^{p^d} - x$ has at most p^d roots in $\mathbf{F}_{p^n}$, and since F is a set of p^d different roots of it,

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

This shows there is at most one subfield 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 dividing n there is a subfield of $\mathbf{F}_{p^n}$ with order p^d, we turn things around and consider $\{t \in \mathbf{F}_{p^n} : t^{p^d} = t\}$. It is a field by the same proof that S is a field in the proof of Theorem 2.2. To show $|S| = p^d$ we want to show $x^{p^d} - x$ has p^d roots in $\mathbf{F}_{p^n}$. We'll do this in two ways. First, $d \mid n \Rightarrow (p^d - 1) \mid (p^n - 1) \Rightarrow x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \Rightarrow x^{p^d} - x \mid x^{p^n} - x$, so since $x^{p^n} - x$ splits with distinct roots in $\mathbf{F}_{p^n}[x]$, its factor $x^{p^d} - x$ does too. Second, $d \mid n \Rightarrow (p^d - 1) \mid (p^n - 1)$ and $\mathbf{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, so it contains $p^d - 1$ solutions to $t^{p^d-1} = 1$. Along with 0 we get p^d solutions in $\mathbf{F}_{p^n}$ to $t^{p^d} = t$. □

Example 2.9. In the diagram below are the subfields of $\mathbf{F}_{p^8}$ and $\mathbf{F}_{p^{12}}$.



These resemble the lattice of divisors of 8 and divisors of 12. Even though p^k divides p^{12} for $k \leq 12$, that does not mean $\mathbf{F}_{p^k} \subset \mathbf{F}_{p^{12}}$ for $k \leq 12$: the only $\mathbf{F}_{p^k}$ that can lie in $\mathbf{F}_{p^{12}}$

are those for which $[\mathbf{F}_{p^k} : \mathbf{F}_p]$ divides $[\mathbf{F}_{p^{12}} : \mathbf{F}_p]$, which means k divides 12. Theorem 2.8 guarantees when $k \mid 12$ that elements of $\mathbf{F}_{p^k}$ are solutions to $t^{p^k} = t$ in $\mathbf{F}_{p^{12}}$.

Example 2.10. One field of order $16 = 2^4$ is $\mathbf{F}_2[x]/(x^4+x+1)$. All elements satisfy $t^{16} = t$. The solutions to $t^2 = t$ are the subfield $\{0, 1\}$ of order 2 and the solutions to $t^4 = t$ are the subfield $\{0, 1, x^2 + x, x^2 + x + 1\}$ of order 4.

3. Describing $\mathbf{F}_p$-conjugates

Two elements in a finite field are called $\mathbf{F}_p$-*conjugate* if their minimal polynomials over $\mathbf{F}_p$ agree. We will show that $\mathbf{F}_p$-conjugates can be obtained from each other by successive p-th powers. A precise statement is in Theorem 3.4.

Lemma 3.1. *For every $f(x) \in \mathbf{F}_p[x]$, $f(x)^{p^m} = f(x^{p^m})$ for $m \geq 0$.*

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

In a 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

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

Example 3.2. In $\mathbf{F}_5[x]$, $(2x^4 + x^2 + 3)^5 = 2x^{20} + x^{10} + 3$.

Theorem 3.3. *For irreducible $\pi(x)$ in $\mathbf{F}_p[x]$ of degree d and $n \geq 0$, $\pi(x) \mid (x^{p^n} - x) \iff d \mid n$.*

Proof. We will prove ($\Longleftarrow$) in two ways using Theorem 2.5, which is a special case. For the first proof, write $n = kd$. Starting with $x^{p^d} \equiv x \bmod \pi(x)$ (from Theorem 2.5) and applying the p^d-th power to both sides k times, we obtain

$$x \equiv x^{p^d} \equiv x^{p^{2d}} \equiv \cdots \equiv x^{p^{kd}} \bmod \pi(x).$$

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

For the second proof, $\pi(x) \mid (x^{p^d} - x)$ by Theorem 2.5, and $(x^{p^d} - x) \mid (x^{p^n} - x)$ by the proof of Theorem 2.8.

