

6. RADICAL AND CYCLIC EXTENSIONS

The main purpose of this section is to look at the Galois groups of $x^n - a$. The first case to consider is $a = 1$.

Definition 6.1. *Let K be a field. An element $\omega \in K$ is said to be a **primitive n th root of unity** if*

$$\omega^n = 1,$$

but no smaller power is equal to one.

*Let L/K be a field in which $x^n - 1$ splits. The **n th cyclotomic polynomial** is defined to be*

$$\Phi_n(x) = \prod_{\omega} (x - \omega),$$

where the product runs over the primitive n th roots of unity.

Definition 6.2. *Let L/K be a Galois extension with Galois group G .*

*Let α be an element of L . We say that β is a **conjugate** of α if β lies in the same orbit as α under the natural action of G .*

Lemma 6.3. *Let L/K be a Galois extension with Galois group G .*

Suppose that $f(x) \in L[x]$ splits in L .

Then $f(x) \in K[x]$ iff the set of roots of $f(x)$ is a union of orbits of G . Furthermore $f(x)$ is irreducible iff the set of roots is an orbit of G .

In particular if $\alpha \in L$, then the minimum polynomial of α is

$$\prod_{\beta} (x - \beta),$$

where the product runs over the conjugates of α .

Proof. It suffices to prove that $f(x) \in K[x]$ is irreducible iff the set of roots of $f(x)$ is an orbit of G , that is it suffices to prove the last statement.

Suppose that

$$f(x) = \prod_{\beta} (x - \beta),$$

where the product runs over the conjugates of $\alpha \in L$. Then $f(x)$ is invariant under the action of the Galois group, since any element of the Galois group simply switches the factors and this won't change the product. But then each individual coefficient of $f(x)$ is invariant under every element of G , that is each coefficient lies in $L^G = K$. Thus $f(x) \in K[x]$.

On the other hand G acts transitively on the roots of any irreducible polynomial. □

Lemma 6.4. $\Phi_n(x)$ lies in the groundfield K .

Proof. $x^n - 1$ is certainly a polynomial with coefficients in K . Let L/K be a splitting field, with Galois group G . Now $\Phi_n(x)$ certainly divides $x^n - 1$ in L . On the other hand, if ω is a primitive n th root of unity, then the other roots of $x^n - 1$ are simply given as the n powers of ω ,

$$\omega, \omega^2, \omega^3, \dots, \omega^n.$$

Thus $L = K(\omega)$. Thus the action of an element ϕ of G is determined by its effect on ω . As ϕ must send ω to another generator, the conjugates of ω are all primitive roots of unity. Now apply 6.3. \square

Lemma 6.5.

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

Proof. Easy, since any n th root of unity is a primitive root of unity for some unique $d|n$. \square

Example 6.6. $\Phi_1(x) = x - 1$.

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

Thus $\Phi_2(x) = x + 1$ (also clear, since -1 is the unique primitive 2th root of unity).

$$x^4 - 1 = (x^2 - 1)(x^2 + 1).$$

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

Lemma 6.7. In characteristic zero, $\Phi_n(x) \in \mathbb{Z}(x)$.

Proof. We already know that $\Phi_n(x) \in \mathbb{Q}$. On the other hand, by induction

$$x^n - 1 = \Phi_n(x)f(x)$$

where both $\Phi_n(x)$ and, by induction and 6.5 $f(x)$ is integral. The result follows as in the proof of Gauss' Lemma. \square

Definition 6.8. U_n denotes the group of units in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 6.9. Let K be a field whose characteristic is coprime to n and let L/K be a splitting field for $x^n - 1$.

Then the Galois group G of L/K is naturally isomorphic to a subgroup U_n , with equality iff $\Phi_n(x)$ is irreducible over K .

Proof. First note that $x^n - 1$ is separable, as its derivative is $nx^{n-1} \neq 0$. Thus L/K is Galois. Let ω be a primitive n th root of unity.

Define a map

$$f: G \longrightarrow U_n$$

by sending σ to i , where $\sigma(\omega) = \omega^i$. This makes sense, as σ must permute the roots of $x^n - 1$, and the roots are nothing more than the powers of ω . On the other hand, ω is a generator of L/K , so that ω^i is also a generator of L/K . Thus ω^i is also a primitive root of unity. Thus i is coprime to n , so that i is a unit modulo n . Further σ is determined by its action on ω , so that f is injective.

Suppose that $f(\sigma) = i$ and $f(\tau) = j$. Then $\sigma(\omega) = \omega^i$ and $\tau(\omega) = \omega^j$. In this case

$$\begin{aligned} (\tau \circ \sigma)(\omega) &= \tau(\sigma(\omega)) \\ &= \tau(\omega^i) \\ &= (\tau(\omega))^i \\ &= (\omega^j)^i \\ &= \omega^{ij}. \end{aligned}$$

Thus $f(\tau\sigma) = ij$ and so f is a group homomorphism. The calculation above also shows that if we pick another primitive root of unity ω^i , that τ also acts on ω^i , by raising to the power j . Thus G is naturally isomorphic to a subset of U_n . Now $G = U_n$ iff we can move ω to any other primitive root of unity. But, by 6.3, this is equivalent to saying that $\Phi_m(x)$ is irreducible. \square

Here is the main Theorem

Theorem 6.10. $\Phi_n(x)$ is irreducible over \mathbb{Q} .

Proof. Suppose not. Then by Gauss' Lemma, we may write

$$\Phi_m(x) = f(x)g(x),$$

where $f(x)$ and $g(x)$ are monic integral polynomials of non-zero degree and $f(x)$ is irreducible.

