Cheat Sheet Algebra

Grundstrukturen

n-stellige Verknüpfung Sind $A_1, \dots, A_n, B$ Mengen, dann nennt man eine Abbildung $\circ : A_1 \times \dots \times A_n \to B$ eine n-stellige Verknüpfung auf B. $\circ A^n \to A$ nennt man eine n-stellige Verknüpfung auf A.

Einfache algebraische Strukur bezeichnet ein Paar $S = (A, (f_i)_{i \in I})$. Dabei heisst die Menge A Grundmenge von S. $(f_i)_{i \in I}$ ist eine endliche Familie von Verknüpfungen auf diese Grundmenge.

Zusammengesetze algebraische Struktur bezeichnete die verallgemeinerte einfache algebraische Struktur. Sie ist ein Tupel $S = (A_1, \dots, A_n, (f_i)_{i \in I})$. Sie besteht aus endlich vielen Grundmengen $(A_1, \dots, A_n)$ und einer endlichen Familie von von Vernupfungen, so dass es für alle $i \in I$ natürliche Zahlen p, m und Grundmengen A_r, A_s, A_k gibt mit:

$$f_i : A_r^p \times A_s^m \to A_k$$

Signatur von S $(f_i)_{i \in I}$ heisst Signatur von S.

Für zweiwertige (binäre) Verknüpfunge $\circ$ werden folgende Begriffe verwendet:
Assoziativitat: wenn $\forall a, b, c \in A(A \circ (b \circ c) = (a \circ b) \circ c)$
Kommutativität: wenn $\forall a, b \in A(A \circ b = b \circ a)$

Neutralität

Ein Element $e_i \in A$ ist:
linksneutral bezüglich $\circ$ falls $\forall a \in A(e_i \circ a = a)$
linksneutral bezüglich $\circ$ falls $\forall a \in A(a \circ e_1 = a)$
neutral bezüglich $\circ$ falls $\forall a \in A(e_i \circ a = a \circ e_i = a)$
Wenn es ein neutrales Element gibt, kann es kein zweites neutrales Element geben.

Halbgruppen, Gruppen und Monoide

Eine Struktur $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ : G \times G \to G$ heisst:

Halbgruppe	wenn die Verknüpfung assoziativ ist
Monoid	wenn zusätzlich ein neutrales Element $e \in G$ existiert
Gruppe	wenn zusätzlich ein für jedes $g \in G$ ein inverses Element g^{-1}existiert
Kommutative Gruppe	wenn die Gruppe zusätzlich kommutativ ist.

Für inverse Elemente gilt: $(a^{-1})^{-1} = a$. (Das inverse vom inversen ist das element selbst)

- In Halbgruppen kann gekürzt werden $(a \cdot x = b \cdot x \Rightarrow a = b)$

Beispiele für Halbgruppen, Gruppen und kommutative Gruppen

Halbgruppen	$(\mathbb{N}, +), (\mathbb{Z}, -)$
Monoid	$(\mathbb{N} \cup 0, +)$
Gruppe	$(\mathbb{Q}, *)$
Kommutative Gruppe	$(\mathbb{Z}, +)$

Unterstrukturen

Sei $(A, \circ)$ eine Struktur und $U \subset A$. U heisst abgeschlossen falls gilt:

$$\forall a, b \in U(a \circ b \in U)$$

Je nach übergeordneter Struktur handelt es sich um Unterhalbgruppen, Untermonoide oder Untergruppen.

Regeln

- Ist $(G, \circ)$ eine Halbgruppe und seien $(U_i)_{i \in I}$ Unter..., dann ist $\bigcap_{i \in I} U_i$ ebenfalls eine Unter....

Jede (Halb-) Gruppe besitzt eine kleinste Unter(halb)gruppe und jeder Monoid besitzt einen kleinsten Untermonoid, die eine gegebene Teilmenge der (Halb-) Gruppe bzw. des Monoids enthalten.

Morphismen

Homomorphismus

Ein (Halb-) Gruppenhomomorphismus ist die Abbildung $f : G \to G'$ einer Struktur $(G, \circ)$ in eine andere Struktur $(G', \sim)$, so dass für alle $a, b \in G$ gilt:

$$f(a \circ b) = f(a) \sim f(b)$$

Beim Monoidhomomorphismus wird zusätzliche das neutrale Element von $(G, \circ)$ auf das neutrale Element von $(G', \;)$ abgebildet.

Monomorphismus bezeichnet injektive (d. h. jedes $a \in G$ wird auf ein anderes $b \in G'$ abgebildet) Homomorphismen.

Epimorphismus bezeichnet surjektive (d. h. durch die Abbildung wird jedes $b \in G'$ erreicht) Homomorphismen

Isomorphismus bezeichnet Homomorphismen die sowohl injektiv als auch bijektiv sind.

