universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Noethersche und Dedekindsche Ringe

Verfasserin

Simone Lechner BSc.

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag. rer. nat.)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 190 406 884
Studienrichtung lt. Studienblatt:	Lehramtsstudium UF Mathematik, UF Informatik und Informatikmanagement
Betreuer:	Ao. Univ.-Prof. Dr. Gerhard Kowol

Inhaltsverzeichnis

Kapitel 1

Einleitung

Im Buch IX der "Elemente" beweist Euklid den folgenden Satz ([Thaer]):

IX,14: Die kleinste Zahl, die von gewissen Primzahlen gemessen wird, läßt sich durch keine andere Primzahl messen außer den ursprünglich messenden.

In moderner Form besagt das, dass quadratfreie natürliche Zahlen eine eindeutige Primfaktorzerlegung besitzen. Dabei beweist Euklid bereits in Buch VII, Sätze 29 und 32, dass so eine Zerlegung überhaupt existiert. Auch wenn dies in den "Elementen" nicht ausdrücklich hervorgehoben wird, so war Euklid sicher auch der allgemeine Fall bekannt, wonach jede natürliche Zahl eine (bis auf die Reihenfolge) eindeutige Primfaktorzerlegung besitzt.

Diese Aussage lässt sich unmittelbar auf $\mathbb{Z}$ übertragen:

Jede ganze Zahl $n \neq 0, \pm 1$ *lässt sich eindeutig bis auf die Reihenfolge als Produkt* $n = \pm p_1^{k_1} ... p_r^{k_r}$ *schreiben, wobei die* $p_i,\ i = 1, ..., r$, *Primzahlen in* $\mathbb{N}$ *sind.*

Bei gewissen zahlentheoretischen Untersuchungen wurde C. F. Gauß um 1820 auf die Frage geführt, ob auch in anderen Zahlbereichen eine solche Zerlegung möglich sei. Er konnte zeigen, dass in $\mathbb{Z}[i] = \{a+bi |\ a, b \in \mathbb{Z}\}$ und in $\mathbb{Z}[\zeta] = \{a+b\zeta |\ a, b \in \mathbb{Z}\},\ \zeta = \frac{-1+\sqrt{-3}}{2}$ eine dritte Einheitswurzel, sich jede Zahl, die verschieden von 0 und keine Einheit ist, eindeutig bis auf die Reihenfolge als Produkt von Primfaktoren darstellen lässt ([KM82], S. 31). Dabei wird der Begriff der Primzahl etwas erweitert. Ich werde die genaue Definition, ebenso wie die der Einheit im nächsten Kapitel "Grundlagen" bringen. Wendet man diesen erweiterten Primzahlbegriff auf $\mathbb{Z}$ an, so gilt dasselbe Resultat auch für $\mathbb{Z}$ wie für die genannten beiden Bereiche.

Bald danach wurden beim Versuch der Lösung des sogenannten großen Fermatschen Problems (auch als Fermatsche Vermutung bezeichnet) weitere Zahlbereiche dieser Art wichtig. Dieses Problem besagt, dass es für $n \geq 3$ keine nicht verschwindenden, zueinan-

der relativ primen ganzen Zahlen x, y, z gibt mit $x^n + y^n = z^n$. E. Lamé präsentierte 1847 einen Beweis des großen Fermatschen Problems, doch machte ihn J. Liouville darauf aufmerksam, dass er dabei die eindeutige Faktorzerlegung in den auftretenden Zahlbereichen voraussetzte, was nicht bewiesen sei. Auch E. E. Kummer ist bei seinem 1844 eingereichten Beweis des großen Fermatschen Problems demselben Irrtum unterlegen. Hier war es L. Dirichlet, der auf dieselbe Problematik hinwies. (Mündliche Mitteilung von Prof. Kowol.)

Schon bald zeigte sich, dass in allgemeineren Zahlbereichen die eindeutige Faktorzerlegung wirklich nicht gegeben ist. Beispielsweise gibt es in

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\}$$

die beiden wesentlich verschiedenen Zerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in nicht mehr weiter zerlegbare Elemente. Durch Einführung sogenannter idealer Primzahlen konnte Kummer den Sachverhalt klären und zumindest einen Teil seines Beweises retten. Wir werden darauf im letzten Kapitel "Spezialfälle" eingehen.

Während eine ideale Primzahl dem betrachteten Zahlbereich nicht angehört, ersetzte Dedekind sie durch die Menge aller derjenigen Elemente des Zahlbereiches, die durch jene Zahl teilbar sind. Damit war der Begriff des Primideals und allgemein des Ideals geboren. Die Idealtheorie erwies sich als wesentliches Mittel bei der Untersuchung der Struktur von kommutativen Ringen. Speziell für die Zahlbereiche R gilt in Abschwächung der eindeutigen Faktorzerlegung, dass jedes Ideal $\neq (0), R$ sich eindeutig bis auf die Reihenfolge als Produkt von Primidealen schreiben lässt. Im obigen Fall lautet die entsprechende Zerlegung für das Hauptideal (6):

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Dies wird in Kapitel 5 "Zahlbereiche" gezeigt.

Zwar wurden die weiteren Lösungsversuche des großen Fermatschen Problems mit neuen Hilfsmitteln in Angriff genommen, doch entwickelte sich die Idealtheorie in Hinblick auf die Produktdarstellung weiter. Was das Fermatsche Problem betrifft, so wurde die Lösung, also die Richtigkeit der Aussage, erst 1996 durch A. Wiles gefunden, wobei tiefliegende Theorien aus der algebraischen Geometrie zur Anwendung kamen.

Schon beim Polynombereich $\mathbb{Z}[x]$ zeigt sich, dass das eben für Zahlbereiche genannte Resultat nicht allgemein gilt. So lässt sich etwa das Ideal $(4, x)$ nicht als Produkt von

Primidealen darstellen. A. Walfisz hat für diesen Bereich gezeigt, dass sich jedes Ideal $\neq (0), \mathbb{Z}[x]$ als Durchschnitt von endlich vielen sogenannten Primäridealen darstellen lässt und zwar im wesentlichen eindeutig (nach [VdW67], S. 132). Die allgemeine Theorie schließlich geht auf die Mathematikerin Emmy Noether zurück. Sie bewies, dass in kommutativen Ringen mit Einselement, die die aufsteigende Kettenbedingung für Ideale erfüllen, stets ein derartiges Theorem gültig ist. Solche Ringe werden heute Noethersche Ringe genannt.

In meiner Arbeit bringe ich zunächst ein Kapitel 2 „Grundlagen“, in welchem die notwendigen Begriffe und vorausgesetzten Sätze zusammengestellt sind. Ein Großteil davon wird beweislos referiert, soweit er in der Lehrveranstaltung “Algebra” (Bachelor) durchgenommen wurde. Dann folgt das Kapitel 3 über Noethersche Ringe, wobei der grundlegende Hilbertsche Basissatz auf zwei Arten bewiesen wird. Sodann werden zwei Darstellungssätze für Ideale mittels Primäridealen hergeleitet und danach die Frage der Eindeutigkeit behandelt.

Im nächsten Kapitel 4 behandle ich die allgemeine Theorie der Dedekindschen Ringe. Definitionsgemäß sind das Noethersche Integritätsringe R, in denen jedes Ideal $\neq (0), R$ Produkt einer endlichen Anzahl von Primidealen ist. Hierfür gibt es sehr viele äquivalente Charakterisierungen, von denen ich fünf bringe und die Äquivalenz beweise. Diese Ringe sind insofern bedeutsam als wichtige Zahlbereiche darunter fallen. Die genaue Definition für sie und die allgemeine Beschreibung von ihren Elementen bringe ich in Kapitel 5. Ausführlicher gehe ich dann auf die speziellen Bereiche $\mathbb{Z}[\sqrt{d}]$ mit $d \in \mathbb{Z}$, d quadratfrei, ein.

Kapitel 2

Grundlagen

In diesem Kapitel stelle ich die für die weitere Arbeit wichtigen Grundbegriffe und Sätze zusammen, die mir zum Großteil aus der Vorlesung "Algebra" (Bachelorstudium) bekannt sind. Ergebnisse, die mir daraus nicht bekannt sind, beweise ich oder gebe eine Stelle an, wo ein Beweis zu finden ist.

Nachdem ich in meiner Arbeit mehrmals auf das Zornsche Lemma verweisen werde, sei dieses vorab hier ohne Beweis angeführt:

Lemma 2.0.1 (Zornsches Lemma)**.** *Sei $\mathscr{M}$ eine partiell geordnete Menge, in der jede Kette eine obere Schranke in $\mathscr{M}$ besitzt. Die Menge $\mathscr{M}$ enthält dann ein maximales Element.*

Grundsätzliches. Die im Folgenden betrachteten Ringe sind stets als *kommutativ* vorausgesetzt. Des Weiteren bezeichen die Symbole $\subset$ bzw. $\supset$ stets die *echte Inklusion.* Schließlich werden Polynome mit $p(x)$ statt nur mit p bezeichnet werden, um die Variable genau zu kennzeichnen.

Definition 2.0.2. *Sei R ein kommutativer Ring. Eine Teilmenge $I \subseteq R, I \neq \emptyset$, heißt Ideal, falls (i) mit $a, b \in I$ stets auch $a - b \in I$ und (ii) mit $a \in I,\ x \in R$ stets $ax \in I$.*

Die Ideale $0 := \{0\}$ und R heißen triviale Ideale, alle anderen echte Ideale.

Für zwei Ideale $I,\ J$ von R mit $I \subseteq J$ nennen wir J einen Teiler von I.

Da der Durchschnitt von Idealen wieder ein Ideal ist, ist folgende Definition sinnvoll:

Definition 2.0.3. *Sei R ein kommutativer Ring und $M \subseteq R$. Dann heißt*

$$(M) = \bigcap \{I | I \text{ Ideal von } R, M \subseteq I\}$$

das von M erzeugte Ideal. Wie üblich schreiben wir bei endlichen Mengen $M = \{a_1, ..., a_n\}$ statt $(\{a_1, ..., a_n\})$ kurz $(a_1, ..., a_n)$. Ein Ideal der Gestalt $I = (a)$ heißt Hauptideal.

Lemma 2.0.4. *Sei R ein kommutativer Ring und $M \subseteq R$. Dann gilt*

$$(M) = \{\sum_{endl.} (x_i a_i + n_i b_i) | a_i, b_i \in M, x_i \in R, n_i \in \mathbb{Z}\}.$$

Besitzt R ein Einselement e, so gilt speziell

$$(M) = \{\sum_{endl.} (x_i a_i) | a_i \in M, x_i \in R\}.$$

Der Beweis findet sich in [KM82], Korollar (S.87).

Für Ideale $I, J \subseteq R$ lassen sich zwei Operationen definieren

$$I + J := \{i + j | i \in I, j \in J\} = (I \cup J),$$

$$IJ := \{\sum_{endl.} i_k j_k | i_k \in I, j_k \in J\} = (\{ij | i \in I, j \in J\}).$$

$I + J$ und IJ sind wieder Ideale. Für $I = (a_1, ..., a_n), J = (b_1, ..., b_m)$ folgt insbesondere

$$IJ = (\{a_i b_j | i = 1, ..., n; j = 1, ..., m\}).$$

Speziell ist das Produkt zweier Hauptideale stets wieder ein Hauptideal. Allgemein gilt $IJ \subseteq I \cap J$.

Satz 2.0.5. *Ist I ein Ideal eines kommutativen Ringes R, dann ist die Menge $R/I = \{a+I |\ a \in R\}$, $a+I = \{a+i |\ i \in I\}$, und der Äquivalenzrelation $a+I \sim b+I \Leftrightarrow a-b \in I$ mit den wohldefinierten Operationen*

$$(a + I) + (b + I) = (a + b) + I \quad und \quad (a + I)(b + I) = ab + I$$

wieder ein kommutativer Ring, der Faktorring (Quotientenring) von R nach I.

Für $x \in a + I$ schreiben wir auch oft $x \equiv a(I)$.

Definition 2.0.6. *Seien R, S kommutative Ringe. Eine Abbildung $\varphi : R \to S$, die*

$$(i)\ \varphi(a + b) = \varphi(a) + \varphi(b); \quad (ii)\ \varphi(ab) = \varphi(a)\varphi(b)$$

erfüllt, heißt (Ring-)Homomorphismus. Ist φ bijektiv, so heißt φ Isomorphismus ($\cong$).

Diesbezüglich gelten die folgenden Sätze:

Satz 2.0.7 (Homomorphiesatz)**.** *Seien R, S kommutative Ringe.*

(i) Ist $\varphi : R \to S$ ein Homomorphismus, so gilt $\varphi(R)$ ist Unterring von S, $ker\varphi = \{r \in R | \varphi(r) = 0_S\}$ ist ein Ideal in R und $R/ker\varphi \cong \varphi(R)$.

(ii) Ist I ein Ideal von R, so ist R/I surjektives homomorphes Bild von R unter dem natürlichen Homomorphismus $\nu : R \to R/I$ gegeben durch $\nu(a) = a + I, a \in R$.

Satz 2.0.8 (2. Homomorphiesatz)**.** *Es sei I ein Ideal eines (kommutativen) Ringes R und $\mathscr{I} = \{J \supseteq I | J \text{ Ideal von } R\}$. Dann ist die Abbildung $\varphi : \mathscr{I} \to R/I$ gegeben durch $\varphi(J) = J/I$ bijektiv. Daher hat jedes Ideal von R/I die Gestalt J/I mit $J \in \mathscr{I}$ und es gilt $(R/I)/(J/I) \cong R/J$.*

Einen *Beweis* findet man in [Hun74], Theorem III.2.12 (S. 126).

Definition 2.0.9. *Sei I Ideal eines kommutativen Ringes R.*

(i) I heißt Primideal, wenn aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

(ii) I heißt maximales Ideal, wenn aus $I \subset J$, J Ideal von R, folgt $J = R$.

(iii) I heißt irreduzibel, falls I keine Darstellung der Gestalt $I = J_1 \cap J_2$ mit Idealen $J_1, J_2 \supset I$ erlaubt.

Es gilt

Lemma 2.0.10. *Es sei R ein kommutativer Ring.*

(i) I ist Primideal von R genau dann, wenn R/I ein Integritätsring ist.

(ii) Besitzt R ein Einselement, so ist I maximales Ideal von R genau dann, wenn R/I ein Körper ist.

(iii) Jedes Primideal ist irreduzibel.

Beweis. (iii) Indirekt angenommen, das Primideal I gestatte die Darstellung $I = J_1 \cap J_2$ mit Idealen $J_1, J_2 \supset I$. Seien $a_i \in J_i \backslash I,\ i = 1, 2$. Dann folgt $a_1 a_2 \in J_1 \cap J_2 = I$, ein Widerspruch zur Primidealeigenschaft von I. □

Bemerkung. Es gelten somit für Ideale die Implikationen

$$\text{maximal} \Rightarrow \text{prim} \Rightarrow \text{irreduzibel}$$

Satz 2.0.11. *Seien R ein kommutativer Ring und A, B, C Ideale von R. Ist C Primideal und gilt $C \supseteq AB$, so ist $C \supseteq A$ oder $C \supseteq B$.*

Beweis siehe [Spi94], (6.3.) Proposition (S.94)
Ist R ein Integritätsring, so wird die Teilbarkeit wie üblich definiert.

Definition 2.0.12. *Es sei R ein Integritätsring mit Einselement e.*

(i) Die Teiler von e heißen Einheiten.

(ii) $p \in R,\ p \neq 0$ *und keine Einheit, heißt prim, wenn aus* $p|ab$ $(a, b \in R)$ *stets folgt* $a|p$ *oder* $b|p$*.*

(iii) $q \in R,\ q \neq 0$ *und keine Einheit, heißt unzerlegbar oder irreduzibel, wenn aus* $q = ab$ $(a, b \in R)$ *stets folgt* a *oder* b *ist Einheit.*

(iv) Ist R *kommutativer Ring, so heißt* $a \in R$ *nilpotent, falls es ein* $n \in \mathbb{N}$ *gibt mit* $a^n = 0$*.*

Es gilt, dass jedes prime Element auch irreduzibel ist. In Hauptidealringen gilt auch die Umkehrung, daher sind dort genau die irreduziblen Element auch die primen.

Schließlich benötigen wir noch folgenden

Satz 2.0.13 (Lemma von Gauß)**.** *Ein Polynom* $p \in \mathbb{Z}[x]$ *dessen Koeffizienten relativ prim sind, ist genau dann über* $\mathbb{Q}$ *reduzibel, wenn es über* $\mathbb{Z}$ *reduzibel ist.*

Einen *Beweis* findet man in [KM82], Satz 7.5 (S. 127).

Kapitel 3

Noethersche Ringe

Emmy Noether studierte die Teilbarkeitseigenschaften von Idealen in kommutativen Ringen. Diese stellen eine Verallgemeinerung der entsprechenden Eigenschaften des Ringes der ganzen Zahlen $\mathbb{Z}$ dar. Ausgehend von der faktoriellen Eigenschaft in $\mathbb{Z}$ lässt sie sich folgendermaßen motivieren:

Da sich in $\mathbb{Z}$ jedes Element x, $x \neq 0$, $x \neq \pm 1$, eindeutig als Produkt von irreduziblen Elementen darstellen lässt, gibt es zwei Möglichkeiten: x ist irreduzibel oder x besitzt einen echten Teiler x_1. Wir verfahren so weiter, bis wir schließlich zu einem irreduziblen Element x_n gelangen, da stets $1 < |x_{i+1}| < |x_i|$, $i = 1, \ldots, n-1$ gilt. Diese Kette von Teilern

$$x_1|x,\ x_2|x_1,\ \ldots, x_{n-2}|x_{n-1},\ x_{n-1}|x_n$$

bricht nach endlich vielen Schritten ab. Drückt man diese Teilerkette mittels der zugehörigen Hauptideale aus, so ergibt sich

$$(x) \subset (x_1) \subset (x_2) \subset \ldots \subset (x_{n-2}) \subset (x_{n-1}) \subset (x_n).$$

Insbesondere bricht jede solche Kette nach endlich vielen Schritten ab.

3.1 Kettenbedingung

In diesem Abschnitt untersuchen wir kommutative Ringe, die eben diese spezielle Kettenbedingung erfüllen. Wir überlegen uns welche Eigenschaften aus dieser Bedingung folgen und bringen typische Beispiele. Sofern es nicht anders erwähnt wird, sind die betrachteten Ringe stets kommutativ und haben ein Einselement, das wir mit e bezeichnen.

Definition 3.1.1. *Sei R ein kommutativer Ring. Man sagt R genügt der aufsteigenden*

Kettenbedingung für Ideale, wenn jede aufsteigende Kette von Idealen

$$I_1 \subset I_2 \subset \ldots I_n \subset \ldots,\ I_i \neq I_j \text{ für } i \neq j,\ I_j \text{ Ideal von } R,\quad i,j \in \mathbb{N}$$

nach endlich vielen Schritten abbricht.

Ein kommutativer Ring, der die aufsteigende Kettenbedingung erfüllt, heißt Noethersch.

Bemerkungen.

1. Oft wird die Definition auch so formuliert, dass jede aufsteigende Kette von Idealen in der Form

$$I_1 \subseteq I_2 \subseteq \ldots I_n \subseteq \ldots,\ I_i \neq I_j \text{ für } i \neq j,\ I_j \text{ Ideal von } R,\quad i,j \in \mathbb{N}$$

ab einem gewissen Index stationär wird, das heißt alle Glieder der Idealkette ab diesem Index gleich sein müssen. Offenbar sind die beiden Fassungen äquivalent. Wir verwenden je nach Bedarf die passende davon.

2. Ein kommutativer Ring, in dem jede absteigende Kette von Idealen abbricht, heißt *Artinsch* (nach Emil Artin, einem Schüler von Emmy Noether). Dass diese Bedingung im Allgemeinen stärker ist als die aufsteigende Kettenbedingung zeigen die folgenden beiden Resultate.

Satz 3.1.2. *Ein Artinscher Integritätsring R mit Einselement ist ein Körper.*

Beweis. Sei $a \in R,\ a \neq 0$. Aufgrund der absteigenden Kettenbedingung gibt es ein $n \in \mathbb{N}$ mit $(a^n) = (a^{n+1})$. Somit lässt sich a^n darstellen als $a^n = a^{n+1}c$ mit einem geeigneten $c \in R$. Es folgt $a^n(ac - e) = 0$. Da der erste Faktor nicht verschwindet, muss $ac - e = 0$, also $ac = e$ gelten. a besitzt somit ein Inverses, d.h. R ist Körper. □

Satz 3.1.3. *(Satz von Hopkins–Levitzky) Jeder Artinsche Ring mit Einselement ist noethersch.*

Beweis. Zitiert nach [KM84], S. 91. Ein *Beweis* findet sich zum Beispiel in [Spi94], (11.28) Theorem (S. 214). □

Ein einfaches Beispiel einer aufsteigenden Idealkette, die notwendigerweise abbricht, ist

$$(2^n) \subset (2^{n-1}) \subset \ldots \subset (2^3) \subset (2^2) \subset (2) \subset (1)$$

im Ring $\mathbb{Z}$ der ganzen Zahlen. Diese Kette ist nicht mehr verfeinerbar und enthält sämtliche Ideale, die (2^n) umfassen.

$\mathbb{Z}$ erfüllt sogar die aufsteigende Kettenbedingung für Ideale: Da $\mathbb{Z}$ Hauptidealring ist, können wir von einem Ideal $(m),\ m \in \mathbb{N}_0$, ausgehen. Nun ist $(m) \subset (n)$ echt enthalten,

genau dann, wenn n ein echter Teiler von m ist. Da aber jedes Element aus $\mathbb{Z}$ nur endlich viele Teiler besitzt, folgt das Abbrechen jeder aufsteigenden Kette.

Bemerkung.

1. Dieses Beispiel zeigt auch, dass es Noethersche Integritätsringe mit Einselement gibt, die nicht Artinsch sind. $\mathbb{Z}$ ist ja kein Körper.

2. Jeder endliche kommutative Ring ist klarerweise Noethersch (und Artinsch) und damit sind es insbesondere die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ für beliebiges $n \in \mathbb{N}$. Ebenso ist jeder Körper Noethersch, da er nur die trivialen Ideale (0) und $(e) = K$ besitzt.

Um mit Noetherschen Ringen zu arbeiten, erweist sich folgende Charakterisierung als sehr nützlich:

Satz 3.1.4. *Sei R ein kommutativer Ring mit Einselement e. Dann sind äquivalent:*

1) R erfüllt die aufsteigende Kettenbedingung

2) Jede nichtleere Menge $\mathscr{S}$ von Idealen $\neq R$ besitzt ein maximales Element bzgl. $\subseteq$ (Maximalitätsbedingung).

3) Jedes Ideal von R ist endlich erzeugt.

Beweis.

1) $\Rightarrow$ 2) Sei $\mathscr{S} \neq \emptyset$ eine nichtleere Menge von Idealen und sei $I_1 \in \mathscr{S}$. Wenn I_1 maximal ist in $\mathscr{S}$, dann ist 2) bewiesen. Wenn nicht, dann gibt es ein echt größeres Ideal $I_2 \in \mathscr{S}$, $I_1 \subset I_2$. Wenn I_2 maximal ist, dann sind wir ebenfalls fertig. Andernfalls setzen wir dieses Verfahren fort und erhalten eine aufsteigende Kette von Idealen $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$, die nach Voraussetzung nach endlich vielen Schritten, etwa bei I_{n_0} abbricht. Dann ist nach Konstruktion I_{n_0} maximal in $\mathscr{S}$.

2) $\Rightarrow$ 3) Für $I = R$ ist die Aussage wegen $R = (e)$ klar. Sei also $I \neq R$ ein beliebiges Ideal und $\mathscr{S}$ die Menge von Idealen, die in I enthalten und endlich erzeugt sind. Wir zeigen, dass aus der Maximalitätsbedingung in $\mathscr{S}$ folgt, dass I auch endlich erzeugt sein muss.

$\mathscr{S}$ ist sicher nicht leer, da $(0) \in \mathscr{S}$. Nach Voraussetzung besitzt $\mathscr{S}$ ein maximales Element J. J sei endlich erzeugt von $\{a_1, \ldots a_n\}$. Nach Konstruktion gilt $J \subseteq I$. Wir zeigen $J = I$. Wäre nämlich $J \neq I$, also J echt enthalten in I, dann gäbe es ein $b \in I$ mit $b \notin J$ und es würde gelten $J \subset J + (b) \subseteq I$. Dann wäre aber $J + (b) = \{a_1, \ldots, a_n, b\}$ in $\mathscr{S}$, was im Widerspruch zur Maximalität von J in $\mathscr{S}$ steht. Somit muss also $I = J$ gelten.

3) $\Rightarrow$ 1) Sei $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ eine aufsteigende Kette von Idealen von R. Wir zeigen, dass diese nach endlich vielen Schritten abbricht, wenn jedes Ideal endlich erzeugt ist. Dazu betrachten wir $\bigcup_{j\geq 1} I_j := I$.

I ist ein Ideal in R, das nach Voraussetzung endlich erzeugt ist. Sei $\{a_1, \ldots, a_n\}$ ein Erzeugendensystem. Wegen $a_k \in \bigcup_{j\geq 1} I_j$ existieren Indizes j_k mit $a_k \in I_{j_k}$ für $1 \leq k \leq n$. Sei j_0 ein solcher Index, sodass alle I_{j_k} im Ideal I_{j_0} enthalten sind: $I_{j_k} \subseteq I_{j_0}$ für $k = 1, \ldots n$. Es folgt $I = (a_1, \ldots, a_n) \subseteq I_{j_0}$; andererseits gilt $I_{j_0} \subseteq \bigcup_{j\geq 1} I_j$. Zusammen also $\bigcup_{j\geq 1} I_j = I_{j_0}$. Die Kette von Idealen muss daher spätestens bei I_{j_0} stationär werden. $\square$

Da in einem Hauptidealring per definitionem jedes Ideal sogar von nur einem Element erzeugt wird, folgt aus dem obigen Satz unmittelbar:

Korollar 3.1.5. *Jeder Hauptidealring ist Noethersch.*

Mit dieser Folgerung haben wir also nochmals bestätigt, dass $\mathbb{Z}$ als klassisches Beispiel eines Hauptidealringes Noethersch ist.

Bemerkung. Die Umkehrung von Korollar 3.1.5 gilt nicht! Denn $\mathbb{Z}[x]$ ist Noethersch (siehe Hilbertscher Basissatz 3.1.9) aber kein Hauptidealring, da $(2, x)$ kein Hauptideal ist:

Angenommen $(2, x)$ ließe sich von nur einem Element, etwa $p(x) \in \mathbb{Z}[x]$, erzeugen, dann teilt $p(x)$ sowohl 2 als auch x. Wenn $p(x)$ Teiler von 2 ist, dann muss $p(x)$ ein konstantes Polynom sein, und zwar $p(x) = \pm 1$ oder $p(x) = \pm 2$. Da aber das von (± 1) erzeugte Ideal bereits $\mathbb{Z}[x]$ und ± 2 kein Teiler von x ist, kann es ein solches Polynom nicht geben.

Die Bedingung, dass jedes Ideal endlich erzeugt ist als notwendiges und hinreichendes Kriterium für Noethersche Ringe kann noch verschärft werden:

Satz 3.1.6. *Ein kommutativer Ring R mit Einselement e ist Noethersch genau dann, wenn jedes Primideal endlich erzeugt ist.*

Beweis.

($\Leftarrow$) Angenommen R ist nicht Noethersch, dann gibt es nach Satz 3.1.4 Ideale, die nicht endlich erzeugt sind. Sei $\mathscr{S}$ die Menge der Ideale, die nicht endlich erzeugt sind. Nach Voraussetzung gilt $\mathscr{S} \neq \emptyset$ und nach dem Zornschen Lemma besitzt jede nichtleere Menge ein maximales Element, in unserem Fall ein maximales Ideal P.

Wir zeigen, dass P ein Primideal ist. Dazu nehmen wir indirekt an es gilt $ab \in P$ und $a \notin P$ und $b \notin P$. Dann enthalten $P + (a)$ und $P + (b)$ sicher P echt. Da P maximal ist in der Menge $\mathscr{S}$ der nicht endlich erzeugten Ideale, müssen $P+(a)$ und $P+(b)$ endlich erzeugt

sein. Seien $(p_1 + r_1a, \ldots, p_n + r_na)$ und $(p'_1 + r'_1b, \ldots p'_m + r'_mb)$ die Erzeugendensysteme von $P + (a)$ und $P + (b)$ mit $p_i, p'_j \in P,\ r_i, r'_j \in R,\ i = 1, ..., n,\ j = 1, ..., m$.

Wir betrachten die Menge $J = \{r \in R | ra \in P\}$. Sie ist ein Ideal von R, denn für $r_1, r_2 \in J$ gilt $(r_1 - r_2)a = r_1a - r_2a \in P$, weil P ein Ideal ist und demnach $r_1 - r_2 \in J$; und für $x \in R,\ r \in J$ gilt $(xr)a = x(ra) \in P$ und folglich auch $xr \in J$.

Wegen $ba = ab \in P$ nach Annahme ist sicher $b \in J$. Andererseits ist auch $P \subseteq J$, da $za = az \in P\ \forall z \in P$. Zusammen folgt $(P, b) = P + (b) \subseteq J$. Wegen der Maximalität von P muss auch J endlich erzeugt sein. Sei $J = (j_1, \ldots, j_k)$.

Für jedes $x \in P$ folgt $x \in P + (a)$ und somit lässt sich x darstellen als

$$x = \sum_{i=1}^{n} s_i(p_i + r_ia) = \sum_{i=1}^{n} s_ip_i + (\sum_{i=1}^{n} s_ir_i)a$$

für geeignete $s_i \in R$. Mithin gilt $\sum_{i=1}^{n} (s_ir_i)a = x - \sum_{i=1}^{n} s_ip_i \in P$, also liegt $\sum_{i=1}^{n} (s_ir_i) \in J$. Daher gibt es $t_i \in R$ mit $\sum_{i=1}^{n} s_ir_i = \sum_{i=1}^{k} t_ij_i$ mit $j_i \in J,\ i = 1, ..., k$. x lässt sich somit darstellen als $x = \sum_{i=1}^{n} s_ip_i + (\sum_{i=1}^{k} t_ij_i)a$, also als Linearkombination von $p_1, \ldots, p_n, j_1a, \ldots, j_ka$. Wir haben für beliebiges $x \in P$ eine Darstellung mit endlich vielen festen Erzeugenden gefunden, was im Widerspruch zur Voraussetzung steht, dass P nicht endlich erzeugt ist. Somit muss aus $ab \in P$ folgen, dass $a \in P$ oder $b \in P$, d.h. P ist Primideal.

Wir halten fest, dass unter der Annahme $\mathscr{S} \neq \emptyset$ das maximale Ideal $P \in \mathscr{S}$ ein nicht endlich erzeugtes Primideal ist. Dies ist ein Widerspruch zur Voraussetzung. Somit muss $\mathscr{S} = \emptyset$ und damit jedes Ideal in R endlich erzeugt sein. R ist also Noethersch.

($\Rightarrow$) Die Umkehrung ist klar. □

Bevor wir uns mit Primidealen in Noetherschen Ringen befassen (Abschnitt 3.2), werden wir noch zeigen, dass Ringhomomorphismen die Kettenbedingung mitübertragen und daran anschließend den Hilbertschen Basissatz formulieren und beweisen.

