Kurze Notizen zu einem Teil von § 0

Definition 5:
Seien M, N nichtleere Mengen, dann ist $\mathsf{Abb}\,(\boldsymbol{M}, \boldsymbol{N}) = \{f : M \to N\}$ und wenn $M = N$, dann ist $\mathsf{Abb}\,(\boldsymbol{M}) = \{f : M \to M\}$.
Definition 6:
Eine Menge M mit einer Verknüpfung $\varphi : M \times M \to M$ heißt **Monoid**, wenn gilt:
M1: $\varphi(\varphi(a, b), c) = \varphi(a, \varphi(b, c))$ für alle $a, b, c \in M$.
M2: Es gibt ein neutrales Element e in M mit dem für alle $a \in M$ gilt: $\varphi(e, a) = a = \varphi(a, e)$.
Das Monoid heißt **kommutativ**, wenn außerdem gilt $\varphi(a, b) = \varphi(b, a)$ für alle $a, b \in M$.
Man sagt (M, φ) ist ein Monoid, oder auch nur M ist ein Monoid (bezüglich φ).
Je nach Kontext werden **vereinfachende Schreibweisen** für die Verknüpfung φ benutzt. Z.B.

$$\varphi(a, b) = a + b,\ \varphi(a, b) = a \cdot\ b,\ \varphi(a, b) = ab,\ \varphi(a, b) = a * b \text{ oder } \varphi(a, b) = a \circ b.$$

Beispiele 7:
(a) $(M, +)$ und $(M, \cdot\ )$ für $M \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$.
(b) $(\{$ grade Zahlen $\}, \cdot\ )$ ist kein Monoid, denn es gibt kein neutrales Element.
Satz 8: $(\mathsf{Abb}\,(M), \circ)$ ist ein Monoid, oder (üblicher) $\mathsf{Abb}\,(M)$ ist ein Monoid bezüglich $\circ$, der Hintereinanderausführung von Abbildungen. Dabei ist id_M die Abbildung aus $\mathsf{Abb}\,(M)$ mit der Vorschrift $id_M(x) = x$ für alle $x \in M$.
Definition 9: Sei $(M, *)$ ein Monoid mit neutralem Element e.
(a) $a \in M$ heißt invertierbar, wenn es ein $b \in M$ gibt derart, dass $a * b = b * a = e$. b heißt dann Inverses von oder zu a und wird mit a^{-1} bezeichnet.
(b) $(M, *)$ heißt Gruppe (oder nur M ist Gruppe (bezüglich $*$)), wenn alle $a \in M$ invertierbar sind. Eine Gruppe heißt **kommutativ** oder **abelsch** wenn sie als Monoid kommutativ ist.
(c) Die Menge der invertierbaren Elemente im Monoid M bezüglich einer fest vorgegebenen Verknüpfung $*$ wird mit $G(M)$ bezeichnet.
Beobachtung 10:
(a) Inverse und neutrale Elemente in einem Monoid sind eindeutig bestimmt.
(b) Ist M ein Monoid (bezüglich $*$), so ist stets $G(M)$ eine Gruppe (bezüglich $*$).

Im Mittelpunkt von § 0 standen neben Abbildungen die vollständige Induktion und der Monoidbegriff mit dem natürlichen Beispiel $\mathsf{Abb}\,(M)$. Die folgenden Definitionen und Regeln werden in der Vorlesung ab § 1 benutzt.

Definition 11:
Eine Menge R mit zwei Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation) heißt Ring, wenn folgendes gilt:
(a) $(R, +)$ ist eine kommutative Gruppe, deren neutrales Element wir mit 0_R oder 0 bezeichnen.
(b) $(R, \cdot\ )$ ist ein Monoid, dessen neutrales Element wir mit 1_R oder 1 bezeichnen.
(c) Distributivgesetz für alle $a, b, c \in R$: $a \cdot\ (b + c) = a \cdot\ b + a \cdot\ c$ und $(a + b) \cdot\ c = a \cdot\ c + b \cdot\ c$.

