KAPITEL 6

Ringe, Körper und Vektorräume

Nachrichten codiert man gerne als Listen von Bits. Deswegen wird es sich als günstig herausstellen, dass man nicht nur mit Vektoren, deren Einträge reelle Zahlen sind, rechnen kann, sondern auch mit Vektoren, deren Einträge nur 0 oder 1 sein können. Unser Wissen über das Lösen linearer Gleichungssysteme lässt sich auf solche 0/1-Vektoren verallgemeinern; das ist in der Codierungstheorie hilfreich.

1. Ringe

Unser Ziel ist, anstelle der reellen Zahlen auch andere Objekte verwenden zu können, solange man diese Objekte sinnvoll addieren und multiplizieren kann.

DEFINITION 6.1. Das 6-Tupel $\langle R, +, -, 0, \cdot, 1\rangle$ ist ein *Ring mit Eins*, falls gilt:

(1) R ist eine nichtleere Menge,
(2) $+$ und $\cdot$ sind Funktionen von R^2 nach R,
(3) $-$ ist eine Funktion von R nach R,
(4) $0, 1$ sind Elemente von R,
(5) für alle $x, y, z \in R$ gilt:
   (a) $(x + y) + z = x + (y + z)$,
   (b) $0 + x = x$,
   (c) $(-x) + x = 0$,
   (d) $x + y = y + x$,
   (e) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
   (f) $1 \cdot x = x \cdot 1 = x$,
   (g) $x \cdot (y + z) = x \cdot y + x \cdot z$,
   (h) $(x + y) \cdot z = x \cdot z + y \cdot z$.

BEISPIELE 6.2.

(1) Die rellen Zahlen bilden einen Ring; genauer: $\langle \mathbb{R}, +, -, 0, \cdot, 1\rangle$ ist ein Ring.
(2) Die 2×2-Matrizen bilden ein Ring; genauer: $\langle \mathbb{R}^{2\times 2}, +, -, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \cdot, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\rangle$ ist ein Ring.

(3) Die Polynome über $\mathbb{R}$ bilden einen Ring; genauer: $\langle \mathbb{R}[x], +, -, 0, \cdot, 1\rangle$ ist ein Ring.

SATZ 6.1. *Sei $\langle R, +, -, 0, \cdot, 1\rangle$ ein Ring. Dann gelten für alle $x, y \in R$ folgende Eigenschaften:*

(1) $0 \cdot x = 0$
(2) $x \cdot 0 = 0$.
(3) $x \cdot (-y) = -(x \cdot y)$
(4) $(-x) \cdot y = -(x \cdot y)$

DEFINITION 6.3. Sei $\mathbf{R} = \langle R, +, -, 0, \cdot, 1\rangle$ ein Ring. Ein Element $a \in R$ heißt *invertierbar*, wenn es ein $b \in R$ gibt, sodass $a \cdot b = b \cdot a = 1$.

2. Der Ring $\mathbb{Z}_n$

In $\mathbb{Z}$ definieren wir für $n \in \mathbb{N}$ die Relation $\equiv_n$ durch

$$a \equiv_n b :\Leftrightarrow n \mid b - a.$$

Die Relation $\equiv_n$ ist eine Äquivalenzrelation, d.h. reflexiv, symmetrisch und transitiv. Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist

$$\{a + z \cdot n \mid z \in \mathbb{Z}\} =: [a]_n .$$

Die Menge aller Äquivalenzklassen (die Faktormenge) bezeichnen wir mit

$$\mathbb{Z}_n := \left\{[a]_n \mid a \in \mathbb{Z}\right\}.$$

$\mathbb{Z}_n$ hat n Elemente, und zwar $[0]_n, [1]_n, \ldots, [n-1]_n$. Auf $\mathbb{Z}_n$ definieren wir $\oplus$ und $\odot$ durch:

$$\begin{aligned} [a]_n \oplus [b]_n &:= [a + b]_n \\ [a]_n \odot [b]_n &:= [a \cdot b]_n . \end{aligned}$$

