Fakultät für Mathematik
Heinrich Heine-Universität Düsseldorf

PD Dr. Markus Perling
Sommersemester 2014

Lineare Algebra 1

Siebte Woche, 21.5.2014

§4 Ringe und Körper (Fortsetzung)

Satz: *Es sei R ein Ring und $x \in R$. Ist x eine Einheit, dann ist x kein Nullteiler.*

Korollar: *Ein Körper besitzt keine Nullteiler außer der* 0.

Satz: *Es seien K ein Körper, R ein Ring, der nicht der Nullring ist und $f : K \longrightarrow R$ ein Ringhomomorphismus. Dann ist f injektiv.*

Definition: Ein Ringhomomorphismus $f : K \longrightarrow L$, wobei K und L Körper sind, heißt *Körperhomomorphismus.*

Bemerkung: Es folgt aus obigem Satz, daß Körperhomomorphismen immer injektiv sind. In diesem Falle kann man, wenn man möchte, K mit seinem Bild in L identifizieren und als *Unterkörper* von L auffassen. Umgekehrt sagt man auch, daß L eine *Körpererweiterung* von K ist.

Der erweiterte Euklidische Algorithmus

Definition: Für alle $a, b, p \in \mathbb{Z}$ legen sagen wir:

(i) a *teilt* b genau dann, wenn es ein $c \in \mathbb{Z}$ gibt, so daß gilt $a \cdot c = b$. Man sagt, daß a ein *Teiler* von b ist und schreibt kurz $a|b$. Ist a *kein* Teiler von b, dann schreibt man auch $a \nmid b$.

(ii) p heißt *Primzahl*, wenn $p > 1$ und p genau die beiden Teiler 1 und p besitzt.

(iii) a und b heißen *teilerfremd* (bzw. *koprim*, wenn 1, -1 die einzigen gemeinsamen Teiler sind.

(iv) Eine Zahl $c \in \mathbb{Z}$ heißt *größter gemeinsamer Teiler*, kurz $\mathrm{ggT}(a, b)$, wenn gilt:

$$c|a \text{ und } c|b \Rightarrow$$

Satz (Erweiterter Euklidischer Algorithmus)**:** *Es seien $a, b \in \mathbb{Z}$. Wir setzen $a_0 := a$, $a_1 := b$, $x_0 := 1$, $x_1 := 0$, $y_0 := 0$, $y_1 := 1$ und induktiv für $i \geq 1$:*

$$a_{i-1} = q_{i+1}a_i + a_{i+i}$$

wobei $a_{i+1}, q_{i+1} \in \mathbb{Z}$ durch Division mit Rest von a_{i-1} durch a_i eindeutig gegeben sind, so daß gilt $0 \leq a_{i+1} < |a_i|$. Weiterhin setzen wir:

$$x_{i+1} = x_{i-1} - q_{i+1}x_i,$$
$$y_{i+1} = y_{i-1} - q_{i+1}y_i.$$

Dann gibt es ein $k \geq 1$, so daß $a_{k+1} = 0$ und dann ist $\mathrm{ggT}(a, b) = a_k = x_k a + y_k b$.

Korollar: *Für $a, b \in \mathbb{Z} \setminus \{0\}$ sind äquivalent:*

(i) *a und b sind teilerfremd.*

(ii) $\mathrm{ggT}(a, b) = \pm 1$.

(iii) *Es gibt $x, y \in \mathbb{Z}$ mit $xa + yb = 1$.*

Satz: *Es sei $n \in \mathbb{N}$. Dann gilt:*

(i) $(\mathbb{Z}/n\mathbb{Z})^* = \{[i] \mid \mathrm{ggT}(i, n) = 1\}$.

(ii) *Die Menge $\mathbb{Z}/n\mathbb{Z} \setminus (\mathbb{Z}/n\mathbb{Z})^*$ besteht aus Nullteilern.*

(iii) *$\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Satz: *Für jeden Ring R gibt es genau einen Ringhomomorphismus von $\mathbb{Z}$ nach R.*

Definition: Es sei R ein Ring und $f : \mathbb{Z} \longrightarrow R$ der nach dem vorigen Satz existierende und eindeutig definierte Ringhomomorphismus. Dann gilt $\ker(f) = n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$. Dieses n heißt *Charakteristik* von R, $\mathrm{Char}(R)$.

