Lecture 9 Cyclotomic field extensions over $\mathbb{Q}$

We say that an algebraic field extension E/K is *separable* if $\forall\, \alpha \in E$ the minimum polynomial $p_{\alpha/K}(X) \in K[X]$ is s.t.

$$p_{\alpha/K}(X) = \prod_{i=1}^{d} (X - \alpha_i),$$

over the splitting field of $p_{\alpha/K}(X)$, with $\alpha_1, \dots, \alpha_d$ distinct.
We say that E/K is *normal* if E is the splitting field of a family of polinomials over K; if E/K is both normal and separable we say E/K is *Galois*

and say that

$$\mathrm{Aut}(E/K) := \{ g \in \mathrm{Aut}(E) \mid g|_K = id_K \}$$

is the *Galois group* of E/K and denote it $\mathrm{Gal}(E/K)$.

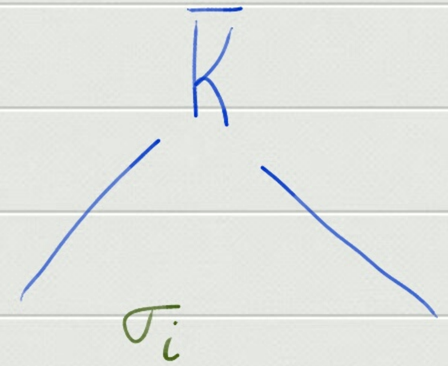
<u>Thm</u> If E/K is finite Galois field ext'n then

$$|\mathrm{Gal}(E/K)| = [E:K]$$

Proof

Assumming the primitive element theorem, the separability of E/K implies that there exists $\alpha \in E$ s.t. $E = K(\alpha)$. Fix an algebraic closure of $\bar{K}$ of K

so that the roots $\alpha_1, \ldots, \alpha_d \in \overline{K}$. For each of these roots we have a diagram



$(\alpha_1 := \alpha)$

$$K[\alpha] = K(\alpha) \xrightarrow{\sim} K(\alpha_i) = K[\alpha_i]$$

$$a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1} \longmapsto a_0 + a_1\alpha_i + \ldots + a_{d-1}\alpha_i^{d-1}$$

The normality of E/K implies that $\forall\, i \in \{1, \dots, d\} : \sigma_i \in \mathrm{Aut}(E/K)$.
Conversely, each $\sigma \in \mathrm{Aut}(E/K)$ is of the form $\sigma = \sigma_i$, where
$\alpha_i = \sigma(\alpha)$. Hence

$$|\mathrm{Aut}(E/K)| = |\{\alpha_1, \dots, \alpha_d\}|.$$

But E/K is separable. Therefore

$$|\mathrm{Aut}(E/K)| = d = [E:K],$$

and the thm follows $\square$

For $n \in \mathbb{Z}_{\geq 1}$ let $\zeta_n := e^{2\pi i/n}$ and $\mu_n := \zeta_n^{\mathbb{Z}}$. We have

$$E = \mathbb{Q}(\zeta_n)$$

$$K = \mathbb{Q}$$

$$\begin{array}{ccc} \mathrm{Aut}(E/K) & \xrightarrow{\kappa} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & \overline{a}_\sigma \end{array}$$

as $\sigma \in \mathrm{Aut}(E/K)$ implies that $\sigma(\zeta_n)$ is another generator of μ_n, thus

$$\sigma(\zeta_n) = \zeta_n^{a_\sigma},$$

where $\overline{a}_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$. Clearly κ is injective.

Thm We have a group isomorphism

$$\begin{array}{ccc} \mathrm{Gal}(E/\mathbb{Q}) & \xrightarrow{K} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & \tilde{a}_\sigma \end{array}$$

Proof — after van der Waerden

It suffices to show that

$$\deg P_{\zeta/\mathbb{Q}}(X) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(n)$$

where ζ is any primitive n-th root of unity over $\mathbb{Q}$.

Claim The polynomial $P_{\zeta_n/\mathbb{Q}}(X) \in \mathbb{Z}[X]$

Proof of claim

By definition $P_{\zeta_n/\mathbb{Q}}(X)$ is monic and lies in $\mathbb{Q}[X]$. Moreover, as ζ_n is a zero of $F(X) = X^n - 1$, then $P_{\zeta_n/\mathbb{Q}}(X) \mid F(X)$, so the Gauß lemma implies that $P_{\zeta/\mathbb{Q}}(X) \in \mathbb{Z}[X]$ $\square$

We need to show that $\forall\ a \in \mathbb{Z}$ s.t. $(a,n)=1$,

$$P_{\xi/\mathbb{Q}}(\xi^a) = 0$$

Claim We may assume WLOG that $a = p$, prime not dividing n.

Proof of claim

[Ex.]

Consider that the factorization over $\mathbb{Q}$ into monic irred's

$$F(X) = X^n - 1 = f_1(X) \cdot \ldots \cdot f_k(X)$$

must be also over $\mathbb{Z}$ by the Gauß lemma, so $\mathbb{Z} \xrightarrow{\text{red}} \mathbb{F}_p$ yields

$$X^n - \tilde{1} = \tilde{f}_1(X) \cdot \ldots \cdot \tilde{f}_k(X)$$

over $\mathbb{F}_p$. Let L be the splitting field of $X^n - \tilde{1}$ over $\mathbb{F}_p$.

As $p \nmid n$, $X^n - \tilde{1} = (X - z_1) \cdot \ldots \cdot (X - z_n)$, with

$z_1, \ldots, z_n \in L$ distinct. Thus $i \neq j$ implies that

$$(\tilde{f}_i, \tilde{f}_j) = 1.$$

Choose the numbering in (★) so that $f_1(X) = P_{\zeta/\mathbb{Q}}(X)$ and suppose ζ_n^p is a root of $f_j(X)$. In particular, ζ is a root of $f_j(X^p)$, so $f_1(X) \mid f_j(X^p)$. Then $\tilde{f}_1(X) \mid \tilde{f}_j(X^p)$.

Hence $\forall$ root $z \in L$ of $\tilde{f}_1(X)$ we have $\tilde{f}_j(z^p) = 0$.

Frobenius

But $\tilde{f}_1(z^p) = \left(\tilde{f}_1(z)\right)^p = 0$, so $\tilde{f}_1(X)$ and $\tilde{f}_j(X)$ are not coprime if $j \neq 1$. Therefore $j = 1$, i.e. $\deg P_{\zeta_n/\mathbb{Q}}(X) = \varphi(n)$ □