Wir müssen zeigen, dass $\oplus$ und $\odot$ wohldefiniert sind; wir geben hier nur den Beweis für die Wohldefiniertheit von $\odot$. Wir wählen also $a, a', b, b' \in \mathbb{Z}$ sodass $[a]_n = [a']_n$ und $[b]_n = [b']_n$. Zu zeigen ist, dass dann

$$[a \cdot b]_n = \left[a' \cdot b'\right]_n$$

gilt. Es ist also zu zeigen, dass

$$n \mid a \cdot b - a' \cdot b'.$$

Klarerweise ist

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

Daraus folgt n teilt $ab - a'b'$, da laut Vorraussetzung $n \mid (b - b')$ und $n \mid (a - a')$ gilt. Daher ist $[a \cdot b]_n = [a' \cdot b']_n$, und somit ist das Ergebnis von $[a]_n \odot [b]_n$ unabhängig von der Auswahl der Repräsentanten.

Wir geben nun ein Beispiel für eine *nicht* wohldefinierte Operation. Auf der Menge $\mathbb{Q}$ definieren wir die Relation

$$a \sim b :\Leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor .$$

$\lfloor a \rfloor$ ist hier die größte ganze Zahl kleiner gleich a. Wir definieren:

$$\lfloor a \rfloor \odot \lfloor b \rfloor := \lfloor a \cdot b \rfloor .$$

$$\begin{array}{lll} a = 0.1 & b = 100 & \lfloor 0.1 \cdot 100 \rfloor = 10 \\ a' = 0 & b' = 100 & \lfloor 0 \cdot 100 \rfloor = 0 \end{array}$$

Da $0 \sim 10$ nicht gilt, ist die Operation $\odot$ also nicht wohldefiniert.

Die Operation $\odot$ zuerst zu definieren, und dann zu zeigen, dass die Definition funktioniert, ist nicht sauber (aber üblich). Richtig ist, die Operation $\odot$ zuerst als Relation zu definieren, also

$$\odot := \{\big(([a]_n, [b]_n), [a \cdot b]_n\big) \mid a, b \in \mathbb{Z}\},$$

und dann zu zeigen, dass die Relation $\odot$ eine Funktion von $\mathbb{Z}_n \times \mathbb{Z}_n$ nach $\mathbb{Z}_n$ ist.

Die algebraische Struktur $\langle \mathbb{Z}_n, \oplus, \ominus, [0]_n, \odot, [1]_n \rangle$ ist ein Ring.

Eine andere Möglichkeit, einen endlichen Ring mit n Elementen zu definieren, ist folgende: Wir wählen die Menge $R = \{0, 1, 2, \ldots, n-1\}$. Wir definieren für alle $a \in \mathbb{Z}$ die Zahl $a \; mod \; n$ als jenes $a' \in \{0, 1, \ldots, n-1\}$ mit $a' \equiv_n a$. Die Zahl a' ist dann genau der Rest der Division von a durch n. Dann definieren wir für $x, y \in \{0, 1, \ldots, n-1\}$

$$\begin{array}{rcl} x +_n y & := & (x + y) \; mod \; n, \\ -_n x & := & (-x) \; mod \; n, \\ x \circ_n y & := & (x\, y) \; mod \; n. \end{array}$$

Die algebraische Struktur $\langle R, +_n, -_n, 0, \circ_n, 1 \rangle$ ist dann ein Ring. "Im wesentlichen", das heißt, bis auf Umbenennung der Elemente, ist dieser Ring der gleiche Ring wie $\langle \mathbb{Z}_n, \oplus, \ominus, [0]_n, \circ_n, [1]_n \rangle$.

Der folgende Satz gibt an, welche Elemente in $\mathbb{Z}_n$ invertierbar sind.

SATZ 6.2 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn* $\mathrm{ggT}(a, n) = 1$.

