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

Elemente der Algebra

Vorlesung 3

In dieser Vorlesung besprechen wir Körper, das sind kommutative Ringe, in denen jedes von 0 verschiedene Element ein Inverses (bezüglich der Multiplikation) besitzt. Solche Elemente nennt man Einheiten. Als einen wichtigen Körper führen wir die komplexen Zahlen ein.

Einheiten

DEFINITION 3.1. Ein Element u in einem Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit

$$uv = vu = 1$$

gibt.

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 $uv = vu = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit

$$u^{-1}$$

oder auch mit $\frac{1}{u}$. Im kommutativen Fall muss man natürlich nur die Eigenschaft $uv = 1$ überprüfen. Eine Einheit ist stets ein Nichtnullteiler. Aus $ux = 0$ folgt ja sofort (unter Verwendung von Lemma 2.5 (1)) $x = u^{-1}ux = 0$.

DEFINITION 3.2. 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 (bezüglich der Multiplikation mit 1 als neutralem Element). Wenn nämlich v und w die Inversen v^{-1} und w^{-1} haben, so ist das Inverse von vw gleich $w^{-1}v^{-1}$ und somit ist das Produkt von zwei Einheiten wieder eine Einheit.

Zu einer Einheit $u \in R$ machen auch Potenzen mit einem negativen Exponenten Sinn, d.h. es ist dann u^n für alle $n \in \mathbb{Z}$ definiert. Die Zahl -1 (also das Negative zu 1) ist stets eine Einheit, da ja (nach Lemma 2.5 (3)) $(-1)(-1) = 1$ 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.

Beispiel 3.3. Wir betrachten den Ring $\mathbb{Z}/(5)$. Die Elemente 1 und $4 = -1$ sind wie in jedem Ring Einheiten. Wegen

$$2 \cdot 3 = 6 = 1$$

sind 2 und 3 invers zueinander und insbesondere Einheiten. Die Einheitengruppe ist also $\{1, 2, 3, 4\} = \mathbb{Z}/(5) \setminus \{0\}$.

Bei $\mathbb{Z}/(12)$ sind wieder 1 und $11 = -1$ Einheiten. Ferner sind wegen

$$5 \cdot 5 = 25 = 1$$

und

$$7 \cdot 7 = 49 = 1$$

auch 5 und 7 Einheiten. Die anderen acht Zahlen sind keine Einheiten.

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 Nenner 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 wie $\mathbb{Q}$ und $\mathbb{R}$ 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 3.4. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Es wird also explizit gefordert, dass $1 \neq 0$ ist und dass jedes von 0 verschiedene Element eine Einheit ist. Die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ bilden einen Körper, die ganzen Zahlen dagegen nicht. Im obigen Beispiel haben wir gesehen, dass $\mathbb{Z}/(5)$ ein Körper ist, aber $\mathbb{Z}/(12)$ 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 0 verschiedenen Elemente eine Gruppe (mit der Multiplikation) bilden.

Definition 3.5. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

Beispielsweise ist $\mathbb{Q}$ ein Unterkörper von $\mathbb{R}$. 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 existiert) 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 3.6. 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.*

Komplexe Zahlen

Die Produktmenge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ ist mit komponentenweiser Addition und komponentenweiser Multiplikation ein kommutativer Ring (wobei $(0,0)$ das Nullelement und $(1,1)$ das Einselement ist). Es handelt sich aber nicht um einen Körper, da beispielsweise $(1,0) \cdot (0,1) = (0,0)$ zeigt, dass es darin Nullteiler gibt. Allerdings kann man $\mathbb{R}^2$ mit einer anderen Multiplikation zu einem Körper machen.

DEFINITION 3.7. Die Menge

$$\mathbb{R}^2$$

mit $0 := (0,0)$ und $1 := (1,0)$, mit der komponentenweisen Addition und der durch

$$(a,b) \cdot (c,d) := (ac - bd, ad + bc)$$

definierten Multiplikation nennt man *Körper der komplexen Zahlen.* Er wird mit

$$\mathbb{C}$$

bezeichnet.

Die Addition ist also einfach die vektorielle Addition im $\mathbb{R}^2$, während die Multiplikation eine neuartige Verknüpfung ist, die zwar numerisch einfach durchführbar ist, an die man sich aber dennoch gewöhnen muss.

LEMMA 3.8. *Die komplexen Zahlen bilden einen Körper.*

Beweis. Siehe Aufgabe 3.11. □

Hierbei sind nur das Assoziativgesetz, das Distibutivgesetz und die Existenz der Inversen nicht unmittelbar klar.

