Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§2.2 Dedekindringe [Julius Wilhelm Richard Dedekind *1831 †1916]

Erinnerung 2.2.1. Sei R ein kommutativer Ring.

(a) Ein Ideal $\mathfrak{p}$ in R heißt prim (oder Primideal), wenn

$$1 \notin \mathfrak{p} \text{ und } \forall a, b \in R : (ab \in \mathfrak{p} \implies (a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p})).$$

(b) Ein Element $p \in R$ heißt prim (oder Primelement), wenn (p) ein Primideal ist, das heißt [→LA16.4.1]

$$p \notin R^\times \text{ und } \forall a, b \in R : (p|ab \implies (p|a \text{ oder } p|b)).$$

(c) Sind $I_1, \dots, I_n$ Ideale von R, so nennt man

$$\prod_{k=1}^{n} I_k := I_1 \cdots I_n := (\{a_1 \cdots a_n \mid a_1 \in I_1, \dots, a_n \in I_n\})$$
$$= \begin{cases} R & \text{falls } n = 0 \\ \{\sum_i a_{i1} \cdots a_{in} \mid a_{i1} \in I_1, \dots, a_{in} \in I_n\} & \text{falls } n \geq 1 \end{cases}$$

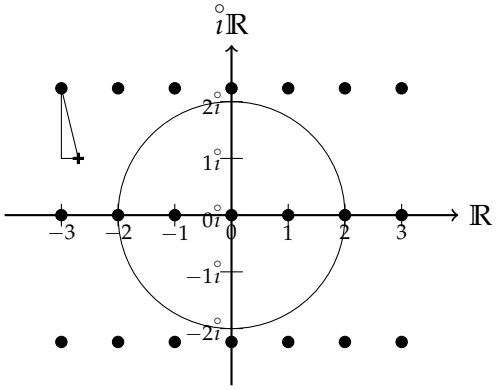
deren *Produkt*. .

(d) In Integritätsringen sind Primfaktorzerlegungen (im Wesentlichen) eindeutig, das heißt ist R Integritätsring, $m, n \in \mathbb{N}_0$ und sind $p_1, \dots, p_m, q_1, \dots, q_n \in R \setminus \{0\}$ prim mit $p_1 \cdots p_m = q_1 \cdots q_n$, so gilt $m = n$ und es gibt $\sigma \in S_n$ mit $(p_i) = (q_{\sigma(i)})$ für $i \in \{1, \dots, n\}$ [→LA16.4.13] (vergleiche auch 1.4.17(b)).

(e) R heißt faktoriell, wenn R ein Integritätsring ist und jedes $a \in R$ eine Primfaktorzerlegung besitzt, das heißt es gibt $c \in R^\times$, $n \in \mathbb{N}_0$ und Primelemente $p_1, \dots, p_n \in R$ mit $a = cp_1 \cdots p_n$ [→LA16.4.14].

(f) R euklidisch $\overset{1.6.3}{\implies}$ R Hauptidealring $\overset{\text{LA16.4.19}}{\implies}$ R faktoriell $\overset{\text{per Def.}}{\implies}$ R Integritätsring

Beispiel 2.2.2. Wegen $-5 \equiv_{(4)} -1 \equiv_{(4)} 3$ sind $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[\mathring{i}]$ und $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\sqrt{5}\mathring{i}]$ quadratische Zahlringe [→2.1.17]. Der Beweis von 1.6.2(c) dafür, dass $\mathbb{Z}[\sqrt{-1}]$ euklidisch ist, funktioniert für $\mathbb{Z}[\sqrt{-5}]$ nicht mehr, da man nur noch $\left|\frac{a}{b} - q\right|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{5}}{2}\right)^2 = \frac{1}{4} + \frac{5}{4} = \frac{6}{4}$ erhält, aber $\frac{6}{4} \geq 1$ ist (siehe Bild unten).