Satz 3.1.7. *Jedes homomorphe Bild S eines Noetherschen Ringes R ist wieder Noethersch.*

Beweis. Sei $\Phi : R \to S$ der surjektive Homomorphismus. Nach dem Homomorphiesatz für Ringe gibt es ein Ideal I von R mit $R/I \cong \Phi(R) = S$. Es genügt somit zu seigen, dass R/I Noethersch ist. Sei dazu

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_i \subseteq J_{i+1} \subseteq \ldots$$

eine aufsteigende Kette von Idealen in R/I. Sei Φ der natürliche Homomorphismus von R auf R/I. Dann finden wir zu jedem Ideal J_i ein Ideal K_i mit $\Phi(K_i) = J_i$. Dabei gilt

$I \subseteq K_i$ und $K_i \subseteq K_{i+1}$ für alle $i = 1, 2, ...$ Insgesamt erhalten wir

$$I \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_i \subseteq K_{i+1} \subseteq \ldots,$$

also eine aufsteigende Kette von Idealen in R. Da R nach Voraussetzung Noethersch ist, muss diese abbrechen, was gleichbedeutend damit ist, dass ein Index N existiert, sodass $K_i = K_N \ \forall i \geq N$ gilt. Also muss auch $J_i = \Phi(K_i) = \Phi(K_N) = J_N$ für $i \geq N$ gelten. Damit ist gezeigt, dass jede beliebige aufsteigende Idealkette in R/I stationär wird. Damit ist R/I und also auch S Noethersch. □

3.1.1 Hilbertscher Basissatz

Sei R ein Noetherscher Ring mit Einselement. Im Folgenden werden wir zeigen, dass der Polynomring $R[x]$ im allgemeinen ebenfalls Noethersch ist. Dafür benötigen wir ein Konzept, mit dem wir Elemente von $R[x]$ mit Elementen von R assoziieren können:

Dazu sei I ein Ideal aus $R[x]$. Wir bezeichnen mit $K_n(I)$ die Menge aller führenden Koeffizienten von Polynomen n-ten Grades in I;

$$K_n(I) = \{a_n | a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in I\}.$$

Die Menge $K_n(I)$ erfüllt folgende Eigenschaften:

Lemma 3.1.8. *Sei R ein kommutativer Ring mit Einselement und seien I, J Ideale von $R[x]$. Dann gilt:*

1) $K_n(I)$ ist ein Ideal in R.

2) $K_n(I) \subseteq K_{n+1}(I)$ für alle $n \geq 0$.

3) Wenn $I \subseteq J$, dann gilt $K_n(I) \subseteq K_n(J)$ für alle $n \geq 0$.

4) Wenn $I \subseteq J$ und $K_n(I) = K_n(J)$ für alle $n \geq 0$ gilt, dann folgt $I = J$.

Beweis.

1) Seien $a_n, b_n \in K_n(I)$, dann gibt es Polynome $a_n x^n + \ldots a_1 x + a_0$ und $b_n x^n + \ldots b_1 x + b_0$ in I. Weil I ein Ideal in $R[x]$ ist, gilt $(a_n - b_n)x^n + \ldots + (a_1 - b_1)x + (a_0 - b_0) \in I$ und daher auch $a_n - b_n \in K_n(I)$. Sei weiters $r \in R$, dann liegt $r(a_n x^n + \ldots a_1 x + a_0)$ ebenfalls in I, woraus $r a_n \in K_n(I)$ folgt.

2) Sei $a_n \in K_n(I)$ und $a_n x^n + \ldots a_1 x + a_0$ ein Polynom in I. Da R ein Ring mit Einselement ist, liegt $x \in R[x]$ und damit ist ebenfalls $a_n x^{n+1} + \ldots a_1 x^2 + a_0 x \in I$. Also gilt $a_n \in K_{n+1}(I)$.

3) Falls $I \subseteq J$, so gilt für jedes Polynom in I, dass es auch in J liegt. Selbiges gilt für die führenden Koeffizienten dieser Polynome.

4) Angenommen es gilt $J \supset I$. Dann sei $f(x) = b_n x^n + \ldots b_1 x + b_0$ ein Polynom mit kleinstem Grad in $J \backslash I$. Wegen $b_n \in K_n(J)$ und $K_n(J) = K_n(I)$ nach Voraussetzung gibt es ein Polynom $g(x) = b_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$ in I. Da $J \supset I$ und J Ideal ist, muss $f(x) - g(x)$ in J liegen. Wenn $f(x) - g(x) = 0$ ist, dann war $f(x) \in I$, ein Widerspruch. Wäre $f(x) - g(x) \in I$, dann wäre auch $f(x) = (f(x) - g(x)) + g(x) \in I$, ein Widerspruch. Also liegt $f(x) - g(x) \in J \backslash I$, es hat aber einen echt kleineren Grad als $f(x)$; dies ist ebenfalls ein Widerspruch, und zwar zur Konstruktion von $f(x)$. □

Mit dem vorigen Lemma können wir nun beweisen, dass jeder Polynomring in endlich vielen Unbekannten über einen Noetherschen Ring mit Einselement ebenfalls Noethersch ist. Man beachte, dass die Eigenschaft 2) aus Lemma 3.1.8 nur unter der Voraussetzung bewiesen wurde, dass R ein Ring mit Einselement ist.

Satz 3.1.9. *(Hilbertscher Basissatz) Sei R ein kommutativer Ring mit Einselement. Wenn R Noethersch ist, dann ist auch $R[x]$ Noethersch.*

1. Beweis. Sei $I_1 \subseteq I_2 \subseteq \ldots$ eine aufsteigende Kette von Idealen in $R[x]$. Wir setzen

$$\mathscr{S} = \{K_n(I_m) |\ n \geq 0,\ m \geq 1\}.$$

Die Menge $\mathscr{S}$ ist eine nichtleere Menge von Idealen in R nach Lemma 3.1.8, 1). Da R nach Voraussetzung Noethersch ist, besitzt $\mathscr{S}$ ein maximales Element $K_p(I_q)$.

Weiters gilt nach Lemma 3.1.8, 2) einerseits

$$K_0(I_m) \subseteq K_1(I_m) \subseteq K_2(I_m) \subseteq \ldots, \quad m \geq 1,$$

und nach Teil 3) jenes Lemmas andererseits

$$K_n(I_1) \subseteq K_n(I_2) \subseteq K_n(I_3) \subseteq \ldots, \quad n \geq 0.$$

Somit muss für $n \geq p$ und $m \geq q$ wegen der Maximalitätsbedingung aus

$$K_p(I_q) \subseteq K_n(I_q) \subseteq K_n(I_m)$$

die Gleichheit $K_n(I_m) = K_p(I_q)$ folgen.

Für jedes $n \geq 0$ existiert nach Voraussetzung (R ist Noethersch) ein Index M_n sodass die aufsteigende Kette $K_n(I_1) \subseteq K_n(I_2) \subseteq \ldots$ ab $K_n(I_{M_n})$ stationär wird. Wir setzen $N = \max\{M_0, M_1, \ldots, M_{p-1}, q\}$.

Sei nun $m \geq N$ beliebig, aber fest. Wir unterscheiden zwei Fälle: Ist $n \geq p$, so folgt wegen $N \geq q$ und $m \geq q$ $K_n(I_m) = K_p(I_q) = K_n(I_N)$.

Wenn $n < p$ ist, dann ist wegen $m \geq M_n$ und $N \geq M_n$ somit $K_n(I_m) = K_n(I_{M_n}) = K_n(I_N)$.

Damit erhalten wir für alle n: $K_n(I_m) = K_n(I_N)$ und nach Lemma 3.1.8, 4) folgt $I_m = I_N$ für alle $m \geq N$. Die aufsteigende Kette $I_1 \subseteq I_2 \subseteq \ldots$ wird also jedenfalls ab I_N stationär und damit ist $R[x]$ ebenfalls Noethersch. □

Ideale in R[x]

I_1	$\subseteq$	I_2	$\subseteq$	I_3	$\subseteq \ldots \subseteq$	I_{M_1}	$\subseteq \ldots \subseteq$	I_q	$\subseteq \ldots \subseteq$	I_{M_0}	$\subseteq \ldots \subseteq$	I_N	$\subseteq \ldots$
$K_0(I_1)$	$\subseteq$	$K_0(I_2)$	$\subseteq$	$K_0(I_3)$	$\subseteq \ldots \subseteq$	$K_0(I_{M_1})$	$\subseteq \ldots \subseteq$	$K_0(I_q)$	$\subseteq \ldots \subseteq$	$\mathbf{K_0(I_{M_0})}$	$= \ldots =$	$\mathbf{K_0(I_N)}$	$= \ldots$
$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$	
$K_1(I_1)$	$\subseteq$	$K_1(I_2)$	$\subseteq$	$K_1(I_3)$	$\subseteq \ldots \subseteq$	$\mathbf{K_1(I_{M_1})}$	$= \ldots =$	$\mathbf{K_1(I_q)}$	$= \ldots =$	$\mathbf{K_1(I_{M_0})}$	$= \ldots =$	$\mathbf{K_1(I_N)}$	$= \ldots$
$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$	
$K_p(I_1)$	$\subseteq$	$K_p(I_2)$	$\subseteq$	$K_p(I_3)$	$\subseteq \ldots \subseteq$	$K_p(I_{M_1})$	$= \ldots =$	$\mathbf{K_p(I_q)}$	$= \ldots =$	$\mathbf{K_p(I_{M_0})}$	$= \ldots =$	$\mathbf{K_p(I_N)}$	$= \ldots$
$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\|$		$\|$		$\|$	
$K_{p+1}(I_1)$	$\subseteq$	$K_{p+1}(I_2)$	$\subseteq$	$K_{p+1}(I_3)$	$\subseteq \ldots \subseteq$	$K_{p+1}(I_{M_1})$	$= \ldots =$	$\mathbf{K_{p+1}(I_q)}$	$= \ldots =$	$\mathbf{K_{p+1}(I_{M_0})}$	$= \ldots =$	$\mathbf{K_{p+1}(I_N)}$	$= \ldots$
$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$	
$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\cap\mathrel{|}$		$\|$		$\|$		$\|$	
$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$	

Ideale in R

Für alle $n \geq 0$ wird jede aufsteigende Kette $\{K_n(I_m)\}_m$ stationär (zeilenweise); für $\{K_n(I_m)\}_n$, m beliebig aber fix gilt $K_n(I_m) \subseteq K_p(I_q)$ (spaltenweise).

Abbildung zum Beweis des Hilbertschen Basissatzes

Wir werden jetzt noch einen weiteren Beweis zum Hilbertschen Basissatz geben, der diesmal von der Eigenschaft, dass jedes Ideal eines Noetherschen Ringes endlich erzeugt ist, Gebrauch macht. Mit diesem Beweis wird nun klar, weshalb dieses Resultat als Basissatz bezeichnet wird.

2. Beweis von Satz 3.1.9. Sei $K_n(I)$ wie oben die Menge der führenden Koeffizienten aller Polynome n-ten Grades in einem Ideal I von $R[x]$. Wir wissen bereits aus dem Lemma 3.1.8,1) dass die Menge $K_n(I)$ ein Ideal in R ist und für jedes Ideal I die Inklusion

$$K_0(I) \subseteq K_1(I) \subseteq K_2(I) \subseteq \ldots$$

gilt. Darüber hinaus muss diese aufsteigende Idealkette in R ab einem gewissen Index abbrechen, da R nach Voraussetzung Noethersch ist. Sei t der Index, ab dem $K_n(I) = K_t(I)$ für alle $n \geq t$ gilt.

Nach Voraussetzung ist jedes $K_n(I)$ endlich erzeugt: $K_n(I) = (a_{n_1}, \ldots a_{n_{i_n}})$. Für jedes a_{n_j} mit $0 \leq n \leq t$ und $1 \leq j \leq i_n$ sei $p_{n_j}(x) \in I$ ein Polynom vom Grad n mit führendem Koeffizienten a_{n_j}. Für $p_{0_j}(x)$ gilt $p_{0_j}(x) = a_{0_j} \in R \subset R[x]$. Wir zeigen, dass das Ideal I

von einer endlichen Menge X von Polynomen erzeugt wird:

$$X = \{p_{n_j}(x) | 0 \leq n \leq t;\ 1 \leq j \leq i_n\}.$$

Klarerweise gilt $(X) \subset I$. Um die umgekehrte Inklusion zu zeigen, gehen wir induktiv vor. Zunächst sind die konstanten Polynome in I genau die Elemente von $K_0(I)$ und somit gilt $K_0(I) \subset (X)$. Nehmen wir an, dass (X) alle Polynome von I mit Grad $< m$ enthält und sei $q(x) \in I$ ein Polynom vom Grad m mit führendem Koeffizienten a ($a \neq 0$), das heißt $a \in K_m(I)$.
Wenn $m \leq t$, dann lässt sich a schreiben als

$$a = r_1 a_{m_1} + r_2 a_{m_2} + \ldots + r_{i_m} a_{m_{i_m}} \text{ für } r_j \in R;$$

dabei waren die a_{m_j} die Erzeugenden von $K_m(I)$. Das Polynom $\sum_{j=1}^{i_m} r_j p_{m_j}(x) \in (X)$ hat somit den führenden Koeffizienten a und Grad m. Weiters gilt, dass $q(x) - \sum_{j=1}^{i_m} r_j p_{m_j}$ höchstens Grad $m-1$ besitzen kann. Es gilt daher $q(x) - \sum_{j=1}^{i_m} r_j p_{m_j}(x) \in (X)$ nach Induktionsvoraussetzung und damit folglich auch $q \in (X)$.

Wenn $m > t$, dann ist $a \in K_m(I) = K_t(I)$ und $a = \sum_{j=1}^{i_t} r_j a_{t_j},\ r_j \in R$. Weiters hat $\sum_{j=1}^{i_t} r_j x^{m-t} p_{t_j}(x)$ führenden Koeffizienten a und Grad m. $q(x) - \sum_{j=1}^{i_t} r_j x^{m-t} p_{t_j}(x)$ hat höchstens Grad $m-1$ und liegt damit in (X). Auch in diesem Fall folgt $q(x) \in (X)$ und daher gilt wirklich $I = (X)$. □

Bemerkungen. Als allgemeine unmittelbare Folgerung ergibt sich, dass zu einem gegebenen Noetherschen Ring R mit Einselement auch der Polynomring in endlich vielen Variablen über R ebenfalls Noethersch ist. Um das zu zeigen, braucht man nur einen Induktionsbeweis nach der Anzahl der Veränderlichen anzuwenden.

Dagegen ist der Polynomring über $\mathbb{Z}$ in unendlich vielen Variablen $x_i,\ i \in \mathbb{N}$ nicht Noethersch, da die Kette von Idealen

$$(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots, x_n) \subset \ldots$$

nicht abbricht.

Für kommutative Ring ohne Einselement stimmt der Hilbertsche Basissatz nicht.

Beispiel. Für $R = 2\mathbb{Z}$ ist der Polynomring $2\mathbb{Z}[x]$ nicht Noethersch.

Zuerst verifizieren wir, dass der Ring $2\mathbb{Z}$ Noethersch ist. Wenn wir zeigen können, dass jedes Ideal in $2\mathbb{Z}$ auch ein Ideal in $\mathbb{Z}$ ist, sind wir fertig, da wir bereits wissen, dass $\mathbb{Z}$ die aufsteigende Kettenbedingung erfüllt. Sei dazu I ein Ideal in $2\mathbb{Z}$ und $a \in I$ das kleinste positive Element von I. Für ein beliebiges $b \in I$ gilt, dass es $r, q \in \mathbb{Z}$ gibt mit

$b = qa + r,\ 0 \leq r < a$ ($\mathbb{Z}$ ist euklidisch). Da sowohl b als auch qa in I liegen, muss auch $b - qa = r \in I$ gelten. Aus $0 \leq r < a$ folgt $r = 0$, da a minimal gewählt war. Damit ist gezeigt, dass jedes Element aus I ein Vielfaches von a ist: $I \subseteq \{qa : q \in \mathbb{Z}\}$. Wegen $a \in I$ gilt aber auch die umgekehrte Inklusion und somit Gleichheit. I ist also auch ein Ideal in $\mathbb{Z}$.

Angenommen $2\mathbb{Z}[x]$ ist Noethersch, dann ist jedes Ideal in $2\mathbb{Z}[x]$ endlich erzeugt und somit auch $2\mathbb{Z}[x]$. Seien $f_1(x), \ldots, f_n(x)$ die Erzeugendenelemente von $2\mathbb{Z}[x]$,

$$(f_1(x), \ldots f_n(x)) = 2\mathbb{Z}[x],$$

mit $f_i(x)$ Polynom d_i-ten Grades in $2\mathbb{Z}[x],\ i = 1, ..., n$, und sei $N = \max\{d_1, \ldots, d_n\}$. Ist $g(x) \in (f_1(x), \ldots f_n(x))$, dann lässt sich $g(x)$ schreiben als

$$g(x) = a_{i_1}(x)f_{i_1}(x) + \ldots a_{i_k}(x)f_{i_k}(x) + h(x),$$

wo $h(x)$ ganzzahlige Linearkombination der $f_i(x)$ ist, also insbesondere vom Grad $\leq N$, und $f_{i_j}(x), a_{i_j}(x) \in 2\mathbb{Z}[x]$. Da sowohl die Basiselemente als auch die $a_{i_j}(x)$ Vielfache von 2 sind, müssen alle Koeffizienten von $g(x)$ ab der $(N+1)$-ten Potenz von x durch 4 teilbar sein. Somit kann das Polynom $2x^{N+1}$ nicht in $(f_1(x), \ldots f_n(x)) = 2\mathbb{Z}[x]$ liegen, ein offensichtlicher Widerspruch. $2\mathbb{Z}[x]$ ist daher nicht endlich erzeugt, also nicht Noethersch.

Dieses Beispiel beinhaltet auch, dass nicht jeder Unterring eines Noetherschen Ringes wieder Noethersch ist. Wie gezeigt wurde ist $2\mathbb{Z}$ als Unterring von $\mathbb{Z}$ Noethersch; für $2\mathbb{Z}[x]$ als Unterring von $\mathbb{Z}[x]$ gilt dies allerdings nicht.

Aber auch wenn der Unterring das Einselement enthält, vererbt sich die Eigenschaft nicht: Der Quotientenkörper $\mathbb{Q}(x_1, x_2, \ldots)$ von $\mathbb{Z}[x_1, x_2, \ldots]$ ist als Körper Noethersch, während das auf $\mathbb{Z}[x_1, x_2, \ldots]$ wie oben erwähnt nicht zutrifft.

Mittels des Hilbertschen Basissatzes lassen sich eine Vielzahl von konkreten Noetherschen Ringen herstellen.

Korollar 3.1.10. *Seien R ein kommutativer Ring mit Einselement e und S ein Noetherscher Unterring von R mit $e \in S$. Existieren endlich viele feste Elemente $r_1, \ldots, r_n \in R$, so dass sich jedes Element aus R durch $p(r_1, \ldots, r_n)$ ausdrücken lässt mit $p \in S[x_1, \ldots, x_n]$, dann ist auch R Noethersch.*

Beweis. Der Polynomring $S[x_1, \ldots, x_n]$ ist nach der Bemerkung zu Satz 3.1.9 Noethersch. Sei $\Phi : S[x_1, \ldots, x_n] \to R$ der Einsetzhomorphismus bezüglich $r_1, \ldots, r_n$ gegeben durch $\Phi(p(x_1, \ldots, x_n)) = p(r_1, \ldots, r_n)$. Nach der Voraussetzung ist Φ surjektiv. Daher ist R nach Satz 3.1.7 Noethersch. □

Beispiele.

1. Die Menge $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} |\ a, b \in \mathbb{Z}\}$ mit $d \in \mathbb{Z},\ \sqrt{d} \notin \mathbb{Z}$, ist nach Korollar 3.1.10 Noethersch. Dazu geht man von $S = \mathbb{Z}$ aus und wählt den Einsetzhomomorphismus bezüglich $\sqrt{d}$, ausgehend von $\mathbb{Z}[x]$. Dann ist $R = \{p(\sqrt{d}) |\ p(x) \in \mathbb{Z}[x]\}$. Und dies ist gerade $\mathbb{Z}[\sqrt{d}]$.

Mit der gleichen Überlegung ergibt sich allgemein

2. Ist α eine ganze algebraische Zahl (also eine Zahl, für die ein normiertes Polynom aus $\mathbb{Z}[x]$ existiert, sodass α Nullstelle ist) mit $\alpha \notin \mathbb{Z}$, dann ist $\mathbb{Z}[\alpha]$ Noethersch. Dabei ist $\mathbb{Z}[\alpha] = \{p(\alpha) |\ p(x) \in \mathbb{Z}[x]\}$.

3.2 Prim- und Primärideale

Hauptidealringe haben die Eigenschaft faktorielle Ringe zu sein, also Ringe, in denen sich jedes Element eindeutig bis auf Einheiten und die Reihenfolge als Produkt von Primfaktoren schreiben lässt. In solchen Ringen, die früher meist als ZPE-Ringe bezeichnet wurden, lässt sich diese Eigenschaft auch auf die (Haupt-)Ideale übertragen:

Jedes echte Ideal eines faktoriellen Ringes lässt sich als Produkt von maximalen (und damit primen und irreduziblen) Idealen darstellen, die abgesehen von der Reihenfolge eindeutig bestimmt sind:

$$(a) = (p_1^{n_1} \cdot \ldots p_r^{n_r}) = (p_1^{n_1}) \cdot \ldots \cdot (p_r^{n_r}) = (p_1)^{n_1} \cdot \ldots \cdot (p_r)^{n_r} = (p_1^{n_1}) \cap \ldots \cap (p_r^{n_r});$$

dabei ist $a \in R, a \neq 0$, keine Einheit und die $p_i, i = 1, ..., r$, sind prime Elemente. Dies folgt unmittelbar aus Lemma 2.0.4 im Kapitel "Grundlagen".

Diese Eigenschaft ist nicht auf faktorielle Ringe beschränkt. Wie schon in der Einleitung erwähnt, ist der Noethersche Ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\}$ nicht faktoriell, da es für das Element $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ die beiden wesentlich verschiedenen Zerlegungen in irreduzible Elemente $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$, die keine Einheiten sind, gibt. Trotzdem lässt sich das von 6 erzeugte Hauptideal eindeutig bis auf die Reihenfolge als Produkt von Primidealen darstellen (wie in Kapitel 5 gezeigt werden wird):

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Doch nicht in allen Noetherschen Ringen gilt diese Eigenschaft.

Beispiel. Das Ideal $(4, x)$ in $\mathbb{Z}[x]$ lässt sich weder als Durchschnitt noch als Produkt von Primidealen schreiben.

Es gilt

$$(4, x) = \{p(x) \in \mathbb{Z}[x] | p(x) = 4r(x) + xs(x) \text{ mit } r(x), s(x) \in \mathbb{Z}[x]\}$$

$$= \{p(x) \in \mathbb{Z}[x] |\ 4 | p(0)\}.$$

Wir zeigen, dass $(4, x)$ kein Primideal ist und es nur ein einziges Ideal $J \subset \mathbb{Z}[x]$ gibt mit $(4, x) \subset J$, so dass sich $(4, x)$ sicher auch nicht als Durchschnitt von Idealen schreiben lässt. Um das zu zeigen betrachten wir den Faktorring $\mathbb{Z}[x]/(4, x)$. Da es nur auf den konstanten Term bei den Polynomen ankommt und alle ganzzahligen Vielfachen von 4

bereits in (4,x) liegen, gilt

$$\mathbb{Z}[x]/(4,x) \cong \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Insbesondere ist $(4,x)$ kein Primideal, da der Restklassenring kein Integritätsring ist.

Dieser Restklassenring besitzt als echtes Ideal nur $\overline{J} = \{\overline{0}, \overline{2}\}$. Nach dem Homomorphiesatz ist daher $J = (2,x) = \{p(x) \in \mathbb{Z}[x] |\ 2|p(0)\}$ der einzige echte Teiler $\neq R$ von $(4,x)$.

$(4,x)$ lässt sich aber auch nicht als Potenz von J darstellen. denn das Produkt zweier Polynome aus J hat stets einen geraden Koeffizienten bei x, was für die Elemente von $(4,x)$ nicht gilt. Es ist also $J^2 \subset (4,x)$.

Das Ideal $(4,x)$ ist kein Produkt von Primidealen, also auch keine Primidealpotenz, doch erfüllt es folgende abgeschwächte Forderung, wie gleich bewiesen wird.

Definition 3.2.1. *Ein Ideal $Q \neq R$ in einem kommutativen Ring R heißt primär, wenn aus $ab \in Q$ $(a,b \in R)$ und $a \notin Q$ folgt $b^n \in Q$ für ein $n > 0$.*

Bemerkungen.

1. Jedes Primideal ist primär, denn in diesem Fall ist die Bedingung bereits für $n = 1$ erfüllt.

2. Betrachten wir in einem kommutativen Ring den Faktorring nach dem primären Ideal Q, dann folgt aus $ab \equiv 0\ (Q)$ und $a \not\equiv 0\ (Q)$, dass die Potenz $b^n \equiv Q$ verschwindet. Oder anders formuliert: *Ein Ideal Q ist primär genau dann, wenn im Faktorring R/Q jeder Nullteiler nilpotent ist.*

Beispiele.

1. Wie sehen die Primärideale von $\mathbb{Z}$ aus? Sei dazu $Q = (n)$ ein beliebiges Ideal von $\mathbb{Z}$ mit $n > 1$. Ist n keine Primzahlpotenz, also $n = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$ mit $r > 1$, so ist $a = p_1^{n_1} \notin Q$, aber auch $b^k = p_2^{kn_1} \cdot \ldots \cdot p_r^{kn_r} \notin Q$ wegen der eindeutigen Primfaktorzerlegung in $\mathbb{N}$. Q ist in diesem Fall also kein Primärideal.

Ist dagegen $n = p^m$, so muss $a = p^r$ mit $r < m$ sein. Dann gilt $p|b = p^{m-r}$ und ein geeignete Potenz von b, zum Beispiel die m-te, liegt in (n). Somit sind die Primärideale von $\mathbb{Z}$ genau die Potenzen der Primideale: $(p)^m = (p^m)$ mit p prim, $m \geq 1$.

2. Das Ideal $(4,x)$ in $\mathbb{Z}[x]$ ist primär. Sei nämlich $p(x)q(x) \in (4,x)$ und $p(x) \notin (4,x)$. Dann gilt $p(0)q(0) \equiv 0(4)$, aber $4 \nmid p(0)$. Damit ist $p(0) \equiv 1,2,3(4)$. Ist $p(0) \equiv 1,3(4)$, so muss $q(0) \equiv 0(4)$ gelten und es ist schon $q(x) \in (4,x)$. Ist dagegen $p(0) \equiv 2(4)$, so ist auch $q(0) \equiv 2(4)$ und daher gilt $q^2(0) \equiv 0(4)$, also $q^2(x) \in (4,x)$.

Das letzte Beispiel zeigt, dass Primärideale nicht notwendigerweise Primidealpotenzen sein müssen. Es ist aber auch umgekehrt die Potenz eines Primideals im Allgemeinen nicht primär:

3. ([VdW67], S.129) Sei

$$R = \{a_0 + a_1 x + ... + a_n x^n |\ 3|a_1,\ a_i \in \mathbb{Z}, i = 1, ..., n\}.$$

Dann ist das Ideal $P = (3x, x^2)$ wegen $R/P \cong \mathbb{Z}$ ein Primideal. Es ist $P^2 = (9x^2, 3x^3, x^4)$. Dieses Ideal ist nicht primär. Das Produkt $9 \cdot x^2$ liegt in P^2, x^2 jedoch nicht. Wäre P^2 primär, müsste somit $9^k \in P^2$ gelten für ein geeignetes $k > 1$, was offensichtlich nicht der Fall ist.

Analog zu faktoriellen Ringen, wo jedes irreduzible Element auch prim (und daher primär) ist, lässt sich in Noetherschen Ringen diese Aussage abgeschwächt auch auf irreduzible Ideale übertragen:

Satz 3.2.2. *In einem Noetherschen Ring ist jedes irreduzible Ideal primär.*

Beweis. Wir zeigen die äquivalente Behauptung, indem wir annehmen, dass das Ideal Q des Noetherschen Ringes R nicht primär ist, und folgern, dass Q dann reduzibel ist.

Wenn Q nicht primär ist, dann gibt es $a, b \in R$ mit $ab \in Q,\ a \notin Q$ und für kein $n > 0$ ist $b^n \in Q$. Wir bilden für jedes $n \in \mathbb{N}$ die Menge

$$S_n = \{r \in R : rb^n \in Q\}.$$

Für alle $n \in \mathbb{N}$ ist die Menge S_n sicher nicht leer, da sie alle Elemente aus Q enthält, weil Q nach Voraussetzung ein Ideal ist. Weiters bildet die Menge S_n ein Ideal in R für alle n: Für $r_{n_1}, r_{n_2} \in S_n$ liegt nämlich $(r_{n_1} - r_{n_2})b^n = r_{n_1}b^n - r_{n_2}b^n$ in Q und somit gilt $r_{n_1} - r_{n_2} \in S_n$. Ebenfalls gilt für $r \in R,\ r_n \in S_n$, dass $(rr_n)b^n = r(r_n b^n) \in Q$ und folglich $rr_n \in S_n$.

Darüber hinaus bilden die S_n eine aufsteigende Idealkette $S_1 \subseteq S_2 \subseteq \ldots$, weil für $r_i \in S_i$ auch $(br_i)b^i = (r_i b)b^i = r_i b^{i+1} \in Q$ gilt und damit $r_i \in S_{i+1}$ folgt. Da R Noethersch ist, bricht diese Idealkette ab einem gewissen Index $k \in \mathbb{N}$ ab, also $S_k = S_t$ für alle $t > k$.

Wir behaupten, dass Q reduzibel ist und sich als Durchschnitt $Q = (Q, a) \cap (Q, b^k)$ darstellen lässt. Sowohl (Q, a) als auch (Q, b^k) sind echte Teiler von Q, da $a \in (Q, a)$, und $a \notin Q$, sowie $b^k \in (Q, b^k)$, und $b^k \notin Q$. Klarerweise gilt $Q \subseteq (Q, a) \cap (Q, b^k)$.

Sei nun $c \in (Q, a) \cap (Q, b^k)$. Wegen $c \in (Q, b^k)$ lässt es sich schreiben als $c = q + r_1 b^k$ für geeignete $q \in Q, r_1 \in R$. Andererseits muss wegen $c \in (Q, a)$ das Produkt cb in Q

liegen (denn für $c = q' + r_2 a,\ r_2 \in R, q' \in Q$, liegt $cb = q'b + r_2 ab = bq' + r_2(ab)$ in Q, da nach Voraussetzung $ab \in Q$ gilt).

Insgesamt folgt daher aus $cb = qb + r_1 b^{k+1} \in Q$, dass $r_1 b^{k+1} \in Q$ und damit $r_1 \in S_{k+1} = S_k$ gilt. Nach Konstruktion von S_k besagt dies $r_1 b^k \in Q$. Damit muss $c = q + r_1 b^k$ ebenfalls in Q liegen und die umgekehrte Inklusion $(Q, a) \cap (Q, S_k) \subseteq Q$ ist gezeigt. $\square$

Die Umkehrung der Aussage des Satzes gilt nicht.

Beispiel. Das Ideal $(4, 2x, x^2)$ ist primär in $\mathbb{Z}[x]$, aber reduzibel: $(4, 2x, x^2) = (4, x) \cap (2, x^2)$. Dabei sind auch die beiden Ideale auf der rechten Seite primär.

Dass alle Ideale primär sind, zeigen wir so wie im Fall $(4, x)$ (Beispiel 2. nach der Definition 3.2.1).

