(2) The polynomial $p(x) = x^{2^m} - t$ over $F = \mathbb{F}_2(t)$ is irreducible with the same separable polynomial part, but with inseparability degree 2^m.

(3) The polynomial $(x^{p^2} - t)(x^p - t)$ over $F = \mathbb{F}_p(t)$ has (two) inseparable irreducible factors so is inseparable. This polynomial cannot be written in the form $f_{sep}(x^{p^k})$ where $f_{sep}(x)$ is separable, which is the reason we restricted to *irreducible* polynomials above. This example also shows that there is no analogous factorization to define the separable and inseparable degrees of a general polynomial.

The notion of separability carries over to the fields generated by the roots of these polynomials.

Definition. The field K is said to be *separable* (or *separably algebraic*) over F if every element of K is the root of a separable polynomial over F (equivalently, the minimal polynomial over F of every element of K is separable). A field which is not separable is *inseparable*.

We have seen that the issue of separability is straightforward for finite extensions of perfect fields since for these fields the minimal polynomial of an algebraic element is irreducible hence separable.

Corollary 39. Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

We shall consider separable and inseparable extensions more after developing some Galois Theory, in particular defining the separable and inseparable *degree* of the extension K/F.

EXERCISES

1. Prove that the derivative D_x of a polynomial satisfies $D_x(f(x) + g(x)) = D_x(f(x)) + D_x(g(x))$ and $D_x(f(x)g(x)) = D_x(f(x))g(x) + D_x(g(x))f(x)$ for any two polynomials $f(x)$ and $g(x)$.
2. Find all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.
3. Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$. [Note that if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.]
4. Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$ (cf. the previous exercise). Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.
5. For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach — prove first that if α is a root then $\alpha + 1$ is also a root. Another approach — suppose it's reducible and compute derivatives.]
6. Prove that $x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive *Wilson's Theorem*: $(p-1)! \equiv -1 \pmod p$.

7. Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extensions of K.

8. Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.

9. Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$.

10. Let $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be a polynomial in the variables $x_1, x_2, \ldots, x_n$ with integer coefficients. For any prime p prove that the polynomial

$$f(x_1, x_2, \ldots, x_n)^p - f(x_1^p, x_2^p, \ldots, x_n^p) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

has all its coefficients divisible by p.

11. Suppose $K[x]$ is a polynomial ring over the field K and F is a subfield of K. If F is a perfect field and $f(x) \in F[x]$ has no repeated irreducible factors in $F[x]$, prove that $f(x)$ has no repeated irreducible factors in $K[x]$.

13.6 CYCLOTOMIC POLYNOMIALS AND EXTENSIONS

The purpose of this section is to prove that the cyclotomic extension

$$\mathbb{Q}(\zeta_n)/\mathbb{Q}$$

generated by the n^{th} roots of unity over $\mathbb{Q}$ introduced in Section 4 is of degree $\varphi(n)$ where φ denotes Euler's phi-function (= the number of integers a, $1 \leq a < n$ relatively prime to n = the order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$).

Definition. Let μ_n denote the *group of n^{th} roots of unity over* $\mathbb{Q}$.

Then as we have already observed, $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$ as groups (under multiplication on the right, addition on the left), given explicitly by the map $a \mapsto (\zeta_n)^a$ for a fixed primitive n^{th} root of unity. The primitive n^{th} roots of unity are given by the residue classes prime to n so there are precisely $\varphi(n)$ primitive n^{th} roots of unity.

If d is a divisor of n and ζ is a d^{th} root of unity, then ζ is also an n^{th} root of unity since $\zeta^n = (\zeta^d)^{n/d} = 1$. Hence

$$\mu_d \subseteq \mu_n \qquad \text{for all } d \mid n.$$

Conversely, the order of any element of the group μ_n is a divisor of n so that if ζ is an n^{th} root of unity which is also a d^{th} root of unity for some smaller d then $d \mid n$.

Definition. Define the n^{th} *cyclotomic polynomial* $\Phi_n(x)$ to be the polynomial whose roots are the primitive n^{th} roots of unity:

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } \in \mu_n} (x - \zeta) = \prod_{\substack{1 \leq a < n \\ (a,n)=1}} (x - \zeta_n{}^a)$$

(which is of degree $\varphi(n)$).