SATZ 6.3. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch $a \cdot b$ invertierbar.*

Beweis: Seien $u, v \in \mathbb{Z}_n$ so, dass $a \cdot u = [1]_n$ und $b \cdot v = [1]_n$. Dann gilt: $a \cdot b \cdot v \cdot u = [1]_n$. ■

DEFINITION 6.4 (Euler'sche φ–Funktion). Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $\varphi(n)$ definiert durch

$$\begin{array}{rcl} \varphi(n) & := & \Big|\big\{a \in \mathbb{Z}_n \mid a \text{ invertierbar}\big\}\Big| = \\ & = & \Big|\big\{x \in \{1, 2, \ldots, n-1\} \mid \mathrm{ggT}(x, n) = 1\big\}\Big|. \end{array}$$

Wir berechnen $\varphi(12) = |\{1, 5, 7, 11\}| = 4$ und $\varphi(8) = |\{1, 3, 5, 7\}| = 4$.

SATZ 6.4 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$, $\mathrm{ggT}(a, n) = 1$. Dann gilt:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Wir überprüfen diesen Satz durch zwei Beispiele:

- Gilt $7^{\varphi(12)} \equiv 1 \pmod{12}$? Ja, denn es ist $7^4 \equiv 1 \pmod{12}$,
- Gilt $3^{\varphi(5)} \equiv 1 \pmod{5}$? Ja, denn es gilt $3^4 \equiv 1 \pmod{5}$.

Beweis von Satz 6.4: Wir wählen $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ beliebig aber fest, und nehmen an, dass $\mathrm{ggT}(a, n) = 1$. Sei

$$I := \left\{ x \in \mathbb{Z}_n \mid x \text{ ist invertierbar} \right\}.$$

Wir wissen bereits, dass $|I| = \varphi(n)$. Wir definieren

$$\begin{array}{rccc} f & : & I & \longrightarrow & \mathbb{Z}_n \\ & & x & \longmapsto & x \odot [a]_n \end{array}$$

und zeigen, dass f injektiv ist. Dazu fixieren wir $x, y \in I$ mit $f(x) = f(y)$. Das heißt: $x \cdot [a]_n = y \cdot [a]_n$. Da $\mathrm{ggT}(a, n) = 1$, gibt es $b \in \mathbb{Z}$ mit $[a]_n \cdot [b]_n = [1]_n$. Wir erhalten also $x \cdot [a]_n \cdot [b]_n = y \cdot [a]_n \cdot [b]_n$ und damit $x = y$. Daher ist f injektiv. Weil das Produkt invertierbarer Elemente invertierbar ist, wissen wir, dass $f(I) \subseteq I$ ist. Die Funktion f ist also eine injektive Abbildung von I nach I. Da I endlich ist, ist f bijektiv. Es gilt also:

$$\begin{aligned} \prod_{x \in I} x &= \prod_{x \in I} f(x) \\ \prod_{x \in I} x &= \prod_{x \in I} \left(x \cdot [a]_n \right) \\ \prod_{x \in I} x &= \left(\prod_{x \in I} x \right) \cdot \left([a]_n \right)^{\varphi(n)} \end{aligned}$$

Sei $y \in \mathbb{Z}_n$ das Inverse zu $\prod_{x \in I} x$. Dann gilt:

$$y \cdot \prod_{x \in I} x = y \cdot \left(\prod_{x \in I} x \right) \cdot \left([a]_n \right)^{\varphi(n)}$$

$$[1]_n = \left([a]_n \right)^{\varphi(n)}$$

$$1 \equiv a^{\varphi(n)} \pmod{n}.$$

■

KOROLLAR 6.5. *Sei p eine Primzahl, und sei $z \in \mathbb{Z}$. Dann gilt*

$$z^p \equiv z \pmod{p}.$$

Falls p kein Teiler von z ist, gilt

$$z^{p-1} \equiv 1 \pmod{p}.$$

Beweis: Wir wählen eine Primzahl p und $z \in \mathbb{Z}$ beliebig, aber fest, und nehmen an, dass p die Zahl z nicht teilt. Wir wissen, dass $\varphi(p) = p - 1$, und daher gilt nach dem Satz von Euler

$$z^{p-1} \equiv 1 \pmod{p}.$$

Da $p|(z^{p-1} - 1)$, gilt auch $p|(z^p - z)$, und somit $z^p \equiv z \pmod{p}$.

