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

Algebraische Zahlentheorie
Übungsblatt 3

Aufgabe 1
Sei $\mathcal{O}$ ein Dedekindring und $(0) \neq \mathfrak{a}, \mathfrak{b} \triangleleft \mathcal{O}$. Sei

$$\begin{aligned} \mathfrak{a} &= \prod \mathfrak{p}^{\nu_\mathfrak{p}}, \quad \nu_\mathfrak{p} \in \mathbb{N}_0, \text{ fast alle } \nu_\mathfrak{p} = 0, \\ \mathfrak{b} &= \prod \mathfrak{p}^{\mu_\mathfrak{p}}, \quad \mu_\mathfrak{p} \in \mathbb{N}_0, \text{ fast alle } \mu_\mathfrak{p} = 0. \end{aligned}$$

Hierbei erstreckt sich das Produkt jeweils über alle Primideale $\neq (0)$ von $\mathcal{O}$.

Zeigen Sie:

a) $\mathfrak{b} \subseteq \mathfrak{a} \iff \mathfrak{a} \mid \mathfrak{b} \iff \nu_\mathfrak{p} \leq \mu_\mathfrak{p}$ für alle $\mathfrak{p}$,

b) $\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}^{\min(\nu_\mathfrak{p}, \mu_\mathfrak{p})}$,

c) $\mathfrak{a} \cap \mathfrak{b} = \prod \mathfrak{p}^{\max(\nu_\mathfrak{p}, \mu_\mathfrak{p})}$.

a) Die erste Äquivalenz gilt per Definition. Zur zweiten Äquivalenz: Man beachte das $\nu_\mathfrak{p}$ eindeutig durch die Bedingung $\mathfrak{a} \subseteq \mathfrak{p}^{\nu_\mathfrak{p}}, \mathfrak{a} \not\subseteq \mathfrak{p}^{\nu_\mathfrak{p}+1}$ festgelegt ist. Analog für $\mu_\mathfrak{p}$. Sei nun $\mathfrak{b} \subseteq \mathfrak{a}$. Dann folgt $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{p}^{\nu_\mathfrak{p}}$, also $\nu_\mathfrak{p} \leq \mu_\mathfrak{p}$. Für die Umkehrung beachte man zuerst die Äquivalenz

$$\mathfrak{p}^{\mu_\mathfrak{p}} \subseteq \mathfrak{p}^{\nu_\mathfrak{p}} \iff \nu_\mathfrak{p} \leq \mu_\mathfrak{p}.$$

Man erhält daher

$$\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{\mu_\mathfrak{p}} = \bigcap_\mathfrak{p} \mathfrak{p}^{\mu_\mathfrak{p}} \subseteq \bigcap_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}} = \mathfrak{a}.$$

b) Sei $\kappa_\mathfrak{p} := \min(\nu_\mathfrak{p}, \mu_\mathfrak{p})$. Dann gilt wegen $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{p}^{\kappa_\mathfrak{p}}$ offensichtlich $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{p}^{\kappa_\mathfrak{p}}$. Sei etwa $\kappa_\mathfrak{p} = \nu_\mathfrak{p}$. Dann folgt aus $\mathfrak{a} \not\subseteq \mathfrak{p}^{\kappa_\mathfrak{p}+1}$ sofort $\mathfrak{a} + \mathfrak{b} \not\subseteq \mathfrak{p}^{\kappa_\mathfrak{p}+1}$.

c) Hier benutzen wir $\mathfrak{p}^{\nu_\mathfrak{p}} \cap \mathfrak{p}^{\mu_\mathfrak{p}} = \mathfrak{p}^{\max(\nu_\mathfrak{p}, \mu_\mathfrak{p})}$ und schließen wir wie folgt

$$\mathfrak{a} \cap \mathfrak{b} = \left(\bigcap_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}} \right) \cap \left(\bigcap_\mathfrak{p} \mathfrak{p}^{\mu_\mathfrak{p}} \right) = \bigcap_\mathfrak{p} \mathfrak{p}^{\max(\nu_\mathfrak{p}, \mu_\mathfrak{p})}.$$

