Leitfaden: Lineare Algebra

Als erstes wollen wir uns "Matrizen" mit Koeffizienten in einem "kommutativen Ring", wie zum Beispiel im Körper $\mathbb{Q}$ der rationalen Zahlen, zuwenden. Bevor wir dies tun können, ist der Begriff "kommutativer Ring" zu definieren. Wir werden sehen, dass es viele Beispiele solcher "kommutativer Ringe" gibt.

Wir setzen hier voraus, dass die Menge $\mathbb{Q}$ der rationalen Zahlen bekannt ist. Mit $\mathbb{Z}$ bezeichnen wir die Menge der ganzen Zahlen, also $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, mit $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ die der natürlichen Zahlen.

(Gelegentlich werden wir auch auf die Menge $\mathbb{R}$ der reellen Zahlen verweisen; grundsätzlich sollte diese Menge von der Schule her bekannt sein. Die Konstruktion dieser Menge ist aber keineswegs einfach. Erst wenn im Rahmen der Vorlesung *Analysis* der "Körper" $\mathbb{R}$ der reellen Zahlen konstruiert (und charakterisiert) worden ist, werden wir auch in dieser Vorlesung damit arbeiten.)

0. Erste Grundbegriffe.

(0.0) Mengen.

Menge, Element, $\in$*:* Dies sind Grundbegriffe, die wir nicht weiter hinterfragen. Wichtige Beispiele von Mengen:

Die Menge $\mathbb{N}_0$ der natürlichen Zahlen $0, 1, 2, \ldots$.

Die Menge $\mathbb{N}_1$ der von Null verschiedenen natürlichen Zahlen.

Die Menge $\mathbb{Z}$ der ganzen Zahlen $\ldots, -2, -1, 0, 1, 2, \ldots$.

Die Menge $\mathbb{Z}^*$ der von Null verschiedenen ganzen Zahlen.

Die Menge $\mathbb{Q}$ der rationalen Zahlen. (Jede rationale Zahl hat die Form $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.)

Die Menge $\mathbb{Q}^*$ der von Null verschiedenen rationalen Zahlen.

Die Menge $\mathbb{R}$ der reellen Zahlen.

Die Menge $\mathbb{R}^*$ der von Null verschiedenen reellen Zahlen.

Ist a ein Element der Menge M, so schreibt man $a \in M$. Mengen können gegeben werden durch eine Aufzählung ihrer Elemente: zum Beispiel kann die Menge S der natürlichen Zahlen, die kleiner oder gleich 4 sind, durch $S = \{0, 1, 2, 3, 4\}$ oder durch $\{1, 1, 4, 0, 1, 3, 2\}$ beschrieben werden. (Bei dieser Beschreibung mit Hilfe der der Mengenklammern $\{\,\}$ kommt es nicht auf die Reihenfolge an, auch prüft man nicht, ob Elemente mehrfach notiert sind.) Ist S eine Menge, die nur endlich viele Elemente enthält, so schreibt man $|S|$ für die Anzahl der Elemente. Zum Beispiel ist $|\{1, 1, 4, 0, 1\}| = 3$.

Sind U, M Mengen, so nennt man U eine *Teilmenge* (oder *Untermenge* von M, falls jedes Element von U auch Element von M ist, und man schreibt $U \subseteq M$. Ist $U \subseteq M$ und $U \neq M$, so schreibt man $U \subset M$ und nennt U eine *echte Teilmenge*

von M. [**Warnung:** Manche Bücher verwenden das Zeichen $\subset$ zur Bezeichnung beliebiger (nicht notwendig echter) Teilmengen.] Untermengen beschreibt man oft durch die Angabe der definierenden Eigenschaften, die Menge $S = \{0, 1, 2, 3, 4\}$ kann zum Beispiel durch $S = \{z \in \mathbb{N}_0 \mid z \leq 4\}$ beschrieben werden. Die leere Menge $\emptyset = \{\}$ – sie enthält kein Element – ist Teilmenge jeder Menge.

Mit $\mathcal{P}(M)$ bezeichnen wir die Menge aller Teilmengen der Menge M, man nennt $\mathcal{P}(M)$ die *Potenzmenge zu* M. Zum Beispiel gilt: $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$; es ist also $\mathcal{P}(\{1,2\})$ eine Menge mit 4 Elementen.

