4.3 Cyclotomic extensions

Def: A <u>root of unity in K</u> is an element $\zeta \in K$ such that $\zeta^n = 1$ for some $n \geq 1$. If it is a <u>primitive n-th root of unity</u> if $\mathrm{ord}(\zeta) = n$ (as element of $K^\times$). In this case, we often write $\zeta_n = \zeta$. We define

- $\mu_n(K) = \{ \zeta \in K \mid \zeta^n = 1 \}$
- $\mu_n = \mu_n(\bar{K}) = \{ \zeta \in \bar{K} \mid \zeta^n = 1 \}$
- $\mu_\infty = \{ \zeta \in \bar{K} \mid \zeta^n = 1 \text{ for some } n \geq 1 \}$

Rem: Since $T^n - 1$ is defined over the prime field of K ($\mathbb{Q}$ or $\mathbb{F}_p$), μ_n depends only on $\mathrm{char}(K)$.

Lemma 1: (1) If $\mathrm{char}(K) \nmid n$, then $T^n - 1$ is separable and $\#\mu_n = n$.

(2) If $\mathrm{char}(K) = p > 0$, then 1 is the only root of $T^{(p^n)} - 1$ for every $n \geq 1$.

proof: (1) For $f = T^n - 1$, $f' = n T^{n-1} \neq 0$ in K, and 0 is the only root of f', but $f(0) \neq 0$. Thus f is separable and has n different roots in $\bar{K}$, i.e. $\#\mu_n = n$.

(2) Clear since $T^{(p^n)} - 1 = (T-1)^{(p^n)}$.

□

Rem: As a finite subgroup of $K^\times$, $\mu_n(K)$ is cyclic, and $K(\zeta_n, \zeta_m) = K(\zeta_{\mathrm{lcm}(n,m)})$

Def: • A field extension L/K is a cyclotomic extension if it is algebraic and if there is a K-linear embedding $L \to K(\mu_\infty)$.

• A finite extension L/K is abelian if it is Galois with abelian Galois group.

Ex: $\zeta_7 \in \overline{\mathbb{Q}}$ primitive 7-th root of unity

Then $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ is cyclotomic, but not generated by roots of unity.

Thm 2: Every finite cyclotomic extension L/K is abelian.

proof: • Fix an embedding $L \hookrightarrow K(\mu_\infty)$. Since L/K is finite, $L \subset K(\zeta_n)$ for some primitive n-th root of unity ζ_n.

$K(\zeta_n)$ / L / K

Since the case $L = K$ is clearly abelian, we may assume that $n \geq 2$ and $\mathrm{char}(k) \nmid n$, i.e. $K(\zeta_n)/K$ is separable. Thus L/K is separable.

• Given a K-linear homomorphism $\sigma: K(\zeta_n) \to \overline{K}$, we have $\sigma(\zeta_n)^n = \sigma(\zeta_n^n) = 1$, and $\sigma(\zeta_n)^k \neq 1$ for all $0 < k < n$. Thus $\sigma(\zeta_n)$ is a primitive n-th root of unity, i.e. $\sigma(\zeta_n) = \zeta_n^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Thus $\operatorname{im}\sigma = K(\zeta_n)$ and $K(\zeta_n)/K$ is normal.

- Since $\sigma : K(\zeta_n) \to \bar{K}$ is determined by $i = i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$, we get an inclusion

$$i : Gal(K(\zeta_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$
$$\sigma \longmapsto i(\sigma)$$

which is a group homomorphism since

$$\zeta_n^{i(\sigma\tau)} = \sigma\tau(\zeta_n) = \sigma(\tau(\zeta_n)) = (\zeta_n^{i(\tau)})^{i(\sigma)} = \zeta_n^{i(\sigma)\cdot i(\tau)},$$

i.e. $i(\sigma\tau) = i(\sigma)\cdot i(\tau)$.

- Thus $Gal(K(\zeta_n)/K) < (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, and every subgroup is normal with abelian quotient. This shows that L/K is normal, and

$$Gal(L/K) \cong Gal(K(\zeta_n)/K)/Gal(K(\zeta_n)/L)$$

is abelian. □

Question: What is the image of $i : Gal(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$

Ex: Consider $\mathbb{F}_{p^m}/\mathbb{F}_p$ for p prime and $m \in \mathbb{N}$.

