LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley

Wintersemester 2019/20

Algebraische Zahlentheorie
Lösung Übungsblatt 4

Aufgabe 1
Sei $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ ein biquadratischer Zahlkörper. Bestimmen Sie die Anzahl der reellen und komplexen Einbettungen in Abhängigkeit von d_1 und d_2. Geben Sie den Minkowski-Raum jeweils explizit an.

Falls $d_1 > 0$ und $d_2 > 0$, so sind alle Einbettungen reell, also $r = 4, s = 0$. Es gilt: $K_{\mathbb{R}} = \mathbb{R}^4$.

Falls $d_1 < 0$ oder $d_2 < 0$, so sind alle Einbetungen komplex, also $r = 0$ und $s = 2$. Sei zum Beispiel $d_1 < 0$ und $d_2 > 0$. Sei $\sigma_1 = id$. Dann ist $\bar{\sigma}_1(\sqrt{d_1}) = -\sqrt{d_1}$ und $\bar{\sigma}_1(\sqrt{d_2}) = \sqrt{d_2}$. Für σ_2 definiert durch $\sigma_2(\sqrt{d_1}) = \sqrt{d_1}$ und $\sigma_2(\sqrt{d_2}) = -\sqrt{d_2}$ erhält man $\bar{\sigma}_2(\sqrt{d_1}) = -\sqrt{d_1}$ und $\bar{\sigma}_2(\sqrt{d_2}) = -\sqrt{d_2}$. Es gilt dann explizit:

$$K_{\mathbb{R}} = \{(v, \bar{v}, w, \bar{w}) \in \mathbb{C}^4 \mid v, w \in \mathbb{C}\}.$$

Aufgabe 2
Sei $\alpha^3 = 2$ und $K = \mathbb{Q}(\alpha)$. Es ist $\mathcal{O}_K = \mathbb{Z}[\alpha]$ (das brauchen Sie nicht zu zeigen).

a) Zeigen Sie, dass die Primzahlzerlegung von $2\mathcal{O}_K$ von der Form $2\mathcal{O}_K = \mathfrak{p}^3$ ist.

b) Geben Sie eine $\mathbb{Z}$-Basis von $\mathfrak{p}$ an.

c) Berechnen Sie das Lebesgue-Volumen von $\Gamma = (f \circ j)(\mathfrak{p})$.

a) Für $\mathfrak{p} = \alpha\mathcal{O}_K$ gilt $\mathfrak{p}^3 = \alpha^3\mathcal{O}_K = 2\mathcal{O}_K$. Die Abbildung $\mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}$, $1 \mapsto 1 + \mathfrak{p}$ ist surjektiv, da $a + b\alpha + c\alpha^2 \equiv a \pmod{\mathfrak{p}}$. Da $2 \in \mathfrak{p}$, induziert sie eine surjektive Abbildung $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}$. Da $\mathbb{Z}/2\mathbb{Z}$ ein Körper ist, ist dies ein Isomorphismus. Also ist $\mathfrak{p}$ maximal, insbesondere prim.

b) Eine $\mathbb{Z}$-Basis ist gegeben durch $\alpha, \alpha^2, 2$. Dies zeigt nochmals $|\mathcal{O}_K/\mathfrak{p}| = 2$.

c) Es ist hier $r = 1$ und $s = 1$. Man berechnet $d_K = -108$. Damit gilt:

$$2^s \mathrm{Vol}_{\mathcal{L}}(\Gamma) = 2\mathrm{Vol}_{\mathcal{L}}(\Gamma) = \mathrm{Vol}_{(\ ,\ )}(f(j(\mathfrak{p}))) = \mathrm{Vol}_{\langle\ ,\ \rangle}(j(\mathfrak{p})) = [\mathcal{O}_K : \mathfrak{p}]\sqrt{|d_K|} = 2\sqrt{108}.$$

Also ist $\mathrm{Vol}_{\mathcal{L}}(\Gamma) = \sqrt{108}$.

Aufgabe 3
Zeigen Sie, dass der Minkowskische Gitterpunktsatz nicht verbessert werden kann, indem man eine konvexe, zentralsymmetrische Menge $X \subseteq V$ mit $\mathrm{Vol}(X) = 2^n\mathrm{Vol}(\Gamma)$ angibt, die keinen von 0 verschiedenen Punkt von Γ enthält.
Ist aber X kompakt, so ist das Gleichheitszeichen zulässig.
Hinweis: Betrachten Sie die Mengen $(1 + \varepsilon)X$ für $\varepsilon > 0$.

Man betrachte $V = \mathbb{R}^n$ mit dem Standardskalarprodukt und $X = \{x \in \mathbb{R}^n \mid |x_i| < 1\}$ und $\Gamma = \mathbb{Z}^n$. Dann ist

$$\mathrm{Vol}_{\mathcal{L}}(\Gamma) = 1 \text{ und } \mathrm{Vol}_{\mathcal{L}}(X) = 2^n.$$

Ferner ist X konvex und zentralsymmetrisch, enthält jedoch keinen Gitterpunkt ungleich 0.