Man sagt, R ist ein Ring, obwohl es natürlich genauer wäre zu sagen, das Tripel $(R, +, \cdot\ )$ ist ein Ring. Das neutrale Element bezüglich der Multiplikation in einem Ring wird auch **Einselement** oder 1-Element genannt. Meist wird nur ab statt $a \cdot\ b$ geschrieben. Ein Ring R heißt **kommutativ**, wenn das Monoid $(R, \cdot\ )$ kommutativ ist. Ein kommutativer Ring R heißt **Körper**, wenn $G(R) = R \setminus \{0\}$ eine Gruppe ist. Insbesondere ist dann $R \setminus \{0\}$ nicht leer und enthält zumindest das dann von 0 verschiedene 1-Element des Ringes.
Die **Einheitengruppe** des Ringes ist die Gruppe (Beobachtung 10) der invertierbaren Elemente im Monoid $(R, \cdot\ )$ und wird mit $\boldsymbol{G(R)}$ bezeichnet.
Beachte: Nicht immer wird von vorne herein gefordert, dass ein Ring ein 1-Element enthält. Unsere Definition ist die gängigste und auch für die lineare Algebra zweckmäßigste.

Beispiele 12:

(a) Ein Extremfall (Ring mit minimaler Elementeanzahl) ist der sogenannte Nullring $\{0\}$. 0 ist hier sowohl das Nullelement, als auch das Einselement. Zwangsläufig ist dann $0 + 0 = 0$ und $0 \cdot\ 0 = 0$.

(b) $(\mathbb{N}, +, \cdot\ )$ ist kein Ring.

(c) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit der üblichen Addition und Multiplikation sind kommutative Ringe. $\mathbb{Q}$ und $\mathbb{R}$ sind bekanntlich Körper.

(d) $\mathbb{Z}_2 = \{0, 1\}$ mit den Rechenregeln: $0 + 0 = 1 + 1 = 0 \cdot\ 1 = 1 \cdot\ 0 = 0 + 0 = 0$ und $0 + 1 = 1 + 0 = 1 \cdot\ 1 = 1$ ist ein Körper. Es wird also in $\mathbb{Z}_2$ mit 0 und 1 gerechnet wie in $\mathbb{Z}$ mit einer Ausnahme: $1 + 1 = 0$!

(e) $\mathbb{Z}_3$ mit den folgenden in Tabellenform gegebenen Rechenregeln ist ebenfalls ein Körper:

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

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(f) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ mit den folgenden Rechenregeln ist ein kommutativer Ring aber kein Körper:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(g) $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ mit den folgenden Rechenregeln ist wieder ein Körper:

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Nachzuprüfen, dass ein Körper vorliegt, ist hier schon etwas mühsamer. Wie man das systematisch angeht, lernt man in der Algebra. Solche und noch viel größere endliche Körper treten in zahlreichen Anwendungen u. A. in Kodierung und Kryptografie auf. Ein Ergebnis der Algebra ist z.B. dass es zu jeder Primzahl und jedem $k \in \mathbb{N}_+$ im Wesentlichen nur einen Körper gibt mit p^k Elementen und dass es keine anderen endlichen Körper mehr gibt. Besonders relevant für Anwendungen sind die Körper mit 2^k Elementen. $\mathbb{Z}_2$ entspricht dem Fall $k = 1$ und $\mathbb{F}_4$ dem Fall $k = 2$.

Beobachtung 13: Rechnen in Ringen und Körpern

Alle beim Rechnen benutzten Regeln müssen auf die Gesetze (Axiome) in den Definitionen zurückgeführt werden! Dies muss man aber nicht jedes mal neu tun. Viele häufig benötigten Regeln wurden auf Vorrat bereits bewiesen und können benutzt werden. Im Zweifelsfall sollte eine Mathematikerin oder ein Mathematiker immer in der Lage sein, die Beweise für solche Regeln zu überprüfen und bei Bedarf auch selbst Regeln herzuleiten.

Die folgenden elementaren Regeln sind uns vom Rechnen mit Zahlen her vertraut:

(a) 0-Element und 1-Element in einem Ring sind eindeutig bestimmt.

(b) Additive und, falls existent, auch multiplikative Inverse in einem Ring sind eindeutig bestimmt. Bezeichnungen: $-a$ und a^{-1}.

(c) In einem Ring R gilt: $0 = 0 \cdot\ a = a \cdot\ 0$ für alle $a \in R$.

(d) In einem Körper K gilt:

$$\forall a, b \in K \ : \quad a \cdot\ b = 0 \ \Rightarrow\ [\ a = 0 \text{ oder } b = 0\ ]$$

(e) Assoziativgesetze für mehr als 3 Operanden bei Addition und Multiplikation.

(f) Distributivgesetze für mehr als zwei Summanden: Sei $n \geq 2$. Für alle $a, b_1, \ldots, b_n \in R$ gilt:

$$a \cdot\ (b_1 + \cdots + b_n) = a \cdot\ b_1 + \cdots + a \cdot\ b_n \quad \text{und} \quad (b_1 + \cdots + b_n) \cdot\ a = b_1 \cdot\ a + \cdots + b_n \cdot\ a$$