# Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 10

## 1 Allgemeine Hinweise

Maximale Punktzahl die man in diesem Arbeitsblatt erwerben kann sind 10 Punkte. Aufgaben können frei gewählt werden.

Lösungen werden nächste Woche (Donnerstag) sowohl elektronisch (als PDF) bereitgestellt, wie auch in der Vorlesungszeit (12:15 – 13:45) live/online von mir via Zoom erklärt.

Bei Unverständnissen, Fragen oder wenn Ihr Fehler findet, bitte an
ilia.pirashvili@math.uni-augsburg.de
wenden.

**Die Punkte der Arbeitsblätter werden in die Endnote eingehen! Abgabefirst ist bis einschließlich Mittwoch (01/07).** Viel Glück und viel Erfolg.

## 2 Aufgaben

*Aufgabe* 1 (1 Punkt). Zur Erinnerung, für einen Zahlenring $\mathfrak{o}_K$, bezeichnen wir mit $\mathcal{I}^*$ die Menge der Ideale von $\mathfrak{o}_K$ ungleich Null. Mit $\mathfrak{o}_K^*$ bezeichnen wir die Menge der Bruchideale ungleich Null. Beweise folgende Aussagen:

1. Die Menge $\mathcal{I}^*$ ist ein Monoid (unter dem Produkt);
2. Die Menge $\mathcal{I}_K^*$ ist ein Monoid (unter dem Produkt).

**Lösung.** Dass das Produkt assoziativ ist und (1) die Einzeit ist wissen wir schon. Des weiteren ist jedes Ideal auch ein Bruchideal. Daher bleibt es nur zu zeigen, dass das Produkt von zwei Bruchidealen $I, J \neq 0$ ungleich Null, wieder ungleich Null ist.

Sein also $I, J \neq 0$ Bruchideale. Wir brauchen nur zu zeigen, dass $IJ \neq 0$. Dies ist jedoch trivial, da, bei Annahme, es $0 \neq i \in I$ und $0 \neq j \in J$ gibt. Da $\mathfrak{o}_K$ ein Integritätsbereich ist, folgt, dass $ij \in IJ$ auch ungleich Null ist. Daher ist $IJ \neq 0$. □

*Aufgabe* 2 (2 Punkte). Sei $\mathfrak{o}_K = \mathbb{Z}$. Entscheide, mit Begründung, welche dieser Mengen ein Bruchideal definiert:

i) $\frac{1}{2}\mathbb{Z} = \left\{\frac{n}{2}, n \in \mathbb{Z}\right\}$

ii) $\mathbb{Z}_2 = \left\{\frac{n}{2^m}, n, m \in \mathbb{Z}\right\}$

iii) $\mathbb{Z}_{\langle 2\rangle} = \left\{\frac{n}{2m}, n, m \in \mathbb{Z}\right\}$

iv) $\mathbb{Z}_{(2)} = \left\{\frac{n}{2m+1}, n, m \in \mathbb{Z}\right\}$

**Lösung.** i) Dies ist ein Bruchideal, da $2 \cdot \frac{1}{2}\mathbb{Z} = \mathbb{Z} \subseteq \mathbb{Z} = \mathfrak{o}_K$ gilt.

ii) Dies ist kein Bruchideal: Angenommen, es gibt ein $0 \neq x \in \mathbb{Z}$, so dass $x \cdot \mathbb{Z}_2 \subseteq \mathbb{Z}$ gilt. Da $\frac{1}{2^m} \in \mathbb{Z}_2$ für jeden $m \in \mathbb{N}$, müsste $\frac{x}{2^m} \in \mathbb{Z}$ gelten für jeden $m$ gelten. Dies ist natürlich nicht der Fall.

