LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley Wintersemester 2019/20

Algebraische Zahlentheorie
Lösung Übungsblatt 2

Aufgabe 1
Wird vollständig unter Aufgabe 6 behandelt.

Aufgabe 2
Sei $G(K/\mathbb{Q}, \bar{\mathbb{Q}}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Dann gilt wegen $\sigma_i(\alpha + m) = \sigma_i(\alpha) + m$:

$$d(\alpha) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \prod_{1 \le i < j \le n} (\sigma_i(\alpha + m) - \sigma_j(\alpha + m))^2 = d(\alpha + m).$$

Aufgabe 3
Es sei $f(x) = (x - \sigma_i(\alpha))g_i(x)$ mit $g_i(x) := \prod_{j \neq i}(x - \sigma_j(\alpha))$. Dann folgt

$$f'(x) = g_i(x) + (x - \sigma_i(\alpha))g_i'(x)$$

und Einsetzen von $x = \sigma_i(\alpha)$ liefert

$$f'(\sigma_i(\alpha)) = g_i(\sigma_i(\alpha)) = \prod_{j \neq i}(\sigma_i(\alpha) - \sigma_j(\alpha)).$$

Hieraus folgt nun

$$\begin{aligned} \prod_{i=1}^{n} f'(\sigma_i(\alpha)) &= \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i(\alpha) - \sigma_j(\alpha)) \\ &= \left(\prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha) \right)^2 (-1)^{1+2+\ldots+(n-1)} \\ &= (-1)^{(n-1)n/2} d(\alpha). \end{aligned}$$

Aufgabe 4
Man berechnet $\mathrm{Tr}(1) = 3, \mathrm{Tr}(\lambda) = 0, \mathrm{Tr}(\lambda^2) = -4, \mathrm{Tr}(\lambda^3) = -3$ und $\mathrm{Tr}(\lambda^4) = 8$. Damit berechnet man weiter

$$d(\lambda) = \det(\mathrm{Tr}(\lambda^i \lambda^j)_{0 \le i,j \le 2} = -59.$$

Da $d(\lambda)$ quadratfrei ist, ist $\mathcal{O}_K = \mathbb{Z}[\lambda]$.

Aufgabe 5

Sei K ein algebraischer Zahlkörper von Grad n über Q. Zeigen Sie, dass gilt:

$$d_K \equiv 0, 1 \bmod 4.$$

Man nennt diese Tatsache auch das *Stickelberger-Kriterium*

Sei K ein algebraischer Zahlkörper mit $[K:\mathbb{Q}] = n$. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine Ganzheitsbasis von K (diese existiert laut einem Satz der Vorlesung). Für jedes $i = 1, 2, \ldots, n$, seien $\sigma_1(\alpha_i), \ldots, \sigma_n(\alpha_i)$ die Konjugierten von α_i über $\mathbb{Q}$. Per Definition gilt nun

$$d_K = d(\alpha_1, \ldots, \alpha_n) := \det(\sigma_j(\alpha_i))^2.$$

Sei nun A_n die alternierende Gruppe und $B_n := S_n \setminus A_n$. Also ist $\sqrt{d_K}$ die Summe über $n!$ Terme (Leibnizformel für Determinanten) und wir erhalten

$$\sqrt{d_K} = \det(\sigma_j(\alpha_i)) = \sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i) - \sum_{\pi \in B_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i) = P - N,$$

wobei P bzw. N jeweils eine abkürzende Schreibweise für den ersten bzw. zweiten Summanden ist.
Wir sehen zuerst, dass $P, N \in \mathcal{O}_K$. Für unser K finden wir nun eine Erweiterung L, so dass $K \subseteq L \subseteq \mathbb{C}$ mit $L/\mathbb{Q}$ endlich und galoissch. Wir erinnern uns, dass für alle Einbettungen $\sigma_i : K \to \mathbb{C}$ gilt $\sigma_i K \subseteq L$. Für $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$ ist also $\varphi \circ \sigma_i$ eine Einbettung $K \to \mathbb{C}$ und $\sigma \mapsto \varphi \circ \sigma_i$ ist eine Bijektion von $\{\sigma_1, \ldots, \sigma_n\}$ nach $\{\sigma_1, \ldots, \sigma_n\}$. Somit können wir aber auch ein $\pi \in S_n$ finden, so dass $\varphi \circ \sigma_i = \sigma_{\pi(i)}$.
Wir wollen nun zeigen, dass $\varphi(P+N) = P+N$ und $\varphi(PN) = PN$ gilt. Wir unterscheiden dazu verschiedene Fälle:
Sei zuerst $\tau \in S_n$ gerade, i.e. $\tau A_n = A_n$. Dann gilt:

