Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 17

Wir wollen für den Polynomring in einer Variablen über einem Körper zeigen, dass dort viele wichtige Sätze, die für den Ring der ganzen Zahlen gelten, ebenfalls Gültigkeit haben. Dass ein Hauptidealbereich vorliegt, haben wir schon gesehen. Es gilt aber auch wieder der euklidische Algorithmus und die eindeutige Primfaktorzerlegung. Um diese adäquat formulieren zu können, brauchen wir einige Vorbereitungen zur allgemeinen Teilbarkeitslehre.

Teilbarkeitsbegriffe

DEFINITION 1. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

LEMMA 2. *(Teilbarkeitsregeln) In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jedes Element a gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jedes Element a gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jedes $c \in R$.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid rb + sc$ für beliebige Elemente $r, s \in R$.*

Beweis. Siehe Aufgabe 17.5. □

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

LEMMA 3. *Sei R ein kommutativer Ring und $a, b \in R$. Dann gelten folgende Aussagen.*

(1) *Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.*
(2) *a ist eine Einheit genau dann, wenn $(a) = R = (1)$.*
(3) *Jede Einheit teilt jedes Element.*
(4) *Teilt a eine Einheit, so ist a selbst eine Einheit.*

Beweis. Das ist trivial. □

DEFINITION 4. Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ gibt derart, dass $a = ub$ ist.

Die Assoziiertheit ist eine Äquivalenzrelation, siehe Aufgabe 17.2. In $R = \mathbb{Z}$ sind zwei Zahlen genau dann zueinander assoziiert, wenn ihr Betrag übereinstimmt. Bei $R = K[X]$ sind zwei Polynome zueinander assoziiert, wenn sie durch Multiplikation mit einem Skalar $\lambda \in K$, $\lambda \neq 0$, ineinander übergehen. Durch diese Operation kann man erreichen, dass der Leitkoeffizient eins wird. Jedes Polynom ist also assoziiert zu einen normierten Polynom.

Das folgende Lemma besagt, dass es für die Teilbarkeitsrelation nicht auf Einheiten und Assoziiertheit ankommt.

LEMMA 5. *(Assoziiertheit und Ideale) In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.*
(2) *Ist R ein Integritätsbereich, so gilt $(a) = (b)$ genau dann, wenn a und b assoziiert sind.*

Beweis. Siehe Aufgabe 17.6 □

DEFINITION 6. Sei R ein kommutativer Ring und $a_1, \ldots, a_k \in R$. Dann heißt ein Element $t \in R$ *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn t jedes a_i teilt $(i = 1, \ldots, k)$. Ein Element $g \in R$ heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn g ein gemeinsamer Teiler ist und wenn jeder gemeinsame Teiler t dieses g teilt.

Die Elemente $a_1, \ldots, a_k$ heißen *teilerfremd*, wenn 1 ihr größter gemeinsamer Teiler ist.

BEMERKUNG 7. (Gemeinsamer Teiler) Eine Einheit ist immer ein gemeinsamer Teiler für jede Auswahl von Elementen. Ein größter gemeinsamer Teiler muss nicht existieren im Allgemeinen. Ist t ein gemeinsamer Teiler der $a_1, \ldots, a_k$ und u eine Einheit, so ist auch ut ein gemeinsamer Teiler der $a_1, \ldots, a_k$. Die Elemente $a_1, \ldots, a_k$ sind *teilerfremd* genau dann, wenn jeder gemeinsame Teiler davon eine Einheit ist (es gibt noch andere Definitionen von teilerfremd, die nicht immer inhaltlich mit dieser übereinstimmen).

