contradiction since we have seen in the last section that there are $n$ distinct roots of $x^n - 1$ over any field of characteristic not dividing $n$.

Hence $\zeta^p$ must be a root of $f(x)$. Since this applies to every root $\zeta$ of $f(x)$, it follows that $\zeta^a$ is a root of $f(x)$ for every integer $a$ relatively prime to $n$: write $a = p_1 p_2 \cdots p_k$ as a product of (not necessarily distinct) primes not dividing $n$ so that $\zeta^{p_1}$ is a root of $f(x)$, so also $(\zeta^{p_1})^{p_2}$ is a root of $f(x)$, etc. But this means that *every* primitive $n^{\text{th}}$ root of unity is a root of $f(x)$, i.e., $f(x) = \Phi_n(x)$, showing $\Phi_n(x)$ is irreducible.

**Corollary 42.** The degree over $\mathbb{Q}$ of the cyclotomic field of $n^{\text{th}}$ roots of unity is $\varphi(n)$:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

*Proof:* By the theorem, $\Phi_n(x)$ is the minimal polynomial for any primitive $n^{\text{th}}$ root of unity $\zeta_n$.

**Example**

The cyclotomic field $\mathbb{Q}(\zeta_8)$ of the $8^{\text{th}}$ roots of unity is of degree $\varphi(8) = 4$ over $\mathbb{Q}$. This field contains the $4^{\text{th}}$ roots of unity, i.e., $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$ as well as the element $\zeta_8 + \zeta_8^7 = \sqrt{2}$ (recall the explicit roots of unity in Section 4). It follows that

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}).$$

One interesting number-theoretic application of the cyclotomic polynomials outlined in the exercises is the proof that for any $n$ there are infinitely many primes which are congruent to 1 modulo $n$. The complete factorization in $\mathbb{F}_p[x]$ of $\Phi_\ell(x)$ for a prime $\ell$ (which is irreducible in $\mathbb{Z}[x]$) is described in Exercise 8 below.

We shall return to the example of cyclotomic fields after we have developed some Galois Theory.

## EXERCISES

1. Suppose $m$ and $n$ are relatively prime positive integers. Let $\zeta_m$ be a primitive $m^{\text{th}}$ root of unity and let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity. Prove that $\zeta_m \zeta_n$ is a primitive $mn^{\text{th}}$ root of unity.
2. Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity and let $d$ be a divisor of $n$. Prove that $\zeta_n^d$ is a primitive $(n/d)^{\text{th}}$ root of unity.
3. Prove that if a field contains the $n^{\text{th}}$ roots of unity for $n$ odd then it also contains the $2n^{\text{th}}$ roots of unity.
4. Prove that if $n = p^k m$ where $p$ is a prime and $m$ is relatively prime to $p$ then there are precisely $m$ distinct $n^{\text{th}}$ roots of unity over a field of characteristic $p$.
5. Prove there are only a finite number of roots of unity in any finite extension $K$ of $\mathbb{Q}$.
6. Prove that for $n$ odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.
7. Use the Möbius Inversion formula indicated in Section 14.3 to prove

$$\Phi_m(x) = \prod_{d|n} (x^d - 1)^{\mu(m/d)}.$$

**8.** Let $\ell$ be a prime and let $\Phi_\ell(x) = \frac{x^\ell - 1}{x-1} = x^{\ell-1} + x^{\ell-2} + \ldots + x + 1 \in \mathbb{Z}[x]$ be the $\ell^{\text{th}}$ cyclotomic polynomial, which is irreducible over $\mathbb{Z}$ by Theorem 41. This exercise determines the factorization of $\Phi_\ell(x)$ modulo $p$ for any prime $p$. Let $\zeta$ denote any fixed primitive $\ell^{\text{th}}$ root of unity.

**(a)** Show that if $p = l$ then $\Phi_\ell(x) = (x-1)^{\ell-1} \in \mathbb{F}_\ell[x]$.

**(b)** Suppose $p \neq \ell$ and let $f$ denote the order of $p$ mod $\ell$, i.e., $f$ is the smallest power of $p$ with $p^f \equiv 1 \bmod \ell$. Use the fact that $\mathbb{F}_{p^n}^\times$ is a cyclic group to show that $n = f$ is the smallest power $p^n$ of $p$ with $\zeta \in \mathbb{F}_{p^n}$. Conclude that the minimal polynomial of $\zeta$ over $\mathbb{F}_p$ has degree $f$.

