Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 2

Schon in der ersten Vorlesung haben wir zahlentheoretische Fragestellungen algebraisch mit Ringen formuliert. In dieser Vorlesung werden wir grundlegende ringtheoretische Konzepte einführen, und zwar insbesondere solche, die mit der Teilbarkeit zu tun haben.

Einige ringtheoretische Konzepte

In einem Körper folgt aus $xy = 0$, dass ein Faktor 0 sein muss. Diese Eigenschaft gilt nicht für beliebige Ringe. Ein Element $f \in R$ in einem kommutativen Ring heißt *Nichtnullteiler*, wenn aus $fg = 0$ stets $g = 0$ folgt. Man nennt einen Ring *nullteilerfrei*, wenn 0 der einzige Nullteiler ist.

Definition 2.1. Ein kommutativer, nullteilerfreier, von 0 verschiedener Ring heißt *Integritätsbereich*.

Der Ring $\mathbb{Z}$ der ganzen Zahlen und die Polynomringe $K[X]$ über einem Körper K sind Integritätsbereiche. Das sind für uns besonders wichtigste Beispiele. Ein Unterring eines Körpers ist ein Integritätsbereich.

Definition 2.2. Es 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 $c \in R$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Eine Einheit kann man als einen Teiler der 1 auffassen. Idealtheoretisch kann man die Eigenschaft, dass a das Element b teilt, als Zugehörigkeit $b \in Ra$ auffassen.

Definition 2.3. Es sei R ein kommutativer Ring. Man sagt, dass zwei Elemente $a, b \in R$ *teilerfremd* sind, wenn jedes Element $c \in R$, das sowohl a als auch b teilt, eine Einheit ist.

Definition 2.4. 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 2.5. 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 p 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 prim und irreduzibel zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

LEMMA 2.6. *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. □

Irreduzible Polynome

BEISPIEL 2.7. Ein nichtkonstantes Polynom $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$, wobei K einen Körper bezeichne, ist genau dann irreduzibel, wenn es keine Produktdarstellung $P = QR$ gibt, die die Gradbedingung

$$0 < \operatorname{grad}(Q) < \operatorname{grad}(P)$$

erfüllt.

Die irreduziblen Polynome sind gerade die irreduziblen Elemente im Polynomring $K[X]$ im Sinne der obigen allgemeinen ringtheoretischen Definition. Nach der weiter unten zu beweisenden Aussage könnte man auch von Primelementen bzw. Primpolynomen sprechen. Eine weitere wichtige Charakterisierung ist die Restklassencharakterisierung, die wir in Lemma 3.9 kennenlernen werden.

BEISPIEL 2.8. 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

$$X^2 + 1 = (X + \mathrm{i})(X - \mathrm{i}).$$

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

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

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

Die Existenz der Faktorzerlegung in der folgenden Aussage folgt unmittelbar aus der Definition von irreduzibel, für die Eindeutigkeit muss man aber wissen, dass in einem Polynomring die irreduziblen Polynome auch Primpolynome sind (siehe unten).

LEMMA 2.9. *Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Dann gibt es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung*

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$.

Beweis. Siehe Aufgabe 2.27. □

Hauptidealbereiche

DEFINITION 2.10. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

SATZ 2.11. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealbereich.*

Beweis. Zunächst ist $\mathbb{Z}$ ein Integritätsbereich. Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Damit ist I insbesondere eine (additive) Untergruppe von $\mathbb{Z}$ und hat nach Satz 44.3 (Lineare Algebra (Osnabrück 2017-2018)) die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal. □

SATZ 2.12. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

Beweis. Es sei I ein von 0 verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) \mid P \in I,\, P \neq 0\}\,.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Die Inklusion $\supseteq$ ist klar. Zum Beweis von $\subseteq$ sei $P \in I$ gegeben. Aufgrund von Satz 19.4 (Lineare Algebra (Osnabrück 2017-2018)) gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

In jedem Hauptidealbereich gibt es stes eine Zerlegung in irreduzible Elmente.

LEMMA 2.13. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ als ein Produkt von irreduziblen Elementen darstellen.*

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

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

Die Vereinigung dieser Ideale ist aber nach Aufgabe 2.13 ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. □

Über diese Aussage hinaus ist aber in einem Hauptidealbereich jedes irreduzible Element auch prim und damit gibt es auch stets eine Faktorzerlegung in Primelemente. Der Nachweis davon braucht einige Vorbereitungen, nämlich das *Lemma von Bezout* und das *Lemma von Euklid*.

LEMMA 2.14. *Es sei R ein Hauptidealbereich und seien $a, b \in R$ teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Wir betrachten das von a und b erzeugte Ideal $I = (a, b)$. Da R ein Hauptidealbereich ist, gibt es ein $c \in R$ mit $(a, b) = (c)$. Daher ist c ein Teiler von a und von b. Die Teilerfremdheit impliziert, dass c eine Einheit ist. Wegen $c \in (a, b)$ gibt es eine Darstellung $c = ua + vb$. Multiplikation mit c^{-1} ergibt die Darstellung der 1. □

LEMMA 2.15. *Es 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 dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = acr + ads = a(cr + ds),$$

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

KOROLLAR 2.16. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 2.6 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 dem Lemma von Euklid den anderen Faktor b. □

Eindeutige Primfaktorzerlegung

DEFINITION 2.17. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

SATZ 2.18. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*
(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein zu q_2 assoziiertes Element ergibt. Das gekürzte Element $p_2 \cdots p_s$ hat eine Faktorzerlegung mit $s-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. $\square$

SATZ 2.19. *Ein Hauptidealbereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Korollar 2.16, Lemma 2.13 und Satz 2.18. □

KOROLLAR 2.20. *Es sei R ein faktorieller Ring und seien a und b zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

(wobei die u, v Einheiten sind und die Exponenten auch 0 sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ für alle Exponenten $i = 1, \ldots, k$ ist.

Beweis. Wenn die Exponentenbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann

$$b = a\big(vu^{-1}p_1^{s_1-r_1} \cdots p_k^{s_k-r_k}\big)$$

schreiben, was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in einem faktoriellen Ring. □

Abbildungsverzeichnis