Sei nun X kompakt, zentralsymmetrisch, konvex und es gelte $\mathrm{Vol}(X) = 2^n\mathrm{Vol}(\Gamma)$ (bez. des gegebenen Skalarprodukts auf V). Für $n \in \mathbb{N}$ gibt es dann nach dem Minkowskischen Gitterpunktsatz einen Gitterpunkt $0 \neq \gamma_n \in (1 + \frac{1}{n})X$. Da X beschränkt ist, ist auch $2X$ beschränkt

und offensichtlich gilt $\gamma_n \in 2X$ für alle n. Da in einer beschränkten Menge höchstens endlich viele Gitterpunkte liegen, hat die Folge der γ_n eine konstante Teilfolge mit Wert $\gamma \in \Gamma$. Dann folgt $\gamma = \gamma_n \in (1 + \frac{1}{n})X$ für beliebig große n und da X abgeschlossen ist, erhält man $\gamma \in X$.

Aufgabe 4
Sei K ein algebraischer Zahlkörper und $\mathfrak{a}$ ein ganzes Ideal.

a) Zeigen Sie, dass es eine natürliche Zahl h gibt, so dass $\mathfrak{a}^h = a\mathcal{O}_K$ ein Hauptideal ist.

b) Zeigen Sie, dass $\mathfrak{a}$ im Körper $L = K(\sqrt[h]{a})$ ein Hauptideal wird, d.h. $\mathfrak{a}\mathcal{O}_L = \alpha\mathcal{O}_L$.

c) Zeigen Sie, dass es zu jedem Zahlkörper K eine endliche Erweiterung L gibt, in der jedes Ideal von K ein Hauptideal wird.

a) Für die Klassenzahl $h = h_K$ gilt nach dem sattz von Lagrange $[\mathfrak{a}]^h = [\mathcal{O}_K]$, was gleichbedeutend damit ist, dass $\mathfrak{a}^h$ ein Hauptideal ist.

b) Sei $\mathfrak{a}^h = a\mathcal{O}_K$. Dann gilt mit $\alpha := \sqrt[h]{a}$

$$(\alpha\mathcal{O}_L)^h = a\mathcal{O}_L = \mathfrak{a}^h\mathcal{O}_L = (\mathfrak{a}\mathcal{O}_L)^h.$$

Da die Gruppe der gebrochenen Ideal torsionsfrei ist, folgt $\alpha\mathcal{O}_L = \mathfrak{a}\mathcal{O}_L$.

c) Wenn $\mathrm{cl}_K = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_h]\}$ mit ganzen Idealen $\mathfrak{a}_i$ ist, so leistet $L := K(\sqrt[h]{a_1}, \ldots, \sqrt[h]{a_h})$ das Verlangte, wobei hier gilt $\mathfrak{a}_i^h = a_i\mathcal{O}_K$ sei. Falls nämlich $\mathfrak{b}$ ein beliebiges gebrochenes Ideal ist, so gibt es (genau) ein i und ein $\beta_i \in K^\times$ mit $\mathfrak{b} = \beta_i\mathfrak{a}_i$. Dann wird $\mathfrak{b}$ wegen b) bereits in der Zwischenerweiterung $K(\sqrt[h]{a_i})$ zum Hauptideal.

Aufgabe 5
Sei K ein Zahlkörper.
Für ein ganzes Ideal $\mathfrak{a} \lhd_K, \mathfrak{a} \neq (0)$, definieren wir $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$. Zeigen Sie:

a) Sei $\mathfrak{p}$ ein Primideal und $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Dann ist $N(\mathfrak{p})$ eine p-Potenz.
Hinweis: $\mathcal{O}_K/\mathfrak{p}$ wird zu einem $\mathbb{F}_p$-Vektorraum.

b) $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$ für alle Primideale $\mathfrak{p}$ und alle $n \in \mathbb{N}$.

c) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ für alle Ideale $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$.
Hinweis: Nehmen Sie zunächst an, dass $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$ und wenden Sie den Ch. Restsatz an.

a) Wegen $p \in \mathfrak{p}$ und $|\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p}) < \infty$ ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Sei $f := [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$. Dann gilt offenbar $N(\mathfrak{p}) = p^f$.

b) Wir beweisen die Aussage mittels Induktion über n. Für den Induktionsschritt betrachte man die kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{p}^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{p}^n \longrightarrow 0$$

Es folgt dann

$$N(\mathfrak{p}^{n+1}) = |\mathcal{O}_K/\mathfrak{p}^{n+1}| = |\mathcal{O}_K/\mathfrak{p}^n| \cdot |\mathfrak{p}^n/\mathfrak{p}^{n+1}| = N(\mathfrak{p}^n) \cdot |\mathfrak{p}^n/\mathfrak{p}^{n+1}| = N(\mathfrak{p})^n \cdot |\mathfrak{p}^n/\mathfrak{p}^{n+1}|,$$

wobei die letzte Gleichheit aus der Induktion folgt. Es bleibt also zu zeigen: $N(\mathfrak{p}) = |\mathfrak{p}^n/\mathfrak{p}^{n+1}|$.

Dazu wähle man $\alpha \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$. Dann ist

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}, \quad \beta + \mathfrak{p} \mapsto \alpha\beta + \mathfrak{p}^{n+1},$$

ein Isomorphismus, denn es gilt:

$$\alpha\beta \in \mathfrak{p}^{n+1} \iff \beta \in \mathfrak{p}.$$

Also ist die Abbildung injektiv. Das Bild ist gegeben durch $(\alpha\mathcal{O}_K + \mathfrak{p}^{n+1})/\mathfrak{p}^{n+1}$. Aus $\alpha\mathcal{O}_K + \mathfrak{p}^{n+1} = \mathfrak{p}^n$ folgt schließlich die Surjektivität.