Chapter 4

Finite fields: further properties

8 Roots of unity in finite fields

In this section, we will generalize the concept of roots of unity (well-known for complex numbers) to the finite field setting, by considering the splitting field of the polynomial $x^n - 1$. This has links with irreducible polynomials, and provides an effective way of obtaining primitive elements and hence representing finite fields.

Definition 8.1
Let $n \in \mathbb{N}$. The splitting field of $x^n - 1$ over a field K is called the *nth cyclotomic field* over K and denoted by $K^{(n)}$. The roots of $x^n - 1$ in $K^{(n)}$ are called the nth roots of unity over K and the set of all these roots is denoted by $E^{(n)}$.

The following result, concerning the properties of $E^{(n)}$, holds for an arbitrary (not just a finite!) field K.

Theorem 8.2
Let $n \in \mathbb{N}$ and K a field of characteristic p (where p may take the value 0 in this theorem). Then

(i) If $p \nmid n$, then $E^{(n)}$ is a cyclic group of order n with respect to multiplication in $K^{(n)}$.

(ii) If $p \mid n$, write $n = mp^e$ with positive integers m and e and $p \nmid m$. Then $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ and the roots of $x^n - 1$ are the m elements of $E^{(m)}$, each occurring with multiplicity p^e.

Proof.

(i) The $n = 1$ case is trivial. For $n \geq 2$, observe that $x^n - 1$ and its derivative nx^{n-1} have no common roots; thus $x^n - 1$ cannot have multiple roots and hence $E^{(n)}$ has n elements. To see that $E^{(n)}$ is a multiplicative group, take $\alpha, \beta \in E^{(n)}$: we have $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = 1$ and so $\alpha\beta^{-1} \in E^{(n)}$. It remains to show that the group $E^{(n)}$ is cyclic; this can be proved by an analogous argument to the proof of Theorem 6.9 (exercise: fill in details).

(ii) Immediate from $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$ and part (i).

■

Definition 8.3
Let K be a field of characteristic p and n a positive integer not divisible by p. Then a generator of the cyclic group $E^{(n)}$ is called a *primitive nth root of unity over K*.

By Theorem 1.13, $E^{(n)}$ has $\phi(n)$ generators, i.e. there are $\phi(n)$ primitive nth roots of unity over K. Given one such, ζ say, the set of all primitive nth roots of unity over K is given by

$$\{\zeta^s : 1 \leq s \leq n,\ \gcd(s,n) = 1\}.$$

We now consider the polynomial whose roots are precisely this set.

Definition 8.4
Let K be a field of characteristic p, n a positive integer not divisible by p and ζ a primitive nth root of unity over K. Then the polynomial

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \zeta^s)$$

is called the nth cyclotomic polynomial over K. It is clear that $Q_n(x)$ has degree $\phi(n)$.

Theorem 8.5
Let K be a field of characteristic p and n a positive integer not divisible by p. Then

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$;

(ii) the coefficients of $Q_n(x)$ belong to the prime subfield of K (and in fact to $\mathbb{Z}$ if the prime subfield is $\mathbb{Q}$).

Proof. (i) Each nth root of unity over K is a primitive dth root of unity over K for exactly one positive divisor d of n. Specifically, if ζ is a primitive nth root of unity over K and ζ^s is an arbitrary nth root of unity over K, then $d = n/\gcd(s,n)$, i.e. d is the order of ζ^s in $E^{(n)}$. Since

$$x^n - 1 = \prod_{s=1}^{n} (x - \zeta^s).$$

we obtain the result by collecting together those factors $(x - \zeta^s)$ for which ζ^s is a primitive dth root of unity over K.
(ii) Proved by induction on n. It is clearly true for $Q_1(x) = x - 1$. Let $n > 1$ and suppose it is true for all $Q_d(x)$ where $1 \leq d < n$. By (i),

$$Q_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} Q_d(x)}.$$

By the induction hypothesis, the denominator is a polynomial with coefficients in the prime subfield of K (or $\mathbb{Z}$ if $\mathrm{char} K = 0$). Applying long division yields the result. ■

Example 8.6
Let $n = 3$, let K be any field with $\mathrm{char} K \neq 3$, and let ζ be a primitive cube root of unity over K. Then

$$Q_3(x) = (x - \zeta)(x - \zeta^2) = x^2 - (\zeta + \zeta^2)x + \zeta^3 = x^2 + x + 1.$$

Example 8.7
Let r be a prime and let $k \in \mathbb{N}$. Then

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}}$$

since

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x)\cdots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}$$

by Theorem 8.5 (i). When $k = 1$, we have $Q_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$.

