Bachelorarbeit

Moduln über Dedekindringen

Betreuung
Prof. Dr. Jan Kohlhaase
Fakultät für Mathematik
Universität Duisburg-Essen

vorgelegt von:
Michael Ingelski

Inhaltsverzeichnis

Einleitung

Das Ziel dieser Arbeit ist die Erarbeitung einiger Struktursätze von Moduln über Dedekindringen.
Der erste Teil stützt sich größtenteils auf das Vorlesungsskript zur Zahlentheorie I Wintersemester 2019/20 an der Universität Duisburg-Essen, gehalten von Herrn Prof. Dr. Kohlhaase und die vorige Version des Skripts.
Der zweite Teil basiert auf dem Artikel „Projective Modules Over Dedekind Domains“ von Michelis Kosters, zu finden unter:
https://www.math.leidenuniv.nl/~edix/tag_2009/michiel_3.pdf
Es wird im Folgenden angenommen, dass der Leser mit der linearen Algebra vertraut ist, sowie mit den Grundzügen der Galoistheorie und der kommutativen Algebra.

Konventionen, Notationen:
• Alle Ringe werden als kommutativ mit Eins angenommen.
• Mit (x) bzw. $(x_1, \ldots, x_n)$ bzw. (M) bezeichnen wir die von x bzw. von $x_1, \ldots, x_n$ bzw. von M erzeugte Unterstruktur in der entsprechenden Oberstruktur. Diese wird manchmal mit angegeben, insbesondere immer dann, wenn z.B. innerhalb von Ringerweiterungen Mehrdeutigkeiten bestehen können. Die Beziehung Unterstruktur/Struktur ist z.B. Ideal/Ring, Untermodul/Modul, Untervektorraum/Vektorraum u.s.w....
• Für ein ganzes Element x in einer Ringerweiterung wird eine normierte Gleichung, dessen Nullstelle x ist, manchmal als eine „ganze Gleichung von x“ bezeichnet.
• Unter einer „Ringerweiterung $S|R$ von endlichem Typ“ verstehen wir eine Erweiterung der Form $S = R[s_1, \ldots, s_n]$, für endlich viele $s_i \in S$.
• Ein R-Modul heißt für uns noethersch, wenn alle (R-)Untermoduln endlich erzeugt sind. Äquivalente Bedingungen schlage man in **[AK]** (16.11) (Noetherian Modules) nach.

Die beiden Teile der Arbeit sind einzeln nummeriert. Falls wir in Teil II auf einen Satz aus dem ersten Teil verweisen, tun wir dies mit entsprechendem Zusatz.
Zu allen Behauptungen, die nicht im Hauptteil bewiesen werden wird eine Referenz zu einem Standardwerk angegeben. Ohne Referenz sind nur der Chinesische Restsatz, das Lemma von Zorn und die Eigenschaften einer Vandermonde Matrix angegeben.

Teil I
Allgemeine Theorie von Dedekindringen

1 Ganze Ringerweiterungen

Wir fangen mit der Vorbereitung einiger Grundlagen an, auf die wir uns im weiteren Verlauf stützen werden. Für eine Ringerweiterung $S|R$ bezeichnen wir mit $\mathrm{A}_S(R)$ den ganzen Abschluss von R in S.

Proposition 1.1
Für eine Ringerweiterung $S|R$ sind äquivalent:

(i) $S|R$ ist endlich, d.h. S ist als R-Modul endlich erzeugt.

(ii) $S|R$ ist ganz und von endlichem Typ.

(iii) Es existieren ganze Elemente $s_1, \ldots, s_n \in S$ sodass $S = R[s_1, \ldots, s_n]$.

Beweis
$(i) \Rightarrow (ii)$: Sei $S|R$ endlich, $s \in S$ beliebig und $\mu_s : S \to S, x \mapsto sx$. Der Satz von Cayley-Hamilton (siehe **[AK]** (10.1) (Cayley-Hamilton Theorem)) besagt dann, dass

$$\chi(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in R[t]$$

existiert, so, dass $\chi(\mu_s) = 0 \in \mathrm{End}_R(S)$. Durch Einsetzen von 1 in den Endomorphismus $\chi(\mu_s)$, kriegen eine ganze Gleichung von s, also $s \in \mathrm{A}_S(R)$. Damit ist $S|R$ ganz. Außerdem ist jede endliche Ringerweiterung natürlich von endlichem Typ.
$(ii) \Rightarrow (iii)$: Dieser Zusammenhang folgt unmittelbar.
$(iii) \Rightarrow (i)$: Seien nun $s_0, \ldots, s_n \in S$ so gewählt, dass $S = R[s_0, \ldots, s_n]$. Wir zeigen nun per Induktion **über n**, dass $S|R$ endlich ist.
Für $\mathbf{n = 1}$ haben wir $S = R[s]$ und s ist ganz über R. Es gibt also $a_0, \ldots, a_r \in R$, sodass

$$s^{r+1} + a_r s^r + \ldots + a_0 = 0.$$

Es gilt offensichtlich $s^{r+1} \in \mathrm{span}_R\{1, s, s^2, \ldots, s^r\}$. Wir behaupten nun, dass
$s^{n+m} \in \mathrm{span}_R\{1, s, \ldots, s^r\}$ und zeigen dies durch eine weitere Induktion **nach m**.
Den Induktionsanfang für **m=1** haben wir soeben gesehen.
Laut der Induktionsvoraussetzung **für m** gibt es Elemente $b_0, \ldots, b_r \in R$, sodass

$$s^{n+m} = \sum_{j=0}^{r} b_j s^j$$

Nach Multiplikation mit s erhalten wir mit der Induktionsvoraussetzung

$$s^{r+m+1} = \sum_{j=0}^{r-1} b_j s^{j+1} + b_r s^{r+1} \in \mathrm{span}_R\{1, s, \ldots, s^r\},$$

was die Induktion nach **m** abschließt. Soweit bekommen wir $S = R[s] = \mathrm{span}_R\{1, s, \ldots, s^r\}$, was den Induktionsanfang **nach n** beendet.

Sei nun $S = R[s_0, \ldots, s_n, s_{n+1}] = R'[s_{n+1}]$ mit $R' := R[s_0, \ldots, s_n]$, wobei R' nach unserer Induktionsvoraussetzung **nach n** endlich über R ist. Nun ist s_{n+1} ganz über $R \subseteq R'$, also auch über R'. Nach unserem Induktionsanfang ist $S|R'$ endlich. Aus der Transitivität von Endlichkeit folgt nun, dass $S|R$ endlich ist. □

Satz 1.2
Sei $S|R$ eine Ringerweiterung. Dann ist $\mathrm{A}_S(R)$ ein Unterring von S, der R enthält.

Beweis
Für $r \in R$ ist mit $\mu_r(t) := t - r$ ein normiertes Polynom mit Nullstelle r schnell gefunden, d.h. $R \subseteq \mathrm{A}_S(R)$.
Für $s, t \in \mathrm{A}_S(R)$ betrachten wir $R[s,t]$. Die Ringerweiterung $R[s,t]|R$ ist nach Proposition 1.1 ganz. Per Definition ist nun $R[s,t]$ eine Teilmenge von $\mathrm{A}_S(R)$. Dies zeigt, dass die Verknüpfungen $s \pm t, s \cdot t$ $\mathrm{A}_S(R)$ von beliebigen Elementen s, t in $\mathrm{A}_S(R)$ liegen. □

Satz 1.3
Seien $T|S, S|R$ Ringerweiterungen. Es sind äquivalent:

(i) $T|R$ ganz

(ii) $T|S$ und $S|R$ ganz

Beweis
$(i) \Rightarrow (ii)$: Dieser Zusammenhang ist trivial.
$(ii) \Rightarrow (i)$: Sei $x \in T$. Da x ganz über S ist, gibt es $s_0, \ldots, s_{n-1} \in S$, sodass

$$x^n + s_{n-1}x^{n-1} + \ldots + s_0 = 0.$$

Dies impliziert, dass x ganz über $R[s_0, .., s_n]$ ist. Nach Proposition 1.1 ist die Ringerweiterung $R[s_0, \ldots, s_{n-1}, x]|R[s_0, \ldots, s_{n-1}]$ endlich. Nun sind $s_0, \ldots, s_{n-1}$ ganz über R, das heißt, dass auch $R[s_0, \ldots, s_{n-1}]|R$ endlich ist und deshalb ist auch $R[s_0, \ldots, s_{n-1}, x]|R$ endlich. Wieder nach Proposition 1.1 haben wir $x \in \mathrm{A}_T(R)$ und da x beliebig war ist der Beweis vollendet. □

Definition 1.4
Ein Integritätsbereich R mit Quotientenkörper K heißt ganzabgeschlossen, falls $R = A_K(R)$ gilt.

Lemma 1.5
Sei R ein faktorieller Ring. Dann ist R auch ganzabgeschlossen.

Beweis
Sei $k \in K := \mathrm{Quot}(R)$ ganz über R und

$$k^n + \sum_{i=0}^{n-1} r_i k^i = 0$$

eine ganze Gleichung von k. Wir nehmen eine Darstellung $\frac{a}{b}$ von k, sodass a, b teilerfremd sind und $b \neq 0$. Wenn man die obige Gleichung mit b^n multipliziert erhält man:

$$a^n + \sum_{i=0}^{n-1} r_i b^{n-i} a^i = 0 \Leftrightarrow a^n = \sum_{i=0}^{n-1} -r_i b^{n-i} a^i$$

Da nun auf der rechten Seite der Gleichung in jedem Summanden mindestens ein b vorkommt, ist jeder Primfaktor von b auch einer von a. Da a und b per Annahme keine gemeinsamen Primfaktoren haben, muss b also eine Einheit in R sein. $\square$

2 Dedekindringe und Idealklassengruppen

Wir kommen zu der dieser Arbeit namensgebenden Klasse von Ringen, nämlich zu Dedekindringen.

Definition 2.1
Ein Integritätsbereich R heißt ein Dedekindring, falls gilt:

(i) R ist noethersch.

(ii) R ist ganzabgeschlossen.

(iii) $\dim(R) \leq 1$, wobei damit die Krulldimension gemeint ist.

Beispiele 2.2
Erste Beispiele für Dedekindringe sind Hauptidealringe und damit auch Körper. Hauptidealringe sind offensichtlich noethersch und außerdem ist dort jedes von Null verschiedene Primideal maximal, sodass sie Krulldimension kleiner gleich 1 haben. Mit Lemma 1.5 sind sie als faktorielle Ringe also auch Dedekindringe.

Bevor wir zu einigen Eigenschaften und einer Reihe von weiteren Beispielen kommen, erarbeiten wir uns im Folgenden eine wichtige Charakterisierung von Dedekindringen, die wir im Korollar 2.10 festhalten. Vorher benötigen wir noch etwas Terminologie.

Definition 2.3
Sei R ein Integritätsbereich mit Quotientenkörper K. Ein R-Untermodul $\mathfrak{a} \neq \{0\}$ von K heißt gebrochenes Ideal von R, wenn ein $c \in R \setminus \{0\}$ existiert, mit $c \cdot \mathfrak{a} \subseteq R$.
Falls betont werden soll, dass ein gebrochenes Ideal tatsächlich in R liegt, wird es im folgenden als ganzes Ideal bezeichnet.

Satz 2.4
Sei R ein Integritätsbereich mit Quotientenkörper K und $\mathfrak{a} \neq \{0\}$ ein R-Untermodul von K.

(i) Falls $\mathfrak{a}$ als R-Modul endlich erzeugt ist, so ist $\mathfrak{a}$ ein gebrochenes Ideal.

(ii) Falls $\mathfrak{a}$ ein gebrochenes Ideal ist und R noethersch, so ist $\mathfrak{a}$ als R-Modul endlich erzeugt.

Beweis
(i) Seien $\frac{a_1}{s_1}, \ldots, \frac{a_n}{s_n}$ die R-Erzeuger von $\mathfrak{a}$. Mit $c := s_1 \cdot \ldots \cdot s_n$ haben wir bereits $c \cdot \mathfrak{a} \subseteq R$.
(ii) Sei $c \in R \backslash \{0\}$ mit $c \cdot \mathfrak{a} \subseteq R$. Da R noethersch ist, ist $c\mathfrak{a}$ endlich erzeugt, d.h.

$$c \cdot \mathfrak{a} = \mathrm{span}_R\{b_1, \ldots, b_m\} \text{ für gewisse } b_1, \ldots, b_m \in c\mathfrak{a}.$$

Nun gilt aber auch $\mathfrak{a} = (\frac{1}{c}(c \cdot \mathfrak{a})) = \mathrm{span}_R\{\frac{b_1}{c}, \ldots, \frac{b_m}{c}\}$. Dies beendet den Beweis. □

Definition 2.5

(i) Sei R ein Integritätsbereich und $K := \mathrm{Quot}(R)$. Die Menge der gebrochenen Ideale von R wird mit $\mathbb{I}_R$ bezeichnet.

(ii) Für $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}_R$ definieren wir das Produkt der gebrochenen Ideale als

$$\mathfrak{a} \cdot \mathfrak{b} := \mathrm{span}_R\{a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \subseteq K.$$

(iii) Für $\mathfrak{a} \in \mathbb{I}_R$ definieren wir den R-Untermodul $\mathfrak{a}^{-1}$ von K durch $\mathfrak{a}^{-1} := \{x \in K | x \cdot \mathfrak{a} \subseteq R\}$.

Satz 2.6
Sei R ein Integritätsbereich, $\mathbb{I}_R$ die zugehörige Menge der gebrochenen Ideale.

(i) Für $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}_R$ ist auch $\mathfrak{a} \cdot \mathfrak{b} \in \mathbb{I}_R$. Die Multiplikation $\cdot$ auf $\mathbb{I}_R$ ist assoziativ und kommutativ.

(ii) Es gilt $R \cdot \mathfrak{a} = \mathfrak{a} = \mathfrak{a} \cdot R$ für alle $\mathfrak{a} \in \mathbb{I}_R$.

(iii) $\mathfrak{a}^{-1}$ ist ein gebrochenes Ideal, d.h. $\mathfrak{a}^{-1} \in \mathbb{I}_R$. Es gilt auch $\mathfrak{a}^{-1} \cdot \mathfrak{a} \subseteq R$.
Falls ein $\mathfrak{b} \in \mathbb{I}_R$ mit $\mathfrak{b} \cdot \mathfrak{a} = R$ existiert, so gilt stets $\mathfrak{b} = \mathfrak{a}^{-1}$.

Die Multiplikation der gebrochenen Ideale aus Definition 2.5(ii) ist nach (i) eine kommutative Verknüpfung auf $\mathbb{I}_R$, macht nach (ii) $\mathbb{I}_R$ also zu einem kommutativen Monoid mit neutralem Element R. Falls das in Definition 2.5(iii) definierte und nach (iii) eindeutige bestimmte Ideal $\mathfrak{a}^{-1}$ für alle $\mathfrak{a} \in \mathbb{I}_R$ existiert, wird $\mathbb{I}_R$ also zu einer kommutativen Gruppe. Wir sehen im nächsten Satz, was es bedeutet, dass $\mathbb{I}_R$ eine Gruppe ist.

Beweis
(*i*) Seien für die Abgeschlossenheit $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}_R$ und $c, d \in R \setminus \{0\}$ so gewählt, dass $c \cdot \mathfrak{a} \subseteq R$ und $d \cdot \mathfrak{b} \subseteq R$. Da R nullteilerfrei ist, ist cd von Null verschieden und wir haben dann für alle $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ $(cd) \cdot (ab) = (ca) \cdot (db) \in R$. Daraus folgt $(cd) \cdot (\mathfrak{a} \cdot \mathfrak{b}) \subseteq R$ und $\mathfrak{a} \cdot \mathfrak{b} \in \mathbb{I}_R$.
Für ein weiteres $\mathfrak{n} \in \mathbb{I}_R$ und beliebige $n \in \mathfrak{n}$ gilt $(ab)n = a(bn)$, also gilt auch $(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{n} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{n})$ und $\cdot$ ist damit assoziativ. Es gilt weiterhin

$$\mathfrak{a} \cdot \mathfrak{b} = \mathrm{span}_R\{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} = \{\underbrace{(r \cdot a)}_{\in \mathfrak{a}} b \mid r \in R, a \in \mathfrak{a}, b \in \mathfrak{b}\} = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}.$$

Für beliebige $a \in \mathfrak{a}, b \in \mathfrak{b}$ gilt, dass $ab = ba$ ist, da die Multiplikation innerhalb eines Körpers geschieht. Also ist $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$ und $\cdot$ daher kommutativ.
(*ii*) Dieser Zusammenhang gilt per Definition eines gebrochenen Ideals als R-Modul.
(*iii*) Da $\mathfrak{a} \neq 0$, existiert $0 \neq d = \frac{a}{s} \in \mathfrak{a}$. Es gilt $d \cdot \mathfrak{a}^{-1} \subseteq R$ per Definition von $\mathfrak{a}^{-1}$. Dann ist $sd = a \in R \setminus \{0\}$ mit $(sd) \cdot \mathfrak{a}^{-1} = s \cdot (d \cdot \mathfrak{a}^{-1}) \subseteq R$. Außerdem existiert $c \in R \setminus \{0\}$ mit $c \cdot \mathfrak{a} \subseteq R$, sodass also $c \in \mathfrak{a}^{-1} \setminus \{0\}$ und damit $\mathfrak{a}^{-1} \neq 0$. Dies zeigt $\mathfrak{a}^{-1} \in \mathbb{I}_R$. In der Definition von $\mathfrak{a}^{-1}$ ist bereits $\mathfrak{a}^{-1} \cdot \mathfrak{a} \subseteq R$ verankert.
Sei nun $\mathfrak{b} \in \mathbb{I}_R$ mit $\mathfrak{b} \cdot \mathfrak{a} = R$. Für beliebige $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ gilt $a \cdot b \in R$, also $b \in \mathfrak{a}^{-1}$ und damit $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Es gilt nun

$$R = \mathfrak{b} \cdot \mathfrak{a} \subseteq \mathfrak{a}^{-1} \cdot \mathfrak{a} \subseteq R.$$

Dies impliziert $\mathfrak{a}^{-1} \cdot \mathfrak{a} = R$ und daher auch $\mathfrak{a}^{-1} = R \cdot \mathfrak{a}^{-1} = \mathfrak{b} \cdot \mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{b} \cdot R = \mathfrak{b}$. □

Satz 2.7
Sei R ein Integritätsbereich. Falls $\mathbb{I}_R$ eine Gruppe ist, so ist R ein Dedekindring.