Wir führen zunächst den Nachweis für $(4, 2x, x^2)$:

$$I := (4, 2x, x^2) = \{4r_1(x) + 2xr_2(x) + x^2 r_3(x) |\ r_i(x) \in \mathbb{Z}[x],\ i = 1, 2, 3\}$$

$$= \{a_0 + a_1 x + ...a_n x^n |\ a_i \in \mathbb{Z}, i = 1, ..., n;\ 4|a_0,\ 2|a_1\}.$$

Seien nun $p(x), q(x) \in \mathbb{Z}[x]$ mit $p(x)q(x) \in I$ und $p(x) \notin I$. Da es für die Elemente aus dem Ideal I auf die Terme höheren als 1. Grades nicht ankommt, können wir ansetzen $p(x) = b_0 + b_1 x + x^2(...)$ und $q(x) = c_0 + c_1 x + x^2(...)$ und brauchen nur mit den linearen Termen zu rechnen. Aus $p(x)q(x) \in I$ folgt

$$b_0 c_0 \equiv 0(4) \quad \text{und} \quad b_0 c_1 + b_1 c_0 \equiv 0(2). \tag{3.1}$$

$p(x) \notin I$ besagt $b_0 \equiv 0, 1, 2, 3(4)$ und $b_1 \equiv 0, 1(2)$, wobei aber b_0 nicht durch 4 und zugleich b_1 durch 2 teilbar sein darf.

Wir betrachten nun die einzelnen Fälle:

(i) $b_0 \equiv 0(4)$. Dann muss $b_1 \equiv 1(2)$ sein und $p(x) = x$. Aus der Bedingung 3.1 folgt $c_0 \equiv 0(2)$, also ist $q(x) = 2t + c_1 x + ...$ $(t \in \mathbb{Z})$. Dann gilt $q^2(x) \in I$.

(ii) $b_0 \equiv 1, 3(4)$. Aus 3.1 folgt $c_0 \equiv 0(4)$ und daher gilt sogar $q(x) \in I$, da $c_1 \equiv 0(2)$.

(iii) Ist schließlich $b_0 \equiv 2(4)$, dann muss auch $c_0 \equiv 2(4)$ sein und wieder folgt $q^2(x) \in I$.

Genauso zeigen wir, dass das Ideal $(2, x^2)$ primär ist. Es gilt

$$J := (2, x^2) = \{2s_1(x) + x^2 s_2(x) |\ s_i(x) \in \mathbb{Z}[x],\ i = 1, 2\}$$

$$= \{a_0 + a_1 x + ...a_n x^n |\ a_i \in \mathbb{Z}, i = 1, ..., n;\ 2|a_0,\ 2|a_1\}.$$

Wieder kommt es bei den Elementen aus dem Ideal J auf die Terme höheren als 1. Grades nicht an, so dass wir denselben Ansatz wie zuvor machen können. $p(x) \notin J$ besagt jetzt,

dass b_0, b_1 nicht beide gerade sein dürfen. Der Bedingung 3.1 entspricht jetzt

$$b_0c_0 \equiv 0(2) \quad \text{und} \quad b_0c_1 + b_1c_0 \equiv 0(2). \tag{3.2}$$

Wieder unterscheiden wir Fälle:

(i) $b_0 \equiv 0(2)$. Dann muss $b_1 \equiv 1(2)$ sein und $p(x) = x$. Aus 3.2 folgt $c_0 \equiv 0(2)$, also ist $q(x) = 2t + c_1x + ...$ $(t \in \mathbb{Z})$. Dann gilt $q^2(x) \in J$.

(ii) $b_0 \equiv 1(2)$ liefert in 3.2 wieder $c_0 \equiv 0(2)$, also genauso $q^2(x) \in J$ (sogar $q(x) \in J$).

Es fehlt noch der Beweis, dass $(4, 2x, x^2) = (4, x) \cap (2, x^2)$ gilt.

Die Inklusion $(4, 2x, x^2) \subseteq (4, x) \cap (2, x^2)$ folgt wegen $4, 2x, x^2 \in (4, x) \cap (2, x^2)$. Ist umgekehrt $p(x) \in (4, x) \cap (2, x^2)$, so muss $4|p(0)$ gelten, da $p(x) \in (4, x)$. Und der Koeffizient von x muss gerade sein, da dies für alle Elemente von $(2, x^2)$ gilt. Daher folgt $p(x) \in (4, 2x, x^2)$ und damit $(4, 2x, x^2) \supseteq (4, x) \cap (2, x^2)$.

3.2.1 Primärzerlegungen in Noetherschen Ringe

Mit dem folgenden Satz werden wir zeigen, dass sich jedes Ideal in einem Noetherschen Ring als Durchschnitt von endlich vielen Primäridealen darstellen lässt. Anschließend daran werden wir zeigen, dass es zu jedem Primärideal Q ein kleinstes, eindeutig bestimmtes Primideal P gibt, das Q umfasst und mithilfe diesem Aussagen über die Eindeutigkeit der Darstellungen im Abschnitt 3.2.2 machen.

Satz 3.2.3 (Erster Zerlegungssatz)**.** *In einem Noetherschen Ring ist jedes echte Ideal als Durchschnitt von endlich vielen Primäridealen darstellbar.*

Beweis. Wir werden zeigen, dass sich jedes Ideal als Durchschnitt von endlich vielen irreduziblen Idealen darstellen lässt. Die Behauptung folgt dann sofort aus Satz 3.2.2.

Für irreduzible Ideale von R ist die Behauptung trivialerweise erfüllt.

Sei nun $\mathscr{S}$ die Menge aller Ideale J von R, die sich nicht als Durchschnitt endlich vieler irreduzibler Ideale schreiben lassen. Da nach Voraussetzung $\mathscr{S}$ nicht leer ist, gibt es nach dem Zornschen Lemma in $\mathscr{S}$ ein maximales Ideal I. Dieses muss reduzibel sein, so dass Ideale I_1, I_2 existieren mit

$$I = I_1 \cap I_2, \quad \text{und } R \supset I_1, I_2 \supset I.$$

Da $I_1, I_2 \notin \mathscr{S}$ lassen sie sich als Durchschnitt von endlich vielen irreduziblen Idealen

darstellen:

$$\begin{aligned} I_1 &= Q_1 \cap Q_2 \cap \ldots \cap Q_r, \\ I_2 &= Q_{r+1} \cap Q_{r+2} \cap \ldots \cap Q_s \end{aligned}$$

Damit stellt sich $I = Q_1 \cap Q_2 \cap \ldots \cap Q_r \cap Q_{r+1} \cap Q_{r+2} \cap \ldots \cap Q_s$ als Durchschnitt irreduzibler Ideale dar, im Widerspruch zur Definition von $\mathscr{S}$. Daher gilt $\mathscr{S} = \emptyset$ und die Behauptung ist bewiesen. □

Definition 3.2.4. *Ein Ideal I eines kommutativen Ringes R besitzt eine Primärzerlegung, falls es sich schreiben lässt als $I = Q_1 \cap ... \cap Q_n$ mit Primäridealen $Q_i,\ i = 1, ..., n$.*

Beispiel. Wie das zuletzt gerechnete Beispiel $(4, 2x, x^2) = (4, x) \cap (2, x^2)$ zeigt, kann es für ein Ideal zwei Zerlegungen in Primärideale geben mit unterschiedlicher Anzahl.

Es stellt sich daher die Frage nach der Eindeutigkeit von Primärzerlegungen. Dazu muss man zunächst die Anzahl der Komponenten bei der Darstellung von Idealen so weit wie möglich reduzieren. Die erste Reduktion besteht darin in einer Darstellung von $I = Q_1 \cap \ldots \cap Q_r$ jene Primärideale Q_i zu streichen, die den Durchschnitt anderer umfassen. Um festzustellen, ob es sich danach bereits um eine unverkürzbare Darstellung handelt, ist noch Vorarbeit notwendig:

Wir betrachten zu einem Primärideal Q die Menge P, die alle Elemente $b \in R$ beinhaltet, so dass eine Potenz von b in Q liegt: $P = \{b \in R |\ b^n \in Q \text{ für ein } n > 0\}$.

Lemma 3.2.5. *Sei R ein kommutativer Ring mit Einselement und Q ein Primärideal. Dann erfüllt die Menge $P = \{b \in R | b^n \in Q \text{ für ein } n > 0\}$ folgende Eigenschaften:*

(i) P ist ein Ideal in R,

(ii) P ist prim,

(iii) P ist ein Teiler von Q, d.h. $Q \subseteq P$.

Beweis.

(i) Sei $b \in P$, dann ist $b^n \in Q$ für ein $n \in \mathbb{N}$. Für $r \in R$ folgt, dass das Produkt $r^n b^n = (rb)^n \in Q$, da Q Ideal ist, und demnach $rb \in P$ gilt. Um zu zeigen, dass P abgeschlossen ist, müssen wir zeigen, dass es ein $k > 0$ gibt, sodass $(b - c)^k \in Q$ für $b, c \in P$. Seien $b^n, c^m \in Q$, dann liegt

$$(b - c)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} b^{n+m-i} (-1)^i c^i$$

sicher in Q, da jeder Summand entweder c^m oder b^n beinhaltet. Aus der Ungleichung $\frac{m+n}{2} \geq \frac{2m}{2}$ für oBdA $m \geq n$ sehen wir sofort, dass das auch für die „mittleren“ Summanden gewährleistet ist. (Mit der Forderung $m > 1,\ n > 1$ gilt sogar schon $(b-c)^{n+m-1} \in Q$.)

(ii) Weiters stellen wir fest, dass unsere konstruierte Menge P prim ist. Sei nämlich $ab \equiv 0(P)$ und $a \not\equiv 0(P)$, so folgt für ein $n > 0 : (ab)^n = a^n b^n \equiv 0(Q)$ und $a^n \not\equiv 0(Q)$ (weil $a \not\equiv 0(P)$). Da Q primär ist, muss es also ein $m > 0$ geben, so dass $(b^n)^m = b^{nm} \equiv 0(Q)$ und damit gilt nach Definition von P, dass $b \equiv 0(P)$. Also folgt $b \in P$ und P ist Primideal.

(iii) Ist $b \in Q$, so ist, da Q Ideal ist, auch $b^n \in Q$ sogar für beliebiges $n \in \mathbb{N}$. Daher gilt $b \in P$. □

Das im letzten Satz eingeführte Primideal erweist sich als entscheidend für die Reduktion der Primärzerlegung eines Ideals. Es lässt sich auf verschiedene Arten charakterisieren, von denen wir die in den folgenden zwei Sätzen 3.2.8 und 3.2.9 benötigen. Zuvor werden wir aber noch eine Definition und ein zentrales Resultat, das die Existenz von Primidealen in kommutativen Ringen mit Eins gewährleistet, vorausschicken:

Definition 3.2.6. *Sei R ein kommutativer Ring. Eine nichtleere Teilmenge S von R heißt multiplikativ abgeschlossen, wenn für $s_1, s_2 \in S$ auch das Produkt in S liegt, $s_1 s_2 \in S$.*

Satz 3.2.7. *Sei R ein kommutativer Ring, $S \neq \emptyset$ eine multiplikativ abgeschlossene Menge von R und I ein Ideal von R mit der Eigenschaft $S \cap I = \emptyset$. Dann existiert ein Ideal P das maximal ist in der Menge aller Ideale von R, die zu S disjunkt sind und I enthalten. Das Ideal P ist darüber hinaus ein Primideal von R.*

Beweis. Sei $\mathscr{M}$ die Menge aller Ideale von R, die zu S disjunkt sind und I enthalten:

$$\mathscr{M} = \{J \text{ ist Ideal von } R | J \cap S = \emptyset \text{ und } I \subseteq J\}.$$

$\mathscr{M}$ ist nicht leer, da $I \in \mathscr{M}$ gilt. Auch erfüllen alle $J \in \mathscr{M}$ wegen $S \neq \emptyset$, dass $J \subset R$. Mit „$\subseteq$“ erhält die Menge $\mathscr{M}$ eine partielle Ordnung und da R Noethersch ist, besitzt $\mathscr{M}$ ein maximales Ideal P.

Wir zeigen, dass P ein Primideal ist: Dazu nehmen wir indirekt an, dass es Elemente $u, v \in R$ gibt mit $uv \in P$, aber $u, v \notin P$. Sei $A := (u), B := (v)$, dann gilt somit $AB \subseteq P$ sowie $P + A \supset P$ und $P + B \supset P$. Wegen der Maximalität von P folgt $(P + A) \cap S \neq \emptyset$ und $(P + B) \cap S \neq \emptyset$. Sei $s_1 \in (P + A) \cap S$ und $s_2 \in (P + B) \cap S$, dann lassen sie sich schreiben als $s_1 = p_1 + a,\ s_2 = p_2 + b$ mit $p_1, p_2 \in P$ und $a = r_1 u,\ b = r_2 v$ für geeignete $r_1, r_2 \in R$. Weil S multiplikativ abgeschlossen ist, gilt einerseits $s_1 s_2 \in S$; andererseits ist

$$s_1 s_2 = p_1 p_2 + p_1 b + a p_2 + ab \in P + AB.$$

Wegen der Voraussetzung $AB \subseteq P$ folgt $P + AB \subseteq P$ und somit gilt $s_1 s_2 \in P$. Dies widerspricht der Voraussetzung $P \cap S = \emptyset$. Somit muss $u \in P$ oder $v \in P$ gegolten haben, das heißt P ist Primideal. □

Satz 3.2.8. *Sei Q ein Primärideal in einem kommutativen Ring R. Das im Lemma 3.2.5 beschriebene Primideal $P = \{b \in R | b^n \in Q \text{ für ein } n > 0\}$ ist genau der Durchschnitt aller Primideale, die Q enthalten.*

Der Durchschnitt aller Primideale, die Q umfassen, heißt das Radikal von Q und wird mit $Rad(Q)$ bezeichnet.

Beweis. Sei $Rad(Q) = \bigcap_{i \in I} P_i$ der Durchschnitt aller Primideale $P_i, i \in I$, die Q umfassen. Wir zeigen zuerst, dass $P \subseteq \bigcap_{i \in I} P_i$ gilt. Sei dazu $b \in P$ dann existiert ein $n > 0$ mit $b^n \in Q$. Weiters gilt daher $b^n \in P_i$ nach Voraussetzung für alle $i \in I$. Da die $P_i, i \in I$, Primideale sind folgt $b \in P_i$ für alle $i \in I$ und daher $b \in Rad(Q)$.

Umgekehrt sei $t \notin P$, also $t \in R$ und $t^n \notin Q \ \forall n > 0$. Wir bilden die Menge

$$S = \{t^n + q | n \in \mathbb{N},\ q \in Q\}$$

und überzeugen uns, dass sie multiplikativ abgeschlossen ist und $S \cap Q = \emptyset$ gilt:

Angenommen es existiert ein $s \in S \cap Q$, dann ist $s = t^n + q$ und wegen $q \in Q$ liegt auch $t^n = s - q$ in Q; ein Widerspruch zur Annahme $t^n \notin Q$. Darüber hinaus gilt für $s_1 = t^{n_1} + q_1,\ s_2 = t^{n_2} + q_2 \in S$:

$$s_1 s_2 = (t^{n_1} + q_1)(t^{n_2} + q_2) = t^{n_1 + n_2} + t^{n_1} q_2 + t^{n_2} q_1 + q_1 q_2 \in S,$$

da die letzten drei Summanden im Ideal Q liegen. S ist also multiplikativ abgeschlossen.

Nach Satz 3.2.7 existiert daher ein maximales Ideal $\bar{P}$ mit $\bar{P} \cap S = \emptyset$, $\bar{P} \supseteq Q$ und $\bar{P}$ prim. Nun ist $t = t^1 + 0 \in S$. Wegen $\bar{P} \cap S = \emptyset$ folgt $t \notin \bar{P}$. Da $\bar{P}$ Primideal ist, welches Q umfasst, gilt $\bar{P} \supseteq \bigcap_{i \in I} P_i$. $t \notin \bar{P}$ impliziert daher $t \notin \bigcap_{i \in I} P_i$. Wir haben gezeigt, dass aus $t \notin \bar{P}$ folgt $t \notin Rad(Q)$, was äquivalent ist zu $Rad(Q) \subseteq P$. Insgesamt ergibt sich die Gleichheit beider Mengen. □

Bemerkung. Wir bezeichnen die Menge P auch als *das zu Q zugehörige Primideal* oder sagen kurz *Q ist P-primär*. Wegen der Konstruktion von P zu Q ist auch die Schreibweise $P = \sqrt{Q} = Rad(Q)$ üblich.

Man beachte, dass zu einem gegebenen Primärideal das zugehörige Primideal eindeutig ist, aber es zu einem Primideal mehrere Primärideale geben kann, die P-primär sind.

Umgekehrt können wir bei zwei gegebenen Idealen feststellen, ob eines davon zugehöriges Primideal des anderen ist:

Satz 3.2.9. *Seien P und Q Ideale in einem kommutativen Ring R. Q ist P-primär genau dann wenn*

(i) $Q \subseteq P \subseteq \{b \in R | b^n \in Q$ für ein $n > 0\} = Rad(Q)$ und eine der beiden Bedingungen gilt:

(ii) wenn aus $ab \in Q$ und $a \notin Q$ folgt $b \in P$. oder

(iii) wenn aus $ab \in Q$ und $a \notin P$ folgt $b \in Q$.

Beweis. Wir zeigen nur die Äquivalenz von Q ist P-primär zu den Bedingungen (i) und (ii). Diejenige zu (i) und (iii) kann völlig analog bewiesen werden.

Wir setzen $M = \{b \in R | b^n \in Q$ für ein $n > 0\}$.

($\Leftarrow$) Sei $ab \in Q$ und $a \notin Q$, dann gilt nach Voraussetzung $b \in P \subseteq M$. Nach Definition von M ist Q daher primär.

Um zu zeigen, dass Q primär für P ist, müssen wir $P = M$ nachweisen: Nach (i) gilt $P \subseteq M$. Um die andere Inklusion zu zeigen, sei $b \in M$ und n die kleinste natürliche Zahl, so dass $b^n \in Q$ gilt. Wenn $n = 1$, dann folgt $b \in Q$ und mit (i) weiter $b \in P$. Also gilt in diesem Fall $M \subseteq P$. Wenn $n > 1$, dann ist $b^n = b^{n-1}b$ mit $b^{n-1} \notin Q$ wegen der Minimalität von n. Aus (ii) folgt, dass $b \in P$ und somit ebenfalls $M \subseteq P$ folgt. Damit ist die Gleichheit der beiden Mengen gezeigt.

($\Rightarrow$) Sei Q primär für P, d.h. es gilt $P = M$. Wegen Satz 3.2.8 gilt jedenfalls die Bedingung (i). Um (ii) nachzuweisen sei $ab \in Q$ und $a \notin Q$. Da Q primär ist gibt es ein $n > 0$ mit $b^n \in Q$. Es bleibt zu zeigen, dass $b \in P$ gilt, was aber sofort aus der Beschreibung von

$$P = \{b \in R | b^n \in Q \text{ für ein } n > 0\} = M$$

aus Satz 3.2.8 folgt. □

Bisher haben wir unsere Untersuchungen von Primidealen auf gegebene Primärideale beschränkt. Da in Noetherschen Ringen jedes echte Ideal eine Primärzerlegung besitzt und nach Satz 3.1.4 2) jedes Ideal in einem maximalen Ideal enthalten ist, können wir, wenn R ein Einselement besitzt (diese Voraussetzung sichert, dass das maximale Ideal auch prim ist), zu jedem beliebigen Ideal ein zugehöriges Primideal finden, das es umfasst.

Wir erweitern den Begriff des Radikals von einem Primärideal auf beliebige Ideale I, indem wir analog $Rad(I) = \{x \in R | x^n \in I$ für ein $n > 0\}$ setzen.

Satz 3.2.10. *Seien $I, J, I_1, \ldots I_n$ Ideale eines Noetherschen Rings mit Einselement. Dann gilt:*

a) $Rad(I)$ ist der Durchschnitt aller Primideale, die I umfassen. $Rad(I)$ ist ein Primideal mit der Eigenschaft $I \subseteq Rad(I) \subseteq R$.

b) Aus $I \subseteq J$ folgt $Rad(I) \subseteq Rad(J)$.

c) $Rad(I_1 \cdot \ldots \cdot I_n) = Rad(I_1 \cap \ldots \cap I_n) = Rad(I_1) \cap \ldots \cap Rad(I_n)$.

d) Für jedes I existiert eine natürliche Zahl n mit $(Rad(I))^n \subseteq I$.

Beweis.

a) Die Aussage ist eine Verallgemeinerung von den Sätzen 3.2.5 und 3.2.8.

b) Die Behauptung ist wegen a) klar.

c) Aus $I_1 \cdot \ldots \cdot I_n \subseteq I_1 \cap \ldots \cap I_n$ und b) folgt $Rad(I_1 \cdot \ldots \cdot I_n) \subseteq Rad(I_1 \cap \ldots \cap I_n)$. Umgekehrt sei $a \in Rad(I_1 \cap \ldots \cap I_n)$, dann existiert eine natürliche Zahl k mit $a^k \in I_1 \cap \ldots \cap I_n$ und folglich $a^k \in I_j \ \forall j$. Damit ist $(a^k)^n \in I_1 \cdot \ldots \cdot I_n$, also $a \in Rad(I_1 \cdot \ldots \cdot I_n)$, was die umgekehrte Inklusion $Rad(I_1 \cdot \ldots \cdot I_n) \supseteq Rad(I_1 \cap \ldots \cap I_n)$ zeigt.

Um noch $Rad(I_1 \cap \ldots \cap I_n) = Rad(I_1) \cap \ldots \cap Rad(I_n)$ zu zeigen, verwenden wir zunächst $I_1 \cap \ldots \cap I_n \subseteq I_j \ \forall j$, sodass $Rad(I_1 \cap \ldots \cap I_n) \subseteq Rad(I_j) \ \forall j$ gilt. Daher folgt $Rad(I_1 \cap \ldots \cap I_n) \subseteq Rad(I_1) \cap \ldots \cap Rad(I_n)$. Umgekehrt sei $b \in Rad(I_1) \cap \ldots \cap Rad(I_n)$, dann gilt $b \in Rad(I_j) \ \forall j$ und es existiert für jedes j ein $k_j \in \mathbb{N}$ mit $b^{k_j} \in I_j$. Das Element $b^{k_1+\ldots k_n} = b^{k_1} \cdot \ldots \cdot b^{k_n}$ liegt in $I_1 \cdot \ldots \cdot I_n$ und damit folgt $b \in Rad(I_1 \cdot \ldots \cdot I_n) = Rad(I_1 \cap \ldots \cap I_n)$, was die Gleichheit $Rad(I_1 \cap \ldots \cap I_n) = Rad(I_1) \cap \ldots \cap Rad(I_n)$ zeigt.

d) Da R Noethersch ist, sind sowohl I als auch $Rad(I)$ endlich erzeugt. Sei $Rad(I) = (x_1, \ldots, x_k)$ von den Elementen $x_1, \ldots, x_k$ erzeugt, dann existieren natürliche Zahlen $n_1, \ldots n_k$ mit $x_i^{n_i} \in I$; dabei seien die n_i minimal gewählt. Wir setzen $n := n_1 + \ldots + n_k + k - 1$.

Das Ideal $(Rad(I))^n$ wird von den Produkten $x_1^{r_1} \cdot \ldots x_k^{r_k}$ mit $r_1 + \ldots + r_k = n$ erzeugt. Wenn nun $r_i < n_i$ für alle i gelten würde (damit gilt $x_i^{r_i} \notin I$ wegen der Minimalität der n_i), dann erhielten wir aus $n = r_1 + \ldots r_k < n_1 + \ldots n_k = n - k + 1$, dass $k < 1$ ist, was nicht möglich ist, da $Rad(I)$ von zumindest einem Element erzeugt sein muss. Daher muss $r_i \geq n_i$ für mindestens einen Index i gelten und somit besitzt jedes der Produkte $x_1^{r_1} \cdot \ldots x_k^{r_k}$ mindestens einen Faktor in I und damit gilt $x_1^{r_1} \cdot \ldots x_k^{r_k} \in I$. Insgesamt folgt also $(Rad(I))^n \subseteq I$ für ein $n \in \mathbb{N}$, $n \neq 0$. □

Bemerkung. Der vorige Satz zeigt auch, dass der Durchschnitt von zwei P-primären Idealen ebenfalls P-primär ist. Besitzen hingegen zwei Primärideale Q_1 und Q_2 unterschiedliche zugehörige Primideale P_1 und P_2, dann ist $Q_1 \cap Q_2$ kein Primärideal mehr:

Wegen $P_1 \neq P_2$ existiert oBdA ein $a \in P_2$ mit $a \notin P_1$. Wegen $a \in P_2$ gilt $a^n \in Q_2$ für ein $n \in \mathbb{N}$. Da nach Voraussetzung $Q_1 \supset Q_1 \cap Q_2$ gilt, existiert ein $q_1 \in Q_1 \backslash Q_1 \cap Q_2$ mit $a^n q_1 \in Q_1 \cap Q_2$. Wäre $Q_1 \cap Q_2$ primär, dann muss wegen $q_1 \notin Q_1 \cap Q_2$ ein $m \in \mathbb{N}$ existieren mit $(a^n)^m \in Q_1 \cap Q_2$. Daraus folgt aber $a^n \in P_1$ und wegen der Primeigenschaft von P_1 müsste auch a in P_1 liegen, was im Widerspruch zur Annahme $a \notin P_1$ steht.

Definition 3.2.11. *Sei I ein Ideal in einem kommutativen Ring R. Die Primärzerlegung von $I = Q_1 \cap \ldots \cap Q_r$ heißt reduziert, wenn keines der Primärideale Q_i den Durchschnitt aller anderen umfasst und für alle Q_i die zugehörigen Primideale verschieden sind. In diesem Fall bezeichnet man Q_i als Primärkomponente von I und spricht auch von einer Zerlegung von I in Primärkomponenten.*

Beispiel. Im Beispiel zu Satz 3.2.2 hatten für das Ideal $I = (4, 2x, x^2)$ zwei Primärzerlegung angegeben:

$$I = (4, 2x, x^2) = (4, x) \cap (2, x^2).$$

Dabei ist klarerweise die erste Zerlegung reduziert, da nur ein Primärideal vorhanden ist. Dagegen ist die zweite Zerlegung nicht reduziert, da zu den beiden Primäridealen $(4, x)$ und $(2, x^2)$ dasselbe Primideal gehört, nämlich $(2, x)$.

Wie später gezeigt wird, ist bei reduzierten Zerlegungen die Anzahl der auftretenden Primärideale eindeutig bestimmt (Satz 3.2.16).

Satz 3.2.12 (Zweiter Zerlegungssatz)**.** *Sei I ein Ideal in einem kommutativen Ring R. Wenn I eine Primärzerlegung besitzt, dann besitzt I auch eine reduzierte Primärzerlegung.*

Beweis. Es habe I die Primärzerlegung $I = Q_1 \cap ... \cap Q_n$. Falls ein Q_i den Durchschnitt der restlichen Primärideale enthält,

$$Q_i \supseteq Q_1 \cap ... \cap Q_{i-1} \cap Q_{i+1} \cap ... \cap Q_n,$$

so kann man es klarerweise weglassen. Entfernt man auf diese Weise alle überflüssigen Primärideale, so erhält man, wenn man eine geeignete Umindizierung vornimmt, $I = Q_1 \cap ... \cap Q_m$, wo keines der $Q_j,\ j = 1, ..., m$, den Durchschnitt der übrigen Primärideale enthält. Betrachtet man nun die zugehörigen Primideale $P_j,\ j = 1, ..., m$, so können entweder bereits alle verschieden sein, womit alles bewiesen ist. Oder es kommen darunter gleiche vor, wobei wieder nach Umindizierung $P_1, ..., P_r$ die verschiedenen Primideale seien. Zum Primideal $P_i,\ i = 1, ..., r$, mögen die Primärideale $Q_{i_1}, ..., Q_{i_l}$ gehören. Nach Lemma 3.2.10,(i) ist dann auch der Durchschnitt $Q_i' := Q_{i_1} \cap ... \cap Q_{i_l}$ P_i-primär. Damit hat man die gesuchte reduzierte Darstellung gefunden, nämlich $I = Q_1' \cap ... \cap Q_r'$. □

3.2.2 Eindeutigkeit der Zerlegung in Primärkomponenten

Definition 3.2.13. *Seien I und J Ideale eines kommutativen Ringes R. Die Menge*

$$I : J = \{r \in R : rJ \subseteq I\}$$

heißt Idealquotient von I nach J.

Im Hauptidealring $\mathbb{Z}$ gilt für den Idealquotienten $(m) : (n) = \{r \in \mathbb{Z} : r \cdot n \equiv 0(m)\}$:

$$(m) : (n) = (\frac{m}{ggT(m,n)})$$

nach der Kürzungsregel für Kongruenzen ($ac \equiv bc(m) \Leftrightarrow a \equiv b\ (\frac{m}{ggT(c,m)})$). Speziell ist

$$(m) : (n) = (1) = \mathbb{Z}, \text{ wenn } (m) \subseteq (n) \text{ und } (m) : (n) = (m), \text{wenn } ggT(m,n) = 1.$$

Wie aus der Definition sofort folgt, gilt der eine Extremfall für den Idealquotienten allgemein:

$$I : J = R \Leftrightarrow J \subseteq I.$$

Weitere Eigenschaften des Idealquotienten beschreiben wir im nächsten

Satz 3.2.14. *Seien I, J, K Ideale in einem kommutativen Ring R. Dann sind folgende Eigenschaften erfüllt:*

a) $I : J$ ist ein Ideal in R mit $I \subseteq I : J$. Ferner ist es das größte Ideal K mit der Eigenschaft $K \cdot J \subseteq I$.

b) $(I \cap J) : K = (I : K) \cap (J : K)$

c) $(I : J) : K = I : (JK) = (I : K) : J$.

Beweis.

a) Seien $r_1, r_2 \in I : J$, dann gilt für jedes $j \in J$: $r_1 j \in I$ und $r_2 j \in I$. Da I ein Ideal ist, folgt $(r_1 - r_2)j = r_1 j - r_2 j \in I$ und damit liegt $r_1 - r_2$ in $I : J$. Für $r \in R$ ist ebenfalls $(rr_1)j = r(r_1 j) \in I$ für beliebiges $j \in J$ und demnach $rr_1 \in I : J$. $I \subseteq I : J$ folgt aus der Idealeigenschaft von I; die Maximalität von $I : J$ folgt aus der Definition des Idealquotienten.

b) Sei $r \in (I \cap J) : K$, das heißt $rj \in I \cap J \subseteq I$ und $rj \in I \cap J \subseteq J$ für alle $j \in K$. Daher gilt $r \in I : K$ und $r \in J : K$ und somit $r \in (I : K) \cap (J : K)$. Es ist also $(I \cap J) : K \subseteq (I : K) \cap (J : K)$. Liest man die Argumentation von hinten nach vorne, so folgt die umgekehrte Inklusion.

c) Es ist

$$x \in (I : J) : K \Leftrightarrow x \cdot K \subseteq I : J \Leftrightarrow (x \cdot K)J \subseteq I \Leftrightarrow x(JK) \subseteq I \Leftrightarrow x \in I : (JK).$$

Der Rest folgt wegen $JK = KJ$. □

Für P-primäre Ideale Q in Noetherschen Integritätsbereichen gilt:

Satz 3.2.15. *Sei R ein Noetherscher Ring mit Einselement und seien I ein Ideal von R sowie Q ein Primärideal mit zugehörigem Primideal P ebenfalls von R.*

a) Für $I \not\subseteq P$ folgt $Q : I = Q$.

b) Für $I \subseteq P$, $I \not\subseteq Q$ gilt $Q \subset Q : I \subset R$. Ferner folgt nur aus $I \not\subseteq Q$, dass $Q : I$ ein P-primäres Ideal ist.

c) Für $I \subseteq Q$ folgt $Q : I = R$.

