§3.2 Zerlegung von Primzahlen in Zahlkörpern

Bemerkung. Ein wesentlicher Grund für die Betrachtung von Gittern und vor allem multiplikativen Gittern ist, dass sie oftmals „einfacher“ sind als der Zahlring

Bemerkung. Ein wesentlicher Grund für die Betrachtung von Gittern und vor allem multiplikativen Gittern ist, dass sie oftmals „einfacher“ sind als der Zahlring (zum Beispiel ist für $d \in \not\square_1$ das multiplikative Gitter $\mathbb{Z}[\sqrt{d}]$ „einfacher“ als $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathscr{O}_d$)

Bemerkung. Ein wesentlicher Grund für die Betrachtung von Gittern und vor allem multiplikativen Gittern ist, dass sie oftmals „einfacher“ sind als der Zahlring (zum Beispiel ist für $d \in \not\square_1$ das multiplikative Gitter $\mathbb{Z}[\sqrt{d}]$ „einfacher“ als $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathscr{O}_d$) und für gewisse Zwecke doch den Zahlring ersetzen können.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$,

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$. Insbesondere gilt $m\mathscr{O}_K \subseteq I$ und man kann I sehen als m zusammen mit dem Bild von I unter $\mathscr{O}_K \to \mathscr{O}_K/m\mathscr{O}_K$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$. Insbesondere gilt $m\mathscr{O}_K \subseteq I$ und man kann I sehen als m zusammen mit dem Bild von I unter $\mathscr{O}_K \to \mathscr{O}_K/m\mathscr{O}_K$.

Ein Ideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine natürliche Zahl m und ein Ideal des endlichen Rings $\mathscr{O}_K/m\mathscr{O}_K = (\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n)/(m\mathbb{Z}x_1 + \cdots + m\mathbb{Z}x_n)$,

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$. Insbesondere gilt $m\mathscr{O}_K \subseteq I$ und man kann I sehen als m zusammen mit dem Bild von I unter $\mathscr{O}_K \to \mathscr{O}_K/m\mathscr{O}_K$.

Ein Ideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine natürliche Zahl m und ein Ideal des endlichen Rings $\mathscr{O}_K/m\mathscr{O}_K = (\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n)/(m\mathbb{Z}x_1 + \cdots + m\mathbb{Z}x_n)$, dessen additive Gruppe in natürlicher Weise ein freier $\mathbb{Z}/m\mathbb{Z}$-Modul mit Basis $\overline{x_1}, \ldots, \overline{x_n}$ ist.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathscr{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$. Insbesondere gilt $m\mathscr{O}_K \subseteq I$ und man kann I sehen als m zusammen mit dem Bild von I unter $\mathscr{O}_K \to \mathscr{O}_K/m\mathscr{O}_K$.

Ein Ideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine natürliche Zahl m und ein Ideal des endlichen Rings $\mathscr{O}_K/m\mathscr{O}_K = (\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n)/(m\mathbb{Z}x_1 + \cdots + m\mathbb{Z}x_n)$, dessen additive Gruppe in natürlicher Weise ein freier $\mathbb{Z}/m\mathbb{Z}$-Modul mit Basis $\overline{x_1}, \dots, \overline{x_n}$ ist.

Insbesondere ist $\mathscr{O}_K/I$ endlich mit $\#(\mathscr{O}_K/I) \mid m^n$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(b) Sei $m \in \mathbb{N}$. In Anbetracht von (a) ist der m^n-elementige Ring $\mathscr{O}_K/m\mathscr{O}_K$ von besonderem Interesse.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(b) Sei $m \in \mathbb{N}$. In Anbetracht von (a) ist der m^n-elementige Ring $\mathscr{O}_K/m\mathscr{O}_K$ von besonderem Interesse. Um diesen zu kennen, braucht man aber den Zahlring $\mathscr{O}_K$ oft gar nicht genau zu kennen.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(b) Sei $m \in \mathbb{N}$. In Anbetracht von (a) ist der m^n-elementige Ring $\mathscr{O}_K/m\mathscr{O}_K$ von besonderem Interesse. Um diesen zu kennen, braucht man aber den Zahlring $\mathscr{O}_K$ oft gar nicht genau zu kennen. Es reicht, ein multiplikatives Gitter M in K zu kennen mit $(m, [\mathscr{O}_K : M]) = (1)$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(b) Sei $m \in \mathbb{N}$. In Anbetracht von (a) ist der m^n-elementige Ring $\mathscr{O}_K/m\mathscr{O}_K$ von besonderem Interesse. Um diesen zu kennen, braucht man aber den Zahlring $\mathscr{O}_K$ oft gar nicht genau zu kennen. Es reicht, ein multiplikatives Gitter M in K zu kennen mit $\boxed{(m, [\mathscr{O}_K : M]) = (1)}$. Dann gibt es $s, t \in \mathbb{Z}$ mit $sm + t[\mathscr{O}_K : M] = 1$. Für jedes $x \in \mathscr{O}_K$ gilt dann

