Vorlesung Lineare Algebra I

WiSe'19/'20 hhu
K. Halupczok

§2: Algebraische Grundbegriffe

L7: Gruppen, Ringe, Körper

Stichworte: Halbgruppe, Gruppe, Ring, Körper, Restklassenring $\mathbb{Z}/M$, $\mathbb{Z}/M$ Körper $\Leftrightarrow$ M Primzahl, endliche Körper $\mathbb{F}_p$

7.1. **Def.:** Sei $H \neq \emptyset$ eine Menge. Eine Abb. $H \times H \to H$ heißt Verknüpfung auf H.

7.2. **Bsp.:** $H = \mathbb{Z}$, dann sind $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a,b) \mapsto a+b$, $(a,b) \mapsto a \cdot b$, $(a,b) \mapsto a-b$ Verknüpfungen auf H.
Verknüpfungen werden oft mit $*, \cdot, +$ oder "nichts" bezeichnet, also mit $a*b$, $a \cdot b$, $a+b$, ab

7.3. **Def.:** • Eine Verknüpfung $*$ auf H mit $\forall a,b,c \in H: a*(b*c) = (a*b)*c$ heißt assoziativ. Dann nennt man das Paar $(H,*)$ eine Halbgruppe.
• Ein Element $e \in H$ heißt neutrales Element der Verknüpfung $*$ auf H, wenn für alle $x \in H$ gilt: $e*x = x = x*e$. (Ist eindeutig: $e = e*f = f$)

7.4 **Bsp.:** • $(\mathbb{Z},+)$ und $(\mathbb{Z},\cdot)$ sind Halbgruppen, nicht aber $(\mathbb{Z},-)$, da "$-$" nicht assoziativ ist: $(1-1)-1 = -1$, $1-(1-1) = 1-0 = 1$.
• 0 ist neutr. El. von $(\mathbb{Z},+)$, 1 ist neutr. El. von $(\mathbb{Z},\cdot)$.
• $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{N}_0,+)$ sind Halbgruppen mit neutr. El. 0.
• Für eine Menge $X \neq \emptyset$ ist $H = \{f: X \to X \text{ Abb.}\}$ Halbgruppe bezüglich Komposition "$\circ$", die identische Abb. id_X ist das neutrale Element.

7.5. **Def.:** • Eine Halbgruppe mit neutralem Element heißt Monoid oder Halbgruppe mit Eins.
• Eine Halbgruppe $(H,*)$ heißt kommutativ oder abelsch, falls $\forall x,y \in H: x*y = y*x$.
(!) Ist $\#X \geq 2$, dann ist $\{f: X \to X\}$ mit $\circ$ als Verknüpfung nicht abelsch.
• Eine Halbgruppe $(H,*)$ heißt kürzbar, wenn aus $a*x = a*y$ oder $x*a = y*a$ stets $x = y$ folgt. ("wenn man kürzen kann")

7.6. **Bsp.:** • Addition $+$ liefert auf $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ kürzbare Halbgruppen
• Die Halbgruppe $\mathbb{N}_0$ bzgl. $x*y := \max\{x,y\}$ hat 0 als neutr. El., ist nicht kürzbar

7.8. **Def.:** Eine Halbgruppe $(H,*)$ mit neutralem Element e heißt **Gruppe**, wenn gilt: $\forall x \in H \; \exists y \in H: x*y = e = y*x$, d.h. wenn zu jedem x stets ein y mit $x*y = e = y*x$ ex.

7.9. **Bsp.:** 1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ sind Gruppen (mit neutr. El. 0)
2. $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$ sind keine Gruppen, da $0 \cdot y = 1$ keine Lösung hat.

7.10. **Lemma:** Sei $(G,*)$ eine Gruppe mit neutr. El. e. Dann gilt:
(i) G ist kürzbar
(ii) Zu jedem $x \in G$ ex. genau ein $y \in G$ mit $x*y = e = y*x$.

Bew.: Zu (i): Angenommen, es gilt $a*x = a*y$. Sei b laut Def. "Gruppe" so, dass $a*b = e = b*a$. Dann gilt $b*a*x = b*a*y \Rightarrow e*x = e*y \Rightarrow x = y$. Genauso folgt aus $x*a = y*a$, dass $x = y$ gilt. Dies zeigt (i).
Zu (ii): Dies ist direkte Konsequenz aus (i): aus $x*y = e = x*z$ folgt mit Kürzen sofort $y = z$, ebenso andersherum aus $y*x = e = z*x$. □

7.11. **Def.:** Das nach Lemma 7.10 eindeutig bestimmte **Inverse** zu x wird auch mit x^{-1} bezeichnet, wenn $*$ oder $\cdot$ oder $\circ$ für die Verknüpfung geschrieben wird ("multiplikativ geschriebene Gruppe"). Es wird mit $-x$ bezeichnet wenn diese mit $+$ geschrieben wird ("additiv geschriebene Gruppe").