Bemerkung: Wir können nun für $n \in \mathbb{Z}$ und $x \in R$ die Schreibweise $n \cdot x$ einführen. Hierbei gilt: wenn $n = 0$, dann setzen wir $n \cdot x = 0$, wenn $n > 0$, dann steht $n \cdot x$ für den Ausdruck $x + \cdots + x$ (n Summanden) und wenn $n < 0$, dann steht $n \cdot x$ für $-(-n) \cdot x$. Dann ist der Ringhomomorphismus $\mathbb{Z} \longrightarrow R$ gegeben durch $n \mapsto n \cdot 1_R$. Ist $\mathrm{Char}(R) = n > 0$, dann gilt also $n \cdot 1 = 0$ und somit $n \cdot x = n \cdot (1 \cdot x) = (n \cdot 1) \cdot x = 0 \cdot x = 0$ für jedes $x \in R$.

Satz: *Für einen Körper K gilt entweder* $\mathrm{Char}(K) = 0$ *oder* $\mathrm{Char}(K)$ *ist eine Primzahl.*

Die komplexen Zahlen

Definition: Wir definieren $\mathbb{C}$ als $\mathbb{R}^2$ mit den folgenden Verknüpfungen $+$ und $\cdot$. Für alle $(x, y), (u, v) \in \mathbb{C}$ gelte:

$$\begin{aligned}(x, y) + (u, v) &:= (x + u, y + v)\\ (x, y) \cdot (u, v) &:= (xu - yv, xv + yu).\end{aligned}$$

Für $z = (x, y)$ setzen wir:

$$\begin{aligned}\mathrm{Re}(z) &:= x && \text{Realteil,}\\ \mathrm{Im}(z) &:= y && \text{Imaginärteil.}\end{aligned}$$

Satz: $(\mathbb{C}, +, \cdot)$ *ist ein Körper.*

Das neutrale Element der Multiplikation ist $1_{\mathbb{C}} = (1, 0)$, und es gilt $(0, 1) \cdot (0, 1) = -1_{\mathbb{C}}$.

Definition: Wir setzen $i := (0, 1)$, die *imaginäre Einheit*. Dann schreiben wir für $z = (x, y)$ auch einfach $z = x + iy = \mathrm{Re}(z) + i\,\mathrm{Im}(z)$.

Die Abbildung $\iota : \mathbb{R} \longrightarrow \mathbb{C}$, $x \mapsto x \cdot 1_{\mathbb{C}}$ ist ein Körperhomomorphismus und wir können somit $\mathbb{C}$ als Körpererweiterung von $\mathbb{R}$ betrachten.

Definition: Wir definieren die *komplexe Konjugation* als $\bar{} : \mathbb{C} \longrightarrow \mathbb{C}$, $z = x + iy \mapsto \bar{z} := x - iy$.

Satz: *Für $z, w \in \mathbb{C}$ gelten:*

(i) $\bar{z} + \bar{w} = \overline{z + w}$.

(ii) $\bar{z} \cdot \bar{w} = \overline{z \cdot w}$.

(iii) $\bar{\bar{z}} = z$.

(iv) $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$.

Insbesondere ist die komplexe Konjugation ein Körperautomorphismus von $\mathbb{C}$.

Definition: Die *Betragsfunktion* $|\quad| : \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}$ ist gegeben durch $z = x + iy \mapsto |z| := \sqrt{x^2 + y^2}$.

Satz: *Für $z, w \in \mathbb{C}$ gelten:*

(i) $z \cdot \bar{z} = |z|^2$.

