Universität Konstanz Fachbereich Mathematik und Statistik

Arbeitsheft zur Linearen Algebra I

zur Überbrückung der Weihnachtsferien
im Wintersemester 2005/2006

1. Ringe

Definition 1.1. Ein *Ring* R ist eine Menge zusammen mit zwei Verknüpfungen, genannt *Addition* bzw. *Multiplikation*, geschrieben als Summe bzw. Produkt, so daß die folgenden Bedingungen erfüllt sind:

(i) R bildet bezüglich der Addition eine abelsche Gruppe.

(ii) Die Multiplikation ist assoziativ, das heißt

$$(ab)c = a(bc) \qquad \text{für alle } a, b, c \in R.$$

(iii) Die Multiplikation besitzt ein neutrales Element, das heißt es gibt ein $e \in R$ mit

$$ae = a = ea \qquad \text{für alle } a \in R.$$

(iv) Die Distributivgesetze gelten, das heißt

$$(a+b)c = ac + bc \quad \text{und} \quad c(a+b) = ca + cb \qquad \text{für alle } a, b, c \in R.$$

Sind e, e' neutrale Elemente bezüglich der Multiplikation, so gilt $e = ee' = e'$. Daher gibt es genau ein neutrales Element bezüglich der Multiplikation, welches wir mit 1 bezeichnen. Ebenso ist natürlich das neutrale Element 0 bezüglich der Addition eindeutig bestimmt. Ein Ring R heißt *Integritätsring*, wenn folgende Bedingungen erfüllt sind:

(i) R ist *nichttrivial*, das heißt es gilt $0 \neq 1$.

(ii) R ist *kommutativ*, das heißt es gilt

$$ab = ba \qquad \text{für alle } a, b \in R.$$

(iii) R ist *nullteilerfrei*, das heißt es gilt

$$(ab = 0 \implies (a = 0 \text{ oder } b = 0)) \qquad \text{für alle } a, b \in R.$$

Beispiel 1.2. (i) Jeder Körper ist ein Integritätsring.

(ii) Jede Teilmenge R eines Körpers, die die Elemente 0 und 1 des Körpers enthält und abgeschlossen ist unter der Addition und der Multiplikation des Körpers (das heißt $R + R \subseteq R$ und $R \cdot R \subseteq R$) bildet einen Integritätsring.

(iii) Nach (ii) sind also zum Beispiel $\mathbb{Z}$ und $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ Integritätsringe.

(iv) Die $n \times n$–Matrizen über einem festen Körper K bilden einen Ring.

(v) Die Endomorphismen eines festen Vektorraums bilden einen Ring, wenn man zwei Endomorphismen f und g multipliziert durch Hintereinanderausführung: $fg := f \circ g$.

Aufgabe 1.3. Sei R ein Ring. Zeigen Sie, daß für alle $a, b \in R$ gilt

$$a \cdot 0 = 0 = 0 \cdot a.$$

Aufgabe 1.4. Sei R ein trivialer Ring, das heißt es gelte $0 = 1$ in R. Zeigen Sie, daß dann $R = \{0\}$ gilt.

Aufgabe 1.5. Sei R ein Integritätsring. Zeigen Sie, daß die „Kürzungsregel“

$$ab = ac \implies b = c$$

für beliebige $a, b, c \in R$ mit $a \neq 0$ gilt.

Der Prototyp aller Integritätsringe ist der Ring $\mathbb{Z}$ der ganzen Zahlen. Was diesem Ring zum Körper fehlt, ist die Existenz multiplikativer Inverser, denn die Gleichung $bx = a$ besitzt nicht für alle $a \in \mathbb{Z}$ und $0 \neq b \in \mathbb{Z}$ eine Lösung $x \in \mathbb{Z}$. Zum Beispiel gibt es kein $x \in \mathbb{Z}$ mit $8x = 1$. Ein Mensch, der überhaupt keinen Sinn für Mathematik hat, mag sich damit begnügen, ein Messer zu kaufen und eine Torte in acht gleich große Stücke zu schneiden. Ein Mensch, der ein bißchen Sinn für Mathematik hat, wird diesen gleich großen Stücken zumindest einen Namen geben, etwa „Achtel“. Und ein Mathematiker wird die ganzen Zahlen durch Hinzufügung nicht allzu vieler Elemente zu einem größeren Zahlbereich mit schönen Eigenschaften erweitern, in dem solche Gleichungen stets eine Lösung besitzen. In der Tat kann man die ganzen Zahlen zum Körper $\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, 0 \neq b \in \mathbb{Z} \right\}$ der rationalen Zahlen erweitern.

