7. Let q be a power of a prime p, and let n be a positive integer not divisible by p. We let $\mathbb{F}_q$ be the unique up to isomorphism finite field of q elements. If K is the splitting field of $x^n - 1$ over $\mathbb{F}_q$, show that $K = \mathbb{F}_{q^m}$, where m is the order of q in the group of units $(\mathbb{Z}/n\mathbb{Z})^*$ of the ring $\mathbb{Z}/n\mathbb{Z}$.

8. Let F be a field of characteristic p.

   (a) Let $F^p = \{a^p : a \in F\}$. Show that F^p is a subfield of F.

   (b) If $F = \mathbb{F}_p(x)$ is the rational function field in one variable over $\mathbb{F}_p$, determine F^p and $[F : F^p]$.

9. Show that $x^4 - 7$ is irreducible over $\mathbb{F}_5$.

10. Show that every element of a finite field is a sum of two squares.

11. Let F be a field with $|F| = q$. Determine, with proof, the number of monic irreducible polynomials of prime degree p over F, where p need not be the characteristic of F.

12. Let K and L be extensions of a finite field F of degrees n and m, respectively. Show that KL has degree $\operatorname{lcm}(n, m)$ over F and that $K \cap L$ has degree $\gcd(n, m)$ over F.

13. (a) Show that $x^3 + x^2 + 1$ and $x^3 + x + 1$ are irreducible over $\mathbb{F}_2$.

    (b) Give an explicit isomorphism between $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ and $\mathbb{F}_2[x]/(x^3 + x + 1)$.

14. Let k be the algebraic closure of $\mathbb{Z}_p$, and let $\varphi \in \text{Gal}(k/\mathbb{Z}_p)$ be the Frobenius map $\varphi(a) = a^p$. Show that φ has infinite order, and find a $\sigma \in \text{Gal}(k/\mathbb{Z}_p)$ with $\sigma \notin \langle \varphi \rangle$.

15. Let N be an algebraic closure of a finite field F. Prove that $\text{Gal}(N/F)$ is an Abelian group and that any automorphism in $\text{Gal}(N/F)$ is of infinite order.
    (By techniques of infinite Galois theory, one can prove that $\text{Gal}(N/\mathbb{F}_p)$ is isomorphic to the additive group of the p-adic integers; see Section 17.)

7 Cyclotomic Extensions

An nth root of unity is an element ω of a field with $\omega^n = 1$. For instance, the complex number $e^{2\pi i/n}$ is an nth root of unity. We have seen roots of unity arise in various examples. In this section, we investigate the field extension $F(\omega)/F$, where ω is an nth root of unity. Besides being interesting extensions in their own right, these extensions will play a role in applications of Galois theory to ruler and compass constructions and to the question of solvability of polynomial equations.

Definition 7.1 *If $\omega \in F$ with $\omega^n = 1$, then ω is an nth root of unity. If the order of ω is n in the multiplicative group F^*, then ω is a primitive nth root of unity. If ω is any root of unity, then the field extension $F(\omega)/F$ is called a cyclotomic extension.*

We point out two facts about roots of unity. First, if $\omega \in F$ is a primitive nth root of unity, then we see that $\text{char}(F)$ does not divide n for, if $n = pm$ with $\text{char}(F) = p$, then $0 = \omega^n - 1 = (\omega^m - 1)^p$. Therefore, $\omega^m = 1$, and so the order of ω is not n. Second, if ω is an nth root of unity, then the order of ω in the group F^* divides n, so the order of ω is equal to some divisor m of n. The element ω is then a primitive mth root of unity.

The nth roots of unity in a field K are exactly the set of roots of $x^n - 1$. Suppose that $x^n - 1$ splits over K, and let G be the set of roots of unity in K. Then G is a finite subgroup of K^*, so G is cyclic by Lemma 6.1. Any generator of G is then a primitive nth root of unity.

To describe cyclotomic extensions, we need to use the *Euler phi function*. If n is a positive integer, let $\phi(n)$ be the number of integers between 1 and n that are relatively prime to n. The problems below give the main properties of the Euler phi function. We also need to know about the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$. Recall that if R is a commutative ring with 1, then the set

$$R^* = \{a \in R : \text{there is a } b \in R \text{ with } ab = 1\}$$

is a group under multiplication; it is called the group of units of R. If $R = \mathbb{Z}/n\mathbb{Z}$, then an easy exercise shows that

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a + n\mathbb{Z} : \gcd(a, n) = 1\}.$$

Therefore, $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$.

