

CYCLOTOMIC EXTENSIONS

KEITH CONRAD

1. INTRODUCTION

An extension $K(\zeta_n)/K$, where ζ_n is a root of unity (of order n) is called a *cyclotomic extension* of K . We will see that such extensions have abelian Galois groups and we will look in particular at cyclotomic extensions of both \mathbf{Q} and finite fields. There are not many general methods known for constructing abelian extensions of a field; cyclotomic extensions are essentially the only construction that works for all base fields. (Other constructions are Kummer extensions, Artin-Schreier-Witt extensions, and Carlitz extensions, but these all require conditions on the base field which are not always satisfied.)

We start with an integer $n \geq 2$ such that $n \neq 0$ in K . (That is, K has characteristic 0 and $n \geq 2$ is arbitrary or K has characteristic p and n is not divisible by p .) The polynomial $T^n - 1$ is relatively prime to its derivative $nT^{n-1} \neq 0$ in $K[T]$, so $T^n - 1$ 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 n th 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 n th roots of unity in other fields?

Theorem 1.1. *The group of n th 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 $[n_1, n_2]$. Letting n be the maximal order of an element of G , it follows that the order of every element in G divides n . Thus every element of G is a root of $T^n - 1$, 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 $T^n - 1$ in a splitting field of characteristic not dividing n is a cyclic group, denoted μ_n . A generator of this group is denoted ζ_n . That is, ζ_n denotes a root of unity of exact order n . Any element of μ_n is an n th root of unity, while the generators of μ_n are called *primitive n th roots of unity*. (For comparison, -1 is a 4th root of unity but not a primitive 4th root of unity.) The order of ζ_n^a is $n/(a, n)$, so ζ_n^a is a primitive n th root of unity if and only if $(a, n) = 1$. Therefore the number of different n th 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 n th 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 n th root of unity is the same as adjoining a full set of n th roots of unity.

2. EMBEDDING THE GALOIS GROUP

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

Lemma 2.1. *For $\sigma \in \text{Gal}(K(\mu_n)/K)$ there is an $a \in \mathbf{Z}$ relatively prime to n such that $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$. That is, σ has the same effect on every element of μ_n .*

Proof. Let ζ_n be a generator of μ_n (that is, a primitive n th 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 n th 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

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

□

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

Theorem 2.2. *The map $\sigma \mapsto a(\sigma)$ is an injective group homomorphism $\text{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbf{Z}/(n))^\times$.*

Proof. Pick σ and τ in $\text{Gal}(K(\mu_n)/K)$. For a primitive n th 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 , $a(\sigma\tau) \equiv a(\sigma)a(\tau) \pmod{n}$. This shows we have a homomorphism from $\text{Gal}(K(\mu_n)/K)$ to $(\mathbf{Z}/(n))^\times$.

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

Whenever we view $\text{Gal}(K(\mu_n)/K)$ in $(\mathbf{Z}/(n))^\times$, it will always be understood to be by the mapping in Theorem 2.2.

Since $(\mathbf{Z}/(n))^\times$ is abelian, $\text{Gal}(K(\mu_n)/K)$ is abelian: cyclotomic extensions are abelian extensions. There is no reason that the embedding of $\text{Gal}(K(\mu_n)/K)$ 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 complex roots of unity is to invert them: $\bar{\zeta} = \zeta^{-1}$. Therefore the embedding $\text{Gal}(\mathbf{C}/\mathbf{R}) \hookrightarrow (\mathbf{Z}/(n))^\times$ for $n \geq 3$ via the Galois action on the n th roots of unity in \mathbf{C} has image $\{\pm 1 \pmod{n}\}$, which is smaller than $(\mathbf{Z}/(n))^\times$ when 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 2.3. *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 $\text{Gal}(K(\mu_p)/K) \hookrightarrow (\mathbf{Z}/(p))^\times$ 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 $\text{Gal}(K(\mu_{p^r})/K)$ 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 $\text{Gal}(K(\mu_{2^r})/K)$ is cyclic when $r \geq 3$. A theorem from elementary number theory says $\{a \bmod 2^r : a \equiv 1 \pmod{4}\}$ 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 $1 \pmod{4}$: $i^a = i \Rightarrow a \equiv 1 \pmod{4}$. \square

Remark 2.4. 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 m th and n th 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 is true for $K = \mathbf{Q}$, as we'll see in Section 3, but we will see a counterexample using finite K at the end of Section 4.

