Fakultät für Mathematik
Heinrich Heine-Universität Düsseldorf

PD Dr. Markus Perling
Sommersemester 2014

Lineare Algebra 1

Sechste Woche, 14.5.2014

§4 Ringe und Körper

Definition: Als *Ring* bezeichnen wir eine Menge R zusammen mit zwei Verknüpfungen

$$\begin{aligned} + &: R \times R \longrightarrow R, \quad (x,y) \mapsto x+y && \text{Addition,} \\ \cdot &: R \times R \longrightarrow R, \quad (x,y) \mapsto x \cdot y && \text{Multiplikation,} \end{aligned}$$

so daß folgende Bedingungen erfüllt sind:

(i) $(R,+)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 0 oder 0_R bezeichnet und heißt Null, bzw. Nullelement.

(ii) Für alle $x,y,z \in R$ gilt: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Assoziativität der Multiplikation).

(iii) Es gibt ein Element $1_R \in R$, so daß $1_R \cdot x = x \cdot 1_R = x$ für alle $x \in R$. Dieses Element heißt *Eins* bzw. *Einselement*.

(iv) Für alle $x,y,z \in R$ gilt:

$$\begin{aligned} x \cdot (y+z) &= x \cdot y + x \cdot z && (Distributivgesetz) \\ (x+y) \cdot z &= x \cdot z + y \cdot z \end{aligned}$$

R ist ein *kommutativer* Ring, wenn zusätzlich noch gilt:

(v) Für alle $x,y \in R$ gilt: $x \cdot y = y \cdot x$.

Man beachte, daß wir bei der Klammerung die übliche "Punkt vor Strich"-Regel befolgen.

Bemerkung: Manchmal werden auch Ringe ohne Einselement betrachtet. Diese spielen in dieser Vorlesung jedoch keine Rolle.

Man nehme zur Kenntnis, daß folgende Rechenregeln für alle $x,y,z \in R$ gelten:

(i) $-(-x) = x$,

(ii) $x + y = z \Leftrightarrow x = z - y$,

(iii) $-(x+y) = -x - y$,

(iv) $0 \cdot x = x \cdot 0 = 0$,

(v) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$,

(vi) $(-x) \cdot (-y) = x \cdot y$,

(vii) $x \cdot (y - z) = x \cdot y - x \cdot z$.

Beispiele: 1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Ringe bzgl. der üblichen Addition und Multiplikation.

2) Wir erklären eine Verknüpfung $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}$ wie folgt:

$$[i] \cdot [j] := [i \cdot j]$$

für alle $[i], [j] \in \mathbb{Z}/n\mathbb{Z}$. Damit wird $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ zu einem Ring.

3) Für eine beliebige Menge M und einen Ring R setzen wir:

$$R^M := \{f : M \to R\},$$

d.h. R^M ist die Menge der Abbildungen von M nach R. Wir definieren Addition und Multiplikation auf R^M *punktweise*:

$$+ : R^M \times R^M \to R^M, \quad (f, g) \mapsto (f + g : M \to R)$$

wobei $(f + g)(m) := f(m) + g(m)$ für alle $m \in M$, und:

$$\cdot : R^M \times R^M \to R^M, \quad (f, g) \mapsto (f \cdot g : M \to R)$$

wobei $(f \cdot g)(m) := f(m) \cdot g(m)$ für alle $m \in M$. Bemerkung: ist R kommutativ, dann ist auch R^M kommutativ.

Definition: Es sei R ein Ring. Eine Teilmenge $S \subset R$ heißt *Unterring*, genau dann, wenn folgende Bedingungen erfüllt sind:

(i) S ist Untergruppe von $(R, +)$.

(ii) Für alle $x, y \in S$ gilt: $x \cdot y \in S$.

(iii) $1_R \in S$.

Satz: *Es sei R ein Ring und $S \subset R$ ein Unterring. Dann ist S ein Ring. Ist außerdem R kommutativ, dann ist auch S kommutativ.*

Beispiel: Es sei $D \in \mathbb{N}$, $D \neq 1$ quadratfrei, d.h. es gibt keine Primzahl p, so daß p^2 ein Teiler von D ist. Dann setzen wir

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

$\mathbb{Z}[\sqrt{D}]$ ist ein Unterring von $\mathbb{R}$.

