GALOIS THEORY

DAVID A. COX
Amherst College
Department of Mathematics & Computer Science
Amherst, MA

A JOHN WILEY & SONS, INC., PUBLICATION

9

Cyclotomic Extensions

In this chapter we will explore the Galois theory of *cyclotomic extensions*, which are extensions of the form $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$. This will involve a study of cyclotomic polynomials and Gauss's theory of periods. In the next chapter we will apply these results to determine which regular polygons are constructible by straightedge and compass.

9.1 CYCLOTOMIC POLYNOMIALS

In Section 4.2 we showed that if p is prime, then

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

is the minimal polynomial of $\zeta_p = e^{2\pi i/p}$ over $\mathbb{Q}$. In this section, we will describe the minimal polynomial of

$$\zeta_n = e^{2\pi i/n}$$

over $\mathbb{Q}$, where n is now an arbitrary integer ≥ 1. We will also compute the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. But first, we need two facts from elementary number theory.

A. Some Number Theory. We begin with the Euler ϕ-function. Given a positive integer n, we define $\phi(n)$ to be the number of integers i such that $0 \leq i < n$ and $\gcd(i, n) = 1$. We can interpret $\phi(n)$ in terms of the ring $\mathbb{Z}/n\mathbb{Z}$ as follows. The invertible elements of this ring form the set

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[i] \in \mathbb{Z}/n\mathbb{Z} \mid [i][j] = [1] \text{ for some } [j] \in \mathbb{Z}/n\mathbb{Z}\}.$$

One easily sees that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group under multiplication. In Exercise 1 you will show that $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\phi(n)$. Thus

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|. \tag{9.1}$$

Our first lemma gives the basic properties of the ϕ-function.

Lemma 9.1.1. *Let ϕ be defined as above.*
(a) *If n and m are relatively prime positive integers, then $\phi(nm) = \phi(n)\phi(m)$.*
(b) *If $n > 1$ is an integer, then*

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right),$$

where the product is over all primes p dividing n.

Proof. Since $\gcd(n, m) = 1$, Lemma A.5.2 implies that there is a ring isomorphism $\alpha : \mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In Exercise 2 you will show that α induces a group isomorphism

$$(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

Then $\phi(nm) = \phi(n)\phi(m)$ follows immediately from (9.1).

Next observe that if p is prime and $a \geq 1$, then $\phi(p^a)$ counts the number of integers i such that $0 \leq i < p^a$ and $p \nmid i$. In other words, if

$$S = \{j \in \mathbb{Z} \mid 0 \leq j < p^a \text{ and } p|j\},$$

then $\phi(p^a) = p^a - |S|$. However, $p|j$ for some $0 \leq j < p^a$ if and only if $j = p\ell$ for some $0 \leq \ell < p^{a-1}$. Thus $|S| = p^{a-1}$, so that $\phi(p^a) = p^a - p^{a-1}$.

For arbitrary $n > 1$, write $n = p_1^{a_1} \cdots p_s^{a_s}$, where the p_i are distinct primes and $a_i \geq 1$ for all i. Using part (a) and the formula $\phi(p^a) = p^a - p^{a-1}$, we obtain

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1} \cdots p_s^{a_s}) = \phi(p_1^{a_1}) \cdots \phi(p_s^{a_s}) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_s^{r_s} - p_s^{r_s-1}) \\ &= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdots p_s^{a_s}\left(1 - \frac{1}{p_s}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right).\end{aligned}$$

This completes the proof. □

Our second lemma is sometimes called *Fermat's Little Theorem.*

Lemma 9.1.2. *If p is prime, then $a^p \equiv a \bmod p$ for all integers a.*

Proof. Since the congruence is true when $p|a$, we may assume that $p \nmid a$. Then $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$, so that $[a]^{p-1} = [1]$, since $(\mathbb{Z}/p\mathbb{Z})^*$ is a group of order $p - 1$ under multiplication. In congruence notation, this means that $a^{p-1} \equiv 1 \bmod p$. The desired congruence follows by multiplying each side by a. □

B. Definition of Cyclotomic Polynomials. Our next task is to define the cyclotomic polynomial $\Phi_n(x)$ for $n \geq 1$ and show that it has integer coefficients. We begin with the factorization

$$x^n - 1 = \prod_{0 \leq i < n} (x - \zeta_n^i). \tag{9.2}$$

Then define the *nth cyclotomic polynomial* $\Phi_n(x)$ to be the product

$$\Phi_n(x) = \prod_{\substack{0 \leq i < n \\ \gcd(i,n)=1}} (x - \zeta_n^i). \tag{9.3}$$

Thus the roots of $\Phi_n(x)$ are ζ_n^i for those $0 \leq i < n$ relatively prime to n. It follows that $\Phi_n(x)$ has degree $\phi(n)$. Combining this with (9.1), we see that

$$\phi(n) = \deg\big(\Phi_n(x)\big) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

This link between $\Phi_n(x)$ and $(\mathbb{Z}/n\mathbb{Z})^*$ will be used to determine $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

In Section 8.3 we defined a root of $x^n - 1$ to be a *primitive nth root of unity* if its powers give all roots of $x^n - 1$. In Exercise 3 you will prove that in our situation, the primitive nth roots of unity are ζ_n^i for $0 \leq i < n$ and $\gcd(i, n) = 1$. Thus the roots of $\Phi_n(x)$ are the primitive nth roots of unity in $\mathbb{C}$.

Here are some examples of cyclotomic polynomials.

Example 9.1.3. When $n = 2$, the only primitive square root of unity is -1, so that $\Phi_2(x) = x + 1$. When $n = 4$, the primitive fourth roots of unity are i and $i^3 = -i$, so that

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Since $\Phi_1(x) = x - 1$, we get the factorization

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = \Phi_1(x)\Phi_2(x)\Phi_4(x).$$

Proposition 9.1.5 will show that $x^n - 1$ has a similar factorization. ◁▷

Example 9.1.4. Let p be prime. Since $1, \ldots, p - 1$ are relatively prime to p, it follows that

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

Using $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, we obtain $\Phi_p(x) = x^{p-1} + \cdots + x + 1$, which agrees with the definition of $\Phi_p(x)$ given in Section 4.2. ◁▷

In the following discussion we will write $d|n$ to indicate that d is a positive divisor of n. We now state some elementary properties of cyclotomic polynomials.

Proposition 9.1.5. *$\Phi_n(x)$ is a monic polynomial with integer coefficients and has degree $\phi(n)$. Furthermore, these polynomials satisfy the identity*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{9.4}$$

Proof. $\Phi_n(x)$ is monic by definition and has degree $\phi(n)$ as shown above. Next we prove the factorization (9.4). The basic idea is that every number i in the range $0 \le i < n$ gives a divisor $d = \gcd(i, n)$ of n. Since different values of i can give the same d, we can organize the factorization (9.2) according to d. This gives

$$x^n - 1 = \prod_{d|n} \prod_{\substack{0 \le i < n \\ \gcd(i,n)=d}} (x - \zeta_n^i).$$

For a fixed positive divisor d of n, the corresponding part of this factorization is

$$\prod_{\substack{0 \le i < n \\ \gcd(i,n)=d}} (x - \zeta_n^i). \tag{9.5}$$

But $\gcd(i, n) = d$ implies that $i = dj$ and $n = d\frac{n}{d}$, where $\gcd(j, \frac{n}{d}) = 1$. Also:

- $0 \le i < n$ becomes $0 \le dj < d\frac{n}{d}$, which is equivalent to $0 \le j < \frac{n}{d}$.
- $\zeta_n^d = \zeta_{\frac{n}{d}}$, so that $x - \zeta_n^i = x - \zeta_n^{dj} = x - (\zeta_{\frac{n}{d}})^j$.

It follows that (9.5) can be written

$$\prod_{\substack{0 \le j < \frac{n}{d} \\ \gcd(j, \frac{n}{d})=1}} \left(x - (\zeta_{\frac{n}{d}})^j\right),$$

which by (9.3) is the cyclotomic polynomial $\Phi_{\frac{n}{d}}(x)$. Thus the above factorization of $x^n - 1$ becomes

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

Then (9.4) follows since d is a positive divisor of n if and only if $\frac{n}{d}$ is.

It remains to show that $\Phi_n(x)$ has integer coefficients. We prove this by complete induction on n. The base case $n = 1$ is trivial, since $\Phi_1(x) = x - 1$. Furthermore, if $n > 1$, then (9.4) and our inductive hypothesis imply that

$$\begin{aligned} x^n - 1 &= \Phi_n(x) \cdot \prod_{d|n, d<n} \Phi_d(x) \\ &= \Phi_n(x) \cdot \text{a monic polynomial } g(x) \text{ with integer coefficients.} \end{aligned}$$

Hence $\Phi_n(x)$ is the quotient of $x^n - 1$ by $g(x)$. Since $x^n - 1$ and $g(x)$ lie in $\mathbb{Z}[x]$ and $g(x)$ is monic, the refinement of the division algorithm presented in Exercise 4 implies that $\Phi_n(x) \in \mathbb{Z}[x]$. This completes the proof. □

Here are some examples of how to use the identity (9.4).