$$\begin{aligned}
\varphi\Big(\sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_{\pi(i)}\alpha_i\Big) &= \sum_{\pi \in A_n} \prod_{i=1}^{n} \varphi \circ \sigma_{\pi(i)}\alpha_i, \\
&= \sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_{(\tau\circ\pi)(i)}\alpha_i, \\
&= \sum_{\pi \in \tau A_n} \prod_{i=1}^{n} \sigma_{\pi(i)}\alpha_i, \\
&= \sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_{\pi(i)}\alpha_i.
\end{aligned}$$

In diesem Fall haben wir also gezeigt: $\varphi(P) = P$. Wenn τ gerade ist, gilt $\tau(B_n) = B_n$ und man kann analog folgern: $\varphi(N) = N$.
Für $\tau \in S_n$ ungerade, gilt $\tau A_n = B_n$ und $\tau B_n = A_n$. Ähnliche Argumente wie oben liefern nun $\varphi(P) = N$ und $\varphi(N) = P$. Damit folgt aber sofort, dass $\varphi(P+N) = P+N$ und $\varphi(PN) = PN$ gilt. Also ist $P+N, PN \in \mathbb{Q}$ und somit gilt auch $P+N, PN \in \mathbb{Z}$ (da $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$). Somit gilt insgesamt

$$d_K = (P-N)^2 \equiv (P+N)^2 - 4PN \equiv (P+N)^2 \bmod 4.$$

Da $(2n)^2 \equiv 0 \bmod 4$ und $(2n+1)^2 \equiv 1 \bmod 4$ gilt, folgt die Behauptung.

Aufgabe 6
Sei zunächst $p \neq 2, d \equiv 1 \pmod 4$, $x^2 \equiv d \pmod p$, $x \equiv 1 \pmod 2$. Wir zeigen:

(a) $\mathfrak{p} := \langle p, \frac{x+\sqrt{d}}{2} \rangle_{\mathbb{Z}}$ ist ein $\mathcal{O}_K$-Ideal.

(b) $\mathfrak{p}$ ist ein Primideal.

(c) $\mathfrak{p}\bar{\mathfrak{p}} = p\mathcal{O}_K$.

Ad (a): Wegen $\mathcal{O}_K = \langle 1, \frac{1+\sqrt{d}}{2} \rangle_{\mathbb{Z}}$ genügt es zu zeigen, dass

$$\frac{1+\sqrt{d}}{2} \cdot p \in \mathfrak{p} \text{ und } \frac{1+\sqrt{d}}{2} \cdot \frac{x+\sqrt{d}}{2} \in \mathfrak{p}$$

gilt. Dies sieht man durch elementare Rechnungen ein.

Ad (b): Es gilt $\mathcal{O}_K = \langle 1, \frac{1+\sqrt{d}}{2} \rangle_{\mathbb{Z}} = \langle 1, \frac{x-1}{2} + \frac{1+\sqrt{d}}{2} \rangle_{\mathbb{Z}} = \langle 1, \frac{x+\sqrt{d}}{2} \rangle_{\mathbb{Z}}$. Also ist die Abbildung $\mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}, 1 \mapsto 1 + \mathfrak{p}$ surjektiv und induziert einen Isomorphismus $\mathbb{Z}/p\mathbb{Z} \simeq \mathcal{O}_K/\mathfrak{p}$. Also ist $\mathfrak{p}$ ein Primideal.

Ad (c): Wir rechnen nach

$$\begin{aligned}\mathfrak{p}\bar{\mathfrak{p}} &= \langle p, \frac{x+\sqrt{d}}{2}\rangle_{\mathbb{Z}}\langle p, \frac{x-\sqrt{d}}{2}\rangle_{\mathbb{Z}} \\ &= \langle p^2, p\frac{x+\sqrt{d}}{2}, p\frac{x-\sqrt{d}}{2}, \frac{x^2-d}{4}\rangle_{\mathbb{Z}} \\ &= \dots \\ &= p\mathcal{O}_K.\end{aligned}$$

Denn Fall $d \equiv 2,3 \pmod 4$, $\left(\frac{d}{p}\right) = 1$ behandelt man analog.