Beweis
Wir nehmen im Folgenden an, dass R kein Körper ist, weil sonst nichts zu zeigen ist.
Sei $\mathfrak{a} \in \mathbb{I}_R$ ein ganzes Ideal (Definition 2.3). Wegen $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$ existieren $a_1, \ldots, a_n \in \mathfrak{a}$, $b_1, \ldots, b_n \in \mathfrak{a}^{-1}$ mit $\sum_{i=1}^{n} a_i \cdot b_i = 1$. Für beliebiges $x \in \mathfrak{a}$ ist

$$x = x \cdot 1 = x \cdot \sum_{i=1}^{n} a_i \cdot b_i = \sum_{i=1}^{n} (x \cdot b_i) \cdot a_i.$$

Für alle $i = 1, \ldots, n$ haben wir $b_i \cdot x \in R$ und somit $\mathfrak{a} = \mathrm{span}_R\{a_1, \ldots, a_n\}$. Dies zeigt, dass R noethersch ist.
Für $x \in \mathrm{A}_K(R)$ ist $\mathfrak{n} := R[x] \in \mathbb{I}_R$ nach Proposition 1.1 und Satz 2.4(i), da es ganz und von endlichem Typ und damit endlich erzeugt über R ist. Wegen $x \cdot \mathfrak{n} \subseteq R[x] = \mathfrak{n}$ folgt

$$x \cdot R = x \cdot \mathfrak{n} \cdot \mathfrak{n}^{-1} \subseteq \mathfrak{n} \cdot \mathfrak{n}^{-1} \subseteq R,$$

sodass x in R liegt. Daher ist R ganzabgeschlossen.
Sei $\mathfrak{p}$ ein von Null verschiedenes Primideal von R. Dann ist $\mathfrak{p}$ in einem maximalen Ideal $\mathfrak{m}$ enthalten (vgl. **[AM]** Corollary 1.4.). Angenommen, dieses Ideal enthält $\mathfrak{p}$ echt, also $\mathfrak{p} \subsetneq \mathfrak{m}$. Wir definieren nun $\mathfrak{b} := \mathfrak{p} \cdot \mathfrak{m}^{-1}$. Aus $\mathfrak{p} \subseteq \mathfrak{m}$ erhalten wir

$$\mathfrak{b} = \mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1} = R,$$

das heißt, dass $\mathfrak{b}$ ein ganzes Ideal ist.
Es ist $\mathfrak{b} \not\subseteq \mathfrak{p}$, weil anderenfalls aus $\mathfrak{b} = \mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{p}$ durch Multiplikation mit $\mathfrak{m} \cdot \mathfrak{p}^{-1}$ die Inklusion $R \subseteq \mathfrak{m}$ folgen würde, was im Widerspruch zur Maximalität von $\mathfrak{m}$ stünde. Mit der Tatsache $\mathfrak{b} \not\subseteq \mathfrak{p}$ wählen wir abschließend $x \in \mathfrak{b} \setminus \mathfrak{p}$, $y \in \mathfrak{m} \setminus \mathfrak{p}$ und erhalten $xy \in \mathfrak{p}$, da $xy \in \mathfrak{b} \cdot \mathfrak{m} = \mathfrak{p} \cdot \mathfrak{m}^{-1} \cdot \mathfrak{m} = \mathfrak{p}$, was der Primidealeigenschaft von $\mathfrak{p}$ widerspricht. Ein solches $\mathfrak{m}$ kann also nicht existieren, womit $\mathfrak{p}$ bereits maximal ist. □

Die Umkehrung von Satz 2.7 gilt auch. Dies beweisen wir in Satz 2.9. Vorher brauchen wir noch ein Hilfslemma.

Lemma 2.8
Sei R noethersch und $\mathfrak{a} \subseteq R$ ein Ideal. Dann existieren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit der Eigenschaft, dass $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{a}$.

Beweis
Sei N die Menge der Ideale, für die obige Aussage nicht gilt. Wir nehmen an, dass $N \neq \emptyset$ gilt. Dann ist N induktiv geordnet, weil eine aufsteigende Kette von Idealen stets stationär wird, da R per Annahme noethersch ist (siehe **[AK]** (16.11) (Noetherian Modules)). Nach dem Lemma von Zorn besitzt N also ein maximales Element $\mathfrak{n}$. Dieses $\mathfrak{n}$ ist nicht prim, da es sonst selber $\mathfrak{n} \subseteq \mathfrak{n}$ erfüllt und auch nicht R, weil sonst $\mathfrak{p} \subseteq \mathfrak{n}$ für ein beliebiges Primideal $\mathfrak{p}$ gilt. Es existieren also $b_1, b_2 \in R \setminus \mathfrak{n}$ mit $b_1 \cdot b_2 \in \mathfrak{n}$. Wir definieren nun für $i = 1, 2$ die Ideale $\mathfrak{b}_i := (\mathfrak{n} + b_i R)$. Aufgrund der Maximalität von $\mathfrak{n}$ in N haben wir $\mathfrak{b}_1, \mathfrak{b}_2 \notin N$ und somit existieren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq \mathfrak{b}_1$ und $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subseteq \mathfrak{b}_2$.

Weiterhin gilt $\mathfrak{b}_1 \cdot \mathfrak{b}_2 \subseteq \mathfrak{n}$, denn für beliebige $(x_1 + b_1 y_1) \in \mathfrak{b}_1, (x_2 + b_2 y_2) \in \mathfrak{b}_2$ mit $x_1, x_2 \in \mathfrak{n}$ und $y_1, y_2 \in R$ haben wir

$$(x_1 + b_1 y_1) \cdot (x_2 + b_2 y_2) = x_1 x_2 + b_2 y_2 x_1 + b_1 y_1 x_2 + y_1 y_2 b_1 b_2 \in \mathfrak{n}.$$

Daher ist auch

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subseteq \mathfrak{b}_1 \cdot \mathfrak{b}_2 \subseteq \mathfrak{n},$$

was einen Widerspruch zu $\mathfrak{n} \in N$ bildet. Somit ist N leer und die Aussage ist bewiesen. □

Satz 2.9
Falls ein Ring R ein Dedekindring ist, dann ist $\mathbb{I}_R$ eine Gruppe.
Zudem ist $\mathbb{I}_R$ die freie, abelsche Gruppe über der Menge der von Null verschiedenen Primideale von R. Mit anderen Worten hat jedes gebrochene Ideal $\mathfrak{a}$ von R eine eindeutige Darstellung $\mathfrak{a} = \prod_{0 \neq \mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}^{n_\mathfrak{p}}$ mit eindeutig bestimmten ganzen Zahlen $n_\mathfrak{p} \in \mathbb{Z}$, von denen nur endlich viele ungleich Null sind.

Diese Darstellung wird auch als Primfaktorzerlegung bezeichnet. Die Primideale mit Exponent 0 werden in der Notation häufig weggelassen.

Beweis
Wir unterteilen diesen Beweis in fünf Schritte.
Schritt 1: Für $\mathfrak{a}, \mathfrak{p} \in \mathbb{I}_R$ mit $\mathfrak{p} \in \operatorname{Spec}(R) \backslash \{0\}$ gilt stets $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$.
Wir unterscheiden in diesem Schritt zwei Fälle.
Fall 1: Sei zunächst $\mathfrak{a} = R$, wir zeigen hierfür: $\mathfrak{p}^{-1} \not\subseteq R = \mathfrak{a}$.
Wir wählen $a \in \mathfrak{p} \setminus \{0\}$ und $\mathbb{N} \ni r \geq 1$ minimal mit der Eigenschaft, dass Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ von R existieren mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq aR$ (s. Lemma 2.8). Insbesondere gilt nach dieser Wahl $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{p}$. Wir behaupten, dass ein $i \in \mathbb{N}$ existiert mit $1 \leq i \leq r$, sodass $\mathfrak{p}_i = \mathfrak{p}$.
Angenommen die Behauptung gilt nicht, d.h. $\mathfrak{p}_i \neq \mathfrak{p}$ für alle $i \in \{1, \ldots, r\}$. Da R ein Dedekindring und kein Körper ist, haben wir insbesondere $\dim R = 1$ und Primideale ungleich Null können sich nicht enthalten, was bedeutet, dass $\mathfrak{p}_i \setminus \mathfrak{p} \neq \emptyset$ für alle $i = 1, \ldots, r$. Für alle $i \in \{1, \ldots, r\}$ wählen wir nun beliebige $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ und sehen, dass dann einerseits $x := x_1 \cdot \ldots \cdot x_r \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{p}$ ist, andererseits x als Produkt von Elementen, von denen keines in $\mathfrak{p}$ liegt, wegen der Primidealeigenschaft von $\mathfrak{p}$ nicht in $\mathfrak{p}$ liegen kann. Die getroffene Annahme ist aufgrund dieses Widerspruchs also falsch.
Da r minimal gewählt ist, haben wir $(\prod_{\substack{j=1 \\ j \neq i}}^{r} \mathfrak{p}_j) \not\subseteq aR$ d.h. $(\prod_{\substack{j=1i \\ j \neq i}}^{r} \mathfrak{p}_j) \setminus aR \neq \emptyset$. Wir wählen ein $b \in \prod_{\substack{j=1 \\ j \neq i}}^{r} \mathfrak{p}_j$ mit $b \notin aR$. Wir betonen dass $\frac{b}{a} \notin R$ und $b\mathfrak{p} = b\mathfrak{p}_i \subseteq \prod_{j=1}^{r} \mathfrak{p}_i \subseteq aR$ gelten. Dies impliziert $\frac{b}{a}\mathfrak{p} \subseteq R$, also $\frac{b}{a} \in \mathfrak{p}^{-1} \setminus R$. $\mathfrak{p}^{-1}$ ist also keine Teilmenge von R.
Fall 2: Sei $\mathfrak{a} \in \mathbb{I}_R$ nun beliebig. Wir nehmen an, dass $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$.
Die Multiplikation mit jedem Element $x \in \mathfrak{p}^{-1}$ definiert dann einen R-Modulhomomorphismus von $\mathfrak{a}$ nach $\mathfrak{a}$, den wir mit μ_x bezeichnen. Nach Satz 2.4(ii) ist $\mathfrak{a}$ endlich erzeugt. Der Satz von Cayley-Hamilton ([**AK**] (10.1)) besagt dann, dass ein $\chi(t) = t^n + \sum_{k=1}^{n-1} r_k t^k \in R[t]$ existiert mit $\operatorname{End}_R(\mathfrak{a}, \mathfrak{a}) \ni \chi(\mu_x) = 0$. Jedoch ist $\chi(\mu_x)$ aber genau die Linksmultiplikation mit $x^n + \sum_{k=1}^{n-1} r_k x^k \in K$, daher ist $x^n + \sum_{k=1}^{n-1} r_k x^k = 0$ in K, weil K nullteilerfrei und $\mathfrak{a} \neq 0$ ist. Dies ist eine ganze Gleichung von einem Element $x \in \mathfrak{a}$ in K, also ist $x \in \mathrm{A}_K(R) = R$. Da obiges

für beliebige $x \in \mathfrak{p}^{-1}$ und zugehörige $\mu_x \in \mathrm{End}_R(\mathfrak{a}, \mathfrak{a})$ gelten müsste und $\mathfrak{p}^{-1} \neq R$ bereits gezeigt, ist auch die Annahme $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ falsch.
Schritt 2: Wir zeigen nun, dass alle von Null verschiedenen ganzen Ideale von R sich als ein Produkt von Primidealen darstellen lassen. Für diese ist eine Zerlegung im Sinne des Satzes 2.9 mit nicht negativen Potenzen gegeben, was in Satz 3.1 präzisiert wird.
Sei M die Menge der Ideale von R, für die keine solche Zerlegung existiert. Wir nehmen an, dass M nicht leer ist. Dann ist M induktiv geordnet (siehe Beweis von Lemma 2.8), enthält also nach dem Lemma von Zorn ein maximales Element $\mathfrak{a}$. Für $\mathfrak{a} \in M$ bedeutet dies $\mathfrak{a} \neq R$, da $R = \prod_{\mathfrak{p} \in \mathrm{Spec}\, R \setminus \{0\}} \mathfrak{p}^0$. Wie jedes echte Ideal ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{p}$ enthalten. Wir haben $R \subseteq \mathfrak{p}^{-1}$, denn für alle $r \in R$ ist $r\mathfrak{p} \subseteq R$. Es ist auch $\mathfrak{a} = \mathfrak{a}R \subseteq \mathfrak{a}\mathfrak{p}^{-1}$ und zusammen mit Schritt 1 erhalten wir

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R.$$

Nach Maximalität von $\mathfrak{a}$ gilt $\mathfrak{a}\mathfrak{p}^{-1} \notin M$, also lässt sich $\mathfrak{a}\mathfrak{p}^{-1}$ als ein Produkt von Primidealen darstellen. Sei $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ eine solche Darstellung. Es gilt auch $\mathfrak{p} = \mathfrak{p}R \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, wobei die Echtheit der Inklusion wieder nach Schritt 1 gilt. Nun liefert uns Satz 2.6(iii) die Inklusion $\mathfrak{p}\mathfrak{p}^{-1} \subseteq R$, womit wir aufgrund der Maximalität von $\mathfrak{p}$ die Gleichheit $\mathfrak{p}\mathfrak{p}^{-1} = R$ erhalten. Somit ist jedes Primideal invertierbar.
Man multipliziere nun die Primzerlegung von $\mathfrak{a}\mathfrak{p}^{-1}$ mit $\mathfrak{p}$ und erhalte eine Zerlegung $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \cdot \mathfrak{p}$ von $\mathfrak{a}$, was im Widerspruch zu $\mathfrak{a} \in M$ steht. Daher ist M leer.
Schritt 3: Wir zeigen, dass die Menge der gebrochenen Ideale $\mathbb{I}_R$ eine Gruppe ist.
Sei $\mathfrak{a} \in \mathbb{I}_R$ und $c \in R \setminus \{0\}$ mit $c\mathfrak{a} \subseteq R$. Schritt 2 liefert uns, dass $c\mathfrak{a}$ eine Primfaktorzerlegung besitzt, wobei jedes der Primideale, wie am Ende von Schritt 2 gezeigt, auch invertierbar ist, $c\mathfrak{a}$ ist somit invertierbar. Es ist klar, dass cR sowite $c^{-1}R$ in $\mathbb{I}_R$ sind und dass $c\mathfrak{a} = cR \cdot \mathfrak{a}$ gilt. Wegen $(cR) \cdot (c^{-1}R) = (c \cdot c^{-1})R = R$ ist auch cR invertierbar und damit $\mathfrak{a}$.
Schritt 4: Wir zeigen die Existenz einer Primfaktorzerlegung für ein beliebiges $\mathfrak{a} \in \mathbb{I}_R$.
Jedes ganze Ideal hat laut Schritt 2 eine Primfaktorzerlegung mit nichtnegativen Potenzen der Primideale. Im Beweis von Schritt 2 wird gezeigt, dass jedes Primideal invertierbar ist. Da zudem für beliebige Gruppen G gilt

$$(xy)^{-1} = y^{-1}x^{-1} \text{ für alle } x, y \in G$$

besitzt jedes zu einem ganzen Ideal inverse Ideal ebenfalls eine Primfaktorzerlegung, nämlich

$$\Big(\prod_{0 \neq \mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}^{n_\mathfrak{p}}\Big)^{-1} = \prod_{0 \neq \mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}^{-n_\mathfrak{p}} \text{ für } n_\mathfrak{p} \in \mathbb{N}_0.$$

Nun erfüllt $\mathfrak{a}$ per Definition $c\mathfrak{a} \subseteq R$ für ein $c \in R \setminus \{0\}$ und besitzt ebenfalls eine Primfaktorzerlegung, da

$$\mathfrak{a} = (c^{-1}(c\mathfrak{a})) = ((cR)^{-1})(c\mathfrak{a}) = (c^{-1}R)(c\mathfrak{a})$$

gilt und nach dem eben Aufgeführten $c^{-1}R$, als Inverse des ganzen Ideals cR, eine Zerlegung hat.
Schritt 5: Schließlich zeigen wir die Eindeutigkeit der Primfaktorzerlegung. Wir betrachten o.B.d.A. den Fall $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$.
Da bereits gezeigt ist, dass I_R eine Gruppe ist, kann man nämlich die Gleichung zweier gegebenenfalls unterschiedlicher Zerlegungen durch sukzessives Multiplizieren mit den entsprechenden (eindeutigen) Inversen auf die obige Form bringen. Wir müssen zeigen, dass $r = s$ gilt und nach eventueller Umbenennung auch $\mathfrak{p}_i = \mathfrak{q}_i$ für $i = 1, \ldots, r$.

Wir zeigen dies per Induktion nach $n := \min\{r, s\}$. Sei für den Induktionsanfang ohne Einschränkung $n = r = 1$. Wir haben $\mathfrak{p}_1 = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$ und im Beweis von Schritt 1 sahen wir, dass ein $1 \leq i \leq s$ mit $\mathfrak{q}_i = \mathfrak{p}$ existiert. Die Gruppeneigenschaft besagt, dass $\prod_{\substack{j \neq i \\ i=1}}^{s} \mathfrak{q}_j = R$ ist.
Wir nehmen nun an das $s \geq 2$ und ohne Einschränkung $i = 1$ ist. Dann ist
$R = \prod_{j=2}^{s} \mathfrak{q}_j \subseteq \mathfrak{q}_2 \subseteq R$ und daraus folgt, dass $\mathfrak{q}_2 = R$, was einen Widerspruch bildet und daher $s = 1$ und $\mathfrak{p}_1 = \mathfrak{q}_1$.
Sei für den Induktionsschritt ohne Einschränkung $n = r \leq s$. Es ist $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{p}_1$, also existiert wieder nach Schritt 1 ein $1 \leq i \leq s$ mit $\mathfrak{q}_i = \mathfrak{p}_1$. Die Gruppeneigenschaft liefert $\prod_{i=2}^{r} \mathfrak{p}_i = \prod_{\substack{j=1 \\ j \neq i}}^{s} \mathfrak{q}_j$ und die Behauptung folgt nun nach Induktionsvoraussetzung. □

Bemerkung
Wir benennen noch einmal eine in Schritt 1 des vorigen Satzes 2.9 gezeigte Aussage, um darauf bequem verweisen zu können:
Sei R ein Dedekindring und seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{p}$ von Null verschiedene Primideale von R. Angenommen es gilt $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq \mathfrak{p}$. Dann folgt $\mathfrak{p}_i = \mathfrak{p}$ für ein $i \in \{1, \ldots, n\}$.

