5.8 Cyclotomic extensions

Recording and typing by 9622534, Bin Yeh

Definition: $K(x^n-1)$ is called the *cyclotomic extension* of field K of order n.
Note: If $char(K)=p$ and $n=pm$, then $x^n-1=(x^m-1)^p$. Hence
$K(x^n-1)=K(x^m-1)$.
We assume $char(K)\nmid n$, including $char(K)=0$.

Theorem: $K(x^n-1)=K(\alpha)$, where α is a primitive nth root of 1, i.e. $\alpha^n=1$, $\alpha^i\neq 1\ \forall 1\leq i<n$.
proof:
$(\supseteq)$It's clear to see.
$(\subseteq)1$, α, α^2, ..., α^{n-1} are all distinct roots of x^n-1. ■

Definition: Let α be a primitive nth root of 1, K be a field, then
$g_n(x)=\prod_{1\leq i\leq n,(i,n)=1}(x-\alpha^i)$ is called the nth cyclotomic polynomial over K.

Example: Let $K=\mathbb{Q}$. We have
1. $g_1(x)=x-1$
2. $x^2-1=(x-1)(x+1)$, pick $\alpha=-1$, $g_2(x)=x-(-1)=x+1$.
3. $x^3-1=(x-1)(x-e^{2/3\pi i})(x-e^{4/3\pi i})$, pick $\alpha=e^{2/3}\pi i$, we have
$g_3(x)=(x-\alpha)(x-\alpha^2)=x^2+x+1$.
4. $x^4-1=(x+1)(x-1)(x-i)(x+i)$, pick $\alpha=i$,
$g_4(x)=(x-i)(x-i^3)=x^2+1$.

Theorem: $x^n-1=\prod_{k|n}g_k(x)$
proof:
$x^n-1=\prod_{0\leq i\leq n-1}x-\alpha^i$, where α is a primitive nth root of 1
$=\prod_{k|n}(\prod_{0\leq i\leq n-1,(i,n)=k}(x-\alpha^i))=\prod_{k|n}(\prod_{0\leq\frac{i}{k}\leq\frac{n}{k}-1,(\frac{i}{k},\frac{n}{k})=1}(x-\alpha^k)^{\frac{i}{k}})$, note that α^k is a primitive $\frac{n}{k}th$ root of 1
$=\prod_{k|n}(g_{\frac{n}{k}}(x))=\prod_{k|n}(g_k(x))$ ■

Lemma: $g_n(x)\in K'[x]$, where

$$K'=\begin{cases}\mathbb{Q}, & \text{if } char(K)=0\\ \mathbb{Z}_p, & \text{if } char(K)=p\end{cases}$$

proof: For any $\sigma\in G(K'(x^n-1)/K')$, σ can be extended to an endomorphism on $K'(x^n-1)[x]$ by sending x to x.
Then
$\sigma(g_n(x))=\sigma(\prod_{1\leq i\leq n,(i,n)=1}(x-\alpha^i))=\prod_{1\leq i\leq n,(i,n)=1}(x-\sigma(\alpha^i))=g_n(x)$,
hence $g_n(x)\in K'[x]$. ■