Kapitel 3

Grundlagen

Lernziele

- Formale Definition von Gruppen, Ringen und Körpern,
- Formale Definition von Vektorräumen,
- Formelle Einführung von Polynomen und Polynomringen.

3.1 Gruppen, Ringe und Körper

Hier definieren wir die algebraische Strukturen Gruppen, Ringe und Körper sehr allgemein, indem wir Mengen mit Verknüpfungen betrachten, die gewissen Regeln gehorchen. Die Regeln, die gelten sollen sind an bekannte Rechenregeln in $\mathbb{R}$ angelehnt und wir nennen solche Regeln **Axiome**. Der Vorteil dieses Zugangs ist, dass wir nun Eigenschaften von allen algebraischen Strukturen, die diese Axiome erfüllen, gleichzeitig studieren können. In späteren Vorlesungen werden wir sehen, dass diese Strukturen viele Anwendungen haben.

Definition 3.1

Eine nicht-leere Menge G mit einer binären Verknüpfung $*$ auf G heißt **Gruppe**, falls:

(G1) (Assoziativgesetz) Für alle $a, b, c \in G$ gilt $(a * b) * c = a * (b * c)$.

(G2) (Neutrales Element) Es existiert ein $e \in G$ so dass $a * e = e * a = a$

für alle $a \in G$. Das Element e heißt **neutrales Element von** G.

(G3) (Inverses) Für jedes $a \in G$ existiert ein $b \in G$ mit $a * b = b * a = e$. Das Element b heißt **inverses Element** von a.

Gilt zusätzlich noch, das folgende Axiom
(G4) (Kommutativgesetz) Für alle $a, b \in G$ gilt $a * b = b * a$,
so heißt die Gruppe **abelsch** oder **kommutativ**. Erfüllt $(G, *)$ nur die Axiome (G1) und (G2), so heißt $(G, *)$ eine **Halbgruppe mit 1** oder **Monoid**.

Bemerkung 3.2

Sehr oft schreiben wir die binäre Verknüpfung einer Gruppe G als Multiplikation, d.h. für $a, b \in G$ schreiben wir $a \cdot b$ oder auch nur ab anstatt $a * b$. In diesem Falle bezeichnen wir das neutrale Element auch mit 1_G oder einfach nur mit 1.
In machen Fällen, insbesondere wenn G abelsch ist, kommt es auch oft vor, dass wir die Verknüpfung als $+$ schreiben, d.h. für $a, b \in G$ schreiben wir $a + b$ anstatt $a * b$. In diesem Falle bezeichnen wir das neutrale Element auch mit 0_G oder einfach nur mit 0.

Übung 3.3.
- Man zeige, dass jede Gruppe ein eindeutiges neutrales Element hat.
- Man zeige, dass jedes Element einer Gruppe ein eindeutiges inverses Element besitzt.

Beispiel 3.4

1.) Für $(\mathbb{N}, +)$ gilt nur das Assoziativgesetz (*G1*), und das Kommutativgesetz (*G4*). Also ist $(\mathbb{N}, +)$ keine Gruppe.

2.) $(\mathbb{Z}, +)$ ist eine Gruppe.

3.) Für $a \in \mathbb{Z}$ sei $\mathbb{Z}_{\geq a} := \{r \in \mathbb{Z} \mid r \geq a\}$. Dann sind für $(\mathbb{Z}_{\geq 0}, +)$ das Assoziativgesetz (*G1*), die Existenz des neutralen Elementes

(*G2*), nämlich 0, und das Kommutativgesetz (*G4*) erfüllt. Also ist auch $\mathbb{Z}_{\geq 0}$ keine Gruppe.

4.) Für $\mathbb{Z}_{\geq -1}$ ist nicht einmal $+$ als Verknüpfung definiert.

5.) $(\mathbb{Z}, \cdot)$ ist keine Gruppe, denn $0a = 0$ für alle $a \in \mathbb{Z}$.

6.) $\mathbb{Q}^* := (\mathbb{Q} - \{0\}, \cdot)$ ist eine kommutative Gruppe. Ebenso $\mathbb{R}^* := (\mathbb{R} - \{0\}, \cdot)$.