Beweis.

a) Ist $x \in Q$, so ist $xi \in Q$ für alle $i \in I$, da Q ein Ideal ist. Daher folgt $Q \subseteq Q : I$. Um die umgekehrte Inklusion zu zeigen, sei $x \in Q : I$, das heißt $xI \subseteq Q$. Wäre $x \notin Q$, so folgt aus der Charakterisierung der Eigenschaft P-primär (Satz 3.2.9, (ii)), dass $I \subseteq P$, im Widerspruch zur Voraussetzung. Also gilt $x \in Q$ und daher $Q : I \subseteq Q$.

b) Sei $n \in \mathbb{N}$ derart, dass $P^n \subseteq Q \subseteq P$ (vgl. Satz 3.2.10 d)) und $P^{n-1} \not\subseteq Q$ gilt. Wegen $I \subseteq P$ erhalten wir $IP^{n-1} \subseteq P^n \subseteq Q$, also $P^{n-1} \subseteq Q : I$. Weil $P^{n-1} \not\subseteq Q$, muss Q echt in $Q : I$ enthalten sein. Andererseits gilt $1 \notin Q : I$, weil $I \not\subseteq Q$ ist und damit $Q \subset Q : I \subset R$.

Um noch zu zeigen, dass für $I \not\subseteq Q$ der Idealquotient in P enthalten ist, nehmen wir indirekt an, dass ein $a \in Q : I$ existiert mit $a \notin P$. Sei weiters $b \in I \backslash Q$, dann liegt das Produkt ab in Q, wegen $(Q : I)I \subseteq Q \subseteq P$. Damit gilt $ab \in P$, aber $a \notin P$ und $b \notin P$, was im Widerspruch zur Primeigenschaft von P steht. Daher kann es kein solches $a \in Q : I$ geben, das nicht auch in P liegt. Dass P das gesuchte Radikal von $Q : I$ ist, folgt aus Satz 3.2.10 b), mit dem die Minimalität von P gewährleistet ist.

c) haben wir schon oben angeführt. □

Bemerkungen. Wir haben schon mit Idealquotienten gearbeitet und zwar bei den Beweisen der Sätze 3.1.6 und 3.2.2.

Satz 3.2.16. *(Erster Eindeutigkeitssatz) Sei R Noethersch und I ein Ideal von R. Wenn*

$$I = Q_1 \cap \ldots \cap Q_l = Q'_1 \cap \ldots \cap Q'_{l'}$$

zwei reduzierte Primärzerlegungen besitzt, dann stimmen die Anzahl der Komponenten und die zugehörigen Primideale beider Darstellungen überein.

Beweis. Ist I Primärideal. dann ist die Behauptung trivialerweise erfüllt. Sei daher I kein Primärideal. Wir führen einen Induktionsbeweis nach der Anzahl der Komponenten:

Für

$$I = Q_1 \cap \ldots \cap Q_l = Q'_1 \cap \ldots \cap Q'_{l'}$$

sei $\{P_1, \ldots, P_l, P'_1, \ldots, P'_{l'}\}$ die Menge der zugehörigen Primideale der Q_i und Q'_i. Als endliche Menge besitzt sie ein maximales Element, sei oBdA P_1 maximal.

Behauptung: P_1 ist auch für eines der Q'_is auf der rechten Seite der Darstellung zugehöriges Primideal. Wir nehmen an, dass die Behauptung falsch ist und bilden den Idealquotienten nach Q_1 von I:

Für die linke Seite gilt:

$$I : Q_1 = (Q_1 \cap \ldots \cap Q_l) : Q_1 = (Q_1 : Q_1) \cap \ldots \cap (Q_l : Q_1)$$

und für die rechte:

$$I : Q_1 = (Q'_1 \cap \ldots \cap Q'_{l'}) : Q_1 = (Q'_1 : Q_1) \cap \ldots \cap (Q'_{l'} : Q_1).$$

Für alle $P_i,\ i > 1$, und $P'_k,\ k > 1$, gilt $Q_1 \not\subseteq P_i,\ Q_1 \not\subseteq P'_i$. Angenommen es existierten $P_i \neq P_1$ mit $Q_1 \subseteq P_i$, dann ist $P_1 = (\bigcap_{j \in J} P_j^{(1)})$, wo $P_j^{(1)},\ j \in J$, sämtliche Primideale sind, die Q_1 umfassen. Insbesondere gehört dann P_i dazu, so dass $P_1 \subseteq P_i$ und wegen $P_1 \neq P_i$ weiter $P_1 \subset P_i$. Das ist ein Widerspruch zur Maximalität von P_1. Daher ist $Q_1 \not\subseteq P_i$ für alle $i > 1$. Ein analoges Argument gilt auch für die P'_k: $Q_1 \not\subseteq P'_k$ für alle $k \geq 1$.

Aus $Q_1 \not\subseteq P_i,\ i > 1$, und $Q_1 \not\subseteq P'_k,\ k \geq 1$, folgt nach Lemma 3.2.14, 4) für die Idealquotienten:

$$Q_i : Q_1 = Q_i,\ i = 2, ..., l, \quad \text{und analog} \quad Q'_k : Q_1 = Q'_k,\ k = 1, ..., l'.$$

Mit Lemma 3.2.14, 3) ergibt sich $Q_1 : Q_1 = R$ und insgesamt für $I : Q_1$:

$$R \cap Q_2 \cap \ldots \cap Q_l = Q'_1 \cap Q'_2 \cap \ldots \cap Q'_{l'}.$$

Da die rechte Darstellung die Primärzerlegung von I ist und die linke auf $Q_2 \cap \ldots \cap Q_l$ verkürzt werden kann, erhalten wir einen Widerspruch zur Voraussetzung, dass beide Darstellungen reduziert sind.

Somit muss die Behauptung wahr sein, also P_1 auch zugehöriges Primideal für genau eines der Q'_i sein. Wir ändern die Indizierung der Q_i aus der rechten Darstellung derart, dass Q'_1 eben P_1-primär, also $P'_1 = P_1$ gilt.

Weiters nehmen wir oBdA an $l \leq l'$ an. Wir beweisen, dass $l = l'$ und $P'_i = P_i$ nach geeigneter Umindizierung gilt. Für Ideale, die sich durch weniger als l Primärkomponenten in einer reduzierten Darstellung darstellen lassen, sei die Aussage bereits bewiesen.

Wir bilden für unsere Darstellung von

$$I = Q_1 \cap \ldots \cap Q_l = Q'_1 \cap \ldots \cap Q'_{l'}$$

(Q_1 und Q'_1 sind P_1-primär) den Idealquotienten nach $Q_1Q'_1$:

$$(Q_1 : Q_1Q'_1) \cap \ldots \cap (Q_l : Q_1Q'_1) = (Q'_1 : Q_1Q'_1) \cap \ldots \cap (Q'_{l'} : Q_1Q'_1).$$

Es ergibt sich für die Idealquotienten:

$$\begin{aligned} Q_i : Q_1Q'_1 &= Q_i,\ i = 2, ..., l, \\ Q'_k : Q_1Q'_1 &= Q'_k,\ k = 2, ..., l'. \end{aligned}$$

nach Lemma 3.2.14, 4), da $Q_1Q'_1 \not\subseteq P_i$ für alle $i > 1$ und $Q_1Q'_1 \not\subseteq P'_k$ für alle $k > 1$. (Wäre beispielsweise $Q_1Q'_1 \subseteq P_i$, so würde nach der Bemerkung zu Lemma 3.2.14, 1. der Widerspruch $Q_1 \subseteq P_i$ oder $Q'_1 \subseteq P_i$ folgen, da P_i Primideal ist.) Wiederum nach Lemma 3.2.14, 3) gilt für $i = 1$:

$$Q_1 : Q_1Q'_1 = R \ \text{ und } \ Q'_1 : Q_1Q'_1 = R$$

wegen $Q_1Q'_1 \subseteq Q_1$ und $Q_1Q'_1 \subseteq Q'_1$. Wir erhalten nun für das Ideal $I : Q_1Q'_1$:

$$I : Q_1Q'_1 = R \cap Q_2 \cap \ldots \cap Q_l = R \cap Q'_2 \cap \ldots \cap Q'_{l'},$$

dessen reduzierte Darstellung aus $l - 1$ bzw. $l' - 1$ Komponenten besteht. Nach Induktionsvoraussetzung gilt $l - 1 = l' - 1$ und damit $l = l'$. Weiters folgt aus des Induktionsvoraussetzung, dass je ein Q_i von der linken Seite und ein Q'_k von der rechten Seite dasselbe zugehörige Primideal P_i besitzen. □

Eine Erweiterung von Satz 3.2.16 ist folgender

Satz 3.2.17. *Sei $I = Q_1 \cap \ldots \cap Q_n$ eine reduzierte Primärzerlegung von I mit P_i-primären Q_is. Dann gilt $P_i = Rad(I : (x))$ für ein $x \in R$. Die Anzahl der Primideale P_i hängt nur von I und nicht von der Wahl der Primärkomponenten Q_i ab.*

Ein *Beweis* findet sich in [Spi94], Theorem 6.22 (S. 103).

Bemerkung. Die Wahl von $x \in R$ ist entscheidend:

$$\begin{aligned} x \notin P_i \quad &\Rightarrow I : (x) = (Q_1 : (x)) \cap \ldots \cap (Q_{i-1} : (x)) \cap Q_i \cap (Q_{i+1} : (x)) \cap \ldots \cap (Q_n : (x)) \\ &\Rightarrow Rad(I : (x)) = \textstyle\bigcap_{j=1, j\neq i}^{n} Rad(\underbrace{Q_j : (x)}) \cap P_i \\ &\qquad\qquad\qquad\qquad = Q_j \quad \Leftrightarrow x \notin P_j \text{ nach Satz } 3.2.15, a) \\ &\qquad\qquad\qquad\qquad = R \quad \Leftrightarrow x \in Q_j \\ x \in I \quad &\Rightarrow I : (x) = R \end{aligned}$$

Die Herausforderung besteht nun darin, dass wir die P_is durch die geeignete Wahl von $x \notin P_i$ bestimmen sollten ohne P_i zu kennen. Um solche x zu finden, können wir zumindest die Suche auf multiplikativ abgeschlossene Mengen eingrenzen, denn für ein Primideal P folgt aus $a, b \notin P$ notwendigerweise, dass $ab \notin P$; anders gesehen ist also $R \backslash P$ multiplikativ abgeschlossen.

Dieser Gedanke motiviert folgende

Definition 3.2.18. *Sei R ein kommutativer Ring, I ein Ideal von R und S eine nichtleere multiplikativ abgeschlossene Menge von R. Wir bezeichnen die Menge*

$$I_S = \{r \in R : \exists s \in S \text{ mit } sr \in I\}$$

als S-Komponente von I.

Aus der Definition folgen unmittelbar folgende beide Eigenschaften von I_S:

Lemma 3.2.19. *Seien R, I und S wie soeben, dann gilt für I_S:*

1. I_S ist ein Ideal von R.

2. $I \subseteq I_S$.

Beweis.

1. Seien $r_1, r_2 \in I_s$. Dann existieren $s_1, s_2 \in S$ mit $r_1 s_1 \in I$, $r_2 s_2 \in I$ und damit folgt auch $s_2(r_1 s_1), s_1(r_2 s_2) \in I$. Somit ist $s_1 s_2 (r_1 - r_2) = s_2(s_1 r_1) - s_1(s_2 r_2) \in I$, also $r_1 - r_2 \in I_S$. Für $r \in R$ folgt für $r_1 \in I_S$ auch $r(r_1 s_1) = (r r_1) s_1 \in I$ und somit gilt $r r_1 \in I_S$.

2. Denn für $a \in I$ folgt für alle $r \in R$: $ra \in I$. Also gilt auch für die Teilmenge S: $sa \in I$ für alle $s \in S$, das heißt $a \in I_S$. □

Der nächste Satz zeigt, welche Bedeutung die S-Komponente auf die reduzierte Primärzerlegung besitzt:

Satz 3.2.20. *Seien R ein Noetherscher Ring, S eine multiplikativ abgeschlossene Teilmenge von R und $I = Q_1 \cap \ldots \cap Q_h \cap Q_{h+1} \cap \ldots \cap Q_r$ eine reduzierte Primärzerlegung*

eines Ideals I aus R mit $Q_i \cap S = \emptyset$ für $1 \leq i \leq h$. Dann lässt sich die S-Komponente von I darstellen als $I_S = Q_1 \cap \ldots \cap Q_h$.

Bemerkung. Für $h = 0$ soll dies $I_S = R$ bedeuten.

Beweis. Wir zeigen zunächst $I_S \subseteq Q_1 \cap \ldots Q_h$. Sei dazu $x \in I_S$, dann existert ein $s \in S$ mit $sx \in I$ und demnach $sx \in Q_i$ für alle i, $1 \leq i \leq r$. Nach Voraussetzung gilt $Q_i \cap S = \emptyset$ für $1 \leq i \leq h$, daher folgt $s \notin Q_i$. Da S multiplikativ abgeschlossen ist, gilt $s^n \in S$ für $n \geq 1$ und damit $s^n \notin Q_i$ für alle $n \in \mathbb{N}$, $1 \leq i \leq h$. Also liegt s nach Lemma 3.2.7 nicht im zu Q_i zugehörigen Primideal P_i, $1 \leq i \leq h$.

Wenn $s \notin P_i$ und $sx \in Q_i$ für $1 \leq i \leq h$ ist, dann muss $x \in Q_i$ gelten; denn angenommen $x \notin Q_i$, dann muss $s^n \in Q_i$ sein für ein $n \in \mathbb{N}$, da Q_i Primärideal ist. Wenn $s^n \in Q_i$ gilt, dann ist aber nach Satz ... auch $s \in P_i$, ein Widerspruch zur Annahme $s \notin P_i$. Damit ist gezeigt, dass $x \in Q_i$, $1 \leq i \leq h$, gilt, was $I_S \subseteq Q_1 \cap \ldots Q_h$ impliziert.

Sei nun umgekehrt $x \in Q_1 \cap \ldots \cap Q_h$. Nach Voraussetzung existieren $s_j \in S \cap Q_j$ für $h + 1 \leq j \leq r$ und da S multiplikativ abgeschlossen ist, liegt das Produkt dieser s_j, das wir mit $s = s_{h+1} \cdot \ldots \cdot s_r$ bezeichnen, in S. Weiters gilt, dass einerseits $sx \in Q_1 \cap \ldots \cap Q_h$ liegt weil die Menge ein Ideal bildet und andererseits $sx \in Q_{h+1} \cap \ldots \cap Q_r$ gilt wegen der Wahl von s. Folglich liegt sx in I und daher gilt $x \in I_S$, das heißt $Q_1 \cap \ldots Q_h \subseteq I_S$. □

Die zugrundeliegende Idee ist also in Satz 3.2.20 zu einem gegebenen Ideal I in reduzierter Primärdarstellung eine multiplikativ abgeschlossene Teilmenge S des Ringes heranzuziehen, um eine – eindeutige, wie wir noch später sehen werden – Darstellung für den Teiler I_S von I zu erzielen. Dabei ist die Wahl von S entscheidend um I_S möglichst minimal, wenn möglich gleich I zu machen. Dazu wäre die geeignete Bedingung für S: $S \cap Q_i = \emptyset$ für alle $i = 1, ..., r$, denn dann gilt $I_S = I$. Dagegen liefert der Fall $S \cap Q_i \neq \emptyset$ für alle $i = 1, ..., r$ gar keine Aussage, denn dann ist $I_S = R$.

Bemerkung. Die multiplikativ abgeschlossene Menge S unterteilt also die Primärkomponenten Q_i in solche, die S treffen und S nicht treffen. Aus $S \cap Q_i = \emptyset$ folgt aus der multiplikativen Abgeschlossenheit von S, dass $S \cap P_i = \emptyset$ gilt. Fassen wir die Primärkomponenten Q_i mit $Q_i \cap S = \emptyset$ zur Menge $\{Q_1, \ldots Q_h\}$ zusammen, dann gilt für die Menge der zugehörigen Primideale $\{P_1 \ldots, P_h\}$ dass keines der P_i Teiler von P_j, $h + 1 \leq j \leq r$ sein kann, weil $P_j \cap S \neq \emptyset$ ist. Innerhalb der Menge $\{Q_1, \ldots, Q_h\}$ kann aber sehr wohl für die zugehörigen Primideale $P_i \supseteq P_j$, $i \neq j$, $1 \leq 1, j \leq h$ gelten.

Wir bezeichnen die Menge $\{Q_1, \ldots, Q_h\}$ als *isoliert*, wenn für die Menge der zugehörigen Primideale $\{P_1, \ldots, P_h\}$ die Eigenschaft $P_i \not\supseteq P_j$ für alle $1 \leq i \leq h$, $h + 1 \leq j \leq r$ erfüllt ist. Ferner bezeichnen wir die isolierte Menge $\{Q_1, \ldots, Q_h\}$, da sie von der Wahl von S abhängig ist, als *die durch S bestimmte isolierte Komponente* von I.

Im nächsten Satz zeigen wir umgekehrt, dass zu einer isolierten Menge von Primärkomponenten die Menge der zugehörigen isolierten Primideale eindeutig die isolierte S-Komponente von I, d.h. I_S, festlegt.

Satz 3.2.21. *Seien R ein Noetherscher Ring und $I = Q_1 \cap \ldots \cap Q_h \cap Q_{h+1} \cap \ldots \cap Q_r$ die Darstellung eines Ideals I von R in reduzierter Primärdarstellung. Sei weiters $\{Q_1, \ldots, Q_h\}$ eine isolierte Menge von Primärkomponenten, dann ist der Durchschnitt $Q_1 \cap \ldots \cap Q_h$ durch die Angabe der zugehörigen Primideale $\{P_1, \ldots, P_h\}$ eindeutig bestimmt.*

Beweis. Wir konstruieren zur isolierten Menge $\{Q_1, \ldots, Q_h\}$ eine multiplikativ abgeschlossene Menge S, sodass $S \cap P_i = \emptyset$ für alle $1 \leq i \leq h$ gilt.

Dazu setzen wir

$$S = R\backslash(\bigcup_{i=1}^{h} P_i) = \bigcap_{i=1}^{h}(R\backslash P_i)$$

und zeigen, dass $R\backslash P_i$ für alle $1 \leq i \leq h$ multiplikativ abgeschlossen ist: Angenommen es existieren $a, b \in R\backslash P_i$ für deren Produkt $ab \notin R\backslash P_i$ gilt. Daher muss ab im Primideal P_i liegen und damit $a \in P_i$ oder $b \in P_i$ gelten. Dies widerspricht der Voraussetzung $a, b \notin P_i$. Da somit jede Komponente $R\backslash P_i$ multiplikativ abgeschlossen ist, ist es auch S.

Weiters gilt nach Voraussetzung $P_i \not\supseteq P_j$ für alle i, j mit $1 \leq i \leq h,\ h+1 \leq j \leq r$, d.h. es gibt ein $p \in P_j$, das nicht in P_i liegt. Nach Konstruktion muss daher $p \in S$ gelten und wir können Satz 3.2.20 heranziehen, aus dem eben folgt, dass der Durchschnitt $Q_1 \cap \ldots \cap Q_h$ genau der S-Komponente I_S von I entspricht. S haben wir hier durch die zugehörigen Primideale aus der isolierten Menge bestimmt, so dass dieser Durchschnitt durch sie eindeutig festgelegt ist. □

Korollar 3.2.22. *(Zweiter Eindeutigkeitssatz) Die isolierten Primärkomponenten in einer reduzierten Primärzerlegung eines Ideals I eines Noetherschen Ringes R sind eindeutig bestimmt.*

Beweis. Sei P_i isoliertes zugehöriges Primideal von Q_i. Dann bilden wir die nichtleere multiplikativ abgeschlossene Menge $S = R\backslash P_i$. Für alle anderen P_j existiert ein p_j mit $p_j \notin P_i$ und somit $p_j \in S$. Somit folgt $I_S = Q_i$. I_S ist durch I und S, also durch I und P_i eindeutig bestimmt. Die isolierten P_is sind nach Satz 3.2.17 wiederum durch I eindeutig bestimmt. □

Wählen wir wie in Satz 3.2.21 für S die Menge $S = R\backslash P$, so bezeichnet man die Menge I_S in diesem speziellen Fall als die *P-Komponente* von I. Zu der P-Komponente eines Ideals führen wir folgende Teilmengen ein:

Definition 3.2.23. *Sei P ein Primideal eines kommutativen Ringes R und sei $m \in \mathbb{N}$. Die Menge*

$$P^{(m)} := \{r \in R | \exists s \in R\backslash P : rs \in P^m\}$$

heißt symbolische Potenz von P.

Die Eigenschaften von symbolischen Potenzen sind im nächsten Satz zusammengefasst.

Satz 3.2.24. *Sei P ein Primideal eines kommutativen Ringes und sei $m \in \mathbb{N}$.*

a) $P^m \subseteq P^{(m)} \subseteq P$

b) $P^{(m)}$ ist ein Primärideal.

c) Wenn P^m eine reduzierte Primärzerlegung $P^m = Q_1 \cap \ldots \cap Q_n$ besitzt mit P_i-primären Q_i $(i = 1, \ldots, n)$, dann ist P genau eines der Elemente von $\{P_1, \ldots, P_n\}$ und $P \subseteq P_i$ für alle $1 \leq i \leq n$. Darüber hinaus ist $P^{(m)}$ die zugehörige Primärkomponente von P.

Beweis.

a) Sei $r \in P^m$. Da P^m Ideal ist, folgt $rs \in P^m$ für alle $s \in R$, also gilt $P^m \subseteq P^{(m)}$. Ist andererseits $r \in P^{(m)}$, so existiert ein $s \in R\backslash P$ mit $rs \in P^m \subseteq P$. Aus der Primeigenschaft von P folgt $r \in P$; daher gilt $P^{(m)} \subseteq P$.

b) Zuerst zeigen wir, dass $P^{(m)}$ ein Ideal ist: Seien $r_1, r_2 \in P^{(m)}$ mit $r_1 s_1, r_2 s_2 \in P^m$ für gewisse $s_1, s_2 \in R\backslash P$. Da P^m ein Ideal ist, gilt $P^m \ni s_2(s_1 r_1) - s_1(s_2 r_2) = s_1 s_2(r_1 - r_2)$ und damit $r_1 - r_2 \in P^{(m)}$. Für ein $r \in R$ gilt ebenfalls $r r_1 s_1 \in P^m$, also $r r_1 \in P^{(m)}$.

Wir zeigen nun, dass $P^{(m)}$ primär ist und verwenden dazu Satz 3.2.9. Die Eigenschaft (i), also $P^{(m)} \subseteq P \subseteq Rad(P^{(m)})$ gilt wegen dem eben gezeigten Teil a). Sei nun $rt \in P^{(m)}$. Dann ist $(rt)s \in P^m$ für ein $s \in R\backslash P$. Wenn $t \notin P$, dann ist $r(ts) \in P^m$ und $ts \in R\backslash P$ wegen der multiplikativen Abgeschlossenheit von $R\backslash P$. Also folgt $r \in P^{(m)}$, d.h. Eigenschaft (iii) ist erfüllt.

c) Gehen wir bei der Gleichung $P^m = Q_1 \cap \ldots \cap Q_n$ zu den Radikalen über, so erhalten wir $P = P_1 \cap \ldots \cap P_n$. Wegen $P_1 \cdot \ldots \cdot P_n \subseteq P_1 \cap \ldots \cap P_n = P$ folgt aus der Primeigenschaft von P, dass eines der P_i, es sei P_{i_0} in P enthalten ist. Wegen $P = P_1 \cap \ldots \cap P_n \subseteq P_i$ für $i = 1, \ldots, n$ folgt nun $P = P_{i_0}$ und $P \subset P_i$ für alle $i \neq i_0$, da die Darstellung von P^m reduziert war. Das liefert die Minimalität von P. Für $S = R\backslash P$ ist damit P das einzige Ideal mit der Eigenschaft $P \cap S = \emptyset$ und seine Primärkomponente Q_{i_0} ist isoliert. Die P-Komponente von P^m ist daher Q_{i_0}, also gilt $Q_{i_0} = P^{(m)}$ nach der Definition der symbolischen Potenz. □

Bemerkung. Wenn von Eindeutigkeit die Rede ist, dann nur im Sinne der zugehörigen Primideale. Wir erinnern uns, dass zu einem solchen Primideal P mehrere Primärideale existieren können, die alle P-primär sind.

Sind jedoch alle Primärkomponenten isoliert, also $P_i \not\supseteq P_j,\ i \neq j,\ i, j = 1, ..., r$, dann hat man sogar eine eindeutige Darstellung als Durchschnitt von Primäridealen erreicht.

Für spezielle Noethersche Ringe lässt sich diese Eigenschaft realisieren:

Satz 3.2.25. *Sei R ein Noetherscher Integritätsring mit Einselement, in dem jedes Primideal von R maximal ist. Dann lässt sich jedes Ideal $I \neq \{0\}, R$ eindeutig als Durchschnitt von Primäridealen darstellen.*

Beweis. Sei oBdA. $I = Q_1 \cap \ldots \cap Q_r$ eine reduzierte Primärzerlegung von I. Da nach Voraussetzung jedes Primideal maximal ist, gilt insbesondere für die zugehörigen Primideale $P_i : P_i \not\supseteq P_j,\ i \neq j,\ 1 \leq i, j \leq r$. Damit kann für die Primärideale Q_i, Q_j gelten:

$$(1)\ Q_i \supseteq Q_j \ \text{ bzw. } \ Q_i \subseteq Q_j \quad \text{oder} \quad (2)\ Q_i \not\supseteq Q_j.$$

Der erste Fall ist nicht möglich, da nach Voraussetzung die Primärzerlegung reduziert ist. Daher muss $Q_i \not\supseteq Q_j$ für alle $i \neq j,\ 1 \leq i, j \leq r$ gelten.

Wir setzen $S = R\backslash(\bigcup_{i=1}^{r} P_i)$ und erhalten wie bereits in Satz 3.2.21 gezeigt, eine multiplikativ abgeschlossene Menge. Für jede Primärkomponente Q_i gilt sodann wegen $S \cap P_i = \emptyset$ und $P_i \supset Q_i$ für alle i: $S \cap Q_i = \emptyset$. Nach Satz 3.2.20 lässt sich die isolierte S-Komponente als $I_S = Q_1 \cap \ldots \cap Q_r$ darstellen und nach Satz 3.2.21 ist diese Darstellung durch die zugehörigen Primideale eindeutig bestimmt. Nachdem $I = I_S$ gilt, ist damit alles gezeigt. □

Abschließend werden wir noch zeigen, dass die eindeutige Darstellung eines Ideals als Durchschnitt von Primäridealen unter den aus Satz 3.2.25 geltenden Voraussetzungen in eine Produktdarstellung überführt werden kann. Entscheidend ist dafür die Voraussetzung, dass jedes Primideal maximal ist, denn dann folgt mit dem nächsten Satz die notwendige Eigenschaft der Primärideale.

Satz 3.2.26. *Sei R ein Noetherscher Ring mit Eins, in dem jedes Primideal maximal ist. Zwei Primärideale Q_1, Q_2 aus R sind komaximal, d.h. $Q_1 + Q_2 = R$, genau dann, wenn die zugehörigen Primideale P_1, P_2, $P_1 \neq P_2$, aus R komaximal sind.*

Beweis.

($\Leftarrow$) Wenn jedes Primideal P maximal ist, dann folgt für ein $a \in R\backslash P$, dass $P + (a) = R$ gilt. Somit folgt für die beiden maximalen Ideale P_1, P_2, dass sie komaximal sind, also $P_1 + P_2 = R$ gilt.

Wir wählen ein $x \in Q_2$ so, dass $x \notin P_1$ gilt (ein solches Element muss existieren, denn sonst wäre Q_2 P_1-primär). Dann gilt $R = P_1 + (x)$. Somit existiert ein $a \in P_1$ mit $a + x = 1$ und ein $n \in \mathbb{N}$, sodass $a^n \in Q_1$ gilt. Wir betrachten $\underbrace{a^n}_{\in Q_1} = (1-x)^n = 1 - \underbrace{\sum_{k=1}^{n} (-1)^{k-1} x^k}_{\in Q_2}$

und folgern $1 \in Q_1 + Q_2$, also $Q_1 + Q_2 = R$.

($\Rightarrow$) Die Umkehrung ist klar. □

Zusammen mit dem vorigen Satz und dem nächsten erhalten wir schlussendlich eine *eindeutige Produktdarstellung für Ideale in Noetherschen Ringen mit Eins.*

Satz 3.2.27. *Sei R ein kommutativer Ring mit Eins. Wenn die Ideale $I_1, \ldots, I_n$ paarweise komaximal sind, dann gilt $I_1 \cap I_2 \cap \ldots \cap I_n = I_1 \cdot I_2 \ldots \cdot I_n$.*

Beweis. Wir führen einen Induktionsbeweis nach n. Für $n = 1$ ist nichts zu zeigen. Wir betrachten den Fall $n = 2$. Für $I_1 + I_2 = R$ erhalten wir $I_1 \cap I_2 = R(I_1 \cap I_2) = (I_1 + I_2)(I_1 \cap I_2) \subseteq I_1 \cdot I_2$. Die umgekehrte Inklusion $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ ist trivialerweise erfüllt.

Sei nun $n \geq 3$ und die Behauptung $I_1 \cap I_2 \cap \ldots \cap I_{n-1} = I_1 \cdot I_2 \cdot \ldots \cdot I_{n-1}$ stimmt für $n-1$ Ideale. Wir behaupten $I_n + J = R$ für $J := I_1 \cdot I_2 \cdot \ldots \cdot I_{n-1}$.

Weil $I_n + I_k = R$ für alle $k \neq n$ gilt, finden wir ein $x_k \in I_k$ und ein $y_k \in I_n$ mit $x_k + y_k = 1$. Damit gilt $J \ni \prod_{k=1}^{n-1} x_k = \prod_{k=1}^{n-1} (1 - y_k)$, also

$$\underbrace{\prod_{k=1}^{n-1} (1 - y_k)}_{\in J} = 1 - \underbrace{(\sum_{i=1}^{n} y_i - \sum_{i \neq j} y_i y_j + \sum_{i \neq j \neq k} y_i y_j y_k - + \ldots (-1)^{n-1} \prod_{i=1}^{n} y_i)}_{\in I_n},$$

damit $1 \in J + I_n$ und schließlich $J + I_n = R$. Unter Anwendung des Falles $n = 2$ erhalten wir $I_1 \cdot I_2 \cdot \ldots \cdot I_{n-1} \cdot I_n = J \cdot I_n = J \cap I_n = I_1 \cap I_2 \cap \ldots \cap I_n$. □

3.3 Moduln und ganze Ringerweiterungen

Wir starten diesen Abschnitt mit Grundsätzlichem über Moduln; alles Notwendige, was wir benötigen werden, ist hier zusammengefasst:

Definition 3.3.1. *Sei R ein Ring. Ein Modul über R oder kurz R-Modul ist eine abelsche Gruppe $(A,+)$ zusammen mit einer Operation von R auf A, also einer Abbildung $R\times A \to A$, $(r,a)\mapsto ra$, wobei für $a,b\in A$, $r,s,\in R$ die folgenden Bedingungen erfüllt sind:*

1) $r\cdot(a+b) = r\cdot a + r\cdot b$

2) $(r+s)\cdot a = r\cdot a + s\cdot a$

3) $(r\cdot s)\cdot a = r\cdot(s\cdot a)$.

Besitzt R ein Einselement e, so soll zusätzlich gelten:

4) $e\cdot a = a$ *für alle* $a\in A$.

Eine Untergruppe B von A heißt R-Submodul, wenn $r\cdot b\in B$, $\forall r\in R$, $b\in B$ gilt, d.h. B ist selbst ein Modul über R.

Bemerkung. Genauer heißt A R-Linksmodul. Da wir aber ausschließlich nur solche betrachten, sprechen wir kurz von R-Moduln bzw. auch nur von Moduln, wenn der Operatorenbereich R klar ist.

Beispiele.