Aufgabe 2
Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K. Für ein Primideal $\mathfrak{p} \neq 0$ und $\alpha \in K^\times$ defineren wir

$$v_\mathfrak{p}(\alpha) := v_\mathfrak{p}(\alpha\mathcal{O}).$$

Zeige:

a) $v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta)$.

b) $v_\mathfrak{p}(\alpha + \beta) \geq \min(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta))$, mit Gleichheit, falls $v_\mathfrak{p}(\alpha) \neq v_\mathfrak{p}(\beta)$.

a) folgt unmittelbar aus der Definition,

$$v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha\beta\mathcal{O}_K) = v_\mathfrak{p}(\alpha\mathcal{O}_K \cdot \beta\mathcal{O}_K) = v_\mathfrak{p}((\alpha\mathcal{O}_K) + v_\mathfrak{p}((\beta\mathcal{O}_K) = v_\mathfrak{p}((\alpha) + v_\mathfrak{p}((\beta).$$

b) Man beachte, dass $v_\mathfrak{p}(\alpha + \beta)$ eindeutig durch

$$(\alpha + \beta)\mathcal{O}_K \subseteq \mathfrak{p}^{v_\mathfrak{p}(\alpha+\beta)}, (\alpha + \beta)\mathcal{O}_K \not\subseteq \mathfrak{p}^{v_\mathfrak{p}(\alpha+\beta)+1}$$

bestimmt ist. Dies ist äquivalent zu

$$(\alpha + \beta) \in \mathfrak{p}^{v_\mathfrak{p}(\alpha+\beta)}, (\alpha + \beta) \notin \mathfrak{p}^{v_\mathfrak{p}(\alpha+\beta)+1}.$$

Analoge Charakterisierungen haben wir für $v_\mathfrak{p}(\alpha)$ und $v_\mathfrak{p}(\beta)$ Sei nun oE $v_\mathfrak{p}(\alpha)$ das Minimum. Dann gilt

$$\alpha \in \mathfrak{p}^{v_\mathfrak{p}(\alpha)}, \alpha \notin \mathfrak{p}^{v_\mathfrak{p}(\alpha)+1}, \beta \in \mathfrak{p}^{v_\mathfrak{p}(\beta)} \subseteq \mathfrak{p}^{v_\mathfrak{p}(\alpha)},$$

und somit

$$\alpha + \beta \in \mathfrak{p}^{v_\mathfrak{p}(\alpha)}$$

Es folgt also $v_\mathfrak{p}(\alpha + \beta) \geq v_\mathfrak{p}(\alpha)$.

Es gelte nun zusätzlich $v_\mathfrak{p}(\alpha) < v_\mathfrak{p}(\beta)$. Angenommen es gelte $v_\mathfrak{p}(\alpha + \beta) > v_\mathfrak{p}(\alpha)$. Dann folgt $\alpha + \beta \in \mathfrak{p}^{v_\mathfrak{p}(\alpha)+1}$ und wegen $\alpha \notin \mathfrak{p}^{v_\mathfrak{p}(\alpha)+1}$ auch $\beta \notin \mathfrak{p}^{v_\mathfrak{p}(\alpha)+1}$. Wegen $\beta \in \mathfrak{p}^{v_\mathfrak{p}(\alpha)}$ wäre also $v_\mathfrak{p}(\beta) = v_\mathfrak{p}(\alpha)$, Widerspruch!

Aufgabe 3
Sei $\mathcal{O}$ ein Dedekindring mit nur endlich viele Primidealen. Zeige: $\mathcal{O}$ ist ein Hauptidealring.

Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ die endlich vielen Primideale $\neq 0$ in $\mathcal{O}$. Da jedes Ideal ein Produkt von Primidealpotenzen ist, genügt es zu zeigen, dass jedes Primideal $\mathfrak{p}_i$ ein Hauptideal ist. Wähle dazu $\pi \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ und bestimme mit dem chinesischen Restsatz ein $\alpha \in \mathcal{O}$ mit

$$\begin{aligned} \alpha &\equiv \pi \pmod{\mathfrak{p}_i^2}, \\ \alpha &\equiv 1 \pmod{\mathfrak{p}_j}, \quad j \neq i. \end{aligned}$$

Dann folgt aus der ersten Kongruenz $\alpha \in \mathfrak{p}_i$ und $\alpha \notin \mathfrak{p}_i^2$, also $v_{\mathfrak{p}_i}(\alpha) = 1$. Für $j \neq i$ liefern die anderen Kongruenzen $\alpha \in \mathcal{O}$ und $\alpha \notin \mathfrak{p}_j$, also $v_{\mathfrak{p}_j}(\alpha) = 0$. Hieraus folgt $\alpha\mathcal{O}_K = \mathfrak{p}_i$.

Aufgabe 4

Sei $K = \mathbb{Q}(\zeta_m)$. Zeige:

a) Falls $m = p^r$ eine Primzahlpotenz ist, so ist $\mathfrak{p} := (1 - \zeta_m)\mathcal{O}_K$ ein Primideal und es gilt:

$$\mathfrak{p}^{p^{r-1}(p-1)} = p\mathcal{O}_K.$$

b) Falls m zusammengesetzt ist, so ist $1 - \zeta_m$ eine Einheit in $\mathcal{O}_K$.

c) Für alle m und alle $1 \leq a \leq m$ mit $(m, a) = 1$ ist $\frac{1-\zeta_m^a}{1-\zeta_m}$ eine Einheit in $\mathcal{O}_K$.

a) Wegen $\mathcal{O}_K = \mathbb{Z}[1 - \zeta_{p^r}]$ ist die Abbildung $\mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}$ surjektiv. Wegen

$$p = \prod_{1 \leq k \leq p^r, p \nmid k} (1 - \zeta_{p^r}^k) \tag{1}$$

ist die induzierte Abbildung $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}$ wohldefiniert. Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist dies ein Isomorphismus, also ist $\mathfrak{p}$ ein Primideal.

Ferner sind die Zahlen $1 - \zeta_{p^r}^k$ sämtlich zu $1 - \zeta_{p^r}$ assoziiert, da

$$\begin{aligned} \frac{1 - \zeta_{p^r}^k}{1 - \zeta_{p^r}} &= \sum_{j=0}^{k-1} \zeta_{p^r}^j \in \mathcal{O}_K, \\ \frac{1 - \zeta_{p^r}}{1 - \zeta_{p^r}^k} &= \frac{1 - \zeta_{p^r}^{kl}}{1 - \zeta_{p^r}^k} = \sum_{j=0}^{l-1} \zeta_{p^r}^{kj} \in \mathcal{O}_K \end{aligned}$$

wobei $l \in \mathbb{Z}$ so gewählt ist, dass $kl \equiv 1 \pmod{p^r}$ gilt.

Es folgt also $(1 - \zeta_{p^r}^k)\mathcal{O}_K = \mathfrak{p}$ für alle k wie in (1). Die Anzahl der k ist gegeben durch $\varphi(p^r) = p^{r-1}(p-1)$. Daher folgt aus (1) die Behauptung $\mathfrak{p}^{p^{r-1}(p-1)} = p\mathcal{O}_K$.

b) Seien p, q zwei verschiedene Primteiler von m. Sei $m = p^k n, (m, n) = 1$ Dann gilt

$$\frac{1 - \zeta_{p^k}}{1 - \zeta_m)} = \frac{1 - \zeta_m^n}{1 - \zeta_m)} = \sum_{j=0}^{n-1} \zeta_m^j \in \mathcal{O}_K.$$

Also folgt $1-\zeta_m \mid 1-\zeta_{p^k} \mid p$ und analog $1-\zeta_m \mid 1-\zeta_{q^l} \mid q$. Da p und q teilerfremd sind, ist $1-\zeta_m$ eine Einheit.