$$x = 1 \cdot x = s \underbrace{mx}_{\in m\mathscr{O}_K} + t \underbrace{[\mathscr{O}_K : M]x}_{\in M},$$

weshalb der kanonische Homomorphismus $M/mM \to \mathscr{O}_K/m\mathscr{O}_K$ surjektiv ist.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(b) Sei $m \in \mathbb{N}$. In Anbetracht von (a) ist der m^n-elementige Ring $\mathscr{O}_K/m\mathscr{O}_K$ von besonderem Interesse. Um diesen zu kennen, braucht man aber den Zahlring $\mathscr{O}_K$ oft gar nicht genau zu kennen. Es reicht, ein multiplikatives Gitter M in K zu kennen mit $\boxed{(m, [\mathscr{O}_K : M]) = (1)}$. Dann gibt es $s, t \in \mathbb{Z}$ mit $sm + t[\mathscr{O}_K : M] = 1$. Für jedes $x \in \mathscr{O}_K$ gilt dann

$$x = 1 \cdot x = s \underbrace{mx}_{\in m\mathscr{O}_K} + t \underbrace{[\mathscr{O}_K : M]x}_{\in M},$$

weshalb der kanonische Homomorphismus $M/mM \to \mathscr{O}_K/m\mathscr{O}_K$ surjektiv ist. Wegen $M/mM \overset{M \text{ Gitter}}{=} m^n = \#\mathscr{O}_K/m\mathscr{O}_K$ ist dieser auch injektiv und wir haben eine kanonische Isomorphie

$$M/mM \cong \mathscr{O}_K/m\mathscr{O}_K.$$

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(c) Wir spezialisieren das unter (a) und (b) Gesagte auf Primideale. Sei $\mathfrak{p} \in M_{\mathscr{O}_K}$. Dann gibt es genau ein $p \in \mathbb{P}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Insbesondere $p\mathscr{O}_K \subseteq \mathfrak{p}$ und man kann $\mathfrak{p}$ sehen als p zusammen mit dem Bild von $\mathfrak{p}$ unter $\mathscr{O}_K \to \mathscr{O}_K/p\mathscr{O}_K$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(c) Wir spezialisieren das unter (a) und (b) Gesagte auf Primideale. Sei $\mathfrak{p} \in M_{\mathscr{O}_K}$. Dann gibt es genau ein $p \in \mathbb{P}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Insbesondere $p\mathscr{O}_K \subseteq \mathfrak{p}$ und man kann $\mathfrak{p}$ sehen als p zusammen mit dem Bild von $\mathfrak{p}$ unter $\mathscr{O}_K \to \mathscr{O}_K / p\mathscr{O}_K$.

Ein Primideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine Primzahl p und ein Primideal des endlichen Ringes $\mathscr{O}_K / p\mathscr{O}_K$, dessen additive Gruppe in natürlicher Weise ein $\mathbb{F}_p$-Vektorraum mit Basis $\overline{x_1}, \dots, \overline{x_n}$ ist.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(c) Wir spezialisieren das unter (a) und (b) Gesagte auf Primideale. Sei $\mathfrak{p} \in M_{\mathscr{O}_K}$. Dann gibt es genau ein $p \in \mathbb{P}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Insbesondere $p\mathscr{O}_K \subseteq \mathfrak{p}$ und man kann $\mathfrak{p}$ sehen als p zusammen mit dem Bild von $\mathfrak{p}$ unter $\mathscr{O}_K \to \mathscr{O}_K/p\mathscr{O}_K$.

Ein Primideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine Primzahl p und ein Primideal des endlichen Ringes $\mathscr{O}_K/p\mathscr{O}_K$, dessen additive Gruppe in natürlicher Weise ein $\mathbb{F}_p$-Vektorraum mit Basis $\overline{x_1}, \ldots, \overline{x_n}$ ist.