**(c)** Show that $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer $a$ not divisible by $\ell$. [One inclusion is obvious. For the other, note that $\zeta = (\zeta^a)^b$ where $b$ is the multiplicative inverse of $a$ mod $\ell$.] Conclude using (b) that, in $\mathbb{F}_p[x]$, $\Phi_\ell(x)$ is the product of $\frac{\ell-1}{f}$ distinct irreducible polynomials of degree $f$.

**(d)** In particular, prove that, viewed in $\mathbb{F}_p[x]$, $\Phi_7(x) = x^6 + x^5 + \ldots + x + 1$ is $(x-1)^6$ for $p = 7$, a product of distinct linear factors for $p \equiv 1 \bmod 7$, a product of 3 irreducible quadratics for $p \equiv 6 \bmod 7$, a product of 2 irreducible cubics for $p \equiv 2, 4 \bmod 7$, and is irreducible for $p \equiv 3, 5 \bmod 7$.

**9.** Suppose $A$ is an $n \times n$ matrix over $\mathbb{C}$ for which $A^k = I$ for some integer $k \geq 1$. Show that $A$ can be diagonalized. Show that the matrix $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ where $\alpha$ is an element of a field of characteristic $p$ satisfies $A^p = I$ and cannot be diagonalized if $\alpha \neq 0$.

**10.** Let $\varphi$ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that $\varphi$ gives an isomorphism of $\mathbb{F}_{p^n}$ to itself (such an isomorphism is called an *automorphism*). Prove that $\varphi^n$ is the identity map and that no lower power of $\varphi$ is the identity.

**11.** Let $\varphi$ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$ as in the previous exercise. Determine the rational canonical form over $\mathbb{F}_p$ for $\varphi$ considered as an $\mathbb{F}_p$-linear transformation of the $n$-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

**12.** Let $\varphi$ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$ as in the previous exercise. Determine the Jordan canonical form (over a field containing all the eigenvalues) for $\varphi$ considered as an $\mathbb{F}_p$-linear transformation of the $n$-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

**13.** (*Wedderburn's Theorem on Finite Division Rings*) This exercise outlines a proof (following Witt) of Wedderburn's Theorem that a finite division ring $D$ is a field (i.e., is commutative).

**(a)** Let $Z$ denote the center of $D$ (i.e., the elements of $D$ which commute with every element of $D$). Prove that $Z$ is a field containing $\mathbb{F}_p$ for some prime $p$. If $Z = \mathbb{F}_q$ prove that $D$ has order $q^n$ for some integer $n$ [$D$ is a vector space over $Z$].

**(b)** The nonzero elements $D^\times$ of $D$ form a multiplicative group. For any $x \in D^\times$ show that the elements of $D$ which commute with $x$ form a division ring which contains $Z$. Show that this division ring is of order $q^m$ for some integer $m$ and that $m < n$ if $x$ is not an element of $Z$.

**(c)** Show that the class equation (Theorem 4.7) for the group $D^\times$ is

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_{D^\times}(x_i)|}$$

where $x_1, x_2, \ldots, x_r$ are representatives of the distinct conjugacy classes in $D^\times$ not contained in the center of $D^\times$. Conclude from (b) that for each $i$, $|C_{D^\times}(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

**(d)** Prove that since $\dfrac{q^n-1}{q^{m_i}-1}$ is an integer (namely, the index $|D^\times : C_{D^\times}(x_i)|$ ) then $m_i$ divides $n$ (cf. Exercise 4 of Section 5). Conclude that $\Phi_n(x)$ divides $(x^n-1)/(x^{m_i}-1)$ and hence that the integer $\Phi_n(q)$ divides $(q^n-1)/(q^{m_i}-1)$ for $i = 1, 2, \ldots, r$.

**(e)** Prove that (c) and (d) imply that $\Phi_n(q) = \prod_{\zeta \text{ primitive}}(q-\zeta)$ divides $q-1$. Prove that $|q-\zeta| > q-1$ (complex absolute value) for any root of unity $\zeta \neq 1$ [note that 1 is the closest point on the unit circle in $\mathbb{C}$ to the point $q$ on the real line]. Conclude that $n = 1$, i.e., that $D = Z$ is a field.

