GANZE ALGEBRAISCHE ZAHLEN UND IDEALFAKTORISIERUNG

ANTONIO CASETTA

In diesem Abschnitt möchten wir zeigen, wie man die Faktorisierung von Idealen berechnen kann und diverse damit zusammenhängende Begriffe.

1. Erinnerung

Definition 1. *Sei $o \subseteq o'$ eine Ringerweiterung, d.h. ein injektiver Ringhomomorphismus. Ein Element $x \in o'$ heißt* ganz *(oder* ganz-algebraisch*) über o, wenn x einer normierten Gleichung genügt, d.h. wenn es $a_1, \dots, a_n \in o$ gibt mit $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Die Menge $\mathcal{O} = \{x \in o' \mid \exists a_1, \dots, a_n \in o\colon x^n + a_1x^{n-1} + \cdots + a_n = 0\}$ heißt* ganzer Abschluss *von o in o'.*

Satz 2. *Eine rationale Zahl ist genau dann ganz-algebraisch, wenn sie in $\mathbb{Z}$ liegt.*

Definition 3. *Wir definieren den Ring der ganzen Zahlen von einem Körper K als*

$$\mathcal{O}_K \coloneqq \mathbb{Z}_K \coloneqq \{b \in K : b \text{ ganz über } \mathbb{Z}\}$$

Satz 4. *$\mathcal{O}_K$ ist ein Dedekind-Ring, i.e. ein noetherscher Integritätsbereich.*

Definition 5. *Sei $\mathcal{O}$ ein Dedekind-Ring und K sein Quotientenkörper. Ein* gebrochenes Ideal *von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K.*

Satz 6. *Sei $\mathcal{O}$ ein Dedekind-Ring. Dann sind die folgenden Aussagen äquivalent:*

(i) $\mathcal{O}$ ist ein Dedekind-Ring.

(ii) Jedes von 0 verschiedene Ideal $\mathfrak{a}$ kann eindeutig als Produkt von Primidealen geschrieben werden:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}, \qquad \nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z} \text{ fast alle gleich null}$$

(iii) Jedes von 0 verschiedene Ideal kann als Produkt von Primidealen geschrieben werden.

(iv) Die Menge der gebrochenen Ideale von K ungleich 0 ist eine Gruppe.

Korollar 7 (Chinesischer Restsatz)**.** *Sei $\mathcal{O}$ ein Dedekind-Ring, $\mathfrak{a} \subseteq \mathcal{O}$ ein Ideal. Dann ist*

$$\mathcal{O}/\mathfrak{a} \cong \prod_{\mathfrak{p}} \mathcal{O}/\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$

Definition 8. *Sei $\mathcal{O}$ ein Integritätsbereich mit Quotientenkörper K. Dann definieren wir:*

(1) Für zwei gebrochene Ideale $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$ ist $\mathfrak{a}|\mathfrak{b}$ genau dann, wenn ein ganzes Ideal $\mathfrak{c}$ gibt, sodass $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$. Dies is äquivalent zu $\nu_{\mathfrak{p}}(\mathfrak{b}) \geqslant \nu_{\mathfrak{p}}(\mathfrak{a})$ für alle Primideale $\mathfrak{p}$. Desweiteren ist es auch äquivalent zu $\mathfrak{b} \subseteq \mathfrak{a}$.

(2) Ein gebrochenes Ideal $\mathfrak{a} \subseteq \mathcal{O}$ heißt invertierbar*, falls es ein gebrochenes Ideal $\mathfrak{a}'$ gibt, so dass $\mathfrak{a} \cdot \mathfrak{a}' = \mathcal{O}$. Also für ein ganzes Ideal $\mathfrak{a} \subseteq \mathcal{O}$ definieren wir $\mathfrak{a}^{-1} \coloneqq \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$.*

Lemma 9. *Seien $\alpha_1, \dots, \alpha_n$ eine $\mathbb{Q}$-Basis eines Körpers K mit alle α_i ganz über K. Falls $d =$ $\operatorname{disk}(\bigoplus_i \alpha_i\mathbb{Z}) = \det(\operatorname{tr}(\alpha_i\alpha_j)_{i,j=1,\dots,n})$ dann gilt $\bigoplus_i \alpha_i\mathbb{Z} \subseteq \mathbb{Z}_K \subseteq \frac{1}{d}\bigoplus_i \alpha_i\mathbb{Z}$.*

