Student: Yu Cheng (Jade)

Math 612

Final Presentation Draft II

May 08, 2011

Cyclotomic Extension

Goal: K is a field, ζ_n is a primitive root of unity in K, of order n.

1. Show the group of nth roots of unity in a field is cyclic
2. Introduce cyclotomic extension $K(\zeta_n)/K$.
3. Show that the cyclotomic extension of a field is Galois.
4. Show that the Galois group of the cyclotomic extension is embeded into the multiplicative group of integers modulo n. The number of elements in these groups is $\varphi(n)$.

$$Gal\left(K\left(\zeta_n\right)/K\right) \quad \hookrightarrow \quad \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}.$$

5. Show that when $K = \mathbb{Q}$, this injective group homomorphism is isomorphic.

$$Gal\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right) \quad \cong \quad \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}.$$

Theorem 1: Any finite subgroup of the nonzero elements of a field, $K^{\times}$, form a cyclic group.

Proof: Let G be a subgroup of $K^{\times}$, the field formed by non-zero elements of K multiplicatively. G is an abelian group since it is embeded in a field which is commutitive. Let n be the maximal order of all elements in G. According to the general theory of abelian groups, if there are elements with orders n_1 and n_2, then there exist an element with an order of $[n_1, n_2]$, the least common multiple.

$$\begin{aligned}
& g_{max} \in G,\ |g_{max}| = n \\
& \forall g' \in G,\ |g'| = n' \\
\Rightarrow\quad & \exists g'',\ |g''| = [n', n] \\
\Rightarrow\quad & [n', n] \le n \\
\Rightarrow\quad & n' \mid n.
\end{aligned}$$

So every element in $g \in G$, g has an order that divides n, the maximal order for a group element. Since $g_{max}^n = 1_K$, every element of G is a root of $x^n - 1_K$.

$$\begin{aligned} \Rightarrow g^n - 1_K &= \left(g^{n'}\right)^{n/n'} - 1_K \\ &= \left(g_{max}^n\right)^{n/n'} - 1_K \\ &= 0. \end{aligned}$$

The polynomial $x^n - 1$ has at most n roots therefore $|G| \leq n$. At the same time, the order of a group element divides the order of the group, $n \mid |G|$. This conclusion follows Lagrange's Theorem.

$$\begin{aligned} & |G| \leq n,\ n \mid |G| \\ \Rightarrow\ & n = |G| \\ \Rightarrow\ & \exists g \in G,\ |g| = |G| \\ \Rightarrow\ & G \text{ is cyclic.} \end{aligned}$$

Example 1: For any prime p, we know that $\mathbb{Z}/p\mathbb{Z}$ forms a field. The group $(\mathbb{Z}/p\mathbb{Z})^\times$ under multiplication modulo n, contains the non-zero elements in $\mathbb{Z}/p\mathbb{Z}$. $(\mathbb{Z}/p\mathbb{Z})^\times$ forms a cyclic group. For instance $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$ is cyclic, and $\{2, 3\}$ are generators.

$\times$	$[x]^1$	$[x]^2$	$[x]^3$	$[x]^4$
1	1	1	1	1
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

Example 2: Note that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is not cyclic, since $\mathbb{Z}/p^r\mathbb{Z}$ is not a field for $r > 1$. For instance $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ is not cyclic.

$\times$	$[x]^1$	$[x]^2$	$[x]^3$	$[x]^4$
1	1	1	1	1
3	3	1	3	1
5	5	1	5	1
7	7	1	7	1

Corollary: The group of nth roots of unity in a field, denoted by μ_n, is cyclic.

Proof: According to proposition 33 in Dummit & Foote, a polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. But $x^n - 1$ does not share any common factor with nx^{n-1}. So $x^n - 1$ does not have duplicated roots in the splitting field over K. $x^n - 1$ is separable over K.

