19

Finite fields

This chapter develops some of the basic theory of finite fields. As we already know (see Theorem 7.7), every finite field must be of cardinality p^w, for some prime p and positive integer w. The main results of this chapter are:

- for every prime p and positive integer w, there exists a finite field of cardinality p^w, and
- any two finite fields of the same cardinality are isomorphic.

19.1 Preliminaries

We begin by stating some simple but useful divisibility criteria for polynomials over an arbitrary field. These will play a crucial role in the development of the theory.

Let F be a field. A polynomial $f \in F[X]$ is called **square-free** if it is not divisible by the square of any polynomial of degree greater than zero. Using formal derivatives (see §16.7), we obtain the following useful criterion for establishing that a polynomial is square-free:

Theorem 19.1. *If F is a field, and $f \in F[X]$ with $\gcd(f, \mathbf{D}(f)) = 1$, then f is square-free.*

Proof. Suppose f is not square-free, and write $f = g^2 h$, for $g, h \in F[X]$ with $\deg(g) > 0$. Taking formal derivatives, we have

$$\mathbf{D}(f) = 2g\mathbf{D}(g)h + g^2\mathbf{D}(h),$$

and so clearly, g is a common divisor of f and $\mathbf{D}(f)$. □

Theorem 19.2. *Let F be a field, and let k, ℓ be positive integers. Then $X^k - 1$ divides $X^\ell - 1$ in $F[X]$ if and only if k divides ℓ.*

Proof. Let $\ell = kq + r$, with $0 \leq r < k$. We have

$$X^\ell \equiv X^{kq} X^r \equiv X^r \pmod{X^k - 1},$$

and $X^r \equiv 1 \pmod{X^k - 1}$ if and only if $r = 0$. □

Theorem 19.3. *Let $a \geq 2$ be an integer and let k, ℓ be positive integers. Then $a^k - 1$ divides $a^\ell - 1$ if and only if k divides ℓ.*

Proof. The proof is analogous to that of Theorem 19.2. We leave the details to the reader. □

One may combine these last two theorems, obtaining:

Theorem 19.4. *Let $a \geq 2$ be an integer, k, ℓ be positive integers, and F a field. Then $X^{a^k} - X$ divides $X^{a^\ell} - X$ in $F[X]$ if and only if k divides ℓ.*

Proof. Now, $X^{a^k} - X$ divides $X^{a^\ell} - X$ if and only if $X^{a^k - 1} - 1$ divides $X^{a^\ell - 1} - 1$. By Theorem 19.2, this happens if and only if $a^k - 1$ divides $a^\ell - 1$. By Theorem 19.3, this happens if and only if k divides ℓ. □

We end this section by recalling some concepts discussed earlier, mainly in §16.1, §16.5, and §16.6, that will play an important role in this chapter.

Suppose F is a field, and E is an extension field of F; that is, F is a subfield of E (or, more generally, F is embedded in E via some canonical embedding, and we identify elements of F with their images in E under this embedding). We may view E as an F-algebra via inclusion, and in particular, as an F-vector space. If E' is also an extension field of F, and $\rho : E \to E'$ is a ring homomorphism, then ρ is an F-algebra homomorphism if and only if $\rho(a) = a$ for all $a \in F$.

Let us further assume that as an F-vector space, E has finite dimension ℓ. This dimension ℓ is called the degree of E over F, and is denoted $(E : F)$, and E is called a finite extension of F. Now consider an element $\alpha \in E$. Then α is algebraic over F, which means that there exists a non-zero polynomial $g \in F[X]$ such that $g(\alpha) = 0$. The monic polynomial $\phi \in F[X]$ of least degree such that $\phi(\alpha) = 0$ is called the minimal polynomial of α over F. The polynomial ϕ is irreducible over F, and its degree $m := \deg(\phi)$ is called the degree of α over F. The ring $F[\alpha] = \{g(\alpha) : g \in F[X]\}$, which is the smallest subring of E containing F and α, is actually a field, and is isomorphic, as an F-algebra, to $F[X]/(\phi)$, via the map that sends $g(\alpha) \in F[\alpha]$ to $[g]_\phi \in F[X]/(\phi)$. In particular, $(F[\alpha] : F) = m$, and the elements $1, \alpha, \ldots, \alpha^{m-1}$ form a basis for $F[\alpha]$ over F. Moreover, m divides ℓ.