3. CYCLOTOMIC EXTENSIONS OF THE RATIONAL NUMBERS

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

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

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

Let ζ_n be a primitive n th root of unity with minimal polynomial $f(T)$. Its \mathbf{Q} -conjugates are the roots of $f(T)$, so we want to show every primitive n th root of unity is also a root of $f(T)$:

$$(a, n) = 1 \implies f(\zeta_n^a) = 0.$$

Since ζ_n^a only depends on $a \bmod n$, we can take $a > 0$. Moreover, since a is a product of primes, each not dividing n , it suffices to show $f(\zeta_n^p) = 0$ for any prime p not dividing n (why?).

Let $g(T)$ be the minimal polynomial of ζ_n^p in $\mathbf{Q}[T]$. We want to show $g(T) = f(T)$. Both $f(T)$ and $g(T)$ are in $\mathbf{Z}[T]$. Indeed, they both divide $T^n - 1$ and any monic factor of $T^n - 1$ in $\mathbf{Q}[T]$ is in $\mathbf{Z}[T]$ by Gauss' lemma.

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

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

Thus $\bar{f}(T)$ and $\bar{g}(T)$ have a common factor in $\mathbf{F}_p[T]$, namely any irreducible factor of $\bar{f}(T)$.

To show $g(T) = f(T)$ (so $f(\zeta_n^p) = 0$), assume otherwise. Then $f(T)$ and $g(T)$ are different monic irreducible factors of $T^n - 1$, so $T^n - 1 = f(T)g(T)k(T)$ with $k(T) \in \mathbf{Q}[T]$, and by Gauss' lemma $k(T) \in \mathbf{Z}[T]$. Reducing this modulo p ,

$$T^n - \bar{1} = \bar{f}(T)\bar{g}(T)\bar{k}(T)$$

in $\mathbf{F}_p[T]$. This is impossible: the right side has a multiple irreducible factor (any common irreducible factor of $\bar{f}(T)$ and $\bar{g}(T)$, which we know exists by the previous paragraph), but $T^n - \bar{1}$ is separable in $\mathbf{F}_p[T]$ since p doesn't divide n . Therefore $g(T) = f(T)$, which shows $f(\zeta_n^p) = 0$. \square

Concretely, Theorem 3.1 says that replacing ζ_n with ζ_n^a for any a relatively prime to n extends to an automorphism of $\mathbf{Q}(\mu_n)/\mathbf{Q}$. This is false over other fields, *e.g.*, 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 .

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 :

$$(3.1) \quad \varphi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right).$$

(Even though there are denominators in the factors of (3.1), the overall value is an integer since each p will cancel with one factor of p in N outside the product.)

Example 3.2. 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 inclusion 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 2.4, 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 $\varphi(N)$,

$$(3.2) \quad [\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi([m,n])}.$$

Using (3.1), (3.2) becomes

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

Since $m, n = mn$, 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.

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 3.3. *For $m \leq n$, $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$ if and only if $m = n$ or m is odd and $n = 2m$.*

Proof. Our argument is adapted from [1, p. 158]. When m is odd, $-\zeta_m$ has order $2m$, so $\mu_{2m} \subset \mathbf{Q}(\mu_m)$. Therefore $\mathbf{Q}(\mu_{2m}) \subset \mathbf{Q}(\mu_m)$. The reverse inclusion is clear since $\mu_m \subset \mu_{2m}$, so $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_{2m})$.

Conversely, assume $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$ with $m < n$. To show m is odd and $n = 2m$, we count the number of roots of unity in $\mathbf{Q}(\mu_m)$. (The answer need not be m , e.g., $\mathbf{Q} = \mathbf{Q}(\mu_1)$ contains 2 roots of unity rather than only 1.) If $\mu_r \subset \mathbf{Q}(\mu_m)$, then $\mathbf{Q}(\mu_r) \subset \mathbf{Q}(\mu_m)$, so taking degrees over \mathbf{Q} shows $\varphi(r) \leq \varphi(m)$. As $r \rightarrow \infty$, $\varphi(r) \rightarrow \infty$ (albeit erratically) so there is a largest r satisfying $\mu_r \subset \mathbf{Q}(\mu_m)$. Then $\mu_m \subset \mu_r$ (because $\mu_m \mu_r = \mu_{[m,r]}$), so $m|r$ and $\mathbf{Q}(\mu_r) = \mathbf{Q}(\mu_m)$. Write $r = ms$. Then

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

Since $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_r)$, 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 only option for n when $n > m$ is $n = 2m$. If m is even then $\varphi(2m) = 2\varphi(m) > \varphi(m)$, so $r \neq 2m$. Thus m is odd and $n = 2m$. \square

Remark 3.4. Theorem 3.3 suggests two ways to parametrize cyclotomic extensions of \mathbf{Q} without duplication: as $\mathbf{Q}(\mu_m)$ for m not twice an odd integer ($m \not\equiv 2 \pmod{4}$) or for m equal to twice an odd integer ($m \equiv 2 \pmod{4}$). 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 (much more important than counting the total number of roots of unity in them) take on a simpler appearance.

