1 Cyclotomic extensions

Let $n \geq 1$. For any field E, define

$$\mu_n(E) = \{\rho \in E : \rho^n = 1\}.$$

The set $\mu_n(E)$ inherits a group structure from the multiplication for E.

The elements of $\mu_n(E)$ are called the *nth roots of unity* in E.

The following is a homework exercise:

Lemma. The group $\mu_n(E)$ is a finite cyclic group.

Proof. Because multiplication in E is commutative, the set $\mu_n(E)$ forms an abelian group.

Notice that if $\omega \in \mu_n(E)$ and $f(x) = x^n - 1$ then $f(\omega) = 0$.

Therefore $f(x + \omega)$ is divisible by x and $f(x) = x^n - 1$ is divisible by $x - \omega$.

Thus $|\mu_n(E)| \leq n$ since $\prod_{\omega \in \mu_n(E)}(x - \omega)$ divides $x^n - 1$.

It remains to show that any finite subgroup of $E \setminus \{0\}$ is cyclic. This is a HW exercise. □

If $|\mu_n(E)| = n$ and $\omega \in \mu_n(E)$ is a generator of $\mu_n(E)$, then we call ω a *primitive* root of unity.

Suppose $\omega \in \mu_n(E)$ is a primitive nth root of unity.

Then all the other primitive nth roots of unity are of the form ω^k, where k is coprime to $|\mu_n(E)|$.

Lemma. Let G be a nontrivial finite cyclic group. Write the group law of G multiplicatively.

Let $k = |G|$ and define $I : (\mathbb{Z}/k\mathbb{Z})^\times \to \mathrm{Aut}(G)$ to be the map given by the formula

$$I(a + k\mathbb{Z}) : \gamma \mapsto \gamma^a$$

for any $a \in \mathbb{Z}$ and $\gamma \in G$. Then I is an isomorphism.

Proof. Any automorphism of G have the form $I(a + k\mathbb{Z})$ for some $a \in \mathbb{Z}$.

We cannot have $a \in k\mathbb{Z}$ as then the automorphism would not be surjective.

On the other hand, it is clear that $I(a + k\mathbb{Z}) = I(b + k\mathbb{Z})$ if and only if $a - b \in k\mathbb{Z}$. □

Now let K be a field and suppose that $\gcd(n, \mathrm{char}(K)) = 1$.

Let L be a splitting field for the polynomial $x^n - 1 \in K[x]$.

Note that $x^n - 1$ has no repeated roots, because $\frac{d}{dx}(x^n - 1) = nx^{n-1} \neq 0$.

Thus $|\mu_n(L)| = n$ and $L \mid K$ is a Galois extension.

In particular, since $\mu_n(L) \cong \mathbb{Z}/n\mathbb{Z}$, there are $\#(\mathbb{Z}/n\mathbb{Z})^\times = \Phi(n)$ primitive nth roots of unity in L.

Here Φ is *Euler's totient function*, whose value at n is the number of $1 \leq k \leq n$ that are coprime to n.

Now let

$$\Phi_{n,K}(x) = \prod_{\text{primitive roots } \omega \in \mu_n(K)} (x - \omega).$$

Note that $\deg(\Phi_{n,K}(x)) = \Phi(n)$.

Also, note that $L \mid K$ is a simple extension, as L is generated over K by any primitive nth root in L.

Lemma. The polynomial $\Phi_{n,K}(x)$ has coefficients in K and depends only on n and K.

Proof. The coefficients of $\Phi_{n,K}(x)$ are symmetric functions in the primitive nth roots.

The primitive $n$the roots are permuted by $\mathrm{Gal}(L \mid K)$.

Hence these coefficients are invariant under $\mathrm{Gal}(L \mid K)$ and so they belong to K.

All splitting K-extensions for $x^n - 1$ are isomorphic

Thus the polynomial $\Phi_{n,K}(x) \in K[x]$ only depends on n and K. □

Proposition. The following properties hold:

(i) There is a natural injection of groups $\phi : \mathrm{Gal}(L \mid K) \hookrightarrow \mathrm{Aut}(\mu_n(L))$.
Thus, there is canonical injection of groups $\phi : \mathrm{Gal}(L \mid K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

(ii) The map ϕ is surjective if and only if $\Phi_{n,K}(x)$ is irreducible over K.

Proof. Part (i) is clear, since $\mu_n(L)$ generates L and $\mathrm{Gal}(L \mid K)$ acts on L by ring automorphisms.

For part (ii) let $\omega \in \mu_n(L)$ be a primitive nth root of unity.

Suppose that $\Phi_{n,K}(x)$ is irreducible over K.

Since $\Phi_{n,K}(x)$ annihilates ω, it must be the minimal polynomial of ω.

Hence $[L : K] \geq \Phi(n)$, and thus we have $|\mathrm{Gal}(L \mid K)| \geq \Phi(n)$.

On the other hand $|\mathrm{Gal}(L \mid K)| \leq \Phi(n)$ by part (i).

Hence $|\mathrm{Gal}(L \mid K)| = \Phi(n)$ and we may conclude from (i) that ϕ is surjective.

Now suppose that ϕ is surjective.

Then $\Phi_{n,K}(x)$ is the minimal polynomial of ω by a result last time, and this polynomial is irreducible. □

Proposition. The polynomial $\Phi_{n,\mathbb{Q}}(x)$ is irreducible and has coefficients in $\mathbb{Z}$.

Proof. This proof requires some additional background on the *Gauss content function* of a polynomial.

For the full details, see the lecture notes. □

2 Kummer extensions

Let K be a field and let n be a positive integer with $\gcd(n, \mathrm{char}(K)) = 1$.

