CYCLOTOMIC EXTENSIONS

KEITH CONRAD

1. Introduction

For any field K, a field $K(\zeta_n)$ where ζ_n is a root of unity (of order n) is called a *cyclotomic* extension of K. The term *cyclotomic* means circle-dividing, and comes from the fact that the nth roots of unity divide a circle into equal parts. We will see that the extensions $K(\zeta_n)/K$ have abelian Galois groups and we will look in particular at cyclotomic extensions of $\mathbf{Q}$ and finite fields. There are not many general methods known for constructing abelian extensions of fields; cyclotomic extensions are essentially the only construction that works for all base fields. (Other constructions of abelian extensions are Kummer extensions, Artin-Schreier-Witt extensions, and Carlitz extensions, but these all require special conditions on the base field and thus are not universally available.)

We start with an integer $n \geq 1$ such that $n \neq 0$ in K. (That is, K has characteristic 0 and $n \geq 1$ is arbitrary or K has characteristic p and n is not divisible by p.) The polynomial $X^n - 1$ is relatively prime to its deriative $nX^{n-1} \neq 0$ in $K[X]$, so $X^n - 1$ is separable over K: it has n different roots in splitting field over K. These roots form a multiplicative group of size n. In $\mathbf{C}$ we can write down the nth roots of unity analytically as $e^{2\pi ik/n}$ for $0 \leq k \leq n-1$ and see they form a cyclic group with generator $e^{2\pi i/n}$. What about the nth roots of unity in other fields?

Theorem 1.1. *The group of nth roots of unity in a field is cyclic. More generally, any finite subgroup of the nonzero elements of a field form a cyclic group.*

Proof. Let F be a field and G be a finite subgroup of $F^\times$. From the general theory of abelian groups, if there are elements in G with orders n_1 and n_2 then there is an element of G with order the least common multiple $[n_1, n_2]$. Letting n be the maximal order of all the elements of G, the order of every element in G divides n: if $g \in G$ has order n and $g' \in G$ has order n', then there is an element of G with order $[n, n'] \geq n$. Since n is the maximal order, $[n, n'] \leq n$, so $[n, n'] = n$, which implies n' divides n. Since all orders divide the maximal order n, every element of G is a root of $X^n - 1$, which implies $\#G \leq n$ (the number of roots of a polynomial in a field does not exceed its degree). At the same time, since all orders divide the size of the group we have $n | \#G$. Hence $n = \#G$, which means some element of G has order $\#G$, so G is cyclic. $\square$

Example 1.2. For any prime p, the group $(\mathbf{Z}/(p))^\times$ is cyclic since these are the nonzero elements in the field $\mathbf{Z}/(p)$ and they form a finite group. The theorem does *not* say $(\mathbf{Z}/(p^r))^\times$ is cyclic for $r > 1$, since $\mathbf{Z}/(p^r)$ is not a field for $r > 1$. In fact, $(\mathbf{Z}/(8))^\times$ is not cyclic.

The roots of $X^n - 1$ in a splitting field of characteristic not dividing n form a cyclic group, denoted μ_n. For instance, in $\mathbf{C}$ we have $\mu_2 = \{1, -1\}$ and $\mu_4 = \{1, -1, i, -i\}$. A generator of μ_n is denoted ζ_n. That is, ζ_n denotes a root of unity of exact order n. Any element of μ_n is an nth root of unity, while the generators of μ_n are called *primitive* nth roots of unity. (For example, -1 is a 4th root of unity but not a primitive 4th root of unity.) For $a \in \mathbf{Z}$, the order of ζ_n^a is $n/(a,n)$, so ζ_n^a is a primitive nth root of unity if and only if $(a,n)=1$. Therefore the number of primitive nth roots of unity is $\varphi(n) = \#(\mathbf{Z}/(n))^\times$. There is no unique generator of μ_n when $n>2$ (*e.g.*, if ζ_n is one generator then ζ_n^{-1} is another one), so writing ζ_n involves making an *ad hoc* choice of generator.

Since any two primitive nth root of unity in a field are powers of each other, the extension $K(\zeta_n)$ is independent of the choice of ζ_n. We will usually write this field as $K(\mu_n)$: adjoining one primitive nth root of unity is the same as adjoining a full set of nth roots of unity.

2. Embedding the Galois group

When $n \neq 0$ in K, the cyclotomic extension $K(\mu_n)/K$ is Galois since X^n-1 is separable in $K[X]$.

Lemma 2.1. *For $\sigma \in \mathrm{Gal}(K(\mu_n)/K)$ there is an $a \in \mathbf{Z}$ relatively prime to n such that $\sigma(\zeta)=\zeta^a$ for all nth roots of unity ζ.*

Proof. Let ζ_n be a generator of μ_n (that is, a primitive nth root of unity), so $\zeta_n^n = 1$ and $\zeta_n^j \neq 1$ for $1 \leq j < n$. Then $\sigma(\zeta_n)^n = 1$ and $\sigma(\zeta_n)^j \neq 1$ for $1 \leq j < n$, so $\sigma(\zeta_n)$ is a primitive nth root of unity. This means $\sigma(\zeta_n) = \zeta_n^a$ where $(a,n)=1$. Any $\zeta \in \mu_n$ has the form ζ_n^k for some k, so

$$\sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = (\zeta_n^a)^k = (\zeta_n^k)^a = \zeta^a.$$

$\square$

The exponent a in Lemma 2.1 is well-defined modulo n, since $\zeta_n^a = \zeta_n^b \Rightarrow a \equiv b \bmod n$, so we can think of it as an element of $(\mathbf{Z}/(n))^\times$. Since it is determined by σ, we will denote it $a(\sigma)$.