Theorem 3.5. *If E/\mathbf{Q} is a finite extension which contains no proper abelian extensions of \mathbf{Q} , $\text{Gal}(E(\mu_n)/E) \cong (\mathbf{Z}/(n))^\times$ 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 $[E(\mu_n) : E] = [\mathbf{Q}(\mu_n) : \mathbf{Q}] = \varphi(n)$. \square

Example 3.6. For any prime $p \geq 3$ and integer $n \geq 2$, $\text{Gal}(\mathbf{Q}(\sqrt[p]{2}, \mu_n)/\mathbf{Q}(\sqrt[p]{2})) \cong (\mathbf{Z}/(n))^\times$.

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} . It is also worth noting that this becomes 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 this 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 $\text{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ 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, $\text{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ is generated by the q th power map $\varphi_q: x \mapsto x^q$ for all x in \mathbf{F} . The standard embedding of $\text{Gal}(\mathbf{F}(\mu_n)/\mathbf{F})$ into $(\mathbf{Z}/(n))^\times$ associates to φ_q the congruence class $q \bmod n$ since φ_q has the effect of raising n th roots of unity to the q th 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 $\text{Gal}(\mathbf{F}(\mu_n)/\mathbf{F}) \hookrightarrow (\mathbf{Z}/(n))^\times$ 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 $\text{Gal}(\mathbf{F}(\mu_n)/\mathbf{F}) \hookrightarrow (\mathbf{Z}/(n))^\times$ is usually not onto.

5. CYCLOTOMIC POLYNOMIALS

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

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

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

- (1) $T^n - 1 = \prod_{d|n} \Phi_d(T)$,
- (2) $\Phi_n(T) = T^{\varphi(n)} \Phi_n(1/T)$ for $n \geq 2$,
- (3) $\Phi_p(T) = T^{p-1} + T^{p-2} + \cdots + T + 1$, $\Phi_p(T + 1)$ is Eisenstein at p ,
- (4) $\Phi_{p^r}(T) = \Phi_p(T^{p^{r-1}})$, $\Phi_{p^r}(T + 1)$ is Eisenstein at p ,
- (5) $\Phi_{2n}(T) = \Phi_n(-T)$ for odd n ,
- (6) $\Phi_{p_1^{r_1} \cdots p_k^{r_k}}(T) = \Phi_{p_1 \cdots p_k}(T^{p_1^{r_1-1} \cdots p_k^{r_k-1}})$,
- (7) if $(p, m) = 1$ then $\Phi_{p^r m}(T) = \Phi_m(T^{p^r}) / \Phi_m(T^{p^{r-1}})$,
- (8) for prime powers p^r , $\Phi_{p^r}(1) = p^r$, 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. 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 $\Phi_n(T)$'s lie in $\mathbf{Z}[T]$ (instead of just being in $\mathbf{C}[T]$, say) or that they are irreducible in $\mathbf{Q}[T]$.

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

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, $\Phi_{105}(T)$ has a coefficient -2 for T^{41} and T^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 $\Phi_n(T)$ when n is a product of distinct odd primes. The polynomial $\Phi_p(T)$ has only coefficient 1 and it can be shown [3] that $\Phi_{pq}(T)$ 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 $\Phi_{105}(T)$ 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 $\Phi_n(T)$ has coefficient $-(t - 1)$ (thus predicting the coefficient of -2 in $\Phi_{105}(T)$). The basic point is that to produce large coefficients in $\Phi_n(T)$ we should give n a lot of odd prime factors and numbers below 100 have at most 2 odd prime factors.

