LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT
Prof. Dr. Werner Bley
Wintersemester 2019/20

Algebraische Zahlentheorie
Übungsblatt 6Lösung

Aufgabe 1
Bestimmen Sie mittels Polynomzerlegungsgsetz nochmals die Zerlegung von $p\mathcal{O}_K$ im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$. Der Fall $d \equiv 2,3 \pmod 4$ wurde in der Vorlesung behandelt. Betrachten Sie hier noch den Fall $d \equiv 1 \pmod 4$.

Dies kann man mittels Polynomzerlegungsgesetz wie in der Vorlesung mit dem Polynomzerlegungsgesetz lösen. Man nehme $\theta := \sqrt{d}$ und erhält den Konduktor $\mathfrak{f} = 2\mathcal{O}_K$. Für $p \neq 2$ ergeben sich die gleichen Rechnungen wie in der Vorlesung. Für $p = 2$ betrachten wir $\theta := (1+\sqrt{d})/2$ mit Minimalpolynom $f(x) = x^2 - x + (1-d)/4$. Für $d \equiv 1 \pmod 8$ ist $(1-d)/2 \equiv 0 \pmod 2$ und man erhält $\bar{f}(x) = x(x-1)$. Also ist die 2 zerlegt. Für $d \equiv 5 \pmod 8$ ist $(1-d)/2 \equiv 1 \pmod 2$ und man sieht, dass $\bar{f}(x) = x^2 + x + 1$ irreduizibel ist. Also ist die 2 prim.

Aufgabe 2
Sei $K = \mathbb{Q}(\omega)$ mit $\omega^3 = 2$. Zeigen Sie mit dem Polynomzerlegungsgesetz, dass 2 und 3 voll verzweigt sind und $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ mit Trägheitsgraden 1 und 2 ist.

Wir wissen, dass $\mathcal{O}_K = \mathbb{Z}[\omega]$ gilt. Damit können wir für alle Primzahlen p das Polynomzerlegungsgesetz mit dem Minimalpolynom $f(x) = x^3 - 2$ von ω anwenden.

Zur Zerlegung der 2: Es gilt $f(x) \equiv x^3 \pmod{2\mathbb{Z}[x]}$, also ist $2\mathcal{O}_K = \mathfrak{p}^3$ mit $\mathfrak{p} = 2\mathcal{O}_K + \omega\mathcal{O}_K = \omega\mathcal{O}_K$ und Restklassenkörpergrad 1.

Zur Zerlegung der 3: Hier gilt $f(x) \equiv (x+1)^3 \pmod{3\mathbb{Z}[x]}$, also ist $2\mathcal{O}_K = \mathfrak{p}^3$ mit $\mathfrak{p} = 3\mathcal{O}_K + (\omega+1)\mathcal{O}_K = \omega\mathcal{O}_K$ und Restklassenkörpergrad 1.

Zur Zerlegung der 5: Hier gilt $f(x) \equiv (x+2)(x^2+3x+4) \pmod{5\mathbb{Z}[x]}$, also ist $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1 = 5\mathcal{O}_K + (\omega+2)\mathcal{O}_K, \mathfrak{p}_2 = 5\mathcal{O}_K + (\omega^2+3\omega+4)\mathcal{O}_K$ und Restklassenkörpergraden $f_1 = 1$ und $f_2 = 2$.

Aufgabe 3
Sei $L/M/K$ ein Turm von Zahlkörpern und P, $\mathfrak{P}$ und $\mathfrak{p}$ Primideale in den jeweiligen Ganzheitsringen. Zeigen Sie, dass der Verzweigungsindex and der Trägheitsgrad multiplikativ in einem Körperturm sind, d.h.

$$e(P|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) \cdot e(P|\mathfrak{P}),$$
$$f(P|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) \cdot f(P|\mathfrak{P}).$$