1. Jeder Ring R ist selbst ein R-Modul.

2. Jedes Ideal von R ist ein R-(Sub-)Modul.

3. Der endliche Durchschnitt und die Summe von Untermoduln eines R-Moduls A sind ebenfalls Untermoduln von A.

4. Ist $R=K$ Körper, so sind die R-Moduln gerade die K-Vektorräume.

Analog zu Faktorringen nach einem Ideal I eines Rings R bildet zu einem gegebenen R-Modul A und einem Untermodul B von A die Menge $A/B = \{a\in A | a+B\}$ zusammen mit der Multiplikation $r\cdot(a+B) = ra+B$ einen R-Modul, den Faktormodul von A nach B.

Eine Abbildung $\varphi: A\to B$ zwischen zwei R-Moduln A,B heißt R-Modul-Homomorphismus, wenn für alle $a,b\in A$, $r\in R$

(i) $\varphi(a+b) = \varphi(a)+\varphi(b)$ und

(ii) $\varphi(ra) = r\varphi(a)$

erfüllt ist.

Ist φ bijektiv, so heißt φ R-Modul-Isomorphismus. Analog zu Ringen gilt auch der Homomorphie-Satz für Moduln:

Ist $\varphi : A \to B$ ein R-Modul-Homomorphismus, dann sind $\varphi(A)$ ein Untermodul von B, φ ein Untermodul von A und es gilt $R/ker\varphi \cong im\varphi$.

Sei weiters A ein R-Modul, dann ist für jedes $a \in A$ $\varphi_a : R \to A$ mit $\varphi_a(x) = xa$ ein R-Modul-Homomorphismus und wir bezeichnen den Kern von φ_a als *Annihilator* von a in R und schreiben $Ann_R(a) = \{x \in R | xa = 0\}$. Das Bild von φ_a wird mit $Ra = \{xa | x \in R\}$ bezeichnet und heißt der von a erzeugte Untermodul von A. Allgemein ist für einen R-Modul A der *Annihilator* von A definiert durch $Ann_R(A) = \{x \in R | xa = 0,\ \forall a \in A\}$.

Für eine beliebige Teilmenge $X \subseteq A$ nennt man $\sum_{x \in X} Rx$ den von X erzeugten Untermodul von A. Ist X endlich, so ist der von X erzeugte Untermodul endlich erzeugt.

Fassen wir einen Noetherschen Ring R als R-Modul auf, der auf sich selbst operiert, dann erfüllt jeder Untermodul von R, da er ein Ideal von R ist, die aufsteigende Kettenbedingung in R.

Wir verallgemeinern daher die Kettenbedingung auf Moduln:

Definition 3.3.2. *Ein Modul M heißt Noethersch, wenn jede aufsteigende Kette von Untermoduln $M_1 \subset M_2 \subset \ldots$ nach endlich vielen Schritten abbricht.*

Analog zu Idealketten, die die aufsteigende Kettenbedingung erfüllen, gilt folgender Satz:

Satz 3.3.3. *Sei M ein R-Modul, dann sind äquvivalent:*

1) M ist Noethersch.

2) Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element.

Wie der nächste Satz zeigt, überträgt sich bei Noetherschen Ringen R die aufsteigende Kettenbedingung auf endlich erzeugte R-Moduln:

Satz 3.3.4. *Sei R ein Noetherscher Ring und A ein R-Modul. Wenn A endlich erzeugt ist, dann ist jeder Untermodul von A endlich erzeugt.*

Den *Beweis* findet man in [Spi94], (11.17) Proposition (S. 210).

Bemerkung. Im Allgemeinen müssen in einem endlich erzeugten R-Modul M nicht alle Untermoduln von M endlich erzeugt sein. Ein Beispiel dazu findet man in Schwermer S. 197.

In Abschnitt 3.1 haben wir uns im Zuge des Hilbertschen Basissatzes 3.1.9 überlegt, dass sich bei einem Ring mit Einselement die Eigenschaft Noethersch zu sein auf gewisse Oberringe überträgt. Wir greifen hier die Idee nochmals auf und adaptieren sie für Moduln:

Da jeder Noethersche Ring als Modul aufgefasst werden kann, besteht der grundlegende Gedanke darin, Oberringe S von Noetherschen Ringen R mit Einselement als R-Moduln aufzufassen. Wenn nun S als R-Modul endlich erzeugt ist, dann ist der Ring S Noethersch.

Um nun feststellen zu können, ob S als R-Modul endlich erzeugt ist, betrachten wir vorerst folgenden Fall:

Sei R ein kommutativer Ring mit Einselement und S ein Oberring von R. Der Erweiterungsring $R[s] = \{r_0 + r_1 s + \ldots + r_n s^n | n \in \mathbb{N},\ r_i \in R\}$, der durch Adjunktion von $s \in S$ aus R entsteht, kann wegen $R \subseteq R[s]$ als R-Modul aufgefasst werden. $R[s]$ ist als R-Modul endlich erzeugt, wenn sich für ein gewisses $n \in \mathbb{N}$ s^n als R-Linearkombination von kleineren Potenzen von s darstellen lässt, d.h. $R[s] = R + Rs + Rs^2 + \ldots + Rs^{n-1}$, denn dann wird $R[s]$ von endlich vielen Elementen $1, s, \ldots, s^{n-1}$ erzeugt.

Dies motiviert folgende Definition

Definition 3.3.5. *Seien R und S kommutative Ringe, $R \subseteq S$.*

(i) Ein Element $s \in S$ heißt ganz über R, wenn $r_0, \ldots, r_{n-1} \in R$ existieren, sodass

$$s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0.$$

Wir sagen S ist ganz über R, wenn jedes Element $s \in S$ ganz über R ist. In diesem Fall bezeichnet $(S : R)$ eine ganze Ringerweiterung.

(ii) Ein Element $s \in S$ heißt algebraisch über R, wenn $r_0, \ldots, r_n \in R$ existieren, sodass

$$r_n s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0.$$

Wir sagen S ist algebraisch über R, wenn jedes Element $s \in S$ algebraisch über R ist. In diesem Fall bezeichnet $(S : R)$ eine algebraische Ringerweiterung.

(iii) Ein Element $s \in S$ heißt transzendent, wenn es nicht algebraisch ist über R. $(S : R)$ heißt dann transzendente Ringerweiterung.

Beispiele.

1. Aus der Definition folgt sofort, dass für kommutative Ringe R, S jedes ganze Element über R auch algebraisch ist.

2. Ist R Körper, so ist ein Element algebraisch genau dann, wenn es ganz ist.

3. Alle reellen Zahlen der Form $\sqrt[v]{a}$ mit $\mathbb{Q} \ni a > 0$ sind ganz über $\mathbb{Q}$, weil $\sqrt[v]{a}$ Nullstelle des Polynoms $x^n - a \in \mathbb{Q}[x]$ ist.

4. Die Eulersche Zahl e und π sind transzendent über $\mathbb{Q}$.

Wir werden nun mit folgendem Satz eine hilfreiche Charakterisierung von ganzen Größen in Bezug auf Moduln beweisen:

Satz 3.3.6. *Seien S ein kommutativer Ring mit Einselement e und $R \subseteq S$ ein Teilring mit $e \in R$. Dann sind für jedes $s \in S$ folgende Aussagen äquvivalent:*

1) s ist ganz über R

2) $R[s]$ ist endlich erzeugt als R-Modul

3) Es existiert ein Zwischenring $R[s] \subseteq Z \subseteq S$, der als R-Modul endlich erzeugt ist.

4) Es existiert ein $R[s]$-Modul A, der als R-Modul endlich erzeugt ist und der Annihilator von A in $R[s]$ besteht nur aus dem Nullelement, d.h. $Ann_{R[s]}(A) = \{0\}$.

Beweis.

1) $\Rightarrow$ 2) Da nach Voraussetzung s ganz über R ist, existieren $a_0, \dots a_{n-1} \in R$ mit

$$s^n = -a_0 - a_1 s - \ldots - a_{n-1} s^{n-1}.$$

Für jedes $k \geq 0$ gilt $s^{n+k} = -a_0 s^k - a_1 s^{k+1} - \ldots - a_{n-1} s^{n+k-1}$ und damit lässt sich jede Potenz $\geq n$ von s als Linearkombination von $1, s \dots, s^{n-1}$ darstellen. Somit erzeugen die n Elemente $1, s \dots, s^{n-1}$ den R-Modul $R[s]$.

2) $\Rightarrow$ 3) Die Aussage ist trivialerweise für $Z := R[s]$ erfüllt.

3) $\Rightarrow$ 4) Sei A ein als R-Modul endlich erzeugter Zwischenring mit der Eigenschaft $R[s] \subseteq A \subseteq S$. Wenn ein $x \in R[s]$ existiert, so dass $x \cdot a = 0 \ \forall a \in A$ gilt, dann folgt, da $e \in A : 0 = x \cdot e = x$, d.h. $Ann_{R[S]}(A) = \{0\}$.

4) $\Rightarrow$ 1) Sei $A = Ra_1 + \ldots Ra_n$ ein endlich erzeugter R-Modul. Da nach Voraussetzung A auch ein $R[s]$-Modul ist, gilt $sA \subseteq A$. Damit existieren Elemente $t_{ij} \in R$ $(1, \leq i, j \leq n)$, mit

$$\begin{aligned} sa_1 &= t_{11}a_1 + \ldots + t_{1n}a_n \\ sa_2 &= t_{21}a_1 + \ldots + t_{2n}a_n \\ \vdots & \quad \vdots \\ sa_n &= t_{n1}a_1 + \ldots + t_{nn}a_n \end{aligned}$$

die als Matrizengleichung

$$s \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & \ldots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \ldots & t_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

und folglich

$$\begin{pmatrix} t_{11} - s & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} - s & \ldots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \ldots & t_{nn} - s \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

dargestellt werden kann.

Wir setzen nun $T := (t_{ij})$ und $a := (a_j)$, dann lässt sich die obige Matrizengleichung kompakt als $(T - sI_n) \cdot a = 0$ darstellen (I_n ist die $(n \times n)$-Einheitsmatrix). Wir wollen zeigen, dass daraus folgt $det(T - sI_n) = 0$. Ist R Körper, so folgt dies sofort aus der Theorie der homogenen Gleichungssysteme. Im allgemeinen Fall müssen wir komplizierter schließen:

Wir behaupten zunächst, dass für die Lösung $a = (a_1, \ldots, a_n)$ des Gleichungssystems $(T - sI_n) \cdot x = 0$ gilt: $det(T - sI_n)a_i = 0$ für alle $1 \leq i \leq n$.

Wir konstruieren dazu eine Matrix A_i mit der Eigenschaft $detA_i = a_i$ und können aus dem Multiplikationssatz für Determinanten aus dieser Hilfsmatrix $det((T - sI_n) \cdot A_i) = det(T - sI_n)detA_i = det(T - sI_n)a_i$ berechnen.

Sei dazu

$$A_i = \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & 1 & \ldots & \ldots & \ldots & 0 \\ \vdots & \vdots & \ddots & \ldots & \ldots & \vdots \\ 0 & 0 & \ldots & a_i & \ldots & 0 \\ \vdots & \vdots & \ldots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & \ldots & 1 \end{pmatrix}$$

eine $(n \times n)$-Matrix mit Eintrag a_i an der Stelle (i,i). In der i-ten Spalte von $(T - sI_n)A_i$ erhalten wir die Einträge

$$\begin{pmatrix} t_{1i}a_i \\ t_{2i}a_i \\ \vdots \\ (t_{ii} - s)a_i \\ \vdots \\ t_{ni}a_i \end{pmatrix},$$

die restlichen Spalten von $(T - sI_n)A_i$ bleiben unverändert, also $((T - sI_n)A_i)_j = (T - sI_n)_j$ $\forall j \neq i$.

Um nun die Determinante von $(T - sI_n)A_i$ zu berechnen, addieren wir zur i-ten Spalte a_j-mal die Spalte $(T - sI_n)_j$ für alle $j \neq i$ und erhalten sodann:

$$\begin{pmatrix} t_{11} - s & t_{12} & \dots & \sum_{j=1}^{n} t_{1j}a_j - sa_1 & \dots & t_{1n} \\ t_{21} & t_{22} - s & \dots & \sum_{j=1}^{n} t_{2j}a_j - sa_2 & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ t_{i1} & t_{i2} & \dots & \sum_{j=1}^{n} t_{ij}a_j - sa_i & \dots & t_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{i2} & \dots & \sum_{j=1}^{n} t_{nj}a_j - sa_n & \dots & t_{nn} - s \end{pmatrix}.$$

Alle Einträge in der i-ten Spalte sind $= 0$, da nach Voraussetzung $(a_1, \dots a_n)$ die Gleichung $(T - sI_n)x = 0$ löst. Somit gilt $det((T - sI_n)A_i) = 0$ und folglich $det(T - sI_n)a_i = 0$ für alle $i = 1, \dots n$.

Nachdem A von $a_1, \dots, a_n$ erzeugt wird, erhalten wir $det(T - sI_n) \cdot A = 0$. Da der Annihilator von A in $R[s]$ nur aus der Null besteht, muss $det(T - sI_n) = 0$ gelten. Werten wir nun die Determinante von $T - sI_n$ aus, so erhalten wir

$$0 = det(T - sI_n) = (t_{11} - s)(t_{22} - s) \cdot \dots (t_{nn} - s) + Q_{n-2}$$

wobei Q_{n-2} ein Polynom vom Grad $\leq n - 2$ in s ist.

Es folgt

$$0 = det(T - sI_n) = (-1)^n s^n + (-1)^{n-1}(t_{11} + t_{22} + \dots + t_{nn}) + Q_{n-2},$$

und damit ist entweder $det(T - sIn)$ oder $-det(T - sIn)$ ein normiertes Polynom aus $R[x]$ mit Nullstelle s, also ist s ganz über R. □

Bemerkung. Die Bedingung $Ann_{R[s]}(A) = \{0\}$ aus 4) macht aus der Abbildung $f_A : R[s] \to A$ mit $f_a(x) = xa$, $a \in A$ wegen $kerf_A = Ann_{R[s]}(A)$ einen $R[s]$-Modul-Isomorphismus. Aus der Isomorphie $R[s]/\{0\} \cong R[s] \cong A \cong AR[s]$ erhalten wir, dass $R[s]$ genau dann als R-Modul erzeugt ist, wenn A es ist.

Mit dem obigen Satz haben wir nun gezeigt, dass Ringe der Gestalt $S = R[s]$, wenn s ganz über R ist, als R-Modul endlich erzeugt sind. Mit der Aussage 3) aus Satz 3.3.6 folgt für eine Ringerweiterung $(S : R)$: Wenn S als R-Modul endlich erzeugt ist, dann ist $(S : R)$ eine ganze Ringerweiterung.

Auch für beliebig viele ganze Elemente $s_1, \ldots s_n$ über R ist der Ring $R[s_1, \ldots, s_n]$ als R-Modul endlich erzeugt. Um das zu zeigen, „hantelt man sich“ bloß entlang der aufsteigenden Kette

$$R \subset R[s_1] \subset R[s_1, s_2] \subset \ldots \subset R[s_1, s_2, \ldots, s_n]$$

aufwärts und verwendet $R[s_1, \ldots s_{i-1}][s_i] = R[s_1, \ldots s_{i-1}, s_i]$.

Definition 3.3.7. *Seien R, S kommutative Ringe mit demselben Einselement und $R \subseteq S$. Die Menge aller ganzen Größen von S über R heißt ganze Hülle von R in S.*

R heißt ganz abgeschlossen in S, wenn die ganze Hülle von R in S genau R ist. Ist die ganze Hülle von R in S gleich S, so heißt S ganz über R oder ganze Ringerweiterung von R.

Wir sagen kurz R ist ganz abgeschlossen, wenn R Integritätsring und ganz abgeschlossen in seinem Quotientenkörper K ist, also die ganze Hülle von R in K genau R ist oder anders ausgedrückt, wenn jedes ganze Element aus K in R liegt.

Beispiel. $\mathbb{Z}$ ist ganz abgeschlossen in $\mathbb{Q}$, aber nicht in $\mathbb{C}$, da $i \in \mathbb{C}$ als Lösung von $x^2 + 1 = 0$ ganz über $\mathbb{Z}$ ist.

Passend dazu zeigen wir:

Satz 3.3.8. *Jeder faktorielle Ring ist ganz abgeschlossen.*

Beweis. Sei R ein faktorieller Ring, K der Quotientenkörper von R und $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ ein Polynom über R mit der Nullstelle $\frac{r}{s} := rs^{-1} \in K$, wobei $r, s \in R$ und r, s teilerfremd sind.

Wir zeigen, dass $\frac{r}{s} \in R$ gilt, falls $\frac{r}{s}$ ganz ist, also $a_n = e$ gilt.

Multiplizieren wir $0 = f(\frac{r}{s}) = a_0 + a_1\frac{r}{s} + a_2(\frac{r}{s})^2 + \ldots + (\frac{r}{s})^n$ mit s^n, so erhalten wir $0 = a_0s^n + a_1s^{n-1} + a_2s^{n-2} + \ldots + \ldots a_{n-1}r^{n-1}s + r^n$. Da s sowohl 0 also auch die ersten n Summanden teilt, folgt $s|r^n$. Nach Voraussetzung sind r und s teilerfremd, somit muss $s|e$ erfüllt sein, d.h. s ist eine Einheit und $\frac{r}{s} \in R$. □

Kehren wir nun zu unserer anfänglichen Problemstellung der Zerlegung von Idealen in Noetherschen Ringen mit Einselement zurück.

In Abschnitt 3.2 haben wir gezeigt, dass sich jedes Ideal als Durchschnitt von endlich vielen Primäridealen darstellen lässt:

$$I = Q_1 \cap \ldots \cap Q_h \tag{3.3}$$

wobei die Darstellung im allgemeinen nicht eindeutig ist (nur die Anzahl der Primärideale muss übereinstimmen, vgl. Satz 3.2.16).

Fordern wir zusätzlich, dass in einem Noetherschen Ring jedes Primideal maximal ist, so wird die Darstellung 3.3 eindeutig und wir erhalten eine Produktdarstellung

$$I = Q_1 \cap \ldots \cap Q_h = Q_1 \cdot \ldots \cdot Q_h \tag{3.4}$$

nach den Sätzen 3.2.25, 3.2.26 und 3.2.27.

Im folgenden Satz zeigen wir, dass die Primärideale in der Produktdarstellung Primidealpotenzen sind, wenn wir die ganze Abgeschlossenheit als Voraussetzung hinzunehmen.

Satz 3.3.9. *Sei R ein Noetherscher ganz abgeschlossener Integritätsring, in dem jedes Primideal maximal ist. Dann ist jedes Primärideal eine Primidealpotenz.*

Beweis. Die Voraussetzung, dass jedes Primideal maximal ist, ist äquivalent dazu, dass es zu keinem Primideal P_1 ein anderes Primideal $P_2 \neq P_1$ mit der Eigenschaft $P_2 \subseteq P_1$ geben kann. Es gilt daher, dass jedes maximale Primideal zugleich minimal ist.

Nach Voraussetzung ist also jedes Primideal $\neq 0$ maximal in R. Wir behaupten: Zu jedem P-primären Ideal Q existiert ein $m \in \mathbb{N}$ mit $Q = P^{(m)}$.

Für $Q = P$ ist die Behauptung trivialerweise erfüllt. Wir nehmen daher $Q \subset P$ an und wählen $a \neq 0 \in P,\ a \notin Q$. Es gilt

$$(a) \subset (a) : P. \tag{3.5}$$

Denn wenn $(a) = Q_1 \cap \ldots \cap Q_n$ eine reduzierte Zerlegung in Primärkomponenten ist, in der jedes Q_i P_i-primär mit Exponenten k_i ist, dann gilt $P_1^{k_1} \cdot \ldots \cdot P_n^{k_n} \subseteq Q_1 \cdot \ldots \cdot Q_n \subseteq Q_1 \cap \ldots \cap Q_n = (a) \subseteq P$. Da P prim ist, existiert ein Index i_0 mit $P_{i_0} \subseteq P$ und wegen der Minimalität von P folgt daraus $P_{i_0} = P$. Es folgt $Q_{i_0} : P \supset Q_{i_0}$ und $Q_i : P = Q_i$ für $i \neq i_0$, da $P_i \not\subseteq P$. Insgesamt gilt daher

$$(a) : P = (Q_1 \cap \ldots \cap Q_n) : P = (Q_1 : P) \cap \ldots \cap (Q_{i_0} : P) \cap \ldots \cap (Q_n : P) \supseteq Q_1 \cap \ldots \cap Q_n = (a).$$

Es bleibt noch zu zeigen, dass die Inklusion $(a) \subseteq (a) : P$ immer echt erfüllt ist: Wenn sie

das nicht wäre, dann hätten wir zwei reduzierte Primärzerlegungen $(a) = Q_1 \cap \ldots \cap Q_{i_0} \cap \ldots \cap Q_n = Q_1 \cap \ldots \cap (Q_{i_0} : P) \cap \ldots \cap Q_n$. Da P minimal ist, ist P isoliert für (a) und die P-Komponente von (a) ist nach Satz 3.2.22 eindeutig bestimmt, also folgt $Q_{i_0} = Q_{i_0} : P$. Dies widerspricht aber Satz 3.2.15, weil $a \notin Q$ und somit muss $(a) \subset (a) : P$ gelten.

Sei weiters $b \in ((a) : P) \backslash (a)$, also $bP \subseteq (a)$ und $b \notin (a)$: Wir betrachten das Element $\frac{b}{a}$ im Quotientenkörper von R; wegen $b \notin (a)$ folgt $\frac{b}{a} \notin R$. Wir bilden das Ideal $I := \frac{b}{a}P$, das wegen $a \in P$ ein Ideal von R ist. Angenommen $I \subseteq P$, dann sind, da R Noethersch ist, sowohl P als auch I endlich erzeugt und damit P ein endlich erzeugter $R[\frac{b}{a}]$-Modul und folglich ein endlich erzeugter R-Modul. Da weiters $rx = 0$, $r \in R[\frac{b}{a}]$, $x \in P$ beliebig dann und nur dann erfüllt ist, wenn $r = 0$ ist, folgt aus Satz 3.3.6, dass $\frac{b}{a}$ ganz über R ist. Da nach Voraussetzung aber R ganz abgeschlossen ist, muss $\frac{b}{a} \in R$ gelten. Die Annahme $I \subseteq P$ führt also zu einem Widerspruch, daher muss

$$I \not\subseteq P \tag{3.6}$$

gelten.

Sei nun k der Exponent von Q, also $P^k \subseteq Q$ und $P^i \not\subseteq Q$ für $i < k$. Es muss $(\frac{b}{a})^k Q \not\subseteq P$ gelten, denn sonst folgt aus $I^k = (\frac{b}{a})^k P^k \subseteq (\frac{b}{a})^k Q \subseteq P$ und der Primeigenschaft von P die Inklusion $I \subseteq P$. Wir wählen nun die größte Zahl $r \in \{0, 1, \ldots k-1\}$ mit $(\frac{b}{a})^r Q \subseteq P$ ($P^r \not\subseteq Q$) und setzen $J := (\frac{b}{a})^{r+1} Q$. Insbesondere gilt $J \not\subseteq P$.

Wegen $J = (\frac{b}{a})(\frac{b}{a})^r Q \subseteq (\frac{b}{a})P = I \subseteq R$ ist J Ideal von R und darüber hinaus gilt

$$JP^{r+1} = (\frac{b}{a})^{r+1} Q P^{r+1} = (\frac{b}{a}P)^{r+1} Q = I^{r+1} Q. \tag{3.7}$$

Wir behaupten, (3.7) impliziert $Q = P^{(r+1)}$. Um die Behauptung zu beweisen, betrachten wir eine reduzierte Zerlegung in Primärkomponenten von $P^{r+1} = P^{(r+1)} \cap Q_2 \cap \ldots \cap Q_n$, bei der alle Q_is P_i-primär sind und alle P_is paarweise verschieden sind. Aus Satz 3.2.24 wissen wir, dass $P^{(r+1)}$ eine Primärkomponente von P^{r+1} mit Primideal P ist. Wir setzen $A := Q_2 \cap \ldots Q_n$. Weil $P^{(r+1)} AJ = (P^{(r+1)} A)J \subseteq (P^{(r+1)} \cap A)J = P^{r+1} J = QI^{r+1} \subseteq Q$ gilt, erhalten wir $P^{(r+1)} \subseteq Q : (AJ) = (Q : A) : J$.

Nehmen wir indirekt $A \subseteq P$ an, dann folgt für die Primideale P_i aus $P_2 \cdot \ldots \cdot P_n \subseteq P_2 \cap \ldots \cap P_n = Rad(A) \subseteq Rad(P^{r+1}) = P$ und der Primeigenschaft von P, dass ein Index i existiert mit $P_i \subseteq P$, aus der Minimalität von P folgt schließlich $P_i = P$. Somit sind in der reduzierten Zerlegung in Primärkomponenten nicht alle zugehörigen Primideale $P, P_2, \ldots, P_n$ verschieden und wir erhalten einen Widerspruch. Somit gilt $A \not\subseteq P$ und daher $Q : A = Q$. Da auch $J \not\subseteq P$ gilt, ergibt sich insgesamt

$$P^{(r+1)} \subseteq (Q : A) : J = Q : J = Q.$$

Umgekehrt erhalten wir aus (3.7) und Satz 3.2.24 $QI^{r+1} = P^{r+1}J \subseteq P^{r+1} \subseteq P^{(r+1)}$ und damit $Q \subseteq P^{(r+1)} : I^{r+1} = P^{(r+1)}$, da aus (3.6) $I^{r+1} \not\subseteq P$ folgt. Damit ist nun gezeigt, dass sich jedes Primärideal von R als symbolische Potenz $Q = P^{(m)}$ für ein $m \in \mathbb{N}$ darstellen lässt.

Wegen $P^m \subseteq P^{(m)}$ ist noch zu zeigen, dass $P^m \subset P^{(m)}$ nicht gelten kann. Angenommen $P^m \subset P^{(m)}$ und sei $P^m = P^{(m)} \cap Q_1 \cap \ldots \cap Q_n$ die reduzierte Darstellung in Primärkomponenten. Für das Radikal von $P^{(m)}$ folgt sodann $P = Rad(P^m) = Rad(P^{(m)}) \cap Rad(Q_1 \cap \ldots \cap Q_n) = P \cap Rad(Q_1 \cap \ldots \cap Q_n)$. Daraus folgt, dass entweder $Rad(Q_1 \cap \ldots \cap Q_n) \supset P$ oder $Rad(Q_1 \cap \ldots \cap Q_n) = P$ gilt. Wäre nun $Rad(Q_1 \cap \ldots \cap Q_n) \supset P$, dann war P nicht maximal, da $Rad(Q_1 \cap \ldots \cap Q_n)$ ein Primideal ist, das P echt umfasst. Gilt hingegen $Rad(Q_1 \cap \ldots \cap Q_n) = P$, so war entgegen der obigen Annahme die Primärzerlegung nicht reduziert. In beiden Fällen erhalten wir also einen Widerspruch, sodass $P^m = P^{(m)}$ für alle Primideale $P \neq 0$ gilt. Da schon gezeigt ist, dass jedes Primärideal von R eine symbolische Potenz ist, folgt die Behauptung. □

Kapitel 4

Dedekindsche Ringe

4.1 Charakterisierungen Dedekindscher Ringe

Wie schon in der Einleitung und in Abschnitt 3.2 erwähnt, funktioniert der Übergang von der Primfaktorzerlegung von Elementen auf eine Primfaktorzerlegung von Idealen in Hauptidealringen R problemlos. Bilden wir jedes Element a eines Hauptidealringes auf das von a erzeugte Hauptideal ab, so bleiben alle multiplikativen Eigenschaften erhalten. Prime Elemente werden zu Primidealen, Primzahlpotenzen zu Primäridealen und irreduzible Elemente zu maximalen Idealen. Der Übergang zu Idealen bedeutet auch, dass wir uns um Einheiten nicht mehr kümmern müssen, weil für ϵ Einheit $(\epsilon) = (e) = (R)$ gilt und für assoziierte Elemente a, b, also $b = \epsilon a$, die Ideale (a) und (b) gleich sind.

Eine natürliche Verallgemeinerung von Hauptidealringen sind daher jene Ringe, in denen sich zumindest jedes Ideal als Produkt von Primidealen darstellen lässt. Diese neue Klasse von Ringen wird hier eingeführt:

Definition 4.1.1. *Ein Integritätsring R heißt Dedekindsch, wenn sich jedes echte Ideal von R als Produkt von Primidealen darstellen lässt.*

In Dedekindschen Ringen wird die Eindeutigkeit der Primidealzerlegung nicht verlangt. Wir werden im Laufe dieses Kapitels jedoch zeigen, dass diese automatisch erfüllt ist.

Weil hier der Fokus auf Ideale anstelle von Elementen gerichtet ist, transferieren wir den Begriff des Einselements auf das Einheitsideal, das der Ring R selbst ist (für jedes Ideal I von R gilt $I \cdot R = R \cdot I = I$). Weil wir uns für multiplikative Eigenschaften interessieren, benötigen wir auch die „Invertierbarkeit von Idealen“. Wenn wir Ideale mit der Eigenschaft $I \cdot J = R$ suchen, dann ist diese nur für $I = J = R$ erfüllt. Wir müssen daher, um einen passenden Invertierbarkeitsbegriff für Ideale zu erhalten, den zu betrachtenden Ring auf den Quotientenkörper und auch den Begriff des Ideals erweitern:

Definition 4.1.2. *Sei R ein Integritätsbereich mit Quotientenkörper K. Ein R-Modul A von K heißt gebrochenes Ideal von R, wenn ein $r \in R$, $r \neq 0$, existiert, sodass $r \cdot A \subseteq R$ gilt.*

Alle Ideale von R sind nach dieser Definition gebrochene Ideale (vgl. Abschnitt 3.3). Um sie von gebrochenen Idealen hervorzuheben, werden sie auch gerne als *ganze Ideale* von R bezeichnet. Wir werden die ganzen Ideale von R fortan als Ideale bezeichnen und sie so von den gebrochenen Idealen von R unterscheiden.

Weiters ist jeder endlich erzeugte R-Modul von K ein gebrochenes Ideal, denn für einen endlich erzeugten R-Modul $A = Rk_1 + \ldots + Rk_n$ mit $k_i = \frac{r_i}{s_i} \in K$ erfüllt das Element $s = s_1 \cdot \ldots \cdot s_n$ die Inklusion $s \cdot A \subseteq R$.

Definition 4.1.3. *Ein gebrochenes Ideal A von R heißt invertierbar, wenn ein gebrochenes Ideal B mit der Eigenschaft $A \cdot B = R$ existiert.*

Bemerkung. Wie unten gezeigt wird (Satz 4.1.5), ist B durch diese Eigenschaft eindeutig bestimmt. B heißt das zu A inverse gebrochene Ideal.

Das Rechnen mit gebrochenen Idealen als R-Moduln ist uns aus dem Abschnitt 3.3 vertraut, neu hingegen ist folgender Sachverhalt:

Satz 4.1.4. *Seien R ein Integritätsbereich mit Quotientenkörper K und A, B gebrochene Ideale von R.*

a) Für $B \neq 0$ ist der Idealquotient $A : B = \{x \in K | xB \subseteq A\}$ von A nach B in K ein gebrochenes Ideal.

b) Es gelten $AR = RA = A$ und $A(R : A) = (R : A)A \subseteq R$.

