Finite fields

We plan to describe all finite fields. Most of the work will be preliminary.
We give two examples first.

Let $F$ be a field. If $f(x)$ is an irreducible element of the polynomial ring $F[x]$, then the principal ideal $(f)$ it generates is a maximal ideal, so the quotient ring $F[x]/(f)$ is a field. This gives us a way to construct field extensions.

Example 1. Let $F = \mathbb{F}_2$ be the field with two elements. We’ll call the elements 0 and 1. There is just one irreducible polynomial of degree 2 in $F[x]$, namely $f(x) = x^2 + x + 1$. The field $K = F[x]/(f)$ has $F$-basis $1, \alpha$, where $\alpha$ denotes the residue of $x$, which is a root of the polynomial $f$. The elements of $K$ are $0, 1, \alpha, 1 + \alpha$. To compute in $K$, one uses the two relations $1 + 1 = 0$ and $\alpha^2 + \alpha + 1 = 0$. Since $1 + 1 = 0$ in $K$, signs are irrelevant: $a = -a$.

The element $1 + \alpha$ is the second root of $f$:

$$(x + \alpha)(x + (1 + \alpha)) = x^2 + x + 1$$

Example 2. Here $F = \mathbb{F}_3$. The elements of $F$ are $0, 1, -1 (= 2)$. The polynomial $x^2 + 1$ has no root in $F$. It is an irreducible element of $F[x]$, and $K = F[x]/(f)$ is a field with $F$-basis $1, \alpha$, where $\alpha$ is the residue of $x$. The elements of $F$ are $0, 1, -1, \alpha, -\alpha, 1 + \alpha, 1 - \alpha, -1 + \alpha, -1 - \alpha$.

The six elements other than $0, 1, -1$ are roots of irreducible quadratic polynomials, so there must be at least three irreducible quadratic polynomials in $F[x]$. In fact, there are exactly three:

$$x^2 + 1, \quad x^2 + x - 1, \quad x^2 - x - 1$$

For example, $1 + \alpha$ is a root of $x^2 + x - 1$.

Now for the preliminary work:

Lemma 1. Let $F$ be a field, let $f$ be a monic irreducible polynomial in $F[x]$, and let $K$ denote the field $F[x]/(f)$. Also, let $\alpha$ denote the residue of $x$ in $K$. Then

(i) $K$ contains $F$ as subfield.

(ii) $\alpha$ is a root of $f(x)$ in $K$.

proof (i) This is almost obvious, but it can be a bit confusing. We consider the homomorphisms $F \subset F[x] \rightarrow F[x]/(f) = K$. The composed map $F \rightarrow K$ is injective because $F$ is a field. (It has no proper ideals). So $F$ is mapped isomorphically to a subfield of $K$ that we identify with $F$.

(ii) Let’s denote the residue in $K$ of an element $z$ of $F[x]$ by $\overline{z}$. Then since we are identifying $F$ with its image in $K$, $\alpha = a$ when $a \in F$.

Say that $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_i \in F$. In the homomorphism $F[x] \rightarrow F[x]/(f)$, the element $f$ maps to zero: $\overline{f(x)} = 0$. Then

$$0 = \overline{f} = \overline{x^d} + a_{d-1}\overline{x^{d-1}} + \cdots + a_0 = \overline{x^d + a_{d-1}x^{d-1} + \cdots + a_0} = f(\alpha)$$

Thus $F[x]/(f)$ is a field extension of $F$ in which the polynomial $f$ has a root. 

Corollary 1. Let $F$ be a field, and let $f(x)$ be an irreducible monic polynomial with coefficients in $F$. There exists a field extension $K$ in which $f$ has a root.

We can say a bit more. A monic polynomial $f(x)$ splits completely in a field $K$ if it is a product of linear factors: $f(x) = (x - \alpha_1 - \cdots - (x - \alpha_d)$ with $\alpha_i \in K$.