In fact, using the Moebius Inversion Formula, we can establish an explicit formula for the nth cyclotomic polynomial Q_n, for every $n \in \mathbb{N}$.

Theorem 8.8
For a field K of characteristic p and $n \in \mathbb{N}$ not divisible by p, the nth cyclotomic polynomial Q_n over K satisfies

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Proof. Apply the multiplicative form of the Mobius Inversion Formula (Theorem 7.12) to the multiplicative group G of non-zero rational functions over K. Take $h(n) = Q_n(x)$ and $H(n) = x^n - 1$ for all $n \in \mathbb{N}$. By Theorem 8.5, the identity (3.3) is satisfied, and so applying Moebius Inversion yields the desired formula. ■

Example 8.9
Let $n = 12$, and let K be any field over which Q_{12} is defined. Then

$$\begin{aligned} Q_{12}(x) &= \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} \\ &= (x^{12}-1)^{\mu(1)}(x^6-1)^{\mu(2)}(x^4-1)^{\mu(3)}(x^3-1)^{\mu(4)}(x^2-1)^{\mu(6)}(x-1)^{\mu(12)} \\ &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = x^4 - x^2 + 1. \end{aligned}$$

Before the next theorem, we make a definition.

Definition 8.10
Let n be a positive integer and b an integer relatively prime to n. Then the least positive integer k such that $n|b^k - 1$ (equivalently, $b^k \equiv 1 \bmod n$) is called the *multiplicative order* of b modulo n, and denoted $\mathrm{ord}_n(b)$.

Example 8.11
(i) $\mathrm{ord}_8(5) = 2$; (ii) $\mathrm{ord}_{31}(2) = 5$; (iii) $\mathrm{ord}_9(4) = 3$.

Theorem 8.12
The cyclotomic field $K^{(n)}$ is a simple algebraic extension of K. Moreover, if $K = \mathbb{F}_q$ with $\gcd(q, n) = 1$, and $d = \mathrm{ord}_n(q)$, then

- *Q_n factors into $\phi(n)/d$ distinct polynomials in $K[x]$ of the same degree d;*
- *$K^{(n)}$ is the splitting field of any such irreducible factor over K;*
- *$[K^{(n)} : K] = d$.*

Proof. If there exists a primitive nth root of unity ζ over K, then $K^{(n)} = K(\zeta)$. Otherwise, we have the situation of Theorem 8.2 (ii); here $K^{(n)} = K^{(m)}$ and the first result again holds.

Now let K be the finite field $\mathbb{F}_q$, assume $\gcd(q, n) = 1$, such that primitive nth roots of unity over $\mathbb{F}_q$ exist. Let η be one of them. Then

$$\eta \in \mathbb{F}_{q^k} \Leftrightarrow \eta^{q^k} = \eta \Leftrightarrow q^k \equiv 1 \bmod n.$$

The smallest positive integer for which this holds is $k = d$, so η is in $\mathbb{F}_{q^d}$ but not in any proper subfield. Thus the minimal polynomial of η over $\mathbb{F}_q$ has degree d. Since η was an arbitrary root of $Q_n(x)$, the result follows, because we can successively divide by the minimal polynomials of the roots of $Q_n(x)$. ■

Example 8.13
Take $q = 11$ and $n = 12$.

