Ex. splitting field of x^3-2 over $\mathbb{Q}$

$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2\right) = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$

.

13.6 Cyclotomic polynomials and extensions.

Recall. For $\zeta_n := e^{\frac{2\pi i}{n}}$,

$$x^n - 1 = \prod_{k=0}^{n-1}(x - \zeta_n^k) \in \mathbb{C}[x]$$

has the splitting field $\mathbb{Q}(\zeta_n)$, the *cyclotomic field of the n-th roots of unity*.
The *n-th roots of unity* $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ form a cyclic multiplicative group $\langle\zeta_n\rangle$.
Generators of $\langle\zeta_n\rangle$ are called the *primitive* n-th roots of unity.

Question. What is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$?

Note.

$$\begin{aligned} x^n - 1 &= \prod_{k=0}^{n-1}(x - e^{k\frac{2\pi i}{n}}) \\ &= \prod_{d|n} \underbrace{\prod_{1\le k\le d, \gcd(k,d)=1} (x - e^{k\frac{2\pi i}{d}})}_{=: \Phi_d(x)} \end{aligned}$$

$\Phi_d(x) := \prod_{\zeta \text{ primitive } d\text{-th root of unity}} (x-\zeta)$ is the d-th *cyclotomic polynomial*

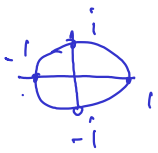
$\deg \Phi_d(x) =$ $\varphi(d)$ Euler's φ

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

$\Phi_2(x) = x+1$ $\qquad x^2-1 = (x-1)(x+1)$ $\qquad \{1,-1\} = \langle -1\rangle$

For p prime, $x^p - 1 = (x-1)\underbrace{(x^{p-1} + \cdots + x + 1)}_{\Phi_{p-1}(x)}$ $\qquad \langle\zeta_p\rangle \cong (\mathbb{Z}_p, \cdot)$

$\Phi_4(x) = (x-i)(x+i) = x^2+1$



Theorem. $\Phi_n(x) \in \mathbb{Z}[x]$ *is monic of degree* $\varphi(n)$*, irreducible over* $\mathbb{Q}[x]$.

Proof. Monic and deg $\varphi(n)$ by definition.

1) $\Phi_n(x) \in \mathbb{Z}[x]$ by induction on n:

$\Phi_1(x) = x - 1$ ✓

Assume $n > 1$. Then

$x^n - 1 = \Phi_n(x) \cdot f(x)$

where $f(x) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \in \mathbb{Z}[x]$ by ind. ass.

By pol. division $\Phi_n(x) \in \mathbb{Q}[x]$ and $\Phi_n(x) \in \mathbb{Z}[x]$ by Gauss' Lemma.

Gauss' Lemma: Let R be a UFD with field of fractions F, $f(x) \in R[x]$

If $f(x) = g(x) \cdot h(x)$ for $g, h \in F[x] \setminus F$, then $\exists a \in F^\times$:

$f(x) = \underbrace{a g(x)}_{\in R[x]} \cdot \underbrace{a^{-1} h(x)}_{\in R[x]}$

2) Assume $\Phi_n(x) = f(x) \cdot g(x)$ for $f(x) \in \mathbb{Z}[x]$ irreducible, $g(x) \in \mathbb{Z}[x]$.

Let ζ be a primitive n-th root of unity such that $f(\zeta) = 0$.

Then $f(x) = m_{\zeta, \mathbb{Q}}(x)$.

Claim: $f(\zeta^m) = 0$ for all $1 \leq m \leq n$, $\gcd(m, n) = 1$.

Let p prime, $p \nmid n$. Then $\Phi_n(\zeta^p) = 0$.

Suppose $g(\zeta^p) = 0$. Then ζ is a root of $g(x^p)$

Thus $g(x^p) = f(x) h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

Modulo p $\quad \overline{g}(x)^p = \overline{g}(x^p) = \overline{f}(x) \cdot \overline{h}(x)$ in $\mathbb{F}_p[x]$

Since $\mathbb{F}_p[x]$ is a UFD, $\gcd(\overline{g}(x), \overline{f}(x)) \neq 1$ in $\mathbb{F}_p$

In $\mathbb{F}_p$, $\overline{\Phi}_n(x) = \overline{f}(x) \cdot \overline{g}(x)$ has a multiple root, contradicting that $x^n - 1$ is separable over $\mathbb{F}_p$.

Thus $f = \Phi_n$ □

Corollary. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

Proof. $m_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x)$ □

Note. For p prime and $q = p^n$, F_q is the splitting field of

$$x^q - x = x(x^{q-1} - 1) = x \prod_{d \mid q-1} \bar{\Phi}_d(x) \in F_p[x].$$

If $F_q^* = \langle \alpha \rangle$, then $m_{\alpha, F_p}(x)$ divides $\bar{\Phi}_{q-1}(x)$ (not necessarily irred in F_p, HW)