Es sei $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}\mathfrak{a}$ mit $\mathfrak{P} \nmid \mathfrak{a}$ und $\mathfrak{P}\mathcal{O}_L = P^{e(P/\mathfrak{P})}B$ mit $P \nmid B$. Dann gilt:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{p}\mathcal{O}_M\mathcal{O}_L = (\mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}\mathfrak{a})\mathcal{O}_L = (\mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}\mathcal{O}_L)\mathfrak{a}\mathcal{O}_L = P^{e(P/\mathfrak{P})\cdot e(\mathfrak{P}|\mathfrak{p})} \cdot \mathfrak{a}B.$$

Da $\mathfrak{a}B$ teilerfremd zu P ist, folgt $e(P/\mathfrak{P}) \cdot e(\mathfrak{P}|\mathfrak{p}) = e(P|\mathfrak{p})$.

Seien $\kappa(P), \kappa(\mathfrak{P})$ und $\kappa(\mathfrak{p})$ die entsprechenden Restklassenkörper. Dann gilt

$$[\kappa(P) : \kappa(\mathfrak{P})] = f(P|\mathfrak{P}), \quad [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f(\mathfrak{P}|\mathfrak{p})$$

und somit aus der Gradformel

$$f(P/\mathfrak{p}) = [\kappa(P) : \kappa(\mathfrak{p})] = [\kappa(P) : \kappa(\mathfrak{P})] \cdot [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f(\mathfrak{P}|\mathfrak{p}) \cdot f(P|\mathfrak{P}).$$

Aufgabe 4

Sei p eine ungerade Primzahl und $K = \mathbb{Q}(\zeta)$, wobei ζ eine primitive p-te Einheitswurzel bezeichnet. Sei μ_K die Gruppe der Einheitswurzeln in K.

a) Bestimmen Sie μ_K.

b) Sei K^+ der maximal reelle Teilkörper von K und sei $\langle\tau\rangle = \mathrm{Gal}(K/K^+)$ (τ ist also die komplexe Konjugation).
Zeigen Sie: $K^+ = K^{\langle\tau\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$.

c) Zeigen Sie, dass die Abbildung

$$\begin{aligned} f : \mathcal{O}_K^\times &\to \mu_K/\mu_K^2, \\ u &\mapsto \frac{u}{\tau(u)} \cdot \mu_K^2 \end{aligned}$$

ein Gruppenhomomorphismus ist mit $\ker(f) = \mu_K \mathcal{O}_{K^+}^\times$.
Hinweis: Es gilt $|\sigma(\frac{u}{\tau(u)})^j| = 1$ für alle Einbettungen σ und alle j.

d) Zeigen Sie: $[\mathcal{O}_K^\times : \mu_K \mathcal{O}_{K^+}^\times] \leq 2$.

a) Sei p eine ungerade Primzahl und ζ_p eine primitive p-te Einheitswurzel. Wir wollen nun μ_K bestimmen für $K = \mathbb{Q}(\zeta_p)$. Zuerst stellen wir fest, dass gilt $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$, da $\zeta_{2p} = -\zeta_{2p}^{p+1} = -\zeta_p^{\frac{p+1}{2}}$.
Wir nehmen nun an, es gibt ein andere k-te primitive Einheitswurzel θ in $\mathbb{Q}(\zeta_{2p})$. Sei $r := \mathrm{kgV}(k, 2p) > 2p$. Es gilt also, dass $\mathbb{Q}(\zeta_{2p})$ die r-te Einheitswurzel enthält. Somit gilt aber auch $\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_{2p})$,also

$$[\mathbb{Q}(\zeta_r) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_{2p}) : \mathbb{Q}],$$

woraus wiederum $\varphi(r) \leq \varphi(2p)$ folgt, dies ist aber ein Widerspruch zur Tatsache, dass wenn $2p$ r echt teilt (was per Konstruktion der Fall ist), auch $\varphi(2p)$ $\varphi(r)$ echt teilen müsste.