Example 9.1.6. Let p be prime. Proposition 9.1.5 implies that

$$x^p - 1 = \Phi_1(x)\Phi_p(x) \quad \text{and} \quad x^{p^2} - 1 = \Phi_1(x)\Phi_p(x)\Phi_{p^2}(x).$$

Thus

$$x^{p^2} - 1 = (x^p - 1)\Phi_{p^2}(x).$$

It follows that

$$\Phi_{p^2}(x) = \frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^{2p} + x^p + 1,$$

where the second equality follows from

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

by replacing x with x^p. ◁▷

Example 9.1.7. In the examples of cyclotomic polynomials given so far, the coefficients are always 0 or ± 1. This is true for all $n < 105$. You will show in Exercise 5 that $\Phi_{105}(x)$ is the polynomial

$$\begin{aligned} 1 &+ x + x^2 - x^5 - x^6 - 2x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} \\ &+ x^{16} + x^{17} - x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} \\ &+ x^{35} + x^{36} - x^{39} - x^{40} - 2x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}. \end{aligned}$$

As n increases, the coefficients of $\Phi_n(x)$ can get arbitrarily large (see [1]). ◁▷

C. The Galois Group of a Cyclotomic Extension. The first step in computing $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is to prove that $\Phi_n(x)$ is irreducible. For this, we will need the following application of symmetric polynomials and Lemma 9.1.2.

Lemma 9.1.8. *Let $f \in \mathbb{Z}[x]$ be monic of positive degree, and let p be prime. If f_p is the monic polynomial whose roots are the pth powers of the roots of f, then:*

(a) $f_p \in \mathbb{Z}[x]$.

(b) *The coefficients of f and f_p are congruent modulo p.*

Proof. If f has roots $\gamma_1, \ldots, \gamma_r$, $r = \deg(f)$, then

$$f_p(x) = \prod_{i=1}^{r}(x - \gamma_i^p) = x^r - \sigma_1(\gamma_1^p, \ldots, \gamma_r^p)x^{r-1} + \cdots + (-1)^r\sigma_r(\gamma_1^p, \ldots, \gamma_r^p).$$

Similarly, $f(x) = x^r - \sigma_1(\gamma_1, \ldots, \gamma_r)x^{r-1} + \cdots + (-1)^r\sigma_r(\gamma_1, \ldots, \gamma_r)$. In these formulas, $\sigma_1, \ldots, \sigma_r$ are the elementary symmetric polynomials from Chapter 2.

Observe that $\sigma_i(x_1^p, \ldots, x_r^p)$ is a symmetric polynomial. In Exercise 6 you will show that the algorithm of Theorem 2.2.2 implies that

$$\sigma_i(x_1^p, \ldots, x_r^p) = \sigma_i^p + S(\sigma_1, \ldots, \sigma_r), \tag{9.6}$$

where $S(\sigma_1, \ldots, \sigma_r)$ is a polynomial in $\sigma_1, \ldots, \sigma_r$ with integer coefficients. However, if we reduce modulo p, then Lemma 5.3.10 implies that

$$\sigma_i^p = \sigma_i(x_1, \ldots, x_r)^p = \sigma_i(x_1^p, \ldots, x_r^p)$$

as polynomials with coefficients in $\mathbb{F}_p$ (see Exercise 6 for details). Combining this with (9.6), we see that the coefficients of $S(\sigma_1, \ldots, \sigma_r)$ are all divisible by p.

Now substitute $\gamma_1, \ldots, \gamma_r$ for $x_1, \ldots, x_r$ in (9.6). Since $\sigma_i(\gamma_1, \ldots, \gamma_r) \in \mathbb{Z}$ for all i and S has integer coefficients, we conclude that $\sigma_i(\gamma_1^p, \ldots, \gamma_r^p) \in \mathbb{Z}$. Since the coefficients of S are all divisible by p, we also have

$$\sigma_i(\gamma_1^p, \ldots, \gamma_r^p) \equiv \sigma_i(\gamma_1, \ldots, \gamma_r)^p \equiv \sigma_i(\gamma_1, \ldots, \gamma_r) \bmod p,$$

where the second congruence follows from Lemma 9.1.2. Thus the coefficients of f and f_p are congruent modulo p. □

We now show that $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$.

Theorem 9.1.9. *The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let $f \in \mathbb{Q}[x]$ be an irreducible factor of $\Phi_n(x)$. Then Gauss's Lemma, in the form of Corollary 4.2.1, allows us to assume that $f \in \mathbb{Z}[x]$ and that

$$\Phi_n(x) = f(x)g(x), \tag{9.7}$$

for some $g \in \mathbb{Z}[x]$. We can also assume that f and g are monic, since $\Phi_n(x)$ is.

Let p be a prime not dividing n. The first step in the proof is to show that

$$\text{If } \zeta \text{ is a root of } f, \text{ then so is } \zeta^p. \tag{9.8}$$

We will prove (9.8) by contradiction, so suppose that $f(\zeta) = 0$ and $f(\zeta^p) \neq 0$.

As in Lemma 9.1.8, let $f_p \in \mathbb{Z}[x]$ be the monic polynomial whose roots are the pth powers of the roots of f. In Exercise 7 you will show that the roots of f_p are distinct primitive nth roots of unity, which implies that f_p divides $\Phi_n(x)$. If f and f_p had a common root, then f would divide f_p, since f is irreducible. This would force $f = f_p$, since they are monic of the same degree. But $f = f_p$ is impossible, since $f(\zeta^p) \neq 0$ and $f_p(\zeta^p) = 0$ (the latter follows from $f(\zeta) = 0$ by the definition of f_p). Thus they have no common roots, so that (9.7) can be written

$$\Phi_n(x) = f(x)f_p(x)h(x).$$

Since $\Phi_n(x)$, $f(x)$, and $f_p(x)$ are monic with integer coefficients, the refined division algorithm of Exercise 4 implies that the same is true for $h(x)$.

Consider the map sending $q(x) \in \mathbb{Z}[x]$ to the polynomial $\overline{q}(x) \in \mathbb{F}_p[x]$ obtained by reducing the coefficients of $q(x)$ modulo p. Since $\overline{f}(x) = \overline{f}_p(x)$ by Lemma 9.1.8, the above factorization implies that $\overline{f}^2(x)$ divides $\overline{\Phi}_n(x)$ in $\mathbb{F}_p[x]$. Thus $\overline{f}^2(x)$ divides $x^n - 1$, so that $x^n - 1$ is not separable in $\mathbb{F}_p[x]$. But $x^n - 1$ is separable, since $p \nmid n$. This contradiction completes the proof of (9.8).

Now let ζ be a fixed root of f and let ζ' be any primitive nth root of unity. In Exercise 7 you will show that $\zeta' = \zeta^j$ for some j relatively prime to n. Let $j = p_1 \cdots p_r$ be the prime factorization of j, and note that each p_i is relatively prime to n. Then successive application of (9.8) shows that

$$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \zeta^{p_1 p_2 p_3}, \ldots, \zeta^{p_1 \cdots p_r} = \zeta'$$

are roots of f. Hence every primitive nth root of unity is a root of f. Since f divides $\Phi_n(x)$, we conclude that $f = \Phi_n(x)$. Thus $\Phi_n(x)$ is irreducible, since f is. □

Theorem 9.1.9 implies that $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$. Thus $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg\big(\Phi_n(x)\big) = \phi(n)$, which proves the following corollary.

Corollary 9.1.10. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. □

This makes it easy to compute the Galois group of a cyclotomic extension.

Theorem 9.1.11. *There is an isomorphism* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ *such that* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *maps to* $[\ell] \in (\mathbb{Z}/n\mathbb{Z})^*$ *if and only if* $\sigma(\zeta_n) = \zeta_n^\ell$.

Proof. We know from (8.6) that $\mathbb{Q} \subset \mathbb{Q}(\zeta n)$ is a Galois extension. Furthermore, an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is uniquely determined by $\sigma(\zeta_n)$, which is a root of $\Phi_n(x)$ because ζ_n is. Thus $\sigma(\zeta_n) = \zeta_n^\ell$ for some ℓ relatively prime to n. By Exercise 4 of Section 6.2, the map $\sigma \mapsto [\ell]$ is a well-defined one-to-one group homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$. Then Corollary 9.1.10 implies that

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

It follows that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ is an isomorphism. □

In the next chapter we will use Corollary 9.1.10 to characterize those n for which a regular polygon with n sides is constructible by straightedge and compass.

Historical Notes

While both Lagrange and Vandermonde made significant use of roots of unity, the first systematic study of cyclotomic extensions is due to Gauss. Most of Gauss's results appear in Section VII of *Disquisitiones Arithmeticae* [4], published in 1801. This amazing book covers a wide range of topics in number theory. In particular, Gauss introduces the congruence notation $a \equiv b \bmod n$ and proves a version of Gauss's Lemma (Theorem A.3.2).

In Section VII Gauss studies the extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, where p is prime. As we will see in the next section, Gauss constructs primitive elements for intermediate

fields and essentially describes the Galois correspondence. In Article 365 of [4] he applies his results to the constructibility of regular polygons by straightedge and compass. We will discuss this in the next chapter.

To study $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, Gauss needed to know that $\Phi_p(x) = x^{p-1} + \cdots + 1$ is irreducible over $\mathbb{Q}$. Not surprisingly, he proves this using Gauss's Lemma. For general $n \geq 1$, the entry dated June 12, 1808 of Gauss's mathematical diary (see [5]) reads as follows:

> The equation ... that contains all primitive roots of the equation $x^n - 1 = 0$ cannot be decomposed into factors with rational coefficients, proved for composite values of n.

