Advanced Algebra I

Galois groups of polynomials, cyclotomic extension

We first recall something about separable extension. The main purpose is to prove the following proposition we used in the previous section.

Proposition 0.1. *Suppose that $F = K(S)$ such that each elements of S is separable over K, then F/K is separable.*

To start with, let $f(x)$ be an irreducible polynomial in $K[x]$ and $f'(x)$ be its derivative (formally). More precisely, if $f(x) = sum_{i=0}^{n} a_i x^i$, then $f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}$. One has the following equivalence:

(1) $f(x)$ is separable, i.e. no multiple roots in $\overline{K}$.
(2) $(f(x), f'(x)) = 1 \in \overline{K}[x]$.
(3) $(f(x), f'(x)) = 1 \in K[x]$.
(4) $f'(x) = 0$.

Therefore, the only possibility to have non-separable polynomial is $char(K) = p$ and $f(x) = g(x^p)$.

Given an element u algebraic over K, one can define the separable degree to be the number of distinct roots of minimal polynomial. This notion can be extended to a general setting:

Definition 0.2. *Let F/K be an extension. Fix an embedding $\sigma : K \to L = \overline{L}$. We define the separable degree of F/K, denoted $[F : K]_s$, to be the cardinality of*

$$S_\sigma := \{\tau : F \to L | \tau_{|K} = \sigma\}.$$

One can check that $[F : K]_s$ is independent of σ and L. Hence the definition is well-defined. Moreover, if $F = K(u)$ for u algebraic over K, then $[F : K]_s = [K(u) : K]_s$ is the number of distinct roots of the minimal polynomial $p(x)$ of u. (By considering K-embedding $\tau : K(u) \to \overline{K}$, $\tau(u)$ must be a root of $p(x)$ and τ is determined by $\tau(u)$).

Proposition 0.3. *If $K \subset E \subset F$, then $[F : K]_s = [F : E]_s [E : K]_s$. Moreover, if F/K is finite, then $[F : K]_s \leq [F : K]$.*

Proof. Fix an embedding $\sigma : K \to L$, there are extensions $\{\sigma_i\}_{i \in I} : E \to L$ with $|I| = [E : K]_s$. And for a fix σ_i, there are extensions $\{\sigma_{i,j}\}_{j \in J} : F \to L$ with $|J| = [F : K]_s$. Thus

$$[F : K]_s = |I| \cdot |J| = [F : E]_s [E : K]_s.$$

If F/K is finite, then $F = K(u_1, ..., u_t)$. It's clear that for all i, $[K(u_1, ..., u_i) : K(u_1, ..., u_{i-1})]_s \leq [K(u_1, ..., u_i) : K(u_1, ..., u_{i-1})]$ since the number of distinct root is less or equal than degree of minimal polynomial. $\square$

Then we have the following useful criterion:

Proposition 0.4. *If F/K is finite, then F/K is separable if and only if $[F:K]_s = [F:K]$.*

Proof. Write $F = K(u_1, ..., u_t)$. If F/K is separable, then for all i, $[K(u_1, ..., u_i)$ is separable over $K(u_1, ..., u_{i-1})]$. Then we have for all i

$$[K(u_1, ..., u_i) : K(u_1, ..., u_{i-1}]_s = [K(u_1, ..., u_i) : K(u_1, ..., u_{i-1}].$$

It follows that $[F:K]_s = [F:K]$.

On the other hand, for any $u \in F$, we have

$$[F:K]_s = [F:K(u)]_s[K(u):K]_s \leq [F:K(u)][K(u):K] = [F:K].$$

Hence all the above are in fact equality, therefore $[K(u):K]_s = [K(u):K]$ and u is separable over K. □

Proof of the Proposition 1. For any $u \in K(S)$, we may assume that $u \in K(u_1, ..., u_t)$ for some $u_1, ..., u_t \in S$ separable over K. It's obvious that $K(u_1, ..., u_i)$ separable over $K(u_1, ..., u_{i-1})$ for all i. Thus one has that $[K(u_1, ..., u_t) : K]_s = [K(u_1, ..., u_t) : K]$ and thus $K(u_1, ..., u_t)$ is separable over K. Thus so is u. □

We now study the Galois groups of polynomials. First of all, for a given $f(x) \in K[x]$, we define the Galois group of $f(x)$ over K, denoted G_f, to be the Galois group of a splitting field F over K.

Theorem 0.5. (1) *If $deg(f(x)) = n$, then $G_f \hookrightarrow S_n$.*
(2) *If $f(x)$ is irreducible and separable of degree n, then G_f is transitive in S_n and $n \big| |G_f|$.*

Proof. For every $\sigma \in G_f$, σ induces a permutation on roots of $f(x)$. Hence the mapping by sending σ to the corresponding permutation gives the required embedding.

Let u_i, u_j be two distinct roots of $f(x)$, then we have an isomorphism $\sigma : K(u_i) \to K(u_j)$ such that $\sigma(u_i) = u_j$. Since the splitting field F is normal, thus σ can be extended to an automorphism of F. Therefore, we have find a K-automorphism sending u_i to u_j for any i, j. Hence it's transitive in S_n.