Man kann aber sogar aus einem *beliebigen* Integritätsring R einen Körper K konstruieren, der grob gesprochen gerade aus Brüchen von Elementen von R besteht:

Satz 1.6. *Sei R ein Integritätsring. Dann gibt es einen Körper K mit $R \subseteq K$, so daß die Verknüpfungen von R sich durch Einschränkung der entsprechenden Verknüpfungen von K ergeben und alle Elemente von K von der Form $\frac{a}{b}$ $(= ab^{-1})$ mit $a, b \in R$ und $b \neq 0$ sind. Wir nennen K den* Quotientenkörper *von R.*

Dieser Satz sagt aus, daß durch die Beispiele (ii) in 1.2 bereits alle Integritätsringe gegeben sind. Wir lassen den bereits angedeuteten Beweis aus, nicht etwa weil er schwierig wäre, sondern weil er etwas abseits des Stoffes der Vorlesung liegt. Es bleibt dem Leser unbenommen, den Beweis nachzuholen, wann und wo er will, sofern er nicht sowieso in späteren Vorlesungen darauf stößt. Noch kennen wir gar keinen Integritätsring, von dem wir nicht auch ohne den letzten Satz schon wüßten, daß er in einem Körper enthalten ist. Dies wird sich aber im nächsten Abschnitt ändern.

Haben wir überhaupt gesagt, wie man im Quotientenkörper K eines Integritätsrings R rechnet? Die Antwort ist überraschend: Es gibt nur eine Möglichkeit, darin zu rechnen, denn man prüft anhand der Körperaxiome sofort nach, daß für jeden Körper K und alle $a, b \in K$ und $0 \neq c, d \in K$ gilt

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{und} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Insbesondere gilt dies für alle $a, b \in R$ und $0 \neq c, d \in R$, aber damit ist klar, wie man in K rechnet, denn alle Elemente von K sind ja von der Form $\frac{a}{b}$ für ein $a \in R$ und $0 \neq b \in R$ und die Ausdrücke $ad + bc$, bd und ac rechnet man ja in R aus.

2. Polynomringe

In der Vorlesung haben wir zu den reellen Zahlen künstlich ein neues Element i hinzugefügt, welches die Beziehung $i^2 = -1$ erfüllt. Auf diese Weise haben wir die komplexen Zahlen erhalten, welche wieder einen Körper bilden. Formal haben wir dies bewerkstelligt, indem wir für $a, b \in \mathbb{R}$ die komplexe Zahl $a + bi$ durch das Paar (a, b) modelliert haben.

Wir wollen nun zu den reellen Zahlen (oder allgemeiner zu einem Körper K) künstlich ein neues Element X hinzufügen, welches *keine* Beziehungen erfüllt. Auf diese Weise werden wir den *Polynomring* über den reellen Zahlen erhalten, der einen Integritätsring, aber keinen Körper bildet. Formal könnte man das bewerkstelligen, indem man für $a_0, \ldots, a_n \in \mathbb{R}$ das „Polynom“ $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ durch die Folge

$$(a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, 0, \ldots)$$

modelliert. Dies ist nur ein bißchen aufwendiger als bei den komplexen Zahlen. Man kann dann folgende Tatsache beweisen:

Satz 2.1. *Sei K ein Körper. Dann gibt es einen Integritätsring $K[X]$, genannt Polynomring in X über K, mit folgenden Eigenschaften:*

(i) *$K[X]$ umfaßt den Körper K und setzt dessen Verknüpfungen fort.*
(ii) *X ist ein Element von $K[X]$.*
(iii) *Die Elemente von $K[X]$ sind alle von der Form*

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

mit $a_0, \ldots, a_n \in K$.
(iv) *Für alle $a_0, \ldots, a_n \in K$ gilt*

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0 \implies a_0 = \cdots = a_n = 0.$$

Man beachte, daß X^i dabei natürlich für $\underbrace{X \cdots X}_{i \text{ Faktoren}}$ steht.