19.2 The existence of finite fields

Let F be a finite field. As we saw in Theorem 7.7, F must have cardinality p^w, where p is prime and w is a positive integer, and p is the characteristic of F. However, we can say a bit more than this. As discussed in Example 7.53, the field $\mathbb{Z}_p$ is embedded in F, and so we may simply view $\mathbb{Z}_p$ as a subfield of F. Moreover, it must be the case that w is equal to $(F : \mathbb{Z}_p)$.

We want to show that there exist finite fields of every prime-power cardinality. Actually, we shall prove a more general result:

> *If F is a finite field, then for every integer $\ell \geq 1$, there exists an extension field E of degree ℓ over F.*

For the remainder of this section, F denotes a finite field of cardinality $q = p^w$, where p is prime and $w \geq 1$.

Suppose for the moment that E is an extension of degree ℓ over F. Let us derive some basic facts about E. First, observe that E has cardinality q^ℓ. By Theorem 7.29, E^* is cyclic, and the order of E^* is $q^\ell - 1$. If $\gamma \in E^*$ is a generator for E^*, then every non-zero element of E can be expressed as a power of γ; in particular, every element of E can be expressed as a polynomial in γ with coefficients in F; that is, $E = F[\gamma]$. Let $\phi \in F[X]$ be the minimal polynomial of γ over F, which is an irreducible polynomial of degree ℓ. It follows that E is isomorphic (as an F-algebra) to $F[X]/(\phi)$.

So we have shown that every extension of degree ℓ over F must be isomorphic, as an F-algebra, to $F[X]/(f)$ for some irreducible polynomial $f \in F[X]$ of degree ℓ. Conversely, given any irreducible polynomial f over F of degree ℓ, we can construct the finite field $F[X]/(f)$, which has degree ℓ over F. Thus, the question of the existence of a finite field of degree ℓ over F reduces to the question of the existence of an irreducible polynomial over F of degree ℓ.

We begin with a simple generalization of Fermat's little theorem:

Theorem 19.5. *For every $a \in F$, we have $a^q = a$.*

Proof. The multiplicative group of units F^* of F has order $q - 1$, and hence, every $a \in F^*$ satisfies the equation $a^{q-1} = 1$. Multiplying this equation by a yields $a^q = a$ for all $a \in F^*$, and this latter equation obviously holds for $a = 0$ as well. □

This simple fact has a number of consequences.

Theorem 19.6. *We have*

$$X^q - X = \prod_{a \in F} (X - a).$$

Proof. Since each $a \in F$ is a root of $X^q - X$, by Theorem 7.13, the polynomial

$\prod_{a \in F}(X - a)$ divides the polynomial $X^q - X$. Since the degrees and leading coefficients of these two polynomials are the same, the two polynomials must be equal. □

Theorem 19.7. *Let E be an F-algebra. Then the map $\sigma : E \to E$ that sends $\alpha \in E$ to α^q is an F-algebra homomorphism.*

Proof. By Theorem 16.3, either E is trivial or contains an isomorphic copy of F as a subring. In the former case, there is nothing to prove. So assume that E contains an isomorphic copy of F as a subring. It follows that E must have characteristic p.

Since $q = p^w$, we see that $\sigma = \tau^w$, where $\tau(\alpha) := \alpha^p$. By the discussion in Example 7.48, the map τ is a ring homomorphism, and hence so is σ. Moreover, by Theorem 19.5, we have

$$\sigma(c1_E) = (c1_E)^q = c^q 1_E^q = c1_E$$

for all $c \in F$. Thus (see Theorem 16.5), σ is an F-algebra homomorphism. □

The map σ defined in Theorem 19.7 is called the **Frobenius map on E over F**. In the case where E is a finite field, we can say more about it:

Theorem 19.8. *Let E be a finite extension of F, and let σ be the Frobenius map on E over F. Then σ is an F-algebra automorphism on E. Moreover, for all $\alpha \in E$, we have $\sigma(\alpha) = \alpha$ if and only if $\alpha \in F$.*

Proof. The fact that σ is an F-algebra homomorphism follows from the previous theorem. Any ring homomorphism from a field into a field is injective (see Exercise 7.47). Surjectivity follows from injectivity and finiteness.