Wenn $p \mid z$, dann teilt p sowohl z als auch z^p. ■

KOROLLAR 6.6. *Für alle $a, b \in \mathbb{Z}_p$ gilt: $(a + b)^p = a^p + b^p$.*

Der folgende Satz ist eine Grundlage für das RSA-Verfahren zur Verschlüsselung mit öffentlichem Schlüssel.

SATZ 6.5. *Seien p, q Primzahlen, $p \neq q$ und seien $a, s \in \mathbb{Z}$. Dann gilt:*

$$a^{1+s(p-1)(q-1)} \equiv a \pmod{p \cdot q}.$$

Beweis:

- *1. Fall:* $\mathrm{ggT}(a, pq) = 1$*:* Wir wissen ja, dass $a^{p-1} \equiv 1 \pmod{p}$ gilt (Satz von Euler), daher gilt auch $\left(a^{p-1}\right)^{(q-1)\cdot s} \equiv 1 \pmod{p}$. Somit ist p ein Teiler von $a^{(p-1)\cdot(q-1)\cdot s} - 1$ und damit auch von $a^{(p-1)\cdot(q-1)\cdot s+1} - a$. Ebenso zeigen wir

  $$q \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

  Damit gilt insgesamt:

  $$pq \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

- *2. Fall:* $\mathrm{ggT}(a, pq) = p$*:* Da der $\mathrm{ggT}(a, q) = 1$ ist, gilt mit dem Satz von Euler $a^{q-1} \equiv 1 \pmod{q}$, und somit $a^{(q-1)\cdot(p-1)} \equiv 1 \pmod{q}$. Das heißt

  $$q \mid a^{(q-1)\cdot(p-1)\cdot s} - 1.$$

  Wir wissen ja, dass $p \mid a$. Daher gilt $p \cdot q \mid \left(a^{(q-1)\cdot(p-1)\cdot s} - 1\right) \cdot a$.
- *3. Fall:* $\mathrm{ggT}(a, pq) = q$*:* Beweis genauso wie im 2. Fall.
- *4. Fall:* $\mathrm{ggT}(a, pq) = p \cdot q$*:* Dann ist zu zeigen, dass $0 \equiv 0 \pmod{pq}$. ■

2.1. RSA-Verschlüsselungsverfahren. RSA ist ein sogenanntes asymmetrisches Verschlüsselungsverfahren. Wenn ein Teilnehmer, Alice, einem zweiten Teilnehmer, Bob, eine verschlüsselte Nachricht übermitteln will, dann beschafft sich Alice den öffentlichen Schlüssel von Bob. Dieser ist allgemein zugänglich. Alice verschlüsselt nun die Nachricht mit Bob's öffentlichen Schlüssel und schickt sie an Bob. Bob kann die empfangene Nachricht mit seinem privaten (geheimen) Schlüssel entschlüsseln. Wichtig dabei ist, dass es praktisch unmöglich ist, Bob's privaten Schlüssel aus seinem öffentlichen Schlüssel zu rekonstrieren.

Schlüsselerzeugung für das RSA-Verfahren:

(1) Bob wählt Primzahlen p, q. Sei $n := pq$. (In der Praxis soll die Binärdarstellung von n mindestens 1024 Bits haben.)
(2) Bob wählt $e \in \mathbb{N}$ mit $1 < e < (p-1)(q-1)$, sodass $\mathrm{ggT}(e, (p-1)(q-1)) = 1$.
(3) Mit dem Euklidischem Algorithmus bestimmt Bob $d \in \mathbb{N}$, sodass $ed \equiv 1 \pmod{(p-1)(q-1)}$.
(4) Bob's öffentlicher Schlüssel lautet (n, e).
(5) Bob's privater Schlüssel lautet (n, d).

RSA Verschlüsselung:

(1) Alice holt sich Bob's öffentlichen Schlüssel (n, e).
(2) Um eine Nachricht $m \in \{0, \ldots, n-1\}$ zu verschlüsseln, berechnet Alice $c := m^e \bmod n$ und schickt c an Bob.