Das selbe Argument gilt auch für iii) und iv). Keines von denen ist ein Bruchideal. □

*Aufgabe* 3 (4 Punkte). Berechne die Inverse der folgenden Ideale:

i) (1 Teilpunkt) $\mathfrak{a} = (2) \subseteq \mathfrak{o}_{\mathbb{Q}}$,

ii) (1 Teilpunkt) $\mathfrak{b} = (2) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$,

iii) (1 Teilpunkt) $\mathfrak{c} = (\sqrt{3}) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$,

iv) (1 Teilpunkt) $\mathfrak{d} = (2, \sqrt{3}) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$.

**Lösung.** Wir benutzen einfach die Definition $I^{-1} = \{x \in K \mid xI \subseteq \mathfrak{o}_K\}$. Es gilt

i) $(2)^{-1} = \{r \in \mathbb{Q} \mid r(2) \subseteq \mathfrak{o}_K = \mathbb{Z}\} = \{r \in \mathbb{Q} \mid 2r \in \mathbb{Z}\} = \left\{\frac{n}{2} \mid n \in \mathbb{Z}\right\}$.

ii) $(2)^{-1} = \{\alpha \in \mathbb{Q}(\sqrt{3}) \mid \alpha(2) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt{3}]\} = \{r + s\sqrt{3} \mid r, s \in \mathbb{Q}, 2(r + s\sqrt{3}) \in \mathbb{Z}[\sqrt{3}]\} = \left\{\frac{n}{2} + \frac{m}{2}\sqrt{3} \mid n, m \in \mathbb{Z}\right\}$.

iii) $(\sqrt{3})^{-1} = \{\alpha \in \mathbb{Q}(\sqrt{3}) \mid \alpha(\sqrt{3}) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt{3}]\} = \{r + s\sqrt{3} \mid r, s \in \mathbb{Q}, \sqrt{3}(r + s\sqrt{3}) \in \mathbb{Z}[\sqrt{3}]\} = \{r + s\sqrt{3} \mid r, s \in \mathbb{Q}, r\sqrt{3} + 3s \in \mathbb{Z}[\sqrt{3}]\} = \left\{n + \frac{m}{3}\sqrt{3} \mid n, m \in \mathbb{Z}\right\}$.

iii) Hier suchen wir nach $r + s\sqrt{3}$, so dass sowohl $2r, 2s \in \mathbb{Z}$, wie auch $r, 3s \in \mathbb{Z}$ gilt. Daher $(2, \sqrt{3})^{-1} = \left\{n + m\sqrt{3} \mid n, m \in \mathbb{Z}\right\} = \mathfrak{o}_K$. Dies hätte man auch direkt merken können, da $\mathfrak{d} = (2, \sqrt{3}) = (2, \sqrt{3}, 3) = (1)$ und wir schon wissen, dass $(1)^{-1} = (1)$.

□

*Aufgabe* 4 (3 Punkte). Sei $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-6}]$ mit Ganzheitsbasis $\{1, \sqrt{-6}\}$. Betrachte die Ideale $\mathfrak{a} = (2, \sqrt{-6})$ und$\mathfrak{b} = (3, \sqrt{-6})$).

i) (1 Teilpunkt) Sind $\mathfrak{a}, \mathfrak{b}$ Maximalideale?

ii) (2 Teilpunkte) Berechne das Bruchideal $\mathfrak{a}^{-1}\mathfrak{b}$.

**Lösung.** i) Wir beweisen es durch den ersten Isomorphiesatz: Sein $R = \mathbb{Z}[X], I = (x^2 + 6)$ und $J = (x^2+6, 2, x) = (2, x)$. Dann ist $R/I = \mathbb{Z}[\sqrt{-6}], J/I = (2, \overline{x})$, oder anders gesagt $J/I = (2, \sqrt{-6}) \subseteq \mathbb{Z}[\sqrt{-6}]$. Es folgt $\mathbb{Z}[\sqrt{-6}]/(2, \sqrt{-6}) \simeq \mathbb{Z}[X]/(2, x) \simeq \mathbb{Z}/2\mathbb{Z}$, was natürlich ein Körper ist. Als solches ist $\mathfrak{a}$ ein Maximalideal. Genauso für $\mathfrak{b}$.