Example 2.2. In $\mathrm{Gal}(\mathbf{Q}(\mu_5)/\mathbf{Q})$, there is an automorphism σ with the effect $\sigma(\zeta)=\zeta^2$ for all $\zeta \in \mu_5$. Note we can also write $\sigma(\zeta) = \zeta^7$ since $\zeta^2 = \zeta^7$ for all 5th roots of unity ζ. The exponent is not well-defined as an integer but it is well-defined as an integer mod 5 and $a(\sigma) = 2 \bmod 5$.

Theorem 2.3. *The map $\sigma \mapsto a(\sigma)$ is an injective group homomorphism* $\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbf{Z}/(n))^\times$.

Proof. Pick σ and τ in $\mathrm{Gal}(K(\mu_n)/K)$. For a primitive nth root of unity ζ_n,

$$(\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{a(\tau)}) = \sigma(\zeta_n)^{a(\tau)} = (\zeta_n^{a(\sigma)})^{a(\tau)} = \zeta_n^{a(\sigma)a(\tau)}.$$

Also $(\sigma\tau)(\zeta_n) = \zeta_n^{a(\sigma\tau)}$, so $\zeta_n^{a(\sigma\tau)} = \zeta_n^{a(\sigma)a(\tau)}$. Since ζ_n has order n, $a(\sigma\tau) \equiv a(\sigma)a(\tau) \bmod n$. This shows we have a homomorphism from $\mathrm{Gal}(K(\mu_n)/K)$ to $(\mathbf{Z}/(n))^\times$.

When σ is in the kernel, $a(\sigma) \equiv 1 \bmod n$, so $\sigma(\zeta_n) = \zeta_n$. Therefore σ is the identity on $K(\zeta_n) = K(\mu_n)$, so σ is the identity in $\mathrm{Gal}(K(\mu_n)/K)$. $\square$

Whenever we view $\mathrm{Gal}(K(\mu_n)/K)$ in $(\mathbf{Z}/(n))^\times$, it will always be understood to be by the mapping in Theorem 2.3.

Since $(\mathbf{Z}/(n))^\times$ is abelian, $\mathrm{Gal}(K(\mu_n)/K)$ is abelian: cyclotomic extensions are abelian extensions. There is no reason that the embedding of $\mathrm{Gal}(K(\mu_n)/K)$ into $(\mathbf{Z}/(n))^\times$ has to be surjective. For instance, if $K = \mathbf{R}$ and $n \geq 3$ then $K(\mu_n)/K = \mathbf{C}/\mathbf{R}$ is a quadratic extension. The nontrivial $\mathbf{R}$-automorphism of $\mathbf{C}$ is complex conjugation, whose effect on roots of unity in $\mathbf{C}$ is to invert them: $\overline{\zeta} = \zeta^{-1}$. Therefore the embedding $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) \hookrightarrow$

$(\mathbf{Z}/(n))^\times$ for $n \geq 3$ has image $\{\pm 1 \bmod n\}$, which is smaller than $(\mathbf{Z}/(n))^\times$ unless $n = 2$, 3, 4, or 6.

The following corollary will not be used later, but it illustrates how knowing the group structure of $(\mathbf{Z}/(n))^\times$ can tell us something about Galois groups of cyclotomic extensions.

Corollary 2.4. *When p is prime and K does not have characteristic p, $K(\mu_p)/K$ and $K(\mu_{p^2})/K$ are cyclic extensions. When p is prime and $r \geq 3$, $K(\mu_{p^r})/K$ is a cyclic extension if either $p \neq 2$ or if $p = 2$ and K contains a square root of -1.*

Proof. There is an embedding $\mathrm{Gal}(K(\mu_p)/K) \hookrightarrow (\mathbf{Z}/(p))^\times$ and $(\mathbf{Z}/(p))^\times$ is cyclic, so any subgroup of it is also cyclic.

When $r \geq 2$, it is a theorem of elementary number theory that $(\mathbf{Z}/(p^r))^\times$ is cyclic for odd p, so the embedded subgroup $\mathrm{Gal}(K(\mu_{p^r})/K)$ is also cyclic. But at the prime 2 something new happens: $(\mathbf{Z}/(2^r))^\times$ is *not* cyclic for $r \geq 3$, so it may or may not be true that $\mathrm{Gal}(K(\mu_{2^r})/K)$ is cyclic when $r \geq 3$. A theorem from elementary number theory says $\{a \bmod 2^r : a \equiv 1 \bmod 4\}$ is a cyclic group (with 5 as a generator, in fact). So if $i := \sqrt{-1} \in K$ then $K(\mu_{2^r})/K$ is cyclic because any element of the Galois group satisfies $\sigma(i) = i$ so the exponent $a(\sigma)$ must be 1 mod 4: $i^a = i \Rightarrow a \equiv 1 \bmod 4$. □

Remark 2.5. The composite field $K(\mu_m)K(\mu_n)$ is $K(\mu_{[m,n]})$. Indeed, both $K(\mu_m)$ and $K(\mu_n)$ lie in $K(\mu_{[m,n]})$, so their composite does too. For the reverse inclusion, a primitive root of unity of order $[m,n]$ can be obtained by multiplying suitable mth and nth roots of unity (why?), so $\mu_{[m,n]} \subset K(\mu_m)K(\mu_n)$, which implies $K(\mu_{[m,n]}) \subset K(\mu_m)K(\mu_n)$. It is natural to guess that a counterpart of $K(\mu_m)K(\mu_n) = K(\mu_{[m,n]})$ for intersections is $K(\mu_m) \cap K(\mu_n) = K(\mu_{(m,n)})$. The inclusion $\supset$ is easy, but the other inclusion is not always true! It's possible for m and n to be relatively prime and $K(\mu_m) \cap K(\mu_n)$ to be larger than $K(\mu_1) = K$. M. Emerton pointed out the following simple example. If $K = \mathbf{Q}(\sqrt{3})$ then $K(i) = \mathbf{Q}(\sqrt{3}, i) = \mathbf{Q}(\sqrt{3}, \sqrt{-3}) = K(\zeta_3)$ because $\zeta_3 = (-1 + \sqrt{-3})/2$. Since $K(\zeta_4)$ and $K(\zeta_3)$ are equal, their intersection is larger than $K(\zeta_{(4,3)}) = K$. When $K = \mathbf{Q}$, it is true that $K(\mu_m) \cap K(\mu_n) = K(\mu_{(m,n)})$, as we'll see in Example 3.4.