7.12. **Bem.:** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ sind abelsche Gruppen.
Mit $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ sind auch $(\mathbb{Q}^*,\cdot)$ und $(\mathbb{R}^*,\cdot)$ abelsche Gruppen. Das zu $x \neq 0$ inverse El. (eines $x \in \mathbb{Q}$ bzw. $x \in \mathbb{R}$) schreibt man außer x^{-1} auch als $\frac{1}{x}$ und erhält das übliche Bruchrechnen, wenn man $\frac{z}{x} := z \cdot \frac{1}{x}$ erklärt.

7.13. **Def.:** Sei $R \neq \emptyset$ eine Menge mit zwei Verknüpfungen $+$ und $\cdot$. Dann heißt $(R,+,\cdot)$ ein **Ring**, falls gilt: (i) $(R,+)$ ist Gruppe mit einem neutr. El. $0 \in R$, (ii) $(R,\cdot)$ ist Halbgruppe mit einem neutr. El. $1 \in R$, (iii) es gelten die **Distributivgesetze** $a \cdot (x+y) = a \cdot x + a \cdot y$, $(x+y) \cdot a = x \cdot a + y \cdot a$.

7.14. **Konvention:** "Punkt vor Strich", d.h. lasse Klammern weg (und Punkt auch, Multiplizieren bindet stärker), also $a(x+y) = ax+ay$, $(x+y)a = xa+ya$.

7.15. **Bsp.:** $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{Z},+,\cdot)$ sind Ringe, aber nicht $(\mathbb{N}_0,+,\cdot)$.

7.16. **Satz (Rechenregeln in Ringen):** Sei $(R,+,\cdot)$ ein Ring mit neutr. El. 0 bzw. 1. Für $x\in R$ sei $-x\in R$ das Inverse von x bzgl. $+$, d.h. $x+(-x) = 0 = (-x)+x$.

Dann: (i) $\forall x,y\in R: x+y = y+x$, d.h. die Addition im Ring ist stets kommutativ,
(ii) $\forall x\in R: 0x = 0 = 0x$, (iii) $\forall x\in R: -(-x) = x$,
(iv) $\forall x,y\in R: -(xy) = (-x)y = x(-y)$, insb. $(-1)x = -x$ und $(-x)(-y) = xy$.

"Minus mal Minus gibt Plus"

Bew.:

(i): $(1+x)(1+y) = 1(1+y)+x(1+y) = 1+y+x+xy$
$= (1+x)1+(1+x)y = 1+x+y+xy$
$\overset{\text{kürzen}}{\Rightarrow} y+x = x+y$,

(ii): $0x = (0+0)x = 0x+0x \overset{\text{kürzen}}{\Rightarrow} 0 = 0x$, genauso $0 = x0$

(iii): $-x+(-(-x)) = 0$, $-x+x = 0$ $\Big\}\overset{\text{kürzen}}{\Rightarrow} x = -(-x)$

(iv): $xy+(-x)y = (x+(-x))y = 0y \overset{(ii)}{=} 0$, $xy+(-xy) = 0$ $\Big\}\overset{\text{kürzen}}{\Rightarrow} (-x)y = -xy$. □

7.17. **Def.:** Ein Ring heißt kommutativ, wenn die Multiplikation $\cdot$ kommutativ ist.

7.18. **Bem.:** Extremes Bsp. für einen Ring: der Nullring $R = \{0\}$ mit $0\cdot 0 = 0+0 = 0$. In diesem Ring gilt $0 = 1$. Soll dieser Ring ausgeschlossen werden, kann man explizit verlangen, dass $0\neq 1$ gelten soll.

Einheiten und Körper

7.19. **Def.:** Sei $(R,+,\cdot)$ ein Ring. Dann heißt ein Element $u\in R$ eine Einheit, wenn es ein $v\in R$ gibt mit $uv = 1 = vu$. Die Menge aller Einheiten von R sei R^*, d.h. $R^* := \{u\in R;\ \exists\, v\in R: uv = 1 = vu\}$.

7.20 **Lemma und Def.:** $(R^*,\cdot)$ ist eine Gruppe und wird Einheitengruppe von R genannt.