Insbesondere ist $\#(\mathscr{O}_K/\mathfrak{p}) \in \{p, p^2, \ldots, p^n\}$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(c) Wir spezialisieren das unter (a) und (b) Gesagte auf Primideale. Sei $\mathfrak{p} \in M_{\mathscr{O}_K}$. Dann gibt es genau ein $p \in \mathbb{P}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Insbesondere $p\mathscr{O}_K \subseteq \mathfrak{p}$ und man kann $\mathfrak{p}$ sehen als p zusammen mit dem Bild von $\mathfrak{p}$ unter $\mathscr{O}_K \to \mathscr{O}_K/p\mathscr{O}_K$.

Ein Primideal $\neq (0)$ des Zahlrings $\mathscr{O}_K$ ist also gegeben durch eine Primzahl p und ein Primideal des endlichen Ringes $\mathscr{O}_K/p\mathscr{O}_K$, dessen additive Gruppe in natürlicher Weise ein $\mathbb{F}_p$-Vektorraum mit Basis $\overline{x_1}, \ldots, \overline{x_n}$ ist.

Insbesondere ist $\#(\mathscr{O}_K/\mathfrak{p}) \in \{p, p^2, \ldots, p^n\}$.

Ist M ein multiplikatives Gitter in K mit $\boxed{p \nmid [\mathscr{O}_K : M]}$, so gilt kanonisch $M/pM \cong \mathscr{O}_K/p\mathscr{O}_K$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen. Dann ist $\mathbb{Z}[a]$ ein multiplikatives Gitter in K.

Setze $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Q}[X]$. Dann $f \in \mathbb{Z}[X]$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen. Dann ist $\mathbb{Z}[a]$ ein multiplikatives Gitter in K.

Setze $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Q}[X]$. Dann $f \in \mathbb{Z}[X]$. Da f normiert ist, gilt $f\mathbb{Q}[X] \cap \mathbb{Z}[X] = f\mathbb{Z}[X]$ (benutze zum Beispiel das Lemma von Gauß). Daher kanonisch $\mathbb{Z}[X]/(f) \hookrightarrow \mathbb{Q}[X]/(f)$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen. Dann ist $\mathbb{Z}[a]$ ein multiplikatives Gitter in K.

Setze $f := \mathrm{irr}_{\mathbb{Q}}(a) \in \mathbb{Q}[X]$. Dann $f \in \mathbb{Z}[X]$. Da f normiert ist, gilt $f\mathbb{Q}[X] \cap \mathbb{Z}[X] = f\mathbb{Z}[X]$ (benutze zum Beispiel das Lemma von Gauß). Daher kanonisch $\mathbb{Z}[X]/(f) \hookrightarrow \mathbb{Q}[X]/(f)$. Bezeichne $\mathbb{Z}[X] \to \mathbb{F}_p[X],\ g \mapsto \overline{g}$ den Homomorphismus mit $\overline{m} = \overline{m}^{(p)}$ ($m \in \mathbb{Z}$) und $\overline{X} = X$. Dann liegt $\overline{f}$ im Kern des Epimorphismus $\mathbb{F}_p[X] \to \mathbb{Z}[a]/p\mathbb{Z}[a]$ mit $X \mapsto \overline{a}$.

Da f normiert ist, gilt $\deg \overline{f} = \deg f = n$ und daher
$\#(\mathbb{F}_p[X]/(\overline{f})) = p^n \overset{\mathbb{Z}[a] \text{ Gitter}}{=} \#(\mathbb{Z}[a]/p\mathbb{Z}[a])$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen. Dann ist $\mathbb{Z}[a]$ ein multiplikatives Gitter in K.

Setze $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Q}[X]$. Dann $f \in \mathbb{Z}[X]$. Da f normiert ist, gilt $f\mathbb{Q}[X] \cap \mathbb{Z}[X] = f\mathbb{Z}[X]$ (benutze zum Beispiel das Lemma von Gauß). Daher kanonisch $\mathbb{Z}[X]/(f) \hookrightarrow \mathbb{Q}[X]/(f)$. Bezeichne $\mathbb{Z}[X] \to \mathbb{F}_p[X],\ g \mapsto \overline{g}$ den Homomorphismus mit $\overline{m} = \overline{m}^{(p)}$ ($m \in \mathbb{Z}$) und $\overline{X} = X$. Dann liegt $\overline{f}$ im Kern des Epimorphismus $\mathbb{F}_p[X] \to \mathbb{Z}[a]/p\mathbb{Z}[a]$ mit $X \mapsto \overline{a}$.