3. Cyclotomic extensions of the rational numbers

The embedding $\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbf{Z}/(n))^\times$ is not always surjective, so showing for a particular K that there is surjectivity for all n requires exploiting a special feature of the field K. We will prove for base field $K = \mathbf{Q}$ that there is surjectivity.

Theorem 3.1. *The embedding* $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/(n))^\times$ *is an isomorphism.*

Proof. The number of primitive nth roots of unity is $\varphi(n) = \#(\mathbf{Z}/(n))^\times$, and the size of $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ is the number of $\mathbf{Q}$-conjugates of a primitive nth root of unity. So proving that $\#\,\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) = \#(\mathbf{Z}/(n))^\times$ is the same as showing all primitive nth roots of unity over $\mathbf{Q}$ are $\mathbf{Q}$-conjugate, and that is what we will do.

Let ζ_n be a primitive nth root of unity. We want to show if $(a,n) = 1$ that ζ_n and ζ_n^a are $\mathbf{Q}$-conjugate. Since ζ_n^a only depends on $a \bmod n$, we can take $a > 0$, and in fact $a > 1$. Write $a = p_1 p_2 \cdots p_r$ as a product of primes p_i, each not dividing n (some p_i's could coincide). To show ζ_n and ζ_n^a are $\mathbf{Q}$-conjugate, it suffices to show for each prime p not dividing n that any primitive nth root of unity and its pth power are $\mathbf{Q}$-conjugate, since then the successive primitive nth roots of unity

$$\zeta_n, \quad \zeta_n^{p_1}, \quad \zeta_n^{p_1 p_2}, \quad \zeta_n^{p_1 p_2 p_3}, \ldots, \quad \zeta_n^{p_1 p_2 \cdots p_r} = \zeta_n^a$$

are all $\mathbf{Q}$-conjugate and each is a prime power of the previous one.

Let $f(X)$ be the minimal polynomial of ζ_n over $\mathbf{Q}$, where ζ_n is an arbitrary primitive nth root of unity. Assume ζ_n and ζ_n^p are not $\mathbf{Q}$-conjugate for some prime p not dividing n. We aim to get a contradiction. The $\mathbf{Q}$-conjugates of ζ_n are the roots of $f(X)$, so $f(\zeta_n^p) \neq 0$. Let $g(X)$ be the minimal polynomial of ζ_n^p in $\mathbf{Q}[X]$, so $g(X) \neq f(X)$. The polynomials $f(X)$ and $g(X)$ are in $\mathbf{Z}[X]$ since they both divide $X^n - 1$ and any monic factor of $X^n - 1$ in $\mathbf{Q}[X]$ is in $\mathbf{Z}[X]$ by Gauss' lemma.

Since $f(X)$ and $g(X)$ are different monic irreducible factors of $X^n - 1$ in $\mathbf{Q}[X]$, we have $X^n - 1 = f(X)g(X)k(X)$ for some $k(X) \in \mathbf{Q}[X]$, and by Gauss' lemma $k(X) \in \mathbf{Z}[X]$. Reducing this equation modulo p,

$$X^n - \overline{1} = \overline{f}(X)\overline{g}(X)\overline{k}(X) \tag{3.1}$$

in $\mathbf{F}_p[X]$. The polynomial $X^n - \overline{1}$ is separable in $\mathbf{F}_p[X]$ since p doesn't divide n, so $\overline{f}(X)$ and $\overline{g}(X)$ are relatively prime in $\mathbf{F}_p[X]$.

Since $g(\zeta_n^p) = 0$, $g(X^p)$ has ζ_n as a root, so $f(X)|g(X^p)$ in $\mathbf{Q}[X]$. Both $f(X)$ and $g(X^p)$ are monic in $\mathbf{Z}[X]$, so $f(X)|g(X^p)$ in $\mathbf{Z}[X]$ by comparing the division theorem for monics in $\mathbf{Z}[X]$ and $\mathbf{Q}[X]$. Hence $g(X^p) = f(X)h(X)$ for some $h(X)$ in $\mathbf{Z}[X]$. Reduce this equation modulo p and use the formula $\overline{g}(X^p) = \overline{g}(X)^p$ in $\mathbf{F}_p[X]$ to get

$$\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$$

in $\mathbf{F}_p[X]$. This implies that any irreducible factor of $\overline{f}(X)$ in $\mathbf{F}_p[X]$ is a factor of $\overline{g}(X)$, which contradicts relative primality of $\overline{f}(X)$ and $\overline{g}(X)$. □

Concretely, Theorem 3.1 says that replacing ζ_n with ζ_n^a in any rational expression for ζ_n, where a is relatively prime to n, is an automorphism of $\mathbf{Q}(\mu_n)/\mathbf{Q}$.

Remark 3.2. Our proof of Theorem 3.1 goes back to Dedekind [2]. Its appearance in van der Waerden's *Moderne Algebra* in 1930 made it the standard proof in later books. Here is another proof, due to Landau [5]. Let $f(X)$ be the minimal polynomial of ζ_n over $\mathbf{Q}$, so $f(X)$ is monic in $\mathbf{Z}[X]$. We want to show when $(a, n) = 1$ that $f(\zeta_n^a) = 0$. For any integer $k \geq 1$, we can write $f(X^k) = f(X)Q_k(X) + R_k(X)$ in $\mathbf{Z}[X]$, where $R_k(X) = 0$ or $\deg R_k < \deg f$. Since $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \deg f$, the polynomial $R_k(X)$ with degree less than $\deg f$ is determined by its value $R_k(\zeta_n) = f(\zeta_n^k)$, so $R_k(\zeta_n)$ only depends on $k \bmod n$. In particular, every $R_k(X)$ is one of $R_1(X), R_2(X), \ldots, R_n(X)$.