Moreover, one sees that $[G_f : K(u_i)'] = [K(u_i) : K] = n$. Thus $n \big| |G_f|$. □

Example 0.6. *The only transitive subgroups in S_3 are S_3 and A_3.*

The only transitive subgroups of order divisible by 4 in S_4 are $S_4, A_4, \cong D_4, V, \cong \mathbb{Z}_4$.

For a given polynomial $f(x)$ with roots $u_1, ..., u_n$. one can define

$$\Delta := \prod_{i<j}(u_i - u_j).$$

Then Δ is preserved by even permutations, i.e. $G_f \cap A_n$. Then $D := \Delta^2$ is preserved by all G_f. One can see that D is in K. D is called the *discriminant* of $f(x)$. Assume that f is irreducible and separable, then F is Galois over K. One can see that $(G_f \cap A_n)' = K(\Delta)$ if $char(K) \neq 2$. Applying this to degree 3, we have:

Theorem 0.7. *Let $f(x)$ be an irreducible separable polynomial of degree 3 over K with $char(K) \neq 2$,then $G_f = A_3$ if and only if D is a perfect square in K and $G_f = S_3$ if and only if D is not a perfect square.*

We also remark that D is computable. For example, if $f(x) = x^3 + px + q$, then $D = -4p^2 - 27q^3$.

The story for degree 4 are similar but more delicate. Let $f(x)$ be an irreducible separable polynomial of degree 4. Let $u_1, ..., u_4$ be the roots of $f(x)$. And let $F = K(u_1, ..., u_4)$ be the splitting field, which is Galois over K. Let $\alpha := u_1u_2 + u_3u_4, \beta := u_1u_3 + u_2u_4, \gamma := u_1u_4 + u_2u_3$. It's clear that they are all distinct since $f(x)$ is separable. We can consider an intermediate field $E := K(\alpha, \beta, \gamma)$. Let $g(x) := (x-\alpha)(x-\beta)(x-\gamma)$. One sees that $g(x) \in K[x]$ and E is s splitting field of $g(x)$. One can check directly that $E' = G_f \cap V$. Thus we have:

Theorem 0.8. *Keep the notation as above. Let $m := [E : K]$. Then*

1. $m = 6 \Leftrightarrow G_f = S_4$.
2. $m = 3 \Leftrightarrow G_f = A_4$.
3. $m = 1 \Leftrightarrow G_f = V$.
4. $m = 2$, *$f(x)$ is irreducible in $E[x]$* $\Leftrightarrow G_f \cong D_4$.
5. $m = 2$, *$f(x)$ is reducible in $E[x]$* $\Leftrightarrow G_f \cong \mathbb{Z}_4$.

Proof. As we have seen that the only transitive subgroup with order divisible by 4 are $S_4, A_4, V_4, \cong D_4, \cong \mathbb{Z}_4$. Hence the first three equivalence are trivial.

If $m = 2$ then $G_f \cong D_4$ or $G_f \cong \mathbb{Z}_4$. If $f(x)$ is irreducible in $E[x]$, then $f(x)$ is the minimal polynomial of u_1. Hence $[F : E] = [F : E(u_1)][E(u_1) : E] = [F : E(u_1)]4$. In particular, $4 \big| [F : E] = |G_f \cap V|$. Therefore, $G_f \cong D_4$.

On the other hand, if $f(x)$ is reducible, then $f(x)$ can not have factor of degree 3 since $3 \not| |G_f \cap V|$. $\square$

We now start the study of cyclotomic extension.

Definition 0.9. *A cyclotomic extension of order n over K is a splitting field of $x^n - 1$.*

Remark 0.10. *If $char(K) = p$ and $n = p^r m$, then $x^n - 1 = (x^m - 1)^{p^r}$. Hence we may assume that either $char(K) = 0$ or $char(K) \nmid p$ in the study of cyclotomic extension.*

The main theorem is the following

Theorem 0.11. *Keep the notation as above. Then we have*

1. *$F = K(\zeta)$, where ζ is a primitive n-th root of unity.*
2. *F/K is Galois whose Galois group $\mathrm{Gal}_{F/K}$ can be identified as a subgroup of $\mathbb{Z}_n^*$.*
3. *If n is prime, then $\mathrm{Gal}_{F/K}$ is cyclic.*

Proof. Let $S := \{u \in F | u^n = 1\}$. And let n' be the maximal order of elements in S. It's clear that S is an abelian multiplicative group. Therefore, it's easy to see that order of elements in S divides n'. It follows that $u^{n'} = 1$ for all $u \in S$.

Since we assume that $(n, chat(K)) = 1$, therefore $x^n - 1$ is separable, $|S| = n$. One sees that $n = n'$, therefore, there are elements of order n in S, denoted ζ. It follows that $F = K(S) = K(\zeta)$.

For any $\sigma \in \mathrm{Gal}_{F/K}$, $\sigma(\zeta) \in S$. Hence $\sigma\zeta = \zeta^i$ for some i. Therefore, we have a natural map $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n$ by $\phi(\sigma) = i$ if $\sigma(\zeta) = \zeta^i$. Since σ are automorphism, one has image in $\mathbb{Z}_n^*$. It's easy to see that $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n^*$ is an injective group homomorphism.

Lastly, if n is prime, then $\mathbb{Z}_p^*$ is cyclic. Hence every subgroup is cyclic. $\square$