Sind M_1, M_2 Untermengen einer Menge M, so nennt man

$$M_1 \cap M_2 = \{x \in M \mid x \in M_1 \quad \text{und} \quad x \in M_2\}$$

den *Durchschnitt* der beiden Mengen und

$$M_1 \cup M_2 = \{x \in M \mid x \in M_1 \quad \text{oder} \quad x \in M_2\}$$

die *Vereinigung* der beiden Mengen M_1, M_2. Die Menge

$$M_1 \setminus M_2 = \{x \in M_1 \mid x \notin M_2\}$$

nennt man die *Differenzmenge;* beachte, dass hier nicht vorausgesetzt wird, dass M_2 eine Teilmenge von M_1 ist.

Seien A, B Mengen. Das *Produkt* $A \times B$ der Mengen A, B ist die Menge aller Paare (a, b) mit $a \in A$, $b \in B$. Eine *Abbildung von* A *nach* B ist eine Teilmenge $f \subseteq A \times B$ mit folgenden Eigenschaften:

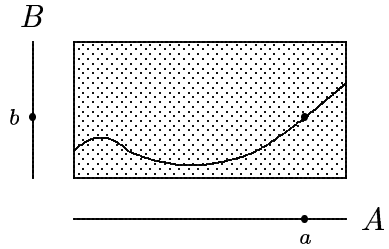
(A1) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in f$.

(A2) Gehören die Paare (a, b_1) und (a, b_2) zu f, mit $a \in A$ und $b_1, b_2 \in B$, so ist $b_1 = b_2$.

Sei f eine Abbildung von A nach B. Meist schreibt man statt $(a, b) \in f$ lieber $f(a) = b$ oder auch $a \mapsto b$, und man schreibt statt f oft $f\colon A \to B$.

Unsere Definition interpretiert eine Abbildung f einfach als die Menge der Paare $(a, f(a))$ mit $a \in A$. Manchmal unterscheidet man auch zwischen der Abbildung f und der Menge $\{(a, f(a)) \mid a \in A\}$, die man den *Graph* der Abbildung f nennt; aber dann muss man irgendwie anders erklären, was eine Abbildung sein soll: Man spricht von einer Zuordnung oder so, aber wie definiert man, was eine Zuordnung ist? Die Zuordnung $a \mapsto f(a)$ sollte man keinesfalls als einen dynamischen Vorgang auffassen, sondern statisch: durch f ist mit $a \in A$ das Element $f(a) \in B$ verbunden; gegeben sind die Paare $(a, f(a))$ in $A \times B$, also der Graph.

Man verwendet manchmal eine Skizze der folgenden Art:



Die punktierte Menge soll $A \times B$ veranschaulichen, die darin gezogene Kurve den Graph von f. Die fetten Punkte markieren ein $a \in A$, das zugehörige $b = f(a) \in B$ und das Paar $(a, b) \in A \times B$.

(0.1) Halbgruppen und Gruppen.

Sei S eine Menge. Eine *Verknüpfung* auf S ist eine Abbildung $\mu\colon S \times S \to S$, statt $\mu(s_1, s_2)$ schreibt man manchmal $s_1 + s_2$ oder $s_1 s_2$ oder $s_1 * s_2$ oder $s_1 \circ s_2$ oder ...

Eine *Halbgruppe* $H = (H, *)$ ist eine Menge H mit einer Verknüpfung (die $(h_1, h_2) \mapsto h_1 * h_2$ geschrieben wird), mit folgenden Eigenschaften:

(H1) Für alle $h_1, h_2, h_3 \in H$ gilt $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$ (Assoziativität).

(H2) Es gibt ein Element $e \in H$ mit $e * h = h = h * e$ für alle $h \in H$. (Man nennt e ein *Einselement*.)

Lemma. *Eine Halbgruppe H hat nur ein Einselement.* (Beweis: Sind Elemente $e, e' \in H$ gegeben mit $e * h = h = h * e$ und $e' * h = h = h * e'$ für alle $h \in H$, so ist $e = e * e' = e'$.) Dieser Beweis zeigt sogar: Das Einselement einer Halbgruppe ist die einzige "Rechts-Eins" und die einzige "Links-Eins"; dabei ist eine "Rechts-Eins" ein Element r mit $h * r = h$ für alle $h \in H$, eine "Links-Eins" ... Man schreibt manchmal 1_H für das Einselement der Halbgruppe H. Ist H eine Halbgruppe, so heißt $h \in H$ *idempotent*, falls $h * h = h$ gilt. Das Einselement einer Halbgruppe ist idempotent, im allgemeinen wird es aber in einer Halbgruppe weitere idempotente Elemente geben.