Polynomringe

Wir haben weiter oben gesehen, daß wir zu gegebenen Ring R auf der Menge $R^{\mathbb{N}_0}$ der Abbildungen von $\mathbb{N}_0$ nach $\mathbb{R}$ eine Ringstruktur definieren können. Wir konstruieren nun eine weitere Ringstruktur auf $R^{\mathbb{N}_0}$, indem wir eine alternative Multiplikation definieren.

Wir fassen Elemente in $R^{\mathbb{N}_0}$ als *Folgen* mit Werten in R auf, welche wir schreiben als:

$$(a_i)_{i \in \mathbb{N}_0} = (a_0, a_1, a_2, \dots).$$

Die Addition behalten wir so bei, wie bereits weiter oben definiert, d.h. für $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$ gilt:

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_0}.$$

Für die Multiplikation definieren wir nun:

$$(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} := (t_i)_{i\in\mathbb{N}_0}, \quad \text{wobei} \quad \forall i \in \mathbb{N}_0 : \; t_i := \sum_{k=0}^{i} a_k b_{i-k},$$

d.h.

$$(t_i)_{i\in\mathbb{N}_0} = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots).$$

Wir führen eine etwas vereinfachende Schreibweise ein:

$$\sum_{k=0}^{i} a_k b_{i-k} =: \sum_{\mu+\nu=i} a_\mu b_\nu,$$

d.h. auf der rechten Seite wird über alle $\mu, \nu \in \mathbb{N}_0$ summiert, für die gilt, daß $\mu + \nu = i$. Der Nachweis, daß $R^{\mathbb{N}_0}$ mit diesem Produkt tatsächlich ein Ring ist, ist im wesentlichen eine Rechenübung. Wir führen dies exemplarisch für die Assoziativität der Multiplikation durch. Es seien $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0}, (a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$, dann gilt:

$$\begin{aligned}
(a_i)_{i\in\mathbb{N}_0} \cdot ((b_i)_{i\in\mathbb{N}_0} \cdot (c_i)_{i\in\mathbb{N}_0}) &= (a_i)_{i\in\mathbb{N}_0} \cdot (\sum_{\mu+\nu=i} b_\mu c_\nu)_{i\in\mathbb{N}_0} \\
&= (\sum_{\lambda+\kappa=i} a_\lambda \sum_{\mu+\nu=\kappa} b_\mu c_\nu)_{i\in\mathbb{N}_0} \\
&= (\sum_{\lambda+\mu+\nu=i} a_\lambda b_\mu c_\nu)_{i\in\mathbb{N}_0},
\end{aligned}$$

wobei hier wieder in vereinfachender Schreibweise die letzte Summe über alle $\lambda, \mu, \nu \in \mathbb{N}_0$ läuft, so daß $\lambda + \mu + \nu = i$. Analog gilt:

$$\begin{aligned}
((a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0}) \cdot (c_i)_{i\in\mathbb{N}_0} &= (\sum_{\lambda+\mu=i} a_\lambda b_\mu)_{i\in\mathbb{N}_0} \cdot (c_i)_{i\in\mathbb{N}_0} \\
&= (\sum_{\kappa+\nu=i} (\sum_{\lambda+\mu=\kappa} a_\lambda b_\mu) c_\nu)_{i\in\mathbb{N}_0} \\
&= (\sum_{\lambda+\mu+\nu=i} a_\lambda b_\mu c_\nu)_{i\in\mathbb{N}_0}.
\end{aligned}$$

Somit sind beide Produkte gleich. Ähnlich weist man das Distributivgesetz nach und die Tatsache, daß folgendes die neutralen Elemente sind:

$$\begin{aligned}
0_{R^{\mathbb{N}_0}} &= (0, 0, \dots), \\
1_{R^{\mathbb{N}_0}} &= (1, 0, 0, \dots).
\end{aligned}$$

Wir benennen nun weitere spezielle Elemente in $R^{\mathbb{N}_0}$. Für jedes $n \in \mathbb{N}_0$ setzen wir:

$$X^n := (a_i)_{i\in\mathbb{N}_0}, \quad \text{wobei} \quad a_i = \begin{cases} 1 & \text{wenn } i = n, \\ 0 & \text{sonst.} \end{cases}$$

also:

$$\begin{aligned} X^0 &= (1, 0, \dots) = 1_{R^{\mathbb{N}_0}} \\ X^1 &= (0, 1, 0, \dots) \\ X^2 &= (0, 0, 1, 0, \dots) \\ &\vdots \end{aligned}$$

Ein Element von der Form $(a_i)_{i\in\mathbb{N}_0}$ für das es ein $n \in \mathbb{N}_0$ gibt, so daß $a_i = 0$ für alle $i \in \mathbb{N}_0 \setminus \{n\}$ schreiben wir dann als:

$$(a_i)_{i\in\mathbb{N}_0} = (0, \dots, 0, a_n, 0, \dots) =: a_n X^n.$$

Außerdem schreiben wir auch einfach X anstatt X^1.