Satz 2.7 und Satz 2.9 ergeben unmittelbar das anfangs angekündigte Resultat:

Korollar 2.10
Ein Integritätsbereich R ist genau dann ein Dedekindring, wenn die Menge der gebrochenen Ideale $\mathbb{I}_R$ eine Gruppe ist. □

Definition 2.11
Sei R ein Dedekindring und $K := \mathrm{Quot}(R)$.

(i) $\mathbb{H}_R := \{Rx |\, x \in K^\times\}$. Das ist offensichtlich eine Untergruppe von $\mathbb{I}_R$, die sogenannte Untergruppe der „gebrochenen Hauptideale“ von R.

(ii) $\mathbb{C}_R := \mathbb{I}_R / \mathbb{H}_R$ heißt die Idealklassengruppe von R.

Bemerkung 2.12
R ist ein Hauptidealring genau dann, wenn $|\mathbb{C}_R| = 1$.
Sei nämlich R ein Hauptidealring und $I \in \mathbb{I}_R$ ein gebrochenes Ideal. Mit einem $0 \neq y \in R$ für das $yI \subseteq R$ gilt ist yI ein ganzes Ideal, also ein Hauptideal. Sei $(x) = yI = (y)I$ für ein $x \in R$. Wir haben dann $I = (x)(y^{-1}) = (\frac{x}{y})$, da $y \neq 0$ ist. Also ist I ein gebrochenes Hauptideal und $|\mathbb{C}_R| = 1$.
Falls anders herum $|\mathbb{C}_R| = 1$ ist, sind insbesondere alle ganzen Ideale per Definition von einem Element erzeugt.

3 Weitere Eigenschaften von Dedekindringen

Satz 3.1
Sei R ein Dedekindring. $I \in \mathbb{I}_R$ ist genau dann ein ganzes Ideal von R, wenn die in der Zerlegung von I vorkommenden Primideale alle nicht negative Exponenten haben. Mit anderen Worten: Es gilt $I = \prod_{i=1}^{n} \mathfrak{p}_i^{n_i}$ mit $n_i \geq 0$ für alle $i = 1, \ldots, n$.

Beweis
Sei $I = \mathfrak{p}_1^{m_1} \cdot \ldots \cdot \mathfrak{p}_s^{m_s}$ mit Primidealen $\mathfrak{p}_i$ und nicht negativen Exponenten $m_i \in \mathbb{N}$ ein gebrochenes Ideal. Dies ist nach der Definition des Produkts ein Ideal in R.
Seien andersherum $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq R$ paarweise verschiedene Primideale in R, die alle ungleich Null sind und $n_1, \ldots, n_r \in \mathbb{Z}$ mit $\prod_{i=1}^{r} \mathfrak{p}_i^{n_i} \subseteq R$. Angenommen es gibt ein j mit $n_j < 0$. Nach Umnummerierung können wir annehmen, dass $n_1, \ldots, n_m$ nicht negativ und $n_{m+1}, \ldots, n_r$ negativ sind mit $m < r$. Die Inklusion $\prod_{i=1}^{r} \mathfrak{p}_i^{n_i} \subseteq R$ liefert $\prod_{i=1}^{m} \mathfrak{p}_i^{n_i} \subseteq \prod_{i=m+1}^{r} \mathfrak{p}_i^{-n_i}$ nach Multiplikation mit $\prod_{i=m+1}^{r} \mathfrak{p}_i^{-n_i}$. Also gilt $\prod_{i=1}^{m} \mathfrak{p}_i^{n_i} \subseteq \prod_{i=m+1}^{r} \mathfrak{p}_i^{-n_i} \subseteq \mathfrak{p}_r$, da $m+1 \geq 1$. Nach der Bemerkung nach Satz 2.9 existiert wegen $-n_i \geq 1$ für $i = 1, \ldots, m$ somit ein $1 \leq j \leq m$ mit $\mathfrak{p}_j = \mathfrak{p}_r$ im Widerspruch zur Wahl der $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. □

Satz 3.2
Sei R ein Dedekindring und I ein Ideal von R mit $I \neq 0$. Dann ist jedes Ideal im Ring R/I ein Hauptideal.

Beweis
Wir nehmen ohne Einschränkung $I \neq R$ an. Wir zeigen in 3 Schritten, dass es ausreichend ist, die Aussage für den Fall $I = \mathfrak{p}^n$ für ein Primideal $\mathfrak{p} \neq 0$ und positives n zu beweisen.
Schritt 1: Seien $\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathrm{Spec}(R) \setminus \{0\}$, paarweise verschieden und $n, n_1, \ldots, n_r \in \mathbb{N}_0$ beliebig, dann gilt: $\mathfrak{p}^n + \prod_{i=1}^{r} \mathfrak{q}_i^{n_i} = R$.
Dass „ $\subseteq$ “ gilt ist klar. Angenommen es ist „ $\subsetneq$ “. Dann ist diese Summe ein echtes Ideal und damit in einem maximalen $\mathfrak{m}$ enthalten. Wir haben dann: $\mathfrak{p}^n \subseteq \mathfrak{p}^n + \prod_{i=1}^{r} \mathfrak{q}_i \subseteq \mathfrak{m}$. Mit der Bemerkung nach Satz 2.9 ist $\mathfrak{p} = \mathfrak{m}$. Genauso ist auch $\prod_{i=1}^{n} \mathfrak{q}_i^{n_i} \subseteq \mathfrak{p}^n + \prod_{i=1}^{n} \mathfrak{q}_i^{n_i}$, wonach auch $\mathfrak{q}_i = \mathfrak{m}$ ist für ein $1 \leq i \leq n$. Wir erhalten $\mathfrak{p} = \mathfrak{q}_i$ im Widerspruch zur Voraussetzung.
Schritt 2: Für $I = \mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_r^{n_r}$ mit paarweise verschiedenen $\mathfrak{p}_i \in \mathrm{Spec}(R)$ und $n_i \geq 1$, $i \in \{1, \ldots, n\}$ ist $R/I \cong R/\mathfrak{p}_1^{n_1} \times \ldots \times R/\mathfrak{p}_r^{n_r}$ laut dem Chinesischen Restsatz und Schritt 1.
Schritt 3: Sind $R_1, \ldots, R_n$ Ringe, in denen jedes Ideal ein Hauptideal ist, so ist jedes Ideal in $R' := R_1 \times \ldots \times R_n$ ein Hauptideal.
Sei I ein Ideal von $R' = R_1 \times \ldots \times R_n$. Indem man das Einselement von R' als Summe der Standardeinheitsvektoren schreibt, sieht man $I = I_1 \times \ldots \times I_n$ mit Idealen I_k von R_k.
Zwischenbehauptung: Für ein Ideal J von R mit $\mathfrak{p}^n \subseteq J$ gilt $J = \mathfrak{p}^m$ für ein $0 \leq m \leq n$.
Falls $J = R$ ist, ist J insbesondere als $J = \mathfrak{p}^0$ darstellbar. Sei J also ungleich R. Sei $\mathfrak{p}^n \subseteq J$ mit $J = \mathfrak{q}_1^{n_1} \cdot \ldots \cdot \mathfrak{q}_r^{n_r}, \mathfrak{q}_i \in \mathrm{Spec}(R) \setminus \{0\}$ paarweise verschieden. Die n_i sind laut Satz 3.1 nicht negativ, weil $J \subseteq R$. Außerdem ist o.B.d.A. $n_1 \geq 1$, da $J \neq R$. Aus $\mathfrak{p}^n \subseteq J \subseteq \mathfrak{q}_1^{n_1} \subseteq \mathfrak{q}_1$ folgt mit der Bemerkung nach Satz 2.9, dass $\mathfrak{p} = \mathfrak{q}_1$ ist.
Die Anzahl r der verschiedenen Ideale kann nicht echt größer als 1 sein, da sonst $\mathfrak{p}^n \subseteq J \subseteq \mathfrak{q}_2$

zur Folge hat, dass $\mathfrak{q}_1 = p = \mathfrak{q}_2$, was entgegen der Annahme ist. Damit haben wir die Zwischenbehauptung bewiesen.
Kommen wir nun zum eigentlichen Beweis von Satz 3.2 im Fall $I = \mathfrak{p}^n$ mit $n \geq 1$.
Wähle ein $c \in \mathfrak{p} \setminus \mathfrak{p}^2$. Das von c erzeugte Ideal stellen wir dar als $(c) = \prod_{i=1}^{s} \mathfrak{p}_i^{m_i}$, mit paarweise verschiedenen Primidealen $\mathfrak{p}_i \in \mathrm{Spec}(R)$ und $m_i \geq 1$. Es ist $(c) \subseteq \mathfrak{p}$, da c ein Element von $\mathfrak{p}$ ist und wir haben $cR = \mathfrak{p}^{m_1} \cdot \prod_{i=2}^{s} \mathfrak{p}_i^{m_i}$ gegebenenfalls nach Umbenennung mit denselben Argumenten wie zuvor. Falls $m_1 > 1$, wäre $(c) \subseteq \mathfrak{p}^2$ und somit $c \in \mathfrak{p}^2$. Daraus folgern wir, dass $(c^m) = c^m R = (cR)^m = \mathfrak{p}^m \cdot \prod_{j=2}^{s} \mathfrak{p}_j^{n_j}$ mit $n_j = m m_j$.
Sei jetzt $J/\mathfrak{p}^n \subseteq R/\mathfrak{p}^n$ ein Ideal. Dann ist $\mathfrak{p}^n \subseteq J$. Die Zwischenbehauptung zeigt $J = \mathfrak{p}^m$ mit $1 \leq m \leq n_j$, und in Schritt 2 wurde gezeigt, dass $\mathfrak{p}^k + \prod_{j=2}^{s} \mathfrak{p}_j^{n_j} = R$ für beliebigs $k \in \mathbb{N}_0$. Insbesondere gilt dies auch für $k = n - m$. Für beliebige Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq R$ gilt $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$. Daraus folgt

$$\mathfrak{p}^n + c^m R = \mathfrak{p}^m \cdot (\mathfrak{p}^{n-m} + \prod_{j=2}^{r} \mathfrak{p}_j^{n_j}) = \mathfrak{p}^m \cdot R = \mathfrak{p}^m = J.$$

Es folgt unmittelbar, dass $\overline{c^m}$, die Äquivalenzklasse von c^m das Ideal $J/\mathfrak{p}^n$ in $R/\mathfrak{p}^n$ erzeugt. □

Satz 3.3
Sei R ein Dedekindring. Es gelten:

(i) Jedes Ideal $I \subseteq R$ wird von höchstens zwei Elementen erzeugt.

(ii) R ist faktoriell $\Leftrightarrow$ R ist ein Hauptidealring.

Beweis
(i) Sei $I \subseteq R$ ein Ideal ungleich Null und $r \in I \setminus \{0\}$. In $R/(r)$ ist nach Satz 3.2 jedes Ideal ein Hauptideal. Sei $x \in R$, sodass $\bar{x} \in R/(r)$ ein Erzeuger von $I/(r)$ ist. R ist noethersch, sodass $I = \mathrm{span}_R\{a_1, \ldots, a_n\}$ für geeignete $a_1, \ldots, a_n \in I$. Ein beliebiges $\bar{a_i} \in I/(r)$ ist ein Vielfaches von $\bar{x}$, also $\bar{a_i} = \bar{x} \cdot \bar{t}$.
Auf Ebene des Rings R heißt das $a_i - xt \in (r)$, d.h. $a_i = xt + rs$ für gewisse $t, s \in R$. Die letzte Bedingung ist insbesondere äquivalent zu: $a_i \in (x, r) \subseteq R$, was die Behauptung für echte Ideale zeigt.
(ii) Die Richtung „ $\Leftarrow$ “ ist klar.
„$\Rightarrow$“: Falls R ein faktorieller Ring ist, existiert insbesondere ein größter gemeinsamer Teiler, $\mathrm{ggT}(x, r)$, von zwei beliebigen Elementen x, r und aus (i) erhält man unmittelbar, dass I von $\mathrm{ggT}(x, r)$ erzeugt wird. $I = (x, r) = \big(\mathrm{ggT}(x, r)\big)$ mit $x, r \in R$ Erzeugern von I. □

4 Lokalisierungen von Dedekindringen

Wir fahren mit weiteren Eigenschaften und Beispielen von Dedekindringen fort.

Satz 4.1
Sei S eine multiplikativ abgeschlossene Teilmenge von R mit $0 \notin S$. Dann ist die Lokalisierung $S^{-1}R$ wieder ein Dedekindring.

Beweis
Dedekindringe besitzen als Integritätsbereiche einen Quotientenkörper. Sämtliche von Null verschiedene Lokalisierungen können als Unterringe von diesem betrachtet werden, sind also nullteilerfrei.
Sei $K := \mathrm{Quot}(R)$. Die Lokalisierungsabbildung $\iota : R \to S^{-1}R$ kann in diesem Fall als Inklusion aufgefasst werden. Wir haben dann $R \subseteq S^{-1}R \subseteq K$ für alle von Null verschiedenen Lokalisierungen $S^{-1}R$ von R.
Zeige zunächst: $S^{-1}R$ ist noethersch. Sei $\mathfrak{b} \subseteq S^{-1}R$ ein Ideal und $\mathfrak{a} := \mathfrak{b} \cap R$. Dann ist $\mathfrak{a}$ ein Ideal von R. Wir behaupten, dass $\mathfrak{b} = S^{-1}\mathfrak{a} := \{\frac{a}{s} \mid a \in \mathfrak{a}, s \in S\}$ gilt. Die Inklusion $S^{-1}\mathfrak{a} \subseteq \mathfrak{b}$ ist unmittelbar klar. Sei umgekehrt $b = \frac{a}{s} \in \mathfrak{b}$. Dann gilt $a = b \cdot s \in R \cap \mathfrak{b} = \mathfrak{a}$ und $b = \frac{a}{s} \in S^{-1}\mathfrak{a}$.
Seien nun $a_1, \ldots, a_n$ Erzeuger von $\mathfrak{a}$, und $b \in \mathfrak{b}$ beliebig. Schreibe $b = \frac{a}{s}$ mit $a \in \mathfrak{a}$ und $s \in S$. Verwende nun die Erzeuger von $\mathfrak{a}$, um den Zähler mit entsprechenden Koeffizienten $\lambda_i \in R$ darzustellen: $b = \frac{\sum_{i=1}^n \lambda_i \cdot a_i}{s} = \sum_{i=1}^n \frac{\lambda_i}{s}\frac{a_i}{1}$. Die Elemente $\frac{a_1}{1} \ldots \frac{a_n}{1}$ sind somit Erzeuger von $\mathfrak{b}$ als $S^{-1}R$-Modul.
Für den Nachweis von $\dim(R) \leq 1$ verweisen wir auf die Abbildung

$$\varphi : \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\} \to \mathrm{Spec}(S^{-1}R), \quad \mathfrak{p} \mapsto \mathfrak{p}S^{-1}R$$

aus **[AK]** Corollary (11.12) (2), die bijektiv und inklusionserhaltend ist. Damit und mit $\dim(R) \leq 1$ ist auch $\dim(S^{-1}R) \leq 1$.
Als letztes zeigen wir die Ganzabgeschlossenheit. Da $S^{-1}R \subseteq K$ ist und K bereits ein Körper ist, ist $K = \mathrm{Quot}(S^{-1}R)$. Sei $x \in K$ ganz über $S^{-1}R$. Per Definition existieren $\frac{\lambda_1}{s_1}, \ldots, \frac{\lambda_{n-1}}{s_{n-1}} \in S^{-1}R$, sodass

$$x^n + \frac{\lambda_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{\lambda_0}{s_0} = 0$$

gilt. Definiere $s := s_1 \cdot \ldots \cdot s_{n-1} \in S$ und multipliziere vorige Gleichung mit s^n. Das ergibt

$$(sx)^n + \underbrace{\frac{s\lambda_{n-1}}{s_{n-1}}}_{\in R}(sx)^{n-1} + \underbrace{\frac{s^2\lambda_{n-2}}{s_{n-2}}}_{\in R}(sx)^{n-2} + \cdots + \underbrace{\frac{\lambda_0 s^n}{s_0}}_{\in R} = 0.$$

Dann ist $r = sx \in \mathrm{A}_K(R) = R$ und damit $x = \frac{r}{s} \in S^{-1}R$. □

Es gibt folgende, lokale Charakterisierungen von Dedekindringen:

Satz 4.2
Sei R ein noetherscher Integritätsbereich. Folgende Eigenschaften sind äquivalent:

(i) R ist ein Dedekindring.

(ii) Für alle $\mathfrak{p} \in \operatorname{Spec} R$ ist $R_\mathfrak{p}$ ein Dedekindring.

(iii) Für alle $\mathfrak{p} \in \operatorname{Spec} R$ ist $R_\mathfrak{p}$ ein Hauptidealring.

(iv) Für alle $\mathfrak{p} \in \operatorname{Spec} R \setminus \{(0)\}$ ist $R_\mathfrak{p}$ ein diskreter Bewertungsring.