7.) Da die Komposition von Abbildungen assoziativ ist, ist $(M^M, \circ)$ eine Halbgruppe mit $1 = \mathrm{Id}_M$ für jede Menge M. Diese ist nicht kommutativ, sobald M mehr als ein Element enthält.

8.) Ist $M \neq \emptyset$ eine Menge, so ist $\mathbb{R}^M$ eine kommutative Gruppe mit der werteweisen Addition: Für $f, g \in \mathbb{R}^M$ definiert man:

$$(f + g)(m) := f(m) + g(m) \text{ für alle } m \in M$$

Übung 3.5. Verifiziere alle Gruppenaxiome für 8).

Definition 3.6

Sei R eine Menge mit zwei binären Verknüpfungen $+ : R \times R \to R : (r, s) \mapsto r + s$ und $\cdot : R \times R \to R : (r, s) \mapsto r \cdot s$, die wir in der Regel **Addition** und **Multiplikation** in R nennen. Dann heißt $(R, +, \cdot)$ ein **Ring**, falls gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) (Assoziativgesetz) Für alle $r, s, t \in R$ gilt $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.

(R3) (Distributivgesetze) Für alle $r, s, t \in R$ gilt $(r + s) \cdot t = rt + st$ und $t \cdot (r + s) = tr + ts$.

$(R, +, \cdot)$ heißt **Ring mit 1** wenn zusätzlich gilt:
(R4) Es gibt ein Element $1 \in R$ mit $1 \cdot r = r \cdot 1 = r$ für alle $r \in R$.

Weiterhin heißt der Ring $(R, +, \cdot)$ **kommutativ**, wenn (R1)-(R3) gelten und zusätzlich gilt:

(R5) Für alle $r, s \in R$ ist $r \cdot s = s \cdot r$.

Von jetzt an nehmen wir immer an, dass ein Ring auch das Axiom (R4) erfüllt, also ein Ring mit 1 ist.

Per Definition ist $(R, +)$ eine Gruppe. Allerdings gibt es viele Beispiele von Ringen, für die $(R\backslash\{0\}, \cdot)$ keine Gruppe ist, z.B. für den Ring $(\mathbb{Z}, +, \cdot)$. Wir können aber die folgende Teilmenge von R betrachten: $R^* = \{r \in R \mid \exists s \in R : r \cdot s = s \cdot r = 1\}$. Dann ist $(R^*, \cdot)$ eine Gruppe und jedes Element $r \in R^*$ heißt **Einheit** oder **invertierbar**.

Definition 3.7

Sei $(K, +, \cdot)$ ein Ring (mit 1). Dann heißt K ein **Körper**, wenn

(K1) $0 \neq 1$.

(K2) Für alle $a, b \in K$ ist $a \cdot b = b \cdot a$.

(K3) Für $K^* := K - \{0\}$ ist $(K^*, \cdot)$ eine Gruppe.

Verzichtet man auf (K2), so spricht man von einem **Schiefkörper**.

Beispiel 3.8

Wir geben einige Beispiele von endlichen Körpern anhand der Verknüpfungstabelle für die Addition und die Multiplikation:

a) $\mathbb{F}_2 = \{0, 1\}$ mit folgenden Verknüpfungen:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

b) $\mathbb{F}_3 = \{0, 1, 2\}$ mit folgenden Verknüpfungen:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

c) $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ mit folgenden Verknüpfungen:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

eine allgemeinere Konstruktion befindet sich am Ende dieses Kapitels.

Bemerkung 3.9

Sei K ein Körper. Dann gilt:
1) $0a = 0$ für alle $a \in K$.
2) Statt $a \cdot b^{-1}$ schreibt man auch $\frac{a}{b}$ für alle $a \in K, b \in K^*$. Man hat für $a, c \in K, b, d \in K^*$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}.$$

Beispiel 3.10

1) $(\mathbb{R}, +, \cdot)$, kurz $\mathbb{R}$, ist ein Körper.
2) $\mathbb{Q}$ ist ein Körper (Teilkörper von $\mathbb{R}$).
3) $\mathbb{Z}$ ist kein Körper, sondern nur ein kommutativer Ring mit 1. Der Körper $\mathbb{Q}$ der rationalen Zahlen geht aus dem Ring $\mathbb{Z}$ durch Bereichsvergrößerung hervor.

3.2 Vektorräume

Vektorräume spielen eine zentrale Rolle in dieser Vorlesung und sollen deshalb schon hier definiert werden.