Unfortunately, Gauss's proof has been lost. The first published proof that $\Phi_n(x)$ is irreducible (Theorem 9.1.9) appeared in 1854 and is due to Kronecker. Our proof is based on arguments of Dedekind, as presented by Jordan in 1870. The key step is (9.8), which we proved using Lemma 9.1.8. Schönemann's proof of this lemma dates from 1846, though Gauss proved it much earlier in an unpublished continuation of [4]. A modern proof of (9.8) is sketched in Exercise 8.

Exercises for Section 9.1

Exercise 1. Prove that a congruence class $[i] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(i, n) = 1$. Conclude that $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\phi(n)$. Be sure that you understand what happens when $n = 1$.

Exercise 2. Assume that $\gcd(n, m) = 1$. By Lemma A.5.2, we have a ring isomorphism $\alpha : \mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ that sends $[a]_{nm}$ to $([a]_n, [a]_m)$. Prove that α induces a group isomorphism $(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.

Exercise 3. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Prove that ζ_n^i for $0 \leq i < n$ and $\gcd(i, n) = 1$ are the primitive nth roots of unity in $\mathbb{C}$.

Exercise 4. Let R be an integral domain, and let $f, g \in R[x]$, where $f \neq 0$. If K is the field of fractions of R, then we can divide g by f in $K[x]$ using the division algorithm of Theorem A.1.14. This gives $g = qf + r$, though $q, r \in K[x]$ need not lie in $R[x]$.

(a) Show that dividing x^2 by $2x + 1$ in $\mathbb{Q}[x]$ gives $x^2 = q \cdot (2x + 1) + r$, where $q, r \in \mathbb{Q}[x]$ are not in $\mathbb{Z}[x]$, even though x^2 and $2x + 1$ lie in $\mathbb{Z}[x]$.

(b) Show that if f is monic, then the division algorithm gives $g = qf + r$, where $q, r \in R[x]$.

Hence the division algorithm works over R provided we divide by *monic* polynomials.

Exercise 5. Verify the formula for $\Phi_{105}(x)$ given in Example 9.1.7.

Exercise 6. This exercise is concerned with the proof of Lemma 9.1.8.

(a) Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be symmetric. Prove that f is a polynomial in $\sigma_1, \ldots, \sigma_n$ with integer coefficients.

(b) Let p be prime and let $h \in \mathbb{F}_p[x_1, \ldots, x_n]$. Prove that $h(x_1, \ldots, x_n)^p = h(x_1^p, \ldots, x_n^p)$.

Exercise 7. This exercise is concerned with the proof of Theorem 9.1.9.

(a) Let ζ be a primitive nth root of unity, and let i be relatively prime to n. Prove that ζ^i is a primitive nth root of unity and that every primitive nth root of unity is of this form.

(b) Let $\gamma_1, \ldots, \gamma_r$ be distinct primitive nth roots of unity and let i be relatively prime to n. Prove that $\gamma_1^i, \ldots, \gamma_r^i$ are distinct.

Exercise 8. This exercise will present an alternate proof of (9.8) that doesn't use symmetric polynomials. Assume that ζ is root of f such that $f(\zeta^p) \neq 0$. As in the text, $q(x) \in \mathbb{Z}[x]$ maps to the polynomial $\overline{q}(x) \in \mathbb{F}_p[x]$. Let $g(x)$ be as in (9.7).

(a) Prove that ζ is a root of $g(x^p)$, and conclude that $f(x)|g(x^p)$.

(b) Use Gauss's Lemma to explain why $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$, and conclude that $\overline{f}(x)$ divides $\overline{g}(x^p)$ in $\mathbb{F}_p[x]$.

(c) Use Exercise 7 to prove that $\overline{g}(x)^p = \overline{g}(x^p)$, and conclude that $\overline{f}(x)$ divides $\overline{g}(x)^p$.

(d) Now let $h(x) \in \mathbb{F}_p[x]$ be an irreducible factor of $\overline{f}(x)$. Show that $h(x)$ divides $\overline{g}(x)$, so that $h(x)^2$ divides $\overline{f}(x)\overline{g}(x)$.

(e) Conclude that $h(x)^2$ divides $x^n - 1 \in \mathbb{F}_p[x]$.

(f) Use separability to obtain a contradiction.

Exercise 9. In proving Fermat's Little Theorem $a^p \equiv a \bmod p$, recall from the proof of Lemma 9.1.2 that we first proved $a^{p-1} \equiv 1 \bmod p$ when a is relatively prime to p. For general $n > 1$, Euler showed that $a^{\phi(n)} \equiv 1 \bmod n$ when a is relatively prime to n. Prove this. What basic fact from group theory do you use?

Exercise 10. Prove that a cyclic group of order n has $\phi(n)$ generators.

Exercise 11. Prove that $n = \sum_{d|n} \phi(d)$.

Exercise 12. Here are some further properties of cyclotomic polynomials.

(a) Given n, let $m = \prod_{p|n} p$. Prove that $\Phi_n(x) = \Phi_m(x^{n/m})$. This shows that we can reduce computing $\Phi_n(x)$ to the case when n is squarefree.

(b) Let n be an odd integer. Prove that $\Phi_{2n}(x) = \Phi_n(-x)$.

(c) Let p be a prime not dividing an integer $n > 1$. Prove that $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

Exercise 13. We know $\Phi_p(x)$ when p is prime. Use this and Exercise 12 to compute $\Phi_{15}(x)$ and $\Phi_{105}(x)$.

Exercise 14. The Möbius function is defined for integers $n \geq 1$ by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^s, & \text{if } n = p_1 \cdots p_s \text{ for distinct primes } p_1, \ldots, p_s, \\ 0, & \text{otherwise.} \end{cases}$$

Prove that $\sum_{d|n} \mu\left(\frac{n}{d}\right) = 0$ when $n > 1$.

Exercise 15. Let μ be the Möbius function defined in Exercise 14. Prove that

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

This representation of $\Phi_n(x)$ is useful when studying the size of its coefficients.

Exercise 16. Let n and m be relatively prime positive integers.

(a) Prove that $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$.

(b) Prove that $\Phi_n(x)$ is irreducible over $\mathbb{Q}(\zeta_m)$.

9.2 GAUSS AND ROOTS OF UNITY (OPTIONAL)

In this section we will explore how Gauss studied $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, where p is an odd prime. Working 30 years before Galois, Gauss described the intermediate fields of this extension and used his results to show that $x^p - 1 = 0$ is solvable by radicals.

A. The Galois Correspondence. If p is an odd prime, then Proposition 9.1.11 implies that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*.$$

Let's recall what we know about this group:

- $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$ by Proposition A.5.3.
- For every positive divisor f of $p-1$, $(\mathbb{Z}/p\mathbb{Z})^*$ has a unique subgroup H_f of order f by Theorem A.1.4.

Following Gauss, we let $e = \frac{p-1}{f}$. Thus

$$ef = p - 1,$$

and H_f has index e in $(\mathbb{Z}/p\mathbb{Z})^*$. We will use this notation throughout the section. One further fact not mentioned earlier is the following:

- If f and f' are positive divisors of $p-1$, then $H_f \subset H_{f'}$ if and only if $f \mid f'$.

You will prove this in Exercise 1. Hence we can easily check when one subgroup is contained in another.

By the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ and the Galois correspondence, the intermediate fields of $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ are the fixed fields

$$L_f = \left\{\alpha \in \mathbb{Q}(\zeta_p) \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \text{ with } \sigma(\zeta_p) = \zeta_p^i,\ [i] \in H_f\right\}$$

as f ranges over all positive divisors of $p-1$. These fixed fields have the following nice properties.

Proposition 9.2.1. *The intermediate fields $\mathbb{Q} \subset L_f \subset \mathbb{Q}(\zeta_p)$ satisfy:*

(a) *L_f is a Galois extension of $\mathbb{Q}$ of degree e.*

(b) *If f and f' are positive divisors of $p-1$, then $L_f \supset L_{f'}$ if and only if $f \mid f'$.*

(c) *If f and f' are positive divisors of $p-1$ such that $f \mid f'$, then $\mathrm{Gal}(L_f/L_{f'})$ is cyclic of order f'/f.*

Proof. You will supply the straightforward proof in Exercise 2. □

In particular, if $p - 1 = q_1 q_2 \cdots q_r$ is the prime factorization of $p-1$, then we get subfields

$$\mathbb{Q} = L_{q_1 \cdots q_r} \subset L_{q_2 \cdots q_r} \subset \cdots \subset L_{q_{r-1} q_r} \subset L_{q_r} \subset L_1 = \mathbb{Q}(\zeta_p) \tag{9.9}$$

where $[L_{q_{i+1} \cdots q_r} : L_{q_i q_{i+1} \cdots q_r}] = q_i$. Thus every element of $L_{q_{i+1} \cdots q_r}$ is the root of a polynomial of degree q_i over $L_{q_i q_{i+1} \cdots q_r}$.

All of this is a simple application of Galois theory. The surprise is that Gauss understood most of this, including (9.9). Before discussing Gauss's results, let's do an example.

