Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z12: Zerlegungsverhalten von Primidealen

Stichworte: Zerlegungsproblem von $B\mathfrak{p}$, Verzweigungsindex $e(\mathfrak{q}|\mathfrak{p})$, Trägheitsgrad $f(\mathfrak{q}|\mathfrak{p})$, Formel $n=\sum_{i=1}^{r} e_i f_i$, zerlegte/verzweigte/träge Primideale, explizite PIZ in $L|K$

12.1. **Einleitung:** Wir untersuchen das Zerlegungsverhalten von $B\mathfrak{p}$ in Primideale von A, wenn B bzw. A die ZRe einer ZKerweiterung $L|K$ bezeichnen und $\mathfrak{p}$ ein Primideal in A ist. Diese Fragestellung beinhaltet insbesondere den Fall $A=\mathbb{Z}$ und die Zerlegbarkeit von Primzahlen $p\in\mathbb{Z}$ in erweiterten ZRen. Wichtige Kenngrößen dabei sind die Verzweigungsindizes $e_1,\dots,e_r$ und Trägheitsgrade $f_1,\dots,f_r$, die die bemerkenswerte Formel $[L:K]=\sum_{i=1}^{r} e_i f_i$ erfüllen. Wir kommen zum Begriff des verzweigten bzw. trägen Primideals. Zuletzt beweisen wir den allgemeinen Satz zur expliziten Zerlegung von $B\mathfrak{p}$ in Primideale.

12.2. **Vor.:** Seien $K\subseteq L$ Zahlkörper mit Zahlringen $A\subseteq B$.

12.3. **Def.:** Sei $\mathfrak{a}\subseteq A$ Ideal. Dann ist $B\mathfrak{a} := \{\sum_{i=1}^{n} b_i a_i ;\ n\in\mathbb{N},\ b_i\in B,\ a_i\in\mathfrak{a}\}$ das von $\mathfrak{a}$ in B erzeugte Ideal.

12.4. **Bem.:** Es gilt $B(\mathfrak{a}_1\cdot\mathfrak{a}_2)=(B\mathfrak{a}_1)\cdot(B\mathfrak{a}_2)$.
„$\supseteq$": r.S. wird erzeugt von allen $(\sum_i b_i a_{1i})(\sum_j b'_j a_{2j})$.
„$\subseteq$": l.S. wird erzeugt von allen $(\sum_i b_i a_{1i} a_{2i})$. ⌋

12.5. **Problem:** Sei $\mathfrak{p}\in\mathcal{P}(A)$. Gesucht ist die Zerlegung von $B\mathfrak{p}$ als
(*) $B\mathfrak{p}=\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$, die $\mathfrak{q}_i\in\mathcal{P}(B)$ p.w.v., die $e_i\in\mathbb{Z}_{>0}$, mit $B\mathfrak{p}\subseteq\mathfrak{q}_i$, $1\le i\le r$, $r\in\mathbb{N}$.
$\rightsquigarrow$ PIZ

12.6. **Bsp.:** Betr. $\mathbb{Z}\subseteq\mathbb{Z}[i]$. Dort ist $2=(1+i)(1-i)$, also $\mathbb{Z}[i]\cdot 2$
$=\mathbb{Z}[i](1+i)\cdot\mathbb{Z}[i]\underbrace{(1-i)}_{=-i(1+i)}=\mathbb{Z}[i]\cdot(1+i)^2$. Die 3 ist prim in $\mathbb{Z}[i]$, vgl. 13.2, 1. Fall(e), da $(\frac{-1}{3})=(\frac{2}{3})=-1$.

12.7. **Lemma:** Die $\mathfrak{q}_i$ in (*) sind genau diejenigen $\mathfrak{q} \in \mathcal{P}(B)$, die "über $\mathfrak{p}$ liegen", d.h. für die $\mathfrak{p} \subseteq \mathfrak{q}$ gilt ($\Leftrightarrow \mathfrak{p} = \mathfrak{q} \cap A$, in Dedekindbereichen).
Bew.: Es gilt: $B\mathfrak{p} \subseteq \mathfrak{q} \Leftrightarrow n_{\mathfrak{q}}(B\mathfrak{p}) \geq 1$. Somit: „$\Leftarrow$": $\mathfrak{p} \subseteq \mathfrak{q} \Rightarrow B\mathfrak{p} \subseteq B\mathfrak{q} = \mathfrak{q}$.
„$\Rightarrow$": $B\mathfrak{p} \subseteq \mathfrak{q} \Rightarrow \mathfrak{p} \subseteq A \cap \mathfrak{q}$, also $\mathfrak{p} = \mathfrak{q} \cap A \subseteq \mathfrak{q}$. □