LEMMA 8. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{a} = (a_1, \ldots, a_k)$ das davon erzeugte Ideal. Ein Element $t \in R$ ist ein gemeinsamer Teiler von $a_1, \ldots, a_k \in R$ genau dann, wenn $\mathfrak{a} \subseteq (t)$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn für jedes $s \in R$ mit $\mathfrak{a} \subseteq (s)$ folgt, dass $(t) \subseteq (s)$ ist. Ein größter gemeinsamer Teiler erzeugt also ein minimales Hauptoberideal von $\mathfrak{a}$.*

Beweis. Aus $\mathfrak{a} = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $(a_i) \subseteq (t)$ für $i = 1, \ldots, k$, was gerade bedeutet, dass t diese Elemente teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in (t)$ und da $a = (a_1, \ldots, a_k)$ das kleinste Ideal ist, das alle a_i enthält, muss $\mathfrak{a} \subseteq (t)$ gelten. Der zweite Teil folgt sofort aus dem ersten. □

Irreduzibel und prim

Für Teilbarkeitsuntersuchungen sind die beiden folgenden Begriffe fundamental. Unter bestimmten Voraussetzungen, etwa wenn ein Hauptidealbereich vorliegt, sind sie äquivalent.

DEFINITION 9. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Begriffsbildung orientiert sich offenbar an den Primzahlen. Dagegen taucht das Wort „prim“ in der folgenden Definition auf.

DEFINITION 10. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Für die ganzen Zahlen und für viele weitere Ringe fallen die beiden Begriffe zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

LEMMA 11. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

Teilbarkeitslehre in Hauptidealbereichen

SATZ 12. *(Lemma von Bezout) Sei R ein Hauptidealring. Dann gilt:*

Elemente $a_1, \ldots, a_n$ besitzen stets einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt Elemente $r_1, \ldots, r_n \in R$ mit $r_1a_1 + r_2a_2 + \ldots + r_na_n = d$.

Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der 1.

Beweis. Sei $I = (a_1, \ldots, a_n)$ das von den Elementen erzeugte Ideal. Da wir in einem Hauptidealring sind, handelt es sich um ein Hauptideal; es gibt also ein Element d mit $I = (d)$. Wir behaupten, dass d ein größter gemeinsamer Teiler der $a_1, \ldots, a_n$ ist. Die Inklusionen $(a_i) \subseteq I = (d)$ zeigen, dass es sich um einen gemeinsamen Teiler handelt. Sei e ein weiterer gemeinsamer Teiler der $a_1, \ldots, a_n$. Dann ist wieder $(d) = I \subseteq (e)$, was wiederum $e|d$ bedeutet. Die Darstellungsaussage folgt unmittelbar aus $d \in I = (a_1, \ldots, a_n)$.

Im teilerfremden Fall ist $I = (a_1, \ldots, a_n) = R$. □

BEMERKUNG 13. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dies ist ein Hauptidealbereich und daher gibt es zu gegebenen Polynomen $P_1, P_2, \ldots, P_n$ einen größten gemeinsamen Teiler, und diesen kann man darstellen als Linearkombination der gegebenen Polynome. Es gibt sogar ein effektives Verfahren, eine solche Darstellung explizit zu finden, das man (wie bei den ganzen Zahlen $\mathbb{Z}$) den *euklidischen Algorithmus* nennt. Wir beschränken uns auf den Fall von zwei Polynomen F und G. Man führt nun sukzessive eine Division mit Rest durch und erhält zunächst

$$F = Q_1 G + R_1 \, .$$

Dann erhält man

$$G = Q_2 R_1 + R_2, \; R_1 = Q_3 R_2 + R_3,$$

usw., bis schließlich der Rest $R_k = 0$ ist. Dieser Fall muss letztlich eintreten, da sich bei jedem Divisionsschritt der Grad der Reste reduziert. Der vorletzte Rest ist dann der größte gemeinsame Teiler, und man kann durch Zurückrechnen entlang der Gleichungen eine Darstellung dieses ggTs mit F und G finden.

LEMMA 14. *(von Euklid) Sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach Lemma 17.12 Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c{=}c1{=}c(ra + sb){=}cra + csb{=}a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

SATZ 15. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 17.11 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach Lemma 17.14) den anderen Faktor b. □

LEMMA 16. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von irreduziblen Elementen.*

Beweis. Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine

unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei a_{n+1} ein nicht-trivialer Teiler von a_n ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots .$$

Die Vereinigung dieser Ideale ist aber ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. $\square$