Wir lösen uns von der Paarschreibweise und schreiben

$$a + bi := (a,b).$$

Insbesondere ist $i = (0,1)$, diese Zahl heißt *imaginäre Einheit.* Diese Zahl hat die wichtige Eigenschaft

$$i^2 = -1.$$

Aus dieser Eigenschaft ergeben sich sämtliche algebraischen Eigenschaften der komplexen Zahlen durch die Körpergesetze. So kann man sich auch die obige Multiplikationsregel merken, es ist ja

$$(a+bi)(c+di) = ac+adi+bic+bidi = ac+bdi^2+(ad+bc)i = ac-bd+(ad+bc)i.$$

Wir fassen eine reelle Zahl a als die komplexe Zahl $a + 0i = (a, 0)$ auf. In diesem Sinne ist $\mathbb{R} \subset \mathbb{C}$ eine Körpererweiterung. Es ist gleichgültig, ob man zwei reelle Zahlen als reelle Zahlen oder als komplexe Zahlen addiert oder multipliziert.

Definition 3.9. Zu einer komplexen Zahl

$$z = a + bi$$

heißt

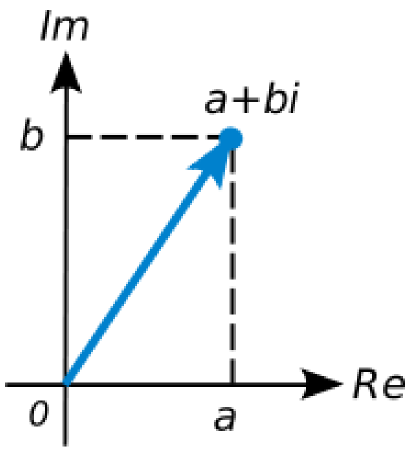
$$\mathrm{Re}\ (z) = a$$

der *Realteil* von z und

$$\mathrm{Im}\ (z) = b$$

heißt der *Imaginärteil* von z.

Man sollte sich allerdings die Menge der komplexen Zahlen nicht als etwas vorstellen, das weniger real als andere Zahlensysteme ist. Die Konstruktion der komplexen Zahlen aus den reellen Zahlen ist bei Weitem einfacher als die Konstruktion der reellen Zahlen aus den rationalen Zahlen. Allerdings war es historisch ein langer Prozess, bis die komplexen Zahlen als Zahlen anerkannt wurden; das Irreale daran ist, dass sie einen Körper bilden, der nicht angeordnet werden kann, und dass es sich daher scheinbar um keine Größen handelt, mit denen man sinnvollerweise etwas messen kann.



Man kann sich die komplexen Zahlen als die Punkte in einer Ebene vorstellen; für die additive Struktur gilt ja einfach $\mathbb{C} = \mathbb{R}^2$. In diesem Zusammenhang spricht man von der *Gaussschen Zahlenebene*. Die horizontale Achse nennt man dann die *reelle Achse* und die vertikale Achse die *imaginäre Achse*.

Lemma 3.10. *Real- und Imaginärteil von komplexen Zahlen erfüllen folgende Eigenschaften (für z und w aus $\mathbb{C}$).*

(1) $z = \mathrm{Re}\,(z) + \mathrm{Im}\,(z)\,i$.
(2) $\mathrm{Re}\,(z+w) = \mathrm{Re}\,(z) + \mathrm{Re}\,(w)$.
(3) $\mathrm{Im}\,(z+w) = \mathrm{Im}\,(z) + \mathrm{Im}\,(w)$.
(4) *Für* $r \in \mathbb{R}$ *ist*

$$\mathrm{Re}\,(rz) = r\,\mathrm{Re}\,(z) \ \textit{ und } \ \mathrm{Im}\,(rz) = r\,\mathrm{Im}\,(z)\ .$$

(5) *Es ist* $z = \mathrm{Re}\,(z)$ *genau dann, wenn* $z \in \mathbb{R}$ *ist, und dies ist genau dann der Fall, wenn* $\mathrm{Im}\,(z) = 0$ *ist.*

Beweis. Siehe Aufgabe 3.16. □

Definition 3.11. Die Abbildung

$$\mathbb{C} \longrightarrow \mathbb{C},\ z = a + bi \longmapsto \overline{z} := a - bi,$$

heißt *komplexe Konjugation.*

Zu z heißt $\overline{z}$ die *konjugiert-komplexe Zahl* von z. Geometrisch betrachtet ist die komplexe Konjugation zu $z \in \mathbb{C}$ einfach die Achsenspiegelung an der reellen Achse.