Beweis
$(i) \Rightarrow (ii)$: folgt sofort aus Satz 4.1.
$(ii) \Rightarrow (iii)$: $R_\mathfrak{p}$ ist als Lokalisierung eines Integritätsbereichs lokal nach **[AK]** Proposition (11.14). Da $\dim R_\mathfrak{p} \leq 1$ ist, gilt für ein primes $\mathfrak{q} \subseteq R_\mathfrak{p}$ welches $(0) \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ erfüllt, dass entweder $\mathfrak{q} = (0)$ oder $\mathfrak{q} = \mathfrak{m}$, mit dem maximalen Ideal $\mathfrak{m}$ von $R_\mathfrak{p}$. Jedes echte Ideal, insbesondere auch jedes Primideal ist in einem maximalen Ideal enthalten, (siehe **[AM]** Corollary 1.4.), in diesem Falle also stets in $\mathfrak{m}$. Für das Primspektrum heißt das $\operatorname{Spec} R_\mathfrak{p} = \{(0), \mathfrak{m}\}$.
Satz 2.9 besagt dann, dass jedes Ideal $\mathfrak{a} \neq (0)$ in $R_\mathfrak{p}$ von der Form: $\mathfrak{a} = \mathfrak{m}^n, n \in \mathbb{Z}$ ist, mit Verweis auf Satz 3.1 sogar $n \in \mathbb{N}_0$. Falls $\mathfrak{m} = (c)$, ein Hauptideal wäre, würde $R_\mathfrak{p}$, ein Hauptidealring sein. Behauptung: $\mathfrak{m}$ ist tatsächlich ein Hauptideal.
Beweis: Zunächst ist aufgrund der Gruppeneigenschaft von $\mathbb{I}_{R_\mathfrak{p}}$, $\mathfrak{m} \neq \mathfrak{m}^2$. Wegen $\mathfrak{m}^2 \subseteq \mathfrak{m}$ ist $\mathfrak{m} \backslash \mathfrak{m}^2$ also nichtleer. Sei $c \in \mathfrak{m} \backslash \mathfrak{m}^2$. Wie oben ist $(c) = \mathfrak{m}^n, n \in \mathbb{N}_0$. Da c keine Einheit ist, gilt $n > 0$. Da $c \notin \mathfrak{m}^2$ gilt außerdem $n < 2$ und damit n=1. Es folgt $(c) = \mathfrak{m}^1 = \mathfrak{m}$, wie behauptet. Wir sehen insgesamt, dass $R_\mathfrak{p}$ ein Hauptidealring ist.
$(iii) \Rightarrow (ii)$: Die Aussage gilt da jeder Hauptidealring ein Dedekindring ist.
$(ii) \Rightarrow (iv)$: Sei $\mathfrak{p} \in \operatorname{Spec} R \backslash \{(0)\}$ beliebig und $\mathfrak{m}$ das maximale Ideal von $R_\mathfrak{p}$.
Wie oben gesehen, ist jedes gebrochene Ideal $\mathfrak{a} \subseteq K$ von der Form $\mathfrak{a} = \mathfrak{m}^n$ mit $n \in \mathbb{Z}$. Auf $K := \operatorname{Quot} R$ definieren wir die Funktion $\nu_\mathfrak{m} : K \to \mathbb{Z} \cup \{\infty\}$ wie folgt: Für $c = 0$ definiere: $\nu_\mathfrak{m}(0) := \infty$. Für $c \in K \setminus \{0\}$ schreibe $(c) = \mathfrak{m}^n, n \in \mathbb{Z}$ und definiere $\nu_\mathfrak{m}(c)$ als $\nu_\mathfrak{m}(c) := n$.
Seien $c_1, c_2 \in R_\mathfrak{p}$ beliebig, $c_1 = \mathfrak{m}^{n_1}$, $c_2 = \mathfrak{m}^{n_2}$. Es gelte o.B.d.A.: $n_1 \leq n_2$, was gleichbedeutend ist mit $\mathfrak{m}^{n_1} \supseteq \mathfrak{m}^{n_2}$. Daraus folgt $(c_1 + c_2) \subseteq (c_1)$ und damit

$$\nu_\mathfrak{m}(c_1 + c_2) \geq \nu_\mathfrak{m}(c_1) = n_1 = \min\{\nu_\mathfrak{m}(c_1), \nu_\mathfrak{m}(c_2)\}.$$

Es gilt auch $(c_1) \cdot (c_2) = \mathfrak{m}^{n_1+n_2}$ und damit

$$\nu_\mathfrak{m}(c_1 \cdot c_2) = (n_1 + n_2) = \nu_\mathfrak{m}(c_1) + \nu_\mathfrak{m}(c_2).$$

Per Konvention gilt hierbei $\infty + k = \infty$, $\infty + \infty = \infty$. Dies macht $\nu_\mathfrak{m}$ zu einer diskreten Bewertung auf K. Betrachte folgende Äqivalenzen:

$$c \in R_\mathfrak{p} \Leftrightarrow (c) = \mathfrak{m}^n \subseteq R_\mathfrak{p} \Leftrightarrow \nu_\mathfrak{m}(c) = n \geq 0$$

Diese gelten nach Satz 3.1 und haben $R_\mathfrak{p} = \{x \in K \mid \nu_\mathfrak{m}(x) \geq 0\}$ zur Folge. Damit ist $R_\mathfrak{p}$ ein diskreter Bewertungsring.
$(iv) \Rightarrow (i)$: Wir teilen den Beweis in 4 Schritte auf. Sei $\operatorname{Spec} R \ni \mathfrak{p} \neq 0$.
Schritt 1. Zeige: $R_\mathfrak{p}$ ist ein (lokaler) Hauptidealring.
Sei ν eine diskrete Bewertung auf $K = \operatorname{Quot}(R)$ mit $R_\mathfrak{p} = \{x \in K \mid \nu(x) \geq 0\}$. Aus

$$\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$$

folgt $\nu(1) = 0$. Für beliebiges $0 \neq c \in K$ gilt dann

$$0 = \nu(1) = \nu(c \cdot c^{-1}) = \nu(c) + \nu(c^{-1}),$$

und damit $\nu(c^{-1}) = -\nu(c)$. Das bedeutet, dass $R^\times = \{r \in K \mid \nu(r) = 0\}$.
Es ist $\mathfrak{m} := \{x \in K \mid \nu(x) > 0\}$ ein Ideal von $R_\mathfrak{p}$, welches trivialerweise $R^\times = R \setminus \mathfrak{m}$ erfüllt.

Nach **[AK]** Lemma (3.5) (Nonunit Criterion) ist $\mathfrak{m}$ das eindeutige, maximale Ideal in $R_\mathfrak{p}$. Sei $(0) \neq \mathfrak{a} \subseteq R_\mathfrak{p}$ ein beliebiges Ideal und wähle $a \in \mathfrak{a}$ so, dass $\nu(a) = \min\{\nu(x) \mid x \in \mathfrak{a}\}$. Es gilt $a \neq 0$, weil $\mathfrak{a} \neq (0)$ und somit hat mindestens ein Element nicht die Bewertung ∞. Für beliebiges $b \in \mathfrak{a}$ gilt dann $\nu(b) \geq \nu(a)$ und daher

$$0 \leq \nu(b) - \nu(a) = \nu(b) + \nu(\frac{1}{a}) = \nu(\frac{b}{a}).$$

Es folgt $\frac{b}{a} \in R_\mathfrak{p}$ und $b = \frac{b}{a} \cdot a \in R_\mathfrak{p}$. Da b beliebig war, ergibt sich $\mathfrak{a} = R_\mathfrak{p} a$, und $R_\mathfrak{p}$ ist ein Hauptidealring.
Schritt 2. Zeige: $\dim(R) \leq 1$. Für den Fall, dass R ein Körper ist, ist $\dim(R) = 0$. Wir nehmen an, R sei kein Körper. Also existiert ein Primideal $\mathfrak{p}$ ungleich Null. Dann ist die Lokalisierung $R_\mathfrak{p}$ auch kein Körper, denn sie ist lokal mit einem maximalen Ideal $\mathfrak{p}R_\mathfrak{p}$ ungleich Null, nach **[AK]** Proposition (11.14).
Seien nun $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R \backslash \{(0)\}$ mit $\mathfrak{p} \subseteq \mathfrak{q}$. Dann sind $(R \backslash \mathfrak{q})^{-1}\mathfrak{p} \subseteq (R \backslash \mathfrak{q})^{-1}\mathfrak{q}$ Primideale in $R_\mathfrak{q}$, die jeweils verschieden von Null sind. Wie wir nach Schritt 1 wissen, ist $R_\mathfrak{q}$ ein Hauptidealring, der kein Körper ist, also hat $R_\mathfrak{q}$ die Krulldimension $\dim R = 1$. Es folgt $(R \backslash \mathfrak{q})^{-1}\mathfrak{p} = (R \backslash \mathfrak{q})^{-1}\mathfrak{q}$. Die Tatsache, dass die Zuordnung

$$\varphi : \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \bigcap (R \setminus \mathfrak{q})\} \to \operatorname{Spec}((R \setminus \mathfrak{q})^{-1}R), \qquad \mathfrak{p} \mapsto \mathfrak{p}S^{-1}R$$

inklusionserhaltend ist (vgl. **[AK]** Corollary (11.12) (2)) verrät dann, dass auch die Ideale $\mathfrak{p}$ und $\mathfrak{q}$ gleich sein müssen, was genau $\dim R = 1$ zur Folge hat.
Schritt 3: Es gilt $R = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} R_\mathfrak{p}$ als Unterringe von K.
Sei $x = \frac{a}{b} \in \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} R_\mathfrak{p}$, mit $a, b \in R, b \neq 0$ und definiere das Ideal $\mathfrak{a} := \{r \in R \mid r \cdot a \in bR\}$.
Angenommen $\mathfrak{a} \subseteq \mathfrak{q}$, für ein $\mathfrak{q} \in \operatorname{Spec} R$. Schreibe $x = \frac{a}{b} = \frac{c}{s} \in R_\mathfrak{q}$, $c \in R, s \in R \setminus \mathfrak{q}$.
Es folgt: $a \cdot s = b \cdot c$ und s liegt somit in $\mathfrak{a}$. Damit ist $s \in \mathfrak{a} \setminus \mathfrak{q}$, was entgegen der Annahme ist. Nach **[AM]** Corollary 1.4., gilt $\mathfrak{a} = R$. Insbesondere ist $1 \in \mathfrak{a}$ und somit $1 \cdot a \in bR$, also existiert ein $t \in R$ sodass $a = t \cdot b$. Das heißt, dass $x = \frac{a}{b} = \frac{tb}{b} = t$, also, dass x in R liegt.
Schritt 4: Jeder der Ringe $R_\mathfrak{p}$ ist nach Schritt 1 ein Hauptidealring, damit faktoriell und somit auch ganzabgeschlossen. Nach Schritt 3 ist R als ein Schnitt von ganzabgeschlossenen Ringen mit demselben Quotientenkörper ebenfalls ganzabgeschlossen.
Da R bereits per Annahme noethersch ist, ist der Beweis damit vollendet. □

5 Ganze Abschlüsse in separablen Körpererweiterungen

Satz 5.1
Sei R ein Integritätsbereich, $K := \mathrm{Quot}(R)$, $E|K$ eine endliche Körpererweiterung und $S := \mathrm{A}_E(R)$, der ganze Abschluss von R in E. Es gelten:

(i) S ist ein ganzabgeschlossener Ring mit Quotientenkörper E.

(ii) Angenommen R ist ganzabgeschlossen. Für $\alpha \in E$ und das Minimalpolynom $\mu_\alpha(t)$ von α über K gilt:

$$[\alpha \text{ ist ganz über } R] \Leftrightarrow [\mu_\alpha \in R[t]\,]$$

Beweis
(i) Wir zeigen zunächst, dass E der Quotientenkörper von S ist. Sei $\alpha \in E$ mit Minimalpolynom

$$\mu_\alpha(t) = t^n + \frac{r_{n-1}}{s_{n-1}}t^{n-1} + \ldots + \frac{r_1}{s_1}t + \frac{r_0}{s_0} \in K[t],$$

wobei $r_i, s_i \in R, s_i \neq 0$ für alle $i = 1, \ldots, n-1$. Wir definieren $s := s_0 \cdot \ldots \cdot s_{n-1}$. Dieses Element s ist in $R \setminus \{0\} \overset{Prop.1.1}{\subseteq} S \setminus \{0\}$ und wir erhalten

$$0 = s^n \cdot 0 = s^n \cdot \mu_\alpha(\alpha) = (s\alpha)^n + \sum_{i=0}^{n-1} \frac{r_i}{s_i} s^{n-i}(s\alpha)^i.$$

Hierbei ist

$$\frac{r_i}{s_i} \cdot s^{n-i} = r_i \cdot s^{n-i-1} \cdot \prod_{\substack{j=1 \\ j\neq i}}^{n-1} s_j \in R \text{ für alle } 0 \leq i \leq n-1,$$

sodass $s\alpha$ ganz über R ist, d.h. $s\alpha \in S$. Dies zeigt $E \subseteq \mathrm{Quot}(S)$. Per Definition von S, ist $S \subseteq E$ eine Teilmenge von E, womit $\mathrm{Quot}(S) = \{\frac{m}{n} \mid m, n \in S, n \neq 0\}$ ein Unterring von E ist, da E ein Körper ist. Es folgt $E = \mathrm{Quot}(S)$.
Nun zeigen wir, dass S ganzabgeschlossen ist, also $\mathrm{A}_E(S) = S$. Die Ringererweiterungen $\mathrm{A}_E(S)|S$ und $S|R$ sind jeweils ganz. Das bedeutet, dass $\mathrm{A}_E(S)|R$ laut Satz 1.3 ebenfalls ganz ist. Insbesondere ist jedes Element $x \in \mathrm{A}_E(S)$ ganz über R und es liegt in E, per Definition liegt es also in $\mathrm{A}_E(R)$. Daher haben wir

$$S \subseteq \mathrm{A}_E(S) \subseteq \mathrm{A}_E(R) = S.$$

Daraus folgt nun $S = \mathrm{A}_E(S) = \mathrm{A}_{\mathrm{Quot}(S)}(S)$, d.h. S ist ganzabgeschlossen.
(ii) Sei $\alpha \in E$ ganz über R, d.h. es existiert ein normiertes $f \in R[t] \subseteq K[t]$ mit $f(\alpha) = 0$. Das Minimalpolynom μ_α teilt f in $K[t]$ per Definition von μ_α. Wir schreiben

$$\mu_\alpha = \prod_{i=1}^{n}(t - \alpha_i) \in F[t],$$

wobei F ein algebraischer Abschluss von K ist. Für alle $i = 1, \ldots, n$ gilt $f(\alpha_i) = 0$ in F, also $\alpha_i \in \mathrm{A}_F(R)$. Nach Ausmultiplizieren von $\prod_{i=1}^{n}(t - \alpha_i)$ folgt, dass alle Koeffizienten von μ_α in $\mathrm{A}_F(R)$ liegen, da $\mathrm{A}_F(R)$ ein Ring ist. Alle Koeffizienten liegen also in $\mathrm{A}_F(R)$ und in K, also $\mathrm{A}_F(R) \cap K = \mathrm{A}_K(R) = R$. Die umgekehrte Implikation ist klar, weil μ_α normiert ist. □

Definition 5.2
Sei $E|K$ eine endliche Körpererweiterung, $\alpha \in E$ und m_α die Darstellungsmatrix der K-linearen Abbildung $(x \mapsto \alpha x : E \to E)$ bezüglich einer beliebigen K-Basis von E. Wir definieren

(i) $\mathrm{N}_{E|K}(\alpha) := \det(m_\alpha)$, in Worten: die Norm von α,

(ii) $\mathrm{Tr}_{E|K}(\alpha) := \mathrm{Tr}(m_\alpha)$, in Worten: die Spur von α,

(iii) $\chi_\alpha(t) := \chi_{m_\alpha,E}(t)$, in Worten: das charakteristische Polynom von α.

Beachte, dass die Wohldefiniertheit der obigen Ausdrücke aus der Transformationsformel der linearen Algebra folgt.

Es gibt noch eine weitere nützliche Eigenschaft vom charakteristischen Polynom:

Korollar 5.3
Seien $E|K, \alpha$ wie in Definition 5.2 und $\chi_\alpha(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_0$. Dann gilt:

$$a_n = (-1)^n, \quad a_{n-1} = \mathrm{Tr}_{E|K}(\alpha) \quad \text{und } a_0 = \mathrm{N}_{E|K}(\alpha).$$

Beweis
Die Charakterisierung von a_n, a_{n-1}, a_0 in $\chi_\alpha(t)$ folgert man schnell aus **[LM]** Lemma 8.3. □

Satz 5.4
Sei R ganzabgeschlossen, $K := \mathrm{Quot}(R)$, $E|K$ eine endliche Körpererweiterung, $S := \mathrm{A}_E(R)$ und $\alpha \in S$. Dann gilt

$$\chi_\alpha(t) \in R[t] \text{ und } \mathrm{N}_{E|K}(\alpha), \mathrm{Tr}_{E|K}(\alpha) \in R.$$

Beweis
Sei

$$\mu_\alpha(t) = t^m + c_{m-1}t^{m-1} + \ldots + c_0 \underset{(ii)}{\overset{5.1}{\in}} R[t]$$

das Minimalpolynom von α über K. Sei $d := [E : K[\alpha]]$ und $(a_1, \ldots, a_d)$ eine $K[\alpha]$-Basis von E. $(1, \alpha, \ldots, \alpha^{m-1})$ ist eine K-Basis von $K[\alpha]$, sodass $(a_1, a_1\alpha, \ldots, a_1\alpha^{m-1}, \ldots, a_d, \ldots, a_d\alpha^{m-1})$ eine K-Basis von E ist, (siehe der Beweis des Gradsatzes, **[BoA]** Satz 2. Kapitel 3.2). Damit können wir nun die Gestalt der Darstellungsmatrix m_α bestimmen.
Sei $j \in \{1, \ldots, d\}$ beliebig, x eine F-Linearkombination von $(a_j, a_j\alpha, \ldots, a_j\alpha^{m-1})$,

$$x = a_j x_1 + a_j x_2 \alpha + \ldots + a_j x_m \alpha^{m-1} = a_j[\sum_{i=1}^{m} x_i \alpha^{i-1}].$$

Nach Multiplikation mit α erhalten wir

$$\begin{aligned}\alpha x &= a_j \cdot \big[x_1\alpha + \ldots + x_{m-1}\alpha^{m-1} + x_m(\underbrace{-c_0 - c_1\alpha - \ldots - c_{m-1}\alpha^{m-1}}_{=\alpha^m(\text{ Umst. v. } \mu_\alpha(\alpha)=0)})\big] \\ &= a_j[-c_0x_m + \alpha(x_1 - c_1x_m) + \alpha^2(x_2 - c_2x_m) + \ldots + \alpha^{m-1}(x_{m-1} - c_{m-1}x_m)].\end{aligned}$$

Dies hat zur Folge, dass m_α eine Blockdiagonalmatrix ist, deren sämtliche Blöcke dieselbe folgende Form haben:

$$\begin{pmatrix} 0 & 0 & . & . & 0 & -c_0 \\ 1 & 0 & . & . & 0 & -c_1 \\ 0 & 1 & 0 & & . & . \\ . & & . & . & . & . \\ . & & & . & 0 & . \\ 0 & . & . & 0 & 1 & -c_{m-1} \end{pmatrix}.$$

Jede solche Blockmatrix hat das charakteristische Polynom

$$(-1)^m[t^m + c_{m-1}t^{m-1} + .. + c_0] = \pm\mu_\alpha(t).$$

Das charakteristische Polynom von α ist dann von der Form: $\chi_\alpha(t) = \pm(\mu_\alpha(t))^d$ und damit folgt aus Satz 5.1(ii) und Korollar 5.3: $\mathrm{N}_{E|F}(\alpha) \in R$ und $\mathrm{Tr}_{E|F}(\alpha) \in R$.

