§11 Ringe und Polynomringe

(11.1) Definition

Ein **Ring** ist eine Menge R, versehen mit zwei Verknüpfungen + und $\bullet$, d.h. $+,\bullet : R\times R \to R$, derart, dass gilt:

I $(R,+)$ ist eine abelsche Gruppe

II $\bullet$ ist assoziativ
$\exists 1 = 1_R \in R: \quad 1\cdot a = a\cdot 1 = a$ für alle $a \in R$

III **Distributivgesetze**
$a\cdot(b+c) = ab + ac$
$(a+b)\cdot c = ac + bc$

Ein Ring heißt **kommutativ**, wenn

IV $a\cdot b = b\cdot a \quad \forall a,b \in R$

(11.2) Beispiele

(1) $\mathbb{Z}$ ist ein kommutativer Ring.

(2) $\mathbb{Z}/\mathbb{Z}n$ ist ein kommutativer Ring.

(3) $\{0\}$ ist ein kommutativer Ring.

(4) Jeder Körper ist ein kommutativer Ring (s. 3.1)

(5) Sei V ein K-VR.
$(\mathrm{End}_K(V),+,\circ)$ ist ein Ring, (8.9)

(6) $\mathrm{Mat}_{n\times n}(K)$ bilden einen Ring (8.8)

(7) Seien R_1, R_2 Ringe. Dann ist $R_1\times R_2$ mit komponentenweiser Addition und Multiplikation ein Ring.
$1_{R_1\times R_2} = (1_{R_1}, 1_{R_2})$

(8) Sei $I \subseteq \mathbb{R}$ ein Intervall
$C^0(I) := \{f : I \to \mathbb{R} : f \text{ stetig}\}$ sind ein kommutativer Ring, Analysis (6.4)

(11.3) Definition

Seien R, R' Ringe.

Ein **Ringhomomorphismus** von R nach R' ist eine Abbildung $R \xrightarrow{f} R'$ derart, dass gilt:

(a) $f(a+b) = f(a) + f(b)$;

(b) $f(a\cdot b) = f(a)\cdot f(b)$

(c) $f(1_R) = 1_{R'}$.

(11.4) Beispiele

(1) id_R, R ein Ring

(2) $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, (1.18)
$a \mapsto \bar{a}$

(3) Sei V ein K-VR mit Basis $V = (v_1,...,v_n)$. Dann ist
$\mathrm{End}_K(V) \to M_{n\times n}(K)$
$f \mapsto M_V^V(f)$
ein Ringisomorphismus, (8.6) + (8.7)
siehe auch (8.10)

(4) Sei $A \in \mathrm{GL}_n(K)$. Dann ist
$\mathrm{Mat}_{n\times n}(K) \xrightarrow{K_A} \mathrm{Mat}_{n\times n}(K)$
$B \mapsto ABA^{-1}$
ein Ringautomorphismus. (Es gilt $K_A(B\cdot C) = ABCA^{-1} = ABA^{-1}ACA^{-1} = K_A(B)\cdot K_A(C)$)

(5) $\mathbb{C} \to \mathbb{C}$
$z \mapsto \bar{z}$
ist ein Körperautomorphismus

(6) $\mathbb{C} \xrightarrow{f} \mathbb{C}\times\mathbb{C}$
$z \mapsto (z,0)$
erfüllt (11.3) (a),(b), nicht aber (c): $f(1_{\mathbb{C}}) \neq 1_{\mathbb{C}\times\mathbb{C}} = (1,1)$.

(11.5) Definition

Sei R ein Ring. $a \in R$ heißt eine **Einheit**, wenn es ein $b \in R$ gibt mit
$a\cdot b = b\cdot a = 1$
Man schreibt dann $b = a^{-1}$.

Sei $R^\times$ die Menge der Einheiten.
$1 \in R^\times$, $(R^\times,\bullet)$ ist eine Gruppe; $(ab)^{-1} = b^{-1}\cdot a^{-1}$.

(11.6) Beispiele

(1) $\mathbb{Z}^\times = \{1,-1\}$

(2) Ist K ein Körper, so ist $K^\times = K\setminus\{0\}$

(3) $(\mathrm{Mat}_{n\times n}(K))^\times = \mathrm{GL}_n(K)$

(4) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : \mathrm{ggT}(a,n) = 1\}$

Sei R nun ein kommutativer Ring.