RSA Entschlüsselung:

(1) Bob erhält eine mit seinem öffentlichen Schlüssel (n, e) verschlüsselte Nachricht $c \in \{0, \ldots, n-1\}$.
(2) Um c zu entschlüsseln, berechnet Bob $m = c^d \bmod n$ mit seinem privaten Schlüssel (n, d).

Die Entschlüsselung ist korrekt, weil nach Satz 6.5 gilt, dass $m^{ed} \equiv m \pmod{n}$ für alle $m \in \{0, \ldots, n-1\}$.

Das RSA-Verfahren ist sicher, weil für große Primzahlen kein effizientes Verfahren bekannt ist, um aus dem öffentlichen Schlüssel (n, e) die Zahl $(p-1)(q-1)$ und damit d zu berechnen.

3. Körper

DEFINITION 6.7. Sei $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1\rangle$ ein Ring. $\boldsymbol{R}$ ist ein *Körper*, wenn folgendes gilt:

(1) $|R| \geq 2$,
(2) für alle $x, y \in R : x \cdot y = y \cdot x$,
(3) für alle $x \in R$ mit $x \neq 0$ gibt es ein $y \in R$, sodass $x \cdot y = 1$.

Der Ring aller 2×2-Matrizen über $\mathbb{R}$ ist kein Körper. Die rellen Zahlen $\mathbb{R}$ sind ein Körper.

SATZ 6.8. *Sei $n \in \mathbb{N}$. Der Ring $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Also ist der zweielementige Ring $\mathbb{Z}_2$ ein Körper. Wir schreiben $\mathbf{0} := [0]_n$, $\mathbf{1} := [1]_n$. Dann gilt $\mathbf{0} \oplus \mathbf{0} = \mathbf{0}$, $\mathbf{0} \oplus \mathbf{1} = \mathbf{1}$, $\mathbf{1} \oplus \mathbf{0} = \mathbf{1}$, $\mathbf{1} \oplus \mathbf{1} = \mathbf{0}$, $\mathbf{0} \odot \mathbf{0} = \mathbf{0}$, $\mathbf{0} \odot \mathbf{1} = \mathbf{0}$, $\mathbf{1} \odot \mathbf{0} = \mathbf{0}$, $\mathbf{1} \odot \mathbf{1} = \mathbf{1}$.

4. Polynome

DEFINITION 6.9. Sei $\boldsymbol{K}$ kommutativer Ring mit Eins. Dann ist $K[x]$ die Menge aller Ausdrücke

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$$

mit $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in K$. Die Elemente von $K[x]$ nennen wir *Polynome*.

Es bietet sich an, Polynome durch die Liste ihrer Koeffizienten darzustellen. Polynome haben beliebig viele, aber immer nur endlich viele Koeffizienten. Somit können wir $K[x]$ mit der Menge aller Folgen aus K identifizieren, in denen nur endlich viele Einträge von 0 verschieden sind,

$$K[x] = \{(a_0, a_1, a_2, \ldots) \in K^{\mathbb{N}_0} \mid \text{fast alle } a_i = 0\}.$$

DEFINITION 6.10. Seien $(a_0, a_1, a_2, \ldots), (b_0, b_1, b_2, \ldots) \in K[x]$. Wir definieren

(1) $(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$
(2) $(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) := (c_0, c_1, c_2, \ldots)$ mit $c_k := \sum_{i+j=k} a_i \cdot b_j$ für alle $k \in \mathbb{N}_0$.

DEFINITION 6.11. Für $f := (a_0, a_1, a_2, \ldots) \in K[x]$ ist der *Grad* von f, $\deg f$, jenes $n \in \mathbb{N}$, sodass $a_n \neq 0$ und $a_i = 0$ für alle $i > n$. Dann nennen wir a_n den führenden Koeffizienten von f. Wir definieren $\deg 0 := -1$.

DEFINITION 6.12. Sei $\boldsymbol{K}$ Körper, und seien $f, g \in K[x]$.