b) Wir haben in der Vorlesung K^+ als den maximal reellen Teilkörper von K definiert, also $K \cap \mathbb{R}$. Es ist also klar, dass $K^+ = K^{\langle\tau\rangle}$ gilt, wobei τ hier die komplexe Konjugation ist. Wir müssen also noch zeigen, dass $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) = K^+$ gilt. Da $\tau(\zeta_p + \zeta_p^{-1}) = \zeta_p^{-1} + \zeta_p$ gilt, erhalten wir $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subseteq K^+$.
Somit gilt aber auch

$$[K : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] \geq [K : K^+] = 2$$

und es bleibt zu zeigen, dass $[K : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] \leq 2$. Dies folgt aber, da ζ_p eine Nullstelle des Polynoms $x^2 - (\zeta_p + \zeta_p^{-1})x + 1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})[x]$ ist.

c) Wir betrachten die Abbildung

$$\begin{aligned} f : \mathcal{O}_K^\times &\to \mu_K/\mu_K^2, \\ u &\mapsto \frac{u}{\tau(u)} \cdot \mu_K^2. \end{aligned}$$

Als erstes wollen wir zeigen, dass die Abbildung wohldefiniert ist, d.h. $f(u) \in \mu_K$ für $u \in \mathcal{O}_K^\times$.
Für jede Einbettung σ gilt aber $|\sigma(\frac{u}{\tau(u)})| = 1$. Also gilt $\frac{u}{\tau(u)} \in \ker(\lambda : \mathcal{O}_K^\times \to \Gamma)$, wobei λ die in der Vorlesung definierte Abbildung ist. Dort haben wir aber auch gezeigt, dass $\ker(\lambda) = \mu_K$ gilt, also ist die Abbildung wohldefiniert.
Dass f ein Gruppenhomomorphismus ist, folgt, da τ ein Automorphismus ist.
Außerdem gilt $\mu_K^2 = \{\zeta_p^n : 0 \leq n < p\}$, da $\zeta_p^n = (\zeta_p^m)^2$ für $m = n/2$, wenn n gerade und $m = (p+n)/2$, wenn n ungerade ist.
Nun wollen wir zeigen $\ker(f) = \mu_K \mathcal{O}_{K^+}^\times$.
Sei dazu $v \in \mathcal{O}_{K^+}^\times$ und $\pm\zeta_p^n \in \mu_K$. Dann gilt:

$$f(\pm\zeta_p^n v) = \frac{\pm\zeta_p^n v}{\tau(\pm\zeta_p^n v)} = \frac{\zeta_p^n v}{\zeta_p^{-n} v} = \zeta_p^{2n} \in \mu_K^2.$$

Andererseits, wenn $\frac{u}{\tau(u)} = \zeta_p^n$, definieren wir $m = n/2$, wenn n gerade und $m = (p+n)/2$, wenn n ungerade ist. Dann gilt:

$$\tau(\zeta_p^{-m} u) = \zeta_p^m \tau(u) = \zeta_p^m \zeta_p^{-n} u = \zeta_p^{m-n} u = \zeta_p^{-m} u.$$

Also folgt $\zeta_p^{-m} u \in \mathcal{O}_{K^+}^\times$ und somit $u = \zeta_p^m(\zeta_p^{-m} u) \in \mu_K \mathcal{O}_{K^+}^\times$.

d) Wir sehen mit Teilaufgaben a) und c) sofort ein, dass $|\mu_K/\mu_K^2| = 2$ gilt und wir die exakte Sequenz

$$1 \to \mu_K \mathcal{O}_{K^+}^\times \to \mathcal{O}_K^\times \to \mu_K/\mu_K^2$$

erhalten. Mit dem Homomorphiesatz gilt also $\mathcal{O}_K^\times/\mu_K\mathcal{O}_{K^+}^\times \cong \mathrm{im}(f) \subseteq \mu_K/\mu_K^2$ und somit auch $[\mathcal{O}_K^\times : \mu_K\mathcal{O}_{K^+}^\times] \leq 2$.