We will prove ($\Longrightarrow$) in two ways. For the first proof we will work in a field $\mathbf{F}_{p^n}$ of order p^n. Since $x^{p^n} - x$ splits completely in $\mathbf{F}_{p^n}[x]$ and $\pi(x)$ is a factor of $x^{p^n} - x$, $\pi(x)$ splits completely in $\mathbf{F}_{p^n}[x]$, so $\pi(x)$ has a root in $\mathbf{F}_{p^n}$, say α. Then $\mathbf{F}_{p^n}$ has the subfield $\mathbf{F}_p(\alpha)$, which has order p^d. Since $[\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ divides $[\mathbf{F}_{p^n} : \mathbf{F}_p]$, we get $d \mid n$.

The second proof uses congruences, not splitting fields. Our divisibility hypothesis says

$$x^{p^n} \equiv x \bmod \pi(x) \tag{3.1}$$

and we want to conclude $d \mid n$. 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 ($\Longleftarrow$), $x^{p^{dq}} \equiv x \bmod \pi$, so $x^{p^n} \equiv x^{p^r} \bmod \pi$. Thus

$$x^{p^r} \equiv x \bmod \pi(x) \tag{3.2}$$

by (3.1). This tells us that in the field $F := \mathbf{F}_p[x]/(\pi(x))$, the congruence class of x is equal to its own p^r-th power. Let's extend this property to all elements of F. For every $f(x) \in \mathbf{F}_p[x]$, $f(x)^{p^r} = f(x^{p^r})$ in $\mathbf{F}_p[x]$ by Lemma 3.1. Combining that with (3.2),

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

Therefore in F, the congruence 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 $t \in F$ satisfies $t^{p^r} = t$ in F. Recall r is the remainder when n is divided by d.

Consider now the polynomial $T^{p^r} - T$ in $F[T]$. When $r > 0$, this is a nonzero polynomial with degree p^r. We have found p^d different roots of this polynomial in the field F, 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 $d \mid n$. □

Theorem 3.4. *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 α. Then $\pi(x)$ has roots $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$. These d roots are distinct; more precisely, when i and j are nonnegative, $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \bmod d$.*

Proof. Since $\pi(x)^p = \pi(x^p)$ by Lemma 3.1, we see α^p is also a root of $\pi(x)$, and likewise $\alpha^{p^2}, \alpha^{p^3}$, and so on by iteration. Once we reach α^{p^d} we have cycled back to the start: $\alpha^{p^d} = \alpha$ by Theorem 3.3: $x^{p^d} = x + \pi(x)g(x)$ for some $g(x) \in \mathbf{F}_p[x]$, and substitute α for x.

Now we will show $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \bmod d$, where $i, j \geq 0$. We may suppose without loss of generality that $i \leq j$, say $j = i + k$ with $k \geq 0$. Then

$$\begin{aligned} \alpha^{p^i} = \alpha^{p^j} &\iff \alpha^{p^i} = (\alpha^{p^k})^{p^i} \\ &\iff (\alpha^{p^k})^{p^i} - \alpha^{p^i} = 0 \\ &\iff (\alpha^{p^k} - \alpha)^{p^i} = 0 \\ &\iff \alpha^{p^k} - \alpha = 0. \end{aligned}$$

Since $\pi(x)$ is irreducible in $\mathbf{F}_p[x]$ and has α as a root, $\pi(x)$ up to scaling is the minimal polynomial of α over $\mathbf{F}_p$. So $\pi(x)$ divides each polynomial in $\mathbf{F}_p[x]$ vanishing at α. Thus

$$\begin{aligned} \alpha^{p^i} = \alpha^{p^j} &\iff \pi(x) \mid (x^{p^k} - x) \text{ in } \mathbf{F}_p[x] \\ &\iff d \mid k \text{ by Theorem 3.3} \\ &\iff i \equiv j \bmod d. \end{aligned}$$

Since $0, 1, \ldots, d-1$ are not congruent modulo d, the above equivalence tells us that the roots $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ are distinct. That implies $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ are a complete set of roots of $\pi(x)$, since $\pi(x)$ has at most $d = \deg \pi$ roots in a field. □

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

Since $y^3 + y^2 + 1 = 0$ in F, we have $y^3 = y^2 + 1$ (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 are y, y^2, and $y^2 + y + 1$.