Aufgabe 2.2. Sei K ein Körper. Zeigen Sie, daß für beliebige $a_0, \ldots, a_n \in K$ und $b_0, \ldots, b_n \in K$ gilt

$$a_n X^n + \cdots + a_0 = b_n X^n + \cdots + b_0 \iff a_0 = b_0, \ldots, a_n = b_n.$$

Definition 2.3. Sei K ein Körper. Die Elemente von $K[X]$ nennt man *Polynome* (in der *Unbestimmten* X mit *Koeffizienten* aus K). Seien $a_0, \ldots, a_n \in K$. Dann heißt a_i der *i–te Koeffizient* des Polynoms $a_n X^n + \cdots + a_0$. Falls $a_n \neq 0$, so sagt man $a_n X^n + \cdots + a_0$ habe den *Grad* n und bezeichnet a_n als den *höchsten Koeffizienten* oder *Leitkoeffizienten* von $a_n X^n + \cdots + a_0$.

Aufgabe 2.4. Sei K ein Körper. Seien $f, g \in K[X]$. Es habe f den Grad m und g den Grad n. Zeigen Sie, daß dann fg den Grad $m + n$ hat.

Der Mangel eines Integritätsrings gegenüber einem Körper ist, daß man bei Division zweier Elemente zu einem größeren Rechenbereich übergehen muß, nämlich zu dem in 1.6 eingeführten Quotientenkörper. Die hier betrachteten Polynomringe verfügen allerdings (wie die ganzen Zahlen) auch über eine Art von Division, die sich innerhalb des Ringes abspielt. Dies ist eine Division *mit Rest*. In den ganzen Zahlen besagt die Tatsache, daß sich $m \in \mathbb{Z}$ durch $n \in \mathbb{Z} \setminus \{0\}$ mit Rest dividieren läßt, gerade, daß es einen „Quotienten“ $q \in \mathbb{Z}$ und einen „Rest“ $r \in \mathbb{Z}$ gibt mit $m = qn + r$ und $|r| < |n|$. In $K[X]$ lautet die entsprechende Aussage wie folgt:

Satz 2.5. *Sei K ein Körper und seien $f, g \in K[X]$, $g \neq 0$. Dann gibt es $q, r \in K[X]$ mit $f = qg + r$, so daß $r = 0$ gilt (das heißt „die Division geht auf“) oder r einen kleineren Grad hat als g.*

Beweis. Wir führen Induktion nach dem Grad von f, wobei wir (nur) für die Dauer dieses Beweises auch dem „Nullpolynom“ $0 \in K[X]$ einen Grad zuordnen wollen, nämlich den Grad -1. Als Induktionsanfang betrachten wir den Fall, daß f kleineren Grad als g hat. Dann leisten $q := 0$ und $r := f$ das Gewünschte. Im Induktionsschritt sei also nun $k := (\text{Grad von } f) - (\text{Grad von } g) \geq 0$. Bezeichne a den Leitkoeffizienten von f und b den von g. Dann ist $f - \frac{a}{b} X^k g \in K[X]$ ein Polynom von kleinerem Grad als f. Wir können also auf dieses Polynom die Induktionsvoraussetzung anwenden und erhalten $p, r \in K[X]$ mit $f - \frac{a}{b} X^k g = pg + r$, so daß r einen kleineren Grad als g hat. Setzt man nun $q := \frac{a}{b} X^k + p$, so leisten q und r das Gewünschte. □

Aufgabe 2.6. Erinnern Sie sich an den in der Schule üblicherweise gelehrten Algorithmus zur „Polynomdivision“. Machen Sie sich klar, daß der obige Beweis zeigt, daß jener Algorithmus wirklich das berechnet, was er soll.

Definition 2.7. Sei $f = a_n X^n + \cdots + a_0 \in K[X]$ ein Polynom mit Koeffizienten $a_0, \ldots, a_n \in K$. Sei $x \in K$. Da $a_0, \ldots, a_n$ durch f nach Aufgabe 2.2 eindeutig bestimmt sind, können wir

$$f(x) := a_n x^n + \cdots + a_0 \in K$$

definieren. Man spricht davon, daß x in f *eingesetzt* wird.

Aufgabe 2.8. Seien $f, g \in K[X]$ und $x \in K$. Zeigen Sie

$$(f+g)(x) = f(x) + g(x) \qquad \text{und} \qquad (fg)(x) = (f(x))(g(x)).$$

Definition 2.9. Sei $f \in K[X]$. Ein $x \in K$ heißt *Nullstelle* von f, falls $f(x) = 0$.

Aufgabe 2.10. Sei $x \in K$ eine Nullstelle von $f \in K[X]$. Zeigen Sie, daß es dann ein $q \in K[X]$ gibt mit $f = q \cdot (X - x)$.