For the second statement, observe that $\sigma(\alpha) = \alpha$ if and only if α is a root of the polynomial $X^q - X$, and since all q elements of F are already roots, by Theorem 7.14, there can be no other roots. □

As the Frobenius map on finite fields plays a fundamental role in the study of finite fields, let us develop a few simple properties right away. Suppose E is a finite extension of F, and let σ be the Frobenius map on E over F. Since the composition of two F-algebra automorphisms is also an F-algebra automorphism, for every $i \geq 0$, the i-fold composition σ^i, which sends $\alpha \in E$ to $\alpha^{q^i} \in E$, is also an F-algebra automorphism. Since σ is an F-algebra automorphism, the inverse function σ^{-1} is also an F-algebra automorphism. Hence, σ^i is an F-algebra automorphism for all $i \in \mathbb{Z}$. If E has degree ℓ over F, then applying Theorem 19.5 to the field E, we see that σ^ℓ is the identity map. More generally, we have:

Theorem 19.9. *Let E be a extension of degree ℓ over F, and let σ be the Frobenius map on E over F. Then for all integers i and j, we have $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{\ell}$.*

Proof. We may assume $i \geq j$. We have

$$\begin{aligned}
\sigma^i = \sigma^j &\iff \sigma^{i-j} = \sigma^0 \iff \alpha^{q^{i-j}} - \alpha = 0 \text{ for all } \alpha \in E \\
&\iff \Big(\prod_{\alpha \in E}(X - \alpha)\Big) \mid (X^{q^{i-j}} - X) \text{ (by Theorem 7.13)} \\
&\iff (X^{q^\ell} - X) \mid (X^{q^{i-j}} - X) \text{ (by Theorem 19.6, applied to } E) \\
&\iff \ell \mid (i - j) \text{ (by Theorem 19.4)} \\
&\iff i \equiv j \pmod{\ell}. \ \square
\end{aligned}$$

From the above theorem, it follows that every power of the Frobenius map σ can be written uniquely as σ^i for some $i = 0, \ldots, \ell - 1$.

The following theorem generalizes Theorem 19.6:

Theorem 19.10. *For $k \geq 1$, let P_k denote the product of all the monic irreducible polynomials in $F[X]$ of degree k. For all positive integers ℓ, we have*

$$X^{q^\ell} - X = \prod_{k \mid \ell} P_k,$$

where the product is over all positive divisors k of ℓ.

Proof. First, we claim that the polynomial $X^{q^\ell} - X$ is square-free. This follows immediately from Theorem 19.1, since $\mathbf{D}(X^{q^\ell} - X) = q^\ell X^{q^\ell - 1} - 1 = -1$.

Thus, we have reduced the proof to showing that if f is a monic irreducible polynomial of degree k, then f divides $X^{q^\ell} - X$ if and only if k divides ℓ.

So let f be a monic irreducible polynomial of degree k. Let $E := F[X]/(f) = F[\xi]$, where $\xi := [X]_f \in E$. Observe that E is an extension field of degree k over F. Let σ be the Frobenius map on E over F.

First, we claim that f divides $X^{q^\ell} - X$ if and only if $\sigma^\ell(\xi) = \xi$. Indeed, f is the minimal polynomial of ξ over F, and so f divides $X^{q^\ell} - X$ if and only if ξ is a root of $X^{q^\ell} - X$, which is the same as saying $\xi^{q^\ell} = \xi$, or equivalently, $\sigma^\ell(\xi) = \xi$.

Second, we claim that $\sigma^\ell(\xi) = \xi$ if and only if $\sigma^\ell(\alpha) = \alpha$ for all $\alpha \in E$. To see this, first suppose that $\sigma^\ell(\alpha) = \alpha$ for all $\alpha \in E$. Then in particular, this holds for $\alpha = \xi$. Conversely, suppose that $\sigma^\ell(\xi) = \xi$. Every $\alpha \in E$ can be written as $\alpha = g(\xi)$ for some $g \in F[X]$, and since σ^ℓ is an F-algebra homomorphism, by Theorem 16.7 we have

$$\sigma^\ell(\alpha) = \sigma^\ell(g(\xi)) = g(\sigma^\ell(\xi)) = g(\xi) = \alpha.$$

Finally, we see that $\sigma^\ell(\alpha) = \alpha$ for all $\alpha \in E$ if and only if $\sigma^\ell = \sigma^0$, which by Theorem 19.9 holds if and only if $k \mid \ell$. $\square$

For $\ell \geq 1$, let $\Pi_F(\ell)$ denote the number of monic irreducible polynomials of degree ℓ in $F[X]$.