Example 3.6. The polynomial $x^3 - 2$ is irreducible in $\mathbf{F}_7[x]$. In the field $F = \mathbf{F}_7[y]/(y^3 - 2)$, $x^3 - 2$ has roots y, y^7, and y^{49}. Since $y^3 = 2$ in F, $y^7 = (y^3)^2 y = 4y$ and $y^{49} = (y^7)^7 = (4y)^7 = 4^7 y^7 = 4 \cdot 4y = 2y$. So the roots of $x^3 - 2$ in F are y, $2y$, and $4y$. This is like the formula for roots of $x^3 - 2$ in $\mathbf{C}$: $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. In characteristic 7, the numbers 2 and 4 are nontrivial cube roots of unity, so they are like ω and ω^2 in $\mathbf{C}$.

Theorem 3.4 says if $\pi(x) \in \mathbf{F}_p[x]$ is irreducible and α is a root of $\pi(x)$ then $\mathbf{F}_p(\alpha)$ is a splitting field of $\pi(x)$ over $\mathbf{F}_p$. This is quite different over $\mathbf{Q}$: $\mathbf{Q}(\sqrt[3]{2})$ is not a splitting field of $x^3 - 2$ over $\mathbf{Q}$. Here is an even more striking contrast between $\mathbf{Q}$ and $\mathbf{F}_p$.

Corollary 3.7. *Let $\pi_1(x)$ and $\pi_2(x)$ be irreducible of the same degree in $\mathbf{F}_p[x]$ and α be a root of $\pi_1(x)$ in an extension field of $\mathbf{F}_p$. Then $\mathbf{F}_p(\alpha)$ is a splitting field of $\pi_2(x)$ over $\mathbf{F}_p$.*

Proof. Set $n = \deg \pi_1(x) = \deg \pi_2(x)$ and $F = \mathbf{F}_p(\alpha) \cong \mathbf{F}_p[x]/(\pi_1(x))$, so F has order p^n. The polynomial $x^{p^n} - x$ splits completely over F (Lemma 2.1), and $\pi_2(x) \mid (x^{p^n} - x)$ in $\mathbf{F}_p[x]$ (Theorem 2.5), so $\pi_2(x)$ splits completely over F. Letting β be a root of $\pi_2(x)$ in F, $\mathbf{F}_p(\beta)$ has order p^n so $F = \mathbf{F}_p(\beta)$. Theorem 3.4 implies that F is a splitting field of $\pi_2(x)$ over $\mathbf{F}_p$. □

Example 3.8. Both $x^3 - 2$ and $x^3 + x^2 + 6x + 5$ are irreducible over $\mathbf{F}_7$. Let α be a root of $x^3 - 2$ over $\mathbf{F}_7$. In $\mathbf{F}_7(\alpha)$, $x^3 + x^2 + 6x + 5$ must have 3 roots. One root is $\alpha^2 + \alpha + 2$ (found by a search). Using the relation $\alpha^3 = 2$, the other two roots of $x^3 + x^2 + 6x + 5$ in $\mathbf{F}_7(\alpha)$ are $(\alpha^2 + \alpha + 2)^7 = 2\alpha^2 + 4\alpha + 2$ and $(\alpha^2 + \alpha + 2)^{49} = 4\alpha^2 + 2\alpha + 2$.

