Martin Gubisch
Lineare Algebra I
WS 2007/2008

Polynomringe

Bemerkung

In (1.2) 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 $(a, b) \in \mathbb{R}^2$ 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 dazu für $a_0, ..., a_n \in \mathbb{R}$ das „Polynom" $a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$ durch die Folge $(a_0, a_1, ..., a_{n-1}, a_n, 0, 0, 0, ...)$ modellieren. Dies ist nur ein bisschen aufwendiger als bei den komplexen Zahlen.

Man kann dann folgende Tatsache beweisen:

Satz

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

(1) $K[X]$ umfasst den Körper K und setzt dessen Verknüpfungen fort.

(2) X ist ein Element von $K[X]$.

(3) Die Elemente von K[X] sind alle von der Form $a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$ mit $a_0, ..., a_n \in K$.

(4) Für alle $a_0, ..., a_n \in K$ gilt: $a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = 0 \Rightarrow a_0 = ... = a_n = 0$.

Bemerkung

(1) Dabei steht X^i natürlich für $\overbrace{X \cdot X \cdot ... \cdot X}^{i \text{ Faktoren}}$.

(2) Für $a_0, ..., a_n, b_0, ..., b_n \in K$ gilt: $a_n X^n + ... + a_0 = b_n X^n + ... + b_0 \Leftrightarrow a_0 = b_0, ..., a_n = b_n$.

Definition

Sei K ein Körper. Die Elemente von $K[X]$ nennt man *Polynome* in der *Unbestimmten* X mit *Koeffizienten* aus K.

Seien $a_0, ..., a_n \in K$. Dann heißt a_i der *i-te Koeffizient* des Polynoms $a_n X^n + ... + a_0$.

Falls $a_n \neq 0$, so sagt man, $a_n X^n + ... + a_0$ habe den *Grad* n und schreibt $\deg(f) = n$.

Weiter bezeichnet man a_n als den *höchsten Koeffizienten* oder *Leitkoeffizienten* von $a_n X^n + ... + a_0$.

Anmerkung

Seien K ein Körper und $f, g \in K[X]$. Hat f Grad m und g Grad n, dann hat fg Grad $m + n$.

Bemerkung

Der Mangel eines Integritätsrings gegenüber einem Körper ist, dass man bei Division zweier Elemente zu einem größeren Rechenbereich, dem Quotientenkörper, übergehen muss. 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 $n \in \mathbb{Z} \backslash \{0\}$ 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

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 eine Induktion über den Grad von f, wobei wir (nur für die Dauer dieses Beweises) dem „Nullpolynom“ $0 \in K[X]$ den Grad -1 zuordnen.

Als Induktionsanfang betrachten wir den Fall, dass f einen kleineren Grad als g hat. Dann leisten $q := 0$ und $r := f$ das Gewünschte. Im Induktionsschritt sei also nun $k := \deg(f) - \deg(g) > 0$. 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.

Definition

Sei $f = a_n X^n + ... + a_0 \in K[X]$ ein Polynom mit Koeffizienten $a_0, ..., a_n \in K$. Sei weiter $x \in K$. Da $a0, ..., a_n$ durch f eindeutig bestimmt sind, können wir $f(x) := a_n x^n + ... + a_0 \in K$ definieren. Man spricht davon, dass x in f „eingesetzt“ wird.

Ein $x \in K$ heißt *Nullstelle* von f, falls $f(x) = 0$ gilt.

Bemerkung

(1) Seien $f, g \in K[X]$ und $x \in K$. Dann gilt $(f + g)(x) = f(x) + g(x)$ und $(fg)(x) = (f(x))(g(x))$.

(2) Sei $x \in K$ eine Nullstelle von $f \in K[X]$. Dann gibt es ein $q \in K[X]$ mit $f = q(X - x)$.

(3) Ein Polynom aus $K[X]\backslash\{0\}$ vom Grad n hat höchstens n verschiedenen Nullstellen in K.

(4) Jedes Polynom $f \in K[X]$ definiert eine Funktion $\begin{smallmatrix} K \to & K \\ x \mapsto & f(x) \end{smallmatrix}$. Funktionen $K \to K$, die sich durch ein Polynom definieren lassen, heißen *Polynomfunktionen*.

Beachte

Es besteht ein Unterschied zwischen einer Polynomfunktion und dem zugehörigen Polynom. Nimmt man für K etwa den zweielementigen Körper $\mathbb{F}_2$, 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.

Bemerkung

Ist K ein unendlicher Körper und sind f, g Polynome in $K[X]$, die die selbe Polynomfunktion darstellen (das heißt $f(x) = g(x)$ für alle $x \in K$), dann gilt bereits $f = g$.

Definition

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

$$f(\varphi) := a_n \varphi^n + ... + a_0 \mathrm{id}_V \in \mathrm{Hom}(V, V)$$

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

Bemerkung

(1) φ^i steht dabei natürlich für die i-malige Hintereinanderausführung $\underbrace{\varphi ... \varphi}_{i \text{ Faktoren}} = \underbrace{\varphi \circ ... \circ \varphi}_{i \text{ Faktoren}}$ und es gilt $\varphi^0 = \mathrm{id}_V$.

(2) Seien $f, g \in K[X]$, V ein K-Vektorraum und $\varphi \in \mathrm{Hom}(V, V)$. Dann gilt $(f + g)(\varphi) = f(\varphi) + g(\varphi)$ und $(fg)(\varphi) = (f(\varphi))(g(\varphi))$.