Da f normiert ist, gilt $\deg \overline{f} = \deg f = n$ und daher $\#(\mathbb{F}_p[X]/(\overline{f})) = p^n \overset{\mathbb{Z}[a] \text{ Gitter}}{=} \#(\mathbb{Z}[a]/p\mathbb{Z}[a])$. Daher haben wir $\mathbb{F}_p[X]/(\overline{f}) \underset{\overline{X} \mapsto \overline{a}}{\overset{\cong}{\to}} \mathbb{Z}[a]/p\mathbb{Z}[a]$.

Bemerkung. Sei K ein Zahlkörper und $x_1, \dots, x_n$ eine $\mathbb{Z}$-Basis von $\mathscr{O}_K$.

(d) Nach dem Satz vom primitiven Element gibt es $a \in K$ mit $K = \mathbb{Q}(a)$. Wegen $K = (\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_K$ kann man leicht $a \in \mathscr{O}_K$ wählen. Dann ist $\mathbb{Z}[a]$ ein multiplikatives Gitter in K.

Setze $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Q}[X]$. Dann $f \in \mathbb{Z}[X]$. Da f normiert ist, gilt $f\mathbb{Q}[X] \cap \mathbb{Z}[X] = f\mathbb{Z}[X]$ (benutze zum Beispiel das Lemma von Gauß). Daher kanonisch $\mathbb{Z}[X]/(f) \hookrightarrow \mathbb{Q}[X]/(f)$. Bezeichne $\mathbb{Z}[X] \to \mathbb{F}_p[X],\ g \mapsto \overline{g}$ den Homomorphismus mit $\overline{m} = \overline{m}^{(p)}$ $(m \in \mathbb{Z})$ und $\overline{X} = X$. Dann liegt $\overline{f}$ im Kern des Epimorphismus $\mathbb{F}_p[X] \to \mathbb{Z}[a]/p\mathbb{Z}[a]$ mit $X \mapsto \overline{a}$.

Da f normiert ist, gilt $\deg \overline{f} = \deg f = n$ und daher $\#(\mathbb{F}_p[X]/(\overline{f})) = p^n \overset{\mathbb{Z}[a] \text{ Gitter}}{=} \#(\mathbb{Z}[a]/p\mathbb{Z}[a])$. Daher haben wir $\mathbb{F}_p[X]/(\overline{f}) \underset{\overline{X} \mapsto \overline{a}}{\overset{\cong}{\to}} \mathbb{Z}[a]/p\mathbb{Z}[a]$. Falls $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, so haben wir auch noch kanonisch $\mathbb{Z}[a]/p\mathbb{Z}[a] \cong \mathscr{O}_K/p\mathscr{O}_K$ und es ergibt sich folgendes kommutative Diagramm:

Bemerkung. Sei K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.

(d)

$$
\begin{tikzcd}
\mathbb{Q}[X]/(f) \arrow[r, "\cong", "\overline{X}\mapsto a"'] & K & \\
& & \mathcal{O}_K \arrow[ul, hook', "\supseteq"'] \arrow[dd, two heads] \\
\mathbb{Z}[X]/(f) \arrow[uu, hook] \arrow[r, "\cong", "\overline{X}\mapsto a"'] \arrow[d, two heads] & \mathbb{Z}[a] \arrow[ur, hook, "\subseteq"] \arrow[d, two heads] & \\
\mathbb{F}_p[X]/(\overline{f}) \arrow[r, "\cong", "\overline{X}\mapsto \overline{a}"'] & \mathbb{Z}[a]/p\mathbb{Z}[a] \arrow[r, "\begin{array}{c}\boxed{p \nmid [\mathcal{O}_K : \mathbb{Z}[a]]} \\ \Downarrow \\ \cong\end{array}"] & \mathcal{O}_K/p\mathcal{O}_K
\end{tikzcd}
$$

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \mathrm{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Da $\mathbb{F}_p[X]$ ein Hauptidealring ist, sind die verschiedenen Primideale darin, die $(\overline{f})$ enthalten, genau die $(\overline{g_1}), \ldots, (\overline{g_m})$. Deren Bilder $(\overline{g_1(a)}), \ldots, (\overline{g_m(a)})$ unter $\varphi\colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K,\ \overline{X} \mapsto \overline{a}$ sind genau die verschiedenen Primideale von $\mathscr{O}_K/p\mathscr{O}_K$.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Da $\mathbb{F}_p[X]$ ein Hauptidealring ist, sind die verschiedenen Primideale darin, die $(\overline{f})$ enthalten, genau die $(\overline{g_1}), \dots, (\overline{g_m})$. Deren Bilder $(\overline{g_1(a)}), \dots, (\overline{g_m(a)})$ unter $\varphi\colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K,\ \overline{X} \mapsto \overline{a}$ sind genau die verschiedenen Primideale von $\mathscr{O}_K/p\mathscr{O}_K$. Daher sind $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ als deren Urbilder unter $\mathscr{O}_K \to \mathscr{O}_K/p\mathscr{O}_K$ genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \ldots, m\}$ folgt $e_1, \ldots, e_m, f_1, \ldots, f_m \in \mathbb{N}$, $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \ldots, m\}$ folgt $e_1, \ldots, e_m, f_1, \ldots, f_m \in \mathbb{N}$, $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) : \mathbb{F}_p]$ und $\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) \cong (\mathscr{O}_K/p\mathscr{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als Ring