Then $\mathbb{F}_{p^m} = \mathbb{F}_p(\zeta_r)$ is generated by a primitive r-th root of unity $\zeta_r \in \mathbb{F}_{p^m}$ where $r = p^m - 1$, and the image of $Gal(\mathbb{F}_{p^m}/\mathbb{F}_p) = \langle Frob_p \rangle$ is a cyclic subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$ of order $k = \frac{m}{n}$.

Thm 3: p prime

$\mathrm{char}(K) \neq p$

$\exists \zeta_p \in \overline{K}$ primitive p-th root of unity

$f = T^{p-1} + T^{p-2} + \cdots + T + 1$

If f is irreducible over K, then $[K(\zeta_p) : K] = p-1$, f is the minimal polynomial of ζ_p over K, and

$$\mathrm{Gal}(K(\zeta_p)/K) = (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

proof: • Since $f \cdot (T-1) = T^p - 1$, ζ_p^i is a root of f for $i = 1 - p-1$. Since f is irreducible, $\zeta_p^i \notin K$ for all $i = 1 - p-1$. Thus $K(\zeta_p) \simeq K[T]/(f)$ is the splitting field of f and of degree $p-1$ over K.

• By Lemma 1, f is separable and $K(\zeta_p)/K$ is Galois. Thus $\varphi : \mathrm{Gal}(K(\zeta_p)/K) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ is an isomorphism, and f is the minimal polynomial of ζ_p over K. □

Cor 4: $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$.

proof: • By Thm. 3, it suffices to show that $f = T^{p-1} + \cdots + T + 1$ is irreducible over $\mathbb{Q}$, which is the case iff. $f(T+1)$ is so.

• We have

$$f(T+1) = \frac{(T+1)^p - 1}{(T+1) - 1}$$

$$= \frac{1}{T}\left(\sum_{i=0}^{p} \binom{p}{i} T^i - 1\right)$$

$$= T^{p-1} + \binom{p}{p-1} T^{p-2} + \cdots + \binom{p}{2} T + \binom{p}{1}$$

- Since $\binom{p}{i}$ is divisible by p for $i = 1, \ldots, p-1$ and $\binom{p}{1} = p$ is not divisible by p^2, $f(T+1)$ is irreducible by Eisenstein's criterion. □

Def: Euler's φ-function or totient function is $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ for $n \geq 1$.

Thm 5: $\zeta_n \in \overline{\mathbb{Q}}$ primitive n-th root of unity. The map $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a group isomorphism. Consequently, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

proof: Let f be the minimal polynomial of ζ_n. Then $f \mid T^n - 1$, i.e. $T^n - 1 = f \cdot g$ for some $g \in \mathbb{Q}[T]$. Since f and $T^n - 1$ are monic, g is so, too. Thus $f \cdot g \in \mathbb{Z}[T]$ by the Gauss Lemma.

Claim: If p is prime and $p \nmid n$, then $f(\zeta_n^p) = 0$.

Assume that $f(\zeta_n^p) \neq 0$. Then $g(\zeta_n^p) = 0$,

and ζ_n is a root of $\tilde{g} = g(T^p)$.

$\Rightarrow f \mid \tilde{g}$, i.e. $\tilde{g} = f \cdot h$.

Since f and $\tilde{g}$ are monic, so is h.

By the Gauss Lemma, $h \in \mathbb{Z}[T]$.

$\Rightarrow \bar{g}^p = \bar{f} \cdot \bar{h}$ for the residue classes of g, f and h in $\mathbb{F}_p[T]$

$\Rightarrow \bar{f}$ and $\bar{g}$ have a common factor in $\mathbb{F}_p[T]$

$\Rightarrow T^n - \bar{1} = \bar{f} \cdot \bar{g}$ has multiple roots in $\bar{\mathbb{F}}_p$

$\Rightarrow p \mid n$ (by Lemma 1). ↯

- Since $p \nmid n$, ζ_n^p is a primitive n-th root of unity. Conversely, $\zeta_n^i = \zeta_n^{p_1 \cdots p_r}$ if $i = p_1 \cdots p_r$ is a prime decomposition. If ζ_n^i is primitive, then $\gcd(i, n) = 1$, i.e. $p_j \nmid n$ for all $j = 1, \dots, r$.

Applying the claim successively to $p_1, \dots, p_r$ shows that $f(\zeta_n^i) = 0$ for all primitive n-th roots of unity ζ_n^i. Thus $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg f = \varphi(n)$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

□

A deep theorem from number theory, which we will not prove here, is the following.

Thm (Kronecker–Weber)

Every abelian extension of $\mathbb{Q}$ is cyclotomic.