For any prime p, $R_p(\zeta_n) = f(\zeta_n^p) = f(\zeta_n^p) - f(\zeta_n)^p$, so $R_p(X)$ is the remainder when $f(X^p) - f(X)^p$ is divided by $f(X)$. Since $f(X)^p \equiv f(X^p) \bmod p$, we have $f(X^p) - f(X)^p \in p\mathbf{Z}[X]$, which implies (why?) $R_p(X) \in p\mathbf{Z}[X]$. Letting C be the largest absolute value of any coefficient in $R_1(X), R_2(X), \ldots, R_n(X)$, for any prime $p > C$ the polynomial $R_p(X)$ must be 0: its coefficients are smaller in absolute value then C and are divisible by p. Therefore $f(X^p) = f(X)Q_p(X)$ when $p > C$, so $f(\zeta_n^p) = 0$. This implies, by iteration, that $f(\zeta_n^k) = 0$ for any positive integer k whose prime factors all exceed C. If $(a, n) = 1$ and $a > 1$, set $k = a + n\prod_{p \leq C, (p,a)=1} p$. Then $k \equiv a \bmod n$, so $(k, n) = 1$. The two terms in the sum defining k are relatively prime, so every prime factor of k is larger than C (why?), which implies $0 = f(\zeta_n^k) = f(\zeta_n^a)$.

When K is a field such that the natural embedding $\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^\times$ is not surjective, ζ_n and ζ_n^a are not conjugate over K for some a relatively prime to n.

Example 3.3. From Galois theory for finite fields the automorphisms of the extension $\mathbf{F}_2(\mu_7)/\mathbf{F}_2$ are determined by the different 2-power iterates of ζ_7: $\zeta_7 \mapsto \zeta_7$, $\zeta_7 \mapsto \zeta_7^2$, and

$\zeta_7 \mapsto \zeta_7^4$. The next one would be $\zeta_7 \mapsto \zeta_7^8 = \zeta_7$, so we have returned to the identity. There are only 3 automorphisms of $\mathbf{F}_2(\mu_7)/\mathbf{F}_2$. In particular, ζ_7 and ζ_7^3 in characteristic 2 are both primitive 7th roots of unity but they are *not* conjugate over $\mathbf{F}_2$, since ζ_7^3 is not any of ζ_7, ζ_7^2, or ζ_7^4. Maybe this seems weird: all the nontrivial 7th roots of unity in characteristic 0 are conjugate over $\mathbf{Q}$, so "why" in characteristic 2 are the nontrivial 7th roots of unity not all conjugate? What happens is the common minimal polynomial of the nontrivial 7th roots of unity over $\mathbf{Q}$ is reducible in characteristic 2. We'll see this explicitly in Example 5.5.

By Theorem 3.1, $[\mathbf{Q}(\mu_N) : \mathbf{Q}] = \#(\mathbf{Z}/(N))^\times = \varphi(N)$ for any positive integer N. There is a formula for $\varphi(N)$ in terms of the prime factors of N:

$$\varphi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right). \tag{3.2}$$

Example 3.4. Let's use Theorem 3.1 to prove $\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) = \mathbf{Q}(\mu_{(m,n)})$; in particular, if $(m,n) = 1$ then $\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) = \mathbf{Q}$.

Since $\mathbf{Q}(\mu_d) \subset \mathbf{Q}(\mu_m)$ when $d|m$, we have $\mathbf{Q}(\mu_{(m,n)}) \subset \mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n)$. To show this containment is an equality we will show $\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n)$ and $\mathbf{Q}(\mu_{(m,n)})$ have the same degree over $\mathbf{Q}$.

For any finite Galois extensions L_1/K and L_2/K inside a common field, $[L_1L_2 : K] = [L_1 : K][L_2 : K]/[L_1 \cap L_2 : K]$. The composite field $\mathbf{Q}(\mu_m)\mathbf{Q}(\mu_n)$ is $\mathbf{Q}(\mu_{[m,n]})$ by Remark 2.5, so

$$[\mathbf{Q}(\mu_{[m,n]}) : \mathbf{Q}] = [\mathbf{Q}(\mu_m)\mathbf{Q}(\mu_n) : \mathbf{Q}] = \frac{[\mathbf{Q}(\mu_m) : \mathbf{Q}][\mathbf{Q}(\mu_n) : \mathbf{Q}]}{[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}]}.$$

Replacing each $[\mathbf{Q}(\mu_N) : \mathbf{Q}]$ with $\varphi(N)$,

$$[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi([m,n])}. \tag{3.3}$$

Using (3.2), (3.3) becomes

$$[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}] = \frac{m\prod_{p|m}(1 - 1/p) \cdot n\prod_{p|n}(1 - 1/p)}{[m,n]\prod_{p|[m,n]}(1 - 1/p)}.$$

Since $[m,n](m,n) = mn$, the ratio $mn/[m,n]$ is (m,n). The prime factors of $[m,n]$ are those dividing either m or n, so the ratio of products over primes is the product of $1 - 1/p$ over all primes dividing m and n, which means the prime factors of (m,n). Therefore

$$[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}] = (m,n) \prod_{p|(m,n)} \left(1 - \frac{1}{p}\right) = \varphi((m,n)),$$

which is $[\mathbf{Q}(\mu_{(m,n)}) : \mathbf{Q}]$, so $\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n)$ has the same degree over $\mathbf{Q}$ as $\mathbf{Q}(\mu_{(m,n)})$, hence the fields are equal since we already saw one is a subfield of the other.

