2.7 Hauptidealringe und Euklidische Ringe

In Abschnitt 5 waren uns bereits frappierende Ähnlichkeiten zwischen $\mathbb{Z}$ und dem Polynomring über einem Körper aufgefallen. In diesem Abschnitt wollen wir die Gemeinsamkeiten nun in einen allgemeineren Kontext setzen.

Definition 2.7.1 *Ein Integritätsring R heißt* **euklidischer Ring**, *falls es eine Abbildung*

$$d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

gibt, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

$$a = qb + r \quad \text{mit} \quad (r = 0 \quad \text{oder } d(r) < d(b)).$$

Bemerkung 2.7.2 *Beachten Sie, dass im allgemeinen Fall keine Eindeutigkeitsaussage der Division mit Rest gefordert wird.*

Sobald wir Division mit Rest haben, können wir auch über größte gemeinsame Teiler sprechen. Dazu sollten wir allerdings unsere Definition von Teiler und größtem gemeinsamem Teiler auf diesen allgemeineren Fall erweitern, was aber keine inhaltlichen Schwierigkeiten bietet.

Definition 2.7.3 *Sei R ein Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann ist b* **Teiler** *von a, falls es ein $q \in R$ gibt, so dass $a = qb$. In diesem Fall heisst a* **Vielfaches** *von b.*

Diese Begriffe sind uns im Fall der ganzen Zahlen schon aus Kapitel 1 bekannt. Ihre Verwendung wie auch das Symbol $b \mid a$ übernehmen wir auch in anderen Integritätsringen. Die Aussagen 1.1.5 gelten entsprechend mit Ausnahme von Aussage g). Diese finden wir hier in der allgemeinen Form wieder:

Definition 2.7.4 *Sei R ein Integritätsring, sei $\varepsilon \in R^*$ und seien $a, b \in R \setminus \{0\}$ mit $a = \varepsilon b$. Dann heissen a und b zueinander* **assoziiert**, *kurz $a \sim b$.*

Lemma 2.7.5 *Seien $a, b \in R$. Dann gilt:*

$$a \mid b \text{ und } b \mid a \implies a \sim b.$$

Die Beweisidee des vorigen Lemmas ist identisch mit der aus Kapitel 1.1. Der Unterschied in der Aussage beruht auf der Tatsache, dass $\mathbb{Z}^* = \{1, -1\}$, während in anderen Integritätsringen in der Regel viele mehr Einheiten existieren.

Bemerkung 2.7.6 *Die früher bereits betrachtete Gleichheit von Hauptidealen läßt sich nun auch formulieren als:*

$$\langle a \rangle = \langle b \rangle \iff a \sim b.$$

In Hauptidealringen sind zwei Ideale also genau dann gleich, wenn sie von zueinander assoziierten Elementen erzeugt werden.

In Kapitel 1 folgte dann auf die Betrachtung der Teilbarkeit, der Begriff des größten gemeinsamen Teilers. Dieser Begriff läßt sind in Integritätsringen definieren.

Definition 2.7.7 *Sei R Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann heißt eine Element $d \in R$* **ein größter gemeinsamer Teiler** *von a und b, falls*

a) d ist Teiler sowohl von a als auch von b

b) Jeder gemeinsame Teiler $c \in R$ von a und b ist auch Teiler von d.

Besonders einfach zu handhaben ist der Begriff eines größten gemeinsamen Teilers in euklidischen Ringen aufgrund der folgenden Beobachtung:

Bemerkung 2.7.8 *Ist R euklidischer Ring, so läßt sich die Bedingung in der Definition 2.7.3 auch schreiben als 'falls der Rest der Division von a durch b Null ist'.*

Der folgende Algorithmus, genannt Euklidischer Algorithmus, erlaubt uns die Bestimmung von größten gemeinsamen Teilern in euklidischen Ringen:

Algorithmus 2.7.9 *(Euklidischer Algorithmus)*

Voraussetzung:	*R euklidischer Ring*
Input:	*$a, b \in R$, $b \neq 0$*
Output:	*ein größter gemeinsamer Teiler von a und b*

- `WHILE` $(b \neq 0)$ $\{$
- $\quad r = a \bmod b$
- $\quad a = b$
- $\quad b = r\}$
- `RETURN`(a)

Der Algorithmus sieht erst einmal sehr abstrakt aus und Sie werden sich unter Umständen fragen, was da überhaupt geschieht. Ehe wir also die Korrektheit und die Terminierung des Algorithmus beweisen, betrachten wir dazu ein Beispiel. Das ist eigentlich immer eine gute Idee, wenn man mit einem Algorithmus oder einer Konstruktion konfrontiert ist und den Einstieg in das Erarbeiten nicht findet.

Bemerkung 2.7.10 *(mit Beispiel) Damit wir die Übersicht über die verschiedenen Durchläufe durch die* `WHILE`*-Schleife behalten, werden wir den auftretenden r jeweils einen Index geben, der beschreibt im wievielten Schleifendurchlauf sie entstanden sind. So starten wir mit $r_{-1} = a$ und $r_0 = b$ und erzeugen dann r_1,r_2 und so weiter. Damit liest sich die Rechnung des Algorithmus in induktiver Schreibweise für bereits bestimmte r_{i-1} und r_i wie folgt:*

$$r_{i+1} = r_{i-1} \bmod r_i.$$

In einem konkreten Beispiel haben wir dann für $a = 96$ und $b = 66$:

	a	b	*neuer Rest*	a *konkret*	b *konkret*	*neuer Rest*
Anfangswerte	r_{-1}	r_0	r_1	96	66	30
Durchlauf 1	r_0	r_1	r_2	66	30	6
Durchlauf 2	r_1	r_2	r_3	30	6	0

Damit wird wegen $r_3 = 0$ der Wert von r_2, also 6, vom Algorithmus zurückgegeben.