Definition 3.11

Sei K ein Körper. Eine abelsche Gruppe $(V, +)$ zusammen mit einer äußeren Verknüpfung, genannt **Skalarmultiplikation**,

$$K \times V \to V : (a, v) \mapsto av$$

heißt **Vektorraum** über K oder **K-Vektorraum**, falls gilt

(V1)	$(a+b)v$	$=$	$av + bv$	für alle $a, b \in K$ und $v \in V$
(V2)	$a(u+v)$	$=$	$au + av$	für alle $a \in K$ und $u, v \in V$
(V3)	$(ab)v$	$=$	$a(bv)$	für alle $a, b \in K$ und $v \in V$
(V4)	$1v$	$=$	v	für alle $v \in V$

Die Elemente von V heißen **Vektoren**. Die Elemente von K heißen **Skalare**.

Bemerkung 3.12

Ist V ein K-Vektorraum, so gilt:
1) $0v = 0$ für alle $v \in V$, wobei die linke Null das Nullelement von K ist und die rechte das Nullelement von V.
2) $(-1)v = -v$ für alle $v \in V$.

Beweis. 1) $0v = (0+0)v = 0v + 0v$, also durch Subtraktion von $0v$ auf beiden Seiten folgt die Behauptung.
2) Übung q. e. d.

Wir werden im Verlauf der Vorlesung noch viele Beispiele von Vektorräumen kennen lernen. Das folgende Beispiel aber ist besonders wichtig.

Satz 3.13

Sei K ein Körper und $M \neq \emptyset$ eine nicht leere Menge. Dann ist die Menge K^M der Abbildungen von M nach K ein Vektorraum über K mit werteweiser Addition:

$$f + g : M \to K : m \mapsto f(m) + g(m) \qquad \text{für alle } f, g \in K^M$$

und skalarer Multiplikation

$$af : M \to K : m \mapsto af(m) \qquad \text{für alle } f \in K^M \text{ und } a \in K$$

Der Beweis ist eine ganz wichtige Übung.

Ein weiteres Beispiel ist das folgende:

Beispiel 3.14

Seien K und L Körper mit $K \subseteq L$. Dann ist $(L, +)$ ein K-Vektorraum, wobei die skalare Multiplikation eines Elementes aus K mit einem Element in L durch die Multiplikation in L definiert ist.

Definition 3.15

Seien $m, n \in \mathbb{N}$ natürliche Zahlen. Eine $m \times n$-**Matrix** über einem Körper K ist eine Abbildung

$$A : \underline{m} \times \underline{n} \to K : (i, j) \mapsto a_{i,j}.$$

Notation:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n-1} & a_{m,n} \end{pmatrix}.$$

Ist $m = 1$ so ist die Matrix eine **Zeile**, wenn $n = 1$ ist sie eine **Spalte**.

Mit anderen Worten, die Positionen in der Matrix entsprechen dem Definitionsbereich (i-Zeile, j-te Spalte entspricht (i, j)) und der Wert von A für (i, j) wird in die entsprechende Position eingetragen. Die Menge aller $m \times n$-Matrizen über K wird mit $K^{n \times m}$ bezeichnet. Beson-

dere Matrizen sind die Elemente von $K^{n\times 1}$, die wir **Spaltenvektoren** nennen, und die Elemente von $K^{1\times n}$, die wir **Zeilenvektoren** nennen. Der Einfachheit halber lassen wir bei Spaltenvektoren den Zeilenindex und bei Zeilenvektoren den Spaltenindex weg. Das heißt, ein Element $v \in K^{n\times 1}$ schreiben wir als

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

mit $a_1, \ldots, a_n \in K$.

