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

Einführung in die Algebra

Vorlesung 13

Einheiten

DEFINITION 1. Ein Element u in einem Ring R heißt *Einheit*, wenn es ein Element $v \in R$ gibt mit

$$uv = vu = 1\,.$$

Das Element v mit der Eigenschaft $uv = vu = 1$ ist dabei eindeutig bestimmt. Hat nämlich auch w die Eigenschaft $uw = wu = 1$, so ist

$$v = v1 = v(uw) = (vu)w = 1w = w\,.$$

Das im Falle der Existenz eindeutig bestimmte v mit $uv = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit

$$u^{-1}\,.$$

Im kommutativen Fall muss man natürlich nur die Eigenschaft $uv = 1$ überprüfen. Eine Einheit ist stets ein Nichtnullteiler. Aus $ux = 0$ folgt ja sofort $x = u^{-1}ux = 0$.

DEFINITION 2. Die *Einheitengruppe* in einem Ring R ist die Teilmenge aller Einheiten in R. Sie wird mit $R^\times$ bezeichnet.

Die Menge aller Einheiten in einem Ring bilden in der Tat eine Gruppe (bzgl. der Multiplikation mit 1 als neutralem Element). Wenn v und w die Inversen v^{-1} und w^{-1} haben, so ist das Inverse von vw gleich $w^{-1}v^{-1}$.

Zu einer Einheit $u \in R$ machen auch Potenzen mit einem negativen Exponenten Sinn, d.h. es ist dann u^n für $n \in \mathbb{Z}$ definiert. Die Zahl -1 (also das Negative zu 1) ist stets eine Einheit, da ja $(-1)(-1) = 1$ ist. Bei $\mathbb{Z}$ besteht die Einheitengruppe aus diesen beiden Elementen, also $\mathbb{Z}^\times = \{1, -1\}$. Die Null ist mit der Ausnahme des Nullrings nie eine Einheit. Für eine Einheit ist auch die *Bruchschreibweise* erlaubt und gebräuchlich. D.h. wenn u eine Einheit ist und $x \in R$ beliebig, so setzt man

$$\frac{x}{u} = xu^{-1}\,.$$

Wie gesagt, der Zähler muss eine Einheit sein!

Wenn außer der Null alle Elemente Einheiten sind, so verdient das einen eigenen Namen, wovon der folgende Abschnitt handelt.

Körper

Viele wichtige Zahlbereiche haben die Eigenschaft, dass man durch jede Zahl - mit der Ausnahme der Null! - auch dividieren darf. Dies wird durch den Begriff des Körpers präzisiert.

Definition 3. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Es sind also die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$ Körper, die ganzen Zahlen dagegen nicht. Wir werden im Laufe dieser Vorlesung noch viele weitere Körper kennenlernen. Einen Körper kann man auch charakterisieren als einen kommutativen Ring, bei der die von null verschiedenen Elemente eine Gruppe (mit der Multiplikation) bilden.

Definition 4. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

Wenn ein Unterring $R \subseteq K$ in einem Körper vorliegt, so muss man nur noch schauen, ob R mit jedem von null verschiedenen Element x auch das Inverse x^{-1} (das in K exisitiert) enthält. Bei einem Unterring $R \subseteq S$, wobei R ein Körper ist, aber S nicht, so spricht man nicht von einem Unterkörper. Die Situation, wo ein Körper in einem anderen Körper liegt, wird als Körpererweiterung bezeichnet.

Definition 5. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Ringhomomorphismen

Definition 6. Seien R und S Ringe. Eine Abbildung

$$\varphi : R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(2) $\varphi(1) = 1$
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Ein Ringhomomorphismus ist also zugleich ein Gruppenhomomorphismus für die additive Struktur und ein Monoidhomomorphismus für die multiplikative Struktur. Einen bijektiven Ringhomomorphismus nennt man einen *Ringisomorphismus*, und zwei Ringe heißen *isomorph*, wenn es einen Ringisomorphismus zwischen ihnen gibt. Zu einem Unterring $S \subseteq R$ ist die natürliche Inklusion ein Ringhomomorphismus. Die konstante Abbildung $R \longrightarrow 0$ in den Nullring ist stets ein Ringhomomorphismus, dagegen ist die umgekehrte Abbildung, also $R \longrightarrow 0$, nur bei $R = 0$ ein Ringhomomorphismus.