The roots of the polynomial $x^n - 1$ are precisely the n^{th} roots of unity so we have the factorization

$$x^n - 1 = \prod_{\substack{\zeta^n=1 \\ \text{i.e. } \zeta\in\mu_n}} (x - \zeta).$$

If we group together the factors $(x - \zeta)$ where ζ is an element of order d in μ_n (i.e., ζ is a primitive d^{th} root of unity) we obtain

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta\in\mu_d \\ \zeta \text{ primitive}}} (x - \zeta).$$

The inner product is $\Phi_d(x)$ by definition so we have the factorization

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{13.4}$$

Note incidentally that comparing degrees gives the identity

$$n = \sum_{d|n} \varphi(d).$$

This factorization allows us to compute $\Phi_n(x)$ for any n recursively: clearly $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Then

$$x^3 - 1 = \Phi_1(x)\Phi_3(x) = (x - 1)\Phi_3(x)$$

which gives

$$\Phi_3(x) = x^2 + x + 1.$$

Similarly

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x - 1)(x + 1)\Phi_4(x)$$

gives

$$\Phi_4(x) = x^2 + 1$$

(in these cases these could also be obtained directly from the explicit roots of unity). Continuing in this fashion we can compute $\Phi_n(x)$ for any n. Note also that for p a prime we recover our polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

For some small values of n the polynomials are

$$\begin{aligned}
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{11}(x) &= x^{10} + x^9 + \cdots + x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1.
\end{aligned}$$

For all the values computed above, $\Phi_n(x)$ was a (monic) polynomial with integer coefficients. This is always the case:

Lemma 40. The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof: It is clear that $\Phi_n(x)$ is monic and has degree $\varphi(n)$. We must show the coefficients lie in $\mathbb{Z}$. We use induction on n. The result is true for $n = 1$ (and $n \leq 12$). Assume by induction that $\Phi_d(x) \in \mathbb{Z}[x]$ for all $1 \leq d < n$. Then $x^n - 1 = f(x)\Phi_n(x)$ where $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ is monic and has coefficients in $\mathbb{Z}$. Since $f(x)$ clearly divides $x^n - 1$ in $F[x]$ where $F = \mathbb{Q}(\zeta_n)$ is the field of n^{th} roots of unity and both $f(x)$ and $x^n - 1$ have coefficients in $\mathbb{Q}$, $f(x)$ divides $x^n - 1$ in $\mathbb{Q}[x]$ by the Division Algorithm (cf. the remark at the end of Section 9.2). By Gauss' Lemma, $f(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, hence $\Phi_n(x) \in \mathbb{Z}[x]$.

We remark in passing that while all the coefficients of $\Phi_n(x)$ in the examples computed above were $0, \pm 1$, it is known that there are cyclotomic polynomials with arbitrarily large coefficients.

Theorem 41. The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof: We must show that $\Phi_n(x)$ is irreducible. If not then we have a factorization

$$\Phi_n(x) = f(x)g(x) \qquad \text{with } f(x), g(x) \text{ monic in } \mathbb{Z}[x]$$

where we take $f(x)$ to be an *irreducible* factor of $\Phi_n(x)$. Let ζ be a primitive n^{th} root of 1 which is a root of $f(x)$ (so then $f(x)$ is the minimal polynomial for ζ over $\mathbb{Q}$) and let p denote *any* prime not dividing n. Then ζ^p is again a primitive n^{th} root of 1, hence is a root of either $f(x)$ or $g(x)$.

Suppose $g(\zeta^p) = 0$. Then ζ is a root of $g(x^p)$ and since $f(x)$ is the minimal polynomial for ζ, $f(x)$ must divide $g(x^p)$ in $\mathbb{Z}[x]$, say

$$g(x^p) = f(x)h(x), \qquad h(x) \in \mathbb{Z}[x].$$

If we reduce this equation mod p, we obtain

$$\bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \qquad \text{in } \mathbb{F}_p[x].$$

By the remarks of the last section,

$$\bar{g}(x^p) = (\bar{g}(x))^p$$

so we have the equation

$$(\bar{g}(x))^p = \bar{f}(x)\bar{h}(x)$$

in the U.F.D. $\mathbb{F}_p[x]$. It follows that $\bar{f}(x)$ and $\bar{g}(x)$ have a factor in common in $\mathbb{F}_p[x]$.

Now, from $\Phi_n(x) = f(x)g(x)$ we see by reducing mod p that $\overline{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$, and so by the above it follows that $\overline{\Phi}_n(x) \in \mathbb{F}_p[x]$ has a multiple root. But then also $x^n - 1$ would have a multiple root over $\mathbb{F}_p$ since it has $\overline{\Phi}_n(x)$ as a factor. This is a