Beweis.

a) $A : B$ ist ein R-Modul von K (das ist eine Verallgemeinerung des Satzes 3.2.14). Es bleibt daher nur noch zu zeigen, dass ein Element $t \neq 0$ aus R existiert, sodass $t(A : B) \subseteq R$ gilt. Da A und B gebrochene Ideale sind, existieren $r, s \in R$ mit $rA \subseteq R$ und $sB \subseteq R$. Wir wählen ein $b_0 \in B \backslash \{0\}$. $b := sb_0$ liegt sowohl in B als auch in R und damit in $B \cap R$. Setzen wir $t := rb$, so erhalten wir $t(A : B) = rb(A : B) \subseteq rA \subseteq R$.

b) $AR = RA = A$ ist trivialerweise erfüllt (A ist R-Modul) und da $R : A$ nach a) ebenfalls ein R-Modul ist, ist auch die zweite Aussage klar. □

Satz 4.1.5. *Sei R ein Integritätsring mit Quotientenkörper K.*

a) Wenn A, B gebrochene Ideale mit $AB = R$ sind, dann ist B eindeutig bestimmt. Ferner ist $B = R : A$ und wir schreiben $B = A^{-1}$.

b) Wenn $AC = BC$ gilt mit C invertierbar, dann folgt $A = B$.

c) Das Produkt $A_1 \cdot \ldots \cdot A_n$ von gebrochenen Idealen ist invertierbar genau dann, wenn jeder Faktor A_i invertierbar ist und es gilt $(A_1 \cdot \ldots \cdot A_n)^{-1} = A_1^{-1} \cdot \ldots \cdot A_n^{-1}$.

d) Angenommen es gilt für ein gebrochenes Ideal A, dass $P_1 \cdot \ldots \cdot P_m = A = Q_1 \cdot \ldots \cdot Q_n$ mit Primidealen P_i, Q_j aus R. Wenn jedes P_i als gebrochenes Ideal invertierbar ist, dann gilt $m = n$ und $P_i = Q_i$ nach Umordnen der Faktoren.

e) Wenn A invertierbar ist, dann ist A endlich erzeugt als R-Modul.

Beweis.

a) Sei $AB = R$, dann gilt $B \subseteq R : A$. Andererseits ist $R : A = R \cdot (R : A) = BA(R : A) \subseteq BR \subseteq B$ und damit insgesamt $B = R : A$.

b) Multipliziere beide Seiten der Gleichung $AC = BC$ mit C^{-1} um $AR = BR$, also $A = B$ zu erhalten.

c) ($\Rightarrow$) Sei B ein gebrochenes Ideal von R , sodass $B(A_1 \cdot \ldots \cdot A_n) = R$ gilt. Für jedes A_i gilt: $A_i(B \cdot A_1 \cdot \ldots \cdot A_{i-1} \cdot A_{i+1} \cdot \ldots \cdot A_n) = R$ (R ist kommutativ) . Somit ist $B \cdot A_1 \cdot \ldots \cdot A_{j-1} \cdot A_{j+1} \cdot \ldots \cdot A_n$ das Inverse von A_i und A_i invertierbar.

($\Leftarrow$) Wenn jedes A_i invertierbar ist, dann gilt: $A_i \cdot A_i^{-1} = R$ für $i = 1, \ldots, n$ und folglich $(A_1 \cdot A_2 \cdot \ldots \cdot A_n) \cdot (A_1^{-1} \cdot A_2^{-1} \cdot \ldots \cdot A_n^{-1}) = R$, weshalb auch $A_1 \cdot A_2 \cdot \ldots \cdot A_n$ invertierbar ist.

d) Wir führen einen Induktionsbeweis nach m: Für $m = 1$ besitzt A die Darstellungen $P_1 = A = Q_1 \cdot \ldots \cdot Q_n$. Da P_1 prim ist, folgt aus $P_1 = Q_1 \cdot \ldots \cdot Q_n$, dass $Q_i \subseteq P_1$ für einen Index i gilt. Andererseits ist $P_1 \subseteq Q_1 \cdot \ldots \cdot Q_n \subseteq Q_i$ was die Gleichheit $P_1 = Q_i$ zeigt. Es bleibt also noch zu zeigen, dass Q_i der einzige Faktor ist. Wir nehmen indirekt an, dass es noch weitere Faktoren in der Darstellung von A gibt: Sei dazu $Q_0 := \prod_{j \neq i} Q_j$, dann gilt $P_1 = Q_i \cdot Q_0$. Multiplizieren wir beide Seiten der Gleichung mit P_1^{-1}, dann erhalten wir $R = Q_0$. Da die Q_is echt enthalten sind in R, gilt das klarerweise auch für ihr Produkt Q_0 und damit erhalten wir einen Widerspruch. Somit gilt $P_1 = Q_i = A$.

Sei nun $m > 1$ und die Behauptung für $m - 1$ gezeigt. Wir wählen ein P_i so, dass es kein anderes umfasst. Sei P_1 jenes Ideal für das $P_i \not\subseteq P_1$ für alle $i \neq 1$ gilt. Weil $Q_1 \cdot \ldots \cdot Q_n = P_1 \cdot \ldots \cdot P_m \subseteq P_1$ gilt und P_1 Primideal ist, muss auch eines der Q_is in P_1 enthalten sein; sei oBdA $Q_1 \subseteq P_1$. Ebenso gilt $P_1 \cdot \ldots \cdot P_m = Q_1 \cdot \ldots \cdot Q_n \subseteq Q_1$ und auch hier existiert ein Index $i \in \{1, \ldots, n\}$ sodass $P_i \subseteq Q_1$ gilt. Insgesamt erhalten wir also $P_i \subseteq Q_1 \subseteq P_1$ und da P_1 so gewählt war, dass $P_1 \not\supseteq P_i$ gilt, folgt $P_i = Q_1 = P_1$. Weil $P_1 = Q_1$ invertierbar ist, können wir die Gleichung $P_1 \cdot \ldots \cdot P_m = Q_1 \cdot \ldots \cdot Q_n$ mit P_1^{-1} multiplizieren und wir erhalten $P_2 \cdot \ldots \cdot P_m = Q_2 \cdot \ldots \cdot Q_n$ eine Produktdarstellung mit $m - 1$ Faktoren, bei der nach Induktionsvoraussetzung die Anzahl der Faktoren auf

beiden Seiten übereinstimmt und weiters $P_i = Q_i$ nach Umordnen der Q_is, $i = 2, \ldots, m$, gilt.

e) Weil $e \in R = A^{-1}A$ gilt, existieren Elemente $x_i \in A^{-1}$ und $y_i \in A$ mit $e = \sum_{i=1}^{n} x_i y_i$. Sei nun $a \in A$ beliebig, dann gilt $a = a \cdot e = \sum_{i=1}^{n} (ax_i)y_i \in Ry_1 + \ldots + Ry_n$. Aus $ax_i \in R$ folgt $x_i \in R : A$, da a beliebig war. Damit ist gezeigt, dass A von den endlich vielen Elementen $y_1, \ldots y_n$ als R-Modul erzeugt wird. □

Satz 4.1.6. *Sei R ein Dedekindscher Ring, dann ist jedes Primideal $P \neq 0$ von R maximal und invertierbar.*

Beweis. Sei $p \in P\backslash\{0\}$. Da R Dedekindsch ist, existieren Primideale P_i sodass $(p) = P_1 \cdot \ldots \cdot P_n$ gilt. Klarerweise gilt $(p) \subseteq P$ und wegen $(p) = P_1 \cdot \ldots \cdot P_n \subseteq P$ liegt zumindest ein Primideal, es sei P_j, in P, also $P_j \subseteq P$. Andererseits ist das Ideal (p) invertierbar, da zu dem Hauptideal (p) das Inverse $(\frac{1}{p})R$ existiert. Das Produkt der Primideale P_i ist somit invertierbar und nach Satz 4.1.5 sind es auch alle P_is, $i = 1, \ldots, n$.

Um die Maximalität von P zu zeigen, wählen wir ein $a \in R\backslash P$ und zeigen, dass $P + (a) = R$ gilt. Wenn $P + (a) \subset R$ gelten würde, dann behaupten wir $P = P^2 + Pa$.

Da R Dedekindsch ist, existieren Primideale $P_1, \ldots, P_m$ und $P'_1, \ldots, P'_n$ mit $P + (a) = P_1 \cdot \ldots \cdot P_m$ und $P + (a^2) = P'_1 \cdot \ldots P'_n$. Klarerweise gilt $P \subset P + (a) \subseteq P_i$, $i = 1 \ldots, m$.

Wir betrachten die Bilder der natürlichen Projektion $\pi : R \to R\backslash P$ und erhalten $\pi(P + (a)) = (\bar{a}) = \bar{P}_1 \cdot \ldots \bar{P}_m$ und $\pi(P + (a^2)) = (\bar{a}^2) = \bar{P}'_1 \cdot \ldots \cdot \bar{P}'_n$; dabei gilt $\bar{P}_i = \pi(P_i) = P_i/P$ und $\bar{P}'_j = \pi(P'_j) = P'_j/P$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$. Die Ideale $(\bar{a})$ und $(\bar{a}^2)$ sind als Ideale in R/P invertierbar und damit sind nach Satz 4.1.5 auch die einzelnen Primideale $\bar{P}_1, \ldots \bar{P}_m, \bar{P}'_1, \ldots \bar{P}'_n$ invertierbar.

Andererseits folgt aus der Primeigenschaft der P_i, dass R/P_i ein Integritätsbereich ist. Wegen $R/P_i \cong (R/P)/(P_i/P)$ ist daher $P_i/P = \bar{P}_i$ ein Primideal von R/P $(\forall P_i,\ 1 \leq i \leq m)$. Ein analoges Argument gilt für $P'_j/P = \bar{P}'_j$ $(1 \leq j \leq n)$. Da $\bar{P}'_1 \cdot \ldots \cdot \bar{P}'_n = (\bar{a}^2) = (\bar{a})^2 = (\bar{P}_1 \cdot \ldots \cdot \bar{P}_m)^2 = \bar{P}_1^{\,2} \cdot \ldots \cdot \bar{P}_m^{\,2}$ gilt, folgern wir wegen Satz 4.1.5, dass $n = 2m$ und $\bar{P}_i = \bar{P}'_{2i} = \bar{P}'_{2i-1}$ für $1 \leq i \leq m$ ist. Damit gilt für die Urbilder $P_i = P'_{2i} = P'_{2i-1}$. Folglich erhalten wir $P \subseteq P + (a^2) = P'_1 \cdot \ldots \cdot P'_n = (P_1 \cdot \ldots \cdot P_m)^2 = (P + (a))^2 \subseteq P^2 + (a)$.

Sei nun $p \in P$ beliebig, dann können wir schreiben $p = x + ra$ mit $x \in P^2$, $r \in R$. Wegen $x \in P^2 \subseteq P$ gilt $p - x = ra \in P$, aber $a \notin P$. Da P prim ist, muss $r \in P$ gelten und damit erhalten wir $P \subseteq P^2 + Pa$. Die umgekehrte Inklusion $P^2 + Pa \subseteq P$ ist trivialerweise erfüllt. Wir haben also $P = P^2 + Pa$ gezeigt. Multiplizieren wir mit P^{-1}, so folgt der Widerspruch $R = P^{-1}P = P^{-1}(P^2 + Pa) = P + (a)$.

Somit ist P maximal und da es beliebig gewählt war, sind alle Primideale in R maximal. Daher gilt $P_j = P$ und P ist maximal und invertierbar. □

Da nun jedes Primideal invertierbar ist, folgt nach Satz 4.1.5, d) die Eindeutigkeit der Primidealzerlegung für jedes Ideal eines Dedekindschen Ringes.

Im nächsten Satz werden wir Charakterisierungen Dedekindscher Ringe beweisen; insbesondere die, dass Dedekindsche Ringe genau die Noetherschen, ganz abgeschlossenen Integritätsringe sind, in denen jedes Primideal maximal ist.

Theorem 4.1.7. *Sei R ein Integritätsring mit Quotientenkörper K. Dann sind die folgenden Aussagen äquivalent:*

1) R ist Dedekindsch.

2) Jedes echte Ideal kann eindeutig als Produkt von Primidealen dargestellt werden.

3) Jedes Ideal $I \neq 0$ ist invertierbar als gebrochenes Ideal.

4) Jedes gebrochene Ideal $I \neq 0$ von R ist invertierbar.

5) R ist Noethersch, ganz abgeschlossen und jedes Primideal $\neq 0$ ist maximal.

6) R ist Noethersch, jedes Primideal $\neq 0$ ist maximal und jedes Primärideal in R ist eine Primidealpotenz.

Beweis.

1) $\Rightarrow$ 2) Wurde gerade bewiesen.

2) $\Rightarrow$ 3) Da sich nach Voraussetzung jedes echte Ideal eindeutig als Produkt von Primidealen darstellen lässt, reicht es nach Satz 4.1.5, c) zu zeigen, dass jedes Primideal invertierbar ist. Dies gilt aber aufgrund des letzten Satzes 4.1.6.

3) $\Rightarrow$ 4) Jedes gebrochene Ideal hat die Form $k \cdot I$ mit $k \in K,\ k \neq 0$, und I ein Ideal aus R. Da nach Voraussetzung I invertierbar ist, ist $k^{-1} \cdot I^{-1}$ das zu $k \cdot I$ inverse gebrochene Ideal.

4) $\Rightarrow$ 5) Sei I ein beliebiges Ideal $\neq 0$ von R. Da es sich nach Voraussetzung invertierbar ist, folgt aus Satz 4.1.5, e), dass es als R-Modul endlich erzeugt ist. Daher ist R Noethersch.

Sei $\alpha \in K$ ganz über R. Wir zeigen $\alpha \in R$. Der Ring $S := R[\alpha]$ ist nach Satz 3.3.6 endlich erzeugter R-Modul und damit ist S ein gebrochenes Ideal, das nach Voraussetzung invertierbar ist. Somit können wir $S = R \cdot S = (S^{-1}S)S = S^{-1}(SS) = S^{-1}S = R$ folgern. Es gilt also $R[\alpha] = R$ und damit $\alpha \in R$, was die ganze Abgeschlossenheit von R in K beweist.

Es bleibt noch zu zeigen, dass jedes Primideal $\neq 0$ maximal ist. Angenommen es existiert ein Primideal $P \neq 0$, das nicht maximal ist. Dann existiert ein Ideal M mit $P \subset M$. Nach Voraussetzung ist M als gebrochenes Ideal invertierbar. Es gilt $M^{-1}P \subseteq M^{-1}M = R$ und $M^{-1}P$ ist ein Ideal in R. Wir können daher $P = M(M^{-1}P)$ als Produkt

von zwei Idealen von R darstellen. Da P prim ist und $M \not\subseteq P$ muss $M^{-1}P \subseteq P$ gelten und damit

$$R = M^{-1}M \subseteq M^{-1}R = M^{-1}(PP^{-1}) = (M^{-1}P)P^{-1} \subseteq PP^{-1} = R,$$

also $R = M^{-1}R = M^{-1}$ und wir erhalten daraus $R = MM^{-1} = MR = M$, also den gesuchten Widerspruch zu P ist nicht maximal.

5) $\Rightarrow$ 6) folgt nach Satz 3.3.9

6) $\Rightarrow$ 1) Sei I eine echtes Ideal von R. Da R Noethersch ist, besitzt es eine reduzierte Primärzerlegung $I = Q_1 \cap \ldots \cap Q_n$ mit Q_i P_i-primär. Nach Voraussetzung sind die verschiedenen Primideale maximal und damit paarweise komaximal. Nach Satz 3.2.10 folgt, dass auch die Q_is paarweise komaximal sind, sodass wir mit Satz 3.2.27 $I = Q_1 \cap \ldots \cap Q_n = Q_1 \cdot \ldots \cdot Q_n$ erhalten. Aus der Voraussetzung, dass jedes Primärideal eine Primidealpotenz ist, folgt, dass für jedes i, $1 \leq i \leq n$, eine natürliche Zahl k_i existiert mit $Q_i = P_i^{k_i}$. Das führt zu $I = P_1^{k_1} \cdot \ldots P_n^{k_n}$, einer Produktdarstellung von I durch Primideale. □

Damit gilt nun auch

Satz 4.1.8. *Die Menge aller gebrochenen Ideale von R bilden eine multiplikative Gruppe.*

Korollar 4.1.9. *Zu jedem Ideal A aus R existiert ein gebrochenes Ideal A', sodass AA' ein Hauptideal ist.*

4.2 Teilbarkeitsbegriff im Idealverband

Aufgrund der eindeutigen Zerlegung jedes Ideals aus R in ein Produkt von endlich vielen Primidealen gelingt es zu $\mathbb{Z}$ völlig analoge Eigenschaften für die Menge der Ideale in R herzuleiten. Speziell zeigen wir das am Beispiel der Teilbarkeit für Ideale:

Satz 4.2.1. *Sei R ein Dedekindscher Ring und $(P_i)_{i \in I}$ eine Menge von Primidealen. Weiters seien $A = \prod_{i \in I} P_i^{e_i}$ und $B = \prod_{i \in I} P_i^{f_i}$ zwei Ideale von R in Primidealzerlegung. Folgende Aussagen sind äquivalent:*

1) $A \supseteq B$

2) $0 \leq e_i \leq f_i$ für alle $i \in I$

3) Aus $A|B$ (d.h. $A \supseteq B$) folgt, dass ein Ideal C in R existiert mit $B = CA$.

Beweis.

1) $\Rightarrow$ 2) Wir multiplizieren die Ungleichung

$$A = \prod_{i \in I} P_i^{e_i} \supseteq \prod_{i \in I} P_i^{f_i} = B$$

mit dem gebrochenen Ideal $(\prod_{i \in I} P_i^{min(e_i, f_i)})^{-1}$ und erhalten

$$\prod_{i \in I_0} P_i^{a_i} \supseteq \prod_{i \in I_1} P_i^{b_i}$$

mit den Indexmengen $I_0 = \{i \in I | e_i > f_i\}$ und $I_1 = \{i \in I | e_i < f_i\}$; diese beiden Indexmengen sind klarerweise disjunkt (existiert ein Index i_k, sodass $e_{i_k} = f_{i_k}$ gilt, dann ist $i_k \notin I_0$ und $i_k \notin I_1$).

Wenn wir $I_0 \neq \emptyset$ annehmen, so können wir ein Element $i_0 \in I_0$ auswählen und es gilt $\prod_{i \in I_1} P_i^{b_i} \subseteq P_{i_0}$. Wegen der Primeigenschaft finden wir einen Index $i \in I_1$, sodass $P_i \subseteq P_{i_0}$ gilt und mit der Maximalität der Primideale folgt $P_i = P_{i_0}$ und damit $i = i_0$. Dies widerspricht aber $I_1 \cap I_0 = \emptyset$ und somit muss $I_0 = \emptyset$ gelten. Damit ist nun $f_i > e_i$ für alle $i \in I_1$; für die restlichen Indizes $j \in I \backslash I_1$ gilt nach Konstruktion $f_j = e_j$, also insgesamt $f_i \geq e_i$ für alle $i \in I$.

2) $\Rightarrow$ 3) Das Ideal $C := \prod_{i \in I} P_i^{f_i - e_i}$ erfüllt die Gleichung $AC = B$.

3) $\Rightarrow$ 1) Aus $B = CA$ erhalten wir, da $C \subseteq R$ gilt, die gewünschte Inklusion $B = CA \subseteq RA = A$. □

Korollar 4.2.2. *Jedes Ideal besitzt nur endlich viele Teiler.*

Satz 4.2.3. *In einem Dedekindschen Ring ist ein Ideal genau dann irreduzibel, wenn es prim ist.*

Beweis.

($\Leftarrow$): In jedem beliebigen Integritätsring ist jedes Primideal irreduzibel (vgl. Satz 2.0.10).

($\Rightarrow$): Sei umgekehrt A ein irreduzibles Ideal. Dann ist $A = 0$ (und damit prim, weil jeder Dedekindsche Ring ein Integritätsbereich ist) oder $A \neq 0$, also ein Produkt von Primidealen. Da aber nach Voraussetzung A unzerlegbar ist, kann es kein Produkt von mehr als einem Primideal sein, also ist A prim. □

In selber Art und Weise wie für zwei Elemente eines faktoriellen Ringes können wir den größten gemeinsamen Teiler (ggT) und das kleinste gemeinsame Vielfache (kgV) von zwei Idealen A, B ermitteln. Dabei ist $C = ggT(A, B)$ definiert durch $C|A$, $C|B$ und aus $D|A$, $D|B$ für ein Ideal D von R folgt $C|D$; $K = kgV(A, B)$ ist definiert durch $A|K$, $B|K$ und aus $A|L$, $B|L$ für ein Ideal L aus R folgt $K|L$.

Satz 4.2.4. *Seien R ein Dedekindscher Ring und $(P_i)_{i\in I}$ eine Menge von Primidealen. Weiters seien $A = \prod_{i\in I} P_i^{e_i}$ und $B = \prod_{i\in I} P_i^{f_i}$ zwei Ideale von R in Primidealzerlegung. Es gelten:*

a) $ggT(A,B) = A + B = \prod_{i\in I} P_i^{\min(e_i,f_i)}$

b) $kgV(A,B) = A \cap B = \prod_{i\in I} P_i^{\max(e_i,f_i)}$

Beweis.

a) Wir zeigen zunächst, dass $ggT(A,B) = C := A + B$ ist. Klarerweise gilt $A, B \subseteq C$. Ist nun D ein Ideal von R mit $A, B \subseteq D$, so folgt $A + B \subseteq D$, womit alles gezeigt ist.

Es habe C die Primidealzerlegung $C = \prod_{i\in I} P_i^{g_i}$. Weil $A \subseteq C$ und $B \subseteq C$ gilt, folgt aus Satz 4.2.1 $g_i \leq e_i$ und $g_i \leq f_i$ für alle $i \in I$; damit gilt also $g_i \leq \min(e_i, f_i)$. Wir erhalten daher $C \supseteq \prod_{i\in I} P_i^{\min(e_i,f_i)}$.

Andererseits ist

$$C = \prod_{i\in I} P_i^{e_i} + \prod_{i\in I} P_i^{f_i} = \prod_{i\in I} P_i^{\min(e_i,f_i)} \underbrace{\left(\prod_{i\in I} P_i^{e_i-\min(e_i,f_i)} + \prod_{i\in I} P_i^{f_i-\min(e_i,f_i)}\right)}_{\subseteq R \text{ weil } e_i-\min(e_i,f_i)\geq 0 \text{ und } f_i-\min(e_i,f_i)\geq 0} \subseteq \prod_{i\in I} P_i^{\min(e_i,f_i)}.$$

b) Wieder zeigen wir zuerst, dass $kgV(A,B) = K := A \cap B$ ist. Es ist $K \subseteq A, B$, also ist K gemeinsames Vielfaches von A und B. Ist nun L Ideal von R mit $L \subseteq A$ und $L \subseteq B$, so folgt $L \subseteq A \cap B$.

Hat nun K die Primidealzerlegung $K = \prod_{i\in I} P_i^{g_i}$, so muss $g_i \geq \max(e_i, f_i)$ für alle i gelten wegen $K \subseteq A$ und $K \subseteq B$. Damit ist $K \subseteq \prod_{i\in I} P_i^{\max(e_i,f_i)}$.

Andererseits ist $\prod_{i\in I} P_i^{\max(e_i,f_i)} \subseteq \prod_{i\in I} P_i^{e_i} = A$ und $\prod_{i\in I} P_i^{\max(e_i,f_i)} \subseteq \prod_{i\in I} P_i^{f_i} = B$ und damit $\prod_{i\in I} P_i^{\max(e_i,f_i)} \subseteq A \cap B = K$.

□

Aus der Maximalität der Primideale erhalten wir, dass für eine Menge $(P_i)_{i\in I}$ die darin vorkommenden Primideale paarweise relativ prim sind, also $ggT(P_{i_j}, P_{i_k}) = R$ für alle $i_j \neq i_k$ aus I und damit auch $ggT((P_i)_{i\in I}) = R$.

Das kleinste gemeinsame Vielfache von $(P_i)_{i\in I}$ ist, da keines der Primideale ein anderes umfasst, daher $kgV((P_i)_{i\in I}) = \bigcap_{i\in I} P_i = \prod_{i\in I} P_i$.

Gehen wir bei einem gegebenen Ideal A aus einem Dedekindschen Ring R zum Faktorring R/A über, so können wir zeigen, dass dieser isomorph zum direkten Produkt der Faktorringe nach den Primidealpotenzen ist. Wir kennen diese Eigenschaft bereits aus dem Ring der ganzen Zahlen $\mathbb{Z}$, aus der der Chinesische Restsatz abgeleitet wird.

Satz 4.2.5. *Sei R ein Dedekindscher Ring und $A = \prod_{i=1}^{r} P_i^{e_i}$ ein Ideal in Primidealzerlegung. Dann gilt*

$$R/A \cong \prod_{i=1}^{r} R/P_i^{e_i}.$$

Beweis. Aus Satz 4.2.4 folgern wir, dass $A = \prod_{i=1}^{r} P_i^{e_i} = \bigcap_{i=1}^{r} P_i^{e_i}$ gilt. Da weiters alle Primideale paarweise relativ prim sind, gilt $P_j^{e_j} + P_i^{e_i} = R$ für alle $i \neq j$ und damit insbesondere $P_j^{e_j} + \bigcap_{i=1, i\neq j}^{r} P_i^{e_i} = R$ $(1 \leq i \leq r)$.

Um die Behauptung zu zeigen, definieren wir eine Abbildung $\theta : R \to \prod_{i=1}^{r} R/P_i^{e_i}$ als r-Tupel: $\theta(a) = (\theta_1(a), \ldots \theta_r(a))$, wobei $\theta_i : R \to R/P_i^{e_i}$ die natürliche Projektion ist. θ ist ein Ringhomomorphismus, weil jedes θ_i ein Ringhomomorphismus ist. Sein Kern ist $\bigcap_{i=1}^{r} P_i^{e_i} = A$. Es bleibt daher nur noch die Surjektivität von θ zu zeigen; d.h. wir müssen zu gegebenen $x_i \in R$ $(i = 1, \ldots, r)$ ein Element $x \in R$ finden, sodass $x - x_i \in P_i^{e_i}$ für alle i gilt.

Wir betrachten dazu zuerst folgenden Spezialfall: Es existiert ein Index j, sodass $x_i = 0$ für alle $i \neq j$ gilt. Weil $P_j^{e_j} + \bigcap_{i=1, i\neq j}^{r} P_i^{e_i} = R$ gilt, können wir $x_j = y + z$ mit $y \in P_j^{e_j}$, $z \in \bigcap_{i=1, i\neq j}^{r} P_i^{e_i}$ schreiben. Damit liegt $z - x_j = -y$ in $P_j^{e_j}$ und $z - x_i = z$ in $P_i^{e_i}$ für alle $i \neq j$. Wir können deshalb $x = z$ wählen.

Nun haben wir für jeden Index $1 \leq j \leq r$ ein solches x mit der gewünschten Eigenschaft gefunden. Wir bezeichnen in Abhängigkeit vom Index j die Lösungen des Spezialfalls mit $z_j \in \bigcap_{i=1, i\neq j}^{r} P_i^{e_i}$.

Setzen wir $\bar{x} = \sum_{j=1}^{r} z_j$, dann ist

$$\bar{x} - x_i = \underbrace{\sum_{j=1, j\neq i}^{r} z_j}_{\in \bigcap_{i=j}^{r} P_i^{e_i} = P_i^{e_i}} + \underbrace{(z_i - x_i)}_{\in P_i^{e_i}},$$

also $\bar{x}$ das gesuchte Element. □

Bemerkung. Der vorige Satz ist also eine Verallgemeinerung des Chinesischen Restsatzes auf Dedekindsche Ringe: Durch die Isomorphie $R/A \cong R/P_1^{e_1} \times \ldots \times R/P_r^{e_r}$ finden wir zu einem System von linearen Kongruenzen

$$x_i \equiv r_i(P_i^{e_i}) \quad (1 \leq i \leq r)$$

ein x, das jede Kongruenz erfüllt. Für jede weitere Lösung dieses Systems x' gilt $x' \equiv x(\prod_{i=1}^{r} P_i^{e_i})$.

Der nächste Satz zeigt diesen Sachverhalt für Ideale. Darin werden in b) und c) zwei wesentliche Folgerungen in Dedekindschen Ringen gezeigt:

Satz 4.2.6. *Sei R ein Dedekindscher Ring.*

a) Wenn $0 \neq A \subseteq B$ zwei Ideale in R sind, dann existiert ein $x \in R$ mit der Eigenschaft $A + (x) = B$.

b) Jedes Ideal wird von höchstens zwei Elementen erzeugt.

c) Zu einem gegebenen Ideal A existiert ein Ideal A^*, sodass AA^* ein Hauptideal ist.

Beweis.

a) Wir schreiben für $A \subseteq B$ die beiden Ideale in Primidealzerlegung $A = \prod_{i=1}^{r} P_i^{e_i}$ und $B = \prod_{i=1}^{r} P_i^{f_i}$ mit $e_i \leq f_i$ für alle i an. Wir setzen $C_0 = \prod_{i=1}^{r} P_i^{e_i+1}$ und $C_j := P_j^{e_j} \prod_{i=1 i\neq j}^{r} P_i^{e_i+1}$. Damit gilt $C_j \subseteq P_i^{e_i+1}$ für alle $i \neq j$ und wegen der Eindeutigkeit der Faktorzerlegung weiters $C_j \supset C_0 \; \forall j$, sodass wir ein Element $x_j \in C_j \backslash C_0$ wählen können.

Wir behaupten $x = \sum_{i=1}^{r} x_j$ besitzt die gewünschte Eigenschaft $A + (x) = B$:

Es gilt $(x) \subseteq \sum_{i=1}^{r} (x_j) \subseteq \sum_{i=1}^{r} C_j = ggT(C_1, \ldots, C_r) = B$; B teilt also (x) und wir finden ein Ideal C mit $BC = (x)$. Keines der Primideale P_i teilt C, denn angenommen $P_i | C$, dann folgt $P_i^{e_i+1} | BC = (x)$, also $(x) \subseteq P_i^{e_i+1}$ und damit

$$(x_i) = (x - \sum_{j=1 j\neq i}^{r} x_j) \subseteq (x) + \sum_{j=1 j\neq i}^{r} (x_j) \subseteq (x) + \sum_{j=1 j\neq i}^{r} C_j \subseteq P_i^{e_i+1}.$$

Folglich wäre

$$(x_i) \subseteq P_i^{e_i+1} \cap C_i = P_i^{e_i+1} \cap P_i^{e_i} \prod_{j=1 j\neq i}^{r} P_j^{e_j+1} = \prod_{j=1}^{r} P_j^{e_j+1} = C_0,$$

was der Wahl von $x_i \in C_i \backslash C_0$ widerspricht.

Da nun keines der Primideale C teilt, erhalten wir schließlich $A + (x) = A + BC = B(\prod_{j=1}^{r} P_j^{f_j - e_j} + C) = BR = B$.

b) Sei A ein Ideal von R und $x \in A \backslash \{0\}$. Dann ist $(x) \subseteq A$ und nach a) existiert ein $y \in R$ mit $(x) + (y) = A$, d.h. $(x, y) = A$.

c) Sei A ein Ideal aus R, dann gilt für jedes Ideal B aus R die Inklusion $AB \subseteq A$ und nach a) finden wir ein $x \in R$, sodass $AB + (x) = A$ gilt. Daher ist A Teiler von (x), d.h. es existiert ein A^* mit $AA^* = (x)$. □

Abschließend werden wir noch zeigen, dass in Ringen, die Dedekindsch und faktoriell sind, jedes Ideal von genau einem Element erzeugt wird.

Satz 4.2.7. *Jeder Integritätsbereich, der sowohl Dedekindsch als auch faktoriell ist, ist ein Hauptidealring. Umgekehrt ist jeder Hauptidealring Dedekindsch und faktoriell.*

Beweis.

($\Leftarrow$) Die Umkehrung ist klar, weil Dedekindsche Ringe eine Verallgemeinerung von Hauptidealringen sind und jeder Hauptidealring faktoriell ist.