Eine Halbgruppe H heißt *kommutativ* oder auch *abelsch*, falls gilt: $h_1 * h_2 = h_2 * h_1$ für alle $h_1, h_2 \in H$. In abelschen Halbgruppen bezeichnet man oft die Verknüpfung mit dem Symbol $+$, und man spricht dann statt vom Einselement der Halbgruppe von der *Null* oder dem *Nullelement* der Halbgruppe (Rechenregel: $0 + h = h = h + 0$, für alle $h \in H$). **Warnung:** Die Begriffbildung ist für viele Anfänger sehr verwirrend: Das Element 0 der Halbgruppe $(\mathbb{N}_0, +)$ wird nicht nur "Nullelement" genannt, sondern auch das "Einselement" dieser Halbgruppe. Aber man kann nichts daran ändern: Nach der in (H2) gegebenen Definition hat das Element 0 bezüglich der Addition die Eigenschaften, die von einem Einselement verlangt werden!

Ist $H = (H, \cdot)$ eine Halbgruppe und U eine Untermenge von H, so sagt man, dass U *unter der Multiplikation abgeschlossen* ist, falls gilt: Sind $u_1, u_2 \in U$, so ist auch $u_1 \cdot u_2 \in U$. Eine Untermenge U von H, die unter der Multiplikation abgeschlossen ist und die das Einselement enthält, ist selbst wieder eine Halbgruppe, man nennt U eine *Unterhalbgruppe* von H.

Beispielklassen von Halbgruppen:

Die Potenzmenge als Halbgruppe. Es ist $(\mathcal{P}(M), \cup)$ eine Halbgruppe, jedes Element dieser Halbgruppe ist idempotent, und die leere Menge $\emptyset$ ist Einselement.

Auch $(\mathcal{P}(M), \cap)$ ist eine Halbgruppe, jedes Element dieser Halbgruppe ist idempotent, und die Menge M ist Einselement.

Zahlbereiche, die Halbgruppen sind:

$$\begin{array}{lll} (\mathbb{N}_0, +), & (\mathbb{N}_0, \cdot), & (\mathbb{N}_1, \cdot), \\ (\mathbb{Z}, +), & (\mathbb{Z}, \cdot), & (\mathbb{Z}^*, \cdot), \\ (\mathbb{Q}, +), & (\mathbb{Q}, \cdot), & (\mathbb{Q}^*, \cdot), \\ (\mathbb{R}, +), & (\mathbb{R}, \cdot), & (\mathbb{R}^*, \cdot). \end{array}$$

Ein Element h einer Halbgruppe $(H,\cdot)$ heißt *invertierbar*, wenn es ein $h' \in H$ mit $hh' = h'h = 1_H$ gibt. Existiert ein derartiges Element h', so ist es eindeutig bestimmt und wird das *zu h inverse* Element genannt, und man schreibt h^{-1} statt h'. (Die Eindeutigkeit sieht man so: ist auch $hh'' = h''h = 1_H$, so ist $h' = h' \cdot 1_H = h'(hh'') = (h'h)h'' = 1_H \cdot h'' = h''$.) Sind die Elemente $h_1, h_2 \in H$ invertierbar, so ist auch h_1h_2 invertierbar und es gilt $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1}$. (Beachte die Reihenfolge!)

Gruppen. Eine *Gruppe* $G = (G,*)$ ist eine Halbgruppe, in der zusätzlich gilt:
(G) Zu jedem Element $g \in G$ gibt es ein $g' \in G$ mit $gg' = 1_G$.

Ist G eine Gruppe und gilt $gg' = 1_G$, so gilt auch $g'g = 1_G$, es ist also $g' = g^{-1}$; jedes Element in G ist also invertierbar. (Beweis: Sei $gg' = 1_G$. Zu g' gibt es ebenfalls ein Element $g'' \in G$ mit $g'g'' = 1_G$. Dann ist aber $g = g \cdot 1_G = g(g'g'') = (gg')g'' = 1_G \cdot g'' = g''$. Also gilt $g'g = g'g'' = 1_G$.)

In einer Gruppe G ist das Einselement 1_G das einzige idempotente Element. (In einer Halbgruppe kann es viele idempotente Elemente geben, wie die Halbgruppe $(\mathcal{P}(M),\cup)$ zeigt.)