□

Definition 5.5
Sei $E|K$ eine endliche Körpererweiterung und $a = (a_1, \ldots, a_n)$ eine K-Basis von E. Dann heißt $\mathrm{d}(a) := \det(\mathrm{Tr}_{E|K}(a_i a_j)_{\substack{1\le i\le n \\ 1\le j\le n}})$ die Diskriminante von a.

Proposition 5.6
Sei $E|K$ endlich separabel und a eine K-Basis von E. Dann ist $\mathrm{d}(a) \neq 0$.

Beweis
Für zwei verschiedene K-Basen $a = (a_1, \ldots, a_n)$ und $b = (b_1, \ldots, b_n)$ von E gilt $\mathrm{d}(a) \neq 0$ genau dann wenn $\mathrm{d}(b) \neq 0$. Betrachte dazu die (reguläre) Basiswechselmatrix $C := T_a^b$ von b nach a und die Abbildung: $E \times E \to K : (a, b) \mapsto \mathrm{Tr}_{E|K}(ab)$, die symmetrisch und K-bilinear ist. Es gilt dann mit der Transformationsformel für Bilinearformen:

$$(\mathrm{Tr}_{E|K}(b_i b_j))_{i,j\in\{1,\ldots,n\}} = {}^tC \cdot (\mathrm{Tr}_{E|K}(a_i a_j))_{i,j\in\{1,\ldots,n\}} \cdot C$$

und daher $\mathrm{d}(b) = \mathrm{d}(C)^2 \cdot \mathrm{d}(a)$. Das heißt, dass sich die beiden Diskriminanten um ein von Null verschiedenes Quadrat in K unterscheiden. Sei $n := [E : K]$, und wähle $\vartheta \in E$ so, dass $E = K[\vartheta]$. Aufgrund der Vorbemerkung ist es ausreichend, die Aussage für eine beliebige Basis zu beweisen, was wir für $a = (1, \vartheta, \ldots, \vartheta^{n-1})$ tun.
Sei $\mathbb{H} := \mathrm{Hom}_{\mathrm{id}_K}(E, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$ mit $\sigma_i \neq \sigma_j, i \neq j$. Wähle $\alpha \in E$ mit Minimalpolynom $\mu_\alpha \in K[t]$ und definiere eine Äquivalenzrelation $\sim$ auf $\mathbb{H}$ via

$$\sigma_i \sim \sigma_j \Leftrightarrow \sigma_i(\alpha) = \sigma_j(\alpha) \ (\Leftrightarrow \sigma_i|_{K[\alpha]} = \sigma_j|_{K[\alpha]}).$$

Die Elemente von $\{\sigma(\alpha)\}_{\sigma\in\mathbb{H}/\sim}$ sind dann die paarweise verschiedenen Galoiskonjugierten von α in $\bar{K}$, sodass

$$\mu_\alpha(t) = \prod_{\sigma\in\mathbb{H}/\sim} (t - \sigma(\alpha)),$$

weil die Erweiterung separabel ist. Für ein $\sigma \in \mathbb{H}$ ist die Äquivalenzklasse von σ bezüglich $\sim$ gleich $\{\tau \in \mathrm{Hom}_{id_K}(E, \bar{K}) \mid \tau|_{K[\alpha]} = \sigma|_{K[\alpha]}\} = \mathrm{Hom}_{\sigma|_{K[\alpha]}}(E, \bar{K})$. Sie besteht daher aus genau $d := [E|K[\alpha]]$ Elementen, weil $E|K[\alpha]$ separabel ist.
Aus dem Beweis von Satz 5.4 wissen wir, dass

$$\chi_\alpha(t) = \pm\mu_\alpha(t)^d = \prod_{\sigma\in\mathbb{H}/\sim} (t - \sigma(\alpha))^d = \prod_{\sigma\in\mathbb{H}} (t - \sigma(\alpha)).$$

Ausmultiplizieren und Korollar 5.3 ergeben

$$\mathrm{N}_{E|K}(\alpha) = \prod_{\sigma\in\mathbb{H}} \sigma(\alpha) \text{ und } \mathrm{Tr}_{E|K}(\alpha) = \sum_{\sigma\in\mathbb{H}} \sigma(\alpha).$$

Daraus folgt nun

$$\begin{aligned}\mathrm{d}(a) &= |(\mathrm{Tr}_{E|K}(\vartheta^i \cdot \vartheta^j))_{i,j}| = |\Big(\sum_{k=1}^{n} \sigma_k(\vartheta^i)\sigma_k(\vartheta^j)\Big)_{i,j}| \\ &= |(\sigma_k(\vartheta^i))_{i,k} \cdot (\sigma_k(\vartheta^j))_{k,j}| = \det((\sigma_k(\vartheta^i))_{i,k})^2.\end{aligned}$$

Wir setzen $\vartheta_k := \sigma_k(\vartheta)$, sodass $\sigma_k(\vartheta^i) = \sigma_k(\vartheta)^i = \vartheta_k^i$. Für $l \neq k$ ist dann auch

$$\vartheta_k = \sigma_k(\vartheta) \neq \sigma_l(\vartheta) = \vartheta_l,$$

da sonst wegen $E = K[\vartheta]$ auch $\sigma_k = \sigma_l$ auf ganz E folgen würde. Das ergibt abschließend

$$\mathrm{d}(a) = \det((\vartheta_k^i)_{i,k})^2 \overset{\text{Vandermonde}}{=} \prod_{1\leq k<l\leq n} (\vartheta_k - \vartheta_l)^2 \neq 0.$$

□

Satz 5.7
Sei R ein noetherscher Integritätsbereich, $K := \mathrm{Quot}(R)$ und $E|K$ eine endliche separable Körpererweiterung. Dann ist $S := \mathrm{A}_E(R)$ noethersch als R-Modul und damit auch als Ring.

Beweis
Wir führen diesen Beweis in fünf Schritten.
Schritt 1: Wähle $a = (e_1, \ldots, e_n)$, eine K-Basis von E. Da nach Satz 5.1 (i) $E = \mathrm{Quot}(S)$ gilt, können wir nach Multiplikation mit einem gemeinsamen Nenner annehmen, dass alle e_i in S liegen.
Schritt 2: Setze $V := \mathrm{span}_R\{e_1, \ldots, e_n\} \subseteq S$ und betrachte den R-Untermodul V^* von E, definiert als

$$V^* := \{x \in E \mid \forall y \in V : \mathrm{Tr}_{E|K}(xy) \in R\}.$$

Aus $S \cdot V \subseteq S$ folgt $Tr_{E|K}(S \cdot V) \subseteq \mathrm{Tr}_{E|K}(S) \subseteq R$ nach Satz 5.4, was wiederum $S \subseteq V^*$ impliziert.
Schritt 3: Wir betrachten nun die Abbildung

$$\mu : E \to \mathrm{Hom}_K(E, K), \quad x \mapsto \mu(x)(y) := (y \mapsto \mathrm{Tr}_{E|K}(xy)).$$

Aus der K-Linearität der Spurabbildung folgt unmittelbar, dass auch μ K-linear ist. μ ist sogar ein Isomorphismus. Da $\dim_K(E) = n = \dim_K(\mathrm{Hom}_K(E, K))$ gilt, reicht es aus, die Injektivität von μ zu zeigen.
Sei dafür $x \in E\backslash\{0\}$. Da $x \neq 0$, kann man (x) zu einer K-Basis $b = (x_1, x_2, \ldots, x_n)$ von E mit $x = x_1$ ergänzen. Nach Proposition 5.6 gilt $\mathrm{d}(b) = |(\mathrm{Tr}_{E|K}(x_i x_j))_{i,j}| \neq 0$. Daraus folgt $\mu_x \neq 0 \in \mathrm{Hom}_K(E|K)$, da sonst die erste Spalte von $(x_i x_j)_{i,j}$ und somit auch die Determinante von $(x_i x_j)_{i,j}$ gleich Null wäre. Daher ist μ injektiv und sogar ein Isomorphismus.
Schritt 4: Für $1 \leq j \leq n$ sei $f_j : E \to K$ die eindeutig bestimmte K-lineare Abbildung mit $f_j(e_i) = \delta_{ij}$ für alle $1 \leq i \leq n$. Aufgrund der Surjektivität der Abbildung μ in Schritt 3 existiert $e_j^* \in E$ mit $f_j = \mu(e_j^*)$, d.h.

$$\delta_{ij} = f_j(e_i) = \mu(e_j^*)(e_i) = \mathrm{Tr}_{E|K}(e_j^* e_i) \quad \text{für alle } i, j \in \{1, \ldots, n\}.$$

Diese $e_1^*, \dots, e_n^*$ bilden ebenfalls eine K-Basis von E. Sind nämlich $\lambda_1, \dots, \lambda_n \in K$ mit $\sum_{j=1}^{n} \lambda_j e_j^* = 0$, so gilt für alle $i = 1, \dots, n$

$$0 = \mathrm{Tr}_{E|K}(0 \cdot e_i) = \mathrm{Tr}_{E|K}\big(\sum_{j=1}^{n} \lambda_j e_j^* e_i\big) = \sum_{j=1}^{n} \lambda_j \,\mathrm{Tr}_{E|K}(e_j^* e_i) = \sum_{j=1}^{n} \lambda_j \delta_{ij} = \lambda_i.$$

Schritt 5: Da wir am Ende von Schritt 2 bereits $S \subseteq V^*$ gesehen haben, bleibt zu zeigen, dass V^* als R-Modul endlich erzeugt ist. Dann sind V^* und S endlich erzeugte R-Moduln und S ist damit noethersch.
Wir wollen nun zeigen, dass $V^* = \mathrm{span}_R\{e_1^*, \dots, e_n^*\}$ gilt. Mit der K-Basis $(e_j^*)_j$ von E können wir ein beliebig gewähltes $x \in V^* \subseteq E$ schreiben als $x = \sum_{j=1}^{n} \lambda_j e_j^*$ mit geeigneten $\lambda_1, \dots, \lambda_n \in K$. Für alle $i \in \{1, \dots, n\}$ haben wir $\mathrm{Tr}_{E|F}(xe_i) \in R$ wegen $x \in V^*$ und $e_i \in V$ sodass

$$R \ni \mathrm{Tr}_{E|F}(xe_i) = \mathrm{Tr}_{E|K}\big(\sum_{j=1}^{n} \lambda_j e_j^* e_i\big) = \sum_{j=1}^{n} \lambda_j \,\mathrm{Tr}_{E|K}(e_j^* e_i) = \sum_{j=1}^{n} (\lambda_j \delta_{ij}) = \lambda_i.$$

Es folgt $x \in \mathrm{span}_R\{e_1^*, \dots, e_n^*\}$.
Nun sei $y \in V$ mit $y = \sum_{i=1}^{n} \mu_i e_i$ für geeignete $\mu_i \in R$. Dann liegt $\mathrm{Tr}_{E|F}(e_j^* y)$ in R für alle $j = 1, \dots, n$, denn

$$\mathrm{Tr}_{E|F}(e_j^* y) = \sum_{i=1}^{n} \mu_i \,\mathrm{Tr}_{E|F}(e_j^* e_i) = \mu_i \in R.$$

Daraus folgt nun $e_j^* \in V^*$ für alle $j \in \{1, \dots, n\}$, sodass insgesamt $\mathrm{span}_R\{e_1^*, \dots, e_n^*\} = V^*$.
□

6 Ganze Ringererweiterungen und Zahlkörper

Satz 6.1
Sei $S|R$ eine ganze Ringerweiterung und seien $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ Primideale in S. Ferner seien die Ideale $\mathfrak{a}_i := \mathfrak{b}_i \cap R$ für $i = 1, 2$ definiert. Falls $\mathfrak{a}_1 = \mathfrak{a}_2$ gilt so folgt $\mathfrak{b}_1 = \mathfrak{b}_2$.

Beweis
Sei $\pi : S \to S/\mathfrak{b}_1$ die Quotientenabbildung. Wir nehmen an, dass $\mathfrak{b}_1 \neq \mathfrak{b}_2$ gilt. Dann ist $\mathfrak{b}_1 \subsetneq \mathfrak{b}_2$ und es existiert ein Element $a \in \mathfrak{b}_2 \setminus \mathfrak{b}_1$. Nach Voraussetzung ist a ganz über R und damit ist auch $\bar{a} := \pi(a)$ ganz über $S/\mathfrak{b}_1$. Man wende hierfür π auf eine ganze Gleichung von a an. Sei

$$\bar{a}^n + \bar{\lambda}_{n-1}\bar{a}^{n-1} + \ldots + \bar{\lambda}_0\bar{a}^0 = 0$$

eine ganze Gleichung von $\bar{a}$ in $S/\mathfrak{b}_1$ mit $\lambda_i \in R$ und minimalem Grad n. Es gilt $\bar{\lambda}_0 \neq \bar{0}$. Anderenfalls wäre

$$\bar{a}(\bar{a}^{n-1} + \bar{\lambda}_{n-1}\bar{a}^{n-2} + \ldots + \bar{\lambda}_1) = \bar{0}$$

woraus $\bar{a}^{n-1} + \bar{\lambda}_{n-1}\bar{a}^{n-2} + \ldots \bar{\lambda}_1 = \bar{0}$ folgen würde, da $\bar{a} \neq \bar{0}$ und $S/\mathfrak{b}_1$ nullteilerfrei ist. Die Existenz der letzten Gleichung würde der Minimalität von n widersprechen, also ist $\bar{\lambda}_0 \neq 0$. Wegen der ganzen Gleichung von $\bar{a}$ ist andererseits $\bar{\lambda}_0 \in \mathrm{span}_{S/\mathfrak{b}_1}\{\bar{a}\} \subseteq \pi(\mathfrak{b}_2) \subseteq S/\mathfrak{b}_1$. Da $\lambda_0 \in R$ ist auch

$$\bar{\lambda}_0 \in \pi(\mathfrak{b}_2 \cap R) \overset{\text{Ann.}}{=} \pi(\mathfrak{b}_1 \cap R) = \{0\},$$

im Widerspruch zu $\bar{\lambda}_0 \neq \bar{0}$. Also ist die ursprüngliche Annahme $\mathfrak{b}_1 \neq \mathfrak{b}_2$ falsch und $\mathfrak{b}_1 = \mathfrak{b}_2$, wie behauptet. □

Korollar 6.2
Sei R ein Integritätsbereich und $S|R$ eine ganze Ringerweiterung. Dann gilt die Ungleichung $\dim(S) \leq \dim(R)$.

Beweis
Sei $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_n$ eine Primidealkette in S und $\mathfrak{p}_i := \mathfrak{q}_i \cap R$, $i = 1, \ldots, n$. Laut dem vorangehenden Satz sind die $\mathfrak{p}_i$ paarweise verschieden, bilden also eine Primidealkette. Dies beweist die Aussage. □

Bemerkung
Im vorigen Korollar gilt tatsächlich auch die Gleichheit $\dim(S) = \dim(R)$, die wir hier aber nicht benötigen. Der interessierte Leser schlage den „Going up"-Satz nach ([**AM**] Theorem 5.11.).

Anschließend können wir untersuchen, wie sich Dedekindringe beim Bilden ganzer Abschlüsse in separablen Erweiterungen ihrer Quotientenkörper verhalten.

Definition 6.3

(i) Ein algebraischer Zahlkörper ist eine endliche Erweiterung von $\mathbb{Q}$.

(ii) Ein Ganzheitsring S ist der ganze Abschluss von $\mathbb{Z}$ in einem Zahlkörper E, also $S = \mathrm{A}_E(\mathbb{Z})$.

Korollar 6.4

(i) Sei R ein Dedekindring und $K := \mathrm{Quot}(R)$. Für jede endliche separable Körpererweiterung $E|K$ ist $S := \mathrm{A}_E(R)$ ein Dedekindring.

(ii) Jeder Ganzheitsring ist ein Dedekindring.

Beweis
(*i*) Die Eigenschaften ganzabgeschlossen, $\dim(S) \leq 1$ und noethersch folgen jeweils unmittelbar aus Satz 5.1, Korollar 6.2 und Satz 5.7.
(*ii*) $\mathbb{Z}$ ist ein Hauptidealring, insbesondere also ein Dedekindring, und die Aussage folgt unmittelbar aus (i). Beachte, dass $\mathbb{Q}$ perfekt und damit jede endliche Erweiterung separabel ist. □

Teil II
Projektive Moduln über Dedekindringen

1 Projektive Moduln

Wir bereiten zunächst einige allgemeine Aussagen aus der kommutativen Algebra vor, die wir für die Sätze brauchen, die am Ende dieses zweiten Teils bewiesen werden.