Corollary 2. Let $f(x)$ be a monic polynomial with coefficients in a field $F$. There exists a field extension $K$ of $F$ in which $f(x)$ splits completely.
proof If \( f \) splits completely in \( F \), there is nothing to show. Otherwise, we choose an irreducible factor \( g(x) \) of \( f(x) \), of degree \( > 1 \), and apply Corollary 1. There is field extension \( F_1 \) of \( F \) in which \( g \) has a root \( \alpha \). Then \( \alpha \) is also a root of \( f \) in \( F_1 \), so \( f \) has more roots in \( F_1 \) than in \( F \). We replace \( F \) by \( F_1 \) and repeat this construction. \( \square \)

Lemma 2. Let \( F \) be a field. A polynomial \( f(x) \) in \( F[x] \) of degree \( d \) has at most \( d \) roots in \( F \).

proof We use induction on \( d \). Let \( \alpha \) be a root of \( f \) in \( F \). Then in \( F[x] \), \( f(x) = (x - \alpha)g(x) \) for some \( g \) in \( F[x] \) of degree \( d - 1 \). Any root of \( f \) other than \( \alpha \) must be a root of \( g \). By induction, we may suppose that \( g \) has at most \( d - 1 \) roots. Then \( f \) has at most \( d \) roots. \( \square \)

Proposition 1. Let \( K \) be a field. Every finite subgroup of the multiplicative group \( K^\times \) is a cyclic group.

proof We will use the Structure Theorem for abelian groups, which tells us that a finite abelian group is a direct sum of cyclic groups of some orders \( d_1, d_2, \ldots, d_k \), where \( d_1 \) divides \( d_2 \), etc. The theorem was proved using additive notation for the law of composition, but it remains true when the law is written as multiplication. So \( G = C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k} \). We need the fact that \( d_1 | d_2 | \cdots | d_k \) here. It shows that any element of \( G \) has an order that divides \( d_k \). Therefore the elements of \( G \) are roots of the polynomial \( x^{d_k} - 1 \). Lemma 2 tells us that the order of \( G \) cannot be greater than \( d_k \). On the other hand, the order is the product \( d_1 d_2 \cdots d_k \). Therefore, assuming we have eliminated the trivial groups \( C_1 \), there can be only one cyclic group: \( k = 1 \).

about the derivative

The derivative of a polynomial \( f(x) = \sum a_i x^i \) is defined by the usual calculus rule \( f'(x) = \sum i a_i x^{i-1} \), in which the integer \( i \) stands for \( 1 + 1 + \cdots + 1 \). The derivative satisfies the product rule \( (fg)' = fg' + fg \).

The next lemma gives the most important property of the derivative.

Lemma 3. An element \( \alpha \) is a multiple root of a polynomial \( f \), i.e., \( (x - \alpha)^2 \) divides \( f \), if and only if it is a common root of \( f \) and of \( f' \).

proof Suppose that \( \alpha \) is a root, so that \( f(x) = (x - \alpha)g(x) \) for some polynomial \( g \). Then by the product rule, \( f'(x) = g(x) + (x - \alpha)g'(x) \), and \( f''(\alpha) = g(\alpha) \). So \( \alpha \) is a root of \( f'' \) if and only if it is a root of \( g \), and it is a root of \( g \) if and only if it is a double root of \( f \).

We go to finite fields now.

Let \( K \) be a finite field. We map the integers \( \mathbb{Z} \) to \( K \) by the unique homomorphism: \( \mathbb{Z} \to K \). Because \( K \) is finite, the kernel of \( \varphi \) will be a nonzero ideal, generated by an irreducible element of \( \mathbb{Z} \) – a prime integer \( p \). The image of \( \varphi \) will be isomorphic to the prime field \( \mathbb{Z}/(p) = \mathbb{F}_p \).

• Every finite field \( K \) contains one of the fields \( F = \mathbb{F}_p \), as subfield.

Then \( K \) will be a field extension of \( F \), and the degree \( [K : F] \) will be finite. Say that \( [K : F] = r \). Then \( K \) is an \( F \)-vector space of dimension \( r \). It has an \( F \)-basis of \( r \) elements, so its order is \( p^r \).

Let \( q = p^r \).