Example 9.2.2. Let $p = 7$. Then (9.9) with $p - 1 = 6 = 3 \cdot 2$ becomes

$$\mathbb{Q} = L_6 \subset L_2 \subset L_1 = \mathbb{Q}(\zeta_7),$$

where L_2 is the fixed field of the unique subgroup of order 2 of $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$.

To make this more explicit, consider $\eta_1 = \zeta_7 + \zeta_7^{-1} = \zeta_7 + \overline{\zeta}_7 = 2\cos(2\pi/7)$. In Exercise 3 you will show that $\mathbb{Q}(\eta_1)$ corresponds to the subgroup $\{e, \tau\}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, where τ is complex conjugation. This subgroup has order 2, which implies that

$$L_2 = \mathbb{Q}(\eta_1).$$

In Exercise 3 you will also show that the conjugates of η_1 over $\mathbb{Q}$ are

$$\eta_2 = \zeta_7^2 + \zeta_7^{-2} = 2\cos(4\pi/7) \quad \text{and} \quad \eta_3 = \zeta_7^3 + \zeta_7^{-3} = 2\cos(6\pi/7),$$

and that η_1, η_2, η_3 are roots of the cubic equation

$$y^3 + y^2 - 2y - 1 = 0.$$

It is easy to check that ζ_7 is a root of $x^2 - \eta_1 x + 1 \in L_2[x]$. From here we can express ζ_7 in terms of radicals as follows. Applying Cardan's formulas to the above cubic, one sees that

$$\eta_1 = -\frac{1}{3} + \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} + \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})}, \tag{9.10}$$

provided that the cube roots are chosen correctly (see Exercise 3). Then applying the quadratic formula to $x^2 - \eta_1 x + 1 = 0$ gives

$$\begin{aligned}\zeta_7 = {} & -\frac{1}{6} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})} \\ & + \frac{i}{2}\sqrt{1 - \left(\frac{1}{3} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})}\right)^2},\end{aligned} \tag{9.11}$$

where we use the same cube roots as in (9.10). ◁▷

Notice how (9.11) is similar to the formula

$$\zeta_5 = \frac{-1 + \sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5 + \sqrt{5}}{2}}$$

from Exercise 8 of Section A.2. These formulas were known to Lagrange and Vandermonde in the 1770s. Vandermonde also worked out a similar formula for ζ_{11}, which is more surprising in that it required solving an equation of degree 5 by radicals (see [Tignol, Ch. 11]).

B. Periods. In Section VII of *Disquisitiones*, Gauss proves the existence of radical formulas for ζ_p for any odd prime p. His proof uses *periods*, which for positive divisors f of $p - 1$ are carefully chosen primitive elements of L_f over $\mathbb{Q}$.

Let $ef = p - 1$, and let $H_f \subset (\mathbb{Z}/p\mathbb{Z})^*$ be the unique subgroup of order f. Given an element $a = [i] \in (\mathbb{Z}/p\mathbb{Z})^*$, set $\zeta_p^a = \zeta_p^i$. This is well defined, since $\zeta_p^p = 1$. Hence we can make the following definition.

Definition 9.2.3. *Let $\lambda \in \mathbb{Z}$ be relatively prime to p. This gives $[\lambda] \in (\mathbb{Z}/p\mathbb{Z})^*$ and the coset $[\lambda]H_f$ of H_f in $(\mathbb{Z}/p\mathbb{Z})^*$. Then we define an* ***f*-period** *to be the sum*

$$(f, \lambda) = \sum_{a \in [\lambda]H_f} \zeta_p^a.$$

Here are some simple properties of f-periods.

Lemma 9.2.4. *Let $ef = p - 1$, and let (f, λ) be defined as above. Then:*
(a) *Two f-periods either are identical or have no terms in common.*
(b) *There are e distinct f-periods.*
(c) *The f-periods are linearly independent over $\mathbb{Q}$.*
(d) *Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ satisfy $\sigma(\zeta_p) = \zeta_p^i$. Then, for any f-period (f, λ),*

$$\sigma\big((f, \lambda)\big) = (f, i\lambda).$$

Proof. Recall that $1, \zeta_p, \ldots, \zeta_p^{p-2} \in \mathbb{Q}(\zeta_p)$ are linearly independent over $\mathbb{Q}$, since $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Multiplying by ζ_p shows that the same is true for $\zeta_p, \ldots, \zeta_p^{p-1}$. This implies that two f-periods coincide if and only if the corresponding cosets of H_f are equal. Then part (a) follows because cosets are either identical or disjoint, and part (b) because the number of cosets is the index of H_f in $(\mathbb{Z}/p\mathbb{Z})^*$, which is $e = \frac{p-1}{f}$. Then part (c) is a consequence of part (a) together with the linear independence of $\zeta_p, \ldots, \zeta_p^{p-1}$ over $\mathbb{Q}$.

For part (d), observe that $\zeta_p^i = \zeta_p^{[i]}$. Thus $\sigma(\zeta_p) = \zeta_p^i$ implies that

$$\sigma\big((f, \lambda)\big) = \sum_{a \in [\lambda]H_f} (\zeta_p^i)^a = \sum_{a \in [\lambda]H_f} \zeta_p^{[i]a} = \sum_{b \in [i\lambda]H_f} \zeta_p^b = (f, i\lambda),$$

where the third equality follows via the substitution $b = [i]a$. □

Here are some particularly simple periods.

Example 9.2.5. Since p is odd, the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of order 2 is $H_2 = \{[1], [-1]\}$. The cosets of this subgroup are $[\lambda]H_2 = \{[\lambda], [-\lambda]\}$, so that the 2-periods are

$$(2, \lambda) = \zeta_p^\lambda + \zeta_p^{-\lambda} = 2\cos(2\pi\lambda/p).$$

The number of 2-periods is $e = \frac{p-1}{2}$.

In particular, when $p = 7$, the distinct 2-periods are $(2, 1)$, $(2, 2)$, and $(2, 3)$. These were denoted η_1, η_2, and η_3 in Example 9.2.2. ◁▷

We now prove that f-periods give the desired primitive elements.

Proposition 9.2.6. *Let L_f be the fixed field of H_f. Then:*
(a) *Let $(f, \lambda_1), \ldots, (f, \lambda_e)$ be the distinct f-periods. Then*

$$g(x) = \big(x - (f, \lambda_1)\big) \cdots \big(x - (f, \lambda_e)\big)$$

is in $\mathbb{Q}[x]$ and is the minimal polynomial of any f-period over $\mathbb{Q}$.
(b) *Any f-period is a primitive element of L_f over $\mathbb{Q}$.*

Proof. An f-period $\eta = (f, \lambda)$ corresponds to a coset $[\lambda]H_f$. If $[i] \in (\mathbb{Z}/p\mathbb{Z})^*$, then the f-period $(f, i\lambda)$ corresponding to $[i\lambda]H_f$ is a conjugate of η over $\mathbb{Q}$, by Lemma 9.2.4. Since $[i\lambda]H_f$ gives all cosets of H_f as we vary $[i]$, the conjugates of η over $\mathbb{Q}$ are the e distinct f-periods $(f, \lambda_1), \ldots, (f, \lambda_e)$. Then part (a) follows from the formula for the minimal polynomial given in equation (7.1) of Chapter 7.

It follows that $\mathbb{Q} \subset \mathbb{Q}(\eta)$ and $\mathbb{Q} \subset L_f$ are extensions of degree e. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ has a unique subgroup of index e, the Galois correspondence implies that $\mathbb{Q}(\eta) = L_f$. This proves part (b). □

As a corollary, we get the following interesting basis of L_f over $\mathbb{Q}$.

Corollary 9.2.7. *The f-periods form a basis of L_f over $\mathbb{Q}$.*

Proof. The f-periods lie in L_f by Proposition 9.2.6. Furthermore, Lemma 9.2.4 tells us that the e such periods are linearly independent over $\mathbb{Q}$. The corollary follows, since $[L_f : \mathbb{Q}] = e$ by Proposition 9.2.1. □

Our next task is to describe the extension $L_{f'} \subset L_f$ in terms of periods, where f and f' are positive divisors of $p - 1$ satisfying $f \mid f'$. Set $d = f'/f$, so that $[L_f : L_{f'}] = d$. Any f-period (f, λ) is a primitive element of L_f over $L_{f'}$. We need to describe its minimal polynomial over $L_{f'}$.

This is done as follows. Observe that H_f is a subgroup of index $d = f'/f$ in $H_{f'}$. Hence every coset of $H_{f'}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is a disjoint union of d cosets of H_f. (Do Exercise 4 if you are unsure of this.) In particular, $[\lambda]H_{f'}$ is a disjoint union

$$[\lambda]H_{f'} = [\lambda_1]H_f \cup \cdots \cup [\lambda_d]H_f, \tag{9.12}$$

where we may assume $\lambda_1 = \lambda$, since $[\lambda]H_f \subset [\lambda]H_{f'}$. This leads to the following description of the desired minimal polynomial.

Proposition 9.2.8. *Let f and f' be positive divisors of $p - 1$ such that $f \mid f'$, and set $d = f'/f$. Given an f-period (f, λ), let $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_d$ be as in* (9.12). *Then*

$$h(x) = \big(x - (f, \lambda_1)\big) \cdots \big(x - (f, \lambda_d)\big)$$

is in $L_{f'}[x]$ and is the minimal polynomial of (f, λ) over $L_{f'}$.