Definition 1.1
Sei R ein Ring, N, N' zwei beliebige R-Moduln und $p : N \twoheadrightarrow N'$ eine beliebige R-lineare Surjektion. Ein R-Modul M heißt projektiv, falls für jede R-lineare Abbildung $f : M \to N'$ eine R-lineare Abbildung $g : M \to N$ existiert, sodass $f = p \circ g$. Visualisiert in einem Diagramm:

$$\begin{array}{ccccc} N & \xrightarrow{p} & N' & \longrightarrow & 0 \\ & \nwarrow^{\exists g} & \uparrow{\scriptstyle f} & & \\ & & M & & \end{array}$$

Bemerkung 1.2
Sei durch

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0 \tag{1}$$

eine exakte Sequenz von R-Moduln gegeben und sei M ein R-Modul. Betrachte die folgende Sequenz:

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \xrightarrow{\mathrm{comp}_f} \mathrm{Hom}_R(M, N) \xrightarrow{\mathrm{comp}_g} \mathrm{Hom}_R(M, N'') \longrightarrow 0 \tag{2}$$

Mit comp_f meinen wir die Komposition mit f, also $\mathrm{comp}_f(h) = f \circ h$, für $h \in \mathrm{Hom}_R(M, N')$; analog für comp_g.
Die Sequenz (2) ist nach **[AM]** Proposition 2.9. ii) bereits linksexakt. M ist also genau dann projektiv, wenn für beliebige exakte Sequenzen von R-Moduln der Form (1) die zugehörige Sequenz (2) exakt ist, mit anderen Worten: wenn der Funktor $\mathrm{Hom}_R(M, \bullet)$ exakt ist.

Definition 1.3
Sei

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

eine kurze exakte Sequenz von R-Moduln. Falls R-lineare Abbildungen $\varphi : N \to N'$, $\gamma : N'' \to N$ existieren, sodass: $\varphi \circ f = \mathrm{id}_{N'}$ und $g \circ \gamma = \mathrm{id}_{N''}$, sagen wir, dass die Sequenz zerfällt.

Lemma 1.4
Sei eine kurze exakte Sequenz

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

von R-Moduln gegeben. Es sind äquivalent:

(i) Die Sequenz zerfällt links, d.h. es gibt eine Abbildung $\varphi : N \to N'$ mit $\varphi \circ f = \mathrm{id}_{N'}$.

(ii) Die Sequenz zerfällt rechts, d.h. es gibt eine Abbildung $\gamma : N'' \to N$ mit $g \circ \gamma = \mathrm{id}_{N''}$.

(iii) Es gibt einen R-Untermodul M von N mit $N = \mathrm{im}(f) \oplus M$.

(iv) Die Sequenz zerfällt.

Beweis
$(iii) \Rightarrow (i)$: Die Abbildung $f : N' \to \mathrm{im}(f)$ ist ein Isomorphismus. Wir definieren φ als die Projektion $N = \mathrm{im}(f) \oplus M \to \mathrm{im}(f)$ verknüpft mit der Inversen von $f : N' \to \mathrm{im}(f)$.
$(iii) \Rightarrow (ii)$: Wegen $\mathrm{im}(f) = \ker(g)$ schränkt sich g zu einem Isomorphismus $M \to N''$ ein. Wir definieren γ als den inversen Isomorphismus $N'' \to M$ verknüpft mit der Inklusion $M \subseteq \mathrm{im}(f) \oplus M = N$.
$(i) \Rightarrow (iii)$: Wir zeigen $N = \mathrm{im}(f) \oplus \ker(\varphi)$ und können dann $M = \ker(\varphi)$ sehen. Sei dazu $n \in N$ ein beliebiges Element. Es gilt $n = (n - (f \circ \varphi)(n)) + (f \circ \varphi)(n)$. $(f \circ \varphi)(n)$ liegt sicherlich im Bild von f. Desweiteren liegt $(n - (f \circ \varphi(n))$ im Kern von φ, denn

$$\varphi(n - (f \circ \varphi)(n)) = \varphi(n) - (\underbrace{\varphi \circ f}_{=\mathrm{id}_{N'}} \circ \varphi)(n) = \varphi(n) - \varphi(n) = 0.$$

Es folgt $N = \mathrm{im}(f) + \ker(\varphi)$. Sei nun $n \in \mathrm{im}(f) \cap \ker(\varphi)$. Dann existiert ein $n' \in N'$ mit $f(n') = n$ und $\varphi(n) = 0$. Es ist $n' = \varphi(f(n')) = \varphi(n) = 0$, somit auch $n = 0$.
$(ii) \Rightarrow (iii)$ Zeige ähnlich zum vorigen Schritt $N = \ker(g) \oplus \mathrm{im}(\gamma)$. Setze dann $M := \mathrm{im}(\gamma)$ und beachte $\ker(g) = \mathrm{im}(f)$. Sei $n \in N$ beliebig. Schreibe n als $n = (n-(\gamma \circ g)(n)) + (\gamma \circ g)(n)$. Dieser Ausdruck liegt in $\ker(g) + \mathrm{im}(\gamma)$, denn:

$$g(n - (\gamma \circ g)(n)) = g(n) - (g \circ \gamma \circ g)(n) = g(n) - g(n) = 0$$

und $(\gamma \circ g)(n) \in \mathrm{im}(\gamma)$. Für $n' \in \ker(g) \cap \mathrm{im}(\gamma)$ ist $g(n') = 0$ und $n' = \gamma(n'')$ für ein $n'' \in N''$ also wie eben $0 = g(n') = (g \circ \gamma)(n'') = n''$.

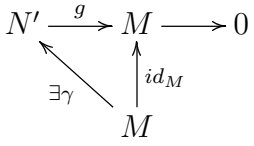
Die Bedingung (iv) ist per Definition genau $(i) \wedge (ii)$. Es ist bereits gezeigt, dass
$(i) \Leftrightarrow (iii) \Leftrightarrow (ii)$ gilt, daraus folgt die gesamte Aussage. □

Lemma 1.5
Sei R ein Ring und M ein R-Modul. M ist projektiv genau dann, wenn jede kurze exakte Sequenz der Form

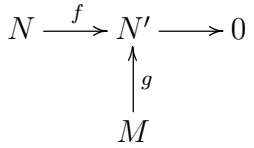
$$0 \longrightarrow N \longrightarrow N' \longrightarrow M \longrightarrow 0$$

zerfällt.

Beweis
„ ⇒ “ Sei M projektiv und $0 \longrightarrow N \longrightarrow N' \xrightarrow{g} M \longrightarrow 0$ eine kurze exakte Sequenz. Betrachte folgendes Diagramm:



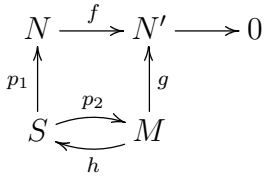
Nach Satz 1.4(ii) bedeutet die Kommutativität des Diagramms, dass die Sequenz zerfällt.
„ ⇐ “ Sei ein Diagramm mit exakter Zeile der folgender Form gegeben:



Definiere $S := \{(x, y) \in N \oplus M |\ f(x) = g(y)\} \subseteq N \oplus M$. Als Untermodul einer direkten Summe, besitzt S die zwei Projektionen $p_1 : S \to N$ und $p_2 : S \to M$. Da f surjektiv ist, ist $\mathrm{im}(f) = N' \supseteq \mathrm{im}(g)$. Für beliebige $g(m)$ existiert also ein $n \in N$ mit $f(n) = g(m)$. Also ist p_2 surjektiv. Wir erhalten eine exakte Sequenz:

$$0 \longrightarrow \ker(p_2) \hookrightarrow S \xrightarrow{p_2} M \longrightarrow 0\,.$$

Per Annahme zerfällt die Sequenz. Es gibt also eine Abbildung
$h : M \to S$ mit $p_2 \circ h = \mathrm{id}_M$. Ergänze damit das letzte Diagramm zu



Wir haben $f \circ p_1 = g \circ p_2$. Für ein beliebiges $s = (n, m) \in S$ ist nämlich

$$(f \circ p_1)(s) = f(n) = g(m) = (g \circ p_2)(s).$$

Dann ist $p_1 \circ h : M \to N$ genau die gesuchte Abbildung: $f \circ p_1 \circ h = g \circ p_2 \circ h = g$. □

Satz 1.6
Sei M ein R-Modul. M ist projektiv genau dann, wenn M direkter Summand eines freien Moduls ist, d.h. wenn ein R-Modul L existiert, sodass $M \oplus L$ frei ist.

Beweis
„ ⇒ “ Angenommen M ist projektiv und $R^{(I)}$ der freie R-Modul über $I = M$ mit der Standardbasis $(e_m)_{m \in M}$. Betrachte nun die surjektive R-lineare Abbildung $\varphi : R^{(I)} \to M$ mit $\varphi(e_m) := m$. Man erhält die kurze exakte Sequenz

$$0 \longrightarrow \ker(\varphi) \hookrightarrow R^{(I)} \xrightarrow{\varphi} M \longrightarrow 0\,.$$

Nach Lemma 1.4 und Lemma 1.5 ist dann $R^{(I)} \cong \ker(\varphi) \oplus M$.
„ ⇐ “ Sei $p : N \twoheadrightarrow N'$ eine R-lineare Surjektion. Nach Bemerkung 1.2 genügt es zu zeigen, dass $\mathrm{Hom}_R(M, N) \xrightarrow{\mathrm{comp}_p} \mathrm{Hom}_R(M, N')$ ebenfalls eine Surjektion ist.

Wir haben per Annahme $M \oplus L \cong R^{(I)}$ mit einem R-Modul L und einer Indexmenge I. Die universelle Eigenschaft der direkten Summe liefert uns

$$\mathrm{Hom}_R(R^{(I)}, N) \cong \mathrm{Hom}_R(M, N) \oplus \mathrm{Hom}_R(L, N).$$

Sei nun $f : R^{(I)} \to N'$ eine beliebige R-lineare Abbildung. Zu jedem $i \in I$ wähle $n_i \in N$ mit $p(n_i) = f(e_i)$, wobei wir die Surjektivität von p verwenden. Sei ferner $g : R^{(I)} \to N$ die eindeutig bestimmte R-lineare Abbildung mit $g(e_i) = n_i$ für alle $i \in I$.
Es ist $p(g(e_i)) = p(n_i) = f(e_i)$. Das impliziert $p \circ g = f$, sodass comp_p eine Surjektion ist. Das nächste Diagramm zeigt dann die Surjektivität von $\mathrm{Hom}_R(M, N) \twoheadrightarrow \mathrm{Hom}_R(M, N')$:

$$\begin{array}{ccc} \mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(L,N) & & \mathrm{Hom}_R(M,N') \oplus \mathrm{Hom}_R(L,N') \\ \downarrow \cong & & \downarrow \cong \\ \mathrm{Hom}_R(R^{(I)}, N) & \xrightarrow{\mathrm{comp}_p} & \mathrm{Hom}_R(R^{(I)}, N') \end{array}$$

□

Lemma 1.7
Sei R ein Ring und M ein R-Modul. Wenn M projektiv ist, dann ist M flach.

Beweis
Zunächst hat man für beliebige R-Moduln A, B, C die Isomorphismen

$$A \cong R \underset{R}{\otimes} A \text{ und } (A \oplus B) \underset{R}{\otimes} C \cong (A \underset{R}{\otimes} C) \oplus (B \underset{R}{\otimes} C)$$

(siehe **[AM]** Proposition 2.14. iv) und ii)). Für einen freien Modul A gilt dann für eine geeignete Indexmenge I

$$A \underset{R}{\otimes} N \cong R^{(I)} \underset{R}{\otimes} N \cong (\underset{I}{\oplus} R) \underset{R}{\otimes} N \cong \underset{I}{\oplus} (R \underset{R}{\otimes} N) \cong \underset{I}{\oplus} N.$$

Also sind freie Moduln aufgrund der universellen Eigenschaft der direkten Summe flach.
Nach Satz 1.6 ist $M := M \oplus M' \cong R^{(I)}$ für einen R-Modul M'. Sei $N \xrightarrow{f} N'$ eine R-lineare Injektion. Nach dem eben Gezeigten ist dann $\mathrm{id}_{M \oplus M'} \otimes f : (M \oplus M') \otimes_R N \to (M \oplus M') \otimes_R N'$ ebenfalls injektiv. Insbesondere ist mit der universellen Eigenschaft der direkten Summe auch $\mathrm{id}_M \otimes f : M \otimes_R N \to M \otimes_R N'$ injektiv. □

2 Projektive Moduln über lokalen Ringen

Als Vorbereitung für die Untersuchung von projektiven Moduln über Dedekindringen brauchen wir zunächst ein paar Aussagen über projektive Moduln über lokalen Ringen.

Definition 2.1

(i) Seien $f \in R$ und $\mathfrak{p} \in \mathrm{Spec}(R)$. Zudem sei $\iota_\mathfrak{p} : R \to R_\mathfrak{p}$ die kanonische Lokalisierungsabbildung und $\pi_p : R_\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ die Restklassenabbildung. Definiere $f(\mathfrak{p}) := (\pi_\mathfrak{p} \circ \iota_\mathfrak{p})(f)$.

(ii) Ein R-Modul M heißt lokal frei von endlichem Rang, falls für alle $\mathfrak{p} \in \mathrm{Spec}(R)$ ein $f \in R$ existiert, sodass $f(\mathfrak{p}) \neq 0$ und $M_f = M \otimes_R R_f$ frei von endlichem Rang ist.

Definition 2.2
Ein R-Modul M heißt endlich präsentiert, falls eine exakte Sequenz folgender Form existiert:

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0 \text{ mit } m, n \in \mathbb{N}.$$

Bevor wir dieses Unterkapitel mit Lemma 2.4 abschließen, holen wir uns den folgenden Zusammenhang, der in **[BoG]** Proposition 3. Chapter 4.4 nachzulesen ist, vor Augen:

Proposition 2.3
Sei M ein R-Modul. Es sind äquivalent:

(i) M ist lokal frei von endlichem Rang.

(ii) M ist endlich präsentiert und flach.

(iii) M ist endlich präsentiert und für alle maximalen Ideale $\mathfrak{m} \in \mathrm{Spec}(R)$ ist $M \otimes_R R_\mathfrak{m}$ frei.

□

Lemma 2.4
Sei R ein noetherscher lokaler Ring. Für einen endlich erzeugten R-Modul M sind die folgenden Aussagen äquivalent:

(i) M ist frei.

(ii) M ist projektiv.

(iii) M ist flach.

Beweis
$(i) \Rightarrow (ii)$: Wir haben das in Satz 1.6 gesehen.
$(ii) \Rightarrow (iii)$: Man entnehme dies Lemma 1.7.
$(iii) \Rightarrow (i)$: Über einem noetherschen Ring R ist jeder R-Modul genau dann endlich erzeugt wenn er endlich präsentiert ist. Da R lokal ist, ist weiterhin $R \setminus \mathfrak{m} = R^\times$, und daher $M \cong M_\mathfrak{m}$ frei nach Proposition 2.3.

□

3 Projektive Moduln über Dedekindringen

Lemma 3.1
Sei R ein Integritätsbereich. Ein R-Modul $M \neq 0$ ist genau dann torsionsfrei, wenn für alle maximalen Ideale $\mathfrak{m}$ von R der R_m-Modul $M_\mathfrak{m}$ torsionsfrei ist.

Beweis
„ $\Rightarrow$ “ Angenommen $\frac{r}{s}\frac{a}{s'} = 0$ mit $s, s' \in R \setminus \mathfrak{m}$, $r \in R$ und $a \in M$. Per Definition existiert dann ein $s'' \in R \setminus \mathfrak{m}$ mit $s''ra = 0$. Es gilt $s'' \neq 0$, da $s'' \notin \mathfrak{m}$. Falls $a \neq 0$ ist, ist $r = 0$, da R ein Integritätsbereich und M torsionsfrei ist. Daher ist auch $\frac{r}{s} = 0$.
„ $\Leftarrow$ “ Sei M nicht torsionsfrei. Dann existiert ein $0 \neq x \in M$ mit $\mathrm{Ann}_R(x) \neq 0$. Es gilt $\mathrm{Ann}_R(x) \neq R$, da sonst $1 \cdot x = x = 0$. Also ist $\mathrm{Ann}_R(M)$ ein echtes Ideal und daher $0 \neq \mathrm{Ann}_R(x) \subseteq \mathfrak{m}$ für ein maximales Ideal $\mathfrak{m}$.
Nun zeigt $0 = \frac{0}{1} = \frac{x}{1} \cdot \frac{a}{1}$ für $a \in \mathrm{Ann}_R(x) \setminus \{0\}$ dass $M_\mathfrak{m}$ nicht torsionsfrei ist. □

Lemma 3.2
Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul. M ist flach genau dann, wenn für alle $\mathfrak{m} \in \max(R)$ $M_\mathfrak{m}$ ein freier $R_\mathfrak{m}$-Modul ist.

Beweis
[AM] Proposition 3.10. besagt, dass M genau dann flach ist, wenn $M_\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ flach als $R_\mathfrak{m}$-Modul ist.
$R_\mathfrak{m}$ ist nach **[AK]** Proposition (11.14) lokal und nach dem Beweis von Satz 4.1 aus Teil I noethersch, da R noethersch ist. Es greift also das Lemma 2.4.
Insgesamt haben wir, dass M flach als R-Modul ist genau dann, wenn $M_\mathfrak{m}$ flach als $R_\mathfrak{m}$-Modul ist, genau dann wenn $M_\mathfrak{m}$ frei als $R_\mathfrak{m}$-Modul ist. □

Lemma 3.3
Sei R ein Ring und M, N zwei R-Moduln. Für $f, g : M \to N$ gilt $f = g$ genan dann, wenn $f_\mathfrak{m} = g_\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$. Hierbei bezeichnen $f_\mathfrak{m}$ bzw. $g_\mathfrak{m}$ die von f bzw. g induzierten $R_\mathfrak{m}$-linearen Abbildungen $M_\mathfrak{m} \to N_\mathfrak{m}$.

Beweis
„ $\Rightarrow$ “ Diese Richtung ist offensichtlich.
„ $\Leftarrow$ “ Sei $f_\mathfrak{m} = g_\mathfrak{m}$ und $a \in M$ beliebig. Für alle maximalen Ideale existiert dann ein $s_\mathfrak{m} \in R \setminus \mathfrak{m}$ mit $s_\mathfrak{m}(f(a) - g(a)) = 0$. Sei I das von allen $s_\mathfrak{m}$ erzeugte Ideal von R. Es ist per Definiton im Annihilator $\mathrm{Ann}_R(f(a) - g(a))$ enthalten. Für jedes maximale Ideal $\mathfrak{m}$ ist das zugehörige $s_\mathfrak{m}$ per Konstruktion kein Element aus $\mathfrak{m}$. **[AM]** Corollary 1.4. gibt uns $R = (s_\mathfrak{m})_{\mathfrak{m} \subseteq R \text{ max.}} = I$. Insbesondere gilt $0 = 1 \cdot (f(a) - g(a))$ für beliebige a und somit $f = g$. □

Satz 3.4
Sei R ein Dedekindring und M ein endlich erzeugter R-Modul. Folgende Aussagen sind äquivalent:

(i) M ist torsionsfrei.

