Advanced Algebra I

CYCLIC EXTENSION

Definition 0.1. *We say that an extension is cyclic (resp. abelian) if it's algebraic Galois and* $\mathrm{Gal}_{F/K}$ *is cyclic (resp. abelian). An cyclic extension of order* n *is an cyclic extension whose Galois group is isomorphic to* $\mathbb{Z}_n$.

The following theorem characterize cyclic extension except some exceptional case.

Theorem 0.2. *Suppose that* $char(K) = 0$ *or* $char(K) = p \nmid n$. *Suppose furthermore that there is a primitive* n*-th root of unity in* K*, say* ζ. *Then* F/K *is a cyclic of order* n *if and only if* $F = K(u)$ *where* u *is a root of irreducible polynomial* $x^n - a \in K[x]$.

Before we get into the proof. Let's consider the "difference" between u and $\sigma(u)$ for $\sigma \in \mathrm{Gal}_{F/K}$. Let F/K be a finite Galois extension. Then in this circumstance, norm and trace (which we will define more generally later) are nothing but $N_{F/K}(u) := \prod_{\sigma \in \mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K} := \sum_{\sigma \in \mathrm{Gal}_{F/K}} \sigma u$. It's easy to see that $T(u - \sigma(u)) = 0$ and $N(u/\sigma(u)) = 1$. The follows lemma says that the converse is also true for cyclic extension, which will play the central role in the study of cyclic extension.

Lemma 0.3. *Let* F/K *be an cyclic extension with* σ *the generator of the Galois group.*

(1) *If* $T_{F/K}(u) = 0$*, then there exists an* $v \in F$ *such that* $u = v - \sigma(v)$.
(2) *If* $N_{F/K}(u) = 1$*, then there exists an* $v \in F$ *such that* $u = v/\sigma(v)$.

Proof of the Theorem. Let u be a root of $x^n - a$, then all the roots are $u\zeta^i$ for $i = 0, ..., n-1$. Since $\zeta \in K$. It's clear that $F = K(\zeta)$ is a cyclic extension over K.

Conversely, suppose that F/K is a cyclic extension of order n. Since there is a primitive n-th root $\zeta \in K$, one has $N(\zeta) = \zeta^n = 1$. By the Lemma, there exist an v such that $\zeta = v/\sigma(v)$. Let $u = v^{-1}$, then $\sigma(u) = \zeta u$. Hence $\sigma(u^n) = u^n \in K$. Therefore u satisfies $x^n - a \in K[x]$ for some $a \in K$.

Moreover, for $u\zeta^i$ and $u\zeta^j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^n - a$. One the other hand, $p(x)$ has n distinct roots $u\zeta^i$ for $i = 0, ..., n-1$. It follows that $p(x) = x^n - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. $\square$

Theorem 0.4. *Suppose that $char(K) = p \neq 0$. Then F/K is a cyclic extension of order n if and only if $F = K(u)$, where u is a root of an irreducible polynomial $x^p - x - a \in K[x]$.*

Proof. The proof is parallel to the previous one.

Let u be a root of $x^p - x - a$, then all the roots are $u + i$ for $i = 0, ..., p-1$. It's clear that $F = K(\zeta)$ is a cyclic extension over K with Galois group generated by σ such that $\sigma(u) = u + 1$.

Conversely, suppose that F/K is a cyclic extension of order n. One has $T(1) = p = 0$. By the Lemma, there exist an v such that $1 = v - \sigma(v)$. Let $u = -v$, then $\sigma(u) = u + 1$. Hence $\sigma(u^p) = u^p + 1$ and $\sigma(u^p - u) = u^p - u$. Therefore u satisfies $x^p - x - a \in K[x]$ for some $a \in K$.

Moreover, for $u + i$ and $u + j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^p - x - a$. One the other hand, $p(x)$ has p distinct roots $u + i$ for $i = 0, ..., p-1$. It follows that $p(x) = x^p - x - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. $\square$

It remains to define norm and trace, and prove the main lemma.

We first recall something about separable degree.

Proposition 0.5. *If F/K is a finite extension, then $[F : K]_s \big| [F : K]$. Moreover, $[F : K]/[F : K]_s = p^n$ for some n.*

Proof. Let $S := \{u \in F | u \text{ is separable over } K\}$. One can prove that S is a field separable over K. We claim that F is "purely inseparable" over S, i.e. for all $u \in F$, $u^{p^n} \in S$ for some n, or equivalently, minimal poly of $u \in F$ is of the form $x^{p^n} - a$.

To see this, let $p(x)$ be the minimal polynomial of $u \in F - S$ over S. Then $p'(x) = 0$ otherwise, u is separable over S, hence separable over K, u is indeed in S. We can write $p(x) = f(x^p)$. If $u^p \in S$, we are done. If $u^p \ni S$, then the minimal polynomial of u^p is $f(x)$. One infers that $f'(x) = 0$. By repeating this process, we have proved the claim.

If follows that $[F : S] = p^n$ for some n since F is finitely generated over S.