Proof. The proof is similar to what we did in part (b) of Proposition 9.2.6. Setting $\eta = (f, \lambda)$, we need to show that as σ varies over $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'})$, the elements $\sigma(\eta)$ give the f-periods $(f, \lambda_1), \ldots, (f, \lambda_d)$.

To prove this, let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'})$, so that $\sigma(\zeta_p) = \zeta_p^i$ for $[i] \in H_{f'}$. Then

$$\sigma(\eta) = \sigma\big((f, \lambda)\big) = (f, i\lambda).$$

This f-period corresponds to the coset $[i\lambda]H_f$. However,

$$[i\lambda]H_f \subset [i\lambda]H_{f'} = [\lambda][i]H_{f'} = [\lambda]H_{f'},$$

where the final equality uses $[i] \in H_{f'}$. By (9.12), it follows that $[i\lambda]H_f = [\lambda_j]H_f$ for some j, so that $\sigma(\eta) = (f, i\lambda) = (f, \lambda_j)$. Since every (f, λ_j) arises in this way (see Exercise 5), the proposition is proved. □

We will give an example of Proposition 9.2.8 below.

C. Explicit Calculations. The above results are pretty but somewhat abstract. To compute specific examples, we need a concrete way to work with periods. The key idea, due to Gauss, is to pick a generator $[g]$ of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Since this group has order $p - 1$, it follows that

$$(\mathbb{Z}/p\mathbb{Z})^* = \big\{[1], [g], [g^2], \ldots, [g^{p-2}]\big\}.$$

In other words, the $p - 1$ numbers $1, g, g^2, \ldots, g^{p-2}$ represent the nonzero congruence classes modulo p. We call g a *primitive root* modulo p.

Given a primitive root g and $ef = p - 1$ as usual, Exercise 1 implies that H_f is generated by g^e, that is,

$$H_f = \big\{[1], [g^e], [g^{2e}], \ldots, [g^{(f-1)e}]\big\}.$$

It follows that the coset $[\lambda]H_f$ gives the f-period

$$(9.13) \qquad (f, \lambda) = \zeta_p^{\lambda} + \zeta_p^{\lambda g^e} + \zeta_p^{\lambda g^{2e}} + \cdots + \zeta_p^{\lambda g^{(f-1)e}} = \sum_{j=0}^{f-1} \zeta_p^{\lambda g^{je}}.$$

So far, we have assumed that $[\lambda] \in (\mathbb{Z}/p\mathbb{Z})^*$, that is, $p \nmid \lambda$. However, (9.13) makes sense for *any* integer λ. Since $\zeta_p^p = 1$, one easily sees that

$$(f, \lambda) = f \quad \text{when} \quad p|\lambda.$$

For an arbitrary $\lambda \in \mathbb{Z}$, we call (f, λ) a *generalized period*. Thus a generalized period is an ordinary period if $p \nmid \lambda$ and is equal to f if $p|\lambda$.

In order to compute the minimal polynomials appearing in Propositions 9.2.6 and 9.2.8, we need to know how to multiply f-periods. Gauss expressed the product of two f-periods in terms of generalized periods as follows.

Proposition 9.2.9. *If (f, λ) and (f, μ) are f-periods with $p \nmid \lambda$ and $p \nmid \mu$, then*

$$(f,\lambda)(f,\mu) = \sum_{[\lambda']\in[\lambda]H_f} (f, \lambda' + \mu) = \sum_{j=0}^{f-1} (f, \lambda g^{je} + \mu).$$

Proof. Following [4, Art. 345], we set $h = g^e$, so that

$$(f,\mu) = \sum_{\ell=0}^{f-1} \zeta_p^{\mu h^\ell}$$

since $[h]$ generates H_f. We also have $[\lambda]H_f = [\lambda h^\ell]H_f$ for any ℓ, which implies that $(f, \lambda) = (f, \lambda h^\ell)$. Thus

$$\begin{aligned}(f,\lambda)(f,\mu) &= \sum_{\ell=0}^{f-1} (f,\lambda)\,\zeta_p^{\mu h^\ell} = \sum_{\ell=0}^{f-1} (f,\lambda h^\ell)\,\zeta_p^{\mu h^\ell} \\ &= \sum_{\ell=0}^{f-1} \Big(\sum_{j=0}^{f-1} \zeta_p^{\lambda h^\ell h^j} \Big) \zeta_p^{\mu h^\ell} = \sum_{j=0}^{f-1} \Big(\sum_{\ell=0}^{f-1} \zeta_p^{(\lambda h^j + \mu) h^\ell} \Big) \\ &= \sum_{j=0}^{f-1} (f, \lambda h^j + \mu).\end{aligned}$$

This gives the desired formula, since $h = g^e$. □

Here is an example from [4, Art. 346].

Example 9.2.10. In this example and three that follow, we will consider the 6-periods for $p = 19$. In Exercise 7 you will show that $g = 2$ is a primitive root modulo 19. Since $f = 6$ implies $e = 3$, the unique subgroup of order 6 in $(\mathbb{Z}/19\mathbb{Z})^*$ is generated by $[2]^3 = [8]$. Thus

$$H_6 = \{[1], [8], [8]^2, [8]^3, [8]^4, [8]^5\} = \{[1], [8], [7], [18], [11], [12]\} \subset (\mathbb{Z}/19\mathbb{Z})^*.$$

For simplicity, we will write $[n]$ as n, so that

$$H_6 = \{1, 7, 8, 11, 12, 18\}.$$

The $e = 3$ cosets of H_6 in $(\mathbb{Z}/19\mathbb{Z})^*$ are H_6 together with

$$\begin{aligned}2H_6 &= \{2, 14, 16, 22, 24, 36\} = \{2, 3, 5, 14, 16, 17\}, \\ 4H_6 &= \{4, 28, 32, 44, 48, 72\} = \{4, 6, 9, 10, 13, 15\}.\end{aligned}$$

(Remember that we are working modulo 19.)

According to Proposition 9.2.9,

$$\begin{aligned}(6,1)^2 &= (6,1+1)+(6,7+1)+(6,8+1)+(6,11+1)+(6,12+1)+(6,18+1) \\ &= (6,2)+(6,8)+(6,9)+(6,12)+(6,13)+6,\end{aligned}$$

where the second equality uses $(6, 19) = 6$. This shows that generalized periods can arise when we multiply ordinary periods. However,

$$(6, 8) = (6, 1)$$

since 8 and 1 lie in the same coset of H_6. Using similar simplifications, we get

$$(6, 1)^2 = 2(6, 1) + (6, 2) + 2(6, 4) + 6.$$

By Exercise 6 we also have

$$(6, 1) + (6, 2) + (6, 4) = -1.$$

Then the formula for $(6, 1)^2$ simplifies to

$$(6, 1)^2 = 4 - (6, 2).$$

You will work out similar formulas in Exercise 7. ◁▷

Example 9.2.11. Still assuming $p = 19$, our next task is to compute the minimal polynomial of the 6-periods over $\mathbb{Q}$. We will use the notation of the previous example. By Proposition 9.2.6, the minimal polynomial is

$$(x - (6, 1))(x - (6, 2))(x - (6, 4)). \tag{9.14}$$

In Exercise 7 you will use the methods of Example 9.2.10 to show that

$$\begin{aligned} (6, 1)(6, 2) &= (6, 1) + 2(6, 2) + 3(6, 4), \\ (6, 1)(6, 4) &= 2(6, 1) + 3(6, 2) + (6, 4), \\ (6, 2)(6, 4) &= 3(6, 1) + (6, 2) + 2(6, 4). \end{aligned} \tag{9.15}$$

Note that these sum to $6(6, 1) + 6(6, 2) + 6(6, 4) = -6$, since (as noted above) $(6, 1) + (6, 2) + (6, 4) = -1$.

Using (9.15) and $(6, 1)^2 = 4 - (6, 2)$ (from Example 9.2.10), we have

$$\begin{aligned} (6, 1)(6, 2)(6, 4) &= (6, 1)\big(3(6, 1) + (6, 2) + 2(6, 4)\big) \\ &= 3(6, 1)^2 + (6, 1)(6, 2) + 2(6, 1)(6, 4) \\ &= 12 + 5(6, 1) + 5(6, 2) + 5(6, 4) = 7 \end{aligned}$$

(see Exercise 7 for the details). It follows that multiplying out (9.14) gives

$$x^3 + x^2 - 6x - 7. \tag{9.16}$$

This is the minimal polynomial of the 6-periods over $\mathbb{Q}$. Its splitting field is $\mathbb{Q} \subset L_6$, the extension generated by the 6-periods. ◁▷

Example 9.2.12. Now consider the 3-periods for $p = 19$. Since $6/3 = 2$, we see that $L_6 \subset L_3$ is an extension of degree 2. Hence 3-periods have quadratic minimal polynomials over L_6.