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \dots, m\}$ folgt $e_1, \dots, e_m, f_1, \dots, f_m \in \mathbb{N}$, $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) : \mathbb{F}_p]$ und $\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) \cong (\mathscr{O}_K/p\mathscr{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als abelsche Gruppe

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \ldots, m\}$ folgt $e_1, \ldots, e_m, f_1, \ldots, f_m \in \mathbb{N}$, $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) : \mathbb{F}_p]$ und $\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) \cong (\mathscr{O}_K/p\mathscr{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als $\mathbb{Z}$-Modul

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathcal{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathcal{O}_K + p\mathcal{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathcal{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathcal{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathcal{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \ldots, m\}$ folgt $e_1, \ldots, e_m, f_1, \ldots, f_m \in \mathbb{N}$, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathcal{O}_K/(g_i(a)\mathcal{O}_K + p\mathcal{O}_K) : \mathbb{F}_p]$ und $\mathcal{O}_K/(g_i(a)\mathcal{O}_K + p\mathcal{O}_K) \cong (\mathcal{O}_K/p\mathcal{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als $\mathbb{Z}/(p)$-Modul

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathcal{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathcal{O}_K + p\mathcal{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathcal{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathcal{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathcal{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \dots, m\}$ folgt $e_1, \dots, e_m, f_1, \dots, f_m \in \mathbb{N}$, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathcal{O}_K/(g_i(a)\mathcal{O}_K + p\mathcal{O}_K) : \mathbb{F}_p]$ und $\mathcal{O}_K/(g_i(a)\mathcal{O}_K + p\mathcal{O}_K) \cong (\mathcal{O}_K/p\mathcal{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als $\mathbb{F}_p$-Vektorraum.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind genau die verschiedenen Primideale von $\mathscr{O}_K$, die (p) enthalten. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i)$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i)$ für $i \in \{1, \ldots, m\}$ folgt $e_1, \ldots, e_m, f_1, \ldots, f_m \in \mathbb{N}$, $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Es gilt $f_i = [\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) : \mathbb{F}_p]$ und $\mathscr{O}_K/(g_i(a)\mathscr{O}_K + p\mathscr{O}_K) \cong (\mathscr{O}_K/p\mathscr{O}_K)/(\overline{g_i(a)}) \cong \mathbb{F}_p[X]/(\overline{g_i})$ als $\mathbb{F}_p$-Vektorraum. Somit $f_i = \deg \overline{g_i}$.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i) \geq 1$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$ für $i \in \{1, \dots, n\}$ gilt $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i) \geq 1$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$ für $i \in \{1, \ldots, n\}$ gilt $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Wendet man $\varphi \colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K$, $\overline{X} \mapsto \overline{a}$ auf die Gleichung $f = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m}$ an, so erhält man $\overline{g_1(a)}^{\alpha_1} \cdots \overline{g_m(a)}^{\alpha_m} = 0$ in $\mathscr{O}_K/p\mathscr{O}_K$, also $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} \subseteq p\mathscr{O}_K$,

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \ldots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \ldots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \ldots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i) \geq 1$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$ für $i \in \{1, \ldots, n\}$ gilt $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Wendet man $\varphi \colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K$, $\overline{X} \mapsto \overline{a}$ auf die Gleichung $f = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m}$ an, so erhält man $\overline{g_1(a)}^{\alpha_1} \cdots \overline{g_m(a)}^{\alpha_m} = 0$ in $\mathscr{O}_K/p\mathscr{O}_K$, also $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} \subseteq p\mathscr{O}_K$, das heißt $1 \leq e_i = \widetilde{v}_{\mathfrak{p}_i}(p\mathscr{O}_K) \leq \alpha_i$ für alle $i \in \{1, \ldots, m\}$.