Nun können wir noch ein wichtiges Beispiel eines Vektorraums angeben. Eigentlich wissen wir schon, dass es sich dabei um einen Vektorraum handelt, nach Satz 3.13. Genauer, $K^{n\times 1}, K^{1\times n}, K^{m\times n}, K^K, K^{\mathbb{N}}$ subsumieren sich alle unter dieses Beispiel und wir identifizieren K^n mit dem Spaltenraum $K^{n\times 1}$. Beachte weiter, $K \equiv K^1$ ist ebenfalls Vektorraum über K. Wir führen dennoch das folgende Beispiel aus:

Beispiel 3.16

$(K^{n\times 1}, +)$ ist ein K-Vektorraum: Auf $K^{n\times 1}$ ist eine Verknüpfung $+$ gegeben, die **Addition** heißt,

$$+ : K^{n\times 1} \times K^{n\times 1} \to K^{n\times 1} : (v, w) \mapsto v + w$$

definiert durch

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, w = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} := \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

Weiter ist eine sogenannte äußere Verknüpfung $\cdot$ auf $K^{n\times 1}$ mit K gegeben, genannt **Skalarmultiplikation** durch

$$\cdot : K \times K^{n\times 1} \to K^{n\times 1} : (r, v) \mapsto r \cdot v$$

definiert durch

$$r \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} := \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}$$

Wir schreiben rv anstatt $r \cdot v$.

Definition 3.17

Sind $v_1, \ldots, v_k \in K^{n\times 1}$ und $c_1, \ldots, c_k \in K$, so heißt

$$c_1v_1 + \cdots + c_kv_k \qquad (\in K^{n\times 1})$$

die **Linearkombination** der (Spaltenvektoren) v_i mit den Koeffizienten (Skalaren) c_i.

Beispiel 3.18

Sei $K = \mathbb{F}_3$, der Körper mit drei Elementen und sei

$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, u = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Dann ist

$$w = 2v + u = \begin{pmatrix} 2 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

eine Linearkombination von v und u.

3.3 Polynomringe

Wir haben bereits kommutative Ringe kennengelernt. Wir wollen jetzt über einen ganz wichtigen Ring sprechen, der, wie sich später herausstellt, gleichzeitig Vektorraum ist und der eine absolut grundlegende Rolle in der linearen Algebra spielt.

Definition 3.19

Sei K ein Körper.
1) Auf dem K-Vektorraum $K^{\mathbb{Z}_{\geq 0}}$ definieren wir eine Multiplikation durch

$$(a_0, a_1, a_2, a_3, \ldots) \cdot (b_0, b_1, b_2, b_3, \ldots) := (c_0, c_1, c_2, c_3, \ldots)$$

mit

$$c_0 := a_0b_0, c_1 := a_0b_1 + a_1b_0, c_2 := a_0b_2 + a_1b_1 + a_2b_0, \ldots$$

allgemein für alle $n \geq 0$:

$$c_n := a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$$

$(K^{\mathbb{Z}_{\geq 0}}, +, \cdot)$ zusammen mit der K-Vektorraumstruktur von $K^{\mathbb{Z}_{\geq 0}}$ wird auch mit $K[[X]]$ bezeichnet und heißt der **Potenzreihenring** über K in $X := (0, 1, 0, 0, \ldots)$, oder der Ring der **formalen Potenzreihen** über K.
(Statt $(a_0, a_1, a_2, a_3, \ldots)$ schreibt man auch $\sum_{i=0}^{\infty} a_i X^i$.)
2) Eine Potenzreihe $f = (a_0, a_1, a_2, a_3, \ldots) \in K[[X]]$ heißt **Polynom**, falls ein $n \in \mathbb{Z}_{\geq 0}$ existiert mit $a_i = 0$ für alle $i > n$. Man schreibt auch $f = \sum_{i=0}^{n} a_i X^i$. Für $f \neq 0$ heißt das kleinste derartige n der **Grad** von f. (Manchmal setzt man $\mathrm{Grad}(0) := -\infty$.) Die Menge aller Polynome zusammen mit der Vektorraumstruktur und der von $K[[X]]$ ererbten Multiplikation heißt der **Polynomring** $K[X]$ über K (Selbstverständlich kann man auch einen anderen Buchstaben als X für die **Unbestimmte** benutzen.)