Since 2 is a primitive root modulo 19, the subgroup $H_3 \subset (\mathbb{Z}/19\mathbb{Z})^*$ is generated by $[2]^6 = [8]^2 = [7]$. Using the notation of Example 9.2.10, we have

$$H_6 = \{1, 7, 8, 11, 12, 18\} = \{1, 7, 11\} \cup \{8, 12, 18\} = H_3 \cup 8H_3.$$

This shows that

$$(6, 1) = (3, 1) + (3, 8),$$

and in a similar way, one obtains

$$(6, 2) = (3, 2) + (3, 16),$$
$$(6, 4) = (3, 4) + (3, 13).$$

However, Proposition 9.2.9 implies that

$$(3, 1)(3, 8) = (3, 1 + 8) + (3, 7 + 8) + (3, 11 + 8) = (3, 9) + (3, 15) + 3,$$

and since $(3, 9) = (3, 4)$ and $(3, 15) = (3, 13)$ (do you see why?), we get

$$(3, 1)(3, 8) = (3, 4) + (3, 13) + 3 = (6, 4) + 3.$$

By Proposition 9.2.8, the minimal polynomial of $(3, 1)$ and $(3, 8)$ over L_6 is

$$(x - (3, 1))(x - (3, 8)) = x^2 - (6, 1)x + (6, 4) + 3. \tag{9.17}$$

Exercise 7 will consider the minimal polynomials of the other 3-periods. ◁▷

Example 9.2.13. The 1-periods for $p = 19$ are the primitive 19th roots of unity $(1, \lambda) = \zeta_{19}^{\lambda}$ for $\lambda = 1, \ldots, 18$. In Example 9.2.12, we noted that $H_3 = \{1, 7, 11\}$, which means that

$$(3, 1) = \zeta_{19} + \zeta_{19}^7 + \zeta_{19}^{11}.$$

By Exercise 7 the minimal polynomial of ζ_{19}, ζ_{19}^7 and ζ_{19}^{11} over L_3 is

$$(x - \zeta_{19})(x - \zeta_{19}^7)(x - \zeta_{19}^{11}) = x^3 - (3, 1)x^2 + (3, 8)x - 1. \tag{9.18}$$

Combining this with (9.17) and (9.16), one can write an explicit formula for ζ_{19} that involves only square and cube roots. ◁▷

In Exercises 8 and 9 you will use similar methods to derive the formula

$$\begin{aligned}\cos(2\pi/17) = &-\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{34 - 2\sqrt{17}} \\ &+\tfrac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}},\end{aligned} \tag{9.19}$$

due to Gauss. In Chapter 10, we will see that this leads immediately to a straightedge-and-compass construction of a regular 17-gon.

One reason these methods work so well is that the f-periods are linearly independent over $\mathbb{Q}$ by Lemma 9.2.4. Hence any linear combination of f-periods with coefficients in $\mathbb{Z}$ or $\mathbb{Q}$ is unique. However, we've seen cases where generalized periods (f, λ), $p|\lambda$, also occur. But this is no problem, since $(f, \lambda) = f$ in such a case, and we also know that the distinct f-periods sum to -1 (see Exercise 6). Thus a generalized f-period can be expressed in terms of ordinary f-periods. Hence we can always reduce to an expression involving only f-periods, where we know that the representation is unique.

D. Solvability by Radicals. When studying $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, we saw in (9.9) that a prime factorization $p - 1 = q_1 q_2 \cdots q_r$ gives intermediate fields

$$\mathbb{Q} = L_{q_1 \cdots q_r} \subset L_{q_2 \cdots q_r} \subset \cdots \subset L_{q_{r-1} q_r} \subset L_{q_r} \subset L_1 = \mathbb{Q}(\zeta_p)$$

such that $[L_{q_{i+1} \cdots q_r} : L_{q_i q_{i+1} \cdots q_r}] = q_i$. If we focus on one of these fields and the next larger one, then we get an extension of the form

$$L_{fq} \subset L_f \tag{9.20}$$

where fq divides $p - 1$ and q is prime. The theory of periods shows that $(f, 1)$ is a primitive element of L_f and the examples given above make it clear that in any particular case we can compute the minimal polynomial of $(f, 1)$ over L_{fq}.

When $p = 19$, the minimal polynomials found in Examples 9.2.10 to 9.2.13 have degrees 2 or 3. Hence their roots can be found by known formulas. But when $p = 11$, the period $(2, 1) = 2\cos(2\pi/11)$ has minimal polynomial

$$y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1$$

(see Exercise 10). Is this polynomial solvable by radicals? More generally, are the minimal polynomials of periods solvable by radicals?

For a theoretical point of view, this question is trivial, since $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ is a radical extension ($\zeta_p^p = 1 \in \mathbb{Q}$). It follows by definition that any f-period (f, λ) is expressible by radicals over $\mathbb{Q}$, since $(f, \lambda) \in \mathbb{Q}(\zeta_p)$. Things become even more trivial if you recall that when we studied solvability by radicals in Chapter 8, we felt free to adjoin any roots of unity we needed, including ζ_p.

Hence it appears that solving the minimal polynomials of periods by radicals is completely uninteresting. The problem is that this ignores the *inductive* nature of what's going on. The real goal, which goes back to Lagrange's strategy for solving equations, is to construct pth roots of unity using only radicals and roots of unity of *lower degree* (we will discuss Lagrange's strategy in Chapter 12). This is what Gauss does in *Disquisitiones*.

Thus, when studying $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, we may assume inductively that we know all mth roots of unity for $m < p$. Furthermore, as explained in the discussion preceding (9.20), it suffices to consider the extension $L_{fq} \subset L_f$, where we may assume that the fq-periods are known. The idea is to express an f-period in terms of radicals that are qth roots involving fq-periods and qth roots of unity. These roots of unity are known, since $q < p$.

To do this in practice, we will use Lagrange resolvents. Let ω be a primitive qth root of unity. In Exercise 11 you will prove that

$$\mathrm{Gal}(L_f(\omega)/L_{fq}(\omega)) \simeq \mathrm{Gal}(L_f/L_{fq}) \simeq \mathbb{Z}/q\mathbb{Z}.$$

Since $L_{fq}(\omega)$ contains a primitive qth root of unity, Lemma 8.3.2 implies that $L_f(\omega)$ is obtained from $L_{fq}(\omega)$ by adjoining a qth root. Furthermore, the proof of Lemma 8.3.2 shows that the element adjoined is a Lagrange resolvent. Recall from (8.7) that if σ is a generator of $\mathrm{Gal}(L_f(\omega)/L_{fq}(\omega))$ and $\beta \in L_f(\omega)$, then we get the *Lagrange resolvents*

$$\alpha_i = \beta + \omega^{-i}\sigma(\beta) + \cdots + \omega^{-i(q-1)}\sigma^{q-1}(\beta)$$

for $i = 0, \ldots, q-1$. We will use $\beta = (f, 1) \in L_f \subset L_f(\omega)$. In Exercise 11 you will show that we can pick the generator σ so that for any f-period (f, λ),

$$\sigma\big((f, \lambda)\big) = (f, g^{e/q}\lambda) \tag{9.21}$$

(note that $q|e$, since $fq|p-1$). Thus the above Lagrange resolvents can be written

$$\alpha_i = (f, 1) + \omega^{-i}(f, g^{e/q}) + \cdots + \omega^{-i(q-1)}(f, g^{(q-1)e/q}). \tag{9.22}$$

If we set $A_i = \alpha_i^q$, then we can define $\sqrt[q]{A_i} = \alpha_i$. Then the f-periods in (9.22) can be expressed in terms of radicals as follows.

Theorem 9.2.14. *Let α_i and $A_i = \alpha_i^q$ be defined as above.*
(a) *$\alpha_0 \in L_{fq}(\omega)$ and $A_i = \alpha_i^q \in L_{fq}(\omega)$ for $1 \le i \le q-1$.*
(b) *For $0 \le \ell \le q-1$,*

$$(f, g^{\ell e/q}) = \frac{1}{q}\Big(\alpha_0 + \omega^{\ell}\sqrt[q]{A_1} + \omega^{2\ell}\sqrt[q]{A_2} + \cdots + \omega^{(q-1)\ell}\sqrt[q]{A_{q-1}}\Big).$$

Before beginning the proof, let's explain the f-periods appearing in the theorem. The extension $L_{fq} \subset L_f$ corresponds to the subgroups $H_f \subset H_{fq}$ of $(\mathbb{Z}/p\mathbb{Z})^*$. Since $e = \frac{p-1}{f}$, Exercise 1 shows that these subgroups are generated by $[g^e]$ and $[g^{e/q}]$ respectively. In Exercise 11 you will use this to prove that

$$H_{fq} = H_f \cup g^{e/q}H_f \cup g^{2e/q}H_f \cup \cdots \cup g^{(q-1)e/q}H_f. \tag{9.23}$$

By Proposition 9.2.8, the f-periods $(f, g^{\ell e/q})$ are the conjugates of $(f, 1)$ over L_{fq}.