Bew.: Ist $u,w\in R^*$, d.h. ex. $v,z\in R$ mit $uv = vu = 1 = wz = zw$, so folgt $(uw)(zv) = uv = 1 = zw = (zv)(uw)$, also $uw\in R^*$. Auch $v\in R^*$, $1\in R^*$. □

7.21. **Bsp.:** $\mathbb{R}^* = \{x \in \mathbb{R};\ x \neq 0\} = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{Z}^* = \{\pm 1\}$

7.22. **Def.:** Ein kommutativer Ring $(K, +, \cdot)$ mit $1 \neq 0$ heißt **Körper**, wenn $K^* = K \setminus \{0\}$ gilt, d.h. wenn jedes Element $x \in K \setminus \{0\}$ eine Einheit ist, d.h. wenn jedes Element $x \in K \setminus \{0\}$ invertierbar ist.

7.23. **Lemma:** Sei $(K, +, \cdot)$ ein Körper. Dann: $\forall x, y \in K: x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$.

Bew.: Es sei $x \cdot y = 0$. 1. Fall: $x = 0$ ✓, 2. Fall: $x \neq 0$, dann: $x \cdot y = 0 \overset{7.16(ii)}{=} x \cdot 0 \overset{\text{mal } x^{-1}}{\Rightarrow} y = 0$. □

7.24. **Bsp.:** $\mathbb{R}$, $\mathbb{Q}$ sind Körper, $\mathbb{Z}$ ist kein Körper, $\mathbb{F}_2 = \{0, 1\}$ mit $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ $\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$ ist Körper mit 2 Elementen (nachrechnen...).

Restklassenringe

Hier knüpfen wir an an die Idee aus 5.17.6., wo $\mathbb{N}_0 / \sim = \{\text{g}, \text{u}\}$ war. Statt mit "gerade/ungerade" wollen wir mit den Resten "rechnen", die wir bei Division ganzer Zahlen durch $M = 12$ erhalten:

7.25. Betr. $X = \mathbb{Z}$ und definiere

$n \sim m :\Leftrightarrow n$ und m lassen denselben Rest bei Division durch 12

$\Leftrightarrow$ 12 teilt $m - n$

$\Leftrightarrow \exists\, k \in \mathbb{Z} : m = n + 12k$

Für $n \in \mathbb{Z}$ ist $[n] = \{m \in \mathbb{Z};\ 12 \text{ teilt } m - n\}$.

7.26. Dann ist also
$[0] = [12] = [24] = \ldots = \{\ldots, -12, 0, 12, 24, \ldots\}$ (alle mit Rest 0)
$[1] = [13] = [25] = \ldots = \{\ldots, -11, 1, 13, 25 \ldots\}$ (alle mit Rest 1)
$\vdots$
$[11] = [23] = [47] = \ldots = \{\ldots, -1, 11, 23, \ldots\}$ (alle mit Rest 11)

$\rightsquigarrow$ identifiziere die $\sim$-Klassen mit den 12 möglichen Resten 0, 1, ..., 10, 11.

Haben: $\{0, 1, \ldots, 11\}$ ist vollst. Repr.system, aber auch z.B. $\{12, 1, \ldots, 9, 10, 23\}$, ...

7.27. Somit: $\mathbb{Z}/\sim = \{[0], [1], \ldots, [11]\} = \{[12], [1], \ldots, [10], [23]\}, \ldots$

diese Darstellung der $\sim$-Klassen gefällt uns am besten.

Leichter zu schreiben ist $\{\bar{0}, \bar{1}, \ldots, \bar{11}\}$, eine andere gebräuchliche Notation.

"Rechnen" mit Resten (d.h. mit $\tilde{A}$-Klassen, den El. von $\mathbb{Z}/\sim$):

7.28. erklären wir repräsentantenweise: $[k]+[l] := [k+l]$, d.h. $\bar{k}+\bar{l} := \overline{k+l}$,
$[k]\cdot[l] := [k\cdot l]$, d.h. $\bar{k}\cdot\bar{l} := \overline{k\cdot l}$,

zunächst $k,l \in \{0,\dots,11\}$

für $k,l \in \mathbb{Z}$ (!). Wir haben hier die Def. von "+", "·" auf $\mathbb{Z}/\sim$ von k,l abhängig gemacht, obwohl wir doch nur $[k]$, $[l]$ miteinander verknüpfen wollten; prinzipiell könnte je nach Repräsentantenwahl ein anderes Ergebnis nach der Verknüpfung herauskommen. Tut es hier aber nicht! Denn:
Es ist egal, welche Repräsentanten wir wählen für $[k]$, $[l]$,
sagen wir mal $[k]=[n]$ und $[l]=[\nu]$,
dann ist nämlich $[k+l]=[n+\nu]$.