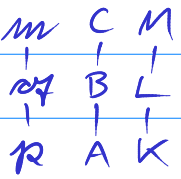
12.8. **Lemma:** Es gilt $B\mathfrak{p} \neq B$.
Bew.: Andernfalls gilt $1 = \sum_{i=1}^{n} b_i a_i$ für gewisse $b_i \in B$, $a_i \in \mathfrak{p}$. Sei $c \in \mathfrak{p}^{-1} \setminus A$.
Dann ist $c = \sum_{i=1}^{n} b_i (c a_i) \in K \cap B$, $K = \mathrm{Quot}A$. Somit ist, da B ganz über A ist, also $c \in A$, da A ganz abgeschlossen in K. ↯. □

12.9. **Bem.:** Sei $\mathfrak{q} \in \mathcal{P}(B)$. Dann ist $\mathfrak{p} := \mathfrak{q} \cap A \in \mathcal{P}(A)$.
Bew.: Haben: $A \hookrightarrow B$, $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ → also ist $A/\mathfrak{p}$ endlich. Da $B/\mathfrak{q}$ Körper, ist dann auch $A/\mathfrak{p}$ Körper, also $\mathfrak{p} \in \mathcal{P}(A)$. □

12.10. **Def.:** $e(\mathfrak{q}|\mathfrak{p}) := n_{\mathfrak{q}}(B\mathfrak{p})$ heißt **Verzweigungsindex** von $\mathfrak{q}|\mathfrak{p}$,
$f(\mathfrak{q}|\mathfrak{p}) := [B/\mathfrak{q} : A/\mathfrak{p}]$ heißt **Trägheitsgrad** von $\mathfrak{q}|\mathfrak{p}$.
Englisch: ramification index, inertial degree

12.11. **Bsp.:** Im Bsp. 12.6 ist $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$, und $B \cdot 2 = \mathfrak{q}^2$ mit $\mathfrak{q} = B \cdot (1+i)$, $\mathfrak{p} = \mathbb{Z} \cdot 2$.
Haben also $e(\mathfrak{q}|\mathfrak{p}) = 2$ und weiter $f(\mathfrak{q}|\mathfrak{p}) = [B/\mathfrak{q} : A/\mathfrak{p}] = 1$,
denn $A/\mathfrak{p} = \mathbb{Z}/(2) = \mathbb{F}_2$ und $B/\mathfrak{q} = \mathbb{Z}[i]/(1+i) \cong \mathbb{Z}/(2)$, $a+bi + (1+i) \mapsto a-b+(2)$.

12.12. **Lemma:** Seien $K \subseteq L \subseteq M$ Zahlkörper mit Zahlringen $A \subseteq B \subseteq C$,
$\mathfrak{m} \in \mathcal{P}(C)$, $\mathfrak{q} := \mathfrak{m} \cap B$, $\mathfrak{p} := \mathfrak{m} \cap A$. Dann gilt:



(i) $e(\mathfrak{m}|\mathfrak{p}) = e(\mathfrak{m}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p})$,
(ii) $f(\mathfrak{m}|\mathfrak{p}) = f(\mathfrak{m}|\mathfrak{q}) \cdot f(\mathfrak{q}|\mathfrak{p})$.

Bew.: Schreiben $B\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, die $\mathfrak{q}_i \in \mathcal{P}(B)$ p.w.v., $\mathfrak{q} = \mathfrak{q}_1$,
und schreiben $C\mathfrak{q}_i = \mathfrak{m}_{i1}^{e_{i1}} \cdots \mathfrak{m}_{is_i}^{e_{is_i}}$, die $\mathfrak{m}_{ij} \in \mathcal{P}(C)$ p.w.v., $\mathfrak{m} = \mathfrak{m}_{11}$.
Dann ist $C\mathfrak{p} = C(B\mathfrak{p}) = C(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}) \overset{12.4}{=} \prod_{i,j} \mathfrak{m}_{ij}^{e_i e_{ij}}$.
Somit folgt: $e(\mathfrak{m}|\mathfrak{p}) = e_{11} e_1 = e(\mathfrak{m}|\mathfrak{q})\, e(\mathfrak{q}|\mathfrak{p})$, also (i).