Proof of Theorem 9.2.14. Part (a) follows easily from the properties of Lagrange resolvents presented in the proof of Lemma 8.3.2. For part (b), let $\lambda_\ell = g^{\ell e/q}$. Then for any integer m we have

$$\begin{aligned}\sum_{i=0}^{q-1}\omega^{mi}\alpha_i &= \sum_{i=0}^{q-1}\omega^{mi}\Big(\sum_{\ell=0}^{q-1}\omega^{-i\ell}(f, \lambda_\ell)\Big)\\ &= \sum_{\ell=0}^{q-1}\Big(\sum_{i=0}^{q-1}\omega^{(m-\ell)i}\Big)(f, \lambda_\ell) = q\,(f, \lambda_m),\end{aligned}$$

where the last equality follows from Exercise 9 of Section A.2. This gives the desired formula for (f, λ_m), since $\alpha_i = \sqrt[q]{A_i}$ for $i > 0$. □

From a computational point of view, the results of this section give a systematic method for expressing $A_i = \alpha_i^q$ in terms of fq-periods and qth roots of unity. This works because f-periods and fq-periods are linearly independent not only over $\mathbb{Q}$ but also over $\mathbb{Q}(\omega)$, where ω is a primitive qth root of unity (you will prove this in Exercise 12). Thus the radical formula for $(f, g^{\ell e/q})$ given in Theorem 9.2.14 is explicitly computable.

Mathematical Notes

Here are comments on two topics relevant to what we did in this section.

▪ **Primitive Roots Modulo p.** The formulas presented in this section illustrate the usefulness of knowing primitive roots modulo p. Gauss explains a method for finding primitive roots in [4, Art. 73–74]. See also [9, p. 163].

Let g_p denote the smallest positive primitive root modulo p. For example, 2 is a primitive root modulo 19, which implies that $g_{19} = 2$. In 1962 Burgess [3] proved that for any $\varepsilon > 0$ there is a positive constant $C(\varepsilon)$ such that

$$g_p \leq C(\varepsilon) p^{\frac{1}{4}+\varepsilon}$$

for all odd primes p. This says that g_p can't be too big relative to p. On the other hand, Kearnes [8] proved in 1984 that given any integer $m > 0$ there are infinitely many primes $p > m$ such that $g_p > m$. So g_p can still get large.

If we fix a primitive root g modulo p, then the *discrete log* problem asks the following: given an integer a not divisible by p, find i such that $a \equiv g^i \bmod p$. We write this as $i = \log_g a$. It is easy to describe an algorithm for finding $\log_g a$ (divide $a - g^i$ by p for $i = 0, 1, 2, \ldots$, and stop when the remainder is zero). But finding an *efficient* algorithm for $\log_g a$ is much more difficult. Several modern encryption schemes, including the Pohig–Hellman symmetric key exponentiation cipher (described in [9, Sec. 3.1]) and the Diffie–Hellman key exchange protocol (described in [2, Sec. 7.4] and [9, Sec. 3.1]), would be easy to break if discrete logs were easy to compute.

Primitive roots modulo p are also used in the *Digital Signature Algorithm* suggested by the National Institute of Standards and Technology. A description can be found in [2, Sec. 11.5]. As above, one could forge digital signatures if discrete logs were easy to compute.

There are also purely mathematical questions about primitive roots modulo p. A list of unsolved problems can be found in [6, Sec. F.9].

▪ **Periods and Gauss Sums.** Let $p = 17$. By Exercise 9 we have

$$(8, 1) = \tfrac{1}{2}(-1 + \sqrt{17}),$$
$$(8, 3) = \tfrac{1}{2}(-1 - \sqrt{17}),$$

which easily implies

$$(8, 1) - (8, 3) = \sqrt{17}.$$

In Exercise 13 you will show that this can be written

$$\sum_{a=0}^{17} \left(\frac{a}{17}\right) \zeta_{17}^{a} = \sqrt{17}, \tag{9.24}$$

where, for an odd prime p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a, \\ +1, & \text{if } p \nmid a,\ x^2 \equiv a \bmod p \text{ has a solution}, \\ -1, & \text{if } p \nmid a,\ x^2 \equiv a \bmod p \text{ has no solution}. \end{cases}$$

More generally, for an odd prime p, a *quadratic Gauss sum* is defined to be

$$g_\ell = \sum_{a=0}^{p} \left(\frac{a}{p}\right) \zeta_p^{\ell a}.$$

Gauss used these sums to prove quadratic reciprocity. He also proved the remarkable formula

$$g_1 = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p}, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Notice how this generalizes (9.24). A careful discussion of quadratic Gauss sums can be found in [7, Ch. 6].

Historical Notes

Most results of this section are implicit in Section VII of *Disquisitiones*. The main difference is that we have stated things in terms of the Galois correspondence, which to each divisor f of $p - 1$ associates the subgroup H_f of $(\mathbb{Z}/p\mathbb{Z})^*$ and the subfield L_f of $\mathbb{Q}(\zeta_p)$. For Gauss, on the other hand, each divisor f gets associated to the collection of f-periods (f, λ). In general, he considers elements rather than the fields in which they lie. For example, consider [4, Art. 346], which asserts that given (f, λ), any other f-period (f, μ) can be expressed as

$$(f, \mu) = \alpha_0 + \alpha_1(f, \lambda) + \alpha_2(f, \lambda)^2 + \cdots + \alpha_{e-1}(f, \lambda)^{e-1}$$

for some uniquely determined integers $\alpha_0, \ldots, \alpha_{e-1}$. For us, this gives the unique representation of (f, μ) as an element of $L_f = \mathbb{Q}\big((f, \lambda)\big)$.

Another difference is our use of cosets. For example, if g is a primitive root modulo p and f divides $p - 1$, then Gauss notes that the distinct f-periods are

$$(f, 1), (f, g), (f, g^2), \ldots, (f, g^{e-1}),$$

where $e = \frac{p-1}{f}$. For us, this follows from Lemma 9.2.4, since $H_f \subset (\mathbb{Z}/p\mathbb{Z})^*$ is generated by $[g^e]$, so that its cosets in $(\mathbb{Z}/p\mathbb{Z})^*$ are

$$[1]H_f, [g]H_f, [g^2]H_f, \ldots, [g^{e-1}]H_f.$$

Cosets give a conceptual basis for what Gauss is doing, and the same is true for the minimal polynomials computed in Proposition 9.2.8.

It is also interesting to note that Gauss makes implicit use of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. We saw in Lemma 9.2.4 that $\sigma(\zeta_p) = \zeta_p^k$ implies that $\sigma\big((f, \lambda)\big) = (f, k\lambda)$. Now consider the following quote from [4, Art. 345]:

> IV. It follows that if in any rational integral algebraic function $F = \phi(t, u, v, \ldots)$ we substitute for the unknowns t, u, v, etc. respectively the similar periods (f, λ), (f, μ), (f, ν), etc., its value will be reducible to the form
>
> $$A + B(f, 1) + B'(f, g) + B''(f, g^2) \ldots + B^{\varepsilon}(f, g^{e-1})$$
>
> and the coefficients A, B, B', etc. will all be integers if all the coefficients in F are integers. But if afterward we substitute $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$, etc. for t, u, v, etc. respectively, the value of F will be reduced to $A + B(f, k) + B'(f, kg) + \text{etc.}$

A "rational integral algebraic function" is a polynomial with coefficients in $\mathbb{Q}$. Here is an example of what this means.

Example 9.2.15. In Example 9.2.10, we showed that

$$(6, 1)^2 = 4 - (6, 2)$$

when $p = 19$. Using $k = 2$, the above quotation from Gauss tells us that

$$(6, 2)^2 = 4 - (6, 4).$$

In modern terms, this follows by applying the automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q})$ that takes ζ_{19} to ζ_{19}^2. So the Galois action is implicit in Gauss's theory! ◁▷

Gauss's result that $x^p - 1$ is solvable by radicals is less compelling from the modern perspective, though it is still interesting when one thinks inductively. But historically, being able to solve special but nontrivial equations of high degree was important. Here is what Gauss says in [4, Art. 359]:

> Everyone knows that the most eminent geometers have been unsuccessful in the search for a general solution of equations higher than the fourth degree, or (to define the search more accurately) for the THE REDUCTION OF MIXED EQUATIONS TO PURE EQUATIONS. ... Nevertheless, it is certain that there are innumerable mixed equations of every degree that admit a reduction to pure equations, and we trust that geometers will find it gratifying if we show that our equations are always of this kind.

For Gauss, an equation is "pure" if it is of the form $x^m - A = 0$ and "mixed" otherwise. Thus, reducing "mixed equations to pure equations" is what we call solvability by radicals. Of course, in saying "our equations," Gauss is referring to the minimal polynomials satisfied by the periods, as constructed in Proposition 9.2.8.

Gauss's study of the pth roots of unity is an important midpoint in the development leading from Lagrange to the emergence of Galois theory. Gauss uses Lagrange's inductive strategy to work out the Galois correspondence for $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, and his theory of periods makes everything explicit and computable. He also shows that Lagrange resolvents are the correct tool for studying solvability by radicals, paving the way for Galois's analysis of the general case.

In spite of its beauty, what Gauss does in Section VII of [4] is not perfect. Some proofs are omitted and others have gaps. For example, Gauss does not prove the assertion about the Galois action made in the quotation before Example 9.2.15. Also, as noted in [Tignol, p. 195], Gauss's study of solvability assumes without proof that when fq divides $p-1$, the f-periods are linearly independent over the field generated by the qth roots of unity. (You will prove this in Exercise 12.)