Beweis: (2.7.9) Terminierung:
Da r_{i+1} der Rest der Division von r_{i-1} durch r_i ist, gilt

$$d(r_0) > d(r_1) > \ldots d(r_i) > \ldots.$$

Es entsteht also eine strikt absteigende Sequenz von natürlichen Zahlen, die wegen der Endlichkeit der Menge $\{n \in \mathbb{N}_0 \mid n < d(r_0)\}$ nur endlich viele Elemente enthalten kann. Damit endet die Schleife nach endlich vielen Durchläufen, was bedeutet, dass zu diesem Zeitpunkt $r_n = 0$.

Korrektheit:
Es bleibt zu zeigen, dass r_{n-1} ein größter gemeinsamer Teiler der beiden Eingabewerte ist.
Wir wissen:

$$r_{i-1} = q_i \dot{r}_i + r_{i+1} \text{ für alle } 0 \leq i < n,$$

weswegen ein gemeinsamer Teiler zweier aufeinanderfolgender Reste r_{i-1} und r_i auch Teiler des darauffolgenden r_{i+1} und des vorausgehenden r_{i-2}, soweit deren Indizes noch zwischen 0 und $n-1$ liegen. Iterieren wir dieses Argument, so muss dieser Teiler gemeinsamer Teiler aller r_i sein.
Einerseits wissen wir ebenfalls:

$$r_{n-1} \mid r_{n-2} \text{ wegen } r_n = 0,$$

so dass r_{n-1} damit tatsächlich gemeinsamer Teiler von $r_{-1} = a$ und $r_0 = b$ sein muss. Andererseits muss aber auch jeder gemeinsame Teiler von $r_{-1} = a$ und $r_0 = b$ ein Teiler von r_{n-1}, weswegen r_{n-1} beide Bedingungen an einen größten gemeinsamen Teiler erfüllt.

□

Korollar 2.7.11 *(Bézout-Identität) Sei R ein euklidischer Ring und seien $a, b \in R$ mit $b \neq 0$. Sei ferner $d \in R$ ein größter gemeinsamer Teiler von a und b. Dann gilt*

$$\langle a, b \rangle = \langle d \rangle.$$

Überlegen Sie, wie man diese Aussage mit Hilfe der Schritte des euklidischen Algorithmus beweisen könnte. Hinweis: Alle r_i, die in Algorithmus 2.7.9 auftauchen, sind Linearkombinationen von a und b.

Bemerkung 2.7.12 *Bitte beachten Sie, dass wir im allgemeinen keine Eindeutigkeit für größte gemeinsame Teiler zweier Elemente eines euklidischen Rings fordern können. Alle zu einem gegebenen größten gemeinsamen Teiler assoziierten Elemente erfüllen ebenfalls beide Bedingungen an einen größten gemeinsamen Teiler.*

In $\mathbb{Z}$ hatten wir Eindeutigkeit erzwungen durch eine Positivitätsbedingung an den ggT*. Analog können wir in $K[t]$, dem Polynomring in einer Variable über einem Körper, Eindeutigkeit des* ggT *erzwingen durch* **Normieren** *des Polynoms, d.h. indem wir fordern, dass der Leitkoeffizient* 1 *ist.*

Satz 2.7.13 *Jeder euklidische Ring ist Hauptidealring.*

Verwenden Sie die Ideen aus dem Beweis von Satz 1.2.6 und passen Sie die (wenigen) Details an, die einer Änderung bedüfen.

Analog zum größten gemeinsamen Teiler können wir auch das kleinste gemeinsame Vielfache zweier Elemente eines Integritätsrings definieren:

Definition 2.7.14 *Sei R Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann heißt $k \in R$ ein kleinstes gemeinsames Vielfaches von a und b, falls gilt:*

a) k ist Vielfaches sowohl von a als auch von b

b) Jedes gemeinsame Vielfaches $\ell \in R$ a und b ist auch Vielfaches von k.

Satz 2.7.15 *Sei R ein Hauptidealring und seien $a, b \in R$ mit $b \neq 0$. Dann gilt:*

a) Es gibt ein kleinstes gemeinsames Vielfaches $k \in R$ von a und b, für das gilt:

$$\langle a \rangle \cap \langle b \rangle = \langle k \rangle.$$

b) Mit dem k aus a) und einem größten gemeinsamen Teiler $d \in R$ von a und b gilt:

$$\langle a \cdot b \rangle = \langle k \cdot d \rangle.$$

Beweis:

a) $J = \langle a \rangle \cap \langle b \rangle$ ist nach Lemma 2.6.10 wieder ein Ideal. Da R ein Hauptidealring ist kann dieses von einem Element $k \in R$ erzeugt werden. Die Elemente von J sind jedoch genau die gemeinsamen Vielfachen von a und b, so dass k ein gemeinsames Vielfaches von a und b sein muss. Da k sogar Erzeuger von J ist, ist jedes andere gemeinsame Vielfache von a und b darüberhinaus auch Vielfaches von k. Damit ist k ein kleinstes gemeinsames Vielfaches von a und b.

b) Dies istÜbungsaufgabe. Denken Sie an HA3.2b.

□