Zu (ii): Haben $A/\mathfrak{p} \overset{f(\mathfrak{q}/\mathfrak{p})}{\hookrightarrow} B/\mathfrak{q} \overset{f(\mathfrak{m}/\mathfrak{q})}{\hookrightarrow} C/\mathfrak{m}$, $f(\mathfrak{m}/\mathfrak{p})$ ✓. □

Eine wichtige Beziehung zwischen Verzweigungsindizes und Trägheitsgraden beinhaltet folgender Satz:

12.13. **Satz:** Seien $K \subseteq L$ Zahlkörper mit Zahlringen $A \subseteq B$, $n := [L:K]$, $\mathfrak{p} \in \mathcal{P}(A)$, $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathcal{P}(B)$ die über $\mathfrak{p}$ liegenden Primideale, $e_i := e(\mathfrak{q}_i/\mathfrak{p})$ und $f_i := f(\mathfrak{q}_i/\mathfrak{p})$, $1 \le i \le r$. Dann gilt:

$$n \overset{(1)}{=} \dim_{A/\mathfrak{p}} B/B\mathfrak{p} \overset{(2)}{=} \sum_{i=1}^{r} e_i f_i .$$

Bew.: Zu (2): Sei $\mathfrak{b} \subseteq B$ irgendein Ideal. Dann gibt es keine Ideale $\mathfrak{k}$ mit $\mathfrak{b}\cdot\mathfrak{q}_i \subsetneq \mathfrak{k} \subsetneq \mathfrak{b}$ wegen der Eindeutigkeit der PIZ in Dedekindbereichen. Somit ist der $B/\mathfrak{q}_i$-VR $\mathfrak{b}/\mathfrak{b}\mathfrak{q}_i$ eindimensional, wo $A/\mathfrak{p} \subseteq B/\mathfrak{q}_i$, also ist $f_i = \dim_{A/\mathfrak{p}} \mathfrak{b}/\mathfrak{b}\mathfrak{q}_i$ ⊗. Betr. nun folgende Idealkette

$$\mathfrak{K}: B \supseteq \mathfrak{q}_1 \supseteq \mathfrak{q}_1^2 \supseteq \dots \supseteq \mathfrak{q}_1^{e_1} \supseteq \mathfrak{q}_1^{e_1}\mathfrak{q}_2 \supseteq \dots \supseteq \mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r} = B\mathfrak{p}.$$

Wenden darauf die Projektion $\pi: B \to B/B\mathfrak{p}$ an, und erhalten die Kette von $A/\mathfrak{p}$-Vektorräumen

$$\pi\mathfrak{K}: B/B\mathfrak{p} \supseteq \pi\mathfrak{q}_1 \supseteq \pi\mathfrak{q}_1^2 \supseteq \dots \supseteq 0.$$

Lin. Alg.: $\dim V/W = \dim V - \dim W$

Beachte nun: in VR gilt: $V = V_0 \supseteq V_1 \supseteq \dots \supseteq V_m = 0 \Rightarrow \dim V = \sum_{i=1}^{m-1} \dim V_i/V_{i+1}$.

Da entsprechende Quotienten in $\mathfrak{K}$ und $\pi\mathfrak{K}$ isomorph sind, folgt, dass

$$\dim_{A/\mathfrak{p}} B/B\mathfrak{p} = \sum_{i=1}^{r}\sum_{j=1}^{e_i} \underbrace{\dim_{A/\mathfrak{p}} \mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_{i-1}^{e_{i-1}}\mathfrak{q}_i^{j-1}/\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_{i-1}^{e_{i-1}}\mathfrak{q}_i^{j}}_{= f_i \text{ nach } ⊗}$$