Theorem 19.11. *For all $\ell \geq 1$, we have*

$$q^\ell = \sum_{k|\ell} k\Pi_F(k). \tag{19.1}$$

Proof. Just equate the degrees of both sides of the identity in Theorem 19.10. □

From Theorem 19.11 it is easy to deduce that $\Pi_F(\ell) > 0$ for all ℓ, and in fact, one can prove a density result—essentially a "prime number theorem" for polynomials over finite fields:

Theorem 19.12. *For all $\ell \geq 1$, we have*

$$\frac{q^\ell}{2\ell} \leq \Pi_F(\ell) \leq \frac{q^\ell}{\ell}, \tag{19.2}$$

and

$$\Pi_F(\ell) = \frac{q^\ell}{\ell} + O\Big(\frac{q^{\ell/2}}{\ell}\Big). \tag{19.3}$$

Proof. First, since all the terms in the sum on the right hand side of (19.1) are non-negative, and $\ell\Pi_F(\ell)$ is one of these terms, we may deduce that $\ell\Pi_F(\ell) \leq q^\ell$, which proves the second inequality in (19.2). Since this holds for all ℓ, we have

$$\ell\Pi_F(\ell) = q^\ell - \sum_{\substack{k|\ell \\ k<\ell}} k\Pi_F(k) \geq q^\ell - \sum_{\substack{k|\ell \\ k<\ell}} q^k \geq q^\ell - \sum_{k=1}^{\lfloor \ell/2 \rfloor} q^k.$$

Let us set

$$S(q,\ell) := \sum_{k=1}^{\lfloor \ell/2 \rfloor} q^k = \frac{q}{q-1}(q^{\lfloor \ell/2 \rfloor} - 1),$$

so that $\ell\Pi_F(\ell) \geq q^\ell - S(q,\ell)$. It is easy to see that $S(q,\ell) = O(q^{\ell/2})$, which proves (19.3). For the first inequality of (19.2), it suffices to show that $S(q,\ell) \leq q^\ell/2$. One can verify this directly for $\ell \in \{1,2,3\}$, and for $\ell \geq 4$, we have

$$S(q,\ell) \leq q^{\ell/2+1} \leq q^{\ell-1} \leq q^\ell/2. \quad \square$$

We note that the inequalities in (19.2) are tight, in the sense that $\Pi_F(\ell) = q^\ell/2\ell$ when $q = 2$ and $\ell = 2$, and $\Pi_F(\ell) = q^\ell$ when $\ell = 1$. The first inequality in (19.2) implies not only that $\Pi_F(\ell) > 0$, but that the fraction of all monic degree ℓ polynomials that are irreducible is at least $1/2\ell$, while (19.3) says that this fraction gets arbitrarily close to $1/\ell$ as either q or ℓ are sufficiently large.

EXERCISE 19.1. Starting from Theorem 19.11, show that

$$\Pi_F(\ell) = \ell^{-1} \sum_{k|\ell} \mu(k) q^{\ell/k},$$

where μ is the Möbius function (see §2.9).

EXERCISE 19.2. How many irreducible polynomials of degree 30 over $\mathbb{Z}_2$ are there?

19.3 The subfield structure and uniqueness of finite fields

Let E be an extension of degree ℓ over a field F. If K is an intermediate field, that is, a subfield of E containing F, then Theorem 16.23 says that $(E : F) = (E : K)(K : F)$, and so in particular, the degree of K over F divides ℓ.

In the case where F is a finite field, we can say much more about such intermediate fields. Recall that if $\rho : E \to E$ be an F-algebra homomorphism, then the subalgebra of E fixed by ρ is defined as $K := \{\alpha \in E : \rho(\alpha) = \alpha\}$ (see Theorem 16.6). Not only is K a subalgebra of E, but it is also a field, and so K is itself an intermediate field.

Theorem 19.13. *Let E be an extension of degree ℓ over a finite field F. Let σ be the Frobenius map on E over F. Then the intermediate fields K, with $F \subseteq K \subseteq E$, are in one-to-one correspondence with the divisors k of ℓ, where the divisor k corresponds to the subalgebra of E fixed by σ^k, which has degree k over F.*

Proof. Let q be the cardinality of F.

Suppose k is a divisor of ℓ. By Theorem 19.6 (applied to E), the polynomial $X^{q^\ell} - X$ splits into distinct monic linear factors over E. By Theorem 19.4, the polynomial $X^{q^k} - X$ divides $X^{q^\ell} - X$. Hence, $X^{q^k} - X$ also splits into distinct monic linear factors over E. This says that the subalgebra of E fixed by σ^k, which consists of the roots of $X^{q^k} - X$, has precisely q^k elements, and hence is an extension of degree k over F.