Beispiel 3.20

(Stichwort: schriftliche Multiplikation ohne Übertrag) In $\mathbb{F}_7[X]$ berechnen wir fg mit $f := (1, 2, 3, 4, 0, 0, \ldots) = 1 + 2X + 3X^2 + 4X^3$ und $g := (4, 3, 2, 1, 0, 0, \ldots) = 4 + 3X + 2X^2 + X^3$ wie folgt:

$$\begin{aligned}
f \cdot 4 &= (4, 1, 5, 2, 0, 0, \ldots) = 4 + 1X + 5X^2 + 2X^3 \\
f \cdot 3X &= (0, 3, 6, 2, 5, 0, 0, \ldots) = 3X + 6X^2 + 2X^3 + 5X^4 \\
f \cdot 2X^2 &= (0, 0, 2, 4, 6, 1, 0, 0, \ldots) = 2X^2 + 4X^3 + 6X^4 + X^5 \\
f \cdot X^3 &= (0, 0, 0, 1, 2, 3, 4, 0, 0, \ldots) = X^3 + 2X^4 + 3X^5 + X^6
\end{aligned}$$

d.h. $fg = (4, 4, 6, 2, 6, 4, 4, 0, 0, \ldots) = 4 + 4X + 6X^2 + 2X^3 + 6X^4 + 4X^5 + 4X^6$.

Bemerkung 3.21

1) $1 := (1, 0, 0, \ldots) \in K[X]$ ist das neutrale Element der Multiplikation in $K[[X]]$ und auch in $K[X]$.

2) $Xa = (0, a_0, a_1, \ldots)$ für alle $a \in K[[X]]$.

3) Es gilt $X^i X^j = X^{i+j}$. Man setzt $X^0 := 1$. (Man sieht, wie die Multiplikation der Monome X^i der Addition der Exponenten entspricht.)

4) Sei $f \in K[X]$ ein Polynom vom Grad n, dann gilt

$$f = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n.$$

Dies liefert eine offensichtliche Identifikation von K mit

$$\{0\} \cup \{f \in K[X] \mid \mathrm{Grad}(f) = 0\}.$$

5) $K[X]_{\mathrm{Grad}<n} := \{0\} \cup \{f \in K[X] \mid \mathrm{Grad}(f) < n\}$ ist ein Vektorraum.

6) Für $f, g \in K[X] - \{0\}$ gilt $\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.

Definition 3.22

Sei R ein Ring mit Eins, der gleichzeitig ein K-Vektorraum für den Körper K ist. Man nennt dann R eine **assoziative K-Algebra** mit Eins oder kürzer **K-Algebra** , falls gilt:

$$a(rs) = (ar)s = r(as)$$

für alle $r, s \in R$ und $a \in K$.

Satz 3.23

Sei K ein Körper.
1) $K[X]$ ist ein kommutativer Ring mit Eins, genauer, eine kommutative K-Algebra mit 1.

2) **(Division mit Rest)** Für $f, g \in K[X]$ mit $g \neq 0$ existieren eindeutige $q, r \in K[X]$ mit

$$f = qg + r \text{ und } \operatorname{Grad}(r) < \operatorname{Grad}(g) \text{ oder } r = 0.$$

Beweis. 1) Dass die Multiplikation kommutativ ist und wir ein Einselement haben folgt sofort aus der Kommutativität der Multiplikation in K. Das Distributivgesetz, d.h. $(f+g)h = fh + gh$ für alle $f, g, h \in K[X]$, ist leicht zu zeigen. Außerdem kann man sehr leicht zeigen, dass das Assoziativgesetz für Skalare gilt, d.h. $(af)g = a(fg) = (fg)a = (fa)g$ für alle $f, g, h \in K[X], a \in K$. Wir zeigen nun, dass das Assoziativgesetz gilt, d.h. dass für alle $f, g, h \in K[X]$ gilt $(fg)h = f(gh)$. Wir führen den Beweis durch Induktion nach $\operatorname{Grad}(h)$. Falls $\operatorname{Grad}(h) = 0$, dann ist $h \in K$ und die Behauptung gilt aufgrund des Assoziativgesetzes für Skalare. Angenommen die Behauptung gelte für alle h mit $\operatorname{Grad}(h) \leq n$. Ist $\operatorname{Grad}(h) > 0$, dann ist $h = \tilde{h} + a_{n+1}X^{n+1}$, wobei $\tilde{h} \in K[X]$ ein Polynom vom Grad höchstens n ist oder $\tilde{h} = 0$. Also gilt nach Induktionsvoraussetzung, $(fg)\tilde{h} = f(g\tilde{h})$. Mit dem Distributivgesetz und dem Assoziativgesetz für Skalare gilt nun:

$$\begin{aligned}
(fg)h &= (fg)(\tilde{h} + a_{n+1}X^{n+1}) \\
&= (fg)\tilde{h} + (fg)a_{n+1}X^{n+1} \\
&= f(g\tilde{h}) + f(ga_{n+1})X^{n+1} \\
&= f(g\tilde{h} + ga_{n+1}X^{n+1}) \\
&= f\big(g(\tilde{h} + a_{n+1}X^{n+1})\big) \\
&= f(gh).
\end{aligned}$$