Aufgabe 5

Sei L/K eine endliche Erweiterung von Zahlkörpern und $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathcal{O}_K$. Zeigen Sie, dass dann gilt

a) $\mathfrak{a} = \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$.

b) $\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \mathfrak{a}\mathcal{O}_L \mid \mathfrak{b}\mathcal{O}_L$.

a) Für Primideale $\mathfrak{p}$ gilt mit

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

die Inklusion

$$\mathfrak{p}\mathcal{O}_L \cap K = \left(\mathfrak{P}_1^{e_1} \cap \mathcal{O}_K\right) \cap \ldots \cap \left(\mathfrak{P}_r^{e_r} \cap \mathcal{O}_K\right) \subseteq \left(\mathfrak{P}_1 \cap \mathcal{O}_K\right) \cap \ldots \cap \left(\mathfrak{P}_r \cap \mathcal{O}_K\right) = \mathfrak{p}.$$

Wegen $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L \cap K$ folgt die Behauptung für Primideale.

Weiter folgt: $\mathfrak{p}^{\nu-1}(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K) = \mathfrak{p}^\nu$. Wir zeigen:

$$\mathfrak{p}^{\nu-1}(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K) = \mathfrak{p}^\nu \mathcal{O}_K \cap \mathcal{O}_K. \tag{1}$$

Damit folgt die Behauptung also für Primidealpotenzen. Um (1) zu zeigen, lokalisieren wir nach Primidealen $\mathfrak{q}$ von $\mathcal{O}_K$ und beachten, dass Lokalisieren mit Schnittbildung und Produkten vertauscht. Es sei $S := \mathcal{O}_K \setminus \mathfrak{q}$.

Für $\mathfrak{q} \neq \mathfrak{p}$ ist $S^{-1}\mathfrak{p} = \mathcal{O}_{K,\mathfrak{q}}$ und linke wie auch rechte Seite sind gleich $\mathcal{O}_{K,\mathfrak{q}}$. Für $\mathfrak{q} = \mathfrak{p}$ und $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ist $S^{-1}\mathfrak{p} = \pi\mathcal{O}_{K,\mathfrak{p}}$. Für die linke Seite erhält man also

$$\pi^{\nu-1}\left(\pi\mathcal{O}_{L,\mathfrak{p}} \cap \mathcal{O}_{K,\mathfrak{p}}\right) = \pi^\nu \mathcal{O}_{L,\mathfrak{p}} \cap \pi^{\nu-1}\mathcal{O}_{K,\mathfrak{p}}$$

Für die rechte Seite ergibt sich

$$\pi^\nu \mathcal{O}_{L,\mathfrak{p}} \cap \mathcal{O}_{K,\mathfrak{p}}.$$

Man sieht leicht, dass beide Seiten übereinstimmen.

Schließlich ist die Behauptung noch für beliebige ganze Ideale zu beweisen. Sei dazu $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r}$. Dann gilt:

$$\begin{aligned}
\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K &= \mathfrak{p}_1^{\nu_1}\mathcal{O}_L \cdots \mathfrak{p}_r^{\nu_r}\mathcal{O}_L \cap \mathcal{O}_K \\
&= \mathfrak{p}_1^{\nu_1}\mathcal{O}_L \cap \ldots \cap \mathfrak{p}_r^{\nu_r}\mathcal{O}_L \cap \mathcal{O}_K \\
&= \left(\mathfrak{p}_1^{\nu_1}\mathcal{O}_L \cap \mathcal{O}_K\right) \cap \ldots \cap \left(\mathfrak{p}_r^{\nu_r}\mathcal{O}_L \cap \mathcal{O}_K\right) \\
&= \mathfrak{p}_1^{\nu_1} \cap \ldots \cap \mathfrak{p}_r^{\nu_r} \\
&= \mathfrak{a}.
\end{aligned}$$

b) Es gilt:

$$\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a} \overset{(a)}{\iff} \mathfrak{b}\mathcal{O}_L \subseteq \mathfrak{a}\mathcal{O}_L \iff \mathfrak{a}\mathcal{O}_L \mid \mathfrak{b}\mathcal{O}_L.$$