We now describe cyclotomic extensions of an arbitrary base field.

Proposition 7.2 *Suppose that* $\text{char}(F)$ *does not divide n, and let K be a splitting field of $x^n - 1$ over F. Then K/F is Galois, $K = F(\omega)$ is generated by any primitive nth root of unity ω, and* $\text{Gal}(K/F)$ *is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Thus,* $\text{Gal}(K/F)$ *is Abelian and $[K : F]$ divides $\phi(n)$.*

Proof. Since $\text{char}(F)$ does not divide n, the derivative test shows that $x^n - 1$ is a separable polynomial over F. Therefore, K is both normal and separable over F; hence, K is Galois over F. Let $\omega \in K$ be a primitive nth root of unity. Then all nth roots of unity are powers of ω, so $x^n - 1$ splits over $F(\omega)$. This proves that $K = F(\omega)$. Any automorphism of K that fixes F is determined by what it does to ω. However, any automorphism restricts to a group automorphism of the set of roots of unity, so it maps the set of primitive nth roots of unity to itself. Any primitive nth root of unity in K is of the form ω^t for some t relatively prime to n. Therefore, the map $\theta : \mathrm{Gal}(K/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ given by $\sigma \mapsto t + n\mathbb{Z}$, where $\sigma(\omega) = \omega^t$, is well defined. If $\sigma, \tau \in \mathrm{Gal}(K/F)$ with $\sigma(\omega) = \omega^t$ and $\tau(\omega) = \omega^s$, then $(\sigma\tau)(\omega) = \sigma(\omega^s) = \omega^{st}$, so θ is a group homomorphism. The kernel of θ is the set of all σ with $\sigma(\omega) = \omega$; that is, $\ker(\theta) = \langle \mathrm{id} \rangle$. Thus, θ is injective, so $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of the Abelian group $(\mathbb{Z}/n\mathbb{Z})^*$, a group of order $\phi(n)$. This finishes the proof. □

Example 7.3 The structure of F determines the degree $[F(\omega) : F]$ or, equivalently, the size of $\mathrm{Gal}(F(\omega)/F)$. For instance, let $\omega = e^{2\pi i/8}$ be a primitive eighth root of unity in $\mathbb{C}$. Then $\omega^2 = i$ is a primitive fourth root of unity. The degree of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is 4, which we will show below. If $F = \mathbb{Q}(i)$, then the degree of $F(\omega)$ over F is 2, since ω satisfies the polynomial $x^2 - i$ over F and $\omega \notin F$. If $F = \mathbb{R}$, then $\mathbb{R}(\omega) = \mathbb{C}$, so $[\mathbb{R}(\omega) : \mathbb{R}] = 2$. In fact, if $n \geq 3$ and if τ is any primitive nth root of unity in $\mathbb{C}$, then $\mathbb{R}(\tau) = \mathbb{C}$, so $[\mathbb{R}(\tau) : \mathbb{R}] = 2$.

Example 7.4 Let $F = \mathbb{F}_2$. If ω is a primitive third root of unity over F, then ω is a root of $x^3 - 1 = (x-1)(x^2+x+1)$. Since $\omega \neq 1$ and x^2+x+1 is irreducible over F, we have $[F(\omega) : F] = 2$ and $\min(F, \omega) = x^2 + x + 1$. If ρ is a primitive seventh root of unity, then by factoring $x^7 - 1$, by trial and error or by computer, we get

$$x^7 - 1 = (x-1)\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right).$$

The minimal polynomial of ω is then one of these cubics, so $[F(\omega) : F] = 3$. Of the six primitive seventh roots of unity, three have $x^3 + x + 1$ as their minimal polynomial, and the three others have $x^3 + x^2 + 1$ as theirs. This behavior is different from cyclotomic extensions of $\mathbb{Q}$, as we shall see below, since all the primitive nth roots of unity over $\mathbb{Q}$ have the same minimal polynomial.

We now investigate cyclotomic extensions of $\mathbb{Q}$. Let $\omega_1, \ldots, \omega_r$ be the primitive nth roots of unity in $\mathbb{C}$. Then

$$\{\omega_1, \ldots, \omega_r\} = \left\{e^{2\pi i r/n} : \gcd(r, n) = 1\right\},$$

so there are $\phi(n)$ primitive nth roots of unity in $\mathbb{C}$. In Theorem 7.7, we will determine the minimal polynomial of a primitive nth root of unity over $\mathbb{Q}$, and so we will determine the degree of a cyclotomic extension of $\mathbb{Q}$.