Nicht jeder Homomorphismus zwischen zwei Monoiden ist zwingend ein Monoidhomomorphismus. Beispiel:

$$f : (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$$
$$f(0) = 0$$
$$f(0 + 0) = f(0) \cdot f(0) = 0$$

Aber das neutrale Element der Addition (1) wird nicht auf das neutralen Element der Multiplikation abgebildet.

Regeln

1. Sind $f : (G, \cdot) \to (G', \circ)$ und $h : (G', \sim) \to (G'', \bullet)$ Homomorphismen, dann ist auch $h \circ f : (G, \cdot) \to (G'', \bullet)$ ein entsprechender Homomorphismus.
2. Ist $f : (G, \sim) \to (G', \circ)$ ein Homomorphismus, dann ist das Bild $Im(f) \subset G'$ eine entsprechende Unterstruktur von $(G', \circ)$.
3. Es sei $f : G \to G'$ ein Gruppenhomomorphismus zwischen den Gruppen $(G, \sim)$ und $(G', \circ)$ mit den neutralen Elementen e und e', dann gelten:
   - $f(e) = e'$
   - $\forall a \in G(f(a^{-1}) = f(a)^{-1})$
4. Ist $f : (G, \sim) \to (G', \circ)$ ein Gruppenhomomorphismus, dann der Kern $ker(f) = \{a \in G | f(a) = e'\}$
5. Ist $f : (G, \circ) \to (G', \sim)$ ein Gruppenhomomorphismus mit $ker(f) = \{e\}$, dann ist f injektiv.
6. Ist $f : (G, \sim) \to (G', \circ)$ ein Isomorphismus, dann ist auch $f^{-1} : (G', \circ) \to (G, \sim)$ ein Isomorphismus.

Bild (Im) Menge die durch eine Funktion erzeugt wird.

Kern Alle $g_n \in G$ die auf $e \in G'$ abgebildet werden. Wobei e das neutrale Element von G' ist.

Ringe und Körper

Eine Struktur $(G, \sim, \circ)$ heisst Ring, wenn folgende Bedingungen erfüllt sind:

1. $(G, \sim)$ ist eine kommutative Gruppe
2. $(G, \circ)$ ist eine Halbgruppe
3. Es gilt das Distributivgesetz, d. h. für alle Elemente a, b, c des Ringes gelten:
   - $a \circ (b \sim c) = (a \circ b) \sim (a \circ c)$
   - $(a \sim b) \circ c = (a \circ c) \sim (b \circ c)$

Konventionen

- Wenn $(R, \sim, \circ)$ ein Ring ist, dann bezeichnen wir das neutrale Element von $(G, \sim)$ mit 0
- Falls vorhanden bezeichnen wir das neutrale Element von $(G, \circ)$ mit 1.
- Das inverse Element von $g \in G$ bezüglich $\sim$ bezeichnen wir mit $-g$.
- Das inverse Element von $g \in G$ bezüglich $\circ$ bezeichnen wir mit g^{-1}.

Typische Ringe

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z}, +, \cdot)$. Sowie der Nullring $(\{0\}, +, \cdot)$

Potenz

Sei $(G, +, \cdot)$ ein Ring mit 1, dann ist die n-te Potenz von $g \in G$ definiert als:

$$r^0 := 1$$
$$r^{n+1} := r \cdot r^n$$

Rechenregeln in Ringen

Sei $G, +, \cdot)$ ein Ring. Für alle Elemente $a, b \in R$ und alle Zahlen $n, k \in \mathbb{N}$ gelten folgende Identitäten:

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a) = (-1) \cdot a$
3. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$
4. $(-a) \cdot (-b) = a \cdot b$
5. $0 = 1 \Rightarrow G = \{0\}$
6. $a^n \cdot a^k = a^{n+k}$
7. $a^{n \cdot k} = (r^n)^k$

Begriffe

rechter Nullteiler	falls ein $a \in G \setminus \{0\}$ existiert, so dass $a \cdot b = 0$
linker Nullteiler	falls ein $a \in G \setminus \{0\}$ existiert, so dass $b \cdot a = 0$
Nullteiler	ist sowohl rechter, wie auch linker Nullteiler
Integritätsring	Die Verknüpfung $\circ$ ist kommutativ und $0 \in G$ ist der einzige Nullteiler.
Körper	falls $(G \setminus \{0\}, \circ)$ eine kommutative Gruppe ist.