($\Rightarrow$) Wir zeigen, dass in einem Dedekindschen und faktoriellen Ring jedes Primideal ein Hauptideal ist. Sei P ein Primideal und $a \in P$, $a \neq 0$. Da a keine Einheit ist, ist es ein Produkt von irreduziblen Elementen, also $a = \prod_{i=1}^{r} p_i^{e_i}$. Aus $a \in P$ folgt, dass es einen Index i gibt, sodass $p_i \in P$ gilt. Damit ist $(p_i) \subseteq P$ und wir haben ein Primideal (p_i) gefunden, das in P enthalten ist. Da in einem Dedekindschen Ring jedes Primideal maximal ist, muss $(p_i) = P$ gelten. Ist nun A, $A \neq 0 = (0)$, $A \neq R = (e)$, ein beliebiges Ideal und $A = \prod_{i \in I} P_i^{e_i}$ die Primidealzerlegung mit $P_i = (p_i)$, $i = 1, \ldots, r$, so ist A Hauptideal wegen $A = \prod_{i \in I} (p_i)^{e_i} = \prod_{i \in I} (p_i^{e_i}) = (\prod_{i \in I} p_i^{e_i})$. $\square$

Kapitel 5

Algebraische Zahlkörper und ihre zugehörigen Ganzheitsringe

5.1 Allgemeine Theorie

Wir behandeln in diesem Kapitel spezielle Zahlkörper und Zahlringe, die in der algebraischen Zahlentheorie besonders wichtig sind und auf die die bisher dargestellte Theorie der Noetherschen und Dedekindschen Ringe anwendbar ist.

Definition 5.1.1. *Eine endliche Körpererweiterung L von $\mathbb{Q}$ heißt algebraischer Zahlkörper oder einfach Zahlkörper.*

Bemerkung.

1. Jede endliche Körpererweiterung ist algebraisch. Darüber hinaus wird jede solche Körpererweiterung L von einem primitiven Element $\alpha \in L$ erzeugt, $L = K(\alpha)$. Da $L \supseteq \mathbb{Q}$ ist die Charakteristik von L gleich 0.

2. Der Einfachheit halber setzen wir im Folgenden immer voraus, dass der algebraische Abschluss von L gleich $\mathbb{C}$ ist, also $L \subseteq \mathbb{C}$ gilt.

Wir bezeichnen in Anlehnung an Kapitel 3.3. ein Element $\alpha \in L$ als *ganz algebraisch*, wenn α ganz über $\mathbb{Z}$ ist. Nach Satz 3.3.8 ist der Ring der ganzen Zahlen $\mathbb{Z}$, da er faktoriell ist, ganz abgeschlossen in $\mathbb{Q}$, d.h. seine ganze Hülle in $\mathbb{Q}$ ist genau $\mathbb{Z}$.

Betrachten wir im Zahlkörper L die Menge aller ganz algebraischen Zahlen, so enthält sie sicher $\mathbb{Z}$. Weiters gilt:

Satz 5.1.2. *Die Menge M der ganz algebraischen Zahlen von L bildet einen Integritätsring.*

Beweis. Seien $s, t \in M$, dann liegen s, t in dem endlich erzeugten $\mathbb{Z}$-Modul $\mathbb{Z}[s, t]$. Im Ring $\mathbb{Z}[s, t]$ liegen auch $t - s$ und ts und weil $\mathbb{Z}[s, t]$ als $\mathbb{Z}$-Modul endlich erzeugt ist, sind auch $t - s$ und ts ganz über $\mathbb{Z}$, also $ts, t - s \in M$. □

Wir führen für die Menge der ganz algebraischen Zahlen eine eigene Bezeichnung ein:

Definition 5.1.3. *Die Menge der ganz algebraischen Zahlen bezeichnet man als Ganzheitsring von L oder als Zahlring von L. Man schreibt dafür $\mathcal{O}_L$ oder manchmal $\mathcal{O}_\alpha$, wobei α ganz algebraisch ist.*

Zunächst werden wir zeigen, dass jeder Zahlkörper L von einem ganz algebraischen primitiven Element über $\mathbb{Q}$ erzeugt werden kann.

Satz 5.1.4. *Sei L ein Zahlkörper und $\beta \in L$. Dann existiert ein $z \in \mathbb{Z}$, $z \neq 0$, sodass $\alpha = z\beta$ ganz algebraisch ist. Insbesondere gilt $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.*

Beweis. Da β algebraisch über $\mathbb{Q}$ ist, genügt es einem Polynom $f \in \mathbb{Q}[x]$, $f(\beta) = 0$. Sei $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \ldots + \frac{a_n}{b_n}x^n$. Multiplizieren wir f mit dem Hauptnenner $B = b_0 \cdot \ldots \cdot b_n$ der Koeffizienten von f, so erhalten wir $c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1} + c_n\beta^n = 0$ mit $c_i = \frac{a_i}{b_i}B \in \mathbb{Z}$. Multiplikation dieser Gleichung mit c_n^{n-1} liefert

$$c_0 \cdot c_n^{n-1} + c_1 \cdot c_n^{n-2}(c_n\beta) + \ldots + c_{n-1}(c_n\beta)^{n-1} + (c_n\beta)^n = 0.$$

$c_n\beta$ ist also ganz algebraisch und damit $c_n\beta \in \mathcal{O}_L$. □

Zum Auffinden von ganz algebraischen Zahlen in L hilft folgender

Satz 5.1.5. *Ein Element $\alpha \in L$ ist genau dann ganz algebraisch, wenn das Minimalpolynom m_α von α über $\mathbb{Q}$ in $\mathbb{Z}[x]$ liegt. Alle Konjugierten von α über $\mathbb{Q}$ sind ganz algebraisch.*

Beweis.

($\Leftarrow$) Das Minimalpolynom $m_\alpha \in \mathbb{Z}[x]$ ist normiert, daher ist $\alpha \in L$ ganz algebraisch.

($\Rightarrow$) Umgekehrt sei $\alpha \in L$ ganz über $\mathbb{Z}$, dann gibt es ein normiertes Polynom $f \in \mathbb{Z}[x]$, $f \neq 0$ mit $f(\alpha) = 0$. Für das Minimalpolynom $m_\alpha \in \mathbb{Z}[x]$ gilt $m_\alpha | f$ in $\mathbb{Q}[x]$. Nach dem Lemma von Gauß gilt dann auch $m_\alpha | f$ in $\mathbb{Z}[x]$. Da f normiert ist, muss somit auch $m_\alpha \in \mathbb{Z}[x]$ normiert sein.

Die restliche Aussage des Satzes folgt, da die Konjugierten von α die anderen Nullstellen von m_α sind. □

Im Weiteren werden wir zeigen, dass sich jedes Element eines Zahlringes $\mathcal{O}_\alpha$, $\alpha \neq 0$, keine Einheit, als Produkt irreduzibler Elemente aus $\mathcal{O}_\alpha$ darstellen lässt. Dazu benötigen wir folgendes Hilfsmittel:

Definition 5.1.6. *Sei $L = K(\beta)$ ein Zahlkörper und $m_\beta \in \mathbb{Q}[x]$ das Minimalpolynom von β über $\mathbb{Q}$.*

1. Sind $\beta = \beta_1, \ldots, \beta_n$ die Konjugierten zu β, so heißen die isomorphen Abbildungen $\sigma_i : \mathbb{Q}(\beta) \to \mathbb{Q}(\beta_i)$, die durch $\sigma_i(\beta) = \beta_i$, $\sigma_i(q) = q$ für alle $q \in \mathbb{Q}$, $i = 1, \ldots, n$ festgelegt sind, die zu L gehörigen $\mathbb{Q}$-Isomorphismen.

2. Für $\alpha \in L$ ist die Norm $N_{L:\mathbb{Q}}(\alpha)$ von α bezüglich L definiert durch $N_{L:\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

Folgende grundlegende Eigenschaften gelten für die Norm:

Satz 5.1.7.

1. Sei L ein algebraischer Zahlkörper und $\alpha \in L$ mit Minimalpolynom $m_\alpha = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$. Dann gilt $N_{L:\mathbb{Q}}(\alpha) = ((-1)^n a_0)^{[L:\mathbb{Q}(\alpha)]} \in \mathbb{Q}$.

2. Für beliebige $\alpha, \beta \in L$ gilt $N_{L:\mathbb{Q}}(\alpha\beta) = N_{L:\mathbb{Q}}(\alpha) N_{L:\mathbb{Q}}(\beta)$.

Beweis. Siehe [Hun74], Ch. V, Theorem 7.3, S. 290f. □

Bemerkung. Teil 1 impliziert, dass die Definition der Norm unabhängig vom primitiven Element $\beta \in L$ ist. Auch folgt aus Teil 1, dass $N_{L:\mathbb{Q}}(\alpha) \in \mathbb{Z}$ für ganz algebraisches $\alpha \in L$ gilt.

Für den zugehörigen Ganzheitsring $\mathcal{O}_L$ von L können wir nun zeigen:

Satz 5.1.8.

1. Ein Element $\alpha \in \mathcal{O}_L$ ist genau dann Einheit, wenn die $N_{L:\mathbb{Q}}(\alpha) = \pm 1$ gilt.

2. Seien $\alpha, \beta \in \mathcal{O}_L$. Wenn α echter Teiler von β ist, dann ist auch $|N_{L:\mathbb{Q}}(\alpha)|$ echter Teiler von $|N_{L:\mathbb{Q}}(\beta)|$.

3. Jedes $\alpha \in \mathcal{O}_L$, $\alpha \neq 0$, keine Einheit, lässt sich als Produkt irreduzibler Elemente aus $\mathcal{O}_L$ darstellen.

Beweis.

1. ($\Rightarrow$) Wenn α eine Einheit von $\mathcal{O}_L$ ist, dann existiert ein $\alpha' \in \mathcal{O}_L$, sodass $\alpha \cdot \alpha' = 1$ gilt. Gehen wir über zur Norm, so folgt $N(\alpha \cdot \alpha') = N(\alpha) \cdot N(\alpha') = 1$ ($N = N_{L:\mathbb{Q}}$). Wegen $N(\alpha), N(\alpha') \in \mathbb{Z}$ ist $N(\alpha)$ Einheit und damit $N(\alpha) = \pm 1$.

($\Leftarrow$) Umgekehrt sei $N(\alpha) = \pm 1$. Mit den zu α gehörigen $\mathbb{Q}$-Isomorphismen $\sigma_1 = id, \sigma_2, \ldots, \sigma_n$ gilt nach Definition $\pm 1 = N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \cdot \prod_{i=2}^{n} \sigma_i(\alpha)$. Da der zweite Faktor ganz algebraisch ist, ist α Teiler von $1 \in \mathcal{O}_L$; α ist daher Einheit.

2. Wenn α echter Teiler von β ist, so existiert ein $\gamma \in \mathcal{O}_L$ mit $\alpha \cdot \gamma = \beta$ und $|N_{L:\mathbb{Q}}(\gamma)| > 1$. Damit folgt aus der Multiplikativität der Norm das Resultat.

3. Wir beweisen den Satz mittels Induktion nach $|N(\alpha)|$.

Nach Voraussetzung ist $|N(\alpha)| > 1$. Sei also zunächst $|N(\alpha)| = 2$. In diesem Fall ist α selbst irreduzibel. Aus $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathcal{O}_L$ folgt nämlich $2 = |N(\alpha)| = |N(\beta)||N(\gamma)|$. Da die Faktoren auf der linken Seite in $\mathbb{N}$ liegen, muss einer, etwa $|N(\beta)|$, gleich 1 sein. Dann ist aber β nach 1. notwendigerweise Einheit.

Sei nun die Aussage für $|N(\alpha)| \leq k$, $k \geq 2$, bewiesen. Für $\alpha \in \mathcal{O}_L$ mit $|N(\alpha)| = k+1$ gibt es zwei Möglichkeiten. Entweder α ist irreduzibel, so ist nichts mehr zu zeigen; oder α lässt sich echt zerlegen, dh. $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathcal{O}_L$ und β, γ keine Einheiten. Wegen $|N(\alpha)| = |N(\beta)||N(\gamma)|$ und $1 < |N(\beta)|, |N(\gamma)| \leq k$ kann man auf β und γ die Induktionsvoraussetzung anwenden, so dass beide Elemente sich als Produkt irreduzibler Elemente darstellen lassen. Das gilt dann auch für das Produkt $\beta\gamma = \alpha$. □

Wie schon öfter erwähnt, ist diese Produktdarstellung jedoch im allgemeinen nicht eindeutig. Doch werden wir zeigen, dass $\mathcal{O}_L$ stets ein Dedekindscher Ring ist, indem wir nachweisen, dass er Noethersch und alle Primideale von $\mathcal{O}_L$ maximal sind. (Die ganze Abgeschlossenheit geht aus der Konstruktion dieser Ringe hervor.) Somit lassen sich zumindest alle Ideale $I \neq 0$ von $\mathcal{O}_L$ eindeutig als Produkt von Primidealen schreiben.

Wir beginnen mit folgendem

Satz 5.1.9. *Jedes Ideal $I \neq 0$ von $\mathcal{O}_L$ enthält eine Basis von L über $\mathbb{Q}$.*

Beweis. Sind allgemein $K \subseteq L$ zwei Körper, so ist L auch K-Vektorraum über K. Sei also $B = \{\gamma_1, \ldots, \gamma_n\}$ eine Basis von L über $\mathbb{Q}$. Nach Satz 5.1.4 gibt es $z_i \in \mathbb{Z},\ z_i \neq 0$ mit $z_i\gamma_i \in \mathcal{O}_L$, $i = 1, \ldots, n$. Wir setzen $z = z_1 \cdot \ldots \cdot z_n \in \mathbb{Z}$. Ist weiters $\alpha \in I,\ \alpha \neq 0$ fest, dann ist $\{\alpha z\gamma_1 \ldots, \alpha z\gamma_n\} \subseteq I$ eine Basis von L. Dazu ist nur zu zeigen, dass diese Menge linear unabhängig ist. Aus $\lambda_1(\alpha z\gamma_1) + \ldots + \lambda_n(\alpha z\gamma_n) = 0$ ($\lambda_i \in \mathbb{Q}$) folgt aber $(\lambda_1\alpha z)\gamma_1 + \ldots + (\lambda_n\alpha z)\gamma_n = 0$. Da B Basis ist, muss $\lambda_i\alpha z = 0\ \forall i$ gelten. Wegen $\alpha z \neq 0$ ist daher $\lambda_i = 0\ \forall i$. □

Als nächstes zeigen wir, dass die Ideale von $\mathcal{O}_L$ stets spezielle Basen von L über $\mathbb{Q}$ enthalten.

Definition 5.1.10. *Sei $I \neq 0$ Ideal von $\mathcal{O}_L$. Eine Basis $B = \{\gamma_1, \ldots, \gamma_n\} \subseteq \mathcal{O}_L$ von L heißt Ganzheitsbasis, wenn sich jedes Element von I als ganzzahlige Linearkombination von B darstellen lässt, d.h. $I = \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_n$.*

Für den Beweis des nächsten Satzes benötigen wir auch den Begriff der Diskriminante. Es sei $L = \mathbb{Q}(\alpha)$ ein Zahlkörper vom Grad $[L : \mathbb{Q}] = n$. Es lässt sich also jedes Element $\beta \in L$ eindeutig darstellen als

$$\beta = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1},\ c_j \in \mathbb{Q},\ j = 0, \ldots, n-1.$$

Sind $\alpha^{(1)} = \alpha, \ldots, \alpha^{(n)}$ die Konjugierten von α, so setzen wir

$$\beta^{(i)} = c_0 + c_1\alpha^{(i)} + \ldots + c_{n-1}(\alpha^{(i)})^{n-1},\ i = 1, \ldots, n.$$

Definition 5.1.11. *Es sei $B = \{\gamma_1 \ldots, \gamma_n\} \subseteq \mathscr{O}_L$ eine Basis von L über $\mathbb{Q}$. Dann heißt*

$$\begin{vmatrix} \gamma_1 & \ldots & \gamma_n \\ \gamma_1^{(2)} & \ldots & \gamma_n^{(2)} \\ \vdots & \ldots & \vdots \\ \gamma_1^{(n)} & \ldots & \gamma_n^{(n)} \end{vmatrix}^2 =: \Delta(\gamma_1, \ldots, \gamma_n)$$

die Diskriminante von B.

Die Diskriminante besitzt folgende Eigenschaften:

Satz 5.1.12. *Es seien $B = \{\gamma_1, \ldots, \gamma_n\}$, $B' = \{\gamma_1', \ldots, \gamma_n'\} \subseteq \mathscr{O}_L$ zwei Basen von L über $\mathbb{Q}$ und M die Matrix zum Basiswechsel $B \mapsto B'$. Dann gilt:*

1. $\Delta(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}\backslash\{0\}$.

2. $\Delta(\gamma_1', \ldots, \gamma_n') = (detM)^2 \cdot \Delta(\gamma_1, \ldots, \gamma_n)$.

Siehe [IR90], Proposition 12.1.2., S. 173.

Bemerkung. Sind B, B' zwei Ganzheitsbasen von $\mathscr{O}_L$, so gilt $\Delta(B') = \Delta(B)$. Diesen Wert bezeichnet man als die *Diskriminante* Δ *von* $\mathscr{O}_L$. Um das einzusehen, brauchen wir nur zu beachten, dass die Eintragungen der Matrizen M und M' zum Basiswechsel $B \mapsto B'$ und $B' \mapsto B$ ganzzahlig sein müssen, sodass $detM, detM' \in \mathbb{Z}$ gilt. Aus 2. folgt dann $\Delta(B)|\Delta(B')$ und $\Delta(B')|\Delta(B)$ in $\mathbb{Z}$, also $\Delta(B') = \Delta(B)$.

Jetzt können wir den folgenden grundlegenden Satz beweisen:

Satz 5.1.13. *Jedes Ideal I von $\mathscr{O}_L$, $I \neq 0$, besitzt eine Ganzheitsbasis.*

Beweis. Sei $C = \{\beta_1, \ldots, \beta_n\} \subseteq I$ eine beliebige Basis von L über $\mathbb{Q}$. Dann ist $D(C) := |\Delta(\beta_1, \ldots, \beta_n)| \in \mathbb{N}$. Es gibt somit eine Basis $B = \{\gamma_1, \ldots, \gamma_n\} \subseteq I$ derart, dass $D(B) \leq D(C)$ für alle Basen $C \subseteq I$ gilt. Wir behaupten, dass B eine Ganzheitsbasis von L ist. Dazu nehmen wir indirekt an, B wäre keine solche. Dann gibt es ein Element $\alpha \in I$ derart, dass bei der Darstellung von α mittels B, $\alpha = c_1\gamma_1 + \cdots + c_n\gamma_n$, nicht alle Koeffizienten ganzzahlig sind: Sei etwa $c_1 \in \mathbb{Q}\backslash\mathbb{Z}$. Dann lässt sich c_1 schreiben als $c_1 = z + \zeta$ mit $z \in \mathbb{Z}$ und $0 < \zeta < 1$. Wir gehen nun zu einer neuen Basis $B' = \{\gamma_1', \ldots, \gamma_n'\} \subseteq I$ über mit

$$\gamma_1' = \alpha - z\gamma_1 = \zeta\gamma_1 + \cdots + c_n\gamma_n,\ \gamma_i' = \gamma_i \text{ für } 2 \leq i \leq n.$$

Die Basiswechselmatrix M hat die Gestalt $\begin{pmatrix} \zeta & c_2 & \dots & c_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$, also gilt $detM = \zeta$. Mit Eigenschaft 2. des vorigen Satzes erhalten wir somit den Widerspruch $D(B') = \zeta^2 D(B) < D(B)$. □

Bemerkung. Es haben alle Ganzheitsbasen dieselbe Diskriminante. Sind nämlich B, B' zwei Ganzheitsbasen, so haben die beiden Matrizen M zum Basiswechsel $B \mapsto B'$ und M^{-1} zum Basiswechsel $B' \mapsto B$ definitionsgemäß ganzzahlige Eintragungen. Es ist also $detM, detM^{-1} \in \mathbb{Z}\backslash\{0\}$. Die Beziehungen $D(B) = (detM)^2 D(B')$ und $D(B') = (detM^{-1})^2 D(B)$ liefern $D(B')|D(B)$ und $D(B)|D(B')$, also $D(B') = D(B)$.

Satz 5.1.14. *Es sei L ein Zahlkörper. Für jedes Ideal I von $\mathscr{O}_L$, $I \neq 0$ gilt $I \cap \mathbb{Z} \neq \{0\}$.*

Beweis. Sei $\alpha \in I$, $\alpha \neq 0$. Dann gilt für die Norm von α: $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Z}\backslash\{0\}$. Wegen $\sigma_1(\alpha) = \alpha \in I$ liegt auch $N(\alpha)$ in I; insgesamt folgt $N(\alpha) \in I \cap \mathbb{Z}$. □

Wir kommen nun zum angekündigten Ergebnis über die grundlegende Eigenschaft der algebraischen Zahlringe.

Satz 5.1.15. *Es sei L Zahlkörper über $\mathbb{Q}$. Dann ist $\mathscr{O}_L$ ein Dedekindscher Ring.*

Beweis. Wir verwenden dazu die in Satz 4.1.7, 5) angegebene Charakterisierung Dedekindscher Ringe.

(i) Um zu zeigen, dass $\mathscr{O}_L$ Noethersch ist, sei $I \neq 0$ ein Ideal von $\mathscr{O}_L$. Wie wir eben abgeleitet haben, gibt es ein $m \in \mathbb{Z} \cap I$, $m \neq 0$. Sei $B = \{\beta_1, \dots, \beta_n\} \subseteq I$ eine Ganzheitsbasis. Dann besitzt $\mathscr{O}_L/(m)$ nur endlich viele Elemente, nämlich

$$c_1\beta_1 + \dots c_n\beta_n + (m) \text{ mit } c_i \in \mathbb{Z},\ 0 \leq c_i < m \text{ für } i = 1, \dots n. \tag{5.1}$$

Folglich hat auch $\mathscr{O}_L/I$ als homomorphes Bild von $\mathscr{O}_L/(m)$ nur endlich viele Elemente.

Nach dem 2. Homomorphiesatz gibt es daher auch nur endlich viele Ideale $I_1, \dots I_k$ mit $I_j \supseteq I$, $j = 1, \dots k$. Somit muss jede aufsteigende Kette von Idealen nach endlich vielen Schritten abbrechen.

(ii) Dass $\mathscr{O}_L$ ganz abgeschlossen ist, gilt definitionsgemäß.

(iii) Ist $I \neq 0$ ein Primideal, so ist nach dem in Teil (i) Gezeigten $\mathscr{O}_L/I$ endlich. Da $\mathscr{O}_L/I$ Integritätsring und jeder endliche Integritätsring schon Körper ist, folgt I ist maximales Ideal. □

Bemerkung. Aus dem Beweis von Teil (i) ergibt sich sogar, dass $|\mathcal{O}_L/(m)| = m^n$ gilt. Dazu zeigen wir, dass die obige Darstellung (5.1) eindeutig ist. Ist nämlich $c_1\beta_1+\ldots c_n\beta_n \equiv c_1'\beta_1+\ldots c_n'\beta_n(m)$, so folgt $(c_1-c_1')\beta_1+\ldots(c_n-c_n')\beta_n \equiv 0(m)$, d.h. die linke Seite ist gleich $md_1\beta_1+\ldots md_n\beta_n$. Da B Basis ist, folgt $c_i - c_i' = md_i$, $i = 1,\ldots,n$. Wegen $0 \leq c_i, c_i' < m$ muss daher $c_i = c_i'$ $\forall i$ sein.

Aufgrund des Satzes wissen wir nun, dass sich jedes Ideal I von $\mathcal{O}_L$, $I \neq 0$, eindeutig bis auf die Reihenfolge als Produkt von Primidealen darstellen lässt. Zum Abschluss dieses Abschnitts überlegen wir uns noch wie sich das für ein Ideal (p), p Primzahl in $\mathbb{Z}$, gestaltet. Dazu benötigen wir einen erweiterten Normbegriff:

Definition 5.1.16. *Sei I Ideal von $\mathcal{O}_L$, $I \neq 0$. Dann heißt $N(I) := |\mathcal{O}_L/I| \in \mathbb{N}$ die Norm von I.*

Satz 5.1.17. *Es seien I, J Ideale von $\mathcal{O}_L$ und $\alpha \in \mathcal{O}_L$. Dann gilt:*

1. $N((\alpha)) = |N_{L:\mathbb{Q}}(\alpha)|$.
2. $N(IJ) = N(I) \cdot N(J)$.

Der *Beweis* dieser beiden Aussagen findet sich in [Rib01] in den Abschnitten **F** bzw. **D** von Kapitel 8.1 (S. 142f.).

Im folgenden Satz bezeichne $\bar{\varphi_p} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ den surjektiven Homomorphismus, der den natürlichen Homomorphismus $\varphi_p : \mathbb{Z} \to \mathbb{Z}_p$ fortsetzt.

Satz 5.1.18 (Zerlegungssatz, [Ash03], Chapter 4, 4.3.1 Theorem)**.** *Seien $p \in \mathbb{N}$ eine Primzahl und L ein Zahlkörper vom Grad n, weiters sei $\alpha \in \mathcal{O}_L$ primitives Element von L, also $L = \mathbb{Q}(\alpha)$, und es gelte $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Es bezeichne $m_\alpha \in \mathbb{Z}[x]$ das Minimalpolynom von α, $\bar{m_\alpha} = \bar{\varphi_p}(m_\alpha) \in \mathbb{Z}_p[x]$ dessen Bild unter $\bar{\varphi_p}$. Hat $\bar{m_\alpha}$ die Darstellung $\bar{m_\alpha} = \bar{g_1}^{e_1} \cdot \ldots \cdot \bar{g_r}^{e_r}$ als Produkt irreduzibler Polynome über $\mathbb{Z}_p$, dann gilt $(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ mit Primidealen P_i von $\mathcal{O}_L$, wobei $P_i = (p, g_i(\alpha))$ und $g_i \in \mathbb{Z}[x]$ ein Urbild von $\bar{g_i} \in \mathbb{Z}_p[x]$ ist. Weiters gilt $n = \sum_{i=1}^r e_i f_i$ für $f_i = |\mathcal{O}_L/P_i|$.*

Beweis. Es sei K ein Zerfällungskörper des Polynoms $\bar{g_1} \cdot \ldots \cdot \bar{g_r} \in \mathbb{Z}_p[x]$ und seien $\gamma_i \in K$ mit $\bar{g_i}(\gamma_i) = 0$, $i = 1,\ldots,r$ fix gewählt. Es gilt dann $\mathbb{Z}_p[x]/(\bar{g_i}) \cong \mathbb{Z}_p[\gamma_i]$, $i = 1,\ldots,r$. Durch Nachrechnen lässt sich zeigen, dass die Abbildungen $\psi_i : \mathbb{Z}[\alpha] \to \mathbb{Z}_p[\gamma_i]$ gegeben durch $\psi_i(q(\alpha)) = \bar{q}(\gamma_i)$, $q \in \mathbb{Z}[x]$,$\bar{q} = \bar{\varphi_p}(q)$, $i = 1,\ldots r$ surjektive Homomorphismen sind. (Dabei wird verwendet, dass $\bar{q}(\gamma_i) = 0$ ist, falls $q(\alpha) = 0$. Das gilt, da aus $m_\alpha | q$ folgt $\bar{m_\alpha} | \bar{q}$.) Da $\mathbb{Z}_p[\gamma_i]$ Körper ist, ist $ker\psi_i$ ein maximales Ideal und daher insbesondere ein Primideal.

Wir zeigen $ker\psi_i = P_i$ für $i = 1,\ldots,r$. Wegen $\psi_i(p) = 0$ und $\psi_i(g_i(\alpha)) = \bar{g_i}(\gamma_i) = 0$ gilt $(p, g_i(\alpha)) = P_i \subseteq ker\psi_i$. Sei umgekehrt $h(\alpha) \in ker\psi_i$. Dann ist $\bar{h}(\gamma_i) = 0$ sodass das

Minimalpolynom $\bar{g_i}$ von γ_i Teiler von $\bar{h}$ ist. Es gibt somit ein Polynom $\bar{t_i} \in \mathbb{Z}_p[x]$ mit $\bar{h} = \bar{t_i}\bar{g_i}$. Geht man zu den Urbildern über, so existiert ein Polynom $t_i \in \mathbb{Z}[x]$, sodass sämtliche Koeffizienten von $h - t_i g_i$ durch p teilbar sind. Damit folgt

$$h(\alpha) = \underbrace{(h(\alpha) - t_i(\alpha)g_i(\alpha))}_{\in(p)} + \underbrace{t_i(\alpha)g_i(\alpha)}_{\in(g_i(\alpha))} \in P_i.$$

Wir zeigen als nächstes, dass $(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ gilt. Verwendet man die Beziehung $(I + J_1)(I + J_2) \subseteq I + J_1 J_2$ für beliebige Ideale, so folgt $P_i^{e_i} \subseteq (p) + (g_i(\alpha))^{e_i}$, $i = 1, \ldots, r$. Damit ergibt sich weiter $P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} \subseteq (p) + ((g_1^{e_1} \cdot \ldots \cdot g_r^{e_r})(\alpha))$.

Wegen $\bar{m_\alpha} = \bar{g_1}^{e_1} \cdot \ldots \cdot \bar{g_r}^{e_r}$ sind die Koeffizienten des Polynoms $m_\alpha - g_1^{e_1} \cdot \ldots \cdot g_r^{e_r}$ sämtlich durch p teilbar. Wegen $m_\alpha(\alpha) = 0$ sind es auch die Koeffizienten von $g_1^{e_1} \cdot \ldots \cdot g_r^{e_r}(\alpha)$. Diese Zahl liegt also in (p). Insgesamt erhalten wir $(p) \supseteq P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$.

Somit gibt es ein Ideal I von $\mathcal{O}_L$ mit $(p)I = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$. Da $\mathcal{O}_L$ Dedekindscher Ring ist und daher die Faktorisierung in Primideale eindeutig ist, folgt $(p) = P_1^{k_1} \cdot \ldots \cdot P_r^{k_r}$ mit $0 \leq k_i \leq e_i$, $i = 1, \ldots, r$. Nach Satz 4.2.5 ist $\mathcal{O}_L/(p) \cong \mathcal{O}_L/P_1^{k_1} \times \ldots \times \mathcal{O}_L/P_r^{k_r}$. Somit gilt

$$N((p)) = |\mathcal{O}_L/(p)| = \prod_{i=1}^{r} |\mathcal{O}_L/P_i^{k_i}| = \prod_{i=1}^{r} N(P_i^{k_i}) = \prod_{i=1}^{r} N(P_i)^{k_i}.$$

Wie wir gezeigt haben, ist $\mathcal{O}_L/P_i \overset{\text{Vor.}}{=} \mathbb{Z}[\alpha]/P_i \cong \mathbb{Z}_p[\gamma_i]$ für $i = 1, \ldots, r$. Es ist $|\mathbb{Z}_p[\gamma_i]| = p^{f_i}$ mit $f_i = grad\bar{g_i}$. Mithin folgt $N((p)) = p^{\sum f_i k_i}$. Wegen $N((p)) = p^n$ ergibt sich einerseits $n = \sum_{i=1}^{r} f_i k_i$. Andererseits ist $n = grad m_\alpha = grad \bar{m}_\alpha = \sum_{i=1}^{r} (grad\bar{g_i})e_i = \sum_{i=1}^{r} f_i e_i$. Wegen $0 \leq k_i \leq e_i$ für alle $i = 1, \ldots, r$ folgt notwendigerweise $k_i = e_i$ für alle i, also wirklich $(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$. □

Bemerkung. Die Zahl r in der Darstellung $(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ heißt *Zerlegungszahl* von (p); e_i der *Verzweigungsindex* des Primideals P_i und $f_i = |\mathcal{O}_L/P_i|$ dessen *Trägheitsgrad*.