These distinct roots form a multiplicative group of size n. It is easy to show they follow the group properties (PFTS). In $\mathbb{C}$ we can write down the nth roots of unity analytically as $e^{2\pi ik/n}$ for $0 \leq k \leq n-1$ and they form a cyclic group with generator $e^{2\pi i/n}$. In general, $\left(e^{2\pi i/n}\right)^a$ are generators for $\forall a,\ (a, n) = 1$

Obviously this group is finite since the number or roots in $x^n - 1$ is n. According Theorem 1, any finite subgroup of the nonzero elements of a field, $K^{\times}$, form a cyclic group, The nth roots of unity in a field, μ_n, is cyclic.

Definition: Cyclotomic Extension

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. 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.

Theorem 2: When $n \neq 0$ in K, the cyclotomic extension $K(\zeta_n)/K$ is a Galois extension, where ζ_n is a primative nth root of unity.

Proof: Recall the several equivalent conditions for a field extension, K/F, to be Galois:

- K is a splitting field of a separable polynomial over F.
- The fixed field of $Aut\,(K/F)$ is F.
- $[K : F] = |Aut\,(K/F)|$
- K is a finite normal separable extension of F.

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 can 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.

In the proof of Theorem 1 Corollary, we've shown that $x^n - 1$ is separable over K. Also $K(\zeta_n)$ is a splitting field of $x^n - 1$. So $K(\zeta_n)$ is a splitting field of a separable polynomial over K, $K(\zeta_n)/K$ is a Galois extension according to the first condition.

Theorem 3: For $\sigma \in Gal\left(K\left(\mu_n\right)/K\right)$, there is an $a \in \mathbb{Z}$ relatively prime to n such that $\sigma\left(\zeta\right) = \zeta^a$ for all nth roots of unity ζ. This a is well-defined modulo n.

Proof: Let ζ_n be a generator of μ_n. In other words, ζ_n is a primitive nth root of unity. μ_n is a cyclic group as we've proved, so $\zeta_n^n = 1$, as well as any other primitive nth root of unity, $\left(\zeta_n^a\right)^n = 1$, where $(a, n) = 1$.

$$
\begin{array}{rrcll}
 & \sigma\left(1\right) & = & \sigma\left(\zeta_n^n\right) & \\
 & & = & \left[\sigma\left(\zeta_n\right)\right]^n & \because \sigma \text{ is an automorphism} \\
 & & = & 1 & \because \sigma \text{ fixes everything in } K \\
\Rightarrow & \left[\sigma\left(\zeta_n\right)\right]^n - 1 & = & 0 & \sigma\left(\zeta_n\right) \text{ satisfies } x^n - 1 \\
\Rightarrow & \sigma\left(\zeta_n\right) & = & \zeta_n^a & \text{where } (a, n) = 1.
\end{array}
$$

This a satisfies the condition to be proven.

$$
\begin{array}{rcll}
\sigma\left(\zeta\right) & = & \sigma\left(\zeta_n^k\right) & \text{for some } k \because \zeta_n \text{ is a generator in } \mu_n \\
 & = & \left[\sigma\left(\zeta_n\right)\right]^k & \because \sigma \text{ is an automorphism} \\
 & = & \left(\zeta_n^a\right)^k & \text{as we've shown above} \\
 & = & \left(\zeta_n^k\right)^a & \because \sigma \text{ is an automorphism} \\
 & = & \zeta^a & \because \zeta = \zeta_n^k.
\end{array}
$$

We can think of a as an element in $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$, then this operation becomes a map from $Gal\left(K\left(\mu_n\right)/K\right)$ to $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$, $\theta : \sigma \mapsto a$.

Theorem 4: The map $\theta : Gal\left(K\left(\mu_n\right)/K\right) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ is an injective group homomorphism, where θ is defined by $\theta : \sigma \mapsto a$ such that $\sigma\left(\zeta\right) = \zeta^a$.