- From Example 8.9, we have $K = \mathbb{F}_{11}$ and $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. We are interested in $K^{(12)}$.
- Since $12 \nmid 11 - 1$ but $12 | 11^2 - 1$, the multiplicative order d of 11 modulo 12 is 2.
- So, $Q_{12}(x)$ factors into $\phi(12)/2 = 4/2 = 2$ monic quadratics, both irreducible over $\mathbb{F}_{11}[x]$, and the cyclotomic field $K^{(12)} = \mathbb{F}_{121}$.
- We can check that the factorization is in fact $Q_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$.

The following result, which ties together cyclotomic and finite fields, is very useful.

Theorem 8.14
The finite field $\mathbb{F}_q$ is the $(q-1)$st cyclotomic field over any one of its subfields.

Proof. Since the $q - 1$ non-zero elements of $\mathbb{F}_q$ are all the roots of the polynomial $x^{q-1} - 1$, this polynomial splits in $\mathbb{F}_q$. Clearly, it cannot split in any proper subfield of $\mathbb{F}_q$, so that $\mathbb{F}_q$ is the splitting field of $x^{q-1} - 1$ over any one of its subfields. ■

9 Using cyclotomic polynomials

Cyclotomic fields give us another way of expressing the elements of a finite field $\mathbb{F}_q$. Since $\mathbb{F}_q$ is the $(q-1)$st cyclotomic field over $\mathbb{F}_p$, we can construct it as follows:

- Find the decomposition of the $(q-1)$st cyclotomic polynomial $Q_{q-1} \in \mathbb{F}_p[x]$ into irreducible factors in $\mathbb{F}_p[x]$, which are all of the same degree.
- A root α of any of these factors is a primitive $(q-1)$st root of unity over $\mathbb{F}_p$, and hence a primitive element of $\mathbb{F}_q$.
- For such an α we have $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\}$.

Example 9.1
Consider the field $\mathbb{F}_9$.

- $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, the eighth cyclotomic field over $\mathbb{F}_3$.
- As in Example 8.7,
$$Q_8(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1 \in \mathbb{F}_3[x].$$
Its decomposition into irreducible factors in $\mathbb{F}_3[x]$ is
$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2);$$
we have $\phi(8)/\mathrm{ord}_8(3) = 4/2 = 2$ factors of degree 2.
- Let ζ be a root of $x^2 + x + 2$; then ζ is a primitive eighth root of unity over $\mathbb{F}_3$. Hence $\mathbb{F}_9 = \{0, \zeta, \zeta^2, \ldots, \zeta^7, \zeta^8 = 1\}$.

We can now ask: how does this new representation for $\mathbb{F}_9$ correspond to our earlier viewpoint, where $\mathbb{F}_9$ was considered as a simple algebraic extension of $\mathbb{F}_3$ of degree 2, obtained by adjoining a root of an irreducible quadratic?

Example 9.2
Consider the polynomial $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. This quadratic is irreducible over $\mathbb{F}_3$. So we can build $\mathbb{F}_9$ by adjoining a root α of $f(x)$ to $\mathbb{F}_3$. Then $f(\alpha) = \alpha^2 + 1 = 0$ in $\mathbb{F}_9$, and the nine elements of $\mathbb{F}_9$ are given by $\{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

Now, note that the polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$, from Example 9.1, has $\zeta = 1 + \alpha$ as a root. So, the elements in the two representations of $\mathbb{F}_9$ correspond as in the following table

i	ζ^i
1	$1+\alpha$
2	2α
3	$1+2\alpha$
4	2
5	$2+2\alpha$
6	α
7	$2+\alpha$
8	1

Another use of cyclotomic polynomials is that they help us to determine irreducible polynomials.

Theorem 9.3
Let $I(q, n; x)$ be (as in Theorem 7.16) the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n. Then for $n > 1$ we have

$$I(q, n; x) = \prod_m Q_m(x),$$

where the product is extended over all positive divisors m of $q^n - 1$ for which n is the multiplicative order of q modulo m, and where $Q_m(x)$ is the mth cyclotomic polynomial over $\mathbb{F}_q$.

Proof.

