Satz 22.3.1: Die Galoisgruppe von $L_n/\mathbb{Q}$.

Vorüberlegung Wähle primitive n-te EHW ξ. Dann kann ich jede andere EHW η in der Form $\eta = \xi^k$ schreiben, wo $k \in \mathbb{Z}$ ist. Dabei ist k eindl. modulo n, denn $\xi^k = \xi^{k+n}$. Also erhalte ich Abb.

$$\mu: \{\text{n-ten EHW}\} \to \mathbb{Z}/(n).$$

Satz 17.4.6 Ein EHW η ist genau dann primitiv, ~~w~~ wenn $\mu(\eta) \in \left(\mathbb{Z}/(n)\right)^*$

Zum Beweis: Jedes Elt. der Galoisgruppe $Gal(L_n/\mathbb{Q})$ permutiert die n-ten EHW.
Also erhalte ich eine Abb.

$$\alpha: Gal(L_n/\mathbb{Q}) \to \mathbb{Z}/(n)$$
$$\sigma \mapsto \mu(\sigma(\xi))$$

Beob: Das Minimalpolynom von ξ ist $\Phi_n \in \mathbb{Z}[x]$

$\to$ jedes Elt. der Galoisgruppe $Gal(L_n/\mathbb{Q})$ permutiert $\underbrace{\text{die Nst. von } \Phi_n}_{=\text{ primitiven n-ten EHW}}$

Konsequenz: $Bild(\alpha) \subset \left(\mathbb{Z}/(n)\right)^*$; wir erhalten also Abb.

$$\beta: Gal(L_n/\mathbb{Q}) \to \left(\mathbb{Z}/(n)\right)^*$$

und das ist ein Gruppenmorphismus!

Wir wissen auch: jedes $\sigma \in Gal(L_n/\mathbb{Q})$ ist durch $\sigma(\xi)$ eindeutig festgelegt!

Konsequenz: ~~Di~~ Der Gruppenmorph. β ist injektiv!

Aber links und rechts stehen ~~z~~ Gruppen mit jeweils genau $\varphi(n)$ vielen Elten. $\Rightarrow$ β ist bijektiv, also isomorph! $\square$