Definition 7.5 *The nth cyclotomic polynomial is $\Psi_n(x) = \prod_{i=1}^{r}(x - \omega_i)$, the monic polynomial in $\mathbb{C}[x]$ whose roots are exactly the primitive nth roots of unity in $\mathbb{C}$.*

For example,

$$\Psi_1(x) = x - 1,$$
$$\Psi_2(x) = x + 1,$$
$$\Psi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Moreover, if p is prime, then all pth roots of unity are primitive except for the root 1. Therefore,

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

From this definition of $\Psi_n(x)$, it is not clear that $\Psi_n(x) \in \mathbb{Q}[x]$, nor that $\Psi_n(x)$ is irreducible over $\mathbb{Q}$. However, we verify the first of these facts in the next lemma and then the second in Theorem 7.7, which shows that $\Psi_n(x)$ is the minimal polynomial of a primitive nth root of unity over $\mathbb{Q}$.

Lemma 7.6 *Let n be any positive integer. Then $x^n - 1 = \prod_{d|n} \Psi_d(x)$. Moreover, $\Psi_n(x) \in \mathbb{Z}[x]$.*

Proof. We know that $x^n - 1 = \prod(x - \omega)$, where ω ranges over the set of all nth roots of unity. If d is the order of ω in $\mathbb{C}^*$, then d divides n, and ω is a primitive dth root of unity. Gathering all the dth root of unity terms together in this factorization proves the first statement. For the second, we use induction on n; the case $n = 1$ is clear since $\Psi_1(x) = x - 1$. Suppose that $\Psi_d(x) \in \mathbb{Z}[x]$ for all $d < n$. Then from the first part, we have

$$x^n - 1 = \left(\prod_{d|n, d<n} \Psi_d(x) \right) \cdot \Psi_n(x).$$

Since $x^n - 1$ and $\prod_{d|n} \Psi_d(x)$ are monic polynomials in $\mathbb{Z}[x]$, the division algorithm, Theorem 3.2 of Appendix A, shows that $\Psi_n(x) \in \mathbb{Z}[x]$. □

We can use this lemma to calculate the cyclotomic polynomials $\Psi_n(x)$ by recursion. For example, to calculate $\Psi_8(x)$, we have

$$x^8 - 1 = \Psi_8(x)\Psi_4(x)\Psi_2(x)\Psi_1(x),$$

so

$$\Psi_8(x) = \frac{x^8 - 1}{(x - 1)(x + 1)(x^2 + 1)} = x^4 + 1.$$

The next theorem is the main fact about cyclotomic polynomials and allows us to determine the degree of a cyclotomic extension over $\mathbb{Q}$.

Theorem 7.7 *Let n be any positive integer. Then $\Psi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. To prove that $\Psi_n(x)$ is irreducible over $\mathbb{Q}$, suppose not. Since $\Psi_n(x) \in \mathbb{Z}[x]$ and is monic, $\Psi_n(x)$ is reducible over $\mathbb{Z}$ by Gauss' lemma. Say $\Psi_n = f(x)h(x)$ with $f(x), h(x) \in \mathbb{Z}[x]$ both monic and f irreducible over $\mathbb{Z}$. Let ω be a root of f. We claim that ω^p is a root of f for all primes p that do not divide n. If this is false for a prime p, then since ω^p is a primitive nth root of unity, ω^p is a root of h. Since $f(x)$ is monic, the division algorithm shows that $f(x)$ divides $h(x^p)$ in $\mathbb{Z}[x]$. The map $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ given by reducing coefficients mod p is a ring homomorphism. For $g \in \mathbb{Z}[x]$, let $\overline{g}$ be the image of $g(x)$ in $\mathbb{F}_p[x]$. Reducing mod p yields $\overline{\Psi_n(x)} = \overline{f} \cdot \overline{h}$. Since $\overline{\Psi_n(x)}$ divides $x^n - \overline{1}$, the derivative test shows that $\overline{\Psi_n(x)}$ has no repeated roots in any extension field of $\mathbb{F}_p$, since p does not divide n. Now, since $a^p = a$ for all $a \in \mathbb{F}_p$, we see that $\overline{h(x^p)} = \overline{h(x)^p}$. Therefore, $\overline{f}$ divides $\overline{h^p}$, so any irreducible factor $\overline{q} \in \mathbb{F}_p[x]$ of $\overline{f}$ also divides $\overline{h}$. Thus, $\overline{q^2}$ divides $\overline{fh} = \overline{\Psi_n(x)}$, which contradicts the fact that $\overline{\Psi_n}$ has no repeated roots. This proves that if ω is a root of f, then ω^p is also a root of f, where p is a prime not dividing n. But this means that all primitive nth roots of unity are roots of f, for if α is a primitive nth root of unity, then $\alpha = \omega^t$ with t relatively prime to n. Then $\alpha = \omega^{p_1 \cdots p_r}$, with each p_i a prime relatively prime to n. We see that ω^{p_1} is a root of f, so then $(\omega^{p_1})^{p_2} = \omega^{p_1 p_2}$ is also a root of f. Continuing this shows α is a root of f. Therefore, every primitive nth root of unity is a root of f, so $\Psi_n(x) = f$. This proves that $\Psi_n(x)$ is irreducible over $\mathbb{Z}$, and so $\Psi_n(x)$ is also irreducible over $\mathbb{Q}$. □