- For $n > 1$, let S be the set of elements of $\mathbb{F}_{q^n}$ that are of degree n over $\mathbb{F}_q$. Then every $\alpha \in S$ has a minimal polynomial over $\mathbb{F}_q$ of degree n and is therefore a root of $I(q, n; x)$. Conversely, if β is a root of $I(q, n; x)$, then β is a root of some monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree n, implying $\beta \in S$. Thus
$$I(q, n; x) = \prod_{\alpha \in S} (x - \alpha).$$
- If $\alpha \in S$, then $\alpha \in \mathbb{F}_{q^n}^*$, so the order of α in that multiplicative group is a divisor of $q^n - 1$. In fact, the order m of an element of S must be such that n is the least positive integer with $m | q^n - 1$, i.e. $n = \mathrm{ord}_m(q)$. This is because an element $\gamma \in \mathbb{F}_{q^n}^*$ lies in a proper subfield $\mathbb{F}_{q^d}$ if and only if $\gamma^{q^d} = \gamma$, i.e. if and only if the order of γ divides $q^d - 1$.
- For a positive divisor m of $q^n - 1$ which satisfies $n = \mathrm{ord}_m(q)$, let S_m be the set of elements of S of order m. Then S is the disjoint union of the subsets S_m, so we have
$$I(q, n; x) = \prod_m \prod_{\alpha \in S_m} (x - \alpha).$$
Now, S_m contains precisely all elements of $\mathbb{F}_{q^n}^*$ of order m. So S_m is the set of primitive mth roots of unity over $\mathbb{F}_q$. From the definition of cyclotomic polynomials, we have
$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m(x),$$
and hence the result follows.

■

Example 9.4
We determine all monic irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2.

- Here $q = 3$ and $n = 2$, so $q^n - 1 = 8$ and $2 = \mathrm{ord}_m(3)$ for divisors $m = 4$ and $m = 8$ of $q^n - 1$. Thus from Theorem 9.3 we have
$$I(3, 2; x) = Q_4(x)Q_8(x).$$
- From Theorem 8.12, we know that $Q_4(x)$ factors into $\phi(4)/2 = 1$ monic irreducible quadratic over $\mathbb{F}_3$, while $Q_8(x)$ factors into $\phi(8)/2 = 2$ monic irreducible quadratics over $\mathbb{F}_3$.
- By Theorem 8.8,
$$Q_4(x) = \prod_{d|4}(x^{\frac{4}{d}} - 1)^{\mu(d)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1,$$
while
$$Q_8(x) = x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$$
as in Example 9.1. Thus the irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2 are x^2+1, x^2+x+2 and $x^2 + 2x + 2$.

Example 9.5
We determine all monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 4.

- Here $q = 2$ and $n = 4$, so $q^n - 1 = 15$ and $4 = \mathrm{ord}_m(2)$ for divisors $m = 5$ and $m = 15$ of $q^n - 1$. Thus from Theorem 9.3 we have
$$I(2, 4; x) = Q_5(x)Q_{15}(x).$$
- From Theorem 8.12, we know that $Q_5(x)$ factors into $\phi(5)/4 = 1$ monic irreducible quartic over $\mathbb{F}_2$, while $Q_{15}(x)$ factors into $\phi(15)/4 = 8/4 = 2$ monic irreducible quartics over $\mathbb{F}_2$.
- By Theorem 8.8,
$$Q_5(x) = \prod_{d|5}(x^{\frac{5}{d}} - 1)^{\mu(d)} = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$
and
$$\begin{aligned} Q_{15}(x) &= \prod_{d|15}(x^{\frac{15}{d}} - 1)^{\mu(d)} \\ &= \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} \\ &= \frac{x^{10} + x^5 + 1}{x^2 + x + 1} \\ &= x^8 + x^7 + x^5 + x^4 + x^3 + x + 1. \end{aligned}$$
We note that $Q_5(x + 1) = x^4 + x^3 + 1$ is also irreducible in $\mathbb{F}_2[x]$ and hence must divide $Q_{15}(x)$, leading to the factorization
$$Q_{15}(x) = (x^4 + x^3 + 1)(x^4 + x + 1).$$
Thus the irreducible polynomials in $\mathbb{F}_2[x]$ of degree 4 are $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x + 1$.