Since cyclotomic polynomials are in $\mathbf{Z}[T]$, let's reduce them modulo p and ask how they factor. It suffices to look at $\overline{\Phi}_n(T) = \Phi_n(T) \bmod p$ when $(p, n) = 1$ since the sixth algebraic identity above for cyclotomic polynomials, reduced modulo p , becomes

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

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

Theorem 5.2. *When the prime p does not divide n , the monic irreducible factors of $\overline{\Phi}_n(T) \in \mathbf{F}_p[T]$ are distinct and each have degree equal to the order of $p \bmod n$.*

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

Let α be a root of $\overline{\Phi}_n(T)$ in an extension of \mathbf{F}_p . We will show that α inherits the expected algebraic property of being a root of $\overline{\Phi}_n(T)$: it is a primitive n th root of unity. Since $\overline{\Phi}_n(T) | T^n - \overline{1}$ 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 $T^m - \overline{1} = \prod_{d|m} \overline{\Phi}_d(T)$, so $\overline{\Phi}_d(\alpha) = 0$ for some d properly dividing n . Since $d|n$, $T^n - \overline{1}$ is divisible by $\overline{\Phi}_n(T)\overline{\Phi}_d(T)$, α is a double root of $T^n - \overline{1}$, but $T^n - \overline{1}$ has no repeated roots. Therefore we have a contradiction, so α is a primitive n th root of unity.

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

Example 5.3. The polynomial $\Phi_5(T) = T^4 + T^3 + T^2 + T + 1$ factors over \mathbf{F}_p into irreducible factors whose degrees equal the order of $p \bmod 5$. For example, $T^4 + T^3 + T^2 + T + 1$ is irreducible in $\mathbf{F}_3[T]$, while

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

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

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

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

Corollary 5.4. *The reduction $\overline{\Phi}_n(T)$ is irreducible in $\mathbf{F}_p[T]$ if and only if $(p, n) = 1$ and $p \bmod n$ is a generator of $(\mathbf{Z}/(n))^\times$.*

Proof. If $\overline{\Phi}_n(T)$ is irreducible in $\mathbf{F}_p[T]$ then $(p, n) = 1$ by (5.1), so Theorem 5.2 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 5.2 tells us the irreducible factors of $\overline{\Phi}_n(T)$ in $\mathbf{F}_p[T]$ have degree $\varphi(n) = \deg(\overline{\Phi}_n(T))$, so $\overline{\Phi}_n(T)$ is irreducible. \square

Thus many cyclotomic polynomials give us some examples of irreducible polynomials in $\mathbf{Z}[T]$ which 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 5.4 says there is no prime p such that $\Phi_n(T) \bmod p$ is irreducible. In other words, $\Phi_n(T) \bmod p$ factors for all primes p .

Example 5.5. The least n such that $(\mathbf{Z}/(n))^\times$ is non-cyclic is $n = 8$, and $\Phi_8(T) = T^4 + 1$. Here are some factorizations:

$$\begin{aligned}\Phi_8(T) &\equiv (T + 1)^4 \pmod{2}, & \Phi_8(T) &\equiv (T^2 + T + 2)(T^2 + 2T + 2) \pmod{3}, \\ \Phi_8(T) &\equiv (T^2 + 2)(T^2 + 3) \pmod{5}.\end{aligned}$$

The first prime modulo which $\Phi_8(T)$ splits completely is 17. In every factorization the irreducible factors all have degree 1 or all have degree 2 since the degree has to divide $\#(\mathbf{Z}/(8))^\times = 4$ and is not 4.

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

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

The polynomial $\Phi_{p^r}(T)$ is irreducible over \mathbf{Q} since $\Phi_{p^r}(T + 1)$ is Eisenstein with respect to p using the above formula for $\Phi_{p^r}(T)$. Therefore $[\mathbf{Q}(\mu_{p^r}) : \mathbf{Q}] = p^{r-1}(p - 1) = \varphi(p^r) = \#(\mathbf{Z}/(p^r))^\times$, which forces the embedding $\text{Gal}(\mathbf{Q}(\mu_{p^r})/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/(p^r))^\times$ to be an isomorphism. Therefore we have obtained an alternate proof of Theorem 3.1 when n is a prime power which is much simpler than the proof we gave before. It is possible, using ideas from algebraic number theory, to extend this argument to an alternate proof of Theorem 3.1 for all n .

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 $p \equiv 1 \pmod n$ [4, Cor. 2.11]. A second result is a proof of Wedderburn's theorem that all finite division rings are commutative [2, Thm. 13.1].

REFERENCES

- [1] Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
- [2] T. Y. Lam, "A First Course in Noncommutative Rings," Springer-Verlag, New York, 1991.
- [3] T. Y. Lam and K. H. Cheung, *On the cyclotomic polynomial $\Phi_{pq}(T)$* , Amer. Math. Monthly **103** (1996), 562–564.
- [4] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 1997.