If ω is a primitive nth root of unity in $\mathbb{C}$, then the theorem above shows that $\Psi_n(x)$ is the minimal polynomial of ω over $\mathbb{Q}$. The following corollary describes cyclotomic extensions of $\mathbb{Q}$.

Corollary 7.8 *If K is a splitting field of $x^n - 1$ over $\mathbb{Q}$, then $[K : \mathbb{Q}] = \phi(n)$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Moreover, if ω is a primitive nth root of unity in K, then $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i : \gcd(i, n) = 1\}$, where σ_i is determined by $\sigma_i(\omega) = \omega^i$.*

Proof. The first part of the corollary follows immediately from Proposition 7.2 and Theorem 7.7. The description of $\mathrm{Gal}(K/\mathbb{Q})$ is a consequence of the proof of Proposition 7.2. □

If ω is a primitive nth root of unity in $\mathbb{C}$, then we will refer to the cyclotomic extension $\mathbb{Q}(\omega)$ as $\mathbb{Q}_n$.

Example 7.9 Let $K = \mathbb{Q}_7$, and let ω be a primitive seventh root of unity in $\mathbb{C}$. By Corollary 7.8, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^*$, which is a cyclic group of order 6. The Galois group of $K/\mathbb{Q}$ is $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, where $\sigma_i(\omega) = \omega^i$. Thus, $\sigma_1 = \mathrm{id}$, and it is easy to check that σ_3 generates this group. Moreover, $\sigma_i \circ \sigma_j = \sigma_{ij}$, where the subscripts are multiplied modulo 7. The subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ are then

$$\langle \mathrm{id} \rangle\,,\ \langle \sigma_3^3 \rangle\,,\ \langle \sigma_3^2 \rangle\,,\ \langle \sigma_3 \rangle\,,$$

whose orders are 1, 2, 3, and 6, respectively. Let us find the corresponding intermediate fields. If $L = \mathcal{F}(\sigma_3^3) = \mathcal{F}(\sigma_6)$, then $[K : L] = |\langle \sigma_6 \rangle| = 2$ by the fundamental theorem. To find L, we note that ω must satisfy a quadratic over L and that this quadratic is

$$(x - \omega)(x - \sigma_6(\omega)) = (x - \omega)(x - \omega^6).$$

Expanding, this polynomial is

$$x^2 - (\omega + \omega^6)x + \omega\omega^6 = x^2 - (\omega + \omega^6)x + 1.$$

Therefore, $\omega + \omega^6 \in L$. If we let $\omega = \exp(2\pi i/7) = \cos(2\pi/7) + i\sin(2\pi/7)$, then $\omega + \omega^6 = 2\cos(2\pi/7)$. Therefore, ω satisfies a quadratic over $\mathbb{Q}(\cos(2\pi/7))$; hence, L has degree at most 2 over this field. This forces $L = \mathbb{Q}(\cos(2\pi/7))$. With similar calculations, we can find $M = \mathcal{F}(\sigma_3^2) = \mathcal{F}(\sigma_2)$. The order of σ_2 is 3, so $[M : \mathbb{Q}] = 2$. Hence, it suffices to find one element of M that is not in $\mathbb{Q}$ in order to generate M. Let

$$\alpha = \omega + \sigma_2(\omega) + \sigma_2^2(\omega) = \omega + \omega^2 + \omega^4.$$

This element is in M because it is fixed by σ. But, we show that α is not in $\mathbb{Q}$ since it is not fixed by σ_6. To see this, we have

$$\begin{aligned} \sigma_6(\omega) &= \omega^6 + \omega^{12} + \omega^{24} \\ &= \omega^6 + \omega^5 + \omega^3. \end{aligned}$$