In einem Integritätsring gilt stets: $1 \neq 0$.
Ein kommuativer Ring $(G, \sim, \circ)$ mit $G \neq \{0\}$, ist genau dann ein Integritätsring, wenn für jedes $g \in G \setminus \{0\}$ die Abbildung $f_g : (G, \sim) \to (G, \sim)$ mit $f_g(x) := g \cdot x$ ein injektiver Gruppenhomomorphismus ist.
Ein Integritätsring $(R, \sim, \circ)$ ist genau dann ein Körper, wenn alle Funktionen $f_g : G \to G$ mit $f_g(x) = r \cdot x$ mit $r \in G \setminus \{0\}$ surjektiv sind.

Folgerungen

1. Jeder endliche Integritätsring ist ein Körper.
2. Für $p \in \mathbb{N} gilt : (\mathbb{Z}_{/p}, +, \cdot)$ ist ein Körper $\Leftrightarrow p$ ist eine Primzahl.

Ringhomomorphismus

Es seien die Ringe $(R, +, \cdot)$ und $(R', +', \cdot')$ gegeben. Ein Ringhomomorphismus $f : (R, +, \cdot) \to (R', +', \cdot')$ ist eine Abbildung $f : R \to R'$, die:

1. Ein Gruppenhomomorphismus $f : (R, +) \to (R', +')$ und
2. ein Halbgruppenhomomorphismus $f : (R, \cdot) \to (R', \cdot')$ ist.
3. Sind $(R, \cdot)$ und $(R', \cdot')$ Monoide, muss f ein Monoidhomomorphismus sein.

Vektorräume

Es sei K ein Körper, seine Elemente heissen *Skalare*. Sie sind mit k bezeichnet.

K-Vektorraum (K-VR) ist ein Tripel $(V, +, \cdot)$ mit:

1. $(V, +)$ ist eine kommutative Gruppe (s. o.)
2. Es ist $\cdot : K \times V \to V$ und für alle Elemente $k_1, k_2 \in K$ und $v_1, v_2 \in V$ gelten:
   a) $k_1 \cdot (k_2 \cdot v_1) = k_1 \cdot k_2 \cdot v_1$
   b) $k_1 \cdot (v_1 + v_2) = k_1 \cdot v_1 + k_1 \cdot v_2$
   c) $(k_1 + k_2) \cdot v_1 = k_1 \cdot v_1 + k_2 \cdot v_1$
   d) Für die 1 von K gilt: $1 \cdot v_1 = v_1$

Elemente von V werden mit v bezeichnet.

$\Rightarrow$ K selbst mit seiner Addition und Multiplikation ist ein K-VR
$\Rightarrow$ Der Körper $\mathbb{C}$ ist ein 2-dimensionaler VR über $\mathbb{R}$
$\Rightarrow$ Der Körper $\mathbb{R}$ ist ein ∞-dimensionaler VR über $\mathbb{Q}$
$\Rightarrow$ Die Menge $\mathbb{R} \times \mathbb{R}$ ist ein 2-dimensionaler $\mathbb{R}$-VR.

Rechenregeln

$0_K \cdot v = 0_V = k \cdot 0_V$
$-k \cdot v = -(k \cdot v) = k \cdot (-v)$
$k \cdot v \Rightarrow (k = 0_K) \vee (v = 0_v)$

Untervektorraum

Ist V ein K-VR und $U \subset V$ $(U \neq \emptyset)$ abgeschlossen unter den Verknüpfungen $\cdot, +$, dann ist U ein Untervektorraum von V und somit auch ein K-VR.
Jede Gerade in $\mathbb{R}^2$ durch den Nullpunkt ist ein solcher 1-dimensionaler Untervektorraum.

Erzeugender Untervektorraum

$$\langle U \rangle := \left\{ \sum_{i=1}^{n} k_i \cdot v_i | (n \in \mathbb{N}) \wedge (k_1, \ldots, k_n \in K) \wedge (v_1, \ldots v_n \in V) \right\}$$

Beispiele:

- $\langle \emptyset \rangle = \{(0, 0, 0)\}$
- $\langle \{(1, 0), (0, 1)\} \rangle = \mathbb{R}^2$

Erzeugendensystem bezeichnet eine Menge U, wenn gilt $\langle U \rangle = V$ mit $U \subset V$

Lineare unabhängig (frei) ist eine Menge U wenn für alle paarweise verschiedenen Vektoren $v_1, \ldots, v_n \in U$ und für alle Skalare $k_1, \ldots k_n \in K$ stet gilt:

$$\sum_{i=0}^{n} k_i \cdot v_i \neq 0 \text{ oder } r_1, \ldots, r_n = 0$$

Basis bezeichnet ein linear unabhängiges (freies) Erzeugendensystem (geschrieben als B).