Proof: First we will show this map is a group *homomorphism*. Let $\sigma_1, \sigma_2 \in Gal\left(K\left(\mu_n\right)/K\right)$, ζ_n be a primitive nth root of unity. $\sigma_1\left(\zeta_n\right) = \zeta_n^a$ and $\sigma_2\left(\zeta_n\right) = \zeta_n^b$ where $a, b \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$.

$$
\begin{array}{rrcll}
 & \sigma_1 \circ \sigma_2\left(\zeta_n\right) & = & \sigma_1\left(\zeta_n^b\right) & \sigma_2\left(\zeta_n\right) = \zeta_n^b \\
 & & = & \left[\sigma_1\left(\zeta_n\right)\right]^b & \because \sigma' \text{s are automorphisms} \\
 & & = & \left(\zeta_n^a\right)^b & \sigma_1\left(\zeta_n\right) = \zeta_n^a \\
 & & = & \left(\zeta_n\right)^{a \cdot b} & \because \sigma' \text{s are automorphisms} \\
\Rightarrow & \theta\left(\sigma_1 \circ \sigma_2\right) & = & a \cdot b & \\
 & & = & \theta\left(\sigma_1\right) \cdot \theta\left(\sigma_2\right). &
\end{array}
$$

Now we want to show this group homomorphism is ***injective***. We will prove this by showing that the kernel of this group homomorphism is trival. Let $\theta(\sigma) = 1$, hence $\sigma(\zeta) = \zeta$, so σ is the identity map of $K(\zeta_n) = K(\mu_n)$. Basically, σ fixes everything in K and now it needs to fix every nth root of unity. Therefore σ is the identity map in $Gal(K(\mu_n)/K)$. $K(\mu_n)/K$ extensions have abelian Galois groups.

$$Gal(K(\zeta_n)/K) \quad \hookrightarrow \quad (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Corollary: The group homomorphism defined above is an isomorphism when $K = \mathbb{Q}$.

$$Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \quad \cong \quad (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Proof: We need to show this group homomorphism is ***surjective***. In other words, since we've shown the map is injective, we now want to show the size of two groups are the same. By definition, $\left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right| = \varphi(n)$, the number of integers that are relatively prime to n. We want to show that $|Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})|$is also $\varphi(n)$.

According to Theorem 2, $Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})$ is a Galois extension we have

$$[\mathbb{Q}(\mu_n) : \mathbb{Q}] \quad = \quad |Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})|.$$

So we need to show the degree of this field extension is $\varphi(n)$. Recall that the degree of a field extension, $[K(\alpha) : K]$ is the degree of $K(\alpha)$ as a vector space over K and therefore the degree of the field extension is equal to the degree of the minimum polynomial of α over K. So we want to show the degree of the minimum polynomial of ζ_n is $\varphi(n)$.

We've proved that $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x)$ is irriducible over $\mathbb{Q}$. This tells us $deg(\Phi_n(x)) = deg(m_{\zeta_n,n}(x))$. The minimal polynomial of every primitive nth root of unity is in fact the cyclotomic polynomial, $\Phi_n(x)$. By definition, $deg(\Phi_n(x)) = \varphi(n)$. We are done.

In summary, we derived the conclusion of θ being isomorphic through the following steps.

$$\begin{aligned}
|Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})| &= [\mathbb{Q}(\mu_n) : \mathbb{Q}] && \text{cyclotomic extension is Galois} \\
&= deg(m_{\zeta_n,n}(x)) && \text{proposition of extension field} \\
&= deg(\Phi_n(x)) && \text{follow the fact that } \Phi_n(x) \text{ is irreducible over } \mathbb{Q} \\
&= \varphi(n) && \text{proposition of cyclotomic polynomial } \Phi_n(x) \\
&= \left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right| && \text{proposition of the group of nonzero elements from a field}
\end{aligned}$$

Therefore, θ is a group isormorphism, and we've shown $Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Theorem 5: Let F be a finite field with size $q = p^r$, where p is a prime. When n is not divisible by the prime p, the image of $Gal(F(\mu_n)/F)$ in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is $\langle q \bmod n\rangle$. In particular $[F(\mu_n) : F]$ is the order of q mod n.

Proof: PFTS

Summary: 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 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.