Lemma 3.12. *Für die komplexe Konjugation gelten die folgenden Rechenregeln (für beliebige* $z, w \in \mathbb{C}$*).*

(1) $\overline{z+w} = \overline{z} + \overline{w}$.
(2) $\overline{-z} = -\overline{z}$.
(3) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
(4) *Für* $z \neq 0$ *ist* $\overline{1/z} = 1/\overline{z}$.
(5) $\overline{\overline{z}} = z$.
(6) $\overline{z} = z$ *genau dann, wenn* $z \in \mathbb{R}$ *ist.*

Beweis. Siehe Aufgabe 3.24. □

Das Quadrat d^2 einer reellen Zahl ist stets nichtnegativ, und die Summe von zwei nichtnegativen reellen Zahlen ist wieder nichtnegativ. Zu einer nichtnegativen reellen Zahl c gibt es eine eindeutige nichtnegative *Quadratwurzel* $\sqrt{c}$. Daher liefert folgende Definition eine wohldefinierte nichtnegative reelle Zahl.

Definition 3.13. Zu einer komplexen Zahl

$$z = a + bi$$

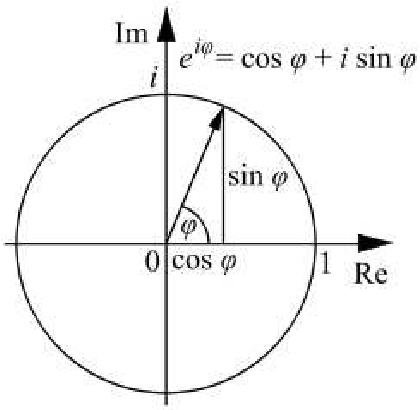
ist der *Betrag* durch

$$|z| = \sqrt{a^2 + b^2}$$

definiert.

Der Betrag einer komplexen Zahl z ist aufgrund des *Satzes des Pythagoras* der Abstand von z zum Nullpunkt $0 = (0,0)$. Insgesamt ist der Betrag eine Abbildung

$$\mathbb{C} \longrightarrow \mathbb{R}_{\geq 0},\ z \longmapsto |z|\,.$$



Die Menge aller komplexen Zahlen mit einem bestimmten Betrag bilden einen Kreis mit dem Nullpunkt als Mittelpunkt und mit dem Betrag als Radius. Insbesondere bilden alle komplexen Zahlen mit dem Betrag 1 den *komplexen Einheitskreis*. Es sei hier erwähnt, dass das Produkt von zwei komplexen Zahlen auf dem Einheitskreis sich ergibt, indem man die zugehörigen Winkel, gemessen von der positiven reellen Achse aus gegen den Uhrzeigersinn, addiert.

LEMMA 3.14. *Für eine komplexe Zahl z gelten die folgenden Beziehungen.*

(1) $|z| = \sqrt{z\ \overline{z}}$.
(2) $\operatorname{Re}(z) = \frac{z+\overline{z}}{2}$.
(3) $\operatorname{Im}(z) = \frac{z-\overline{z}}{2i}$.
(4) $\overline{z} = \operatorname{Re}(z) - i\operatorname{Im}(z)$.
(5) *Für $z \neq 0$ ist $z^{-1} = \frac{\overline{z}}{|z|^2}$.*

Beweis. Siehe Aufgabe 3.17. $\square$

LEMMA 3.15. *Für den Betrag von komplexen Zahlen gelten folgende Eigenschaften.*

(1) *Für reelles z stimmen reeller und komplexer Betrag überein.*
(2) *Es ist $|z| = 0$ genau dann, wenn $z = 0$ ist.*
(3) $|z| = |\overline{z}|$.
(4) $|zw| = |z|\,|w|$.
(5) $|\operatorname{Re}(z)|\,, |\operatorname{Im}(z)| \leq |z|$.
(6) $|z+w| \leq |z| + |w|$.
(7) *Für $z \neq 0$ ist $|1/z| = 1/\,|z|$.*

Beweis. Wir zeigen die Dreiecksungleichung, für die anderen Aussagen siehe Aufgabe 3.18. Zunächst gilt nach (5) für jede komplexe Zahl u die Abschätzung $\mathrm{Re}\,(u) \leq |u|$. Daher ist

$$\mathrm{Re}\,(z\overline{w}) \leq |z|\,|w| \ ,$$

und somit ist

$$\begin{aligned} |z+w|^2 &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \\ &= |z|^2 + 2\,\mathrm{Re}\,(z\overline{w}) + |w|^2 \\ &\leq |z|^2 + 2\,|z|\,|w| + |w|^2 \\ &= (|z|+|w|)^2. \end{aligned}$$

Durch Wurzelziehen ergibt sich die gewünschte Abschätzung. $\square$

Abbildungsverzeichnis