2) Sei $\operatorname{Grad}(f) = m$, $\operatorname{Grad}(g) = n$ und $f = \sum_{j=0}^{m} a_j X^j$ und $g = \sum_{j=0}^{n} b_j X^j$. Falls $f = 0$ so ist $q = 0$ und $r = 0$. Falls $m < n$, sind wir bereits fertig, denn dann ist $q = 0$ und $r = f$.

Wir betrachten nun den Fall $m \geq n$ und beweisen die Existenz von q und r per Induktion nach m. Für $m = 0$ ist $n = 0$ und $f = a_0$ und $g = b_0$. Wir setzen $q = \frac{a_0}{b_0}$ und $r = 0$ und sehen, dass $f = qg + r$.

Sei nun $m > 0$ und wir nehmen an, dass für jedes Polynom h mit $\text{Grad}(h) \leq m-1$ Polynome $\tilde{q}$ und $\tilde{r}$ existieren mit $\text{Grad}(\tilde{r}) < \text{Grad}(g)$ und $h = \tilde{q}g + \tilde{r}$.

Definiere nun $\tilde{f} := f - \frac{a_m}{b_n} X^{m-n} g$. Dann ist $\text{Grad}(\tilde{f}) \leq m-1$. Also existierten nach Induktionsannahme $\tilde{q}$ und $\tilde{r}$ mit $\text{Grad}(\tilde{r}) < \text{Grad}(g)$ und $\tilde{f} = \tilde{q}g + \tilde{r}$. Also ist

$$f = \tilde{f} + \frac{a_m}{b_n} X^{m-n} g = \tilde{q}g + \tilde{r} + \frac{a_m}{b_n} X^{m-n} g = (\tilde{q} + \frac{a_m}{b_n} X^{m-n})g + \tilde{r}.$$

Daher ist mit $q = \tilde{q} + \frac{a_m}{b_n} X^{m-n}$ und $r = \tilde{r}$ die Existenz gezeigt.

Zur Eindeutigkeit: Sei $f = qg + r$ und $f = \tilde{q}g + \tilde{r}$ mit $\text{Grad}(r) < \text{Grad}(g)$ und $\text{Grad}(\tilde{r}) < \text{Grad}(g)$. Dann folgt

$$r - \tilde{r} = (q - \tilde{q})g$$

Wäre $q - \tilde{q} \neq 0$, dann wäre $\text{Grad}(r - \tilde{r}) \geq \text{Grad}(g)$, was ein Widerspruch ist. Also ist $q = \tilde{q}$ und $r = \tilde{r}$. q. e. d.

Beispiel 3.24

$f = X^6 - X - 1, g = X^2 - X + 1 \in \mathbb{Q}[X]$. Wir suchen den Quotienten q und den Rest r. Dies können wir sehr ähnlich zur schriftlichen Division berechnen:

$$\begin{array}{rl}
(X^6 & -X-1) : (X^2 - X + 1) = X^4 + X^3 - X - 1 + \dfrac{-X}{X^2 - X + 1} \qquad r = -X \\
\underline{-X^6 + X^5 - X^4} & \\
X^5 - X^4 & \\
\underline{-X^5 + X^4 - X^3} & \\
-X^3 & -X \\
\underline{X^3 - X^2 + X} & \\
-X^2 & -1 \\
\underline{X^2 - X + 1} & \\
-X &
\end{array}$$

Also ist $f = (X^4 + X^3 - X - 1)g + (-X)$, d.h.
$q = -1 - X + X^3 + X^4$ und $r = -X$.

3.4 Der Restklassenring modulo n

Wir führen eine Konstruktion für einige endliche Ringe und endliche Körper ein.

Definition 3.25

Sei $n \in \mathbb{N}$. Auf der Menge $\mathbb{Z}$ der ganzen Zahlen definieren wir eine Relation $\sim_n$ vermöge:

$$a \sim b \text{ genau dann, wenn } n \mid (a-b).$$

Dies bedeutet, dass zwei Zahlen a und b genau dann äquivalent sind, wenn sie nach Division mit n den selben Rest haben.