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $\boxed{p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i) \geq 1$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$ für $i \in \{1, \dots, n\}$ gilt $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Wendet man $\varphi\colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K$, $\overline{X} \mapsto \overline{a}$ auf die Gleichung $f = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m}$ an, so erhält man $\overline{g_1(a)}^{\alpha_1} \cdots \overline{g_m(a)}^{\alpha_m} = 0$ in $\mathscr{O}_K/p\mathscr{O}_K$, also $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} \subseteq p\mathscr{O}_K$, das heißt $1 \leq e_i = \widetilde{v}_{\mathfrak{p}_i}(p\mathscr{O}_K) \leq \alpha_i$ für alle $i \in \{1, \dots, m\}$. Es folgt $n = \sum_{i=1}^m e_i f_i \leq \sum_{i=1}^m \alpha_i f_i = \sum_{i=1}^m \alpha_i \deg(\overline{g_i}) = n$

Satz. Seien $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $p \in \mathbb{P}$ mit $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, $f := \operatorname{irr}_{\mathbb{Q}}(a) \in \mathbb{Z}[X]$, $m \in \mathbb{N}$, $g_1, \dots, g_m \in \mathbb{Z}[X]$ und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ mit

$$\overline{f} = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m} \qquad \text{in } \mathbb{F}_p[X],$$

wobei $\overline{g_1}, \dots, \overline{g_m}$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{F}_p[X]$ seien. Dann ist $\mathfrak{p}_i := g_i(a)\mathscr{O}_K + p\mathscr{O}_K$ für jedes $i \in \{1, \dots, m\}$ ein Primideal von $\mathscr{O}_K[X]$ mit Trägheitsindex $f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ sind paarweise verschieden und es gilt

$$p\mathscr{O}_K = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}.$$

Beweis. Mit $e_i := e_{\mathbb{Z}}(\mathfrak{p}_i) \geq 1$ und $f_i := f_{\mathbb{Z}}(\mathfrak{p}_i) = \deg \overline{g_i}$ für $i \in \{1, \dots, n\}$ gilt $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ und $\sum_{i=1}^m e_i f_i = n := [K : \mathbb{Q}] = \deg f = \deg \overline{f}$. Wendet man $\varphi \colon \mathbb{F}_p[X]/(\overline{f}) \to \mathscr{O}_K/p\mathscr{O}_K$, $\overline{X} \mapsto \overline{a}$ auf die Gleichung $f = \overline{g_1}^{\alpha_1} \cdots \overline{g_m}^{\alpha_m}$ an, so erhält man $\overline{g_1(a)}^{\alpha_1} \cdots \overline{g_m(a)}^{\alpha_m} = 0$ in $\mathscr{O}_K/p\mathscr{O}_K$, also $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} \subseteq p\mathscr{O}_K$, das heißt $1 \leq e_i = \widetilde{v}_{\mathfrak{p}_i}(p\mathscr{O}_K) \leq \alpha_i$ für alle $i \in \{1, \dots, m\}$. Es folgt $n = \sum_{i=1}^m e_i f_i \leq \sum_{i=1}^m \alpha_i f_i = \sum_{i=1}^m \alpha_i \deg(\overline{g_i}) = n$ und daher $e_i = \alpha_i$ für alle $i \in \{1, \dots, m\}$.

Bemerkung. Sei $K = \mathbb{Q}(a)$ ein Zahlkörper, a ganz über $\mathbb{Z}$, $f := \mathrm{irr}_{\mathbb{Q}}(a)$ und $p \in \mathbb{P}$ mit $p^2 \nmid N_{K|\mathbb{Q}}(f'(a))$. Dann $p \nmid [\mathscr{O}_K : \mathbb{Z}[a]]$, denn

$$|N_{K|\mathbb{Q}}(f'(a))| = |d(\mathbb{Z}[a])| = [\mathscr{O}_K : \mathbb{Z}[a]]^2 |d(\mathscr{O}_K)|.$$

Beispiel. Sei $d \in \mathbb{Z}$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Setze $f := \operatorname{irr}_{\mathbb{Q}}(\sqrt{d})$. Es gilt

$$N_{K|\mathbb{Q}}(f'(\sqrt{d})) = (\sqrt{d} - (-\sqrt{d}))((-\sqrt{d}) - \sqrt{d}) = -4d,$$

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und

$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Setze $f := \operatorname{irr}_{\mathbb{Q}}(\sqrt{d})$. Es gilt

$$N_{K|\mathbb{Q}}(f'(\sqrt{d})) = (\sqrt{d} - (-\sqrt{d}))((-\sqrt{d}) - \sqrt{d}) = -4d,$$

also $\boxed{p^2 \nmid N_{K|\mathbb{Q}}(f'(\sqrt{d}))}$ für alle $p \in \mathbb{P} \setminus \{2\}$.