Now let K be an arbitrary intermediate field, and let k be the degree of K over F. As already mentioned, we must have $k \mid \ell$. Also, by Theorem 19.8 (applied with K in place of F), K is the subalgebra of E fixed by σ^k. □

The next theorem shows that up to isomorphism, there is only one finite field of a given cardinality.

Theorem 19.14. *Let E and E' be finite extensions of the same degree over a finite field F. Then E and E' are isomorphic as F-algebras.*

Proof. Let q be the cardinality of F, and let ℓ be the degree of the extensions.

As we have argued before, we have $E' = F[\alpha']$ for some $\alpha' \in E'$, and so E' is isomorphic as an F-algebra to $F[X]/(\phi)$, where ϕ is the minimal polynomial of α' over F. As ϕ is an irreducible polynomial of degree ℓ, by Theorem 19.10, ϕ divides $X^{q^\ell} - X$, and by Theorem 19.6 (applied to E), $X^{q^\ell} - X = \prod_{\alpha \in E}(X - \alpha)$, from which it follows that ϕ has a root $\alpha \in E$. Since ϕ is irreducible, ϕ is the minimal polynomial of α over F, and hence $F[\alpha]$ is isomorphic as an F-algebra to $F[X]/(\phi)$. Since α has degree ℓ over F, we must have $E = F[\alpha]$. Thus, $E = F[\alpha] \cong F[X]/(\phi) \cong F[\alpha'] = E'$. □

EXERCISE 19.3. This exercise develops an alternative proof for the existence of finite fields—however, it does not yield a density result for irreducible polynomials. Let F be a finite field of cardinality q, and let $\ell \geq 1$ be an integer. Let E be a splitting field for the polynomial $X^{q^\ell} - X \in F[X]$ (see Theorem 16.25), and let σ be the Frobenius map on E over F. Let K be the subalgebra of E fixed by σ^ℓ. Show that K is an extension of F of degree ℓ.

EXERCISE 19.4. Let E be an extension of degree ℓ over a finite field F of cardinality q. Show that at least half the elements of E have degree ℓ over F, and that the total number of elements of degree ℓ over F is $q^\ell + O(q^{\ell/2})$.

EXERCISE 19.5. Let E be a finite extension of a finite field F, and suppose $\alpha, \beta \in E$, where α has degree a over F, β has degree b over F, and $\gcd(a, b) = 1$. Show that β has degree b over $F[\alpha]$, that α has degree a over $F[\beta]$, and that $\alpha+\beta$ has degree ab over F. Hint: consider the subfields $F[\alpha]$, $F[\beta]$, $F[\alpha][\beta] = F[\alpha, \beta] = F[\beta][\alpha]$, and $F[\alpha + \beta]$, and their degrees over F.

19.4 Conjugates, norms and traces

Throughout this section, F denotes a finite field of cardinality q, E denotes an extension of degree ℓ over F, and σ denotes the Frobenius map on E over F.

Consider an element $\alpha \in E$. We say that $\beta \in E$ is **conjugate to α (over F)** if $\beta = \sigma^i(\alpha)$ for some $i \in \mathbb{Z}$. The reader may verify that the "conjugate to" relation is an equivalence relation. We call the equivalence classes of this relation **conjugacy classes**, and we call the elements of the conjugacy class containing α the **conjugates of α**.

Starting with α, we can start listing conjugates:

$$\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots.$$

As σ^ℓ is the identity map, this list will eventually start repeating. Let k be the smallest positive integer such that $\sigma^k(\alpha) = \sigma^i(\alpha)$ for some $i = 0, \ldots, k-1$. It must

be the case that $i = 0$—otherwise, applying σ^{-1} to the equation $\sigma^k(\alpha) = \sigma^i(\alpha)$ would yield $\sigma^{k-1}(\alpha) = \sigma^{i-1}(\alpha)$, and since $0 \leq i - 1 < k - 1$, this would contradict the minimality of k.

Thus, $\alpha, \sigma(\alpha), \ldots, \sigma^{k-1}(\alpha)$ are all distinct, and $\sigma^k(\alpha) = \alpha$. Moreover, for every integer i, we have $\sigma^i(\alpha) = \sigma^j(\alpha)$, where $j = i \bmod k$. Therefore, the k distinct elements $\alpha, \sigma(\alpha), \ldots, \sigma^{k-1}(\alpha)$ are all the conjugates of α. Also, $\sigma^i(\alpha) = \alpha$ if and only if k divides i, and since $\sigma^\ell(\alpha) = \alpha$, it must be the case that k divides ℓ. In addition, the conjugates of α are powers of α, and in particular, they all belong to $F[\alpha]$.