Lemma 4. The polynomial \( x^q - x \) has no multiple root in any field \( K \) of characteristic \( p \).

proof Let \( f(x) = x^q - x \). Then \( f'(x) = qx^{q-1} - 1 \). Since \( q \) is a power of \( p \), it is zero in \( K \), and \( f'(x) = -1 \). Then \( f' \) has no root, and so \( f \) and \( f' \) have no common root. \( \square \)

Lemma 5. Let \( K \) be a finite field of order \( q = p^r \). The elements of \( K \) are roots of the polynomial \( x^q - x \).

proof The multiplicative group \( K^\times \) is a finite group of order \( q - 1 \), and Proposition 1 tells us that \( K^\times \) is a cyclic group. All of its elements have orders that divide \( q - 1 \). They are roots of the polynomial \( x^{q-1} - 1 \). Since \( 0 \) is a root of the polynomial \( x \), all elements of \( K \) are roots of \( x(x^{q-1} - 1) = x^q - x \). \( \square \)

Lemma 6. Let \( R \) be a ring that contains the prime field \( F = \mathbb{F}_p \) as a subring, and let \( q = p^r \). Then if \( a, b \) are elements of \( R \), then \( (a + b)^q = a^q + b^q \).

proof The fact that \( (x + y)^q = x^q + y^q \) follows from the binomial expansion: \( (x + y)^q = \sum \binom{q}{i} x^i y^{q-i} \). The binomial coefficients \( \binom{q}{i} \) are divisible by \( p \) when \( i = 1, \ldots, p - 1 \). Therefore they are zero in \( F \). Then
Lemma 7. Let $L$ be a field that contains $F = \mathbb{F}_p$, and let $K$ be the set of roots of the polynomial $x^q - x$ in $L$, where $q = p^r$. Then $K$ is a subfield of $L$.

The roots are the elements $a$ of $L$ such that $a^q = a$, or if $a \neq 0$, such that $a^{q-1} = 1$.

**proof** We have to show that $K$ contains $1$, is closed under the operations $+,-,\times$, and contains the inverses of its nonzero elements. If $a, b$ are in $K$, Lemma 6 shows that $a + b$ is in $K$. A somewhat interesting point is that if $a$ is in $K$, then $-a$ is in $K$: If $p$ is odd, then $q$ is odd, and $(-a)^q = -a^q$. If $q$ is even, i.e., $p = 2$, then $(-a)^q = a^q = a$. However, in this case, $a = -a$ so $(-a)^q = -a$ as well.

Lemma 8. Let $k$ and $r$ be integers such that $k$ divides $r$, and let $q = p^r$ and $q' = p^k$. The polynomial $x^{(q'-1)} - 1$ divides $x^{(q-1)} - 1$.

**proof** This is tricky. Say that $r = ks$. We substitute $y = p^k$ and $n = s$ into the equation

$$y^n - 1 = (y-1)(y^{n-1} + y^{n-2} + \cdots + y + 1)$$

obtaining $q - 1 = (p^k)^s - 1 = (p^k - 1)(\ell) = (q' - 1)(\ell)$, where $\ell$ is an integer. So $q' - 1$ divides $q - 1$.

Next, we substitute $y = x^{(q'-1)}$ and $n = \ell$ into the same displayed equation: $x^{(q'-1)} - 1 = (x^{(q'-1)} - 1)(\ell - 1)\varphi(x)$, for some polynomial $\varphi$. So $x^{(q'-1)} - 1$ divides $x^{(q-1)} - 1$.

The main results about finite fields are the next theorems, in which $p$ is a prime integer and $q = p^r$.

**Theorem 1.** There exists a finite field of order $q$, and any two fields of order $q$ are isomorphic.

**Theorem 2.** Let $K$ be a field of order $q = p^r$, and let $K'$ be a field of order $q' = p^k$. Then $K$ contains a subfield isomorphic to $K'$ if and only if $k$ divides $r$.

**Theorem 3.** The polynomial $x^q - x$ is the product of the irreducible polynomials in $F[x]$ whose degrees divide $r$.

In Theorem 3, each factor appears just once in the product because $x^q - x$ has no multiple root.

**Examples 3.** (i) ($q = 2^2$) In $\mathbb{F}_2[x]$, the polynomial $x^4 - x$ is the product $x(x+1)(x^2 + x + 1)$.

(ii) ($q = 3^2$) In $\mathbb{F}_3[x]$, $x^9 - x = x(x+1)(x^2 + 1)(x^2 - x - 1)$.