4. Galois groups

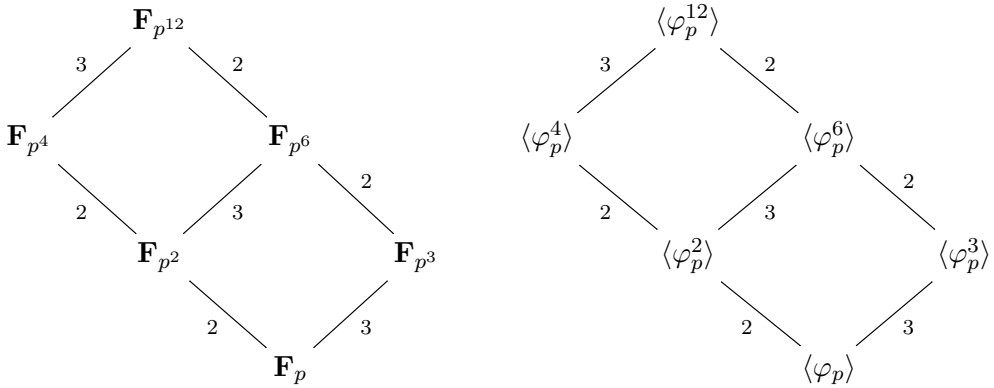
Since $\mathbf{F}_{p^n}$ is the splitting field over $\mathbf{F}_p$ of $x^{p^n} - x$, which is separable, $\mathbf{F}_{p^n}/\mathbf{F}_p$ is Galois. It is a fundamental feature that the Galois group is cyclic, with a canonical generator.

Theorem 4.1. *The p-th power map $\varphi_p \colon t \mapsto t^p$ on $\mathbf{F}_{p^n}$ generates* $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$.

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

The size of $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ is $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. We will show φ_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 φ_p^r is the identity 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 $r \geq 1$), so it has at most p^r roots in $\mathbf{F}_{p^n}$. Thus $p^n \leq p^r$, so $n \leq r$. Hence φ_p has order at least n in $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$, a group of order n, so φ_p generates the Galois group: every element of $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ is an iterate of φ_p. □

Galois theory makes Theorem 2.8 follow from Theorem 4.1: an extension with a cyclic Galois group has its lattice of intermediate fields resemble the lattice of subgroups of a cyclic group, with the unique subfield of degree d over $\mathbf{F}_p$ corresponding to the unique subgroup of the Galois group with *index* d. In the diagram below are subfields of $\mathbf{F}_{p^{12}}$ on the left and corresponding subgroups of $\mathrm{Gal}(\mathbf{F}_{p^{12}}/\mathbf{F}_p) = \langle \varphi_p \rangle \cong \mathbf{Z}/(12)$ on the right.



Theorem 3.4 can be explained in a second, shorter, way as a corollary of Theorem 4.1 and we also get part of Theorem 2.5.

Corollary 4.2. *If $\pi(x) \in \mathbf{F}_p[x]$ is irreducible with degree d then it is separable and if α is one of its roots in some extension field of $\mathbf{F}_p$ then its full set of roots is $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$.*

Proof. We have seen already that a 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 $\pi(x)$ in $\mathbf{F}_p(\alpha)$ can be obtained from α by applying $\mathrm{Gal}(\mathbf{F}_p(\alpha)/\mathbf{F}_p)$ to this root. Since the Galois group is generated by the p-th power map, the roots of $\pi(x)$ are $\alpha, \alpha^p, \alpha^{p^2}, \ldots$. Once we reach α^{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 and *all* elements in a field of order p^d satisfy $t^{p^d} = t$. Therefore the list $\alpha, \alpha^p, \alpha^{p^2}, \ldots$ of all possible roots of $\pi(x)$ is $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$. Why are they all distinct?

Since $\mathbf{F}_p(\alpha)/\mathbf{F}_p$ is Galois and $\pi(x)$ is irreducible over $\mathbf{F}_p$ with a root α in $\mathbf{F}_p(\alpha)$, $\pi(x)$ is separable over $\mathbf{F}_p$ and splits completely over $\mathbf{F}_p(\alpha)$. Therefore $\pi(x)$ has d distinct roots in $\mathbf{F}_p(\alpha)$, so the list $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ has to consist of *distinct* elements. □

The p-th power map on $\mathbf{F}_{p^n}$ is called the *Frobenius automorphism*. This function, whose formula doesn't involve n, generates $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ for all $n \geq 1$.