With α and k as above, consider the polynomial

$$\phi := \prod_{i=0}^{k-1} (X - \sigma^i(\alpha)).$$

The coefficients of ϕ obviously lie in E, but we claim that in fact, they lie in F. This is easily seen as follows. Extend the domain of definition of σ from E to $E[X]$ by applying σ coefficient-wise to polynomials; this yields a ring homomorphism from $E[X]$ into $E[X]$, which we also denote by σ (see Example 7.46). Applying σ to ϕ, we obtain

$$\sigma(\phi) = \prod_{i=0}^{k-1} \sigma(X - \sigma^i(\alpha)) = \prod_{i=0}^{k-1} (X - \sigma^{i+1}(\alpha)) = \prod_{i=0}^{k-1} (X - \sigma^i(\alpha)),$$

since $\sigma^k(\alpha) = \alpha$. Thus we see that $\sigma(\phi) = \phi$. Writing $\phi = \sum_i c_i X^i$, it follows that $\sigma(c_i) = c_i$ for all i, and hence by Theorem 19.8, $c_i \in F$ for all i. Hence $\phi \in F[X]$. We further claim that ϕ is the minimal polynomial of α. To see this, let $f \in F[X]$ be any polynomial over F for which α is a root. Then for every integer i, by Theorem 16.7, we have

$$0 = \sigma^i(0) = \sigma^i(f(\alpha)) = f(\sigma^i(\alpha)).$$

Thus, all the conjugates of α are also roots of f, and so ϕ divides f. That proves that ϕ is the minimal polynomial of α. Since ϕ is the minimal polynomial of α and $\deg(\phi) = k$, it follows that the number k is none other than the degree of α over F.

Let us summarize the above discussion as follows:

Theorem 19.15. *Let $\alpha \in E$ be of degree k over F, and let ϕ be the minimal polynomial of α over F. Then k is the smallest positive integer such that $\sigma^k(\alpha) = \alpha$, the distinct conjugates of α are $\alpha, \sigma(\alpha), \ldots, \sigma^{k-1}(\alpha)$, and ϕ factors over E (in fact, over $F[\alpha]$) as*

$$\phi = \prod_{i=0}^{k-1} (X - \sigma^i(\alpha)).$$

Another useful way of reasoning about conjugates is as follows. First, if $\alpha = 0$, then the degree of α over F is 1, and there is nothing more to say, so let us assume that $\alpha \in E^*$. If r is the multiplicative order of α, then note that every conjugate $\sigma^i(\alpha)$ also has multiplicative order r — this follows from the fact that for every positive integer s, $\alpha^s = 1$ if and only if $(\sigma^i(\alpha))^s = 1$. Also, note that we must have $r \mid |E^*| = q^\ell - 1$, or equivalently, $q^\ell \equiv 1 \pmod{r}$. Focusing now on the fact that σ is the q-power map, we see that the degree k of α is the smallest positive integer such that $\alpha^{q^k} = \alpha$, which holds if and only if $\alpha^{q^k - 1} = 1$, which holds if and only if $q^k \equiv 1 \pmod{r}$. Thus, the degree of α over F is simply the multiplicative order of q modulo r. Again, we summarize these observations as a theorem:

Theorem 19.16. *If $\alpha \in E^*$ has multiplicative order r, then the degree of α over F is equal to the multiplicative order of q modulo r.*

For $\alpha \in E$, define the polynomial

$$\chi := \prod_{i=0}^{\ell-1} (X - \sigma^i(\alpha)).$$

It is easy to see, using the same type of argument as was used to prove Theorem 19.15, that $\chi \in F[X]$, and indeed, that

$$\chi = \phi^{\ell/k},$$

where k is the degree of α over F. The polynomial χ is called the **characteristic polynomial of α (from E to F)**.