$$= \sum_{i=1}^{r} e_i f_i .$$

Zu (1): Speziell: Sei $K = \mathbb{Q}$. Dann ist $A = \mathbb{Z}$, und $B = \hat{\bigoplus}_{i=1} \mathbb{Z} b_i$ ist freie abelsche Gruppe vom Rang n. Nun ist $\mathfrak{p} = (p)$, also ist

$$B/B\mathfrak{p} = \hat{\bigoplus}_{i=1}^{n} \mathbb{Z} b_i / \hat{\bigoplus}_{i=1}^{n} \mathbb{Z} p b_i \cong \hat{\bigoplus}_{i=1}^{n} \mathbb{Z} b_i / \mathbb{Z} p b_i \cong \bigoplus_{i=1}^{n} \mathbb{Z}/\mathbb{Z}p$$

ein $[L:k] = n$-dimensionaler $\mathbb{Z}/\mathbb{Z}p = A/\mathfrak{p}$-Vektorraum.

Allgemein: „$\geq$": z.z.: Zu $b_{n1},\dots,b_{n+n} \in B$ ex. $a_{n1},\dots,a_{n+n} \in A$, nicht alle $a_i \in \mathfrak{p}$, mit $\sum_{i=n}^{n+n} a_i b_i \in B\mathfrak{p}$. Wegen $[L:K]=n$ ex. $a_{n1},\dots,a_{n+n} \in K$, nicht alle $a_i = 0$, mit $\sum_{i=n}^{n+1} a_i b_i = 0$, dabei seien o.E. alle $a_i \in A$. Seien nun alle $a_i \in \mathfrak{p}$, d.h. $\mathfrak{a} := (a_{n1},\dots,a_{n+n}) \subseteq \mathfrak{p}$. Wählen nun $x \in \mathfrak{a}^{-1} \setminus A$ mit $xa_j \notin \mathfrak{p}$ für ein j [$\mathfrak{a}^{-1}\cdot\mathfrak{a} = A$]. Dann ist $\sum_{i=n}^{n+1} (xa_i) b_i = 0$, wo alle $xa_i \in A$ [$\mathfrak{a}^{-1}\cdot\mathfrak{a} = A$], aber $xa_j \notin \mathfrak{p}$.

„$\leq$": Sei $\mathfrak{p} \cap \mathbb{Z} = (p)$, $n = [K:\mathbb{Q}]$.

$\mathfrak{q}$	B	L
$\mathfrak{p}$	A	K
(p)	$\mathbb{Z}$	$\mathbb{Q}$

Ferner sei $A\mathfrak{p} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ die PFZ von $A\mathfrak{p}$, $\mathfrak{p} = \mathfrak{p}_1$, und seien $\mathfrak{q}_{1,1},\dots,\mathfrak{q}_{1,s_1}$ die über $\mathfrak{p}_1$ liegenden Primideale von B.

Dann ist nach dem Spezialfall dann $n\cdot m = \sum_{i,j} e(\mathfrak{q}_{i,j}|(p))\, f(\mathfrak{q}_{i,j}|(p))$

$\overset{12.12}{=} \sum_{i,j} e(\mathfrak{q}_{i,j}|\mathfrak{p}_i)e(\mathfrak{p}_i|(p)) \cdot f(\mathfrak{q}_{i,j}|\mathfrak{p}_i) f(\mathfrak{p}_i|(p))$

$= \underbrace{\sum_i e(\mathfrak{p}_i|(p)) f(\mathfrak{p}_i|(p))}_{=m \text{ nach Spezialfall}} \cdot \underbrace{\sum_j e(\mathfrak{q}_{i,j}|\mathfrak{p}_i) f(\mathfrak{q}_{i,j}|\mathfrak{p}_i)}_{\leq n \text{ nach Vorigem}}$,

also folgt: $\sum_j e(\mathfrak{q}_{i,j}|\mathfrak{p}_i) f(\mathfrak{q}_{i,j}|\mathfrak{p}_i) = n$, insb. für $i=1$,

somit ist $\dim_{A/\mathfrak{p}} B/B\mathfrak{p} = \sum_j e_j f_j = n = [L:K]$. □

12.14. **Def.:** $\mathfrak{p}$ heißt **verzweigt in L**, falls (mind.) ein $e_i > 1$,

$\mathfrak{p}$ heißt **träge in L**, falls $B\mathfrak{p}$ prim ist, d.h. $f(B\mathfrak{p}|\mathfrak{p}) = n$.