Let's compute some concrete Galois groups over $\mathbf{F}_p$.

Example 4.3. The polynomial $x^3 + x^2 + 1$ is irreducible over $\mathbf{F}_2$. If α is a root of it over $\mathbf{F}_2$ then $\mathbf{F}_2(\alpha)/\mathbf{F}_2$ is a cubic Galois extension and $\mathrm{Gal}(\mathbf{F}_2(\alpha)/\mathbf{F}_2) = \{\beta \mapsto \beta, \beta \mapsto \beta^2, \beta \mapsto \beta^4\}$. The second element is the Frobenius automorphism φ_2 and the third is φ_2^2. By Example 3.5 we have $\alpha^4 = \alpha^2 + \alpha + 1$, so we can make a table below describing each automorphism's effect on α in the $\mathbf{F}_2$-basis $\{1, \alpha, \alpha^2\}$.

σ	id.	φ_2	φ_2^2
$\sigma(\alpha)$	α	α^2	$\alpha^2 + \alpha + 1$

Example 4.4. The polynomial $x^2 + 1$ is irreducible over $\mathbf{F}_3$. Let α be a root, so $\mathbf{F}_3(\alpha)/\mathbf{F}_3$ is a Galois extension of degree 2. Its Galois group is $\{\beta \mapsto \beta, \beta \mapsto \beta^3\}$. A basis of $\mathbf{F}_3(\alpha)$ over $\mathbf{F}_3$ is $\{1, \alpha\}$ and the Frobenius automorphism φ_3 on a typical element $\varphi_3(a + b\alpha) = (a + b\alpha)^3 = a + b\alpha^3$ since $a^3 = a$ and $b^3 = b$ for $a, b \in \mathbf{F}_3$.

The two roots of $x^2 + 1$ are α and α^3, but they are also α and $-\alpha$, so $\alpha^3 = -\alpha$. That can be seen by a direct calculation as well: $\alpha^3 = (\alpha^2)\alpha = -\alpha$. So we could also describe the Frobenius automorphism in $\mathrm{Gal}(\mathbf{F}_3(\alpha)/\mathbf{F}_3)$ by $\varphi_3(a + b\alpha) = a - b\alpha$.

Example 4.5. The polynomial $x^3 - 2$ is irreducible over $\mathbf{F}_7$. If α is a root of it then $\mathbf{F}_7(\alpha)/\mathbf{F}_7$ is a Galois extension and $\mathrm{Gal}(\mathbf{F}_7(\alpha)/\mathbf{F}_7) = \{\beta \mapsto \beta, \beta \mapsto \beta^7, \beta \mapsto \beta^{49}\}$. From the work in Example 3.6, $\alpha^7 = 4\alpha$ and $\alpha^{49} = 2\alpha$. Therefore we can also describe the automorphisms in $\mathrm{Gal}(\mathbf{F}_7(\alpha)/\mathbf{F}_7)$ by their effect on α as in the table below.

σ	id.	φ_7	φ_7^2
$\sigma(\alpha)$	α	4α	2α

5. General finite base fields

In addition to working with finite fields as extensions of $\mathbf{F}_p$, we can fix a finite field $\mathbf{F}_q$ of possibly nonprime size (*e.g.*, $q = 4$ or 27) and look at finite extensions of $\mathbf{F}_q$. While every $a \in \mathbf{F}_p$ satisfies $a^p = a$, in $\mathbf{F}_q$ every element a satisfies $a^q = a$. This follows from the proof of Lemma 2.1, but we give the proof again since it's short: if $a \in \mathbf{F}_q^\times$ then $a^{q-1} = 1$ by Lagrange's theorem, so $a^q = a$, and this last equation is satisfied by 0 too. In a finite extension $F/\mathbf{F}_q$, the q-th power map $F \to F$ is an automorphism (it is an iterate of the