Two functions that are often useful are the "norm" and "trace." The **norm of α (from E to F)** is defined as

$$\mathbf{N}_{E/F}(\alpha) := \prod_{i=0}^{\ell-1} \sigma^i(\alpha),$$

while the **trace of α (from E to F)** is defined as

$$\mathbf{Tr}_{E/F}(\alpha) := \sum_{i=0}^{\ell-1} \sigma^i(\alpha).$$

It is easy to see that both the norm and trace of α are elements of F, as they are fixed by σ; alternatively, one can see this by observing that they appear, possibly with a minus sign, as coefficients of the characteristic polynomial χ — indeed, the constant term of χ is equal to $(-1)^\ell \mathbf{N}_{E/F}(\alpha)$, and the coefficient of $X^{\ell-1}$ in χ is $-\mathbf{Tr}_{E/F}(\alpha)$.

The following two theorems summarize the most important facts about the norm and trace functions.

Theorem 19.17. *The function $\mathbf{N}_{E/F}$, restricted to E^*, is a group homomorphism from E^* onto F^*.*

Proof. We have

$$\mathbf{N}_{E/F}(\alpha) = \prod_{i=0}^{\ell-1} \alpha^{q^i} = \alpha^{\sum_{i=0}^{\ell-1} q^i} = \alpha^{(q^\ell-1)/(q-1)}.$$

Since E^* is a cyclic group of order $q^\ell - 1$, the image of the $(q^\ell - 1)/(q-1)$-power map on E^* is the unique subgroup of E^* of order $q-1$ (see Theorem 6.32). Since F^* is a subgroup of E^* of order $q-1$, it follows that the image of this power map is F^*. □

Theorem 19.18. *The function $\mathbf{Tr}_{E/F}$ is an F-linear map from E onto F.*

Proof. The fact that $\mathbf{Tr}_{E/F}$ is an F-linear map is a simple consequence of the fact that σ is an F-linear map. As discussed above, $\mathbf{Tr}_{E/F}$ maps into F. Since the image of $\mathbf{Tr}_{E/F}$ is a subspace of F, the image is either $\{0\}$ or F, and so it suffices to show that $\mathbf{Tr}_{E/F}$ does not map all of E to zero. But an element $\alpha \in E$ is in the kernel of $\mathbf{Tr}_{E/F}$ if and only if α is a root of the polynomial

$$X + X^q + \cdots + X^{q^{\ell-1}},$$

which has degree $q^{\ell-1}$. Since E contains q^ℓ elements, not all elements of E can lie in the kernel of $\mathbf{Tr}_{E/F}$. □

Example 19.1. As an application of some of the above theory, let us investigate the factorization of the polynomial $X^r - 1$ over F, a finite field of cardinality q. Let us assume that $r > 0$ and is relatively prime to q. Let E be a splitting field of $X^r - 1$ (see Theorem 16.25), so that E is a finite extension of F in which $X^r - 1$ splits into linear factors:

$$X^r - 1 = \prod_{i=1}^{r} (X - \alpha_i).$$

We claim that the roots α_i of $X^r - 1$ are distinct—this follows from the Theorem 19.1 and the fact that $\gcd(X^r - 1, rX^{r-1}) = 1$.

Next, observe that the r roots of $X^r - 1$ in E actually form a subgroup of E^*, and since E^* is cyclic, this subgroup must be cyclic as well. So the roots of $X^r - 1$ form a cyclic subgroup of E^* of order r. Let ζ be a generator for this group. Then all the roots of $X^r - 1$ are contained in $F[\zeta]$, and so we may as well assume that $E = F[\zeta]$.

Let us compute the degree of ζ over F. By Theorem 19.16, the degree ℓ of ζ over F is the multiplicative order of q modulo r. Moreover, the $\varphi(r)$ roots of

$X^r - 1$ of multiplicative order r are partitioned into $\varphi(r)/\ell$ conjugacy classes, each of size ℓ (here, φ is Euler's phi function); indeed, as the reader is urged to verify, these conjugacy classes are in one-to-one correspondence with the cosets of the subgroup of $\mathbb{Z}_r^*$ generated by $[q]_r$, where each such coset $C \subseteq \mathbb{Z}_r^*$ corresponds to the conjugacy class $\{\zeta^a : [a]_r \in C\}$.

More generally, for every $s \mid r$, every root of $X^r - 1$ whose multiplicative order is s has degree k over F, where k is the multiplicative order of q modulo s. As above, the $\varphi(s)$ roots of multiplicative order s are partitioned into $\varphi(s)/k$ conjugacy classes, which are in one-to-one correspondence with the cosets of the subgroup of $\mathbb{Z}_s^*$ generated by $[q]_s$.