$\mathfrak{p}$ heißt **voll zerlegt in L**, falls $r = [L:K]$ (d.h. alle $e_i = f_i = 1$).

[engl.: ramified, inert, splitdecomposed]

Wir kommen zum allgemeinen Satz zur Primidealzerlegung in bel. ZKerweiterungen.

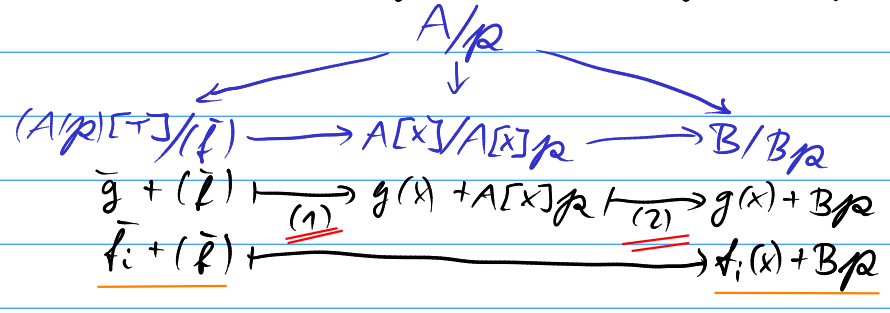
12.15. **Satz (explizite PIZ in ZKerweiterungen):** Seien $K \subseteq L$ ZK mit ZR $A \subseteq B$, $x \in B$ mit $L = K(x)$, $f \in A[T]$ das Mipo von x/K, $\mathfrak{p} \subseteq A$ ein Primideal, $\mathfrak{p} \cap \mathbb{Z} = (p)$. Weiter sei $A[T] \to (A/\mathfrak{p})[T]$, $g \mapsto \bar{g}$, die Projektion,

sowie $\bar{f} = \bar{f}_1^{e_1}\cdots\bar{f}_r^{e_r}$ die PFZ von $\bar{f} \in (A/\mathfrak{p})[T]$, die $f_i \in A[T]$ normiert und p.W.V., und sei $\mathfrak{q}_i := Bf_i(x) + B\mathfrak{p}$, für $1 \leq i \leq r$. [$\mathfrak{q}_i = (f_i(x), \mathfrak{p})$]

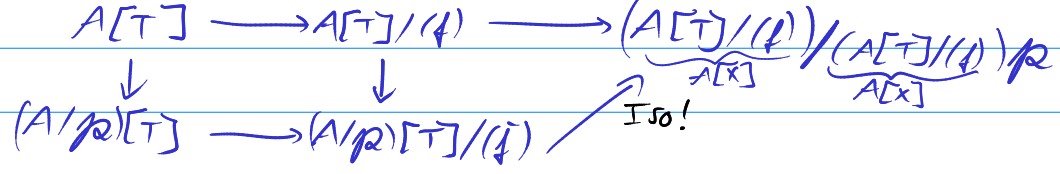
Falls $p \nmid [B:A[x]]$, so sind alle $\mathfrak{q}_i$ p.W.V. Primideale in B, und $B\mathfrak{p} = \mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$ ist die PIZ von $B\mathfrak{p}$ in B.

12.16. **Bem.:** Ist $B = A[x]$ oder ($K = \mathbb{Q}$ und $p \nmid \mathrm{disc}(x)$), so ist $p \nmid [B : A[x]]$.
⌜Es ist $\mathrm{disc}(x) = \mathrm{disc}(L) \cdot [B : A(x)]$, ähnlich wie in 8.6/8.7/8.12 zu sehen.⌟

12.17. **Bew.:** Haben Kommutatives Diagramm von Ringhomomorphismen:

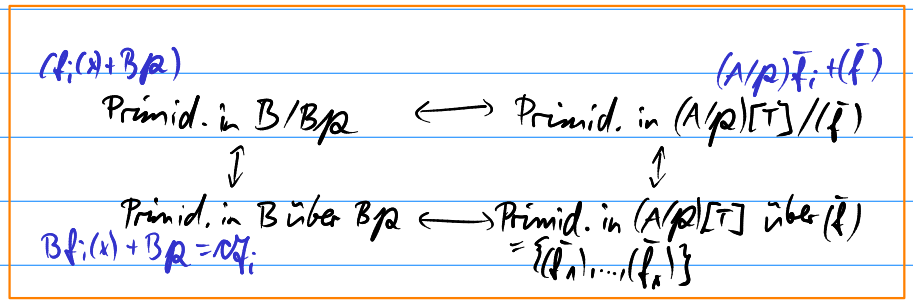


In diesem Diagramm sind (1) und (2) Isomorphismen.
⌜(1): Es gilt: $A[x] \cong A[T]/(f)$ ⌜bekannt aus Algebra A18.17(i), betrachten:



(2): Allg. gilt: $A \subseteq B$ komm. Ringe, $\mathfrak{a} \subseteq A$ Id., $[B:A] = m$ endlich, p prim, $p \in \mathfrak{a}$, $p \nmid m$
$\Rightarrow \varphi : A/\mathfrak{a} \xrightarrow{\cong} B/B\mathfrak{a}$, wo $\varphi : x + \mathfrak{a} \mapsto x + B\mathfrak{a}$ der natürliche Ringhom. ist.
⌜Denn: Seien $u, v \in \mathbb{Z}$ mit $up + vm = 1$ (ex. da $p \nmid m$).
• φ surj.: Sei $b \in B$, dann ist $b = 1 \cdot b = \underbrace{upb}_{\in B\mathfrak{a}} + v \underbrace{mb}_{\in A}$, da $m = \#(B/A)$ als ab. Gruppe
$\Rightarrow \varphi(vmb + \mathfrak{a}) = b + B\mathfrak{a}$.
• φ inj.: z.z.: $B\mathfrak{a} \cap A \subseteq \mathfrak{a}$ ⌜$\Rightarrow \varphi(x + \mathfrak{a}) = x + B\mathfrak{a} = 0 + B\mathfrak{a} \Rightarrow x + \mathfrak{a} = \mathfrak{a} = 0 + \mathfrak{a}$ für $x \in A$⌟
Daher sei $x = \sum_{i=1}^{n} b_i a_i \in A$, die $b_i \in B$, $a_i \in \mathfrak{a}$.
Dann ist $x = x \cdot 1 = \underbrace{upx}_{\in \mathfrak{a}} + \sum_{i=1}^{n} v \underbrace{m b_i}_{\in A} a_i \in \mathfrak{a}$.⌟

Erhalten Bijektionen:



somit folgt:

Die Primideale von B über $B\mathfrak{p}$ sind genau die Urbilder in B der von den Restklassen von $f_1(X), \dots, f_n(X)$ in $B/B\mathfrak{p}$ erzeugten Hauptideale.

Dies sind genau die Ideale $\mathfrak{P}_1, \dots, \mathfrak{P}_n$.

Wegen $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_n^{e_n}$ ist $f_1(X)^{e_1} \cdots f_n(X)^{e_n} \in B\mathfrak{p}$. Also ist

$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n} = (Bf_1(X) + B\mathfrak{p})^{e_1} \cdots (Bf_n(X) + B\mathfrak{p})^{e_n} \subseteq B\mathfrak{p}$.

Insgesamt ist somit $B\mathfrak{p} = \mathfrak{P}_1^{d_1} \cdots \mathfrak{P}_n^{d_n}$ für gewisse $d_i \leq e_i$ die PIZ von $B\mathfrak{p}$.

Nach 12.13 gilt: $\deg f = [L:K] = \sum_{i=1}^{n} d_i [B/\mathfrak{P}_i : A/\mathfrak{p}]$.

Wegen $B/\mathfrak{P}_i \cong (A/\mathfrak{p})[T]/(\bar{f}_i)$ ist $[B/\mathfrak{P}_i : A/\mathfrak{p}] = \deg f_i$.

Also ist $\sum_{i=1}^{n} d_i \deg f_i = [L:K] = \deg f = \sum_{i=1}^{n} e_i \deg f_i$, und da alle $d_i \leq e_i$,

ist somit $e_i = d_i$ für $1 \leq i \leq n$. Also ist $B\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$ die gewünschte PIZ von $B\mathfrak{p}$ in B. □