5.2 Quadratische Zahlkörper und quadratische Zahlringe

Wir werden uns hier mit quadratischen Körpererweiterungen L von $\mathbb{Q}$ befassen, also mit Körpern L, die den Grad der Körpererweiterung $[L : \mathbb{Q}] = 2$ besitzen. Ein Zahlkörper L mit $[L : \mathbb{Q}] = 2$ heißt *quadratischer Zahlkörper*.

Klarerweise ist jeder Körper der Gestalt $L = \mathbb{Q}(\sqrt{d})$, $d \neq 1$, $d \in \mathbb{Z}$ quadratfrei, ein quadratischer Zahlkörper, weil das Minimalpolynom $m_{\sqrt{d}}(x) = x^2 - d$ von $\sqrt{d}$ über $\mathbb{Q}$ den Grad 2 besitzt.

Wir weisen hier direkt nach, dass jeder quadratische Zahlkörper die Gestalt $\mathbb{Q}(\sqrt{d})$, $d \neq 1$, $d \in \mathbb{Z}$ quadratfrei, besitzt:

Sei also L ein quadratischer Zahlkörper. Wir wissen, dass L von einem ganz algebraischen Element $\alpha \in L$ erzeugt werden kann. Es sei dessen Minimalpolynom

$$m_\alpha(x) = x^2 + ax + b,\ a, b \in \mathbb{Z}.$$

Nach der Lösungsformel für quadratische Gleichungen gilt

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Setzen wir $\beta = 2\alpha + a$, so ist β sicher in L und es gilt $\beta^2 = (2\alpha + a)^2 = a^2 - 4b \in \mathbb{Q}$. β hat also Grad 2 und ist daher auch ein primitives Element für L. $a^2 - 4b$ ist sicher kein Quadrat in $\mathbb{Q}$, denn wäre $a^2 - 4b = c^2$ für ein $c \in \mathbb{Q}$, dann ist $\alpha \in \mathbb{Q}$, ein Widerspruch. Möglicherweise gilt $a^2 - 4b = c^2 d$ für $c, d \in \mathbb{Q}$. Dann ist sicher $\frac{1}{c^2}(a^2 - 4b)$ quadratfrei und $\frac{1}{c}\beta$ erzeugt ebenfalls L über $\mathbb{Q}$. Damit ist nun gezeigt, dass jede Körpererweiterung vom Grad 2 von einer quadratfreien Zahl $d \in \mathbb{Z}$, $d \neq 1$, erzeugt werden kann. Dies wird für $\mathbb{Q}(\sqrt{d})$ im Folgenden stets vorausgesetzt.

Wie sehen nun die Elemente des Ringes der ganz algebraischen Zahlen von $\mathbb{Q}(\sqrt{d})$ aus? Er wird mit $\mathcal{O}_d$ bezeichnet.

Satz 5.2.1. *Für den Ganzheitsring $\mathcal{O}_d$ gilt*

$\mathcal{O}_d = \{a + b\sqrt{d}; a, b \in \mathbb{Z}\}$ *falls* $d \equiv 2, 3(4)$,

$\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2}; a, b \in \mathbb{Z},\ a \equiv b(2)\}$ *falls* $d \equiv 1(4)$.

Beweis. Bezeichnet man die rechts stehenden Mengen jeweils mit M, so zeigen wir zunächst die Inklusion $M \subseteq \mathcal{O}_d$.

Ist $d \equiv 2, 3(4)$, so genügt $a + b\sqrt{d}$ jedenfalls dem Polynom $p(x) = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Z}[x]$; die zweite Nullstelle ist $a - b\sqrt{d}$. $a \pm b\sqrt{d}$ sind also sicher ganz algebraisch.

Ist $d \equiv 1(4)$, so genügt $\frac{a+b\sqrt{d}}{2}$ dem Polynom $p(x) = x^2 - ax + \frac{a^2 - b^2 d}{4}$ mit der zweiten Nullstelle $\frac{a-b\sqrt{d}}{2}$. Wegen $a \equiv b(2)$ sind entweder beide Zahlen a, b gerade, also a^2 und b^2 durch 4 teilbar, weshalb $p(x) \in \mathbb{Z}[x]$ gilt, oder a, b sind beide ungerade, weshalb $a^2 \equiv b^2 \equiv 1(4)$ ist. Wegen $d \equiv 1(4)$ folgt $a^2 - b^2 d \equiv 0(4)$ und $p(x) \in \mathbb{Z}[x]$ auch in diesem Fall. Somit gilt $M \subseteq \mathcal{O}_d$.

Um die umgekehrte Inklusion zu zeigen, sei $\zeta = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$ ganz algebraisch. Da die zweite Nullstelle des zugehörigen Minimalpolynoms $p(x)$ gleich $u - v\sqrt{d}$ ist, hat $p(x)$ nach dem Vietaschen Wurzelsatz die Gestalt $p(x) = x^2 + 2u + u^2 - v^2 d$. Damit $p(x) \in \mathbb{Z}[x]$ gilt, muss also $2u \in \mathbb{Z}$, also $u = \frac{u'}{2}$ mit $u' \in \mathbb{Z}$, und $u^2 - v^2 d \in \mathbb{Z}$ sein.

Setzt man $v = \frac{m}{n}$, $m, n \in \mathbb{Z},\ n > 0$ und $ggT(m,n) = 1$, so liefert die zweite Bedingung $\frac{n^2u'^2 - 4m^2d}{4n^2} \in \mathbb{Z}$. Da n^2 den ersten Summanden teilt, muss es auch den zweiten teilen. Da aber m und n relativ prim sind, folgt wegen d quadratfrei $n^2|4$, d.h. $n = 1$ oder $n = 2$. Wir können also ansetzen $u = \frac{u'}{2}$ und $v = \frac{v'}{2}$ mit $u', v' \in \mathbb{Z}$. Es muss also $u'^2 - v'^2 d \equiv 0(4)$ sein.

Da allgemein $w^2 \equiv 0(4)$ oder $w^2 \equiv 1(4)$ für $w \in \mathbb{Z}$ gilt, folgt im Falle $d \equiv 2(4)$ oder $d \equiv 3(4)$: $u'^2 \equiv v'^2 \equiv 0(4)$, also u', v' gerade, dh. $u, v \in \mathbb{Z}$. Ist dagegen $d \equiv 1(4)$, so ergibt sich $u'^2 \equiv v'^2(4)$, also $u' \equiv v'(2)$. In beiden Fällen erhält man $\mathcal{O}_d \subseteq M$, wie behauptet. □

Wir geben nun eine Ganzheitsbasis für $\mathcal{O}_d$ an. Der quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ besitzt als Vektorraum über $\mathbb{Q}$ die Basis $B = \{1, \sqrt{d}\}$. Im Folgenden zeigen wir, dass B in gewissen Fällen auch eine Basis von $\mathcal{O}_d$ ist:

Satz 5.2.2. *Eine Ganzheitsbasis für $\mathcal{O}_d$ ist im Falle $d \equiv 2(4)$ oder $d \equiv 3(4)$ gegeben durch $\{1, \sqrt{d}\}$; im Falle $d \equiv 1(4)$ ist $\{1, \frac{1+\sqrt{d}}{2}\}$ eine solche. Für die Diskriminante Δ von $\mathcal{O}_d$ gilt $\Delta = d$ falls $d \equiv 2, 3(4)$ und $\Delta = 4d$ falls $d \equiv 1(4)$.*

Beweis. In den Fällen $d \equiv 2, 3(4)$ ist nichts zu zeigen. Sei also $d \equiv 1(4)$. In diesem Fall lässt sich jedes Element aus $\mathcal{O}_d$ schreiben als $\frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2}$, wobei $\frac{a-b}{2} \in \mathbb{Z}$ aufgrund der Bedingung $a \equiv b(2)$. Jedes Element von $\mathcal{O}_d$ ist also ganzzahlige Linearkombination von $B = \{1, \frac{1+\sqrt{d}}{2}\}$. Zugeich ist B auch Basis von $\mathbb{Q}(\sqrt{d})$, denn es ist $a + b\sqrt{d} = (a-b) + 2b(\frac{1+\sqrt{d}}{2})$ $(a, b \in \mathbb{Q})$.

Da die Konjugierte von $\sqrt{d}$ gleich $-\sqrt{d}$ und die zu $\frac{1+\sqrt{d}}{2}$ gleich $\frac{1-\sqrt{d}}{2}$ ist, erhalten wir für die Diskriminante Δ

$$\left| \begin{array}{cc} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{array} \right|^2 = 4d \text{ bzw. } \left| \begin{array}{cc} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{array} \right|^2 = d.$$

□

Als Nächstes bestimmen wir die Einheiten von $\mathcal{O}_d$.

Satz 5.2.3. *Es ist $a + b\sqrt{d}$ Einheit genau dann, wenn $a^2 - b^2 d = \pm 1$ für $d \equiv 2, 3(4)$ und $\frac{a+b\sqrt{d}}{2}$ Einheit genau dann, wenn $a^2 - b^2 d = \pm 4$ für $d \equiv 1(4)$ gilt.*

Beweis. Wir wissen, dass $\epsilon = u + v\sqrt{d}$ Einheit in $\mathcal{O}_d$ ist genau dann, wenn $N(\epsilon) = \pm 1$ gilt. Nun gibt es nur zwei zu $\sqrt{d}$ gehörige $\mathbb{Q}$-Automorphismen: sie sind durch $\sqrt{d} \mapsto \sqrt{d}$ $(\sigma_1 = id)$ und $\sqrt{d} \mapsto -\sqrt{d}$ festgelegt. Daher gilt $N(\epsilon) = \sigma_1(\epsilon)\sigma_2(\epsilon) = (u+v\sqrt{d})(u-v\sqrt{d}) = u^2 - v^2 d$. ϵ ist also Einheit genau dann, wenn $u^2 - v^2 d = \pm 1$ erfüllt ist. Im Fall $d \equiv 2, 3(4)$ erhalten wir daher, dass $a + b\sqrt{d}$ Einheit genau dann ist, wenn $a^2 - b^2 d = \pm 1$ gilt. Im Falle $d \equiv 1(4)$ ist $u = \frac{a}{2}$ und $v = \frac{b}{2}$, also íst $\frac{a+b\sqrt{d}}{2}$ Einheit genau dann, wenn $\frac{a^2 - b^2 d}{4} = \pm 1$ gilt. □

Um weitere Aussagen über die Einheiten zu gewinnen, unterscheiden wir die beiden Fälle: $d < 0$, der sogenannte imaginär-quadratische Fall, und $d > 0$, der reell-quadratische Fall.

- (i) $d < 0$: Hier ist $a^2 - b^2 d > 0$, also gibt es nur endlich viele Einheiten. Ist $|d| \geq 5$, so muss wegen $a^2 - b^2 d = 1$ oder $= 4$ sicherlich $b = 0$ sein. Im ersten Fall ist $a = \pm 1$. Im zweiten Fall ist $a = \pm 2$. Da dann aber die Einheiten die Gestalt $\frac{a+b\sqrt{d}}{2}$ haben, sind in beiden Fällen $\epsilon = \pm 1$ die einzigen Einheiten.

  $d = -1 \equiv 3(4)$: Es muss $a^2 + b^2 = 1$ gelten, was genau für $a = \pm 1$, $b = 0$ oder $a = 0$, $b = \pm 1$ erfüllt ist. Damit erhalten wir die vier Einheiten von $\mathscr{O}_{-1} = \mathbb{Z}[i]$ $\epsilon = \pm 1, \pm i$.

  $d = -3 \equiv 1(4)$: Es muss $a^2 + 3b^2 = 4$ sein. Diese Gleichung besitzt die sechs Lösungen $a = \pm 1, b = \pm 1$ und $a = \pm 2, b = 0$. Damit erhalten wir die Einheiten $\epsilon = \frac{\pm 1 \pm \sqrt{-3}}{2}, \pm 1$ von $\mathscr{O}_{-3}$.

- (ii) $d > 0$: Die Gleichungen $a^2 - b^2 d = \pm 1$ bzw. $a^2 - b^2 d = \pm 4$ haben stets unendlich viele ganzzahlige Lösungen. Genauer gilt

Satz 5.2.4. *Die Einheiten $\epsilon \in \mathscr{O}_d$, $d > 0$, sind bis auf das Vorzeichen gleich einer Potenz einer festen Einheit, der Fundamentaleinheit ϵ_0: $\epsilon = \pm \epsilon_0^n$, $n \in \mathbb{Z}$.*

Einen *Beweis* findet man in [Rib01], Abschnitt **E** von Kapitel 10.2. (S. 140) bzw. [IR90], Proposition 13.1.6. (S. 191).

Zum Abschluss dieses Kapitels spezialisieren wir den Satz 5.1.18 auf den Fall quadratischer Zahlkörper. Das wird es uns ermöglichen, den Grund dafür anzugeben, wieso bei dem schon öfter erwähnten Beispiel $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}] = \mathscr{O}_{-5}$ diese verschiedenen Darstellungen als Produkt irreduzibler Elemente existieren.

Mit den Bezeichnungen von Satz 5.1.18 gilt: $n = 2$, $\alpha = \sqrt{d}$ für $d \equiv 2, 3(4)$. Wegen der Beziehung $2 = n = \sum_{i=1}^{r} e_i f_i$ können nur folgende Fälle eintreten:

(i) $r = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1 : (p) = P_1 P_2$ mit $|\mathscr{O}_d / P_1| = |\mathscr{O}_d / P_2| = p$.

(ii) $r = 1$, $e := e_1 = 2$, $f := f_1 = 1 : (p) = P^2$ mit $|\mathscr{O}_d / P| = p$.

(iii) $r = 1$, $e = 1$, $f = 2 : (p) = P$ mit $|\mathscr{O}_d / P| = p^2$.

Im ersten Fall heißt die Primzahl $p \in \mathbb{Z}$ *(vollständig) zerlegt*, im zweiten Fall *verzweigt* und im dritten Fall *träge*. Wir untersuchen nun, wann die einzelnen Fälle eintreten und verwenden dafür Satz 5.1.18.

Wir beginnen mit dem Fall $d \equiv 2, 3(4)$. Dann ist $B = \{1, \sqrt{d}\}$ eine Ganzheitsbasis und daher ist, wenn wir im Folgenden stets die Bezeichnungen jenes Satzes verwenden: $\alpha = \sqrt{d}$ und $m_\alpha = x^2 - d$.

Satz 5.2.5. *Sei $p > 2$ und $d \equiv 2, 3(4)$. Dann gilt:*

1. Falls $p \not| d$ und d quadratischer Rest ist mod p, dann ist p zerlegt:

$$(p) = (p, a + \sqrt{d})(p, a - \sqrt{d}) \text{ mit } a^2 \equiv d(p).$$

2. Falls $p \not| d$ und d quadratischer Nichtrest ist mod p, dann ist p träge.

3. Falls $p|d$, dann ist p verzweigt mit $(p) = (p, \sqrt{d})^2$.

Beweis. Wir müssen $\bar{m}_\alpha$, also m_α mod p betrachten. Hier gibt es drei Möglichkeiten: (i) $\bar{m}_\alpha$ ist irreduzibel über $\mathbb{Z}_p$; (ii) $\bar{m}_\alpha$ ist reduzibel über $\mathbb{Z}_p$ mit zwei verschiedenen Nullstellen; (iii) $\bar{m}_\alpha$ ist reduzibel über $\mathbb{Z}_p$ mit einer doppelt zu zählenden Nullstelle.

Wir beginnen mit dem reduziblen Fall: $\bar{m}_\alpha = x^2 - d \equiv (x - a)(x - b)(p)$. Durch Koeffizientenvergleich erhalten wir $0 \equiv a + b(p)$, $-d \equiv ab(p)$. Also ist $b \equiv -a(p)$ und daher $d \equiv a^2(p)$, d.h. d ist quadratischer Rest mod p. Dabei gilt entweder $a \not\equiv 0(p)$, also $p \not| d$, oder $a \equiv 0(p)$, d.h. $p|d$.

Im ersten Fall ist nun $\bar{m}_\alpha = (x - a)(x + a)$. Daher folgt nach Satz 5.1.18

$$(p) = P_1 P_2 = (p, \sqrt{d} - a)(p, \sqrt{d} + a) \text{ mit } d \equiv a^2(p);$$

d.h. p ist zerlegt.

Im zweiten Fall ist $\bar{m}_\alpha = x^2$, also $\bar{g_1} = x$ und $e_1 = 2$, sodass p verzweigt ist: $(p) = P^2 = (p, \sqrt{d})^2$.

Es bleibt der Fall übrig, dass $\bar{m}_\alpha = \bar{g_1}$ irreduzibel ist. Aufgrund des eben Gezeigten muss dann $p \not| d$ und d quadratischer Nichtrest mod p sein. Nach Satz 5.1.18 folgt dann $P = (p, m_\alpha(\alpha) = 0) = (p)$; also ist p träge. □

Die Argumentation im Fall $d \equiv 1(4)$ verläuft analog, doch ist jetzt $B = \{1, \frac{1+\sqrt{d}}{2}\}$, also $\alpha = \frac{1+\sqrt{d}}{2}$ und das zugehörige Minimalpolynom $m_\alpha = x^2 - x - \frac{d-1}{4}$.

Satz 5.2.6. *Sei $p > 2$ und $d \equiv 1(4)$. Dann gilt:*

1. Falls $p \not| d$ und d quadratischer Rest ist mod p, dann ist p zerlegt:

$$(p) = (p, \frac{1 + \sqrt{d}}{2} - r(1 + c))(p, \frac{1 - \sqrt{d}}{2} - r(1 - c)) \text{ mit } c^2 \equiv d(p) \text{ und } 2r \equiv 1(p).$$

2. Falls $p \not| d$ und d quadratischer Nichtrest ist mod p, dann ist p träge.

3. Falls $p|d$, dann ist p verzweigt mit $(p) = (p, \frac{1+\sqrt{d}}{2} - a)^2$ mit $2a \equiv 1(p)$.

Beweis. Wir überlegen uns wieder, wann m_α reduzibel ist mod p. Sei also $x^2 - x - \frac{d-1}{4} \equiv (x-a)(x-b)(p)$. Koeffizientenvergleich liefert $1 \equiv a+b(p)$ und $-\frac{d-1}{4} \equiv ab(p)$. $b \equiv 1-a(p)$ in

die zweite Kongruenz eingesetzt ergibt $\frac{d-1}{4} \equiv a^2 - a(p)$ bzw. $d \equiv 4a^2 - 4a + 1 = (2a-1)^2(p)$, d.h. d ist quadratischer Rest mod p. Ist umgekehrt $d \equiv c^2(p)$, so hat $c \equiv 2a - 1(p)$ wegen $p > 2$ eine eindeutig bestimmte Lösung a und $\bar{m}_\alpha$ ist reduzibel: $\bar{m}_\alpha = (x-a)(x-(1-a))$.

Wann besitzt $\bar{m}_\alpha$ eine doppelt zu zählende Nullstelle? Das ist genau dann der Fall, wenn $a \equiv b(p)$ gilt, also $1 \equiv 2a(p)$ ist. Ein solches a existiert wegen $p > 2$. Es folgt $-\frac{d-1}{4} \equiv a^2(p)$, also $d \equiv 0(p)$. $\bar{m}_\alpha \equiv (x-a)^2(p)$ gilt also genau dann, wenn $d \equiv 0(p)$. Wir bekommen somit dieselben Bedingungen für die Reduzibilität wie im vorigen Satz.

Ist nun $\bar{m}_\alpha = (x-a)(x-b)$ mit $a \not\equiv b(p)$ und $d \equiv c^2(p)$, so ist wegen $a = r(1+c)$ und $b = r(1-c)$ mit $2r \equiv 1(p)$

$$(p) = P_1 P_2 = (p, \frac{1+\sqrt{d}}{2} - r(1+c))(p, \frac{1-\sqrt{d}}{2} - r(1-c)).$$

Ist dagegen $\bar{m}_\alpha = (x-a)^2$, so ist

$$(p) = (p, \frac{1+\sqrt{d}}{2} - r)^2.$$

Ist schließlich $\bar{m}_\alpha$ irreduzibel, so muss $p \not| d$ und d quadratischer Nichtrest sein. Nach Satz 5.1.18 folgt $P = (p, m_\alpha(\alpha) = 0) = (p)$. □

Bemerkung.

1. Es gilt $(p, \frac{1+\sqrt{d}}{2} - r) = (p, \sqrt{d})$. Dies lässt sich direkt nachprüfen: Aus $2r \equiv 1(p)$ folgt $2r = 1 + tp$ mit ungeradem t und daher

$$\sqrt{d} = 2(\frac{1+\sqrt{d}}{2} - r) + tp \in (p, \frac{1+\sqrt{d}}{2} - r);$$

also $(p, \sqrt{d}) \subseteq (p, \frac{1+\sqrt{d}}{2} - r)$.

Andererseits ist

$$\frac{1+\sqrt{d}}{2} - r = \frac{-tp + \sqrt{d}}{2} = \underbrace{\frac{-t+\sqrt{d}}{2}}_{\in \mathcal{O}_d} p + \underbrace{\frac{1-p}{2}}_{\in \mathcal{O}_d} \sqrt{d} \in (p, \sqrt{d}),$$

sodass auch umgekehrt $(p, \sqrt{d}) \supseteq (p, \frac{1+\sqrt{d}}{2} - r)$ gilt. Wir erhalten somit nach 5.2 $(p) = (p, \frac{1+\sqrt{d}}{2} - r)^2 = (p, \sqrt{d})^2$.

2. Auch die Zerlegung 5.1 lässt sich vereinfachen. Es gilt

$$(p) = (p, c + \sqrt{d})(p, c - \sqrt{d}).$$

Durch Ausrechnen erhält man nämlich $P_1 P_2 = (p^2, p(c+\sqrt{d}), p(c-\sqrt{d}), c^2 - d) = (p)(c+$

$\sqrt{d}, c-\sqrt{d}, \underbrace{\frac{c^2-d}{p}}_{\in\mathbb{Z}})$. Das letzte Ideal enthält die Zahlen $2c = (c+\sqrt{d})+(c-\sqrt{d}) \in \mathbb{Z}$ und p. Diese sind relativ prim. Wäre nämlich $p|2c$,so folgt entweder $p = 2$, ein Widerspruch zur Voraussetzung; oder $p|c$, was wegen $c^2 \equiv d(p)$ auf $p|d$ führt, ebenfalls ein Widerspruch. Somit enthält das letzte Ideal die Zahl $1 = ggT(2c, p)$. Es ist also gleich $\mathcal{O}_d$ und somit folgt $P_1P_2 = (p)\mathcal{O}_d = (p)$. Aufgrund der eindeutigen Zerlegung von (p) in Primideale folgt daher $\{p, \frac{1+\sqrt{d}}{2} - r(1+c)), (p, \frac{1-\sqrt{d}}{2} - r(1-c))\} = \{(p, c+\sqrt{d}), (p, c-\sqrt{d})\}$.

Es bleibt der Fall $p = 2$.

Satz 5.2.7. *Sei $p = 2$ und $d \equiv 2, 3(4)$. Dann ist 2 verzweigt, $(2) = (2, \sqrt{d})^2$ für $d \equiv 2(4)$; $(2) = (2, \sqrt{d}-1)^2 = (2, \sqrt{d}+1)^2$ für $d \equiv 3(4)$.*

Beweis. Es ist $\bar{m}_\alpha \equiv x^2 - d(2)$; also gibt es nur die Möglichkeiten $\bar{m}_\alpha \equiv x^2(2)$ falls $d \equiv 0(2)$, also $d \equiv 2(4)$, und $\bar{m}_\alpha \equiv x^2 - 1 \equiv (x-1)^2(2)$ falls $d \not\equiv 0(2)$, also $d \equiv 3(4)$. Daher ist (2) stets verzweigt. Nach Satz 5.1.18 folgt die Behauptung. □

Satz 5.2.8. *Sei $p = 2$ und $d \equiv 1(4)$, dann gilt*

1. 2 ist zerlegt, falls $d \equiv 1(8)$: $(2) = (2, \frac{\sqrt{d}+1}{2})(2, \frac{\sqrt{d}-1}{2})$.

2. 2 ist träge, falls $d \equiv 5(8)$.

Beweis. Es ist $\bar{m}_\alpha \equiv x^2 - x - c(2)$ mit $\frac{d-1}{4} \equiv c(2)$ und $c = 0$ oder $c = 1$. Ist $c = 0$, so folgt $d \equiv 1(8)$ und $\bar{m}_\alpha \equiv x^2 - x = x(x-1)$, sodass 2 zerlegt ist. Nach Satz 5.1.18 gilt dabei $(2) = (2, \frac{1+\sqrt{d}}{2})(2, \frac{-1+\sqrt{d}}{2})$.

Ist dagegen $c = 1$, so folgt $d \equiv 5(8)$ und $\bar{m}_\alpha \equiv x^2 - x - 1$. Dieses Polynom ist irreduzibel in $\mathbb{Z}_2$, sodass 2 träge ist. □

Beispiel. Wir betrachten nun den konreten Fall $d = -5$. Hier ist $d \equiv 3(4)$. Was passiert mit den Idealen (2) und (3) in $\mathcal{O}_{-5}$ bei der Zerlegung $6 = 2 \cdot 3$? Nach den letzten beiden Sätzen gilt $(2) = (2, 1+\sqrt{-5})^2$ und $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, da $3 \nmid -5$ und $-5 \equiv 1^2(3)$ quadratischer Rest mod 3 ist. Insgesamt folgt

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Wegen $(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$ kann man dies auch schreiben als

$$(6) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1-\sqrt{-5}).$$

Das Produkt der ersten beiden Ideale ist gleich $(1+\sqrt{-5})$, das der letzten beiden Ideale $(1-\sqrt{-5})$. Es gilt somit $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$, woraus die zweite Zerlegung von 6 folgt: $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Zusammenfassung

Noethersche Ringe kann man als Verallgemeinerung von faktoriellen Ringen ansehen, also von Integritätsringen, in denen sich jedes Element, verschieden von Null und keine Einheit, eindeutig bis auf die Reihenfolge als Produkt irreduzibler Elemente darstellen lässt. Sie erfüllen die aufsteigende Kettenbedingung für Ideale, wodurch Noethersche Ringe charakterisiert sind.

Dedekindsche Ringe stellen einen Spezialfall von Noetherschen Ringen dar. In diesen Ringen gilt zusätzlich, dass jedes Primideal maximal ist und dass sie ganz abgeschlossen in ihrem Quotientenkörper sind. Sie spielen eine wichtige Rolle in der algebraischen Zahlentheorie.

In meiner Arbeit untersuche ich zuerst die grundlegenden Sätze der Theorie der Noetherschen Ringe. Es wird der Hilbertsche Basissatz auf zwei Arten bewiesen. Sodann werden unter anderem zwei Darstellungssätze für echte Ideale hergeleitet, nämlich als Produkt beziehungsweise als Durchschnitt von Primäridealen. Danach wird die Frage der Eindeutigkeit solcher Darstellungen behandelt.

Von hier ausgehend werden Dedekindsche Ringe eingeführt als Ringe, in denen sich jedes echte Ideal als Produkt von Primidealen schreiben lässt. Es wird gezeigt, dass diese Darstellung automatisch eindeutig ist. Im Weiteren werden fünf äquivalente Charakterisierungen Dedekindscher Ringe bewiesen, unter anderem die oben Genannte.

Im letzten Kapitel bringe ich als Beispiele für Dedekindsche Ringe die Ganzheitsringe algebraischer Zahlkörper. Als wichtigsten Satz beweise ich den sogenannten Zerlegungssatz. Er besagt, wie sich ganz allgemein das von einer Primzahl erzeugte Hauptideal in einem Ganzheitsring zerlegt. Ausführlich gehe ich dann auf quadratische Zahlkörper und ihre Ganzheitsringe ein. Insbesondere begründe ich, warum es verschiedene Zerlegungen eines Elementes in ein Produkt von irreduziblen Elementen gibt.

Abstract

Noetherian rings can be seen as a generalization of unique factorization domains, which are domains where essentially every element can be uniquely written up to order as a product of irreducible elements. Such domains satisfy the ascending chain condition for ideals and Noetherian rings are characterized in this way.

If one requires additionally that every prime ideal is maximal and the ring is integrally closed in its quotient field, then one gets Dedekind rings. These rings play an important role in algebraic number theory.

At the beginning of my thesis I investigate the basic theorems of the theory of Noetherian rings: Hilbert's Basissatz is proved in two ways. This is followed by two theorems concerning the representation of proper ideals as product or intersection of primary ideals. Also the problem of uniqueness of these representations is dealt with.

Specializing I introduce Dedekind rings as domains, in which every proper ideal can be written as a product of prime ideals. Here uniqueness follows immediately. Next I prove five characterizations of Dedekind rings, one of it is already mentioned above.

In the last chapter rings of integers of algebraic number fields are treated which are the most important examples of Dedekind rings. The main theorem (Zerlegungssatz) in this part considers generally the factorization of the principal ideal of a prime number in such a ring of integers. Finally I focus on quadratic number fields and their rings of integers. Particularly I explain why certain elements can be factorized into irreducible elements in various ways.

Literaturverzeichnis

[Ash03] R. B. Ash. *A Course In Algebraic Number Theory.* http://www.math.uiuc.edu/~r-ash/ANT.html, 2003.

[Bun08] P. Bundschuh. *Einführung in die Zahlentheorie.* Springer, Berlin, 6. Aufl., 2008.

[Hun74] T. W. Hungerford. *Algebra.* Springer, New York, 1974.

[IR90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, New York, 2nd edition, 1990.

[JS06] J. C. Jantzen and J. Schwermer. *Algebra.* Springer, Berlin, 2006.

[KM82] G. Kowol and H. Mitsch. *Algebra I.* Prugg, Eisenstadt, 1982.

[KM84] G. Kowol and H. Mitsch. *Algebra II.* Prugg, Eisenstadt, 1984.

[LM71] M. D. Larsen and P. J. McCarthy. *Multiplicative Theory of Ideals.* Academic Press, New York, 1971.

[Rib01] P. Ribenboim. *Classical Theory of Algebraic Numbers.* Springer, New York, 2001.

[Spi94] K. Spindler. *Abstract Algebra With Applications II. Rings and Fields.* M. Dekker, New York, 1994.

[Tha80] C. Thaer. *Euklid: Die Elemente. Buch I-XIII.* Wissenschaftliche Buchgesellschaft, Darmstadt, 1980.

[VdW67] B. L. Van der Waerden. *Algebra II.* Springer, Berlin, 1967.

Curriculum vitae

Name:	Simone Lechner BSc.
Geburtsdatum:	26.04.1989
Staatsbürgerschaft:	Österreich
E-Mail:	simone.lechner@firnbergschulen.at

Ausbildung

1995 - 1999	PVS Waldkloster
1999 - 2007	BRG 10 Laaerbergstraße *Oberstufe mit naturwissenschaftlichem Schwerpunkt*
2007 - 2011	Universität Wien *Bachelorstudium Mathematik*
Abschluss-arbeiten:	„Modelle der hyperbolischen Geometrie“, Betreuer: Univ.-Prof. Dr. Andreas Cap „Matrizengruppen und hyperbolische Geometrie“, Betreuer: Univ.-Prof. Dr. Andreas Cap
seit 2010	Universität Wien *Lehramtsstudium UF Mathematik / Informatik und Informatikmanagement*

Berufserfahrungen in der Lehre

2012	Fachtutorium an der Fakultät für Informatik, Universität Wien
2012	Projektmitarbeit bei „Safer Internet“ an der Fakultät für Informatik, Universität Wien (Erstellung eines IT-Sicherheitshandbuchs für Erwachsene)
2013 - 2014	Vertragslehrerin für Mathematik am Akademischen Gymnasium Wien
2014	Vertragslehrerin für Mathematik an der Hertha Firnberg Schule für Wirtschaft und Tourismus in Wien