Alternativ kann man es zeigen, indem man eine Abbildung

$$\lambda : \mathfrak{o}_K \to \mathbb{F}_2 \quad \text{mit} \quad \sqrt{-6} \mapsto 0$$

aufbaut. Es ist klar, dass $\sqrt{-6} \in \mathsf{Ker}(\lambda)$. Es ist auch $2 \in \mathsf{Ker}(\lambda)$, da es in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ abbildet. Daher ist das Kern genau unser Maximalideal $\mathfrak{a}$.

ii) Ein Element $a + b\sqrt{-6}$ ist in $\mathfrak{a}^{-1}$ genau dann wenn

$$2(a + b\sqrt{-6}) \in \mathfrak{o}_K$$

und

$$\sqrt{-6}(a + b\sqrt{-6}) \in \mathfrak{o}_K.$$

Daher, genau dann wenn

$$2a, 2b \in \mathbb{Z} \quad \text{und} \quad a, 6b \in \mathbb{Z}.$$

Dies ist äquivalent zu sagen, dass $a, 2b \in \mathbb{Z}$. Also gilt

$$\mathfrak{a}^{-1} = \frac{1}{2}(2, \sqrt{-6}).$$

Es folgt

$$\mathfrak{a}^{-1}\mathfrak{b} = \frac{1}{2}(2, \sqrt{-6})(3, \sqrt{-6}) = \frac{1}{2}(\sqrt{-6}).$$

□

Ein Noetherscher Ring $R$ heißt *Dedekindring*, wenn es ein Integritätsbereich ist und jedes Ideal eine Zerlegung in Primideale hat. Das heißt, wenn für jeden $\mathfrak{a} \subseteq R$, es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, so dass

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Diese Zerlegung wird dann eindeutig sein (dies kann Bewiesen werden). Für Dedekindringe kann man Bruchideale genau so wie für Zahlenringe einführen und die Bruchideale eines Dedekindringes bilden eine Gruppe unter der Multiplikation, mit $R = (1)$ als die Einheit.

*Aufgabe* 5 (5 Punkte). Sei $R$ ein Dedekindring und $S \subseteq R$ ein Untermonoid.

i) (2 Teilpunkte) Beweise, dass die Lokalisation $S^{-1}R$ ein Dedekindring ist.

ii) (3 Teilpunkte) Sei $\mathfrak{a} \subseteq Q(K)$ ein Bruchideal von $R$.

ii a) Zeige, dass $S^{-1}\mathfrak{a}$ ein Bruchideal von $S^{-1}R$ ist.

ii) b) Zeige, dass die Abbildung $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ einen Gruppenhomomorphismus zwischen den Bruchidealen von $R$ und den Bruchidealen von $S^{-1}R$ definiert.

**Lösung.** Wir verwenden folgende einfach-zu-überprüfende Fakten: Sei $A$ ein Ideal von $R$. Dann ist $S^{-1}A$ ein Ideal von $S^{-1}R$. Sei $f$ die kanonische Abbildung $R \to S^{-1}R$. Wenn $C$ ein Ideal von $S^{-1}R$ ist, dann ist

$$f^{-1}(C) = \{r \in R | \frac{r}{1} \in C\}$$

ein Ideal von $R$ und

$$S^{-1}(f^{-1}(C)) \to C$$

ist eine Isomorphie.

i) Wenn

$$C_1 \subset C_2 \subset C_3 \subset \cdots$$

eine Sequenz von Idealen von $S^{-1}R$ ist, ist

$$f^{-1}(C_1) \subset f^{-1}(C_2) \subset \cdots$$

eine Sequenz von Idealen in $R$. Da $R$ Noethersch ist, gibt es ein $n$, so dass

$$f^{-1}(C_i) = f^{-1}(C_n)$$

für alle $i > n$. Daher haben wir auch

$$C_i = S^{-1}f^{-1}(C_i) = S^{-1}f^{-1}(C_n) = C_n, i > n,$$

was die Noetherheit von $S^{-1}R$ beweist.