Tatsächlich ist $\mathbb{Z}[\sqrt{-5}]$ nicht einmal faktoriell, denn 2 besitzt darin keine Primfaktorzerlegung, weil sonst 2 prim in $\mathbb{Z}[\sqrt{-5}]$ sein müsste (siehe Bild oben), was aber nicht der Fall ist, denn $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$, aber $2 \nmid (1+\sqrt{-5})$ und $2 \nmid (1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Andererseits besitzt (2) eine *Primidealzerlegung*, das heißt ist Produkt von Primidealen, denn $(2, 1+\sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$ ist ein Primideal mit $(2,1+\sqrt{-5})^2 = (2,1+\sqrt{-5})(2,1+\sqrt{-5}) = (4, 2+2\sqrt{-5}, 1+2\sqrt{-5}-5) = (4, 2+2\sqrt{-5}, 2\sqrt{-5}) = (4,2,2\sqrt{-5}) = (2)$. Dass $(2,1+\sqrt{-5})$ prim (sogar maximal) ist, folgt daraus, dass es der Kern des Ringhomomorphismus

$$\varphi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_2,\ a+b\sqrt{-5} \mapsto \overline{a+b} \qquad (a,b \in \mathbb{Z})$$

ist, wie man unter Beachtung von $\varphi(\sqrt{-5})^2 = 1 = -5$ in $\mathbb{F}_2$ sofort nachrechnet.

Motivation 2.2.3. Zahlringe spielen eine wichtige Rolle bei der Untersuchung arithmetischer Eigenschaften von $\mathbb{Z}$. Leider sind sie nicht immer faktoriell. Der Ausweg wird sein, statt Elementen Ideale und statt Primelementen Primideale zu betrachten.

Definition 2.2.4. [vergleiche 2.2.1(e)] Ein Integritätsring heißt *Dedekindring*, wenn darin jedes Ideal ein Produkt von Primidealen ist.

Beispiel 2.2.5. Jeder Hauptidealring ist ein Dedekindring.

Definition 2.2.6. Sei A ein Integritätsring. Ein *gebrochenes Ideal* von A ist ein A-Untermodul I von $\mathrm{qf}(A)$ mit $sI \subseteq A$ für ein $s \in A \setminus \{0\}$. Zyklische [→1.1.4(d)] gebrochene Ideale nennt man *gebrochene Hauptideale*.

Bemerkung 2.2.7. Sei A ein Integritätsring.

(a) Jedes gebrochene Ideal von A ist als A-Modul isomorph zu einem Ideal von A (ist nämlich $s \in A \setminus \{0\}$ mit $sI \subseteq A$, so $I \xrightarrow{\cong} sI,\ a \mapsto sa$).

(b) Die gebrochenen Ideale von A sind genau die $s^{-1}I$ ($s \in A \setminus \{0\}$, I ein Ideal von A).

(c) A ist ein Hauptidealring genau dann, wenn jedes gebrochene Ideal von A ein gebrochenes Hauptideal von A ist.

(d) Jeder endlich erzeugte A-Untermodul von $\mathrm{qf}(A)$ ist ein gebrochenes Ideal.

(e) Ist A noethersch, so sind die gebrochenen Ideale von A genau die endlich erzeugten A-Untermoduln von $\mathrm{qf}(A)$.

Proposition und Definition 2.2.8. Seien A ein Integritätsring und I, J gebrochene Ideale von A. Dann sind auch $I + J$, $I \cap J$, $IJ := \{\sum_i a_i b_i \mid a_i \in I, b_i \in J\}$ und für $J \neq 0$ auch $I : J := \{a \in \mathrm{qf}(A) \mid aJ \subseteq I\}$ gebrochene Ideale von A.

Beweis. Mit I und J sind auch $I + J$, $I \cap J$ (trivial!), IJ und $I : J$ A-Untermoduln von $\mathrm{qf}(A)$ (nachrechnen!). Sind $s, t \in A \setminus \{0\}$ mit $sI \subseteq A$ und $tJ \subseteq A$, so $st(I + J) \subseteq A$, $s(I \cap J) \subseteq A$ und $(st)IJ \subseteq A$. Ist ferner $J \neq 0$, so gibt es $b \in J \cap (A \setminus \{0\})$ und es gilt für $a \in I : J$, dass $(sb)a = s(ab) \in s(aJ) \subseteq sI \subseteq A$, also $sb(I : J) \subseteq A$. □

Definition und Proposition 2.2.9. Sei A ein Integritätsring und I ein gebrochenes Ideal von A. Dann heißt I *invertierbar*, wenn es ein gebrochenes Ideal J von A gibt mit $IJ = A$. In diesem Fall gilt $J = I^{-1} := A : I$ und I und J sind endlich erzeugt.