Satz 7. *Sei R ein Ring. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\mathbb{Z} \longrightarrow R.$$

Beweis. Ein Ringhomomorphismus muss die 1 auf die 1_R abbilden. Deshalb gibt es nach Lemma 5.5 genau einen Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow (R, +, 0),\ n \longmapsto n1_R.$$

Wir müssen zeigen, dass diese Abbildung auch die Multiplikation respektiert, d.h. dass $(mn)1_R = (m1_R) * (n1_R)$ ist, wobei $*$ hier die Multiplikation in R bezeichnet. Dies folgt aber aus dem allgemeinen Distributivgesetz (Lemma 12.5). □

Den in dieser Aussage konstruierten und eindeutig bestimmten Ringhomomorphismus nennt man auch den *kanonischen Ringhomomorphismus* (oder den *charakteristischen Ringhomomorphismus*) von $\mathbb{Z}$ nach R.

Definition 8. Die *Charakteristik* eines kommutativen Ringes R ist die kleinste positive natürliche Zahl n mit der Eigenschaft $n \cdot 1_R = 0$. Die Charakteristik ist 0, falls keine solche Zahl existiert.

Die Charakteristik beschreibt genau den Kern des obigen kanonischen (charakteristischen) Ringhomomorphismus.

Lemma 9. *Sei R ein Integritätsbereich. Dann ist die Charakteristik von R null oder eine Primzahl.*

Beweis. Die Charakteristik sei $n > 0$ und es sei angenommen, dass n keine Primzahl ist, also eine Zerlegung $n = ab$ mit kleineren Zahlen $0 < a, b < n$ besitzt. Nach Definition der Charakteristik ist $n_R = 0$ in R und n ist die kleinste positive Zahl mit dieser Eigenschaft. Aufgrund von Satz 13.7 ist $a_R b_R = n_R = 0$, so dass wegen integer einer der Faktoren null sein muss, im Widerspruch zur Minimalität von n. □

Satz 10. *Sei R ein Ring und sei* $\mathrm{End}(R)$ *der Endomorphismenring der additiven Gruppe $(R, +, 0)$. Dann gibt es einen kanonischen injektiven Ringhomomorphismus*

$$R \longrightarrow \mathrm{End}(R),\ f \longmapsto (g \mapsto fg).$$

Beweis. Für jedes $f \in R$ ist die Multiplikation

$$\mu_f : R \longrightarrow R,\ g \longmapsto fg,$$

ein Gruppenhomomorphismus, wie direkt aus der Distributivität und der Eigenschaft $f0 = 0$ folgt. Die Gesamtabbildung ist also wohldefiniert.

Für die Gesamtzuordnung $f \mapsto \mu_f$ gilt zunächst $\mu_0 = 0$ und $\mu_1 = \mathrm{id} = 1$. Wegen

$$\mu_{f_1+f_2}(g) = (f_1 + f_2)g = f_1 g + f_2 g = \mu_{f_1}(g) + \mu_{f_2}(g) = (\mu_{f_1} + \mu_{f_2})(g)$$

für jedes $g \in R$ ist μ additiv. Die Multiplikativität folgt aus

$$\mu_{f_1 f_2}(g) = f_1 f_2 g = \mu_{f_1}(f_2 g) = \mu_{f_1}(\mu_{f_2}(g)) = (\mu_{f_1} \circ \mu_{f_2})(g).$$

Schließlich ist die Abbildung injektiv, da aus $\mu_f = 0$ folgt, dass insbesondere $f = f1 = 0$ sein muss. □

LEMMA 11. *Seien R und S Ringe und sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Es sei $u \in R^\times$ eine Einheit. Dann ist auch $\varphi(u)$ eine Einheit. Mit anderen Worten: ein Ringhomomorphismus induziert einen Gruppenhomomorphismus

$$R^\times \longrightarrow S^\times.$$

Beweis. Das ist trivial. □

Ideale

Wir beschränken uns im Folgenden auf kommutative Ringe, um nicht zwischen Linksidealen, Rechtsidealen und beidseitigen Idealen unterscheiden zu müssen.