(11.7) Definition

Der **Polynomring** $R[X]$ über R ist die Menge der Ausdrücke

$f = \sum_{k=0}^{n} a_k X^k$ mit $a_k \in R$, $n \in \mathbb{N}$.

Man identifiziert f mit $\sum_{k=0}^{\infty} a_k X^k$, wobei $a_k = 0$, falls $k > n$.

Definiere die **Summe**:

$\sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{m} b_k X^k = \sum_{k=0}^{l} (a_k + b_k) X^k$, wobei $l = \max(n, m)$;

Das **Produkt**:

$\sum_{k=0}^{n} a_k X^k \cdot \sum_{k=0}^{m} b_k X^k = \sum_{l=0}^{n+m} \left(\sum_{r=0}^{l} a_r b_{l-r} \right) X^l$.

(11.8) Satz

$(R[X], +, \bullet)$ ist ein kommutativer Ring, $1_{R[X]} = 1 \cdot X^0$.

Die Abbildung $\begin{array}{l} R \to R[X] \\ a \mapsto a \cdot X^0 \end{array}$ ist ein **injektiver** Ringhomomorphismus. Wir fassen daher R als Unterring von $R[X]$ auf.

Beweis:

Verifiziere (11.1) I – IV. q.e.d.

Sei $f = \sum_{k=0}^{n} a_k X^k \in R[X]$ und sei $a_n \neq 0$. Dann heißt n der **Grad** von f. Offenbar gilt

$\operatorname{grad}(f + g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$

$\operatorname{grad}(f \cdot g) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$

$0 \neq a_n$ heißt der **Leitkoeffizient** von f.

Sei nun S ein kommutativer Ring.

(11.9) Satz

Sei $R \xrightarrow{\varphi} S$ ein Homomorphismus, und sei $s \in S$.

Dann existiert genau ein Homomorphismus $\Phi : R[X] \to S$ mit $\Phi_{|R} = \varphi$ und $\Phi(X) = s$.

Beweis:
Eindeutigkeit. Erfüllt Φ diese Bedingungen, so gilt

$$\Phi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} \varphi(a_k) \cdot s^k$$

Existenz. Definiere Φ durch obige Gleichung. Dann ist Φ ein Homomorphismus. q.e.d.

(11.10) Korollar

Sei $x \in R$. Dann ist

$$R[X] \xrightarrow{\varepsilon_x} R$$

$$f = \sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} a_k x^k =: f(x)$$

ein Homomorphismus.

Beweis:
(11.9) für $\varphi = id_R, s = x, R = S$. q.e.d.

ε_x heißt der **Einsetzungshomomorphismus** zu x.
Sei $f \in R[X]$. Die Abbildung

$$R \xrightarrow{\tilde{f}} R$$

$$x \mapsto f(x)$$

heißt die zu *f* gehörende **Polynomabbildung**.

(11.11) Beispiele

(1) $f = X^2 + X \in \mathbb{Z}/2\mathbb{Z}[X]$
Dann gilt $\tilde{f}(1) = \tilde{f}(0) = 0$
Also $\widetilde{x^2 + x} = \tilde{0}$

(2) Sei $A(R) := \{R \xrightarrow{\varphi} R\}$ die Menge aller Abbildungen.
Diese ist mit $(\varphi \dot{+} \psi)(x) = \varphi(x) \dot{+} \psi(x)$ ein Ring, und die Abbildung
$\Phi : R[X] \to A(R)$
$f \mapsto \tilde{f}$
ist ein Ringhomomorphismus, d.h. $\widetilde{(f \dot{+} g)} = \tilde{f} \dot{+} \tilde{g}$ $\tilde{1} = 1_{A(R)}$
Dieser ist i.A. nicht injektiv

(3) Ein $x_0 \in R$ heißt **Nullstelle** von $f \in R[X]$, wenn $f(x_0) = 0$

(11.12) Satz (Division mit Rest)

Seien $f = \sum_{k=0}^{n} a_k X^k$ und $g = \sum_{k=0}^{m} b_k X^k$ in $R[X]$, b_m sei eine Einheit in R. Dann existieren eindeutige Polynome, $q, r \in R[X]$ mit
$f = q \cdot g + r$ und $\operatorname{grad} r < \operatorname{grad} g$.

