Theorem K/F separable, $F \subseteq L \subseteq K \Rightarrow L/F$, K/L separable

pf $\forall \alpha \in K$, $m_{\alpha,L} \mid m_{\alpha,F}$.

Cyclotomic extensions & polynomials (assume char $F \nmid n$).

F - field. n^{th} cyclotomic extension of F is the splitting field of $x^n - 1$.

n^{th} cyclotomic field is n^{th} c.e. of $\mathbb{Q}$.

Let $K = n^{th}$ c.e. of F. Then $K = F(\omega)$ where ω is one of the $\varphi(n)$ primitive n^{th} roots of 1.

any n^{th} root of 1 is primitive of some degree $d \mid n$.

n^{th} cyclotomic pol-l : $\Phi_n(x) = \prod\limits_{\substack{\alpha:\text{ primitive} \\ n^{th}\text{ root of } 1}} (x - \alpha)$

$$\underbrace{x^n - 1}_{\text{separable}} = \prod_{d \mid n} \Phi_d(x).$$

So $\Phi_n(x) = \dfrac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}$, So Φ_n has integer coefficients

(recall the hom-sm $\mathbb{Z} \longrightarrow F$)

$$\Phi_1(x) = x-1$$

$$\Phi_2(x) = \frac{x^2-1}{x-1} = x+1$$ root is -1, primitive root of deg 3.

$$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$$ roots are primitive roots of deg 3.

$$= \left(x - \frac{\sqrt{-3}-1}{2}\right)\left(x - \frac{-\sqrt{-3}-1}{2}\right)$$

$$\Phi_4(x) = \frac{x^4-1}{(x+1)(x-1)} = x^2+1$$

$$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$$

$$\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1$$

If n is prime, $n=p$, then $\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1$

$$\Phi_{p^2}(x) = \Phi_p(x^p).$$

$$\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}}).$$

If $n = p^r m$, $p \nmid m$, then

$$\Phi_n(x) = \Phi_{pm}(x^{p^{r-1}})$$

so $\Phi_{24}(x) = \Phi_6(x^4) = x^8 - x^4 + 1$

So can reduce to computation of $\Phi_{\text{square-free}}$.

If $n = p_1^{r_1} \cdots p_k^{r_k}$,

$$\Phi_n(x) = \Phi_{p_1 \cdots p_k}\left(x^{p_1^{r_1-1} \cdots p_k^{r_k-1}}\right)$$

<u>Theorem</u> $\forall n$, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

<u>Corollary</u>: over $\mathbb{Q}$, all primitive roots of unity of same degree are conjugate.

<u>corollary</u>: degree over $\mathbb{Q}$ of n^{th} cyclotomic field is $\varphi(n)$.

<u>Proof</u>: Assume not all primitive roots of unity of degree n are conjugate.
Then $\exists$ primitive n^{th} root of unity α and prime $p \nmid n$ s.t. α, α^p are not conjugate

($\omega, \omega^{p_1}, \omega^{p_1 p_2}, \ldots,$ are primitive roots of unity where ω is primitive & each $p_i \nmid n$. not necessarily distinct

at some step, k conjugacy class changes, take $\alpha = \omega^{p_1 \cdots p_{k-1}}$, $p = p_k$).

Then $\Phi_n(x) = f(x)\, g(x)$ such that

$f = m_{\alpha, \mathbb{Q}}$ and α^p is a root of g.

$f(\alpha) = 0$, $\qquad g(\alpha^p) = 0$.

$f, g \in \mathbb{Z}[x]$ by gauss Lemma.

better reason

In $\mathbb{F}_p = \mathbb{Z}/(p)$, $g(\alpha^p) = (g(\alpha))^p = 0$,

and so $g(\alpha) = 0$ and so

Φ_n has a multiple root over $\mathbb{F}_p$.

$g(\alpha^p) = 0$
So $f(x) \mid g(x^p)$,
and this holds
thru factorization.
In $\mathbb{F}_p$, $g(x^p) = g(x)^p$,
so $f \mid g$.

Then $x^n - 1$, which is divisible by Φ_n

is also inseparable in $\mathbb{F}_p$.

but this is not true since $p \nmid n$ and

$(x^n - 1)' = n x^{n-1}$ which only has

0 as a root, no common roots.

Finite fields $|F| < \infty$. let $p = \operatorname{char} F$. let
$n = [F : \mathbb{F}_p]$. Then F has p^n elements.

$|F^\times| = p^n - 1$ (cyclic group of order $p^n - 1$).

Then $\forall \alpha \in F^\times$ $\alpha^{p^n - 1} = 1$.

So $\alpha^{p^n} = \alpha$. ($\forall \alpha \in F$, incl. 0).

So elements of F are roots of $x^{p^n} - x$.

So $x^{p^n} - x$ splits completely in F.

F is a splitting field of $x^{p^n} - x$.

and <u>every</u> element of F is a root of $x^{p^n} - x$.

<u>Theorem</u>: $\forall$ prime p, $\forall n \in \mathbb{N}$, $\exists$ a field with p^n elements and it's unique up to isomorphism.

It is denoted by $\mathbb{F}_{p^n}$.

It is a splitting field of $x^{p^n} - x$.