DEFINITION 12. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich die zweite oben angeführte Eigenschaft erfüllt. Die einfachsten Ideale sind das *Nullideal* 0 und das *Einheitsideal* R.

Für den Ring der ganzen Zahlen $\mathbb{Z}$ sind Untergruppen und Ideale identische Begriffe. Dies folgt einerseits aus der Gestalt $H = \mathbb{Z}d$ für jede Untergruppe von $\mathbb{Z}$, aber ebenso direkt aus der Tatsache, dass für $k \in H$ und beliebiges $r \in \mathbb{N}$ gilt $rk = k + k + \ldots + k$ (r-mal) und entsprechend für negatives r. Die Skalarmultiplikation mit einem beliebigen Ringelement lässt sich also bei $\mathbb{Z}$ auf die Addition zurückführen.

DEFINITION 13. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}.$$

heißt *Hauptideal*.

Wir werden auf Hauptideale im Rahmen der Teilbarkeitstheorie bald zurückkommen.

Definition 14. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \, ,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

Es handelt sich dabei um das kleinste Ideal in R, das alle a_j, $j \in J$, enthält. Dass ein solches Ideal existiert ist auch deshalb klar, weil der Durchschnitt von einer beliebigen Familie von Idealen wieder ein Ideal ist.

Die Idealtheorie in einem Ring reflektiert viele Eigenschaften des Ringes, worauf wir im Rahmen der Teilbarkeitstheorie zurückkommen werden. Eine erste Beobachtung in diese Richtung kommt im folgenden Lemma zum Ausdruck.

Lemma 15. *Es sei R ein kommutativer Ring. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Körper.*
(2) *Es gibt in R genau zwei Ideale.*

Beweis. Wenn R ein Körper ist, so gibt es das Nullideal und das Einheitsideal, die voneinander verschieden sind. Sei I ein von null verschiedenes Ideal in R. Dann enthält I ein Element $x \neq 0$, das eine Einheit ist. Damit ist $1 = xx^{-1} \in I$ und damit $I = R$.

Sei umgekehrt R ein kommutativer Ring mit genau zwei Idealen. Dann kann R nicht der Nullring sein. Sei nun x ein von null verschiedenes Element in R. Das von x erzeugte Hauptideal Rx ist $\neq 0$ und muss daher mit dem anderen Ideal, also mit dem Einheitsideal übereinstimmen. Das heißt insbesondere, dass $1 \in Rx$ ist. Das bedeutet also $1 = xr$ für ein $r \in R$, so dass x eine Einheit ist. □

Ideale unter einem Ringhomomorphismus

Der Zusammenhang zwischen Ringhomomorphismen und Idealen wird durch folgenden Satz hergestellt.

Satz 16. *Seien R und S kommutative Ringe und sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Dann ist der Kern

$$\ker(\varphi) = \{f \in R : \varphi(f) = 0\}$$

ein Ideal in R.

Beweis. Sei $I := \varphi^{-1}(0)$. Wegen $\varphi(0) = 0$ ist $0 \in I$. Seien $a, b \in I$. Das bedeutet $\varphi(a) = 0$ und $\varphi(b) = 0$. Dann ist

$$\varphi(a+b)=\varphi(a)+\varphi(b)=0+0=0$$

und daher $a + b \in I$.

Sei nun $a \in I$ und $r \in R$ beliebig. Dann ist

$$\varphi(ra)=\varphi(r)\varphi(a)=\varphi(r)\cdot 0=0,$$

also ist $ra \in I$. □

Da ein Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der zugrunde liegenden additiven Gruppe ist, gilt wieder das Kernkriterium (Lemma 5.12) für die Injektivität. Eine Anwendung davon ist das folgende Korollar.

KOROLLAR 17. *Es sei K ein Körper und S ein vom Nullring verschiedener Ring. Es sei*

$$\varphi : K \longrightarrow S$$

ein Ringhomomorphismus. Dann ist φ injektiv.

Beweis. Es genügt nach Lemma 5.12 zu zeigen, dass der Kern der Abbildung gleich null ist. Nach Satz 13.16 ist der Kern ein Ideal. Da die 1 auf $1 \neq 0$ geht, ist der Kern nicht ganz K. Da es nach Lemma 13.15 in einem Körper überhaupt nur zwei Ideale gibt, muss der Kern das Nullideal sein. □