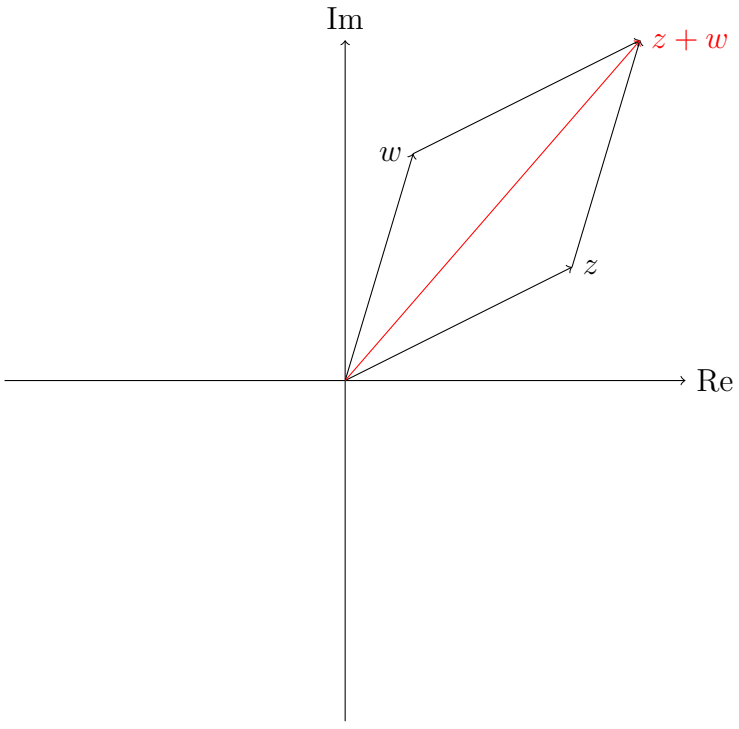
(ii) $|z| \cdot |w| = |z \cdot w|$.

(iii) $z = 0 \Leftrightarrow |z| = 0$.

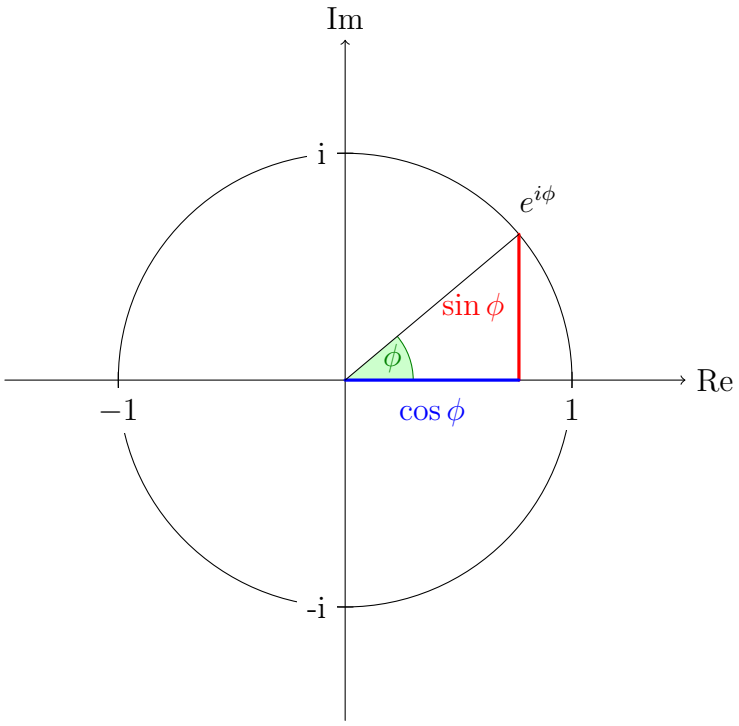
(iv) $|z + w| \leq |z| + |w|$.

Die Gaußsche Zahlenebene

Da die den komplexen Zahlen zugrundeliegende Menge der $\mathbb{R}^2$ ist, spricht man auch oft von der *Gaußschen Zahlenebene* oder der *komplexen Ebene*. Aus geometrischer Sicht kann man die Addition als Addition von Vektoren im $\mathbb{R}^2$ betrachten, was auch Gültigkeit der Dreiecksungleichung erklärt:



Insbesondere ist der Betrag $|z|$ nichts weiter als die euklidische Länge eines Vektors in der Ebene. Komplexe Zahlen z mit $|z| = 1$ liegen auf dem Einheitskreis und können in der Form $z = \cos\phi + i\sin\phi$ für ein $\phi \in \mathbb{R}$ geschrieben werden.