If $\sigma_6(\alpha) = \alpha$, this equation would give a degree 6 polynomial for which ω is a root, and this polynomial is not divisible by

$$\min(\mathbb{Q}, \omega) = \Psi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

a contradiction. This forces $\alpha \notin \mathbb{Q}$, so $M = \mathbb{Q}(\alpha)$. Therefore, the intermediate fields of $K/\mathbb{Q}$ are

$$K,\ \mathbb{Q}(\cos(2\pi/7)),\ \mathbb{Q}(\omega + \omega^2 + \omega^4),\ \mathbb{Q}.$$

Example 7.10 Let $K = \mathbb{Q}_8$, and let $\omega = \exp(2\pi i/8) = (1 + i)/\sqrt{2}$. The Galois group of $K/\mathbb{Q}$ is $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, and note that each of the three nonidentity automorphisms of K have order 2. The subgroups of this Galois group are then

$$\langle \mathrm{id} \rangle\,,\ \langle \sigma_3 \rangle\,,\ \langle \sigma_5 \rangle\,,\ \langle \sigma_7 \rangle\,,\ \mathrm{Gal}(K/\mathbb{Q}).$$

Each of the three proper intermediate fields has degree 2 over $\mathbb{Q}$. One is easy to find, since $\omega^2 = i$ is a primitive fourth root of unity. The group associated to $\mathbb{Q}(i)$ is $\langle\sigma_5\rangle$, since $\sigma_5(\omega^2) = \omega^{10} = \omega^2$. We could find the two other fields in the same manner as in the previous example: Show that the fixed field of σ_3 is generated over $\mathbb{Q}$ by $\omega + \sigma_3(\omega)$. However, we can get this more easily due to the special form of ω. Since $\omega = (1+i)/\sqrt{2}$ and $\omega^{-1} = (1-i)/\sqrt{2}$, we see that $\sqrt{2} = \omega + \omega^{-1} \in K$. The element $\omega + \omega^{-1} = \omega + \omega^7$ is fixed by σ_7; hence, the fixed field of σ_7 is $\mathbb{Q}(\sqrt{2})$. We know $i \in K$ and $\sqrt{2} \in K$, so $\sqrt{-2} \in K$. This element must generate the fixed field of σ_3. The intermediate fields are then

$$K,\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}.$$

The description of the intermediate fields also shows that $K = \mathbb{Q}(\sqrt{2}, i)$.

Problems

1. Determine all of the subfields of $\mathbb{Q}_{12}$.
2. Show that $\cos(\pi/9)$ is algebraic over $\mathbb{Q}$, and find $[\mathbb{Q}(\cos(\pi/9)) : \mathbb{Q}]$.
3. Show that $\cos(2\pi/n)$ and $\sin(2\pi/n)$ are algebraic over $\mathbb{Q}$ for any $n \in \mathbb{N}$.
4. Prove that $\mathbb{Q}(\cos(2\pi/n))$ is Galois over $\mathbb{Q}$ for any n. Is the same true for $\mathbb{Q}(\sin(2\pi/n))$?
5. If p is a prime, prove that $\phi(p^n) = p^{n-1}(p-1)$.
6. Let $\theta : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ be the map that sends $\sum_i a_i x^i$ to $\sum_i \overline{a_i} x^i$, where $\overline{a}$ is the equivalence class of a modulo p. Show that θ is a ring homomorphism.
7. If $\gcd(n, m) = 1$, show that $\phi(nm) = \phi(n)\phi(m)$.
8. If the prime factorization of n is $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, show that $\phi(n) = \Pi_i p_i^{\alpha_i - 1}(p_i - 1)$.
9. Let n, m be positive integers with $d = \gcd(n, m)$ and $l = \operatorname{lcm}(n, m)$. Prove that $\phi(n)\phi(m) = \phi(d)\phi(l)$.
10. Show that $(\mathbb{Z}/n\mathbb{Z})^* = \{a + n\mathbb{Z} : \gcd(a, n) = 1\}$.
11. If n is odd, prove that $\mathbb{Q}_{2n} = \mathbb{Q}_n$.
12. Let n, m be positive integers with $d = \gcd(n, m)$ and $l = \operatorname{lcm}(n, m)$.
    (a) If n divides m, prove that $\mathbb{Q}_n \subseteq \mathbb{Q}_m$.
    (b) Prove that $\mathbb{Q}_n \mathbb{Q}_m = \mathbb{Q}_l$.
    (c) Prove that $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_d$.