Lässt sich ein Vektor eines Untervektorraums aus anderen Vektoren desselben Untervektorraums erzeugen, dann ist der Untervektorraum nicht frei.

$$(v = \sum_{i=1}^{n} k_i \cdot v_i) \wedge (v, v_1, \ldots, v_n \in U) \wedge (k_1, \ldots, k_n \in K) \Leftrightarrow U \text{ ist nicht frei}$$

Jeder Vektor v aus V lässt sich aus jeder beliebigen Basis erzeugen:

$$v = \sum_{i=1}^{n} k_i \cdot b_i \Leftrightarrow B = \{b_1, \ldots, b_n\} \text{ist eine Basis von } V$$

Sätze, Axiome, Theoreme

- Ist A eine Menge und „$\leq$“ eine Halbordnung auf A, so dass für jede total geordnete Teilmenge eine obere Schranke bezüglich $\leq$ existiert, dann besitzt A maximale Elemente.
- Ist $\mathcal{F}$ eine Familie von Mengen mit der Eigenschaft, dass mit jeder Kette $U \subset \mathcal{F}$ die Beziehung $\cup U \in \mathcal{F}$ gilt, dann hat das Paar $(\mathcal{F}, \subset)$ maximale Elemente.
- Ist V ein K-VR und ist $E \subset V$ ein Erzeugendensystem und $F \subset V$ eine freie Teilmenge von V, dann gibt es eine Menge $U \subset V$ mit $X \cap F \neq \emptyset$, so dass $F \cup U$ eine Basis von V ist.
- Jeder Vektorraum hat eine Basis. Hat ein Vektorraum eine endliche Basis, dann ist jede weitere Basis dieses Vektorraums ebenfalls endlich und besitzt gleich viele Elemente.

Dimension

Die Dimension eines Vektorraums V über K ist $\dim_K(V) = |B|$.
Beispiele:

- $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$
- $\dim_{\mathbb{Q}}(\mathbb{Q}) = 1$ (weil $\{1\} \subset \mathbb{Q}$ eine Basis von $\mathbb{Q}$ ist)

Lineare Abbildungen und Matrizen

Sind W und V beides K-VR. Eine Abbildung $f : V \to W$ heisst K-linear oder K-VR Homomorphismus falls für alle Element $\lambda \in K$ und alle Vektoren $v, w \in V$ die Gleichungen:

$$f(v + w) = f(v) + f(w) \qquad f(\lambda v) = \lambda f(v)$$

erfüllt werden. Die Menge aller derartiger Abbildungen wird als $\mathrm{Hom}_K(V, W)$ bezeichnet.
Für K-lineare Abbildungen gilt:

$$f(\sum_{i=1}^{n} \lambda_i \cdot v_i) = \sum_{i=1}^{n} \lambda_i \cdot f(v_i)$$

Beispiele:

- $f : \mathbb{R}^3 \to \mathbb{R}^2$ mit $f((x, y, z)) := (y, z)$
- $f : \mathbb{R}^2 \to \mathbb{R}^3$ mit $f((x, y)) := (0, y, z)$

Kern Für $f \in \mathrm{Hom}_K(V, W)$ ist der Kern definiert als:

$$\ker(f) := \{v \in V | f(v) = 0\}$$

- Sind V und W zwei K-VR und $f, g \in \mathrm{Hom}_K(V, W)$, so dass f und g auf einer Basis von V dieselben Werte annehmen, dann gilt: $f = g$
- Sind V und W zwei K-VR und ist $B = \{b_1, \ldots, b_n\}$ eine Basis von V sowie $f : B \to W$ eine beliebige Funktion, dann lässt sich f eindeutig zu einer K-linearen Abbildung $f : V \to W$ fortsetzen.
- Zwei K-VR gleicher, endlicher Dimension sind stets isomorph zueinander. $\Rightarrow$ Ist V ein endlich dimensionaler K-VR, dann gibt es eine Zahl $n \in \mathbb{N}$, so dass V isomorph zu K^n ist.
- Sind V und W zwei K-VR und ist $f \in \mathrm{Hom}_K(V, W)$, dann ist $\ker(f)$ ein Untervektorraum von V und $\mathrm{im}(f)$ ein Untervektorraum von W.
- Sind V und W zwei K-VR endlicher Dimension und ist $f \in \mathrm{Hom}_K(V, W)$, dann gilt:

$$\dim_K(\mathrm{im}(f)) + \dim_K(\ker(f)) = \dim_K(V) \tag{1}$$

- Sind V und W zwei K-VR endlicher und gleicher Dimension, dann sind für $f \in \mathrm{Hom}_K(V, W)$ folgende Aussage äquivalent:
  - f ist ein Isomorphismus
  - f ist ein Epimorphismus
  - f ist ein Monomorphismus