Beweis von 23.1.3.2 Sei L/K eine Galoiserweiterung mit $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/(n)$.

Wähle primitives Elt. $\sigma \in \mathrm{Gal}(L/K)$. Dann ist

$$\mathrm{Gal}(L/K) = \{ \mathrm{Id}, \sigma, \sigma^2, \ldots, \sigma^{n-1} \}.$$

Wähle prim. n-te Einheitswurzel $\zeta \in K$. [Bem: Annahmen garantieren, dass es exakt n n-te EHW gibt]

betrachte Charaktere $\zeta^i \cdot \sigma^i : L^* \to L$

Erinnerung: Satz 16.1.5 die Charaktere sind K-linear unabhängig, also

$$\sum_{i=0}^{n-1} \zeta^i \cdot \sigma^i \neq 0$$

Das bedeutet: $\exists\, \alpha \in L$: $\underbrace{\sum \zeta^i \cdot \sigma^i(\alpha)}_{=:a} \neq 0$

Wesentliche Eigenschaft von a:

$$\sigma(a) = \sigma\left(\sum \zeta^i \cdot \sigma^i(\alpha)\right) = \sum_{i=0}^{n-1} \zeta^i \sigma^{i+1}(\alpha)$$

$$= \sum_{i=0}^{n-1} \zeta^{i-1} \cdot \sigma^i(\alpha) = \zeta^{-1}\left(\sum_{i=0}^{n-1} \zeta^i \sigma^i(\alpha)\right) = \zeta^{-1} \cdot a.$$

Konsequenz 1 Es ist $\sigma(a^n) = \zeta^{-n} \cdot a^n = a^n$.

Also: $\sigma \in \mathrm{Gal}(L/K)$ lässt a invariant. $\Rightarrow$ $a^n \in \mathrm{Fix}(\mathrm{Gal}(L/K)) = K$.

Konsequenz 2 Die Abb. $\sigma : L \to L$ bildet $K(a)$ ~~auch~~ auf $K(a)$ ab.

Also liefern die Elte. $\mathrm{Id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ n unterschiedliche K-Morphismen $K(a) \to K(a)$.

Satz 14.4.5: $[K(a) : K] \geq n$; aber L/K ist Galois, also

$$n = \#\,\mathrm{Gal}(L/K) = [L : K] \Rightarrow K(a) = L.$$

$\square$