Nun betrachten wir folgende Teilmenge von $R^{\mathbb{N}_0}$:

$$R^{(\mathbb{N}_0)} := \{(a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0} \mid a_i \neq 0 \text{ für endlich viele } i \in \mathbb{N}_0\}.$$

Man überlegt sich, daß $R^{(\mathbb{N}_0)}$ ein Unterring von $R^{\mathbb{N}_0}$ ist. Es gibt zu jedem $(a_i)_{i\in\mathbb{N}_0} \in R^{(\mathbb{N}_0)}$ ein $n \in \mathbb{N}$, so daß $a_i = 0$ für alle $i > n$, und somit können wir schreiben:

$$(a_i)_{i\in\mathbb{N}_0} = \sum_{i=0}^{n} a_i X^i.$$

Definition: Der Ring $R^{(\mathbb{N}_0)}$ ist der *Polynomring mit Koeffizienten in R* und wir bezeichnen ihn mit $R[X]$. Elemente in $R[X]$ der Form $\sum_{i=0}^{n} a_i X^i$ nennen wir *Polynome mit Koeffizienten in R* oder einfach nur *Polynome*.

Polynomaddition und -multiplikation können wir nun wie folgt schreiben:

$$\begin{aligned} \sum_{i=0}^{m} a_i X^i + \sum_{j=0}^{n} b_j X^j &= \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i, \\ \sum_{i=0}^{m} a_i X^i \cdot \sum_{j=0}^{n} b_j X^j &= \sum_{i=0}^{m+n} (\sum_{k=0}^{i} a_k b_{i-k}) X^i, \end{aligned}$$

Hierbei nehmen wir für die erste Formel an, daß die Koeffizienten a_i, bzw b_i ggf. mit 0 fortgesetzt werden, d.h. wenn $m < n$, dann setzt man $a_{n+1} = \cdots = a_m = 0$ und wenn $n < m$, dann setzt man $b_{n+1} = \cdots = b_m = 0$.

Hinweis: Es ist eine gesunde Übung, sich die Summationsregeln und obige Rechnungen für die Multiplikation in $R[X]$ (oder in $R^{\mathbb{N}_0}$) gründlichst klarzumachen.

Bemerkung: Man kann Elemente in $R^{\mathbb{N}_0}$ formal auch als unendliche Summen $(a_i)_{i\in\mathbb{N}_0} = \sum_{i\in\mathbb{N}_0} a_i X^i$ schreiben und der Ring $R^{\mathbb{N}_0}$ wird als *Ring der formalen Potenzreihen* aufgefaßt. Hierfür findet man oft die Notation $R[\![X]\!]$.

Matrixringe

Zu einem Ring R und $n \in N$ können wir die Menge der $n \times n$-Matrizen definieren:

$$\mathrm{Mat}_{n\times n}(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in R \text{ für } 1 \leq i, j \leq n \right\}$$

Für ein Element $A \in \mathrm{Mat}_{n\times n}(R)$ schreiben wir auch $A = (a_{ij})_{1\le i,j\le n}$ oder einfach $A = (a_{ij})$. Wir definieren Addition und Multiplikation wie folgt für alle $A, B \in \mathrm{Mat}_{n\times n}(R)$ mit $A = (a_{ij})$ und $B = (b_{ij})$:

$$A + B = (a_{ij} + b_{ij})_{1\le i,j\le n}$$

$$A \cdot B = (c_{ij})_{1\le i,j\le n}, \quad \text{wobei} \quad \forall\, 1 \le i,j \le n:\ c_{ij} = \sum_{\mu=1}^{n} a_{i\mu} b_{\mu j}.$$

Die Multiplikationsregel ist auch bekannt als "Zeile mal Spalte". Mit Hilfe dieser Verknüpfungen wird $\mathrm{Mat}_{n\times n}(R)$ zu einem Ring. Man beachte, daß ein solcher Ring für $n > 1$ fast niemals kommutativ ist (Ausnahme: R ist der Nullring, siehe unten).

