Satz 5.10. *Sei $\mathfrak{p} \subset A$ prim zum Führer $\mathcal{F}$ von $A[\theta]$ in B und sei*

$$\bar{p} = \bar{p}_1^{e_1} \cdots \bar{p}_g^{e_g}$$

die eindeutige Faktorisierung des Bildes $\bar{p}$ des Minimalpolynoms p von θ in $A/\mathfrak{p}[X]$ in irreduzible normierte Polynome. Seien $p_1, \ldots, p_g \in A[X]$ normierte Vertreter von $\bar{p}_1, \ldots, \bar{p}_g$. Dann sind die Ideale

$$\mathfrak{P}_i = \mathfrak{p}B + p_i(\theta)B, \quad i = 1, \ldots, g,$$

die Primideale über $\mathfrak{p}$ in B. Der Trägheitsgrad f_i von $\mathfrak{P}_i$ ist der Grad von $\bar{p}_i$ und es gilt

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Beweis. Wir betrachten den natürlichen Homomorphismus

$$\psi : A[X] \longrightarrow A[\theta], \ f \longmapsto f(\theta).$$

Dieser ist offenbar surjektiv. Der Kern besteht aus allen Polynomen $f \in A[T]$ mit $f(\theta) = 0$, enthält also insbesondere $pA[X]$. Wir betrachten den induzierten Homomorphismus $\bar{\psi} : A[X]/pA[X] \to A[\theta]$. Dieser ist auch injektiv: Es ist $A[X]/pA[X]$ ein freier A-Modul vom Rang $n = \deg p$. Eine Basis ist gegeben durch die Restklassen von $1, X, \ldots, X^{n-1}$. Wäre $\bar{\psi}$ nicht injektiv, so wären die Bilder $1, \theta, \ldots, \theta^{n-1}$ dieser Basis linear abhängig über A, also auch über K, was nicht der Fall ist. Wir erhalten daher $\ker(\psi) = pA[X]$ und

$$A[\theta] \cong A[X]/p.$$

Wir setzen $B' = A[\theta] \subset B$ und betrachten den natürlichen Homomorphismus.

$$\varphi : B'/\mathfrak{p}B' \longrightarrow B/\mathfrak{p}B.$$

Behauptung: φ ist ein Isomorphismus.

Surjektivität: wegen $\mathcal{F} + \mathfrak{p}B = B$ und $\mathcal{F} \subset B'$.

Injektivität: Da $\mathfrak{p}B$ und $\mathcal{F}$ teilerfremd sind, hat $\mathcal{F}$ in B keinen Primteiler, der über $\mathfrak{p}$ liegt. Daher sind auch $\mathfrak{p}$ und $\mathcal{F} \cap A$ teilerfremd, also $\mathfrak{p} + (\mathcal{F} \cap A) = A$. Wir wählen $a \in \mathfrak{p}$, $f \in \mathcal{F} \cap A$ mit $a + f = 1$. Sei nun $\bar{x} \in \ker(\varphi)$ und $x \in B'$ ein Urbild. Dann gilt $x = ax + fx$. Nun gilt $ax \in \mathfrak{p}B'$. Außerdem liegt nach Annahme $x \in \mathfrak{p}B$, also $x = \sum_{i=1}^r \alpha_i \beta_i$, $\alpha_i \in \mathfrak{p}$, $\beta_i \in B$. Wegen $f \in \mathcal{F}$ gilt $f\beta_i \in B'$ für alle i, also $fx = \sum_{i=1}^r \alpha_i(f\beta_i) \in \mathfrak{p}B'$. Zusammen erhalten wir $x \in \mathfrak{p}B'$, also $\bar{x} = 0$. Dies zeigt die Behauptung.

Setze $k = A/\mathfrak{p}$. Dann gilt

$$B'/\mathfrak{p}B' = A[X]/p \,/\, \mathfrak{p}(A[X]/p) = A/\mathfrak{p}[X]/\bar{p} = k[X]/\bar{p} \cong \prod_{i=1}^{g} k[X]/\bar{p}_i{}^{e_i},$$

wobei $\bar{p} = \bar{p_1}^{e_1} \ldots \bar{p_g}^{e_g}$ die eindeutige Primzerlegung von $\bar{p}$ in $k[X]$ ist.

Seien $p_1, \ldots, p_g \in A[X]$ Vertreter von $\bar{p_1}, \ldots, \bar{p_g}$. Betrachte den induzierten Homomorphismus

$$(*) \qquad B' = A[\theta] \twoheadrightarrow B'/\mathfrak{p}B' \cong \prod_{i=1}^{g} k[X]/\bar{p}_i^{e_i}.$$

Die Primideale im Produktring

$$\prod_{i=1}^{g} k[X]/\bar{p}_i^{e_i}$$

sind gerade die Hauptideale erzeugt von $(1, \ldots, 1, \bar{p_i}, 1, \ldots, 1)$ bzw., da $(\bar{p_i}, \bar{p_j}) = 1$ für $i \neq j$, die Hauptideale $(\bar{p_i}, \ldots, \bar{p_i})$, $i = 1, \ldots, g$. Deren Urbilder $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ unter der Surjektion $(*)$ sind genau die Primideale in B', die $\mathfrak{p}B'$ umfassen. Es gilt

$$\mathfrak{q}_i = \mathfrak{p}B' + p_i(\theta)B',$$

weil $p_i(\theta)$ auf $(\bar{p_i}, \ldots, \bar{p_i})$ abgebildet wird.

Der Isomorphismus φ liefert: Die Primideale in B über $\mathfrak{p}$ sind genau die Primideale

$$\mathfrak{P}_i = \mathfrak{p}B + p_i(\theta)B, \quad i = 1, \ldots, g.$$

Es gilt: $B/\mathfrak{P}_i \cong B'/\mathfrak{q}_i \cong k[X]/\bar{p_i}$, also $f_i = \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i = \deg \bar{p_i}$.

Nun geht $\prod_{i=1}^g \mathfrak{q}_i^{e_i}$ unter der Surjektion $(*)$ auf $\prod_{i=1}^g \bar{p_i}^{e_i}$, welches das Nullideal in $k[X]/\bar{p}$ ist. Daher gilt $\prod_{i=1}^g \mathfrak{q}_i^{e_i} \subset \mathfrak{p}B'$ und deshalb $\prod\limits_{i=1}^{g} \mathfrak{P}_i^{e_i} \subset \mathfrak{p}B$.

Sei nun $\mathfrak{p}B = \prod\limits_{i=1}^{g} \mathfrak{P}_i^{E_i}$. Dann folgt $E_i \leq e_i$ für alle i. Mit $n = [L : K]$ und wegen $n = \deg p = \deg \bar{p}$ folgt

$$n = \dim_k k[X]/\bar{p} = \sum_{i=1}^{g} \dim_k k[X]/\bar{p}_i^{e_i} = \sum_{i=1}^{g} e_i f_i.$$

Andererseits erhalten wir nach 5.7

$$n = \sum_{i=1}^{g} E_i f_i,$$

und wegen $E_i \leq e_i$ folgt $E_i = e_i$ für alle i. $\square$