2. Primidealfaktorisierung

Jedes Primideal $\mathfrak{p} \neq 0$ von $\mathcal{O}_K$ enthält eine rationale Primzahl p und ist ein Teiler des Ideals $p\mathcal{O}_K$. Also fragen wir uns, wie eine Primzahl p in Primidealen des Rings $\mathcal{O}_K$ zerfällt. Wir betrachten dies Problem in einem allgemeinen Kontext, und beginnen mit einem beliebigen Dedekind-Ring o anstatt von $\mathbb{Z}$. Dann, anstatt von $\mathcal{O}_K$, wählen wir den ganzen Abschluss $\mathcal{O}$ von o in einer endlichen Erweiterung von seinem Quotientenkörper.

Für ein Primideal $\mathfrak{p}$ in o hat man immer $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. In der Tat, sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ so, dass $\pi o = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, also $\mathfrak{p} + \mathfrak{a} = o$. Betrachtet $1 = b + s$, mit $b \in \mathfrak{p}$ und $s \in \mathfrak{a}$, finden wir $s \notin \mathfrak{p}$ und $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi o$.

Falls man $\mathfrak{p}\mathcal{O} = \mathcal{O}$ hätte, dann würde es folgen, dass $s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$, also, dass $s = \pi x$ für eine $x \in \mathcal{O} \cap K = \mathcal{o}$, i.e. $s \in \mathfrak{p}$, Widerspruch.

Ein Primideal $\mathfrak{p} \neq 0$ in dem Ring $\mathcal{o}$ zerfällt in $\mathcal{O}$ in einem eindeutigen Weg in einem Produkt von Primidealen

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

Die Primideale $\mathfrak{P}_i$ in der Faktorisierung sind genau die Primideale $\mathfrak{P}$ in $\mathcal{O}$, die über $\mathfrak{p}$ liegen, i.e. man hat die Relation $\mathfrak{p} = \mathfrak{P} \cap \mathcal{o}$. Dies bezeichnen wir als $\mathfrak{P}|\mathfrak{p}$, und wir nennen $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$. Wir bemerken auch, dass $(\mathcal{O}/\mathfrak{P}_i)/(\mathcal{o}/\mathfrak{p})$ eine Körpererweiterung ist, weil die Abbildung $\mathcal{o} \to \mathcal{O} \to \mathcal{O}/\mathfrak{P}$ Kern $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$ hat. Also ist die Abbildung $\mathcal{o}/\mathfrak{p} \hookrightarrow \mathcal{O}/\mathfrak{P}$ injektiv.

Definition 10. *(1) Das Exponent e_i heißt **Verzweigungsindex**.*

*(2) Der Grad von der Körpererweiterung $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$ wird **Trägheitsgrad** von $\mathfrak{P}_i$ über $\mathfrak{p}$ genannt.*

*(3) $\mathfrak{P}_i$ heißt **unverzweigt** über $\mathfrak{p}$, wenn $e_i = 1$ und wenn die Körpererweiterung $(\mathcal{O}/\mathfrak{P}_i)/(\mathcal{o}/\mathfrak{p})$ separabel ist.*

(4) $\mathfrak{p}$ heißt unverzweigt in L/K, wenn für alle $i = 1, \ldots, r : \mathfrak{P}_i/\mathfrak{p}$ unverzweigt über $\mathfrak{p}$ sind.

*(5) $\mathfrak{p}$ heißt **unzerlegt** in L/K, wenn $r = 1$, d.h., wenn es nur ein Primideal $\mathfrak{P}$ über $\mathfrak{p}$ gibt, und **träge**, wenn zusätzlich $p\mathcal{O}_K$ prim ist.*

*(6) $\mathfrak{p}$ heißt **total zerlegt** in L/K, wenn für alle $i = 1, \ldots, r : f_i = 1$ und $e_i = 1$.*

Satz 11. *Sei $\mathcal{o}$ ein Dedekind-Ring mit Quotientenkörper K und ganzem Abschluss $\mathcal{O}$ in einem Körper L, sodass L/K eine separable Körpererweiterung mit Grad $n = [L : K]$ ist. Für jede Primideal $\mathfrak{p} \neq 0$ in $\mathcal{o}$, schreiben wir die Faktorisierung von $\mathfrak{p}$ als*