(iii) ($q = 2^3$) In $\mathbb{F}_2[x]$, $x^8 - x = x(x+1)(x^2 + x + 1)(x^2 + x^2 + 1)$.

(iv) ($q = 2^4$) In $\mathbb{F}_2[x]$, $x^{16} - x = x(x+1)(x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

The factors of $x^q - x$ appear here because 4 = 2^2, $q = 2^4$, and 2 divides 4.

**proof of Theorem 1** We start with the prime field $F = \mathbb{F}_p$. Corollary 2 tells us that there is a field extension $L$ of $F$ in which the polynomial $x^q - x$ splits completely. It has $q$ roots in $L$ (Lemma 4). Lemma 7 tells us that the set $K$ of those roots is a field.

The fact that two fields $K$ and $K'$ a of order $q = p^r$ are isomorphic will follow from Theorem 2. If $K$ and $K'$ have the same order and $K'$ is isomorphic to a subfield of $K$, then that subfield is equal to $K$.

**proof of Theorem 2** Here $[K : F] = r$ and $[K' : F] = k$. If $K'$ is (or is isomorphic to) a subfield of $K$, then $r = [K : F] = [K : K'][K' : F] = [K : K']k$, so $k$ divides $r$.

Conversely, let $k$ be an integer that divides $r$, and let $q' = p^k$. Let $K$ and $K'$ be fields of orders $q$ and $q'$, respectively. We must show that $K$ contains a subfield isomorphic to $K'$. The multiplicative group $K^{*r}$ is cyclic of order $q' - 1$. Let $\beta'$ be a generator for that cyclic group. Then obviously, $K' = F[\beta']$. Let $g(x)$ be the irreducible polynomial in $F[x]$ with root $\beta'$. Since $\beta'$ is also a root of $x^{(q'-1)} - 1$, $g$ divides $x^{(q'-1)} - 1$. Lemma 8 tells us that $x^{(q'-1)} - 1$ divides $x^{(q-1)} - 1$. So $g$ divides $x^{(q-1)} - 1$, which is a polynomial that splits completely in $K$. Therefore $g$ has a root $\beta$ in $K$, and $K' = F[\beta']$ is isomorphic to the subfield $F[\beta]$ of $K$.

So $K$ contains a subfield isomorphic to $K'$. □
Example 4. In Example 2, \( F = F_4 \) and \( K = F[\alpha] = F[x]/(x^2 + 1) \) where \( \alpha \) is the residue of \( x \). The multiplicative group \( K^\times \) has order 8, and the element \( \alpha \) isn’t a generator because \( \alpha^2 = -1 \) and \( \alpha^4 = 1 \). But let \( \beta = 1 + \alpha \). Then \( \beta^2 = 1 - \alpha + \alpha^2 = -\alpha \). So \( \beta \) has order 8. The four elements of \( K \) distinct from 0, 1, \(-1\), \( \alpha \), \(-\alpha \) all have order 8.

proof of Theorem 3 Let \( K \) be a field of order \( q = p^r \), and let \( g(x) \) be an irreducible factor of \( x^q - x \) in \( F[x] \), say of degree \( k \). Since \( x^q - x \) splits completely in \( K \), \( g \) has a root \( \beta \) in \( K \). The subfield \( K' = F[\beta] \) of \( K \) generated by \( \beta \) has degree \( k \) over \( F \). So \( k \) divides \( r \).

Next, let \( g(x) \) be an irreducible polynomial in \( F[x] \) whose degree \( k \) divides \( r \). We are to show that \( g \) divides \( x^q - x \) or, if \( g \) isn’t the polynomial \( x \), that \( g \) divides \( x^{q-1} - 1 \). Let \( \beta' \) be a root of \( g \) in a field extension of \( F \), and let \( K' \) be the field \( F[\beta'] \). Its degree over \( F \) is \( [K' : F] = k \), and \( \beta' \) is also a root of \( x^{q-1} - 1 \). So \( g \) divides \( x^{q-1} - 1 \). Since \( k \) divides \( r \), \( x^{q-1} - 1 \) divides \( x^{(q-1)} - 1 \) (Lemma 8). So \( g \) divides \( x^{(q-1)} - 1 \). □