Beweis. Gelte $IJ = A$. Dann $J \subseteq A : I = (A : I)IJ \subseteq AJ = J$, also $J = A : I$. Schreibe $1 = \sum_i a_i b_i$ mit $a_i \in I$ und $b_i \in J$. Dann

$$I = \left(\sum_i a_i b_i\right) I = \sum_i \underbrace{(b_i I)}_{\subseteq A} a_i \subseteq \sum_i A a_i \subseteq I,$$

womit $I = \sum_i A a_i$ endlich erzeugt ist. Analog für J. □

Beispiel 2.2.10. Jedes gebrochene Hauptideal $\neq 0$ eines Integritätsrings ist invertierbar.

Satz 2.2.11. [Eindeutigkeit der Primidealzerlegung invertierbarer Ideale, unter Beachtung von 2.2.10 und 2.2.1(b) Verallgemeinerung von 2.2.1(d)] *Sei A ein Integritätsring und I ein Ideal in A, was als gebrochenes Ideal invertierbar ist. Seien $m, n \in \mathbb{N}_0$ und $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ Primideale in A mit*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m = I = \mathfrak{q}_1 \cdots \mathfrak{q}_n.$$

Dann gilt $m = n$ und es gibt $\sigma \in S_n$ mit $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ für alle $i \in \{1, \ldots, n\}$.

Beweis. Induktion nach m.

$\underline{m = 0}$ ✓

$\underline{m - 1 \to m \ (m \in \mathbb{N})}$ Mit I sind alle $\mathfrak{p}_i$ und $\mathfrak{q}_j$ invertierbar. Aus $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{p}_1$ folgt, dass es ein j mit $\mathfrak{q}_j \subseteq \mathfrak{p}_1$ gibt (insbesondere $n \geq 1$), denn andernfalls gäbe es $b_1 \in \mathfrak{q}_1 \setminus \mathfrak{p}_1, \ldots, b_n \in \mathfrak{q}_n \setminus \mathfrak{p}_1$ und $b_1 \cdots b_n \in \mathfrak{q}_1 \cdots \mathfrak{q}_n \setminus \mathfrak{p}_1$ ↯. Œ $j = 1$. Nun ist $\mathfrak{p}_1^{-1}\mathfrak{q}_1$ ein Ideal von A, denn $\mathfrak{p}_1^{-1}\mathfrak{q}_1 \subseteq \mathfrak{p}_1^{-1}\mathfrak{p}_1 = A$, weshalb $\mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{q}_1) = \mathfrak{q}_1$ impliziert, dass $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$ oder $\mathfrak{p}_1^{-1}\mathfrak{q}_1 \subseteq \mathfrak{q}_1$, aber letzteres ist unmöglich, da sonst $A = \mathfrak{p}_1\mathfrak{p}_1^{-1}\mathfrak{q}_1\mathfrak{q}_1^{-1} \subseteq \mathfrak{p}_1\mathfrak{q}_1\mathfrak{q}_1^{-1} = \mathfrak{p}_1$ ↯. Also $\mathfrak{q}_1 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{q}_1$ und daher $\mathfrak{p}_1 = \mathfrak{q}_1$. Somit $\mathfrak{p}_2 \cdots \mathfrak{p}_m = I\mathfrak{p}_1^{-1} = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. Wende nun IV an. □

Satz 2.2.12. *Sei A ein Dedekindring. Dann gilt:*

(a) *Jedes Ideal $\neq (0)$ von A ist invertierbar.* [→2.2.9]

(b) *A ist ganz abgeschlossen.* [→2.1.12(b)]

(c) *A ist noethersch.* [→1.4.2(a)]

(d) *In A ist jedes Primideal $\neq (0)$ maximal.*

Beweis. Behauptung 1: Jedes invertierbare Primideal von A ist maximal [in (d) wird dies sogar für alle Primideale $\neq (0)$ behauptet].