(1) f *teilt* g, wenn es $q \in K[x]$ gibt, sodass $g = q \cdot f$.
(2) f ist *irreduzibel über* $\boldsymbol{K}$ (ein irreduzibles Polynom in $K[x]$), wenn $\deg f \geq 1$ und für alle $a, b \in K[x]$ mit $a \cdot b = f$ entweder a oder b Grad 0 hat.
(3) f ist *normiert*, wenn es führenden Koeffizienten 1 hat.

5. Teilbarkeit von Polynomen

SATZ 6.6. *Sei* $\boldsymbol{K}$ *Körper, und seien* $f, g \in K[x]$. *Wenn* $f \neq 0$, *so gibt es* $q, r \in K[x]$ *mit* $g = q \cdot f + r$ *und* $\deg r < \deg f$.

DEFINITION 6.13 (ggT in $\boldsymbol{K}[x]$). Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0. Dann ist $d \in K[x]$ ein *größter gemeinsamer Teiler* von f und g, wenn folgende Bedingungen gelten:

(1) $d|f$ und $d|g$,
(2) Für alle $h \in K[x]$ mit $h|f$ und $h|g$ gilt $\deg(h) \leq \deg(d)$,

(3) d ist normiert.

Wir bezeichnen den Rest von g bei der Division durch f mit $g \bmod f$. Da das Paar (g, f) die gleichen gemeinsamen Teiler wie das Paar $(f, g \bmod f)$ hat, können wir einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus berechnen.

Wir rechnen dazu drei Beispiele:

AUFGABE 6.14. Wir berechnen einen größten gemeinsamen Teiler von $f, g \in \mathbb{R}[x]$ für

$$f = -8x + 4x^2 + 6x^3 - 5x^4 + x^5$$

und

$$g = 4 - 4x - x^2 + x^3.$$

Wir bilden die gleiche Tabelle wie beim Euklidschen Algorithmus für ganze Zahlen und erhalten:

$$\begin{array}{ccc} -8x + 4x^2 + 6x^3 - 5x^4 + x^5 & 1 & 0 \\ 4 - 4x - x^2 + x^3 & 0 & 1 \\ -24 + 32x - 10x^2 & 1 & -6 + 4x - x^2 \\ -\left(\frac{32}{25}\right) + \frac{16x}{25} & \frac{11}{50} + \frac{x}{10} & -\left(\frac{8}{25}\right) + \frac{7x}{25} + \frac{9x^2}{50} - \frac{x^3}{10} \\ 0 & & \end{array}$$

Um einen normierten gemeinsamen Teiler zu erhalten, multiplizieren wir die vorletzte Zeile dieser Tabelle mit $\frac{25}{16}$ und erhalten $-2 + x$ als einen größten gemeinsamen Teiler. Außerdem gilt

$$-2 + x = \left(\frac{11}{32} + \frac{5x}{32}\right) \cdot f + \left(-\left(\frac{1}{2}\right) + \frac{7x}{16} + \frac{9x^2}{32} - \frac{5x^3}{32}\right) \cdot g.$$

AUFGABE 6.15. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in $\mathbb{Z}_2[x]$. Wir erhalten

$$\begin{array}{ccc} 1 + x^3 + x^5 & 1 & 0 \\ 1 + x + x^3 & 0 & 1 \\ 1 + x^2 & 1 & x^2 \\ 1 & x & 1 + x^3 \\ 0 & & \end{array}$$

Daher ist 1 ein größter gemeinsamer Teiler, und es gilt

$$1 = x \cdot f + (1 + x^3) * g.$$

AUFGABE 6.16. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in $\mathbb{Z}_3[x]$. Wir erhalten

$$\begin{array}{ccc} 1 + x^3 + x^5 & 1 & 0 \\ 1 + x + x^3 & 0 & 1 \\ 1 + 2x^2 & 1 & 2x^2 \\ 1 + 2x & x & 1 + 2x^3 \\ 0 & & \end{array}$$