Suppose that ω is a root of $f(x)$. Let p be a prime that does not divide m . I claim that ω^p is a root of $f(x)$. Suppose not. Then ω^p is a root of $g(x)$. But then ω is a root of $h(x) = g(x^p)$. Thus $f(x)$ divides $h(x)$, as $f(x)$ is the minimum polynomial of ω . Thus we have

$$h(x) = f(x)k(x),$$

Now reduce modulo p ,

$$\mathbb{Z} \longrightarrow \mathbb{F}_p.$$

We get $\bar{h}(x) = \bar{g}(x^p) = (\bar{g}(x))^p$. Let q be an irreducible factor of $\bar{f}(x) \in \mathbb{F}_p[x]$. Then q divides $\bar{g}(x)$ and so q^2 divides $\bar{f}\bar{g} = \bar{\Phi}_n(x)$. But

then $\bar{\Phi}_n(x)$ would not be separable, a contradiction as n is coprime to p .

Thus ω^p is also a root of $f(x)$. But given any primitive n th root of unity, we may write it as ω^m , for some m coprime to n . In this case

$$m = p_1, p_2, \dots, p_k.$$

Repeating the argument above, we get that ω^m is a root of $f(x)$. But then $f(x) = \Phi_m(x)$, a contradiction. \square

Example 6.11. *Let us calculate the Galois group of $x^6 - 1$ over \mathbb{Q} . By 6.10 this is isomorphic to U_6 . Of the numbers, 1, 2, 3, 4, 5, only 1 and 5 are coprime to 6. Thus the group has order two and is isomorphic to \mathbb{Z}_2 .*

Now we turn to the general problem.

Lemma 6.12. *Let L/K be a splitting field for $x^n - a \in K[x]$, $a \neq 0$.*

Then there is an intermediary field M which is a splitting field for $x^n - 1$.

Proof. If $n = mp$ and $a = b^p$, where p is the characteristic of K , then

$$x^n - a = (x^m - b)^p.$$

Thus we may as well assume that n is coprime to the characteristic. In particular $x^n - 1$ has n distinct roots $\alpha_1, \alpha_2, \dots, \alpha_n$.

Let α and β be two roots of $x^n - a$. Then α/β is a root of $x^n - 1$. Thus

$$\frac{\alpha_i}{\alpha},$$

where $i = 1 \dots n$ are the n distinct roots of $x^n - 1$. \square

Lemma 6.13. *Let K be a field in which $x^n - 1$ splits and let L/K be a Galois extension with Galois group G of degree coprime to the characteristic.*

Then L/K is the splitting field of an irreducible polynomial $x^n - a$ iff the Galois G is cyclic of order n .

Proof. Suppose that L/K is the splitting field of $x^n - a$ an irreducible polynomial. Let α be a root of $x^n - a$ and let $\omega \in K$ be a primitive n th root of unity. We have already seen that if α is a root of $x^n - a$ then the other roots are $\zeta\alpha$, where $\zeta = \omega^i$ is an n th root of unity. Define a map

$$f: G \longrightarrow \mathbb{Z}_n$$

by sending σ to i . As α generates L , the action of σ is determined by its action on α . Thus f is injective. Now the Galois group is transitive on the roots, as $x^n - a$ is irreducible. Thus f is surjective.

Suppose that σ and $\tau \in G$ and $f(\sigma) = i$ and $f(\tau) = \omega^j$. Thus $\sigma(\alpha) = \omega^i\alpha$ and $\tau(\alpha) = \omega^j\alpha$. In this case

$$\begin{aligned} (\tau \circ \sigma)(\alpha) &= \tau(\sigma(\alpha)) \\ &= \tau(\omega^i\alpha) \\ &= \omega^j\tau(\alpha) \\ &= \omega^j\omega^i\alpha \\ &= \omega^{i+j}\alpha. \end{aligned}$$

Thus f is a group homomorphism and so f is an isomorphism.

Now suppose that G is cyclic, with generator σ . Then the automorphisms

$$1, \quad \sigma, \quad \sigma^2 \dots \sigma^{n-1},$$

are distinct automorphisms and therefore independent over L . Thus

$$1 + \omega\sigma + \omega^2\sigma^2 + \dots + \omega^{n-1}\sigma^{n-1} \neq 0.$$

Thus there is an $\beta \in L$ such that

$$\alpha = \beta + \omega\sigma(\beta) + \omega^2\sigma^2(\beta) + \dots + \omega^{n-1}\sigma^{n-1}(\beta) \neq 0.$$

Note that $\sigma(\alpha) = \omega^{-1}\alpha$. Let $a = \alpha^n$. Then a is invariant under σ , whence G , so that $a \in K = L^G$. Note that G acts transitively on the roots of $x^n - a$, which are $\omega^i\alpha$, so that $x^n - a$ is irreducible. Thus α has degree n over K , so that $L = K(\alpha)$. \square

Corollary 6.14. *Let $x^p - a \in K[x]$, where p is a prime number coprime to the characteristic and suppose that $x^p - 1$ splits in K .*

Then either $x^p - a$ splits in K or $x^p - a$ is irreducible.

Proof. Let L/K be a splitting field for $x^p - a$. Then the Galois group G is a subgroup of \mathbb{Z}_p , since if α is a root of $x^p - a$, then the action of any element of G is to send α to $\omega^i\alpha$, where $i \in \mathbb{Z}_p$ as above. Thus either G is the trivial group, when $x^p - a$ splits in K or $G = \mathbb{Z}_p$, when the Galois group acts transitively on the roots of $x^p - a$ and $x^p - a$ is irreducible. \square