Untergruppen. Sei $G = (G,*)$ eine Gruppe. Eine nicht-leere Teilmenge U von G heißt *Untergruppe,* falls U unter der Multiplikation und unter der Inversen-Bildung abgeschlossen ist. (Es gelten also die beiden Regeln: Sind $u_1, u_2 \in U$, so ist auch $u_1 * u_2 \in U$. Und: Ist $u \in U$, so auch $u^{-1} \in U$.) (Man beachte, dass daraus unmittelbar folgt, dass das Einselement 1_G zu U gehört: wir setzen ja voraus, dass U nicht leer ist, sei etwa $u \in U$; dann ist auch $u^{-1} \in U$ und demnach $1_G = u*u^{-1} \in U$.) Natürlich ist eine Untergruppe selbst eine Gruppe.

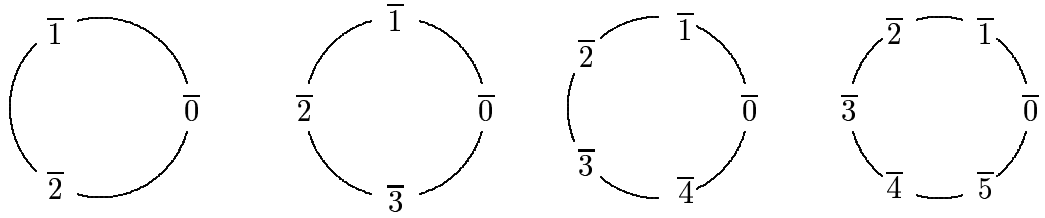
BEISPIELKLASSEN VON GRUPPEN:

Zahlbereiche, die Gruppen sind: $(\mathbb{Z},+), (\mathbb{Q},+), \mathbb{Q}^* = (\mathbb{Q}\setminus\{0\},\cdot)$, usw.

Geometrisch motivierte Gruppen. Sei $n \geq 3$. Sei E_n ein regelmäßiges n-Eck in der Ebene. Sei D_n die Menge aller Symmetrien der Ebene, die das n-Eck auf sich abbilden (also Drehungen und Spiegelungen). Dies ist eine Gruppe (Verknüpfung ist die Hintereinanderschaltung der Abbildungen), man nennt sie die *Symmetriegruppegruppe* von E_n. Insgesamt gibt es n Drehungen (nämlich mit den Drehwinkeln $\frac{i}{n}360$ mit $0 \leq i < n$) und n Spiegelungen. Es gilt also $|D_n| = 2n$. Ist $n \geq 3$, so ist D_n nicht abelsch. In der Gruppe D_n bildet die Menge der Drehungen eine Untergruppe, man nennt dies die *Drehgruppe* des regelmäßigen n-Ecks.

Die zyklischen Gruppen. Sei $n \geq 1$. Sei $n\mathbb{Z}$ die Menge der Vielfachen von n, also die Menge der ganzen Zahlen, die durch n ohne Rest teilbar sind. Für jede ganze Zahl a setze $\overline{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}$. Beachte: *Es gilt $\overline{a_1} = \overline{a_2}$ genau dann, wenn $a_1 - a_2$ durch n teilbar ist.* Ist $0 \leq a < n$, so ist $\overline{a}$ die Menge der ganzen Zahlen, die bei Division durch n den Rest a liefern. (Man nennt dies eine Restklasse modulo n.) Man schreibt $\mathbb{Z}/n\mathbb{Z}$ für die Menge der Restklassen modulo n; zum Beispiel ist $\mathbb{Z}/3\mathbb{Z} = \{\overline{0},\overline{1},\overline{2}\}$ eine Menge mit 3 Elementen. Man definiert auf der Menge $\mathbb{Z}/n\mathbb{Z}$ eine Addition vermöge $\overline{a_1}+\overline{a_2} = \overline{a_1+a_2}$. (Zu zeigen: dies ist "wohl-definiert": gilt $\overline{a_1} = \overline{b_1}$ und $\overline{a_2} = \overline{b_2}$, so ist $\overline{a_1+a_2} = \overline{b_1+b_2}$.) *Mit dieser Addition ist $\mathbb{Z}/n\mathbb{Z}$ eine Gruppe,* die zyklische Gruppe der Ordnung n.

(Für $n \geq 3$ ist dies gerade die Drehgruppe des regulären n-Ecks.) Man nennt diese Gruppen $(\mathbb{Z}/n\mathbb{Z}, +)$ die *endlichen zyklischen Gruppen.* Zusätzlich nennt man $(\mathbb{Z}, +)$ die *unendliche zyklische Gruppe.* Um zu verstehen, warum die endlichen zyklischen Gruppen "zyklisch" heißen, empfiehlt es sich, die Elemente im Kreis anzuorden und die Abbildung $+\overline{1}$ zu betrachten: Hier die Bilder für $n = 3, 4, 5, 6$.