(ii) M ist flach.

(iii) M ist projektiv.

Beweis
$(ii) \Rightarrow (i)$: Nach **[BoG]** Proposition 7(i) Chapter 2.7 gilt das über jedem Ring.
$(iii) \Rightarrow (ii)$ ist die Aussage von Lemma 1.7.
$(i) \Rightarrow (iii)$: Sei $\mathfrak{m}$ ein maximales Ideal von R. Nach Lemma 3.1 ist $M_{\mathfrak{m}}$ endlich erzeugt und torsionsfrei über $R_{\mathfrak{m}}$, wobei $R_{\mathfrak{m}}$ nach Satz 4.2 aus Teil I ein Hauptidealring ist. Nach dem Struktursatz für endlich erzeugte Moduln über Hauptidealringen (**[AK]** Exercise (5.41)) ist $M_{\mathfrak{m}}$ frei und damit projektiv. Da $\mathfrak{m}$ beliebig war, ist M projektiv nach Proposition 2.3 und Lemma 2.4. □

Wir kommen nun zu dem abschließenden Ergebnis dieses Unterkapitels, dem Struktursatz für endlich erzeugte Moduln über Dedekindringen.

Satz 3.5
Sei R ein Dedekindring und M ein endlich erzeugter R-Modul. Dann gilt $M \cong P \oplus \mathrm{T}(M)$. P ist hierbei ein torsionsfreier Modul und $\mathrm{T}(M)$ ist der Torsionsuntermodul von M.
Weiterhin gilt $\mathrm{T}(M) \cong \overset{k}{\underset{i=1}{\oplus}} R/\mathfrak{p}_i^{n_i}$ für gewisse Primideale $\mathfrak{p}_i \neq 0$ und $\mathfrak{n}_i \in \mathbb{Z}_{\geq 1}$. Die Paare $(\mathfrak{p}_i, n_i)$ sind bis auf Permutation eindeutig bestimmt.

Beweis
Zunächst ist $P := M/\mathrm{T}(M)$ torsionsfrei. Daher ist $M/\mathrm{T}(M)$ nach Satz 3.4 projektiv, was nach Lemma 1.5 bedeutet, dass die Sequenz

$$0 \longrightarrow \mathrm{T}(M) \xrightarrow{\iota} M \xrightarrow{\pi} M/\mathrm{T}(M) \longrightarrow 0$$

zerfällt. Wir haben also $M \cong (M/\mathrm{T}(M)) \oplus \mathrm{T}(M)$. Der erste Teil der Aussage ist also gezeigt. Wir untersuchen die Struktur von $\mathrm{T}(M)$ in 4 Schritten.
Schritt 1: $\mathrm{Ann}(\mathrm{T}(M)) \subseteq R$, ist also ein Ideal in einem Dedekindring. Es ist auch von Null verschieden. Im Fall $\mathrm{T}(M) = 0$ ist $\mathrm{Ann}(\mathrm{T}(M))$ der ganze Ring. Im Fall $\mathrm{T}(M) \neq 0$ wählen wir Erzeuger $t_1, \ldots, t_r$ von $\mathrm{T}(M)$ über R, wobei wir verwenden, dass M und damit auch $\mathrm{T}(M)$ endlich erzeugt ist. Zu jedem $i \in \{1, \ldots, t\}$ existiert $a_i \in R \setminus \{0\}$ mit $a_i \cdot t_i = 0$ per Definition von Torsionselementen. Dann ist $a = a_1 \cdot \ldots \cdot a_r \in R \setminus \{0\}$ mit $a \cdot t_i = 0$ für alle i und daher $a \cdot \mathrm{T}(M) = 0$, da $\mathrm{T}(M) = \mathrm{span}_R\{t_1, \ldots, t_r\}$. Also gilt $a \in \mathrm{Ann}(\mathrm{T}(M))$ und daher $\mathrm{Ann}(\mathrm{T}(M)) \neq 0$. Daher kann man $\mathrm{Ann}(\mathrm{T}(M))$ als $\mathrm{Ann}(\mathrm{T}(M)) = \prod_{i=1}^{n} \mathfrak{p}_i^{s_i}$ darstellen, mit paarweise verschiedenen von Null verschiedenen Primidealen $\mathfrak{p}_i$ und natürlichen Zahlen $n, s_i \in \mathbb{Z}_{\geq 1}$.
Definiere $\mathrm{Supp}(\mathrm{T}(M)) := \{\mathfrak{p} \mid \mathrm{T}(M)_{\mathfrak{p}} \neq 0\}$. Nach **[AM]** Exercise 3.19. v) und Schritt 1 aus dem Beweis von Satz 2.9 aus Teil I folgt $\mathrm{Supp}(\mathrm{T}(M)) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Sei $\mathfrak{p} \in \mathrm{Supp}(\mathrm{T}(M))$. Dann ist $R_{\mathfrak{p}}$ ein Hauptidealring (Satz 4.2 aus Teil I) und von Null verschiedene Ideale in $R_{\mathfrak{p}}$ sind von der Form $\mathfrak{p}^n R_{\mathfrak{p}}$ für ein $n \in \mathbb{Z}_{\geq 1}$ (Satz 3.1 aus Teil I). Der Struktursatz für endlich erzeugte Moduln über Hauptidealringen (**[AK]** Exercise (5.41)) zeigt, dass

$$\mathrm{T}(M)_{\mathfrak{p}} \cong \overset{n}{\underset{i=1}{\oplus}} R_{\mathfrak{p}}/\mathfrak{p}^{m_i} R_{\mathfrak{p}}$$

gilt für geeignete $m_1, .., m_n \geq 1$. Hierbei hängen $n, m_1, \ldots, m_n$ von $\mathfrak{p}$ ab.

Schritt 2: Zeige, dass

$$R_{\mathfrak{p}}/(\mathfrak{p}^{m_i}R_{\mathfrak{p}}) \cong (R/\mathfrak{p}^{m_i})_{\mathfrak{p}} \cong R/\mathfrak{p}^{m_i}$$

als R-Moduln. Zunächst zeigen wir $(R/\mathfrak{p}^{m_i})_{\mathfrak{p}} \cong R/\mathfrak{p}^{m_i}$.
Sei $s \notin \mathfrak{p}$ beliebig. Das heißt, dass $\mathfrak{p}$ in der Primfaktorzerlegung des Ideals sR nicht vorkommt und (s) und $\mathfrak{p}$ koprim sind. Im Beweis von Satz 3.1 aus Teil I haben wir gesehen, dass auch (s) und $\mathfrak{p}^{m_i}$ koprim sind. Insbesondere existiert ein $t \in R$ sodass $st - 1 \in \mathfrak{p}^{m_i}$, was heißt, dass $(s + \mathfrak{p}^{m_i}) \cdot (t + \mathfrak{p}^{m_i}) = 1 \in R/\mathfrak{p}^{m_i}$. Insbesondere ist die Skalarmultiplikation mit s auf dem R-Modul $R/\mathfrak{p}^{m_i}$ bijektiv. Aus der universellen Eigenschaft der Lokalisierung folgt dann, dass die kanonische Abbildung $R/\mathfrak{p}^{m_i} \to (R/\mathfrak{p}^{m_i})_{\mathfrak{p}}$ bijektiv ist.
Die Isomorphie $(R/\mathfrak{p}^{m_i})_{\mathfrak{p}} \cong R_{\mathfrak{p}}/\mathfrak{p}^{m_i}R_{\mathfrak{p}}$ folgt aus der Exkatheit des Lokalisierungsfunktors.
Insgesamt erhalten wir, dass $\mathrm{T}(M)_{\mathfrak{p}} \cong \overset{n}{\underset{i=1}{\oplus}} R_{\mathfrak{p}}/\mathfrak{p}^{m_i}R_{\mathfrak{p}} \cong \overset{n}{\underset{i=1}{\oplus}} R/\mathfrak{p}^{m_i}$.
Schritt 3: Sei $\mathfrak{q}$ ein Primideal mit $0 \neq \mathfrak{q} \neq \mathfrak{p}$. Da $\mathfrak{p}$ und $\mathfrak{q}$ maximal sind, gilt $\mathfrak{p} \setminus \mathfrak{q} \neq \emptyset$.
Wir behaupten $(R/\mathfrak{p}^{m_i})_{\mathfrak{q}} = 0$. Sei $s \in \mathfrak{p} \setminus \mathfrak{q} \subseteq R \setminus \mathfrak{q}$. Es folgt $s^{m_i} \in \mathfrak{p}^{m_i}$ und $s^{m_i} \cdot (R/\mathfrak{p}^{m_i}) = 0$, also $(R/\mathfrak{p}^{m_i})_{\mathfrak{q}} = 0$, da s^{m_i} in $R_{\mathfrak{q}}$ eine Einheit ist.
Schritt 4: Es gilt $(\mathrm{T}(M)_{\mathfrak{p}})_{\mathfrak{p}} \cong \mathrm{T}(M)_{\mathfrak{p}}$ und mit dem eben Gezeigten auch $(\mathrm{T}(M)_{\mathfrak{p}})_{\mathfrak{q}} = 0$, falls $\mathfrak{p} \neq \mathfrak{q}$. Wegen $\mathrm{Supp}(\mathrm{T}(M)) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ folgt hieraus, dass die R-lineare Abbildung

$$\mathrm{T}(M) \longrightarrow \overset{n}{\underset{i=1}{\oplus}} \mathrm{T}(M)_{\mathfrak{p}_i}$$

nach Lokalisierung an allen von Null verschiedenen Primidealen von R bijektiv ist. Aus **[AM]**, Proposition 3.9. folgt, dass es sich um einen Isomorphismus handelt. Aus Schritt 1 folgt die Existenz der gefragten Zerlegung von $\mathrm{T}(M)$. Die Eindeutigkeit in der Behauptung ist eine unmittelbare Konsequenz der bis auf Assoziiertheit eindeutigen Charakterisierung der Primelemente im Struktursatz für endlich erzeugte Moduln über Hauptidealringen (**[AK]** Exercise (5.41)). □

4 Projektive Moduln vom Rang 1

Definition 4.1
Sei R ein Integritätsbereich mit Quotientenkörper $\mathrm{Quot}(R) = K$ und M ein endlich erzeugter R-Modul. Der Rang von M über R ist definiert als $\mathrm{rg}_R(M) := \dim_K(M \otimes_R K)$.

Bemerkung
Falls M ein freier R-Modul vom Rang n ist dann ist

$$\dim_K(M \underset{R}{\otimes} K) = \dim_K((\overset{n}{\underset{i=1}{\oplus}} R) \underset{R}{\otimes} K) = \dim_K(\overset{n}{\underset{i=1}{\oplus}} K) = \mathrm{rg}_R(M).$$

Also führt obige Definition eine konsistente Erweiterung des Begriffs eines Rangs auch für nicht freie Moduln ein.

Lemma 4.2
Sei R ein Integritätsbereich. Für ein gebrochenes Ideal I gilt $\mathrm{rg}(I) = 1$.

Beweis
Sei $x \in R \setminus \{0\}$ so gewählt, dass $xI \subseteq R$. Als R-Moduln sind xI und I isomorph, sodass wir $I \subseteq R$ annehmen können.
Wir können aufgrund der Flachheit der Lokalisierung $I \otimes_R K$ auch als Untermodul von $R \otimes_R K \cong K$ asehen. $I \otimes_R K$ kann also über K nur die Dimension 0 oder 1 haben. Die Abbildung $I \otimes_R K \hookrightarrow K$ bildet $i \otimes 1$ auf $1 \cdot i = i$ ab. Wegen $I \neq 0$ gilt also auch $I \otimes_R K \neq 0$ und daher $\mathrm{rg}_R(I) = \dim_K(I \otimes_R K) = 1$. □

Lemma 4.3
Sei R ein Integritätsbereich und I ein gebrochenes Ideal. I ist genau dann projektiv, wenn I invertierbar ist, d.h. eine Einheit im Monoid $\mathbb{I}_R$.

Beweis
„ $\Rightarrow$ “ Sei I also projektiv. In Satz 1.6 haben wir gesehen, dass ein R-Modul S existiert, sodass $I \oplus S \cong R^{(J)}$ für eine Indexmenge J. Sei $i : I \to I \oplus S$ die Inklusion, $p : I \oplus S \to I$ die Projektion, und π_j die Projektion von $R^{(J)}$ auf seine j-te Komponente. Betrachte die Komposition

$$g_j : I \xrightarrow{i} I \oplus S = R^{(J)} \xrightarrow{\pi_j} R$$

und beachte $p \circ i = \mathrm{id}_I$.
Sei nun $a \in I$ ein Element ungleich Null. Für jedes $j \in J$ definiere $b_j := a^{-1} g_j(a) \in \mathrm{Quot}(R)$. Sei B das R-Erzeugnis von allen b_j. Wir behaupten, dass $B = I^{-1}$. Zunächst ist B ein gebrochenes Ideal, da per Definition von B, $aB \subseteq R$ gilt. Sei $x \in I$ beliebig, dann gilt: $xb_j = a^{-1} x g_j(a) = a^{-1} g_j(xa) = g_j(x) \in R$. Das zeigt, dass $BI \subseteq R$ gilt.
Sei weiterhin mit e_j der j-te Einheitsvektor von $R^{(J)}$ bezeichnet. Jedes Element z aus der direkten Summe $I \oplus S = R^{(J)}$ ist eine endliche R-Linearkombination von diesen, es ist nämlich $z = \sum_{j \in J} \pi_j(z) e_j$. Falls wir also $i(x) = (x, 0)$ berachten mit $x \in I$, so gilt $i(x) = \sum_{j \in J} g_j(x) e_j$. Es gilt mit demselben a, welches oben gewählt wurde

$$1 = a^{-1} \underbrace{(p \circ \iota)}_{=\mathrm{id}_I}(a) = a^{-1} p(\sum_{j \in J} g_j(a) e_j) = \sum_{j \in J} (a^{-1} g_j(a)) p(e_j) \in BI,$$

was $BI = R$ zeigt.

„ $\Rightarrow$ “ Sei nun I invertierbar und $f : M \to I$ eine R-lineare Surjektion. Nach Lemma 1.5 müssen wir eine R-lineare Abbildung $g : I \to M$ konstruieren mit $f \circ g = \mathrm{id}_I$. I ist invertierbar, also existieren $x_1, \ldots, x_n \in I$ und $y_1, \ldots, y_n \in I^{-1}$ mit $\sum_{i=1}^n x_i y_i = 1$. Da f surjektiv ist, existiert zu jedem x_i ein Element $c_i \in M$ mit $f(c_i) = x_i$. Wir definieren nun $g : I \to M$ durch $g(x) = \sum_{i=1}^n (xy_i)c_i$. Berechne nun

$$(f \circ g)(x) = f(\sum_{i=1}^n (xy_i)c_i) = \sum_{i=1}^n (xy_i)f(c_i) = x\sum_{i=1}^n (y_i x_i) = x.$$

□

Lemma 4.4
Sei R ein Dedekindring und seien I und J gebrochene Ideale. Es gilt $I \cong J$ als R-Moduln genau dann, wenn es ein $x \in \mathrm{Quot}(R) \setminus \{0\}$ gibt, mit $I = xJ$ als R-Untermoduln von $\mathrm{Quot}(R)$, mit anderen Worten, wenn $\bar{I} = \bar{J} \in \mathbb{C}_R$.

Beweis
” $\Rightarrow$ ” Jeder R-lineare Isomorphismus $\varphi : J \to I$ induziert einen K-linearen Isomorphismus $\varphi \otimes \mathrm{id}_K : J \otimes_R K \to I \otimes_R K$, wobei $K = \mathrm{Quot}(R)$. Der Beweis von Lemma 4.2 zeigt $I \otimes_R K \cong K$ und $J \otimes_R K \cong K$. Jeder K-lineare Automorphismus von K ist aber durch Multiplikation mit einem Element $x \in K^\times$ gegeben. Die Kommutativität des Diagramms

$$\begin{array}{ccc} J & \xrightarrow{\varphi} & I \\ \downarrow & & \downarrow \\ J \otimes_R K & \xrightarrow{\varphi \otimes \mathrm{id}_K} & I \otimes_R K \\ \cong\downarrow & & \downarrow\cong \\ K & \xrightarrow{\cong} & K \end{array}$$

zeigt dann $xJ = I$ als R-Untermoduln von K.
” $\Leftarrow$ ” Trivial, weil notwendigerweise $x \neq 0$ gilt. □

5 Klassifikation projektiver Moduln über Dedekindringen

Wir kommen nun nun zum letzten Abschnitt der Arbeit, der Klassifikation von projektiven Moduln über einem Dedekindring R von beliebigem Rang. Dazu brauchen wir ein wenig Vorbereitung.
Für das nächste Lemma erinnere man sich daran, wie wir in Satz 4.2 in Teil I für jedes $\mathfrak{p} \in \mathrm{Spec}(R) \setminus \{0\}$ eine diskrete Bewertung $\nu_\mathfrak{p} : \mathrm{Quot}(R) \to \mathbb{Z} \bigcup \{\infty\}$ konstruiert haben. Für $x = 0$ ist $\nu_\mathfrak{p}(x) = \infty$. Für ein $x \neq 0$ schreiben wir $(x) = \prod_{0 \neq \mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}^{n_\mathfrak{p}}$ und setzen $\nu_\mathfrak{p}(x) = n_\mathfrak{p}$.

