D-MATH Algebra I HS 2023
Prof. Dr. Lorenz Halbeisen

# Musterlösung Serie 12

POLYNOMRINGE, EUKLIDISCHE RINGE

---

**63**. Zeige: Ist $R$ ein Integritätsring, so ist $R[X]^* = R^*$.

*Lösung*: Wir zeigen zwei Inklusionen. Wir fangen mit $R^* \subseteq R[X]^*$ an. Sei $a_0 \in R^*$. Dann existiert $b_0 \in R^*$ mit $a_0 b_0 = 1$. Weil $a_0, b_0 \in R[X]$, ist $R^* \subseteq R[X]$.

Nun zeigen wir $R[X]^* \subseteq R^*$. Sei $p \in R[X]^*$. Dann existiert ein Element $q \in R[X]^*$ mit $p \cdot q = 1$. Schreibe $p(X) = \sum_i^n a_i X^i$ und $q(X) = \sum_j^m b_j X^j$, mit $a_i, b_j \in R$. Weil $R$ ein Integritätsring ist, ist das Produkt der Leitkoeffizienten $a_n \cdot b_m \neq 0$. Dann gilt $\mathrm{grad}(p) + \mathrm{grad}(q) \geqslant 0$. Andererseits ist $\mathrm{grad}(p \cdot q) = \mathrm{grad}(1) = 0$. Somit folgt $\mathrm{grad}(p) = \mathrm{grad}(q) = 0$, also $n = m = 0$. Dann ist $p = a_0$, $q = b_0$ und $p \cdot q = a_0 \cdot b_0 = 1$, also $p = a_0 \in R^*$.

**64**. Zeige: Ist $K$ ein Körper und $p \in K[X]$ ein Polynom vom Grad $n > 0$. Dann hat $p$ höchstens $n$ verschiedene Nullstellen in $K$.

*Lösung*: Für $k \in \mathbb{N}$, seien $a_1, \ldots, a_k$ die verschiedenen Nullstellen von $p$ in $K$. Aus $p(a_1) = 0$, folgt $(X - a_1) \mid p$, also existiert ein $s_1 \in K[X]$ mit $p = (X - a_1)s_1$.

Weil $p(a_2) = 0$ und $a_1 \neq a_2$, gilt

$$0 = p(a_2) = (a_2 - a_1) \cdot s_1(a_2).$$

Da $K$ ein Integritätsring ist, folgt $s_1(a_2) = 0$, also existiert ein Polynom $s_2 \in K[X]$ mit $s_1 = (X - a_1)s_2$. Also können wir schreiben $p = (X - a_1)(X - a_2)s_2$, mit $\mathrm{grad}(s_2) < \mathrm{grad}(s_1) < n$. Wir wiederholen dieses Argument induktiv, so dass wir erhalten:

$$p(X) = (X - a_1)(X - a_2) \cdots (X - a_k) \cdot s_k(X),$$

mit $s_k \in K[X]$. Schreibe $q = (X - a_1)(X - a_2) \cdots (X - a_k)$. Dann gilt $\mathrm{grad}(q) = k \leqslant n = \mathrm{grad}(p)$.

**65**. Zeige: $X^3 - X$ hat 6 Nullstellen in $\mathbb{Z}/6\mathbb{Z}$.

*Lösung*: Die Zahlen $0^3 - 0,\ 1^3 - 1,\ 2^3 - 2,\ 3^3 - 3,\ (-2)^2 - (-2),\ (-1)^3 - (-1)$ sind alle durch 6 teilbar, somit sind alle Elemente aus $\mathbb{Z}/6\mathbb{Z}$ Nullstellen des besagten Polynoms.

Ein Integritätsring $R$ heiss **euklidisch**, wenn eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}$ existiert mit folgender Eigenschaft:

*Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$, sodass $a = b \cdot q + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$.*

**66**. Zeige:

(a) Jeder euklidische Ring ist Hauptidealring.

(b) $\mathbb{Z}[i]$ und $\mathbb{Z}[i\sqrt{2}]$ sind euklidisch.

*Lösung*: (a) Sei $R$ ein euklidischer Ring und sei $\mathfrak{a} \subseteq R$ ein Ideal, das nicht das Nullideal ist. Sei $a \in \mathfrak{a}$ ein Element mit $\delta(a) = \min\{\delta(b) : b \in \mathfrak{a}\}$. Dieses existiert, da $\delta[\mathfrak{a}\backslash\{0\}] \subseteq \mathbb{N}$ ist und jede nichtleere Teilmenge von $\mathbb{N}$ ein Minimum besitzt. Sei $b \in \mathfrak{a}$. Dann existieren $q, r \in R$ mit $b = qa + r$ und $\delta(r) < \delta(a)$ oder $r = 0$. Mit $a, b \in \mathfrak{a}$ folgt $r \in \mathfrak{a}$. Aus der Minimalitätseigenschaft von $\delta(a)$ folgt $r = 0$ und somit ist $b \in (a)$. Da $b$ beliebig gewählt war, haben wir $\mathfrak{a} = (a)$ bewiesen.