Sei $\mathfrak{q}$ ein Primideal von $S^{-1}R$. Dann ist $f^{-1}(\mathfrak{q})$ ein Primideal von $R$. Wenn $\mathfrak{p}$ ein Primideal von $R$ ist, dann ist $S^{-1}\mathfrak{p}$ ein Primideal von $S^{-1}R$, sofern $S \cap \mathfrak{p} = \varnothing$. (Ohne diese Bedingung ist es kein Ideal).

Sei $C$ ein Ideal von $S^{-1}R$. Bei Annahme hat $f^{-1}(C)$ eine eindeutige Zerlegung in Primideale

$$f^{-1}(C) = \mathfrak{p}_1 \cdots \mathfrak{p}_k,$$

von $R$. Nach Neuordnung können wir annehmen, dass $\mathfrak{p}_i \cap S = \varnothing$ für $i = 1, \cdots, m$ und $\mathfrak{p}_i \cap S = \varnothing$ für all $m < i \leq n$, mit geeignetem $1 \leq m \leq n$. Dann haben wir

$$C = S^{-1}f^{-1}(C) = S^{-1}\mathfrak{p}_1 \cdots S^{-1}\mathfrak{p}_m.$$

Dies zeigt, dass jedes Ideal von $R$ eine Zerlegung in Primideale hat. Es bleibt zu zeigen, dass diese Zerlegung eindeutig ist. Sei

$$\mathfrak{q}_1 \cdots \mathfrak{q}_k = \mathfrak{q}'_1 \cdots \mathfrak{q}'_l,$$

wobei die $\mathfrak{q}_i$'s und $\mathfrak{q}_i'$'s Primideal von $S^{-1}R$ sind. Durch $f^{-1}$ erhalten wir

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{p}_1' \cdots \mathfrak{p}_l',$$

wobei $\mathfrak{p}_i = f^{-1}(\mathfrak{q}_i)$ und $\mathfrak{p}_i' = f^{-1}(\mathfrak{q}_i')$. Da $R$ ein Dedekind ring ist, haben wir $k = l$ nach Neuordnung $\mathfrak{p}_i = \mathfrak{p}_i'$. Daher ist $\mathfrak{q}_i = S^{-1}(\mathfrak{p}_i) = S^{-1}(\mathfrak{p}_i)' = \mathfrak{q}_i'$ und Eindeutigkeit folgt. Daher ist $S^{-1}R$ also ein Dedekind Ring.

ii) Sei $\mathfrak{a} \subseteq K$ ein Bruchideal von $R$. Es gibt eine natürliche Zahl $n$, so dass $n\mathfrak{a}$ ein Ideal ist. Daher ist

$$S^{-1}(n\mathfrak{a})$$

ein Ideal in $S^{-1}R$. Es folgt, dass

$$nS^{-1}(\mathfrak{a}) = S^{-1}(n\mathfrak{a}) \subset S^{-1}R$$

ein Ideal von $S^{-1}R$ ist und $S^{-1}(\mathfrak{a})$ ist ein Bruchideal.

iii) Dies folgt von der Tatsache, dass

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

was wie folgt bewiesen werden kann:

Ein allgemeines Element der rechten Seite ist von der Form

$$\frac{a}{s}\frac{b}{t} \in K,$$

so dass $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ und $s, t \in S$. Das selbe Element kann auch als $\frac{ab}{st}$ geschrieben werden, was in der linken Seite liegt.

Sei nun $\frac{ab}{s}$ ein Element der linken Seite, wobei $s \in S$, $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$. Diese Element ist das selbe wie $\frac{a}{s}\frac{b}{1}$, was ein Element der rechten Seite ist. □