- $k\sim n \iff \exists\, r\in\mathbb{Z}: k-n = 12r$
- $l\sim \nu \iff \exists\, s\in\mathbb{Z}: l-\nu = 12s$

Somit: $k+l \sim n+\nu$, denn $k+l-(n+\nu) = (k-n)+(l-\nu) = 12(r+s)$.

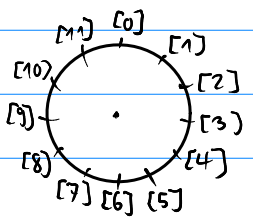
Eine ähnliche Überlegung zeigt $[k\cdot l]=[n\cdot \nu]$. (Ü)

Man sagt, aufgrund dieser Rechnung ist die gegebene Def. von $+,\cdot$ auf den $\tilde{A}$-Klassen in $\mathbb{N}_0/\sim$ repräsentantenunabhängig und deswegen wohldefiniert.

auch: "mod 12"

7.29. In diesem Beispiel sprechen wir vom Rechnen/der Arithmetik modulo 12.
(Die Zahl $M=12$ könnte auch durch einen anderen Modul M ersetzt werden.)
Anschaulich ist die Arithmetik mod 12 das Rechnen mit Stunden auf einer Uhr:

sieht aus wie ein "Ring"



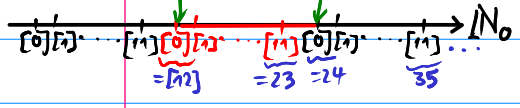
$[2]+[6]=[8]$
$[9]+[4]=[13]=[1]$
$[11]+[11]=[22]=[10]$, ...
$[13]+(-[5])=[8]$, ... usw.

$2\cdot[6]=[2]\cdot[6]=[0]$
$[9]\cdot[5]=[45]$
$=[-3]$
$=[9]$

↳ erkläre $-[5]$ als die Klasse mit $(-[5])+[5]=0$, d.h. $-[5]=[7]$

$[13]+[7]=[20]=[8]$ ...

oder: verklebe Intervall an (zu identifizierenden) Randpunkten zu Kreis



7.30. Diese Verknüpfungen $+, \cdot$ auf $\mathbb{Z}/\sim$ haben viele neue interessante Eigenschaften, abhängig vom gewählten Modul M, hier $M=12$. Für einen beliebigen Modul $M \in \mathbb{N}$, $M \neq 0$, $M \neq 1$, kann ein dazu passendes $\mathbb{Z}/\sim$ konstruiert werden, das wir dann mit $\mathbb{Z}/M$ bezeichnen (manchmal auch als $\mathbb{Z}/M\mathbb{Z}$). Sauber so:

7.31. **Satz und Def.:**

Für $M \in \mathbb{N}$, $M > 1$, ist eine Äq.-Rel. $\sim$ auf $\mathbb{Z}$ definiert durch $x \sim y :\Leftrightarrow \exists k \in \mathbb{Z} : x = y + kM$. Werden die Äq.-klassen mit $\bar{0}, \bar{1}, \ldots, \overline{M-1}$ bezeichnet, so sei $\mathbb{Z}/M := \mathbb{Z}/\sim := \{\bar{0}, \bar{1}, \ldots, \overline{M-1}\}$. Durch $\bar{x} + \bar{y} := \overline{x+y}$ und $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$ sind wohldefinierte (d.h. repräsentantenunabhängige) Verknüpfungen auf $\mathbb{Z}/M$ erklärt. Damit ist $(\mathbb{Z}/M, +, \cdot)$ ein kommutativer Ring, der Restklassenring mod M (auch: Restklassenring modulo M). Die neutralen Elemente sind $\bar{0}$ bzgl. $+$ und $\bar{1}$ bzgl. $\cdot$.

7.32. • Die Äq.-Rel. in Satz 7.29 nennt man auch Kongruenzrelation. Für $x \sim y$ sagt man auch "x kongruent y mod M"
oder "x ist kongruent zu y modulo M"
oder "x lässt bei Division durch M den gleichen Rest wie y"
und schreibt für $x \sim y$ auch $x \equiv y \bmod M$ oder $x \equiv y \ (M)$
oder $x \equiv y \ (\mathrm{mod}\ M)$.
Die Äq.-klassen heißen auch Restklassen modulo M.