The following exercises provide a proof that for any positive integer $m$ there are infinitely many primes $p$ with $p \equiv 1 \pmod{m}$. This is a special case of *Dirichlet's Theorem on Primes in Arithmetic Progressions* which states more generally that there are infinitely many primes $p$ with $p \equiv a \pmod{m}$ for any $a$ relatively prime to $m$.

**14.** Given any monic polynomial $P(x) \in \mathbb{Z}[x]$ of degree at least one show that there are infinitely many distinct prime divisors of the integers

$$P(1), P(2), P(3), \ldots, P(n), \ldots.$$

[Suppose $p_1, p_2, \ldots, p_k$ are the only primes dividing the values $P(n)$, $n = 1, 2, \ldots$. Let $N$ be an integer with $P(N) = a \neq 0$. Show that $Q(x) = a^{-1}P(N + a\,p_1p_2 \ldots p_k\,x)$ is an element of $\mathbb{Z}[x]$ and that $Q(n) \equiv 1 \pmod{p_1p_2 \ldots p_k}$ for $n = 1, 2, \ldots$. Conclude that there is some integer $M$ such that $Q(M)$ has a prime factor different from $p_1, p_2, \ldots, p_k$ and hence that $P(N + ap_1p_2 \cdots p_kM)$ has a prime factor different from $p_1, p_2, \ldots, p_k$.]

**15.** Let $p$ be an odd prime not dividing $m$ and let $\Phi_m(x)$ be the $m^{\text{th}}$ cyclotomic polynomial. Suppose $a \in \mathbb{Z}$ satisfies $\Phi_m(a) \equiv 0 \pmod{p}$. Prove that $a$ is relatively prime to $p$ and that the order of $a$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely $m$. [Since

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \Phi_m(x) \prod_{\substack{d|m \\ d<m}} \Phi_d(x)$$

we see first that $a^m - 1 \equiv 0 \pmod{p}$ i.e., $a^m \equiv 1 \pmod{p}$. If the order of $a$ mod $p$ were less than $m$, then $a^d \equiv 1 \pmod{p}$ for some $d$ dividing $m$, so then $\Phi_d(a) \equiv 0 \pmod{p}$ for some $d < m$. But then $x^m - 1$ would have $a$ as a multiple root mod $p$, a contradiction.]

**16.** Let $a \in \mathbb{Z}$. Show that if $p$ is an odd prime dividing $\Phi_m(a)$ then either $p$ divides $m$ or $p \equiv 1 \pmod{m}$.

**17.** Prove there are infinitely many primes $p$ with $p \equiv 1 \pmod{m}$.

# CHAPTER 14

# Galois Theory

## 14.1 BASIC DEFINITIONS

In the previous chapter we proved the existence of a finite extension of a field $F$ which contains all the roots of a given polynomial $f(x)$ whose coefficients are in $F$. The main idea of Galois Theory (named for Évariste Galois, 1811–1832) is to consider the relation of the group of permutations of the roots of $f(x)$ to the algebraic structure of its splitting field. The connection is given by the Fundamental Theorem of the next section. It can be viewed as another (extremely elegant) application of the important idea in mathematics that one (in our case algebraic) object *acting* on another provides structural information about both.

In this section we introduce the terminology and basic properties of the objects of interest. Let $K$ be a field.

**Definition.**

**(1)** An isomorphism $\sigma$ of $K$ with itself is called an *automorphism* of $K$. The collection of automorphisms of $K$ is denoted $\mathrm{Aut}(K)$. If $\alpha \in K$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.

**(2)** An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to *fix* an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If $F$ is a subset of $K$ (for example, a subfield), then an automorphism $\sigma$ is said to *fix* $F$ if it fixes all the elements of $F$, i.e., $\sigma a = a$ for all $a \in F$.

Note that any field has at least one automorphism, the identity map, denoted by 1 and sometimes called the *trivial* automorphism.

The prime field of $K$ is generated by $1 \in K$ and since any automorphism $\sigma$ takes 1 to 1 (and 0 to 0), i.e., $\sigma(1) = 1$, it follows that $\sigma a = a$ for all $a$ in the prime field. Hence any automorphism of a field $K$ fixes its prime subfield. In particular we see that $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism: $\mathrm{Aut}(\mathbb{Q}) = \{1\}$ and $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$.

**Definition.** Let $K/F$ be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collection of automorphisms of $K$ which fix $F$.

Note that if $F$ is the prime subfield of $K$ then $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$ since every automorphism of $K$ automatically fixes $F$.