Begründung: Sei $\mathfrak{p}$ ein invertierbares Primideal von A. Wir zeigen, dass $A/\mathfrak{p}$ ein Körper ist. Sei hierzu $a \in A$ mit $\overline{a} \neq 0$ in $A/\mathfrak{p}$, das heißt $a \notin \mathfrak{p}$. Zu zeigen: $\overline{a} \in (A/\mathfrak{p})^\times$. Es reicht, $I := aA + \mathfrak{p} = A$ zu zeigen. Da $\mathfrak{p}$ invertierbar ist, reicht es $a\mathfrak{p} + \mathfrak{p}^2 = \mathfrak{p}$ zu zeigen. Wir zeigen zunächst $I^2 = J := a^2A + \mathfrak{p}$, was wegen $I^2 = a^2A + a\mathfrak{p} + \mathfrak{p}^2$ eine Abschwächung der Behauptung ist. Wir wissen $(I/\mathfrak{p})^2 = J/\mathfrak{p}$. Da A ein Dedekindring ist, gibt es $m, n \in \mathbb{N}_0$ und Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ von A mit $I = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ und $J = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Es gilt $\mathfrak{p} \subseteq I \subseteq \mathfrak{p}_i$ für alle $i \in \{1, \ldots, m\}$ und $\mathfrak{p} \subseteq J \subseteq \mathfrak{q}_j$ für alle $j \in \{1, \ldots, n\}$. Da die Primideale in $A/\mathfrak{p}$ den Primidealen von A entsprechen, die $\mathfrak{p}$ enthalten, erhalten wir im Integritätsring $A/\mathfrak{p}$ die Primidealzerlegungen $I/\mathfrak{p} = (\mathfrak{p}_1/\mathfrak{p}) \ldots (\mathfrak{p}_m/\mathfrak{p})$ und $J/\mathfrak{p} = (\mathfrak{q}_1/\mathfrak{p}) \cdots (\mathfrak{q}_n/\mathfrak{p})$. Es folgt $(\mathfrak{p}_1/\mathfrak{p})^2 \cdots (\mathfrak{p}_m/\mathfrak{p})^2 = (I/\mathfrak{p})^2 = J/\mathfrak{p} = (\mathfrak{q}_1/\mathfrak{p}) \cdots (\mathfrak{q}_n/\mathfrak{p})$. Da $J/\mathfrak{p} = (\overline{a}^2) \neq 0$ als Hauptideal nach 2.2.10 invertierbar ist, folgt mit 2.2.11 Œ $(\mathfrak{p}_1/\mathfrak{p}, \mathfrak{p}_1/\mathfrak{p}, \ldots, \mathfrak{p}_m/\mathfrak{p}, \mathfrak{p}_m/\mathfrak{p}) = (\mathfrak{q}_1/\mathfrak{p}, \ldots, \mathfrak{q}_n/\mathfrak{p})$ und daher

$$(\mathfrak{p}_1, \mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{p}_m) = (\mathfrak{q}_1, \ldots, \mathfrak{q}_n).$$

Also $I^2 = J$. Um schließlich $a\mathfrak{p} + \mathfrak{p}^2 = \mathfrak{p}$ zu zeigen, sei $b \in \mathfrak{p}$. Zu zeigen: $b \in a\mathfrak{p} + \mathfrak{p}^2$. Wegen $b \in J$ gilt $b \in I^2 = a^2A + a\mathfrak{p} + \mathfrak{p}^2$. Schreibe $b = a^2c + b'$ mit $c \in A$ und $b' \in a\mathfrak{p} + \mathfrak{p}^2$. Dann $a^2c = b - b' \in \mathfrak{p}$ und daher $c \in \mathfrak{p}$. Somit auch $b \in a\mathfrak{p} + \mathfrak{p}^2$.

Behauptung 2: Jedes Primideal $\neq (0)$ von A ist invertierbar [in (a) wird dies sogar für alle Ideale $\neq (0)$ behauptet].

Begründung. Sei $\mathfrak{p} \neq (0)$ ein Primideal von A. Wähle $a \in \mathfrak{p} \setminus \{0\}$. Schreibe $aA = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ mit Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ von A. Da aA invertierbar ist [→2.2.10] ist es auch jedes $\mathfrak{p}_i$. Wegen $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}$ ist aber $\mathfrak{p}$ eines dieser $\mathfrak{p}_i$, denn es gibt ein i mit $\mathfrak{p}_i \subseteq \mathfrak{p}$ und $\mathfrak{p}_i$ ist maximal nach Behauptung 1.

Wegen der Existenz von Primidealzerlegungen in A folgt aus Behauptung 2 sofort (a). Damit ist Behauptung 1 gleichbedeutend mit (d). Aus (a) folgt (c) mit 2.2.9. Um schließlich (b) zu zeigen, sei $a \in \mathrm{qf}(A)$ ganz über A. Dann ist $A[a]$ ein endlich erzeugter A-Modul [→2.1.5] und damit ein gebrochenes Ideal von A [→2.2.7(d)], das nach (a) invertierbar ist. Aus $A[a]^2 \subseteq A[a]$ folgt daher $A[a] \subseteq A$ und daher $a \in A$ wie gewünscht. □