Galois was very aware of Section VII of *Disquisitiones*. For example, Galois describes the "group" of $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$, n prime, as follows [Galois, pp. 51–53]:

> In the case of the equation $\frac{x^n-1}{x-1} = 0$, if one supposes $a = r$, $b = r^g$, $c = r^{g^2}$, ..., g being a primitive root, the group of permutations will simply be as follows:
>
> $$\begin{array}{cccccc} a & b & c & d & \ldots & k \\ b & c & d & \ldots & k & a \\ c & d & \ldots & k & a & b \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ k & a & b & c & \ldots & i \end{array}$$
>
> in this particular case, the number of permutations is equal to the degree of the equation, and the same will be true for equations where all of the roots are rational functions of each other.

Here, r is a primitive nth root of unity. Each line is a cyclic permutation of the one above it, which leads to a cyclic group of order $n-1$. This quotation also reveals that for Galois, a "permutation" was an arrangement of the roots and that the permutations (in the modern sense) are obtained by mapping the first arrangement in the table to the others. You will work out the details of this in Exercise 14. We will say more about how Galois thought about Galois groups in Chapter 12.

Exercises for Section 9.2

Exercise 1. Let G be a cyclic group of order n and let g be a generator of G.

(a) Let f be a positive divisor of n and set $e = n/f$. Prove that $H_f = \langle g^e \rangle$ has order f and hence is the unique subgroup of order f.

(b) Let f and f' be positive divisors of $p-1$. Prove that $H_f \subset H_{f'}$ if and only if $f | f'$.

Exercise 2. Prove Proposition 9.2.1.

Exercise 3. Let η_1, η_2, η_3 be as in Example 9.2.2.

(a) We know that ζ_7 is a root of $x^6+x^5+x^4+x^3+x^2+x+1 = 0$. Dividing by x^3 gives

$$x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3} = 0.$$

Use this to show that η_1, η_2, η_3 are roots of $y^3 + y^2 - 2y - 1$.

(b) Prove that $[\mathbb{Q}(\eta_1):\mathbb{Q}] = 3$, and conclude that $\mathbb{Q}(\eta_1)$ is the fixed field of the subgroup $\{e, \tau\} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, where τ is complex conjugation.

(c) Prove (9.10).

Exercise 4. Let $A \subset B$ be subgroups of a group G, and assume that A has index d in B. Prove that every left coset of B in G is a disjoint union of d left cosets of A in G.

Exercise 5. Complete the proof of Proposition 9.2.8.

Exercise 6. Prove that the sum of the distinct f-periods equals -1.

Exercise 7. This exercise is concerned with the details of Examples 9.2.10, 9.2.11, 9.2.12, and 9.2.13.

(a) Show that 2 is a primitive root modulo 19.

(b) Use the methods of Example 9.2.10 to obtain formulas for $(6, 2)^2$ and $(6, 4)^2$.

(c) Show that the formulas of part (b) follow from $(6, 1)^2 = 4 - (6, 2)$ and part (d) of Lemma 9.2.4.

(d) Prove (9.15) and use this and Exercise 6 to show that $(6, 1)(6, 2)(6, 4) = 7$.

(e) Find the minimal polynomials of $(3, 2)$ and $(3, 4)$ over the field L_6 considered in Example 9.2.12.

(f) Show that (9.18) is the minimal polynomial of ζ_{19} over the field L_3 considered in Example 9.2.13.

Exercise 8. In this exercise and the next, you will derive Gauss's radical formula (9.19) for $\cos(2\pi/17)$.

(a) Show that 3 is a primitive root modulo 17.

(b) Show that

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\},$$
$$H_4 = \{1, 4, 13, 16\},$$
$$H_2 = \{1, 16\},$$

where we write the congruence class $[n]$ modulo 17 as n.

(c) Use Propositions 9.2.8 and 9.2.9 to compute the following minimal polynomials:

Extension	Primitive Elements	Minimal Polynomial
$\mathbb{Q} \subset L_8$	$(8, 1), (8, 3)$	$x^2 + x - 4$
$L_8 \subset L_4$	$(4, 1), (4, 2)$	$x^2 - (8, 1)x - 1$
	$(4, 3), (4, 6)$	$x^2 - (8, 3)x - 1$
$L_4 \subset L_2$	$(2, 1), (2, 4)$	$x^2 - (4, 1)x + (4, 3)$

The resulting quadratic equations are easy to solve using the quadratic formula. But how do the roots correspond to the periods? For example, the roots $(8, 1)$, $(8, 3)$ of $x^2 + x - 4$ are $(-1 \pm \sqrt{17})/2$. How do these match up? The answer will be given in the next exercise.

Exercise 9. In this exercise, you will use numerical computations and the previous exercise to find radical expressions for various f-periods when $p = 17$.

(a) Show that

$$(8, 1) = 2\cos(2\pi/17) + 2\cos(4\pi/17) + 2\cos(8\pi/17) + 2\cos(16\pi/17),$$
$$(4, 1) = 2\cos(2\pi/17) + 2\cos(8\pi/17),$$
$$(4, 3) = 2\cos(6\pi/17) + 2\cos(10\pi/17),$$
$$(2, 1) = 2\cos(2\pi/17).$$

Then compute each of these periods to five decimal places.

(b) Use the numerical computations of part (a) and the quadratic polynomials of Exercise 8 to show that

$$(8, 1) = \tfrac{1}{2}\left(-1 + \sqrt{17}\right),$$
$$(8, 3) = \tfrac{1}{2}\left(-1 - \sqrt{17}\right),$$
$$(4, 1) = \tfrac{1}{4}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right),$$
$$(4, 2) = \tfrac{1}{4}\left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}\right),$$
$$(4, 3) = \tfrac{1}{4}\left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}\right).$$

(c) Use the quadratic polynomial $x^2 - (4, 1)x - (4, 3)$ and part (b) to derive (9.19).

Exercise 10. Let $p = 11$. Prove that $y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1$ is the minimal polynomial of the 2-period $(2, 1) = 2\cos(2\pi/11)$.

Exercise 11. Let $L_{fq} \subset L_f$ be the extension studied in Theorem 9.2.14. Thus f and fq divide $p - 1$, and q is prime. As usual, $ef = p - 1$ and g is a primitive root modulo p. Finally, let ω be a primitive qth root of unity.

(a) Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ satisfy $\tau(\zeta_p) = \zeta_p^{g^{e/q}}$, and let $\sigma' = \tau|_{L_f}$ be the restriction of τ to L_f. Prove that σ' generates $\mathrm{Gal}(L_f/L_{fq})$.

(b) Prove that $\mathrm{Gal}(L_f(\omega)/L_{fq}(\omega)) \simeq \mathrm{Gal}(L_f/L_{fq})$, where the isomorphism is defined by restriction to L_f.

(c) Let $\sigma \in \mathrm{Gal}(L_f(\omega)/L_{fq}(\omega))$ map to the element $\sigma' \in \mathrm{Gal}(L_f/L_{fq})$ constructed in part (a). Prove that σ satisfies (9.21).

(d) Prove the coset decomposition of H_{fq} given in (9.23).

Exercise 12. Let p be an odd prime, and let m be a positive integer relatively prime to p.

(a) Prove that $1, \zeta_p, \ldots, \zeta_p^{p-2}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.

(b) Explain why part (a) implies that $\zeta_p, \ldots, \zeta_p^{p-1}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.

(c) Let $f|p - 1$. Prove that the f-periods are linearly independent over $\mathbb{Q}(\zeta_m)$.

Exercise 13. Prove (9.24).

Exercise 14. Consider the quotation from Galois given at the end of the Historical Notes.

(a) Show that the permutations obtained by mapping the first line in the displayed table to the other lines give a cyclic group of order $n - 1$. Also explain how these permutations relate to the Galois group.

(b) Explain what Galois is saying in the last sentence of the quotation.

Exercise 15. What are the 1-periods?

Exercise 16. Redo Exercise 3 using periods.

Exercise 17. Let f be an even divisor of $p - 1$, where p is an odd prime. Prove that every f-period (f, λ) lies in $\mathbb{R}$.

REFERENCES

1. G. Bachman, *On the coefficients of cyclotomic polynomials*, Mem. Amer. Math. Soc. **106** (1993).

2. J. A. Buchmann, *Introduction to Cryptography*, Springer-Verlag, New York, Berlin, Heidelberg, 2001.

3. D. A. Burgess, *On character sums and L-series*, Proc. London Math. Soc. **12** (1962), 193-206.

4. C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801. Republished in 1863 as Volume I of [Gauss]. French translation, *Recherches Arithmétiques*, Paris, 1807. Reprint by Hermann, Paris, 1910. German translation, *Untersuchungen über Höhere Arithmetik*, Berlin, 1889. Reprint by Chelsea, New York, 1965. English translation, Yale U. P., New Haven, 1966. Reprint by Springer-Verlag, New York, Berlin, Heidelberg, 1986.

5. J. J. Gray, *A commentary on Gauss's mathematical diary, 1796–1814, with an English translation*, Expo. Math. **2** (1984), 97–130. (The Latin original of Gauss's diary is reprinted in [Gauss, Vol. X.1].)

6. R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1994.

7. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1982.

8. K. Kearnes, *Solution of Problem 6420*, Amer. Math. Monthly **91** (1984), 521.

9. R. A. Mollin, *Introduction to Cryptography*, Chapman & Hall/CRC, Boca Raton, FL, 2001.

GALOIS THEORY

DAVID A. COX
Amherst College
Department of Mathematics & Computer Science
Amherst, MA

A JOHN WILEY & SONS, INC., PUBLICATION