Suppose that $x^n - 1$ splits in K

Let $a \in K$ and let $M \mid K$ be a splitting extension for the polynomial $x^n - a$. Note that $\frac{d}{dx}(x^n - a) = nx^{n-1}$.

Since $\gcd(x^n - a, nx^{n-1}) = 1$, we see that $x^n - a$ is a separable polynomial.

Hence $M \mid K$ is a Galois extension. Such an extension is called a *Kummer extension*.

Lemma. Let $\rho \in L$ be such that $\rho^n = a$.

There is a unique group homomorphism $\phi : \mathrm{Gal}(M \mid K) \to \mu_n(K)$ such that $\phi(\gamma) = \gamma(\rho)/\rho$.

This map does not depend on the choice of ρ and is injective.

Proof. We compute $(\gamma(\rho)/\rho)^n = \gamma(\rho^n)/\rho^n = a/a = 1$ and thus we indeed have $\gamma(\rho)/\rho \in \mu_n(K)$.

To see that the map does not depend on ρ, note that if $\rho_1^n = a$, then $(\rho/\rho_1)^n = a/a = 1$.

Thus there is an nth root of unity $\mu \in K$ such that $\rho_1 = \mu\rho$.

Now, using the fact that $x^n - 1$ splits in K, we may compute

$$\gamma(\rho)/\rho = \mu\gamma(\rho)/(\mu\rho) = \gamma(\mu\rho)/(\mu\rho) = \gamma(\rho_1)/\rho_1$$

so the function ϕ does not depend on ρ.

We now prove that ϕ is a group homomorphism. For any $\gamma, \lambda \in \mathrm{Gal}(M \mid K)$, we have by definition

$$\phi(\gamma\lambda) = \gamma(\lambda(\rho))/\rho$$

and

$$\phi(\gamma)\phi(\lambda) = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho)$$

and thus we have to prove that

$$\gamma(\lambda(\rho))/\rho = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho).$$

In other words, we want to show that

$$\gamma(\lambda(\rho)) = \lambda(\rho)\gamma(\rho)/\rho. \tag{*}$$

Now, again using the fact that $x^n - 1$ splits in K, we compute

$$\gamma(\lambda(\rho)/\rho) = \gamma(\lambda(\rho))/\gamma(\rho) = \lambda(\rho)/\rho. \tag{**}$$

Since equations (*) and (**) are equivalent, we have shown that ϕ is group homomorphism.

Finally, any element of $\ker(\phi)$ would fix all the roots of $x^n - a$, and hence would fix K.

Therefore the map ϕ, must be injective. □

The proof of the previous lemma also shows that a Kummer extension $M \mid K$ is a simple extension.

In fact, $M = K(\alpha)$ for any root α of $x^n - a$.

The following theorem is a kind of converse to previous result.

Let K be a field and let n be a positive integer with $\gcd(n, \mathrm{char}(K)) = 1$.

Suppose that $x^n - 1$ splits in K.

Assume that $L \mid K$ is a Galois extension and that $\mathrm{Gal}(L \mid K)$ is a cyclic group of order n.

Theorem. Let $\sigma \in \mathrm{Gal}(L \mid K)$ be a generator of $\mathrm{Gal}(L \mid K)$.

Then choose a primitive nth root of unity $\omega \in K$. Finally, for any $\alpha \in L$ let

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

Then the following properties hold:

(a) for any $\alpha \in L$, we have $\beta(\alpha)^n \in K$;

(b) if $\beta(\alpha) \neq 0$, then $L = K(\beta)$ and so L is the splitting field of $x^n - \beta(\alpha)^n$;

(c) there is an $\alpha \in L$, such that $\beta(\alpha) \neq 0$.

For the proof, we recall a general property of irreducible characters of algebras.

Let E be a field and suppose H is a group.

A *character* of H with values in E is a group homomorphism $H \to E^\times$.

Notice that this is the same thing as a character of a 1-dimensional representation of $E[H]$.

As 1-d representations are irreducible, any set of distinct characters of H is linearly independent over E.

Proof. Let $\alpha \in L$. We compute

$$\sigma(\beta(\alpha)) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \cdots + \omega^{n-1}\alpha = \omega^{n-1}\beta(\alpha) = \omega^{-1}\beta(\alpha).$$

We deduce from this that for any integer i, we have

$$\sigma^i(\beta(\alpha)) = \omega^{-i}\beta(\alpha).$$

Furthermore, we then have

$$\sigma(\beta(\alpha)^n) = \sigma(\beta(\alpha))^n = \omega^{-n}\beta(\alpha)^n = \beta(\alpha)^n$$

and thus $\beta(\alpha)^n \in K$.

Now note that any element of $\mathrm{Gal}(L \mid K)$ defines a character on $L^\times$ with values in $L^\times$.

We conclude that there is $\alpha \in L^\times$ such that $\beta(\alpha) \neq 0$.

Suppose that $\alpha \in L^\times$ and that $\beta = \beta(\alpha) \neq 0$ from now on.

Let $a = \beta^n$. Since the $\omega^{-i}\beta$ are all roots of $x^n - a$, we have shown that $x^n - a$ splits in L.

Furthermore, we have shown above that $\mathrm{Gal}(L \mid K)$ acts faithfully and transitively on the roots of $x^n - a$.

Thus, by a lemma from last lecture, we conclude that $x^n - a$ is irreducible over K.

Hence $[K(\beta) : K] = n = [L : K]$ so $K(\beta) = L$. Thus L is a splitting field for $x^n - a$. □