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

mit Trägheitsgrade $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$. Dann gilt

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

Beweis. Der Beweis basiert auf dem Chinesichen Restsatz in der folgenden Variante:

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$$

$\mathcal{O}/\mathfrak{p}\mathcal{O}$ und $\mathcal{O}/\mathfrak{P}_i^{e_i}$ sind Vektorräume über dem Körper $\kappa = \mathcal{o}/\mathfrak{p}$, und es ist genug zu zeigen

$$\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{und} \quad \dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$$

Um die erste Identität zu beweisen, seien $\omega_1, \ldots, \omega_m \in \mathcal{O}$ Repräsentanten für eine Basis $\bar{\omega}_1, \ldots, \bar{\omega}_m$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ über κ. Es ist genug zu zeigen, dass $\omega_1, \ldots, \omega_m$ eine Basis von L/K bilden. Wir nehmen an, dass $\omega_1, \ldots, \omega_m$ linear abhängig über K sind, und also über $\mathcal{o}$ auch. Dann gibt es Elemente $a_1, \ldots, a_m \in \mathcal{o}$ nicht alle gleich Null, sodass $a_1\omega_1 + \cdots + a_m\omega_m = 0$. Definiere das Ideal $\mathfrak{a} = (a_1, \ldots, a_m)$ von $\mathcal{o}$ und finde ein $a \in \mathfrak{a}^{-1}$ so, dass $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, also $a\mathfrak{a} \nsubseteq \mathfrak{p}$. Dann liegen die Elemente $aa_1, \ldots, aa_m$ in $\mathcal{o}$, aber nicht alle gehören zu $\mathfrak{p}$. Der Ausdruck $aa_1\omega_1 + \cdots + aa_m\omega_m \equiv 0 \bmod \mathfrak{p}$ impliziert also die lineare Abhängigkeit zwischen die $\bar{\omega}_1, \ldots, \bar{\omega}_m$ über κ, Widerspruch. Die $\omega_1, \ldots, \omega_m$ sind also linear unabhängig über K. Um zu zeigen, dass alle ω_i eine Basis von L/K bilden, betrachten wir die $\mathcal{o}$-Module $M = \mathcal{o}\omega_1 + \cdots + \mathcal{o}\omega_m$ und $N = \mathcal{O}/M$. Seit $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, haben wir $\mathfrak{p}N = N$. Seit L/K separabel ist, sind $\mathcal{O}$ und N endlich erzeugte $\mathcal{o}$-Module. Mit $\alpha_1, \ldots, \alpha_s$ als System von Erzeugenden von N, dann

$$\alpha_i = \sum_j a_{ij}\alpha_j \quad \text{für } a_{ij} \in \mathfrak{p}$$

Sei A die Matrix $(a_{ij}) - I$, wo I ist die unitäre Matrix mit Rank s, und sei B die adjunkte Matrix von A, deren Elementen die Unterdeterminanten von Rank $(s-1)$ von A sind. Dann haben wir $A(\alpha_1, \ldots, \alpha_s)^T = 0$ und $BA = dI$, mit $d = \det(A)$. Also

$$0 = BA(\alpha_1, \ldots, \alpha_s)^T = (d\alpha_1, \ldots, d\alpha_s)^T$$

und also $dN = 0$, i.e. $d\mathcal{O} \subseteq M = \mathcal{o}\omega_1 + \cdots + \mathcal{o}\omega_m$. Wir haben $d \neq 0$, weil wir mit $d = \det((a_{ij}) - I)$ finden, dass $d \equiv (-1)^s \bmod \mathfrak{p}$, weil $a_{ij} \in \mathfrak{p}$. Es folgt, dass $L = dL = K\omega_1 + \cdots + K\omega_m$. $\omega_1, \ldots, \omega_m$ ist also eine Basis von L/K.