Lemma 5.1
Sei R ein Dedekindring und X eine endliche Menge von von Null verschiedenen Primidealen. Zu jedem $\mathfrak{p} \in X$ sei ein $k_\mathfrak{p} \in \mathbb{Z}$ gegeben. Dann existiert ein $x \in \mathrm{Quot}(R)^\times$ mit:

$$\nu_\mathfrak{p}(x) = k_\mathfrak{p} \text{ für alle } \mathfrak{p} \in X \text{ und } \nu_\mathfrak{p}(x) \geq 0 \text{ für alle } \mathfrak{p} \notin X.$$

Beweis
Sei $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ und seien $k_1, \ldots, k_n$ die zugehörigen ganzen Zahlen. Zunächst nehmen wir an, dass alle Zahle nicht negativ sind. Die Ideale $p_i^{k_i+1}$ sind paarweise koprim, wie wir in Schritt 1 aus dem Beweis von Satz 3.2 in Teil I gesehen haben, daher wissen wir, dass die Abbildung $\varphi : R \longrightarrow R/\mathfrak{p}_1^{k_1+1} \times \ldots \times R/\mathfrak{p}_n^{k_n+1}$ surjektiv ist. Aufgrund der eindeutigen Faktorisierung jedes Ideals in einem Dedekindring, die wir in Satz 2.9 im ersten Teil gesehen haben, wissen wir, dass wir stets ein $x_i \in \mathfrak{p}_i^{k_i} \setminus \mathfrak{p}_i^{k_i+1}$ für $i = 1, \ldots, n$ wählen können. Definiere x, als das Urbild von $(x_1 + \mathfrak{p}_1^{k_1+1}, \ldots, x_n + \mathfrak{p}_n^{k_n+1})$ unter φ. Wir haben dann $x - x_i \in \mathfrak{p}_i^{k_i+1}$ für alle $i = 1, \ldots, n$. Aus $x_i \in \mathfrak{p}_i^{k_i} \setminus \mathfrak{p}_i^{k_i+1}$ folgt daher $x \in \mathfrak{p}_i^{k_i} \setminus \mathfrak{p}_i^{k_i+1}$ und daraus $\nu_{\mathfrak{p}_i}(x) = k_i$ für alle $i = 1, \ldots, n$.
Satz 3.1 aus Teil I stellt zudem sicher, dass für alle weiteren Primideale die Bewertung nichtnegativ ist, da x ein Element von R ist.
Für den allgemeinen Fall gelte für die k_i, gegebenenfalls nach Umbenennung, $k_i \geq 0$ für $i = 1, \ldots, m$ mit einem $m \leq n$ und $k_j < 0$ für $j = m+1, \ldots, n$.
Wir wissen aus dem vorangehenden Fall, dass $y \in R$ existiert, welches $\nu_{\mathfrak{p}_j}(y) = -k_i (> 0)$ für $j = m+1, \ldots, n$ und $\nu_{\mathfrak{p}_i}(y) = 0$ für $i = 1, \ldots, m$ erfüllt. Somit enthält die Primfaktorzerlegung von (y) das Ideal $\mathfrak{p}_{m+1}^{-k_{m+1}} \cdot \ldots \cdot \mathfrak{p}_n^{-k_n}$. Wir können also annehmen, dass das von y erzeugte Ideal folgende Gestalt hat:

$$(y) = \prod_{j=m+1}^{n} \mathfrak{p}_j^{-k_j} \cdot \prod_{s=1}^{t} \mathfrak{q}_s^{u_s}$$

mit $\mathfrak{q}_s \in \mathrm{Spec}(R) \setminus \{0, \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ und $u_s \geq 1$ für $s = 1, \ldots, t$. Wir merken an, dass $(y) \neq 0$ und daher $y \neq 0$. Weiterhin wählen wir $x \in R$ mit $\nu_{\mathfrak{p}_i}(x) = k_i$ für $i = 1, \ldots, m$, $\nu_{\mathfrak{p}_j}(x) = 0$ für $j = m+1, \ldots, n$ und $\nu_{\mathfrak{q}_s}(x) = u_s$ für $s = 1, \ldots, t$ und behaupten, dass $\frac{x}{y}$ die Behauptung erfüllt. Das von x erzeugte Ideal hat die Primfaktorzerlegung

$$(x) = \prod_{i=1}^{m} \mathfrak{p}_i^{k_i} \cdot \prod_{s=1}^{t} \mathfrak{q}_s^{u_s} \cdot \prod_{v=1}^{w} {\mathfrak{q}'_v}^{z_v}$$

mit $\mathfrak{q}'_v \in \mathrm{Spec}(R) \setminus \{0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots \mathfrak{q}_t\}$ und $z_v \geq 1$ für $v = 1, \ldots w$.

Betrachte das gebrochene Ideal $(\frac{x}{y})$.

$$\begin{aligned}(\frac{x}{y}) &= (x)\cdot(y^{-1}) = (x)\cdot(y)^{-1}\\ &= \prod_{i=1}^{m}\mathfrak{p}_i^{k_i}\cdot\prod_{s=1}^{t}\mathfrak{q}_s^{u_s}\cdot\prod_{v=1}^{w}\mathfrak{q}_v'^{\,z_i}\cdot\prod_{j=m+1}^{n}\mathfrak{p}_j^{k_j}\cdot\prod_{s=1}^{t}\mathfrak{q}_s^{-u_s}\\ &= \prod_{i=1}^{n}\mathfrak{p}_j^{k_j}\prod_{v=1}^{w}\mathfrak{q}_v'^{\,z_i}\end{aligned}$$

Wir können also ablesen, dass $\frac{x}{y}$ die gewünschten Bedingungen erfüllt. □

In einem Dedekindring R können die Bewertungen $\nu_\mathfrak{p}$ über die eindeutige Primfaktorzerlegung zu Abbildungen $\nu_\mathfrak{p} : \mathbb{I}_R \to \mathbb{Z}$ ausgeweitet werden.

Definition 5.2
Für $I \in \mathbb{I}_R$, $I = \prod_{0\neq\mathfrak{p}\in\mathrm{Spec}(R)} \mathfrak{p}^{n_\mathfrak{p}}$ definiere $\nu_\mathfrak{p}(I) := n_\mathfrak{p}$.

Bemerkung
Es ist unmittelbar klar, dass für ein $0 \neq x \in \mathrm{Quot}(R)$ stets $\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}((x))$ gilt und auch, dass $\nu_\mathfrak{p}(I \cdot J) = \nu_\mathfrak{p}(I) + \nu_\mathfrak{p}(J)$ für alle $I, J \in \mathbb{I}_R$.

Lemma 5.3
Seien I, J ganze Ideale in einem Dedekindring R. I und J sind genau dann koprim, wenn $\nu_\mathfrak{p}(I) \cdot \nu_\mathfrak{p}(J) = 0$ für alle Primideale $0 \neq \mathfrak{p} \subseteq R$.

Beweis
„ $\Leftarrow$ “: Die Gleichung $\nu_\mathfrak{p}(I)\cdot\nu_\mathfrak{p}(J) = 0$ ist äquivalent dazu, dass kein Primideal in der Zerlegung beider Ideale vorkommt. Wäre die Summe $I + J$ nicht der gesamte Ring R, müsste sie in einem maximalen Ideal $\mathfrak{m}$ enthalten sein. Damit wären auch beide Ideale, als Teilmengen von $I + J$, jeweils in $\mathfrak{m}$ enthalten und die Bemerkung im Anschluss an Satz 2.9 aus dem ersten Teil würde uns einen Widerspruch dazu geben, dass die beiden Ideale keinen gemeinsamen Faktor in ihrer Zerlegung besitzen.
„ $\Rightarrow$ “ Wenn I und J koprim sind und ein $\mathfrak{p} \in \mathrm{Spec}(R)$ mit $n := \nu_\mathfrak{p}(I) \cdot \nu_\mathfrak{p}(J) \neq 0$ existiert, so gilt $n > 0$, da I und J ganze Ideale sind (Satz 3.1 aus Teil I). Damit würde $\mathfrak{p}$ in den Zerlegungen beider Ideale vorkommen und damit $R = I + J \subseteq \mathfrak{p}$ im Widerspruch dazu, dass $\mathfrak{p}$ prim ist. □

Lemma 5.4
Sei R ein Dedekindring und I, J von Null verschiedene, gebrochene Ideale. Es existieren $x, y \in \mathrm{Quot}(R)$ sodass xI und yJ ganz und koprim sind.

Beweis
Per Definition existieren $x', y' \in R \setminus \{0\}$, die $x'I \subseteq R$, $y'J \subseteq R$ erfüllen. Daher können wir annehmen, dass I und J ganz sind. Wir schreiben $I = \prod_{i=1}^{n} \mathfrak{p}_i^{n_i}$ und $J = \prod_{i=1}^{n} \mathfrak{p}_i^{m_i}$ mit $n_i, m_i \geq 0$. Nach Lemma 5.1 können wir ein $a \in \mathrm{Quot}(R)$ wählen, mit $\nu_{\mathfrak{p}_i}(a) = n_i$ und $\nu_\mathfrak{q}(a) \geq 0$ für alle Primideale $\mathfrak{q} \neq \mathfrak{p}_i$, $i = 1, \ldots, n$. In der Primfaktorzerlegung von aI^{-1} kommt wegen

$$\nu_{\mathfrak{p}_i}(aI^{-1}) = \nu_{\mathfrak{p}_i}((a)\cdot I^{-1}) = \nu_{\mathfrak{p}_i}(a) - \nu_{\mathfrak{p}_i}(I) = 0$$

nach der Bemerkung im Anschluss an Definition 5.2 also keines der $\mathfrak{p}_i$ vor. Wähle ein Element $b' \in \bigcap_{i=1}^{n}(\mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1})$ beliebig und definiere $b := \frac{a}{b'} \in aI^{-1}$. Es gilt dann für $i = 1, \ldots, n$ $\nu_{\mathfrak{p}_i}(b) = \nu_{\mathfrak{p}_i}(\frac{a}{b'}) = n_i - n_i = 0$. Außerdem gilt $\nu_{\mathfrak{p}_i}(\frac{b}{a}) = -n_i$, womit $\nu_{\mathfrak{p}_i}(\frac{b}{a}I) = 0$ gilt für $i = 1, \ldots, n$. Wegen $\frac{b}{a}I = \frac{1}{a}bI \subseteq \frac{1}{a}aI^{-1}I = R$, ist $\frac{b}{a}I$ ein ganzes Ideal welches $\nu_{\mathfrak{p}}(\frac{b}{a}I)\cdot\nu_{\mathfrak{p}}(J) = 0$ für alle $\mathfrak{p} \in \mathrm{Spec}(R)$ erfüllt. Lemma 5.3 liefert uns nun die Behauptung, indem wir bI und aJ betrachten. □

Lemma 5.5
Sei R ein Dedekindring und seien $I_1, \ldots, I_n$ gebrochene Ideale. Dann sind die R-Moduln $I_1 \oplus \ldots \oplus I_n$ und $R^{n-1} \oplus (I_1 \cdot \ldots \cdot I_n)$ isomorph.

Beweis
Wir zeigen, dass $I \oplus J \cong R \oplus IJ$ gilt, und die Aussage folgt dann induktiv.
Zunächst wollen wir einen speziellen Fall betrachten. Wir nehmen an, I und J seien jeweils ganze, koprime Ideale. Betrachte folgende Abbildungen:

$$\rho : I \bigcap J \longrightarrow I \oplus J,\ i \mapsto (i, -i) \text{ und } \theta : I \oplus J \longrightarrow I + J,\ (i, j) \mapsto i + j.$$

Diese liefern uns eine exakte Sequenz:

$$0 \longrightarrow I \bigcap J \xrightarrow{\rho} I \oplus J \xrightarrow{\theta} I + J \longrightarrow 0$$

Da I, J koprim sind gilt $I \bigcap J = IJ$ und $I + J = R$. $I + J = R$ ist frei über R also auch flach und auch projektiv (vgl. Lemma 1.7). Lemma 1.5 sagt uns dann, dass $I \oplus J \cong R \oplus IJ$, was den speziellen Fall zeigt.
Da wir nach Lemma 5.4 bereits wissen, dass wir zu beliebigen gebrochenen Idealen I und J ganze Ideale $xI \cong I$ und $yJ \cong J$ finden, die den speziellen Fall erfüllen, erhalten wir den allgemeinen Fall durch

$$I \oplus J \cong xI \oplus yJ \cong R \oplus (xI) \cdot (yJ) = R \oplus xy(IJ) \cong R \oplus IJ.$$

□

Lemma 5.6
Sei R ein Dedekindring und seien I, J gebrochene Ideale. Die R-Moduln $R^{n-1} \oplus I$ und $R^{m-1} \oplus J$ sind isomorph genau dann, wenn $n = m$ und $\bar{I} = \bar{J} \in \mathbb{C}_R$ gilt.

Beweis
„ $\Leftarrow$ “ folgt aus Lemma 4.4.
„ $\Rightarrow$ “ Der R-lineare Isomorphismus $R^{n-1} \oplus I \cong R^{m-1} \oplus J$ induziert einen K-linearen Isomorphismus $(R^{n-1} \oplus I) \otimes_R K \cong (R^{m-1} \oplus J) \otimes_R K$. Hierbei gilt nach Lemma 4.2

$$(R^{n-1} \oplus I) \underset{R}{\otimes} K \cong (R^{n-1} \underset{R}{\otimes} K) \oplus (I \underset{R}{\otimes} K) \cong K^{n-1} \oplus K = K^n$$

und analog $(R^{m-1} \oplus J) \otimes_R K \cong K^m$. Es folgt $n = m$.
Nun sei Q die Abbildungsmatrix bezüglich der Standardbasis des obigen K-linearen Isomorphismus $K^n \to K^m = K^n$. Per Konstruktion schränkt er sich zu einem R-linearen Isomorphismus $R^{n-1} \oplus I \to R^{m-1} \oplus J = R^{n-1} \oplus J$ ein. Ist daher $a \in I$, so gilt

$$Q \cdot \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{pmatrix} \in (R^{n-1} \oplus J)^n$$

und daher $\det(Q) \cdot a \in J$, da J ein R-Modul ist. Da a beliebig war, folgt $\det(Q) \cdot I \subseteq J$. Ist umgekehrt $b \in J$, so existitert $A \in (R^{n-1} \oplus J)^n$ mit

$$Q \cdot A = \begin{pmatrix} 1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & 1 & \\ & & & & b \end{pmatrix}.$$

Es folgt $b = \det(Q) \cdot \det(A)$ mit $\det(A) \in I$, da I ein R-Modul ist. Das zeigt $\det(Q) \cdot I = J$ in K und damit $\bar{I} = \bar{J} \in \mathbb{C}_R$.

□

Nun können wir die Struktur eines jeden endlich erzeugten, projektiven Moduls über einem Dedekindring angeben.

Satz 5.7
Sei R ein Dedekindring mit Quotientenkörper K und sei P ein endlich erzeugter, projektiver Modul vom Rang $n > 0$. Dann ist $P \cong R^{n-1} \oplus I$ mit I, einem gebrochenen Ideal I von R, dessen Idealklasse durch P eindeutig bestimmt ist. Ferner gilt $n = \mathrm{rg}_R(P)$.

Beweis
Wir zeigen durch vollständige Induktion, dass wir P als direkte Summe von n gebrochenen Idealen schreiben können. Lemma 5.5 und Lemma 5.6 zeigen dann die Behauptung.
Sei für den Induktionsanfang $n = 1$. Wir wissen aus Lemma 1.7 dass P flach ist. Mit der Beziehung $P \cong P \otimes_R R \subseteq P \otimes_R K \cong K$, können wir P also als R-Untermodul von K auffassen. P ist per Annahme endlich erzeugt, also existiert $c \in R \setminus \{0\}$, ein gemeinsamer Nenner aller R-Erzeuger von P, mit $cP \subseteq R$.
Sei nun P vom Rang n. Betrachte $p_1, \ldots, p_r$, ein Erzeugendensystem von P über R. Dann ist $(p_i \otimes 1)_{i \in \{1 \ldots r\}}$ ein Erzeugendensystem des K-Vektorraums $P \otimes_R K$. Mit der Gleichung $\dim_K(P \otimes_R K) = \mathrm{rg}_R(P) = n$ können wir nach eventueller Umnummerierung annehmen, dass $(p_i \otimes 1)_{i \in \{1 \ldots n\}}$ eine K-Basis von $P \otimes_R K$ ist. Setze $P' := \mathrm{span}_R\{p_1, \ldots p_{n-1}\}$. Dann ist P' ein freier R-Untermodul von P vom Rang $n-1$ und

$$0 \longrightarrow P' \xrightarrow{\iota} P \xrightarrow{\pi} P/P' \longrightarrow 0 \tag{1}$$

ist eine exakte Sequenz (mit ι, der Inklusion und π, der Restklassenabbildung).
Für beliebige multiplikative Mengen $S \subseteq R$ ist $S^{-1}R(\bullet)$ nach **[AK]** Theorem 12.13 ein exakter Funktor. Da zudem nach **[AK]** Corollary 12.10 auch $M \otimes_R S^{-1}R \cong S^{-1}M$ gilt, ist die Sequenz:

$$0 \longrightarrow P' \otimes_R K \xrightarrow{\iota \otimes \mathrm{id}_K} P \otimes_R K \xrightarrow{\pi \otimes \mathrm{id}_K} (P/P') \otimes_R K \longrightarrow 0 \tag{2}$$

ebenfalls exakt ($K = S^{-1}R$ mit $S = R \setminus \{0\}$), d.h. es gilt $(P/P') \otimes_R K \cong (P \otimes_R K)/(P' \otimes_R K)$ und daher $\mathrm{rg}_R(P/P') = 1$. Da $p_n \otimes 1$ nicht in $P' \otimes_R K$ liegt, ist der R-Modul P/P' torsionsfrei und damit projektiv nach Satz 3.4. Nach dem Induktionsanfang ist P/P' isomorph zu einem gebrochenen Ideal I. Die Sequenz (1) zerfällt also nach Lemma 1.5 und wir haben nach Lemma 1.3 $P \cong P' \oplus P/P' \cong R^{n-1} \oplus I$.
Die Eindeutigkeitsaussage folgt aus Lemma 5.6. □

Liteartur

[**AK**] - Allen Altman, Steven Kleiman: A Term Of Commutative Algebra, Worldwide Center of Mathematics, 2013

[**AM**] - Michael Francis Atiyah, Ian Grant MacDonald: Introduction to Commutative Algebra, Adison-Wesley Publishing Company, 1969

[**BoA**] - Siegfried Bosch : Algebra, Springer Verlag, 2013

[**BoG**] - Siegfried Bosch : Algebraic Geometry And Commutative Algebra, Springer Verlag, 2013

[**LM**] - Jörg Liesen, Volker Mehrmann: Lineare Algebra, Springer Fachmedien Wiesbaden, 2015

[**MK**] -Michelis Kosters: Projective Modules Over Dedekind Domains, https://www.math.leidenuniv.nl/~edix/tag_2009/michiel_3.pdf