p-th power automorphism of F, where p is the prime that q is a power of) and the subset of F fixed by the q-th power map is $\mathbf{F}_q$: the equation $a^q = a$ has at most q solutions in F and $\mathbf{F}_q$ is a set of q solutions inside F. **Watch out**: when q is a power of the prime p then $\mathbf{F}_q$ has characteristic p, not characteristic q (unless $q = p$). No field has a composite characteristic. Since $p = 0$ in $\mathbf{F}_q$, also $q = 0$ in $\mathbf{F}_q$, so that aspect looks the same; it's just that q is not the *smallest* positive integer vanishing in $\mathbf{F}_q$ if $q > p$.

Here are analogues over $\mathbf{F}_q$ of results we proved over $\mathbf{F}_p$. Proofs are left to the reader.

Theorem 5.1. *For every positive integer n, there is a monic irreducible of degree n in $\mathbf{F}_q[x]$, and all of them divide $x^{q^n} - x$, which is separable. In particular, every irreducible in $\mathbf{F}_q[x]$ is separable.*

Theorem 5.2. *Between $\mathbf{F}_q$ and $\mathbf{F}_{q^n}$ every intermediate field has order q^d where $d \mid n$. Conversely, for each d dividing n there is a unique field between $\mathbf{F}_q$ and $\mathbf{F}_{q^n}$ of order q^d, which is $\{t \in \mathbf{F}_{q^n} : t^{q^d} = t\}$.*

Lemma 5.3. *For every $f(x) \in \mathbf{F}_q[x]$, $f(x)^{q^m} = f(x^{q^m})$ for $m \geq 0$.*

Lemma 5.4. *Let $\pi(x)$ be irreducible of degree d in $\mathbf{F}_q[x]$. For $n \geq 0$, $\pi(x) \mid (x^{q^n} - x) \iff d \mid n$.*

Theorem 5.5. *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 α. Then $\pi(x)$ has roots $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. These d roots are distinct; more precisely, when i and j are nonnegative, $\alpha^{q^i} = \alpha^{q^j} \iff i \equiv j \bmod d$.*

Theorem 5.6. *For every integer $n \geq 1$, $\mathbf{F}_{q^n}/\mathbf{F}_q$ is a Galois extension and $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ is cyclic with generator the q-th power map $\varphi_q \colon t \mapsto t^q$.*

6. Applications

Finite fields are important in both pure and applied math. Here are some examples.

(1) **Number theory**. Many problems in $\mathbf{Z}$ are studied by reducing mod p, which puts us in the finite fields $\mathbf{Z}/(p)$. In every finite extension K of $\mathbf{Q}$ is a ring $\mathcal{O}_K$ playing a role analogous to that of $\mathbf{Z}$ in $\mathbf{Q}$. (For example, when $K = \mathbf{Q}(\sqrt{2})$, $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$.) Problems in $\mathcal{O}_K$ can often be reduced to working in the fields $\mathcal{O}_K/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal. Every $\mathcal{O}_K/\mathfrak{m}$ is a finite field and often is not of prime order.

(2) **Group theory**. Most nonabelian finite simple groups besides alternating groups A_n ($n \geq 5$) come from matrix groups over finite fields, and their construction is analogous to that of simple Lie groups over $\mathbf{C}$. Galois himself created finite fields of nonprime order in order to describe primitive solvable permutation groups [1, Sect. 14.3], [2], [6, p. 344].

(3) **Combinatorics**. An important theme in combinatorics is q-analogues, which are algebraic expressions in a variable q that become classical objects when $q = 1$, or when $q \to 1$. For example, the q-binomial coefficient is

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})},$$

which for $n \geq k$ is a polynomial in q with integer coefficients. When $q \to 1$ this has the value $\binom{n}{k}$. While $\binom{n}{k}$ counts the number of k-element subsets of a finite set, when q is a prime power the number $\binom{n}{k}_q$ counts the number of k-dimensional subspaces

of $\mathbf{F}_q^n$. Identities involving q-binomial coefficients can be proved by checking them when q runs through prime powers, using linear algebra over the fields $\mathbf{F}_q$.