Wir zeigen in den Übungen, dass $\sim_n$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert.

Für $i, n \in \mathbb{Z}$ sei

$$\overline{i} := i + n\mathbb{Z} = \{i + na \mid a \in \mathbb{Z}\} \text{ und}$$

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0} := n\mathbb{Z}, \overline{1} := 1+n\mathbb{Z}, \overline{2} := 2+n\mathbb{Z}, \ldots, \overline{n-1} := n-1+n\mathbb{Z}\}.$$

Dies ist die Menge der **Äquivalenzklassen auf $\mathbb{Z}$** bezüglich der Äquivalenzrelation $k \sim \ell \Leftrightarrow n \mid (k-\ell)$. Wir definieren die Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}$ anhand von "Vertretern" durch

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) := (a+b) + n\mathbb{Z}, \qquad (a+n\mathbb{Z})(b+n\mathbb{Z}) := ab + n\mathbb{Z}$$

für alle $a, b \in \mathbb{Z}$. Das bedeutet, dass

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Man muß hier zeigen, daß die Addition und Multiplikation **wohldefiniert** sind, also vertreterunabhängig, da in der Definition mit Vertretern der Äquivalenzklassen gearbeitet wird. Wir lassen dies als Übung.

Man hat also eine surjektive Abbildung:

$$^{-} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto \overline{a} = a+n\mathbb{Z},$$

welche das Rechnen überträgt. Man beachte: $\overline{0}$ ist das Nullelement und $\overline{1}$ das Einselement von $\mathbb{Z}/n\mathbb{Z}$. Daher schreiben wir 0 statt $\overline{0}$ und

1 statt $\overline{1}$, etc., wenn klar ist, dass wir in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ arbeiten. Dann ist $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring (Übung).

Im Fall, dass p eine Primzahl ist, dann ist der Ring $\mathbb{Z}/p\mathbb{Z}$ sogar ein Körper. Diesen bezeichnen wir mit

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\overline{0} := p\mathbb{Z}, \overline{1} := 1+p\mathbb{Z}, \ldots, \overline{p-1} := p-1+p\mathbb{Z}\}.$$

Wir lassen es als Übung, dass jedes Element von $\mathbb{F}_p - \{0\}$ ein multiplikativ Inverses besitzt.

Zu diesem Thema wird auch ein **Video** hochgeladen.

Als Zusammenfassung noch einmal die Aussagen, die Sie als Übung zeigen sollten.

Übung 3.26. Sei $n \in \mathbb{N}$.

1. $\sim_n$ definiert eine Äquivalenzrelation auf $\mathbb{Z}$. (Eine Äquivalenzrelation ist reflexiv, transitiv und symmetrisch).
2. Sei $d \in \mathbb{N}$ mit $d \mid n$ und $a \equiv b \pmod{n}$. Dann ist auch $a \equiv b \pmod{d}$.
3. Die oben definierten Verknüpfungen $+$ und $\cdot$ sind wohldefiniert.
4. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.
5. Ist p eine Primzahl, so ist $(\mathbb{Z}/pZ, +, \cdot)$ ein Körper. Diesen bezeichnen wir oft mit $\mathbb{F}_p$.

3.5 Zusammenfassung von Kapitel 1

Sie sollten nun mit den folgenden Themen vertraut sein:

- Formale Definition von Gruppen, Ringen, und Körpern, erste Eigenschaften dieser Bereiche beweisen, e.g. neutrale Elemente sind eindeutig. Als Beispiele für diese Strukturen sollten Sie die symmetrische Gruppe, den Ring $\mathbb{Z}/n\mathbb{Z}$ und den Polynomring $K[X]$, sowie die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ und $\mathbb{F}_p$ kennen.

- Formale Definition von Vektorräumen, und K-Algebren. Als Beispiele von K-Vektorräumen für einen Körper K dienen die Spaltenräume K^n und die Menge K^M der Abbildungen von M nach K.
- Formelle Definition von Polynomen und Polynomringen und der Unterschied zwischen Polynomen und Polynomabbildungen, sowie formale Potenzreihen.

‘