This tells us exactly how $X^r - 1$ splits into irreducible factors over F. Things are a bit simpler when r is prime, in which case, from the above discussion, we see that

$$X^r - 1 = (X - 1) \prod_{i=1}^{(r-1)/\ell} f_i,$$

where the f_i's are distinct monic irreducible polynomials, each of degree ℓ, and ℓ is the multiplicative order of q modulo r.

In the above analysis, instead of constructing the field E using Theorem 16.25, one could instead simply construct E as $F[X]/(f)$, where f is any irreducible polynomial of degree ℓ, and where ℓ is the multiplicative order of q modulo r. We know that such a polynomial f exists by Theorem 19.12, and since E has cardinality q^ℓ, and $r \mid (q^\ell - 1) = |E^*|$, and E^* is cyclic, we know that E^* contains an element ζ of multiplicative order r, and each of the r distinct powers $1, \zeta, \ldots, \zeta^{r-1}$ are roots of $X^r - 1$, and so this E is a splitting field of $X^r - 1$ over F. □

EXERCISE 19.6. Let E be an extension of degree ℓ over a finite field F. Show that for $a \in F$, we have $\mathbf{N}_{E/F}(a) = a^\ell$ and $\mathbf{Tr}_{E/F}(a) = \ell a$.

EXERCISE 19.7. Let E be a finite extension of a finite field F. Let K be an intermediate field, $F \subseteq K \subseteq E$. Show that for all $\alpha \in E$

(a) $\mathbf{N}_{E/F}(\alpha) = \mathbf{N}_{K/F}(\mathbf{N}_{E/K}(\alpha))$, and

(b) $\mathbf{Tr}_{E/F}(\alpha) = \mathbf{Tr}_{K/F}(\mathbf{Tr}_{E/K}(\alpha))$.

EXERCISE 19.8. Let F be a finite field, and let $f \in F[X]$ be a monic irreducible polynomial of degree ℓ. Let $E = F[X]/(f) = F[\xi]$, where $\xi := [X]_f$.

(a) Show that

$$\frac{\mathbf{D}(f)}{f} = \sum_{j=1}^{\infty} \mathbf{Tr}_{E/F}(\xi^{j-1}) X^{-j}.$$

(b) From part (a), deduce that the sequence of elements

$$\mathbf{Tr}_{E/F}(\xi^{j-1}) \quad (j = 1, 2, \ldots)$$

is linearly generated over F with minimal polynomial f.

(c) Show that one can always choose a polynomial f so that sequence in part (b) is purely periodic with period $q^\ell - 1$.

EXERCISE 19.9. Let F be a finite field, and $f \in F[X]$ a monic irreducible polynomial of degree k over F. Let E be an extension of degree ℓ over F. Show that over E, f factors as the product of d distinct monic irreducible polynomials, each of degree k/d, where $d := \gcd(k, \ell)$.

EXERCISE 19.10. Let E be a finite extension of a finite field F of characteristic p. Show that if $\alpha \in E$ and $0 \neq a \in F$, and if α and $\alpha + a$ are conjugate over F, then p divides the degree of α over F.

EXERCISE 19.11. Let F be a finite field of characteristic p. For $a \in F$, consider the polynomial $f := X^p - X - a \in F[X]$.

(a) Show that if $F = \mathbb{Z}_p$ and $a \neq 0$, then f is irreducible.

(b) More generally, show that if $\mathbf{Tr}_{F/\mathbb{Z}_p}(a) \neq 0$, then f is irreducible, and otherwise, f splits into distinct monic linear factors over F.

EXERCISE 19.12. Let E be a finite extension of a finite field F. Show that every F-algebra automorphism on E must be a power of the Frobenius map on E over F.

EXERCISE 19.13. Show that for all primes p, the polynomial $X^4 + 1$ is reducible in $\mathbb{Z}_p[X]$. (Contrast this to the fact that this polynomial is irreducible in $\mathbb{Q}[X]$, as discussed in Exercise 16.49.)

EXERCISE 19.14. This exercise depends on the concepts and results in §18.6. Let E be an extension of degree ℓ over a finite field F. Let σ be the Frobenius map on E over F.

(a) Show that the minimal polynomial of σ over F is $X^\ell - 1$.

(b) Show that there exists $\beta \in E$ such that the minimal polynomial of β under σ is $X^\ell - 1$.

(c) Conclude that $\beta, \sigma(\beta), \ldots, \sigma^{\ell-1}(\beta)$ form a basis for E over F. This type of basis is called a **normal basis**.