Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 6

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 euklidischer Bereich vorliegt, haben wir schon gesehen. Es gilt aber auch die eindeutige Primfaktorzerlegung. Um diese adäquat formulieren zu können, brauchen wir einige Vorbereitungen zur allgemeinen Teilbarkeitslehre.

Teilbarkeitsbegriffe

DEFINITION 6.1. 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 $a|b$.

Beispielsweise ist 2 ein Teiler von 6 in $\mathbb{Z}$, aber kein Teiler von 5. In $\mathbb{C}[X]$ ist $X - i$ ein Teiler von $X^2 + 1$, aber nicht von $X + 2$.

LEMMA 6.2. *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 6.7. □

DEFINITION 6.3. 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 6.3.

In $R = \mathbb{Z}$ sind zwei Zahlen genau dann zueinander assoziiert, wenn ihr Betrag übereinstimmt, wenn sie also gleich oder negativ zueinander sind. 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 6.4. *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 hiervon auch die Umkehrung.*

Beweis. Siehe Aufgabe 6.4. □

Irreduzibel und prim

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

DEFINITION 6.5. 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 6.6. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R 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 6.7. *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. □

In vielen wichtigen Ringen gilt hiervon auch die Umkehrung, worauf wir noch ausführlich zu sprechen kommen.

Irreduzible Polynome

Die irreduziblen Elemente im Polynomring $K[X]$ über einem Körper K sind nicht einfach zu charakterisieren. Die Antwort hängt auch wesentlich vom Körper ab, und nicht für jeden Körper lassen sich die irreduziblen Polynome übersichtlich beschreiben. Bei Irreduzibilitätsfragen kann man stets mit Einheiten multiplizieren, daher muss man nur normierte Polynome untersuchen.

Beispiel 6.8. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2+1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2+1 = (X+i)(X-i)\,.$$

Ebenso ist das Polynom $X^2-5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2-5 = (X-\sqrt{5})(X+\sqrt{5})\,.$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.

Als echte Faktoren für ein Polynom kommen nur Polynome von kleinerem Grad in Frage. Insbesondere sind daher *lineare Polynome*, also Polynome von Typ $aX+b$, $a \neq 0$, stets irreduzibel. Eine notwendige Bedingung an die Irreduzibilität eines Polynoms $P \in K[X]$ ist wegen Lemma 5.5, dass es keine Nullstelle in K besitzt. Deshalb und aufgrund des Fundamentalsatzes der Algebra sind daher in $\mathbb{C}[X]$ die linearen Polynome die einzigen irreduziblen Polynome.

Lemma 6.9. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann ist ein Polynom vom Grad zwei oder drei genau dann irreduzibel, wenn es keine Nullstelle in K besitzt.*

Beweis. In einer echten Primfaktorzerlegung von P, $\operatorname{grad}(P) \leq 3$, muss ein Polynom vom Grad eins vorkommen, also ein lineares Polynom. Ein lineares Polynom $X-a$ teilt aber nach Lemma 5.5 das Polynom P genau dann, wenn $P(a)=0$ ist. □

Beispiel 6.10. Das Polynom X^4+1 ist im Reellen stets positiv und hat daher keine reelle Nullstelle. Daher besitzt es in $\mathbb{R}[X]$ nach Lemma 5.5 auch keinen linearen Faktor. Wegen der Zerlegung

$$X^4+1 \;=\; \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$$

ist das Polynom aber nicht irreduzibel.

Größter gemeinsamer Teiler

DEFINITION 6.11. 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.

„Größer“ ist hier bezüglich der Teilbarkeitsrelation zu verstehen, wenn b von a geteilt wird, so gilt es gemäß diesem Sprachgebrauch als größer. Dies rührt natürlich von der Situation in $\mathbb{N}$ her, wo Vielfache in der Tat größer im Sinne der natürlichen Ordnung als die Teiler sind.

BEMERKUNG 6.12. 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).

DEFINITION 6.13. Es sei R ein kommutativer Ring und

$$a_1, \ldots, a_n \in R\,.$$

Ein Element $b \in R$ heißt ein *gemeinsames Vielfaches* der $a_1, \ldots, a_n$, wenn b ein Vielfaches von jedem a_i ist, also von jedem a_i geteilt wird. b heißt ein *kleinstes gemeinsames Vielfaches* der $a_1, \ldots, a_n$, wenn b ein gemeinsames Vielfaches ist und wenn jedes andere gemeinsame Vielfache ein Vielfaches von b ist.