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Setze $f := \operatorname{irr}_{\mathbb{Q}}(\sqrt{d})$. Es gilt

$$N_{K|\mathbb{Q}}(f'(\sqrt{d})) = (\sqrt{d} - (-\sqrt{d}))((-\sqrt{d}) - \sqrt{d}) = -4d,$$

also $\boxed{p^2 \nmid N_{K|\mathbb{Q}}(f'(\sqrt{d}))}$ für alle $p \in \mathbb{P} \setminus \{2\}$. Wegen der vorherigen Bemerkung können wir für $p \in \mathbb{P} \setminus \{2\}$ den Satz mit $a := \sqrt{d}$ anwenden.

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K") und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K") und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K") und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Setze $f := \mathrm{irr}_{\mathbb{Q}}(\sqrt{d})$. Es gilt

$$N_{K|\mathbb{Q}}(f'(\sqrt{d})) = (\sqrt{d} - (-\sqrt{d}))((-\sqrt{d}) - \sqrt{d}) = -4d,$$

also $\boxed{p^2 \nmid N_{K|\mathbb{Q}}(f'(\sqrt{d}))}$ für alle $p \in \mathbb{P} \setminus \{2\}$. Wegen der vorherigen Bemerkung können wir für $p \in \mathbb{P} \setminus \{2\}$ den Satz mit $a := \sqrt{d}$ anwenden. Für $p = 2$ können wir im Fall $d \in \not\square_{2,3}$ wegen $\mathscr{O}_K = \mathbb{Z}[\sqrt{d}]$ immer noch $a := \sqrt{d}$ setzen,

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Setze $f := \operatorname{irr}_{\mathbb{Q}}(\sqrt{d})$. Es gilt

$$N_{K|\mathbb{Q}}(f'(\sqrt{d})) = (\sqrt{d} - (-\sqrt{d}))((-\sqrt{d}) - \sqrt{d}) = -4d,$$

also $\boxed{p^2 \nmid N_{K|\mathbb{Q}}(f'(\sqrt{d}))}$ für alle $p \in \mathbb{P} \setminus \{2\}$. Wegen der vorherigen Bemerkung können wir für $p \in \mathbb{P} \setminus \{2\}$ den Satz mit $a := \sqrt{d}$ anwenden. Für $p = 2$ können wir im Fall $d \in \not\square_{2,3}$ wegen $\mathscr{O}_K = \mathbb{Z}[\sqrt{d}]$ immer noch $a := \sqrt{d}$ setzen, während wir im Fall $d \in \not\square_1$ die kompliziertere Wahl $a := \frac{1+\sqrt{d}}{2}$ treffen müssen (beachte $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\frac{1+\sqrt{d}}{2})$).

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Fall 1 $p \in \mathbb{P} \setminus \{2\}$

Setze $a := \sqrt{d}$, $f := \mathrm{irr}_{\mathbb{Q}}(a) = X^2 - d$.

Fall 1.1 $\overline{d}$ ist ein Quadrat in $\mathbb{F}_p$.

Wähle $c \in \mathbb{Z}$ mit $\overline{d} = \overline{c}^2$ in $\mathbb{F}_p$.
Dann $\overline{f} = (X - \overline{c})(X + \overline{c})$ in $\mathbb{F}_p[X]$.

Fall 1.1.1 $p \mid d$

$\overline{c} = \overline{d} = 0$ und $\overline{f} = X^2$ in $\mathbb{F}_p[X]$

$p\mathscr{O}_K = \underbrace{(\sqrt{d}, p)}_{\in M_{\mathscr{O}_K}}{}^2 \rightsquigarrow$ verzweigt

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K") und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K") und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K") und

$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Fall 1 $p \in \mathbb{P} \setminus \{2\}$

Setze $a := \sqrt{d}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - d$.

Fall 1.1 $\overline{d}$ ist ein Quadrat in $\mathbb{F}_p$.

Wähle $c \in \mathbb{Z}$ mit $\overline{d} = \overline{c}^2$ in $\mathbb{F}_p$.
Dann $\overline{f} = (X - \overline{c})(X + \overline{c})$ in $\mathbb{F}_p[X]$.