(4) **Coding theory**. This is the study of clear communication over noisy channels. Messages sent back to earth by NASA space probes, information engraved on a DVD, and signals allowing many mobile phone conversations on the same channel are created using codes where the code words are coefficients of a polynomial over a finite field.

(5) **Cryptography**. This is the study of secret communication. The usual way information is stored securely on an ATM card involves elliptic curves over finite fields.

The lesson from the last two examples is that even people who say "math sucks" are using finite fields every day without realizing it.[3]

7. History

Fields of prime order, namely $\mathbf{Z}/(p)$, were studied by many of the early number theorists such as Fermat, Euler, Lagrange, Legendre, and Gauss. The first mathematician to publish a paper on finite fields of non-prime order was Galois in 1830. Gauss had developed the theory of finite fields earlier [3], discovering such critical properties as Theorems 2.8 and Corollary 4.2, 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 α is the root of an irreducible polynomial $\pi(x)$ in $\mathbf{F}_p[x]$ while Gauss worked with finite fields as $\mathbf{F}_p[x]/(\pi(x))$. Galois wrote that there is an irreducible in $\mathbf{F}_p[x]$ of every degree but he did not give a proof.

In 1893, at the International Mathematical Congress in Chicago, E. H. Moore proved that every finite field is isomorphic to a field of the form $\mathbf{F}_p[x]/(\pi(x))$, a theorem which he described with the comment [7, 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 [7, p. 208]. So to Moore, a field meant what we'd call a finite field. He called a field constructed in the concrete form $\mathbf{F}_p[x]/(\pi(x))$ a *Galois field*, so for Moore a Galois field was a particular 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, the term Galois field lives on today among coding theorists in computer science and electrical engineering as a synonym for finite field and Moore's notation $\mathrm{GF}(q)$ is often used in place of $\mathbf{F}_q$.

Appendix A. The maximal order in a finite abelian group

In the proof that the nonzero elements in a finite field form a cyclic group (Lemma 1.6), we relied on the following property of finite abelian groups that we will prove here.

Theorem A.1. *If G is a finite abelian group and m is the maximal order of the elements of G then the order of every element of G divides m.*

The proof of Theorem A.1 is based on a corollary of the following basic property of elements in a finite abelian group having relatively prime order.

[3]Professional mathematicians who never use finite fields might hold them in low esteem. For example, Joseph Ritt, who created differential algebra, always worked over the real and complex numbers and called all fields of characteristic p, not just the finite ones, "monkey fields" [5, p. xiii].

Theorem A.2. *Let g_1 and g_2 have respective orders n_1 and n_2 in an abelian group. If $(n_1, n_2) = 1$ then g_1g_2 has order n_1n_2.*

Proof. Let n be the order of g_1g_2. Since

$$(g_1g_2)^{n_1n_2} = g_1^{n_1n_2}g_2^{n_1n_2} = (g_1^{n_1})^{n_2}(g_2^{n_2})^{n_1} = 1 \cdot 1 = 1,$$

we have $n \mid n_1n_2$.

Since $(g_1g_2)^n = 1$, by raising both sides to the n_1 power we get $g_2^{nn_1} = 1$. Therefore $n_2 \mid nn_1$, so from $(n_1, n_2) = 1$ we conclude $n_2 \mid n$. Exchanging the roles of n_1 and n_2, we get in a similar way that $n_1 \mid n$. Since $n_1 \mid n$ and $n_2 \mid n$ *and* $(n_1, n_2) = 1$, we get $n_1n_2 \mid n$. We already showed $n \mid n_1n_2$ (in the first paragraph), so $n = n_1n_2$. □

Remark A.3. Commutativity is used in the proof of Theorem A.2 to say $(g_1g_2)^r = g_1^rg_2^r$ for all $r \geq 1$. All we need is that g_1 and g_2 commute, not that the whole group is abelian.