7.33. Beachte: Für $M=1$ würde man den uninteressanten Nullring $\mathbb{Z}/1 = \{\bar{0}\}$ erhalten.

7.34. Def: Eine natürliche Zahl $n \in \mathbb{N}$ heißt Primzahl, wenn sie genau zwei natürliche Teiler hat, d.h. $\#\{t \in \mathbb{N};\ \exists k \in \mathbb{N} : tk = n\} = 2$.

7.35. Bem.: 1 ist keine Primzahl, die kleinste PZ ist 2, dann 3, 5, 7, 11, 13, ...
Primzahlen sind die wichtigsten Bausteine des Zahlensystems, denn jede natürliche Zahl ist (bis auf Reihenfolge) eindeutig schreibbar als Produkt von Primzahlen (in dem Faktoren mehrfach auftauchen dürfen).

→ vgl. Zahlentheorie

7.36. **Satz:** Sei $M \in \mathbb{N}$, $M > 1$. Der Restklassenring $\mathbb{Z}/M$ ist genau dann ein Körper, wenn M eine Primzahl ist.

Bew.: „$\Rightarrow$": Sei $\mathbb{Z}/M$ ein Körper und $t \neq 1$ ein Teiler von M, etwa $s \cdot t = M$, $s \neq M$. Dann ist $\bar{s} \cdot \bar{t} = \overline{s \cdot t} = \bar{M} = \bar{0} \overset{7.23}{\Rightarrow} \bar{s} = \bar{0} \vee \bar{t} = \bar{0}$, also ist s oder t ein Vielfaches von M. Da dies für s nicht zutrifft, ist t ein Vielfaches von M. Da t aber gleichzeitig Teiler von M ist, folgt $t = M$ und $s = 1$. Also ist M PZ.

„$\Leftarrow$": Sei M Primzahl und $\bar{t} \in \mathbb{Z}/M$, $\bar{t} \neq \bar{0}$. Dann haben wir

⊛ $(\mathbb{Z}/M) \setminus \{\bar{0}\} = \{\bar{t} \cdot \bar{1}, \bar{t} \cdot \bar{2}, \dots, \bar{t} \cdot \overline{M-1}\}$. [Denn wäre „$\supseteq$" anstelle „$=$" hier richtig, so gäbe es $i, j \in \{1, 2, \dots, M-1\}$ mit $i \neq j$ und $\bar{t} \cdot \bar{i} = \bar{t} \cdot \bar{j}$. Daraus folgt

pPZ. Dann: $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$ (Lemma von Euklid → Zahlentheorie)

$\bar{t}\bar{i} = \bar{t}\bar{j} \Rightarrow ti \equiv tj \ (M) \Rightarrow M \mid (ti - tj) = t(i-j)$.

Da M Primzahl ist und $M \mid t(i-j)$ gilt, wo $M \nmid t$, folgt $M \mid (i-j)$ nach dem Lemma von Euklid. Dann: $\bar{i} = \bar{j}$ im $\lightning$ zu $i \neq j$, $i, j \in \{1, \dots, M-1\}$.]

Aus Beh. ⊛ und aus $\bar{1} \in (\mathbb{Z}/M) \setminus \{\bar{0}\}$ folgt nun, dass $\exists\ \bar{s} \in \mathbb{Z}/M : \bar{1} = \bar{t} \cdot \bar{s}$. Also ist (jedes) $\bar{t} \neq \bar{0}$ invertierbar.

Es folgt $(\mathbb{Z}/M) \setminus \{\bar{0}\} = (\mathbb{Z}/M)^*$, also ist $(\mathbb{Z}/M, +, \cdot)$ ein Körper. □

7.37. **Def.:** Für eine Primzahl $p \in \mathbb{N}$ bezeichnet man den Körper $\mathbb{Z}/p$ mit $\mathbb{F}_p$.

7.38. **Bem.:** $\mathbb{F}_p$ ist ein endlicher Körper und hat p (viele) Elemente.

Gibt es einen Körper mit M Elementen, so gibt es im wesentlichen (bis auf Isomorphie) genau einen solchen. Genau zu den $M \in \mathbb{N}$, die Potenz $M = p^e$ einer Primzahl sind, gibt es einen Körper mit M (vielen) Elementen. Konstruktion: s. „Algebra"

(4) Konstruieren Sie den Körper $\mathbb{F}_4$ mit 4 Elementen $\{0, 1, a, b\}$.