Complex conjugation is an automorphism of $\mathbf{Q}(\mu_n)/\mathbf{Q}$ with order 2. Under the isomorphism of $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ with $(\mathbf{Z}/(n))^\times$, complex conjugation corresponds to $-1 \bmod n$ since $\overline{\zeta} = \zeta^{-1}$ for any root of unity ζ. The fixed field of complex conjugation on $\mathbf{Q}(\zeta_n)$ is denoted $\mathbf{Q}(\zeta_n)^+$. This field is $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ and $[\mathbf{Q}(\zeta_n) : \mathbf{Q}(\zeta_n)^+] = 2$ when $n \geq 3$. We can now easily create a field K such that $K(\mu_m) \cap K(\mu_n) \neq K$ for any pair of relatively prime integers m and n that are at least 3: use $K = \mathbf{Q}(\zeta_{mn})^+$. Since $[\mathbf{Q}(\zeta_{mn}) : K] = 2$ and

$K \subset \mathbf{R}$, $K(\zeta_m) = \mathbf{Q}(\zeta_{mn})$ and $K(\zeta_n) = \mathbf{Q}(\zeta_{mn})$. Thus $K(\zeta_m) \cap K(\zeta_n) = \mathbf{Q}(\zeta_{mn})$ is larger than K. Emerton's example in Remark 2.5 used $m = 4$ and $n = 3$: $\mathbf{Q}(\zeta_{12})^+ = \mathbf{Q}(\sqrt{3})$.

Knowing the degree of cyclotomic extensions of $\mathbf{Q}$ lets us determine which two cyclotomic fields can coincide. For example, $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\zeta_6)$ since $-\zeta_3$ has order 6. Here is the general result in this direction.

Theorem 3.5. *Let m and n be positive integers.*

(1) *The number of roots of unity in $\mathbf{Q}(\mu_m)$ is $[2, m]$.*
(2) *If $m \neq n$ then $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$ if and only if $\{m, n\} = \{k, 2k\}$ for odd k.*

Proof. 1) Our argument is adapted from [1, p. 158]. The root of unity $-\zeta_m$ is in $\mathbf{Q}(\mu_m)$ and it has order $2m$ is m is odd, and m if m is even, hence $[2, m]$ in general. Therefore $\mu_{[2,m]} \subset \mathbf{Q}(\mu_m)$.

If $\mathbf{Q}(\mu_m)$ contains an rth root of unity then $\mathbf{Q}(\mu_r) \subset \mathbf{Q}(\mu_m)$, and taking degrees over $\mathbf{Q}$ shows $\varphi(r) \leq \varphi(m)$. As $r \to \infty$, $\varphi(r) \to \infty$[1] (albeit erratically) so there is a largest r satisfying $\mu_r \subset \mathbf{Q}(\mu_m)$. Since $\mu_m\mu_r = \mu_{[m,r]}$ is in $\mathbf{Q}(\mu_m)$ we have $[m, r] \leq r$, so $[m, r] = r$. Write $r = ms$. By (3.2), for any positive integers a and b we have

$$\varphi(ab) = \frac{\varphi(a)\varphi(b)(a, b)}{\varphi((a, b))},$$

so

$$\varphi(r) = \varphi(ms) = \varphi(m)\varphi(s)\frac{(m, s)}{\varphi((m, s))} \geq \varphi(m)\varphi(s).$$

Since $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_r)$ for the maximal r, computing degrees over $\mathbf{Q}$ shows $\varphi(m) = \varphi(r) \geq \varphi(m)\varphi(s)$, so $1 \geq \varphi(s)$. Thus $\varphi(s) = 1$, so $s = 1$ or 2, so $r = m$ or $r = 2m$. This shows the number of roots of unity in $\mathbf{Q}(\mu_m)$ is either m or $2m$. If m is even then $\varphi(2m) = 2\varphi(m) > \varphi(m)$, so $r \neq 2m$. Thus when m is even the number of roots of unity in $\mathbf{Q}(\mu_m)$ is m. If m is odd then $-\zeta_m$ has order $2m$, so the number of roots of unity in $\mathbf{Q}(\mu_m)$ is $2m$. In general the number of roots of unity in $\mathbf{Q}(\mu_m)$ is $[2, m]$.

2) If $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$ and $m \neq n$ then counting roots of unity implies $[2, m] = [2, n]$. This becomes $m = [2, n]$ for even m (so $n = m/2$), and $2m = [2, n]$ for odd m (so $n = 2m$). □

Remark 3.6. Theorem 3.5 suggests two ways to parametrize cyclotomic extensions of $\mathbf{Q}$ without duplication: as $\mathbf{Q}(\mu_m)$ for m not twice an odd integer ($m \not\equiv 2 \bmod 4$) or for m equal to twice an odd integer ($m \equiv 2 \bmod 4$). In the first convention, $\mathbf{Q}(\mu_m)$ contains $2m$ roots of unity. The first convention is commonly used, as certain important results about these fields take on a simpler appearance.

Theorem 3.7. *If $E/\mathbf{Q}$ is a finite extension which contains no proper abelian extensions of $\mathbf{Q}$, $\mathrm{Gal}(E(\mu_n)/E) \cong (\mathbf{Z}/(n))^\times$ for all $n \geq 1$, or equivalently $[E(\mu_n) : E] = \varphi(n)$.*

Proof. From Galois theory, for finite extensions L/K and F/K with L/K Galois, $[LF : F] = [L : L \cap F]$. Therefore $[E(\mu_n) : E] = [\mathbf{Q}(\mu_n)E : E] = [\mathbf{Q}(\mu_n) : \mathbf{Q}(\mu_n) \cap E]$. The intersection $\mathbf{Q}(\mu_n) \cap E$ is an abelian extension of $\mathbf{Q}$ since every subfield of $\mathbf{Q}(\mu_n)$ is abelian over $\mathbf{Q}$. Therefore by hypothesis $\mathbf{Q}(\mu_n) \cap E = \mathbf{Q}$, so $[E(\mu_n) : E] = [\mathbf{Q}(\mu_n) : \mathbf{Q}] = \varphi(n)$. □

Example 3.8. For any prime $p \geq 3$ and integer $n \geq 2$, $\mathrm{Gal}(\mathbf{Q}(\sqrt[p]{2}, \mu_n)/\mathbf{Q}(\sqrt[p]{2})) \cong (\mathbf{Z}/(n))^\times$.