Fall 1.1.2 $p \nmid d$

$\overline{c} \neq 0$, da $\overline{d} \neq 0$ in $\mathbb{F}_p$
$\overline{c} \neq -\overline{c}$ in $\mathbb{F}_p$, da $\overline{2} \in \mathbb{F}_p^\times$ (beachte $p \neq 2$)
$p\mathscr{O}_K = \underbrace{(\sqrt{d} - c, p)}_{\in M_{\mathscr{O}_K}}\underbrace{(\sqrt{d} + c, p)}_{\in M_{\mathscr{O}_K}} \rightsquigarrow$ zerlegt

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K") und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K") und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K") und

$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Fall 1 $p \in \mathbb{P} \setminus \{2\}$

Setze $a := \sqrt{d}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - d$.

Fall 1.2 $\overline{d}$ ist kein Quadrat in $\mathbb{F}_p$.

Dann $\overline{f}$ irreduzibel in $\mathbb{F}_p[X]$, also $p\mathscr{O}_K \in M_{\mathscr{O}_K}$. $\rightsquigarrow$ träge

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathscr{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathscr{O}_K}$ („p verzweigt in K“) und $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathscr{O}_K \in M_{\mathscr{O}_K}$ („p träge in K“) und $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathscr{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und

$$\mathscr{O}_K/\mathfrak{q}_1 \cong \mathscr{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Fall 2 $p = 2$

Fall 2.1 $d \in \not\square_{2,3}$

Setze $a := \sqrt{d}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - d$.

$\overline{f} = X^2 - \overline{d} = X^2 - \overline{d}^2 = (X - \overline{d})(X + \overline{d}) = (X - \overline{d})^2$ in $\mathbb{F}_2[X]$, also $2\mathscr{O}_K = \underbrace{(\sqrt{d} - d, 2)}_{\in M_{\mathscr{O}_K}}{}^2 \rightsquigarrow$ verzweigt

Fall 2.2 $d \in \not\square_1$

Setze $a := \frac{1+\sqrt{d}}{2}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - X - \frac{d-1}{4}$.

Fall 2.2.1 $d \equiv_{(8)} 1$

$\overline{f} = X^2 - X = X(X-1)$ in $\mathbb{F}_2[X]$, also

$2\mathscr{O}_K = \underbrace{(\sqrt{d}, 2)}_{\in M_{\mathscr{O}_K}}\underbrace{(\sqrt{d} - 1, 2)}_{\in M_{\mathscr{O}_K}} \rightsquigarrow$ zerlegt

Beispiel. Sei $d \in \not\square$, $p \in \mathbb{P}$ und $K := \mathbb{Q}(\sqrt{d})$. Da $K|\mathbb{Q}$ eine Galoiserweiterung vom Grad 2 ist, tritt genau einer der folgenden Fälle ein:

- $p\mathcal{O}_K = \mathfrak{q}^2$ mit $\mathfrak{q} \in M_{\mathcal{O}_K}$ („p verzweigt in K“) und $\mathcal{O}_K/\mathfrak{q} \cong \mathbb{F}_p$
- $p\mathcal{O}_K \in M_{\mathcal{O}_K}$ („p träge in K“) und $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^2}$
- $p\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1, \mathfrak{q}_2 \in M_{\mathcal{O}_K}$ und $\mathfrak{q}_1 \neq \mathfrak{q}_2$ („p zerlegt in K“) und
$$\mathcal{O}_K/\mathfrak{q}_1 \cong \mathcal{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_p.$$

Fall 2 $p = 2$

Fall 2.1 $d \in \not\square_{2,3}$

Setze $a := \sqrt{d}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - d$.
$\overline{f} = X^2 - \overline{d} = X^2 - \overline{d}^2 = (X - \overline{d})(X + \overline{d}) = (X - \overline{d})^2$ in $\mathbb{F}_2[X]$, also $2\mathcal{O}_K = \underbrace{(\sqrt{d} - d, 2)}_{\in M_{\mathcal{O}_K}}{}^2 \rightsquigarrow$ verzweigt

Fall 2.2 $d \in \not\square_1$

Setze $a := \frac{1+\sqrt{d}}{2}$, $f := \operatorname{irr}_{\mathbb{Q}}(a) = X^2 - X - \frac{d-1}{4}$.

Fall 2.2.2 $d \equiv_{(8)} 5$

$\overline{f} = X^2 - X - 1$ irreduzibel in $\mathbb{F}_2[X]$,
also $2\mathcal{O}_K \in M_{\mathcal{O}_K} \rightsquigarrow$ träge