Beweis:

Existenz. (Induktion über $n - m$)
Ist $m > n$, so setze $q = 0$, $r = f$. Sei $m \le n$.
Sei

$$f_1 = f - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot g$$
$$\operatorname{grad} f_1 < \operatorname{grad} f$$

Sei $f_1 = q_1 \cdot g + r$
so gilt $f = (a_n b_m^{-1} X^{n-m} + q_1) g + r_1$

Eindeutigkeit. Sei $f = q_1 g + r_1 = q_2 g + r_2$
$\Rightarrow (q_1 - q_2) g = r_2 - r_1$
$\Rightarrow \operatorname{grad}(r_2 - r_1) \cdot g < \operatorname{grad}(g)$
Da $b_m \in R^\times$, so gilt für $0 \neq c \in R$:
$c \cdot b_m \cdot b_m^{-1} = c \neq 0$
also $c \cdot b_m \neq 0$. Daher gilt:
$\operatorname{grad}(q_1 - q_2) \cdot g = \operatorname{grad}(q_1 - q_2) + \operatorname{grad} g \quad \ge \operatorname{grad} g$, falls $q_1 - q_2 = 0$
$\Rightarrow q_1 - q_2 = 0 \qquad \Rightarrow r_1 - r_2 = 0$ q.e.d.

(11.13) Beispiele

(1) $f = 2x^3 + x - 4 \qquad g = x^2 + 3x - 1 \in \mathbb{Z}[X]$

$$\begin{array}{l} 2x^3 + x - 4 \;:\; x^2 + 3x - 1 = 2x - 6 \\ \underline{2x^3 + 6x^2 - 2x} \\ \quad -6x^2 + 3x - 4 \\ \quad \underline{-6x^2 - 18x + 6} \\ \qquad\quad 21x - 10 \end{array}$$

$\Rightarrow f = (2x - 6) \cdot g + (21x - 10)$

(2) Sei $g = X - a \in R[X]$, $f \in R[X]$
$\Rightarrow \exists b \in R: \quad f = q(X - a) + b$
$\Rightarrow f(a) = q(a) \cdot 0 + b = b$
$\Rightarrow f = q \cdot (X - a) + f(a)$.

(3) f hat in a eine Nullstelle
$\Leftrightarrow f$ ist teilbar durch $X - a$.

(11.14) Satz

Sei K ein Körper und $0 \neq f \in K[X]$ ein Polynom vom Grad n.
Dann hat f höchstens n Nullstellen in K.

Beweis:
Induktion über n
$n = 0$: $f = b \neq 0$ hat keine Nullstelle.
Sei grad $f = n+1$. Hat f die Nullstelle a_1, so gilt $f = (X - a_1) \cdot g$ und grad $g = n$.
$\Rightarrow g$ hat höchstens n Nullstellen
$a_2, ..., a_m$ $m \leq n+1$.
Sei b eine Nullstelle von f.
$\Rightarrow 0 = f(b) = (b - a_1) \cdot g(b_1)$
$\Rightarrow b \in \{a_1, ..., a_m\}$
$\Rightarrow$ Behauptung q.e.d.

(11.15) Definition

Sei $f, g \in K[X]$.
h heißt ggT(f, g), wenn gilt $h \mid f$, $h \mid g$ und wenn gilt:
ist p ein gemeinsamer Teiler von f und g, so gilt $p \mid h$.

h, h' sind größte gemeinsame Teiler von f und $g \Leftrightarrow h' = c \cdot h, \quad c \in K^{\times}$.

Beweis:
Sind h, h' ggT von f, g
$\Rightarrow h \mid h'$ und $h' \mid h$
$\Rightarrow$ grad $h' =$ grad h und $h' = c \cdot h$
Umgekehrt haben h und h' dieselben Teiler und beide sind gemeinsame Teiler von f und g.
q.e.d.

(11.16) Euklidischer Algorithmus

$g_0 = f$, $g_1 = g$

$g_0, ..., g_n$ seien definiert und $g_n \nmid g_{n-1}$.
sei dann g_{n+1} definiert durch $g_{n-1} = q \cdot g_n + g_{n+1}$
wobei grad $g_{n+1} <$ grad g_n.

Falls $g_n \mid g_{n-1}$ teilt, so sei g_{n+1} nicht definiert.
Das letzte Polynom in dieser Kette ist ggT(f,g).

(11.17) Lemma von Bezout

Sei h ein ggT(f,g). Dann existieren $A,B \in K[X]$ mit

$$h = A \cdot f + B \cdot g$$

Beweis: wie (1.9) q.e.d.