Aufgabe 5
Sei $\mathcal{O}$ ein Dedekindring und $\mathfrak{a}, \mathfrak{b} \in J_{\mathcal{O}}$ gebrochene Ideale. Sei S eine multiplikative Menge in $\mathcal{O}$. Zeige:

a) $S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$.

b) $S^{-1}(\mathcal{O} : \mathfrak{a}) = (S^{-1}\mathcal{O} : S^{-1}\mathfrak{a})$.

c) Sei nun $S = \mathcal{O} \setminus \mathfrak{p}$ für ein Primideal $\mathfrak{p} \neq 0$. Zeige für alle $i \geq 0$ und $\alpha \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ die Gleichheit $S^{-1}\mathfrak{p}^i = \alpha S^{-1}\mathcal{O}$. ($S^{-1}\mathcal{O}$ ist also ein diskreter Bewertungsring.)

a) Ein beliebiges Element der linken Seite ist von der Form $\frac{1}{s}\sum_i a_i b_i$ mit $s \in S, a_i \in \mathfrak{a}$ und $b_i \in \mathfrak{b}$. Offensichtlich gilt:

$$\frac{1}{s}\sum_i a_i b_i = \sum_i \frac{a_i}{s}\frac{b_i}{1} \in (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}).$$

Sei umgekehrt $\sum_i \frac{a_i}{s_i}\frac{b_i}{t_i} \in (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$. Wir setzen $s := \prod_i s_i$ und $t := \prod_i t_i$ und definieren $\hat{s}_i$ bzw. $\hat{t}_i$ durch die Gleichungen $s = \hat{s}_i s_i$ bzw. $t = \hat{t}_i t_i$. Dann gilt:

$$\sum_i \frac{a_i}{s_i}\frac{b_i}{t_i} = \frac{1}{st}\sum_i \hat{s}_i \hat{t}_i a_i b_i \in S^{-1}(\mathfrak{a}\mathfrak{b}).$$

b) Sei $\frac{x}{s}$ mit $x\mathfrak{a} \subseteq \mathcal{O}$ und $s \in S$ gegeben. Sei $\frac{a}{t} \in S^{-1}\mathfrak{a}$, also $a \in \mathfrak{a}$ und $t \in S$. Dann folgt

$$\frac{x}{s}\frac{a}{t} = \frac{1}{st}xa \in S^{-1}\mathcal{O},$$

also $\frac{x}{s} \in (S^{-1}\mathcal{O}, S^{-1}\mathfrak{a})$.

Sei umgekehrt $x \in K$ und es gelte $\frac{xa}{s} \in S^{-1}\mathcal{O}$ für alle $a \in \mathfrak{a}$ und $s \in S$. Es ist zu zeigen: $x \in S^{-1}(\mathcal{O} : \mathfrak{a})$. Sei dazu $a_1, \ldots, a_n$ ein $\mathcal{O}$-Erzeugendensystem von $\mathfrak{a}$. Dann gilt:

$$\begin{aligned}
& x \in (S^{-1}\mathcal{O} : S^{-1}\mathfrak{a}) \\
\iff \quad & xa_i \in S^{-1}\mathfrak{a}, \forall i = 1, \ldots, n, \\
\iff \quad & \forall i \exists r_i \in \mathcal{O}, s_i \in S\colon xa_i = \frac{r_i}{s_i} \\
\iff \quad & \forall i \exists r_i \in \mathcal{O}, s_i \in S\colon s_i x a_i = r_i.
\end{aligned}$$

Es folgt $(s_1 \cdots s_n)xa_i \in \mathcal{O}$ für alle i, also $(s_1 \cdots s_n)x \in (\mathcal{O} : \mathfrak{a})$, bzw. $x \in S^{-1}(\mathcal{O} : \mathfrak{a})$.

c) Nach Voraussetzung ist $\alpha\mathcal{O} = \mathfrak{p}^i\mathfrak{b}$ mit $\mathfrak{b} + \mathfrak{p} = \mathcal{O}$. Also gibt es ein $b \in \mathfrak{b} \setminus \mathfrak{p}$ und es folgt $1 = \frac{b}{b} \in S^{-1}\mathfrak{b}$.

Mit Teilaufgabe a) gilt weiter $\alpha S^{-1}\mathcal{O} = S^{-1}(\alpha\mathcal{O}) \overset{a)}{=} S^{-1}\mathfrak{p}^i \cdot S^{-1}\mathfrak{b} = S^{-1}\mathfrak{p}^i$.