Sei nun $p \neq 2$ und $\left(\frac{d}{p}\right) = -1$. Man betrachte die von $x \mapsto \sqrt{d}$ induzierte Abbildung

$$\mathbb{Z}[x]/(x^2-d) \longrightarrow \mathbb{Z}[\omega],$$

wobei wie üblich $\omega := \sqrt{d}$ bzw. $\omega := (1+\sqrt{d})/2$ ist. Wegen $p \neq 2$ ist diese Abbildung in allen Fällen surjektiv und induziert eine surjektive Abbildung

$$\frac{\mathbb{Z}[x]/(x^2-d)}{p(\mathbb{Z}[x]/(x^2-d))} \longrightarrow \frac{\mathbb{Z}[\omega]}{p\,\mathbb{Z}[\omega]}.$$

Für die linke Seite gilt nun

$$\frac{\mathbb{Z}[x]/(x^2-d)}{p(\mathbb{Z}[x]/(x^2-d))} \simeq \mathbb{F}_p[x]/(x^2-d) \simeq \mathbb{F}_{p^2},$$

da d kein Quadrat in $\mathbb{F}_p$ ist und daher x^2-d in $\mathbb{F}_p[x]$ irreduzibel ist. Also ist $\frac{\mathbb{Z}[\omega]}{p\,\mathbb{Z}[\omega]} \simeq \mathbb{F}_{p^2}$ und $p\,\mathbb{Z}[\omega] = p\mathcal{O}_K$ ist ein Primideal.

Wir betrachten nun den Fall $p \neq 2$, $p \mid d$. Falls $d \equiv 2,3 \pmod 4$, so ist $\langle p, \sqrt{d}\rangle_{\mathbb{Z}}$ ein Primideal und es gilt

$$\langle p, \sqrt{d}\rangle_{\mathbb{Z}}^2 = \langle p^2, p\sqrt{d}, d\rangle_{\mathbb{Z}} = p\mathcal{O}_K.$$

Falls $d \equiv 1 \pmod 4$, so ist $\langle p, \frac{d+\sqrt{d}}{2}\rangle_{\mathbb{Z}}$ ein Primideal und eine einfache Rechnung zeigt

$$\langle p, \frac{d+\sqrt{d}}{2}\rangle_{\mathbb{Z}}^2 = p\mathcal{O}_K.$$

Abschliessend ist noch der Fall $p = 2$ zu betrachten. Ähnliche Rechnugen wie oben liefern das folgende Resultat:

$$\begin{aligned}d \equiv 2 \pmod 4 &\implies 2\mathcal{O}_K = \langle 2, \sqrt{d}\rangle_{\mathbb{Z}}^2, \\ d \equiv 3 \pmod 4 &\implies 2\mathcal{O}_K = \langle 2, 1+\sqrt{d}\rangle_{\mathbb{Z}}^2, \\ d \equiv 1 \pmod 8 &\implies 2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \text{ mit } \mathfrak{p} = \langle 2, \frac{1+\sqrt{d}}{2}\rangle_{\mathbb{Z}}, \\ d \equiv 5 \pmod 8 &\implies 2\mathcal{O}_K \text{ ist prim.}\end{aligned}$$

Hier die Begründung für die letzte Zeile: Das Minimalpolynom von $(1+\sqrt{d})/2$ ist gegeben durch $x^2 - x + \frac{1-d}{2}$ und $x \mapsto (1+\sqrt{d})/2$ induziert einen Isomorphismus

$$\frac{\mathbb{Z}[x]/(x^2-x+\frac{1-d}{2})}{2(\mathbb{Z}[x]/(x^2-x+\frac{1-d}{2}))} \simeq \mathcal{O}_K/2\mathcal{O}_K.$$

Wegen $d \equiv 5 \pmod 8$ ist $x^2 - x + \frac{1-d}{2}$ irreduzibel in $\mathbb{F}_2[x]$ und die linke Seite ist isomporph zu $\mathbb{F}_4$.