Beispiel: Die Ringaxiome schließen nicht aus, daß gilt $1 = 0$. In diesem Fall gilt $x = 1 \cdot x = 0 \cdot x = 0$ für alle $x \in R$. Gilt also $1 = 0$, dann hat der Ring R nur ein Element. Man spricht dann vom *Nullring*.

Definition: Es sei R ein Ring. Ein Element $x \in R$ heißt *Nullteiler*, wenn es ein von 0 verschiedenes Element y in R gibt, so daß $x \cdot y = 0$ oder $y \cdot x = 0$. Ringe, in denen es außer der 0 keine Nullteiler gibt, heißen *nullteilerfrei*. Ein kommutativer, nullteilerfreier Ring, der nicht der Nullring ist, heißt *Integritätsring*.

Definition: Es seien R, S Ringe und $f : R \longrightarrow S$ eine Abbildung. Dann heißt f *Ringhomomorphismus*, wenn für alle $x, y \in R$ gilt:

(i) $f(x + y) = f(x) + f(y)$,

(ii) $f(x \cdot y) = f(x) \cdot f(y)$,

(iii) $f(1_R) = 1_S$.

Wie bei Gruppenhomomorphismen, bezeichnen wir $\mathrm{Kern}(f) := f^{-1}(\{0_S\})$.

Wir beobachten, daß ein Ringhomomorphismus $f : R \longrightarrow S$ insbesondere auch ein Gruppenhomomorphismus zwischen den Gruppen $(R, +)$ und $(S, +)$ ist. Wir verwenden die Begriffe *Monomorphismus*, *Epimorphismus*, *Isomorophismus*, ... auch für einen Ringhomomorphismus, wenn er als Gruppenhomomorphismus ein Monomorphismus, Epimorphismus, Isomorphismus, ... ist.

Satz: *Es sei $f : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt:*

(i) $\mathrm{Kern}(f)$ *ist Untergruppe von* $(R, +)$.

(ii) Für alle $x \in R$ und alle $y \in \mathrm{Kern}(f)$ gilt ist auch $x \cdot y \in \mathrm{Kern}(f)$.

(iii) f ist genau dann injektiv, wenn gilt: $\mathrm{Kern}(f) = \{0_R\}$.

(iv) Ist f bijektiv, dann ist die Umkehrabbildung $f^{-1} : S \longrightarrow R$ ebenfalls ein Ringhomomorphismus.

Satz: *Es sei $f : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt:*

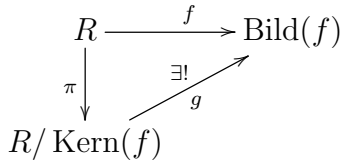
(i) $\mathrm{Bild}(f) \subset S$ *ist ein Unterring.*

(ii) $R/\operatorname{Kern}(f)$ *ist ein Ring. Ist* R *kommutativ, dann ist* $R/\operatorname{Kern}(f)$ *ebenfalls kommutativ.*

(iii) Die Abbildung $\pi : R \to R/\operatorname{Kern}(f)$, $x \mapsto [x]$ *ist ein Ringhomomorphismus.*

Satz (Homomorphiesatz für Ringe)**:** *Es sei* $f : R \longrightarrow S$ *ein Ringhomomorphismus. Dann gibt es einen eindeutig definierten Ringhomomorphismus* $g : R/\operatorname{Kern}(f) \longrightarrow \operatorname{Bild}(f)$*, so daß* $f = g \circ \pi$*.*

In Diagrammform stellt sich die Aussage des Satzes wie folgt dar:



Definition: Es sei R ein kommutativer Ring. Ein Element $x \in R$ heißt *Einheit*, wenn es ein $x' \in x$ gibt, so daß $x' \cdot x = 1_R$. Wir bezeichnen die Menge der Einheiten in R mit R^*

Satz: *Es sei* R *ein kommutativer Ring. Dann ist* $(R^*, \cdot)$ *eine abelsche Gruppe.*

Definition: Ein kommutativer Ring K heißt *Körper*, wenn gilt:

(i) $1 \neq 0$,

(ii) $K^* = K \setminus \{0\}$.

Literatur-/Lesevorschläge

S. Bosch, *Lineare Algebra*, §5
G. Fischer, *Lineare Algebra*, §1.3