[1]This follows from using any bound $\varphi(r) \leq B$ to bound r from above. For any prime power p^e dividing r, $\varphi(p^e) \leq B$, so $p^{e-1}(p-1) \leq B$. Then $2^{e-1} \leq B$ and $p - 1 \leq B$, so we get upper bounds on p and on e, which gives an upper bound on r by unique factorization.

Any discussion of cyclotomic extensions of $\mathbf{Q}$ would not be complete without at least mentioning a deep theorem of Kronecker and Weber: every finite abelian extension of $\mathbf{Q}$ lies inside a cyclotomic extension of $\mathbf{Q}$. This is false if the base field is any proper finite extension of $\mathbf{Q}$: when $1 < [K : \mathbf{Q}] < \infty$ there exist finite abelian extensions of K which do not lie in a cyclotomic extension of K. This doesn't mean the finite abelian extensions of such fields K can't be described, but the means to do so are subtle. It is the subject of class field theory.

4. Cyclotomic extensions of finite fields

The explicit knowledge of Galois groups of finite fields lets us describe Galois groups of cyclotomic extensions of finite fields.

Theorem 4.1. *Let $\mathbf{F}$ be a finite field with size $q = p^r$, where p is prime. When n is not divisible by the prime p, the image of* $\mathrm{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ *in* $(\mathbf{Z}/(n))^\times$ *is* $\langle q \bmod n\rangle$. *In particular,* $[\mathbf{F}(\mu_n) : \mathbf{F}]$ *is the order of* $q \bmod n$.

Proof. From the general theory of finite fields, $\mathrm{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ is generated by the qth power map $\varphi_q \colon x \mapsto x^q$ for all x in $\mathbf{F}(\mu_n)$. The standard embedding of $\mathrm{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ into $(\mathbf{Z}/(n))^\times$ associates to φ_q the congruence class $q \bmod n$ since φ_q has the effect of raising nth roots of unity to the qth power. Since φ_q generates the Galois group, the image of the Galois group in $(\mathbf{Z}/(n))^\times$ is $\langle q \bmod n\rangle$, so the size of the Galois group is the order of q in $(\mathbf{Z}/(n))^\times$. $\square$

Example 4.2. The degree $[\mathbf{F}_p(\mu_5) : \mathbf{F}_p]$ is the order of $p \bmod 5$. So

$$[\mathbf{F}_3(\mu_5) : \mathbf{F}_3] = 4, \quad [\mathbf{F}_{11}(\mu_5) : \mathbf{F}_{11}] = 1, \quad [\mathbf{F}_{19}(\mu_5) : \mathbf{F}_{19}] = 2.$$

Remark 4.3. Using Theorem 4.1

$$\mathbf{F}_3(\mu_5) \cap \mathbf{F}_3(\mu_7) = \mathbf{F}_{3^4} \cap \mathbf{F}_{3^6} = \mathbf{F}_{3^2} \neq \mathbf{F}_3.$$

This is an explicit example where $K(\mu_m) \cap K(\mu_n) \neq K(\mu_{(m,n)})$.

For the standard embedding $\mathrm{Gal}(\mathbf{F}(\mu_n)/\mathbf{F}) \hookrightarrow (\mathbf{Z}/(n))^\times$ to be onto is equivalent to $\langle q \bmod n\rangle = (\mathbf{Z}/(n))^\times$, so in particular $(\mathbf{Z}/(n))^\times$ must be a cyclic group. The groups $(\mathbf{Z}/(n))^\times$ are usually not cyclic, so the standard embedding $\mathrm{Gal}(\mathbf{F}(\mu_n)/\mathbf{F}) \hookrightarrow (\mathbf{Z}/(n))^\times$ is usually not onto.

5. Cyclotomic polynomials

In the complex numbers, the primitive nth roots of unity are $\mathbf{Q}$-conjugate and therefore have a common minimal polynomial in $\mathbf{Q}[X]$. It is called the nth *cyclotomic polynomial* and is denoted $\Phi_n(X)$. The first few are

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1, \quad \Phi_4(X) = X^2 + 1.$$

For all $n \geq 1$, $\Phi_n(X) \in \mathbf{Z}[X]$, $\deg \Phi_n = \varphi(n)$, and $\Phi_n(X)$ is irreducible in $\mathbf{Q}[X]$. Here are some identities involving these polynomials, where p is a prime:

(1) $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$,
(2) $\Phi_n(X) = X^{\varphi(n)}\Phi_n(1/X)$ for $n \geq 2$,
(3) $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$,
(4) $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$,
(5) $\Phi_{2n}(X) = \Phi_n(-X)$ for odd n,

(6) $\Phi_{p_1^{r_1}\cdots p_k^{r_k}}(X) = \Phi_{p_1\cdots p_k}(X^{p_1^{r_1-1}\cdots p_k^{r_k-1}})$,
(7) if $(p,m)=1$ then $\Phi_{p^r m}(X) = \Phi_m(X^{p^r})/\Phi_m(X^{p^{r-1}})$,
(8) for prime powers p^r, $\Phi_{p^r}(1) = p$, while $\Phi_n(1) = 1$ for other $n \geq 2$,

Except for the first and last formulas, these identities can be checked by showing the right side has the correct degree and one correct root to be the cyclotomic polynomial on the left side. (A monic irreducible polynomial is determined by one of its roots.) The first identity can be regarded as a recursive definition of the cyclotomic polynomials, although from this identity it is not obvious in advance that the $\Phi_n(X)$'s lie in $\mathbf{Z}[X]$ (instead of just being in $\mathbf{C}[X]$, say) or that they are irreducible in $\mathbf{Q}[X]$.