Aufgabe 2.11. Zeigen Sie, daß ein Polynom aus $K[X]$ vom Grad n mit $n+1$ verschiedenen Nullstellen in K nur das Nullpolynom sein kann.

Jedes Polynom $f \in K[X]$ definiert eine Funktion

$$K \to K : x \mapsto f(x).$$

Funktionen $K \to K$, die sich durch ein Polynom definieren lassen, heißen *Polynomfunktionen*. Man darf sie nicht verwechseln mit Polynomen. Nimmt man für K den zweielementigen Körper, so gibt es sicher unendlich viele Polynome über K. Es gibt allerdings nur vier Polynomfunktionen $K \to K$, da es überhaupt nur vier Funktionen $K \to K$ gibt.

In der Schule wird zwischen Polynomen und Polynomfunktionen in der Regel nicht unterschieden. Da in der Schule K immer ein unendlicher Körper ist, erfährt dies in der nächsten Übungsaufgabe eine Rechtfertigung. Allerdings wird in der Schule in der Regel konsequent verschleiert, daß eine solche Rechtfertigung notwendig ist, geschweige denn eine solche Rechtfertigung geliefert.

Aufgabe 2.12. Sei K *unendlich* und $f, g \in K[X]$. Zeigen Sie: Wenn f und g dieselbe Polynomfunktion darstellen (das heißt wenn $f(x) = g(x)$ für alle $x \in K$), dann gilt $f = g$.

Wollten wir in der Vorlesung nur Elemente $x \in K$ in Polynome $f \in K[X]$ einsetzen, so wären wir auch mit dem Begriff der Polynomfunktion (den man ja leicht ohne den Begriff „Polynom“ definieren könnte) ausgekommen. Der eigentliche Grund, warum wir Polynome definieren wollen, liegt aber darin, daß wir viel „unheimlichere“ Elemente in f einsetzen wollen, nämlich Endomorphismen eines K–Vektorraums:

Definition 2.13. Sei $f = a_n X^n + \cdots + a_0 \in K[X]$ ein Polynom mit Koeffizienten $a_0, \ldots, a_n \in K$. Sei V ein K–Vektorraum und $\mathrm{Hom}(V,V)$ der Ring der Endomorphismen von V (mit der Hintereinanderausführung als Multiplikation). Sei $\varphi \in \mathrm{Hom}(V,V)$. Da $a_0, \ldots, a_n$ durch f nach Aufgabe 2.2 eindeutig bestimmt sind, können wir

$$f(\varphi) := a_n \varphi^n + a_{n-1}\varphi^{n-1} \cdots + a_0 \mathrm{id}_V = \sum_{i=0}^{n} a_i \varphi^i \in \mathrm{Hom}(V,V)$$

definieren. Man spricht davon, daß der Endomorphismus φ in das Polynom f *eingesetzt* wird.

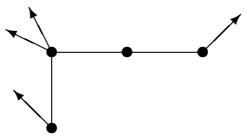
Man beachte, daß X^i dabei natürlich für die i–malige Hintereinanderausführung $\underbrace{\varphi \cdots \varphi}_{i \text{ Faktoren}} = \underbrace{\varphi \circ \cdots \circ \varphi}_{i \text{ Faktoren}}$ steht. Wenn man die Abbildung φ 0–mal hintereinander ausführt, so macht man eben gar nichts und erhält also die Identität id_V auf V: $\varphi^0 = \mathrm{id}_V$.

Aufgabe 2.14. Seien $f, g \in K[X]$. Sei V ein K–Vektorraum und $\varphi \in \mathrm{Hom}(V,V)$. Zeigen Sie

$$(f+g)(\varphi) = f(\varphi) + g(\varphi) \qquad \text{und} \qquad (fg)(\varphi) = (f(\varphi))(g(\varphi)).$$

Abgabe bis Freitag, den 13. Januar, vor Beginn der Vorlesung.

«Si $f(x,y) = x.y(x^6 - y^8)$, $A(f)$ est un arbre de Noël puisque $A(f)$ a la forme suivante:»



Françoise Michel: Courbes polaires pour les singularités de type «arbre de Noël», Comptes Rendus de l'Académie des Sciences, 308 I, p. 55-58, 1989

Wir wünschen frohe Weihnachten und einen schöneren Christbaum als den von Françoise Michel.