Das entsprechende Bild für die unendliche zyklische Gruppe wäre die (ganzzahlige) Zahlengerade, also ein "Zykel mit unendlichem Radius":

$$\cdots \quad — \; -1 — \; 0 \; — \; 1 \; — \; 2 \; — \quad \cdots$$

(0.2). Ringe.

Definition: Ein *Ring* $R = (R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass die folgenden Eigenschaften erfüllt sind:

(R1) $(R, +)$ ist eine abelsche Gruppe.
(R2) $(R, \cdot)$ ist eine Halbgruppe.
(R3) Sind r, r_1, r_2 Elemente von R, so gilt $r(r_1 + r_2) = rr_1 + rr_2$ und $(r_1 + r_2)r = r_1 r + r_2 r$ (Distributivität).

Das Einselement von $(R, +)$ bezeichnet man mit 0_R oder einfach mit 0 und nennt es die *Null* des Rings. Das Einselement von $(R, \cdot)$ bezeichnet man mit 1_R oder einfach mit 1 und nennt es die *Eins* von R. Ein Element $r \in R$ heißt *invertierbar,* wenn es als Element der Halbgruppe $(R, \cdot)$ invertierbar ist, wenn es also ein $r' \in R$ mit $rr' = 1_R = r'r$ gibt, und man schreibt dann r^{-1} statt r'. Ist $(R, \cdot)$ abelsch, so nennt man R einen *kommutativen* Ring.

Einfach zu zeigen ist: *Ist R ein Ring, und $r \in R$, so ist $0 \cdot r = 0 = r \cdot 0$.* Beweis: Es ist $0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r$, also ist $0 \cdot r$ ein idempotentes Element der Gruppe $(R, +)$. Das einzige idempotente Element einer Gruppe ist aber ihr Einselement.

Ist R ein Ring und gibt es eine natürliche Zahl $n \geq 1$ mit $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$, so nennt man die kleinste derartige Zahl n die *Charakteristik* des Rings R, und man schreibt $\operatorname{char} R = n$. Gibt es keine solche Zahl n, so schreibt man $\operatorname{char} R = 0$.

Ist $R = (R, +, \cdot)$ ein Ring und U eine Teilmenge von R, so nennt man U einen *Unterring* von R, falls U sowohl unter $+$ als auch unter $\cdot$ abgeschlossen ist, U bezüglich $+$ eine Gruppe ist und 1_R in U enthalten ist. (Man sieht, dass dann U bezüglich $+$ und $\cdot$ selbst wieder ein Ring ist.)

Beispielklassen von Ringen.

A) Die Zahlbereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind kommutative Ringe. Es ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, und $\mathbb{Q}$ ist ein Unterring von $\mathbb{R}$. (Natürlich ist auch $\mathbb{Z}$ ein Unterring von $\mathbb{R}$.)

B) Sei $n \geq 1$. Auf der abelschen Gruppe $\mathbb{Z}/n\mathbb{Z}$ definiert man eine Multiplikation durch $\overline{a_1} \cdot \overline{a_2} = \overline{a_1 a_2}$. (Wieder ist zu zeigen, dass dies wohl-definiert ist.) Auf diese Weise wird $\mathbb{Z}/n\mathbb{Z}$ zu einem kommutativen Ring. Beachte: Im Ring $\mathbb{Z}/n\mathbb{Z}$ gilt:

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0,$$

$\mathbb{Z}/n\mathbb{Z}$ ist ein Ring der Charakteristik n.

(0.3) Körper.

Ein *Körper* $K = (K, +, \cdot)$ ist ein Ring, in dem die Menge $K^* = K \setminus \{0\}$ unter der Multiplikation abgeschlossen ist und $(K^*, \cdot)$ eine abelsche Gruppe bildet.

BEISPIELE.

A) Die Zahlbereiche $\mathbb{Q}$, $\mathbb{R}$ sind Körper, dagegen ist $\mathbb{Z}$ **kein** Körper.

B) Der Ring $\mathbb{Z}/2\mathbb{Z}$ ist ein Körper, dagegen ist $\mathbb{Z}/4\mathbb{Z}$ **kein** Körper.