(11.18) Definition

Ein Polynom $p \in K[X]$ heißt **prim**, wenn grad $p > 0$ und wenn p keine Teiler hat außer $c \cdot p$, $c \in K^\times$ und $c \in K^\times$.

Ist p prim und $g \in K[X]$ mit $p \nmid g \Rightarrow$ ggT$(p,g) = 1$.

(11.19) Lemma von Euklid

Sei p prim. Falls $p \nmid f$ und $p \nmid g \Rightarrow p \nmid f \cdot g$

Beweis: mit (11.17) wie der Beweis von (1.10) q.e.d.

(11.20) Korollar

Jedes Polynom $f \in K[X]$ ist (im wesentlichen) eindeutig ein Produkt von Primpolynomen.
i.w. heißt: ist $f = p_1 \ldots p_r = q_1 \ldots q_s$ so gilt $r = s$ und bei geeigneter Nummerierung ist $q_i = c_i \cdot p_i$, $c_i \in K^\times$.

Zusatz:
Jedes normierte Polynom ist eindeutig ein Produkt normierter Primpolynome.
(normiert: Leitkoeffizient = 1)

(11.21) Beispiele

(1) $X - a \qquad a \in K$
sind prim

(2) $f = X^2 + aX + b$ ist prim $\Leftrightarrow$ f hat keine Nullstelle
Ist $f(c) = 0 \Rightarrow X - c \mid f$

Ist $f = p \cdot q \Rightarrow \operatorname{grad} p = 1$
$\Rightarrow p = X - a \quad \Rightarrow f(a) = 0$.

(3) **Fundamentalsatz der Algebra**.
Jedes Polynom vom grad > 0 in $\mathbb{C}[X]$ hat eine Nullstelle. (ohne Beweis)
$\Rightarrow X - a, \quad a \in \mathbb{C}$ sind sämtliche normierte Primpolynome in $\mathbb{C}[X]$.

(4) Die normierten Primpolynome in $\mathbb{R}[X]$ sind genau $X - a, \quad a \in \mathbb{R}$ und $X^2 - aX + b$ ohne Nullstelle,
d.h. mit $a^2 - 4b < 0$

Beweis:
Sei $p \in \mathbb{R}[X]$ prim (normiert)
$\Rightarrow p$ als Polynom in $\mathbb{C}[X]$ hat eine Nullstelle z.

(a) $z \in \mathbb{R} \Rightarrow X - z \in \mathbb{R}[X]$ teilt p
$\Rightarrow p = X - z$

(b) $z \notin \mathbb{R}$: sei $p = \sum_{i=0}^{n} a_i X^i, \quad a_i \in \mathbb{R}$

$$\Rightarrow p(z) = \sum_{i=0}^{n} a_i z^i = 0$$

$$\Rightarrow p(\bar{z}) = \sum_{i=0}^{n} a_i \bar{z}^i = \overline{\sum_{i=0}^{n} a_i z^i} = 0$$

$\Rightarrow \bar{z}$ ist Nullstelle, $z \neq \bar{z}$.
In $\mathbb{C}[X]$ gilt $X - z \mid p$
$X - \bar{z} \mid p$
$X - z$ und $X - \bar{z}$ unterscheiden sich nicht um $c \in \mathbb{C}^\times$.
$\underset{(11.20)}{\Rightarrow} (X - \bar{z})(X - z) \mid p$
$g := (X - z)(X - \bar{z}) = X^2 - 2\operatorname{Re} z \cdot X + |z|^2 \quad \in \mathbb{R}[X]$
$\Rightarrow p = g \cdot t$ in $\mathbb{C}[X]$

noch z.z.: $t \in \mathbb{R}[X]$.
Schreibe in $\mathbb{R}[X]$
$p = q \cdot g + r, \quad \operatorname{grad} r < \operatorname{grad} g$
Dies ist auch eine Division mit Rest in $\mathbb{C}[X] \underset{\text{Eindeutigkeit}}{\Rightarrow} r = 0, \quad q = t$
$\Rightarrow g \mid p \underset{p \text{ prim}}{\Rightarrow} p = g$. q.e.d.

(5) Speziell $X^2 + 1$ prim in $\mathbb{R}[X]$
$X^2 + 1 = (X - i)(X + i)$ in $\mathbb{C}[X]$

(6) In $\mathbb{Q}[X]$ gibt es Primpolynome beliebigen Grades.
z.B. $X^n - 2$ ist prim in $\mathbb{Q}[X]$.