Daher ist $2 * (1 + 2x) = 2 + x$ ein größter gemeinsamer Teiler, und es gilt

$$2 + x = 2x \cdot f + (2 + x^3) \cdot g.$$

Wir können also einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus bestimmen. Daraus ergibt sich:

SATZ 6.7. *Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0. Dann gibt es einen größten gemeinsamen Teiler d von f und g, für den es $u, v \in K[x]$ gibt, sodass $u \cdot f + v \cdot g = d$.*

SATZ 6.8. *Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0, und sei $d \in K[x]$. Wir nehmen an, dass es $u, v \in K[x]$ gibt, sodass $d = u \cdot f + v \cdot g$. Dann teilt jeder gemeinsame Teiler von f und g auch das Polynom d.*

Beweis: Sei h ein gemeinsamer Teiler von f und g. Dann gilt $h|uf + vg$, also $h|d$. ■

KOROLLAR 6.17. *Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0. Seien $d_1, d_2 \in K[x]$ beide* ggT *von f und g. Dann gilt $d_1 = d_2$.*

Beweis: Nach Satz 6.7 gibt es einen größten gemeinsamen Teiler d von f und g, der sich als $uf + vg$ mit $u, v \in K[x]$ schreiben lässt. Wegen Satz 6.8 gilt $d_1|d$. Sowohl d_1 als auch d haben den maximal möglichen Grad unter allen gemeinsamen Teilern von f und g. Also gilt $\deg(d_1) = \deg(d)$. Somit gibt es ein $\alpha \in K$, sodass $d = \alpha d_1$. Da d und d_1 normiert sind, gilt $\alpha = 1$ und somit $d = d_1$. Ebenso gilt $d = d_2$, also $d_1 = d_2$. ■

6. Polynomfunktionen und Nullstellen

DEFINITION 6.18. Sei $\boldsymbol{K}$ ein Körper, und sei $f \in K[x]$. Seien $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_n \in K$ so, dass

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Dann ist $\overline{f}$ die Funktion, die durch

$$\begin{array}{rccl} \overline{f} & : & K & \longrightarrow & K \\ & & k & \longmapsto & a_0 + a_1 k + a_2 k^2 + \cdots + a_n k^n \end{array}$$

definiert ist. Sie heißt *die von f induzierte Polynomfunktion*.

DEFINITION 6.19. Sei $\boldsymbol{K}$ ein Körper, sei $f \in K[x]$, und sei $\alpha \in K$. Die Zahl α ist eine *Nullstelle* von f, wenn $\overline{f}(\alpha) = 0$.

SATZ 6.9. *Sei $\boldsymbol{K}$ ein Körper, sei $f \in K[x]$, und sei $\alpha \in K$. Dann ist α genau dann eine Nullstelle von f, wenn $x - \alpha \mid f$ gilt.*

SATZ 6.10. *Sei $\boldsymbol{K}$ ein Körper, sei $n \in \mathbb{N}$, und sei $f \in K[x]$ ein Polynom mit* $\deg(f) = n$. *Dann hat f höchstens n Nullstellen.*

Beweis: Die Aussage stimmt für $n = 1$: ein Polynom der Form $\alpha_1 x + \alpha_2$ hat, wenn $\alpha_1 \neq 0$, nur die Nullstelle $-\alpha_2 \cdot (\alpha_1)^{-1}$.

Wir nehmen nun an, dass $n \geq 1$ ist, und dass jedes Polynom vom Grad n höchstens n Nullstellen hat. Wir zeigen, dass dann jedes Polynom vom Grad $n + 1$ höchstens $n + 1$ Nullstellen haben kann. Sei dazu f ein Polynom vom Grad $n + 1$. Wenn f keine Nullstellen hat, dann sind wir fertig, denn"keine Nullstellen" heißt natürlich auch "weniger als $n + 2$ Nullstellen". Wenn f zumindest eine Nullstelle hat, dann wählen wir eine Nullstelle α. Wir können dann ein Polynom g vom Grad n finden, sodass

$$f = (x - \alpha) \cdot g.$$

Sei nun β eine Nullstelle von f mit $\beta \neq \alpha$. Dann gilt $\overline{f}(\beta) = (\beta - \alpha) \cdot \overline{g}(\beta)$. Also gilt $0 = (\beta - \alpha) \cdot \overline{g}(\beta)$. Wegen $\beta - \alpha \neq 0$ gilt $\overline{g}(\beta) = 0$. Das Element β ist daher eine Nullstelle von g.