Um die zweite Identität zu zeigen, betrachten wir die absteigende Kette

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

von κ-Vektorräumen. Die sukzessive Quotienten $\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}$ in dieser Kette sind isomorph zu $\mathcal{O}/\mathfrak{P}_i$, für $\alpha \in \mathfrak{P}_i^{\nu} \backslash \mathfrak{P}_i^{\nu+1}$, dann hat der Homomorphismus

$$\mathcal{O} \longrightarrow \mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}, \quad a \mapsto a\alpha$$

Kern $\mathfrak{P}_i$ und ist surjektiv, weil $\mathfrak{P}_i^{\nu}$ der ggT von $\mathfrak{P}_i^{\nu+1}$ und $(\alpha) = \alpha\mathcal{O}$ ist, also $\mathfrak{P}_i^{\nu} = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$. Seit $f_i = [\mathcal{O}/\mathfrak{P}_i : \kappa]$, haben wir $\dim_\kappa(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = f_i$ und also

$$\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_\kappa(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = e_i f_i$$

□

Falls $p \in \mathbb{Z}$ eine Primzahl ist, so lässt sich das Ideal $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ faktorisieren. Nun ist $\mathfrak{P}_i \cap \mathbb{Z} = p\mathbb{Z}$. Entsprechend hat man eine Körpererweiterung von endlichen Körpern: $\mathcal{O}_K/\mathfrak{P}_i$ über $\mathbb{Z}/p\mathbb{Z}$. Sagen wir jene ist vom Grad f_i. Nun hat man $[K : \mathbb{Q}] = \sum_{i=1}^r e_i f_i$.
Im nächsten Satz Wählen wir $K = \mathbb{Q}(\theta)$ für eine ganz-algebraische Zahl θ mit Minimalpolynom $Q(X)$. Für die meisten Primzahlen p ist die Faktorisation $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ im Zusammenhang mit der Faktorisierung in $\mathbb{Z}/p\mathbb{Z}[X]$ von der Projektion von $Q(X)$ zu $(\mathbb{Z}/p\mathbb{Z})[X]$.

Satz 12. *Sei $\theta \in \mathbb{Z}_K$ eine ganze primitive Zahl von einem Zahlkörper $K = \mathbb{Q}(\theta)$ vom Grad n über $\mathbb{Q}$ und $d = \operatorname{disk}(1, \theta, \ldots, \theta^{n-1})$. Sei nun $p \in \mathbb{Z}$ eine Primzahl, welche zu d teilerfremd ist. Sei $Q(X) \in \mathbb{Z}[X]$ das Minimalpolynom von θ und nehme an, dass die Reduktion $\overline{Q}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ sich wie folgt*

$$\overline{Q}(X) = \overline{Q}_1(X)^{e_1} \cdots \overline{Q}_r(X)^{e_r}$$

in irreduzible, paarweise teilerfemde Polynome $\overline{Q}_i(X)$ zerlegt. Seien ferner $Q_i(X) \in \mathbb{Z}[X]$ Polynome, welche sich auf $\overline{Q}_i$ reduzieren, dann sind

$$\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$$

die verschiedenen über (p) liegenden Primideale von $\mathbb{Z}_K$. Ferner ist der Trägheitsgrad von $\mathfrak{P}_i$ über (p) gleich dem Grad von $\overline{Q}_i(X)$ und es gilt

$$p\mathbb{Z}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Beweis. Wir zeigen die Isomorphismen

$$\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$$

Wir anfangen mit dem ersten. $1, \theta, \ldots, \theta^{n-1}$ bildet eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\theta]$. $d = \operatorname{disk}(1, \theta, \ldots, \theta^{n-1}) = \det(\operatorname{tr}(\theta^{i+j})_{i,j=0,\ldots,n-1})$, also gilt $\mathbb{Z}[\theta] \subseteq \mathbb{Z}_K \subseteq \frac{1}{d}\mathbb{Z}[\theta]$. Falls nun $(d, p) = 1$, dann ist d invertierbar in $\mathbb{Z}/p\mathbb{Z}$, daraus folgt dann, dass die Abbildung $\mathbb{Z}[\theta] \to \mathbb{Z}_K \to \mathbb{Z}_K/p\mathbb{Z}_K$ surjektiv ist mit Kern $p\mathbb{Z}[\theta]$ und somit $\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathbb{Z}[X]/(p, Q(X))$.

Der zweite Isomorphismus ist aus dem surjektiven Homomorphismus

$$\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$$

ableitbar. Sein Kern ist das Ideal erzeugt von p und $Q(X)$, und aus $\mathbb{Z}[\theta] = \mathbb{Z}[X]/(Q(X))$, haben wir $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$.