Definition: Für ein $\phi \in \mathbb{R}$ setzen wir $\cos\phi + i\sin\phi =: e^{i\phi}$.

Für jede reelle Zahl $r > 0$ beschreibt die Gleichung

$$|z| = \sqrt{x^2 + y^2} = r$$

einen Kreis vom Radius r um den Ursprung. Eine komplexe Zahl $z \in \mathbb{C}^*$ ist somit eindeutig darstellbar als $z = r \cdot e^{i\phi}$ mit $r = |z|$ und $\phi \in \mathbb{R}$.

Bemerkung: Die Eindeutigkeit bezieht sich hier auf die Eindeutigkeit von r und $e^{i\phi}$, aber nicht auf die Eindeutigkeit von ϕ, da gilt: $e^{i\phi} = e^{i\phi+2\pi}$ für alle $\phi \in \mathbb{R}$. Es ist allerdings etwas bequemer, beliebige $\phi \in \mathbb{R}$ zuzulassen, anstatt sich auf ein Intervall, etwa $[0, 2\pi)$, zu beschränken.

Wir können nun die Multiplikation in $\mathbb{C}$ ebenfalls geometrisch interpretieren. Für $z, w \in \mathbb{C}^*$ mit $z = re^{i\phi}$ und $w = se^{i\psi}$ gilt:

$$z \cdot w = (re^{i\phi}) \cdot (se^{i\psi}) = rs \cdot e^{i\phi} \cdot e^{i\psi}.$$

Setzt man die Definition von $e^{i\cdot}$ ein, ergibt sich:

$$e^{i\phi} \cdot e^{i\psi} = (\cos\phi\cos\psi - \sin\phi\sin\psi) + i(\sin\phi\cos\psi + \cos\phi\sin\psi).$$

Diesen Ausdruck können wir vereinfachen mit Hilfe der *Additionstheoreme* für Sinus und Kosinus:

$$\begin{aligned}\cos\phi\cos\psi - \sin\phi\sin\psi &= \cos(\phi + \psi)\\ \sin\phi\cos\psi + \cos\phi\sin\psi &= \sin(\phi + \psi).\end{aligned}$$

Es folgt somit für alle $\phi, \psi \in \mathbb{R}$:

$$e^{i\phi} \cdot e^{i\psi} = e^{i(\phi+\psi)}.$$

Betrachten wir ein $z = re^{i\phi} \in \mathbb{C}^*$ und folgende Abbildung:

$$\mathbb{C} \longrightarrow \mathbb{C}, \quad w \mapsto z \cdot w,$$

dann können wir diese Abbildung als *Drehung* der komplexen Ebene um den Winkel ϕ zusammen mit einer *Streckung* um den Faktor r auffassen.

Bemerkung: Für eine genauere Betrachtung der komplexen Exponentialfunktion und der Additionstheoreme verweisen wir auf die Analysisvorlesung. Im Rahmen dieser Vorlesung können die oben aufgeführten Rechenregeln ohne weitere Begründung verwendet werden.

Mit Hilfe der Polarkoordinatendarstellung ist nun besonders einfach zu sehen, daß jede von 0 verschiedene komplexe Zahl zwei Quadratwurzeln besitzt, d.h. für $z = re^{i\phi}$ gilt:

$$\sqrt{z} = \sqrt{re^{i\phi}} = \pm\sqrt{r} \cdot e^{i\frac{\phi}{2}}.$$

Insbesondere gilt für jedes $x \in \mathbb{R}_{\geq 0}$, daß $\sqrt{-x} = \pm ix$. Weiterhin gilt auch folgende bemerkenswerte Gleichung, die als *Eulersche Formel* bekannt ist:

$$e^{i\pi} + 1 = 0.$$

Literatur-/Lesevorschläge

G. Fischer, *Lineare Algebra*, §1.3
A. Beutelspacher, *Lineare Algebra*, §2.2
S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie*, §3
`http://de.wikipedia.org/wiki/Quaternion`