It remains to check that for every K-embedding $\sigma : S \to \overline{K}$, there is a unique extension to an K-embedding $\bar{\sigma} : F \to \overline{K}$. By extension theorem, there are such extensions. To see the uniqueness, suppose that we have K-embeddings $\tau_1, \tau_2 : F \to \overline{K}$ extending σ. For all $u \in F$, $u^{p^n} \in S$ for some n. One has that

$$\tau_1(u)^{p^n} = \tau_1(u^{p^n}) = \tau_2(u^{p^n}) = \tau_2(u)^{p^n}.$$

Since $char(K) = p$, one has then $\tau_1(u) = \tau_2(u)$. Thus $\tau_1 = \tau_2$. It follows that $[F : K]_s = [S : K]_s$

Combining all theses, we have

$$[F : K]_s = [S : K]_s = [S : K] \big| [F : K].$$

We define the inseparable degree as $[F:K]_i := [F:S]$. Then we have $[F:K]_i = p^n$ for some n. $\square$

Definition 0.6. *Let $[F:K]$ be a finite extension. Let Σ be the set of K-embeddings of F into $\overline{K}$. For any $u \in F$, we define the norm, denoted*

$$N_{F/K}(u) := (\prod_{\sigma\in\Sigma} \sigma(u))^{[F:K]_i}.$$

Similarly, we define the trace as

$$T_{F/K}(u) := (\Sigma_{\sigma\in\Sigma}\sigma(u))[F:K]_i.$$

Example 0.7. *If F/K is finite Galois extension, then the set of all K-embeddings of F is nothing but the Galois group of F (since F is normal). And $[F:K]_i = 1$ since F/K is separable. Therefore, $N_{F/K}(u) = \prod_{\sigma\in \mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K}(u) = \sum_{\sigma\in \mathrm{Gal}_{F/K}} \sigma(u)$*

Here are some basic properties of norma and trace

Proposition 0.8.
1. *$N(u), T(u) \in K$. More precisely, let $p(x) = x^n + a_1x^{n-1} + ... + a_n$ be the minimal polynomial of u over K. Then $N(u) = ((-1)^n a_n)^{[F:K(u)]}$ and $T(u) = ((-1)a_1)[F:K(u)]$.*
2. *If $u \in K$, then $N(u) = u^{[F:K]}, T(u) = [F:K]u$.*
3. *$N(uv) = N(u)N(v)$ and $T(u+v) = T(u) + T(v)$. Therefore, $N_{F/K} : F^* \to K^*$ is a multiplicative group homomorphism and $T_{F/K} : F \to K$ is an additive group homomorphism.*
4. *If $K \subset E \subset F$, then $N_{F/K}(u) = N_{E/K}(N_{F/E}(u))$, and $T_{F/K}(u) = T_{E/K}(T_{F/E}(u))$.*

Proof. $(2), (3)$ follows directly from the definition. To see (4), let $I := \{\sigma : E \to \overline{K} | \sigma_{|K} = \mathbf{1}_K\}$ be a set of K-embeddings of E . For each σ , we fix an extension $\bar{\sigma} : F \to \overline{K}$. Let $J := \{\tau : F \to \overline{K} | \tau_{|E} = \mathbf{1}_E\}$ be the a of E-embeddings of F. If follows that $\{\bar{\sigma}_i\tau_j\}_{i\in I, j\in J}$ is the set of K-embeddings of F. Then

$$N_{F/K}(u) = (\prod_{I,J} \bar{\sigma}_i\tau_j(u))^{[F:K]_i} = (\prod_{I} \bar{\sigma}_i(N_{F/E}(u)))^{[E:K]_i} = N_{E/K}(N_{F/E}(u)).$$

And the proof for trace is similar.

To prove (1), we first assume that u is separable over K. Then $K(u) \subset S$ and every K-embedding of $K(u)$ has $[S:K(u)]$ extensions. Let $u = u_1, ..., u_r$ be the roots of its minimal polynomial. Then one has

$$\prod \sigma(u) = (\prod_{i=1}^{r} u_i)^{[S:K(u)]} = ((-1)^r a_0)^{[S:K(u)]}.$$

And the statement follows easily.

we consider $E = K(u)$. Let $S_E := E \cap S$, then E is purely inseparable over S_E, in particular, $v := u^{p^n} \in S_E$ for some n. let $f(x)$ be the minimal polynomial of v over K, then we have

$$p(x) = f(x^{p^n}) = f(x)^{p^n}.$$

Since v is separable over K, the statement holds for v. Since norm is a homomorphism, the statement holds for u as well. $\square$

Proof of the main Lemma. We only prove that $T(u) = 0$ implies $u = v - \sigma(v)$. The other implication is easy.

Step 1. Find an element $z \in F$ with $T(z) \neq 0$. This is an immediate consequence of independency of automorphism.

Step 2. We normalize it to get $w \in F$ with $T(w) = 1$. In fact, we take $w := \frac{z}{T(z)}$.

Step 3. Let

$$v = uw + (u + \sigma(u))\sigma(w) + ... + (u + \sigma(u) + ... + \sigma^{n-2}(u))\sigma^{n-2}(w).$$

Then we are done.

For the norm, if $N(u) = 1$, then $u \neq 0$. Take

$$v = uy + u\sigma(u)\sigma(y) + ... + u\sigma(u)...\sigma^{n-1}(u)\sigma^{n-1}(y).$$

By independency of automorphism, there exist a y such that v is non-zero. One checks that $u^{-1}v = \sigma(v)$. We are done.

$\square$