Example 5.1. Since $\Phi_2(X) = X+1$, we have $\Phi_8(X) = \Phi_2(X^4) = X^4+1$. Since $\Phi_3(X) = X^2+X+1$, $\Phi_6(X) = \Phi_3(-X) = X^2-X+1$ and $\Phi_{24}(X) = \Phi_6(X^4) = \Phi_3(-X^4) = X^{12}-X^4+1$.

The sequence of cyclotomic polynomials provide an interesting example where initial data can be misleading. The first 100 cyclotomic polynomials only have coefficients 0 and ± 1, but this is not true in general! For instance, $\Phi_{105}(X)$ has a coefficient -2 for X^{41} and X^7 (the other coefficients are 0 and ± 1). Why does it take so long for a coefficient besides 0 and ± 1 to occur? Well, the fourth and fifth formulas above show the nonzero coefficients of cyclotomic polynomials are determined by the coefficients of $\Phi_n(X)$ when n is a product of distinct odd primes. The polynomial $\Phi_p(X)$ only has coefficient 1 and it can be shown [4] that $\Phi_{pq}(X)$ only has coefficients 0 and ± 1. Therefore any n with at most 2 odd prime factors only has coefficients among 0 and ± 1. The first positive integer which does not have at most 2 odd prime factors is $3 \cdot 5 \cdot 7 = 105 > 100$, which shows $\Phi_{105}(X)$ is the first cyclotomic polynomial which even has a chance to have a coefficient other than 0 and ± 1. By a theorem of Schur, if n has t odd prime factors then $\Phi_n(X)$ has coefficient $-(t-1)$ (thus predicting the coefficient of -2 in $\Phi_{105}(X)$). To produce large coefficients in $\Phi_n(X)$ we should give n a lot of odd prime factors and numbers below 100 have at most 2 odd prime factors.

Cyclotomic polynomials for prime-power n, say $n = p^r$, can be written down concretely:

$$\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{k=0}^{p-1} X^{p^{r-1}k}.$$

Theorem 5.2. *The polynomial $\Phi_{p^r}(X+1)$ is Eisenstein with respect to p.*

Proof. The constant term of $\Phi_{p^r}(X+1)$ is

$$\Phi_{p^r}(1) = \sum_{k=0}^{p-1} 1^{p^{r-1}k} = p,$$

which is divisible by p just once. To show the non-leading coefficients are all multiples of p, we reduce the coefficients mod p. Since, in $\mathbf{F}_p[X]$, $X^{p^r}-1 = (X-1)^{p^r}$ and $X^{p^{r-1}}-1 = (X-1)^{p^{r-1}}$, we have (reducing coefficients mod p)

$$\overline{\Phi}_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = (X-1)^{p^r-p^{r-1}} \text{ in } \mathbf{F}_p[X],$$

so

$$\overline{\Phi}_{p^r}(X+1) = X^{p^r-p^{r-1}} \text{ in } \mathbf{F}_p[X].$$

The degree of $\Phi_{p^r}(X+1)$ is $p^r - p^{r-1}$, so all its non-leading coefficients are 0 in $\mathbf{F}_p$, which means the coefficients as integers are multiples of p. □

Using the Eisenstein irreducibility criterion, $\Phi_{p^r}(X+1)$ is irreducible in $\mathbf{Q}[X]$, so $\Phi_{p^r}(X)$ is irreducible in $\mathbf{Q}[X]$. Therefore $[\mathbf{Q}(\mu_{p^r}) : \mathbf{Q}] = p^r - p^{r-1} = \#(\mathbf{Z}/(p^r))^\times$, so the embedding $\mathrm{Gal}(\mathbf{Q}(\mu_{p^r})/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/(p^r))^\times$ is an isomorphism. This is an alternate proof of Theorem 3.1 when n is a prime power which is much simpler than the proof we gave before.

Cyclotomic polynomials can be used to prove some results that don't appear to be about roots of unity in the first place. One such result is an elementary proof that for any $n > 1$ there are infinitely many primes $p \equiv 1 \bmod n$ [6, Cor. 2.11]. A second result is a proof of Wedderburn's theorem that all finite division rings are commutative [3, Thm. 13.1].

Since cyclotomic polynomials are in $\mathbf{Z}[X]$, let's reduce them modulo p and ask how they factor. It suffices to look at $\overline{\Phi}_n(X) = \Phi_n(X) \bmod p$ when $(p, n) = 1$ since the sixth algebraic identity above for cyclotomic polynomials, reduced modulo p, becomes

$$\Phi_{p^r m}(X) = \Phi_m(X)^{p^r - p^{r-1}} \bmod p \tag{5.1}$$

in $\mathbf{F}_p[X]$ when $(p, m) = 1$.

Theorem 5.3. *When the prime p does not divide n, the monic irreducible factors of $\overline{\Phi}_n(X) \in \mathbf{F}_p[X]$ are distinct and each has degree equal to the order of p mod n.*

Proof. Since $\Phi_n(X) | (X^n - 1)$ in $\mathbf{Z}[X]$, this divisibility relation is preserved when reducing modulo p, so $\overline{\Phi}_n(X)$ is separable in $\mathbf{F}_p[X]$ because $X^n - \overline{1}$ is separable in $\mathbf{F}_p[X]$. (Here we need $(p, n) = 1$.)