Da wir angenommen haben, dass jedes Polynom vom Grad n höchstens n Nullstellen hat, hat g höchstens n Nullstellen. Jede Nullstelle von f ist entweder gleich α oder unter diesen n Nullstellen von g. Somit hat f höchstens $n + 1$ Nullstellen. ■

7. Körper aus Polynomringen

Sei f ein Polynom in $K[x]$. Für $a, b \in K[x]$ definieren wir

$$a \equiv b \pmod{f},$$

falls $f | a - b$. Das ist genau dann der Fall, wenn $a \bmod f = b \bmod f$. Wir definieren

$$[a]_f := \{a + q \cdot f \mid q \in K[x]\}.$$

Sei $K[x]/f$ definiert durch

$$K[x]/f := \{[a]_f \mid a \in K[x]\}.$$

Auf $K[x]/f$ definieren wir $+, -, \cdot$ durch

$$\begin{aligned} [a]_f + [b]_f &:= [a + b]_f \\ [a]_f - [b]_f &:= [a - b]_f \\ [a]_f \cdot [b]_f &:= [a \cdot b]_f. \end{aligned}$$

SATZ 6.11. *Sei $\boldsymbol{K}$ ein Körper, und sei $f \in K[x]$. Dann ist $\langle K[x]/f, +, -, \cdot, [0]_f, [1]_f\rangle$ ein Ring mit Eins.*

SATZ 6.12. *Sei $\boldsymbol{K}$ ein Körper, $f \in K[x]$ irreduzibel über $\boldsymbol{K}$. Dann ist $\boldsymbol{K}[x]/f$ ein Körper.*

8. Vektorräume

DEFINITION 6.20. Sei K ein Körper. Ein Tupel $\langle V, \mathbf{+}, \mathbf{-}, \mathbf{0}, *\rangle$ heißt *Vektorraum* über K, wenn $\mathbf{+} : V \times V \to V$, $\mathbf{-} : V \to V$, $\mathbf{0} \in V$ und $* : K \times V \to V$, und für alle $x, y, z \in V$ und $\alpha, \beta \in K$ gilt:

(1) $(x \mathbf{+} y) \mathbf{+} z = x \mathbf{+} (y \mathbf{+} z)$,
(2) $\mathbf{0} \mathbf{+} x = x$,
(3) $(\mathbf{-}x) \mathbf{+} x = \mathbf{0}$,
(4) $x \mathbf{+} y = y \mathbf{+} x$,
(5) $\alpha * (\beta * x) = (\alpha \cdot \beta) * x$,
(6) $(\alpha + \beta) * x = \alpha * x \mathbf{+} \beta * x$,
(7) $\alpha * (x \mathbf{+} y) = \alpha * x \mathbf{+} \alpha * y$,
(8) $1 * x = x$.

BEISPIELE 6.21.

(1) Für jeden Körper K und jedes $n \in \mathbb{N}$ ist K^n (mit geeignet definierten Operationen) ein Vektorraum über K.
(2) Für jeden Unterraum U des $\mathbb{R}^n$ ist U (mit geeignet definierten Operationen) ein Vektorraum über $\mathbb{R}$.

DEFINITION 6.22. Sei K ein Körper und V ein Vektorraum über K. Sei U eine Teilmenge von V. U ist ein *Unterraum* von V, wenn $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha \in K$ gilt $u + v \in U$ und $\alpha * u \in U$.

Wenn U ein Unterraum von $\boldsymbol{V} = \langle V, +, -, 0, *\rangle$ ist, dann ist $\boldsymbol{U} = \langle U, +|_{U\times U}, -|_U, 0, *|_{K\times U}\rangle$ ebenfalls ein Vektorraum über K.