(b) Sei $d \in \{i, i\sqrt{2}\}$. Sei $R = \mathbb{Z}[d]$. Sei

$$\delta\colon R\backslash\{0\} \to \mathbb{N},\ \delta(a + ib) = a^2 - d^2b^2.$$

Wir überprüfen, dass $\delta$ eine euklidische Normfunktion ist. Seien dafür $x, y \in R$ mit $y \neq 0$. Es existieren $a, b \in \mathbb{R}$, so dass $\frac{x}{y} = a + bdi$ gilt (in der Tat liegen $a$ und $b$ in $\mathbb{Q}$). Wähle $m, n \in \mathbb{Z}$ mit

$$|a - m| \leqslant \frac{1}{2} \quad \text{und} \quad |b - n| \leqslant \frac{1}{2}$$

und setze $q := m + ndi$ und $r := x - yq$. Nach Konstruktion haben wir

$$\left|\frac{x}{y} - q\right|^2 = (a - m)^2 - d^2(b - n)^2 \leqslant \left(\frac{1}{2}\right)^2 - d^2 \cdot \left(\frac{1}{2}\right)^2 < 1.$$

Somit ist $x = yq + r$ mit

$$\delta(r) = |x - yq|^2 = \delta(y) \cdot \left|\frac{x}{y} - q\right|^2 < \delta(y).$$

Also ist $\delta$ eine euklidische Normfunktion auf $R$ und $R$ ist ein euklidischer Ring.

**67**. (a) Verallgemeinere den euklidischen Algorithmus zur Berechnung des $\mathrm{ggT}$ zweier Zahlen aus $\mathbb{N}$ auf euklidische Ringe.

(b) Berechne einen $\mathrm{ggT}$ von $X^3 + X^2 + X - 3$ und $X^4 - X^3 + 3X^2 + X - 4$ in $\mathbb{Q}[X]$.

(c) Stelle den $\mathrm{ggT}$ aus (b) als Linearkombination (mit Koeffizienten aus $\mathbb{Q}[X]$) der beiden Polynome $X^3 + X^2 + X - 3$ und $X^4 - X^3 + 3X^2 + X - 4$ dar.

*Lösung*: Sei $R$ ein euklidischer Ring und $\delta\colon R\backslash\{0\} \to \mathbb{N}$ die entsprechende Funktion. Seien $a, b \in R\backslash\{0\}$. Nimm an, dass o.B.d.A. $\delta(a) \geqslant \delta(b)$ gilt. Seien $q, r$ mit $a = bq + r$ und $\delta(q) < \delta(r)$ oder $r = 0$. Ein Teiler von $a$ und $b$ muss dann auch $r$ teilen. Ausserdem teilt ein gemeinsamer Teiler von $b$ und $r$ sicher auch $a$. Daher gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$. Falls $r = 0$ ist, so ist $\mathrm{ggT}(a, b) = b$. Anderenfalls können wir dieses Argument mit $(b, r)$ anstelle von $(a, b)$ wiederholen. Wegen $\delta(a) + \delta(b) > \delta(b) + \delta(r)$ terminiert der Prozess irgendwann.

(b) Mit Polynomdivision finden wir

$$X^4 - X^3 + 3X^2 + X - 4 = (X^3 + X^2 + X - 3) \cdot (X - 2) + (4X^2 + 6X - 10)$$
$$X^3 + X^2 + X - 3 = (4X^2 + 6X - 10) \cdot (\frac{1}{4}X - \frac{1}{8}) + (\frac{17}{4}X - \frac{17}{4})$$
$$4X^2 + 6X - 10 = (\frac{17}{4}X - \frac{17}{4}) \cdot (\frac{16}{17}X + \frac{40}{17}) + 0.$$

Wenn wir mit der Einheit $\frac{4}{17}$ multiplizieren, erhalten wir

$$\mathrm{ggT}(X^4 - X^3 + 3X^2 + X - 4, X^3 + X^2 + X - 3) = X - 1.$$

(c) Wie in Aufgabe 52.(b) berechnen wir mit dem Schema

| | | $X-2$ | $\frac{1}{4}X - \frac{1}{8}$ | $\frac{16}{17}X + \frac{40}{17}$ |
|---|---|---|---|---|
| 0 | 1 | $X-2$ | $\frac{1}{4}X^2 - \frac{5}{8}X + \frac{5}{4}$ | |
| 1 | 0 | 1 | $\frac{1}{4}X - \frac{1}{8}$ | |

die Darstellung

$$17X - 17 = (-X + \frac{1}{2}) \cdot (X^4 - X^3 + 3X^2 + X - 4) + (X^2 - \frac{5}{2}X + 5) \cdot (X^3 + X^2 + X - 3).$$