Corollary A.4. *In an abelian group, if there are elements of order n_1 and n_2 then there is an element with order $[n_1, n_2]$. More precisely, if g_1 and g_2 have respective orders n_1 and n_2 then there are k_1 and k_2 in $\mathbf{Z}^+$ such that $g_1^{k_1}g_2^{k_2}$ has order $[n_1, n_2]$.*

Proof. The basic idea is to write $[n_1, n_2]$ as a product of two relatively prime factors and then find exponents k_1 and k_2 such that $g_1^{k_1}$ and $g_2^{k_2}$ have orders equal to those factors. Then the order of $g_1^{k_1}g_2^{k_2}$ is the product of the factors (Theorem A.2), which is $[n_1, n_2]$.

Here are the details. Factor n_1 and n_2 into primes:

$$n_1 = p_1^{e_1} \cdots p_r^{e_r}, \quad n_2 = p_1^{f_1} \cdots p_r^{f_r}.$$

We use the same list of (distinct) primes in these factorizations, and use an exponent 0 on a prime that is not a factor of one of the integers. The least common multiple is

$$[n_1, n_2] = p_1^{\max(e_1,f_1)} \cdots p_r^{\max(e_r,f_r)}.$$

Break this into a product of two factors, one being a product of the prime powers where $e_i \geq f_i$ and the other using prime powers where $e_i < f_i$. Call these two numbers ℓ_1 and ℓ_2:

$$\ell_1 = \prod_{e_i \geq f_i} p_i^{e_i}, \quad \ell_2 = \prod_{e_i < f_i} p_i^{f_i}.$$

Then $[n_1, n_2] = \ell_1\ell_2$ and $(\ell_1, \ell_2) = 1$ (since ℓ_1 and ℓ_2 have no common prime factors). By construction, $\ell_1 \mid n_1$ and $\ell_2 \mid n_2$. Then $g_1^{n_1/\ell_1}$ has order ℓ_1 and $g_2^{n_2/\ell_2}$ has order ℓ_2. Since these orders are relatively prime, $g_1^{n_1/\ell_1}g_2^{n_2/\ell_2}$ has order $\ell_1\ell_2 = [n_1, n_2]$. □

Example A.5. If g_1 has order $n_1 = 60 = 2^2 \cdot 3 \cdot 5$ and g_2 has order $n_2 = 630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ then $[n_1, n_2] = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = (2^2 \cdot 5) \cdot (3^2 \cdot 7)$, where the first factor divides n_1, the second divides n_2, and the factors are relatively prime. Then g_1^3 has order $2^2 \cdot 5$ and g_2^{10} has order $3^2 \cdot 7$, which are relatively prime, so $g_1^3g_2^{10}$ has order $2^2 \cdot 5 \cdot 3^2 \cdot 7 = [n_1, n_2]$.

We are ready to prove Theorem A.1.

Proof. Let n be the order of an element of G. Since m is also the order of an element in G, by Corollary A.4 some element in G has order $[m, n]$. By maximality of m as an order, $m \geq [m, n]$. Obviously $m \leq [m, n]$ from the definition of $[m, n]$, so $[m, n] = m$, and that implies $n \mid m$. □

References

[1] D. A. Cox, *Galois Theory*, 2nd ed., Wiley, Hoboken, 2012.

[2] D. A. Cox, *Évariste Galois and Solvable Permutation Groups*, https://dacox.people.amherst.edu/lectures/bilbao.pdf.

[3] 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.

[4] E. Galois, *Sur la théorie de nombres*, Bulletin des Sciences Mathématiques de Férussac **13** (1830), 428–435. (Also Collected Works, 1897, pp. 15–23.)

[5] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[6] H. Lüneberg, "On the Early History of Galois Fields," pp. 341–355 of *Finite Fields and Applications* (*Augsburg*, 1999), Springer, Berlin, 1999.

[7] 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. Online at https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM1893/ICM1893.ocr.pdf.