Seit $\overline{Q}(X) = \prod_{i=1}^r \overline{Q}_i(X)^{e_i}$, der Chinesiche Restsatz besagt endlich, dass

$$(\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X)) \cong \bigoplus_{i=1}^r (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}_i(X))^{e_i}$$

Dies zeigt, dass die Primideale des Rings $R = (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$ die Hauptideale $(\overline{Q}_i)$ sind, die erzeugt von den $\overline{Q}_i(X) \bmod \overline{Q}(X)$, für $i = 1, \ldots, r$, sind. Dies zeigt auch, dass der Grad

$[R/(\overline{Q}_i) : \mathbb{Z}/p\mathbb{Z}]$ gleich der Grad von $\overline{Q}_i(X)$ ist, und

$$(0) = (\overline{Q}) = \bigcap_{i=1}^{r} (\overline{Q}_i)^{e_i}$$

Aus dem Isomorphismus $(\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X)) \cong \mathbb{Z}_K/p\mathbb{Z}_K$, $f(X) \mapsto f(\theta)$, gilt das gleiche für $\mathbb{Z}_K/p\mathbb{Z}_K$. Also sind die Primideale $\overline{\mathfrak{P}}_i$ von $\mathbb{Z}_K/p\mathbb{Z}_K$ die Primideale $(\overline{Q}_i)$, und sie sind die Primideale erzeugt von den $Q_i(\theta) \bmod p\mathbb{Z}_K$. Der Grad $[(\mathbb{Z}_K/p\mathbb{Z}_K)/\overline{\mathfrak{P}}_i : \mathbb{Z}/p\mathbb{Z}]$ ist der Grad des Polynoms $\overline{Q}_i(X)$, und wir haben $(0) = \bigcap_{i=1}^{r} \overline{\mathfrak{P}}_i^{e_i}$. Jetzt sei $\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$ das Vorbild von $\overline{\mathfrak{P}}_i$ bezüglich dem Homomorphismus

$$\mathbb{Z}_K \longrightarrow \mathbb{Z}_K/p\mathbb{Z}_K$$

Dann, für $i = 1, \ldots, r$, variiert $\mathfrak{P}_i$ über den Primidealen von $\mathbb{Z}_K$ über p. $f_i = [\mathbb{Z}_K/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}]$ ist der Grad des Polynoms $\overline{Q}_i(X)$. Ausserdem ist $\mathfrak{P}_i^{e_i}$ das Vorbild von $\overline{\mathfrak{P}}_i^{e_i}$ (weil $e_i = \#\{\overline{\mathfrak{P}}^{\nu} \mid \nu \in \mathbb{N}\}$), und $p\mathbb{Z}_K \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$ so, dass $p\mathbb{Z}_K | \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ und folglich $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, weil $\sum_i e_i f_i = n$. □

Bemerkung 13. Desweiteren kann man auch zeigen, dass $d = (-1)^{n(n-1)/2}\mathrm{disk}(Q(X)) = \mathrm{Res}(Q(X), \frac{d}{dX}Q(X))$ gilt. Da nun $(p, d) = 1$ gilt, folgt, dass $\overline{Q}(X) \in \mathbb{Z}/p\mathbb{Z}$ keine mehrfache Nullstelle hat, insbesondere folgt sogar, dass alle $e_i = 1$ und somit p ist unverzweigt.

Beispiel 14. *$\theta = \sqrt[3]{2}$ hat Minimalpolynom $Q(X) = X^3 - 2 \in \mathbb{Z}[X]$.*
Wir bemerken, dass $X^3 - 2 \equiv (X + 2)(X^2 + 3X + 4) \mod (5)$ wobei beide Faktoren irreduzibel in $\mathbb{Z}/5\mathbb{Z}[X]$ sind. Ferner sind 5 und die Diskriminante $d = -108$ von $Q(X)$ teilerfremd. Daraus folgt

$$5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} = \mathfrak{P}_1\mathfrak{P}_2 = \left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{2} + 2)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right)\left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{4} + 3\sqrt[3]{2} + 4)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right)$$

mit Trägheitsgraden $f_1 = 1$ und $f_2 = 2$.

References

[1] A. Schmidt, Einfuhrung in die algebraische Zahlentheorie. Springer, Berlin, 2007

Email address: acasetta@student.ethz.ch