Let α be a root of $\overline{\Phi}_n(X)$ in an extension of $\mathbf{F}_p$. We will show that α inherits the expected algebraic property of being a primitive nth root of unity. Since $\overline{\Phi}_n(X) | X^n - \overline{1}$, from $\overline{\Phi}_n(\alpha) = 0$ we have $\alpha^n = 1$. If α were not of order n then it has some order m which properly divides n. Then α is a root of $X^m - \overline{1} = \prod_{d|m} \overline{\Phi}_d(X)$, so $\overline{\Phi}_d(\alpha) = 0$ for some d properly dividing n. Since $d|n$, $X^n - \overline{1}$ is divisible by $\overline{\Phi}_n(X)\overline{\Phi}_d(X)$, so α is a double root of $X^n - \overline{1}$, but $X^n - \overline{1}$ has no repeated roots. Therefore we have a contradiction, so α is a primitive nth root of unity.

Let $\pi(X)$ be an irreducible factor of $\overline{\Phi}_n(X)$ in $\mathbf{F}_p[X]$ and let α denote a root of $\pi(X)$. Then α is a primitive nth root of unity, so $\deg \pi = [\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ is the order of p mod n by Theorem 4.1. □

Example 5.4. The polynomial $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ factors over $\mathbf{F}_p$ into irreducible factors whose degrees equal the order of p mod 5. For example, $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbf{F}_3[X]$, while

$$X^4 + X^3 + X^2 + X + 1 = (X - 3)(X - 4)(X - 5)(X - 9)$$

in $\mathbf{F}_{11}[X]$ and

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + 5X + 1)(X^2 + 15X + 1)$$

in $\mathbf{F}_{19}[X]$. These are compatible with the formulas for $[\mathbf{F}_p(\mu_5) : \mathbf{F}_p]$ in Example 4.2.

Example 5.5. The polynomial $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ factors over $\mathbf{F}_p$ into irreducible factors whose degrees equal the order of p mod 7. For example, since 2 mod 7 has order 3, $\Phi_7(X)$ factors over $\mathbf{F}_2$ into a product of irreducible cubics:

$$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1)$$

in $\mathbf{F}_2[X]$. This explains what happened in Example 3.3: if ζ is a primitive 7th root of unity in characteristic 2, then it and ζ^3 are roots of the two different cubics on the right side: one has roots ζ, ζ^2, and ζ^4, while the other has roots ζ^3, $(\zeta^3)^2 = \zeta^6$, and $(\zeta^3)^4 = \zeta^5$.

Corollary 5.6. *The reduction $\overline{\Phi}_n(X)$ is irreducible in $\mathbf{F}_p[X]$ if and only if $(p, n) = 1$ and $p \bmod n$ is a generator of $(\mathbf{Z}/(n))^\times$.*

Proof. If $\overline{\Phi}_n(X)$ is irreducible in $\mathbf{F}_p[X]$ then $(p, n) = 1$ by (5.1), so Theorem 5.3 tells us the order of $p \bmod n$ is $\varphi(n)$: $p \bmod n$ generates $(\mathbf{Z}/(n))^\times$. Conversely, if $(p, n) = 1$ and $p \bmod n$ is a generator of $(\mathbf{Z}/(n))^\times$ then Theorem 5.3 tells us the irreducible factors of $\overline{\Phi}_n(X)$ in $\mathbf{F}_p[X]$ have degree $\varphi(n) = \deg(\overline{\Phi}_n(X))$, so $\overline{\Phi}_n(X)$ is irreducible. □

Thus many cyclotomic polynomials are examples of irreducible polynomials in $\mathbf{Z}[X]$ that factor modulo *every* prime: if $(\mathbf{Z}/(n))^\times$ is not a cyclic group then there is no generator for $(\mathbf{Z}/(n))^\times$, so Corollary 5.6 says there is no prime p such that $\Phi_n(X) \bmod p$ is irreducible. In other words, $\Phi_n(X) \bmod p$ factors for all primes p.

Example 5.7. The least n such that $(\mathbf{Z}/(n))^\times$ is non-cyclic is $n = 8$, and $\Phi_8(X) = X^4 + 1$. This polynomial is reducible mod p for all p. Here are some factorizations:

$$\begin{aligned}
\Phi_8(X) &\equiv (X+1)^4 \bmod 2, \\
\Phi_8(X) &\equiv (X^2+X+2)(X^2+2X+2) \bmod 3, \\
\Phi_8(X) &\equiv (X^2+2)(X^2+3) \bmod 5, \\
\Phi_8(X) &\equiv (X^2+3X+1)(X^2+4X+1) \bmod 7, \\
\Phi_8(X) &\equiv (X^2+3X+10)(X^2+8X+10) \bmod 11, \\
\Phi_8(X) &\equiv (X-2)(X-8)(X-9)(X-15) \bmod 17, \\
\Phi_8(X) &\equiv (X^2+6X+18)(X^2+13X+18) \bmod 19, \\
\Phi_8(X) &\equiv (X^2+5X+1)(X^2+18X+1) \bmod 23, \\
\Phi_8(X) &\equiv (X^2+12)(X^2+17) \bmod 29, \\
\Phi_8(X) &\equiv (X^2+8X+1)(X^2+23X+1) \bmod 31, \\
\Phi_8(X) &\equiv (X^2+6)(X^2+31) \bmod 37, \\
\Phi_8(X) &\equiv (X-3)(X-14)(X-27)(X-38) \bmod 41.
\end{aligned}$$

References

[1] Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
[2] R. Dedekind, Beweis für die Irreductibilität der Kreisteilungs-Gleichungen, *J. Reine Angew. Math.* **54** (1857), 27–30.
[3] T. Y. Lam, "A First Course in Noncommutative Rings," Springer-Verlag, New York, 1991.
[4] T. Y. Lam and K. H. Cheung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly **103** (1996), 562–564.
[5] E. Landau, Über die Irreduzibilität der Kreisteilungsgleichung, *Math. Zeitschrift* **29** (1929), 462.
[6] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 1997.