Mathematik III - Wintersemester 14/15

2. Dezember 2014

Inhaltsverzeichnis

1 Algebraische Strukturen mit einer Verknüpfung HALBGRUPPEN, MONOIDE, GRUPPEN

1.1 Definition

Sei $X \neq \emptyset$ eine Menge.

Eine *Verknüpfung* oder (abstrakte) Multiplikation auf X ist eine Abbildung

$$\begin{aligned} \bullet : \quad & X \times X \to X \\ & (a,b) \mapsto a \bullet b \end{aligned}$$

$a \bullet b$ heißt *Produkt* von a und b, muss aber mit der üblichen Multiplikation von Zahlen (ab) nichts zu tun haben.

Beschreibung bei endlichen Mengen oft durch Multiplikationstafeln.

1.2 Beispiel

a) $X = \{a, b\}$

$\bullet$	a	b
a	b	b
b	a	a

$(a \bullet a) \bullet a = b \bullet a = a$
$a \bullet (a \bullet a) = a \bullet b = b$ $\quad \to$ nicht assoziativ

b) $X = \mathbb{Z}^-$ $(= \{0, -1, -2, \dots\})$

Die normale Multiplikation ist auf $\mathbb{Z}^-$ keine Verknüpfung!
(zum Beispiel ist $(-2) \cdot (-3) = 6 \notin \mathbb{Z}^-$)
Aber auf $X = \mathbb{N}, X = \mathbb{Z}$ oder $X = \{1\}, X = \{0, 1\}$

1.3 Definition

Sei $H \neq \emptyset$ eine Menge mit Verknüpfung.

$(H, \bullet)$ heißt *Halbgruppe*, falls gilt:

$$\forall a, b, c \in H \ : \ (a \bullet b) \bullet c = a \bullet (b \bullet c) \qquad \text{(Assoziativgesetz (AG))}$$

1.4 Bemerkung

AG sagt aus: bei endlichen Produkten ist die Klammerung irrelevant, z.B.

$(a \cdot b) \cdot (c \cdot d) = ((a \cdot b) \cdot c) \cdot d = (a \cdot (b \cdot c)) \cdot d$ (usw.)

Deshalb werden Klammern meistens weggelassen.

Die Reihenfolge der Elemente ist i.A. relevant!

1.5 Beispiel

a) $(\mathbb{N}, \bullet), (\mathbb{Z}, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ [1] sind Halbgruppen.

Ebenso $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ [2]

b) $(\mathbb{Q}\backslash\{0\}, :)$ [3] ist *keine* Halbgruppe, denn z.B. $\begin{array}{lcl} (12:6):2 & = & 1 \\ 12:(6:2) & = & 4 \end{array}$

c) vgl. Vorlesung Theoretische Informatik

$A \neq \varnothing$ endliche Menge ("Alphabet")

$A^+ = \cup_{n \in N} A^n$ = Menge aller endlichen Wörter über A
(z.B. $A = \{a, b\}$, dann ist z.B. $\underbrace{(a, a, b)}_{aab} \in A^3$)

Verknüpfung: Konkatenation (Hintereinanderschreiben)
z.B. $aab \bullet abab = aababab$

$A^* = A^+ \cup \{\lambda\}$ λ (oder ϵ) ist das leere Wort

Es gilt: $\lambda \cdot w = w \cdot \lambda = w \; \forall w \in A^*$

$(A^+, \bullet), (A^*, \bullet)$ *Worthalbgruppe* über A

d) $M \neq \varnothing$ Menge, Abb(M, M): Menge aller Abbildungen $M \to M$ mit $\circ$ (Komposition) ist Halbgruppe.

e) (WICHTIG)

$n \in \mathbb{N}$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Verknüpfung: $\begin{array}{l} \oplus : a \oplus b := (a + b) \bmod n \\ \odot : a \odot b := (a \cdot b) \bmod n \end{array}$

$(\mathbb{Z}_n, \oplus), (\mathbb{Z}_n, \odot)$ sind Halbgruppen.

1.6 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *kommutativ*, falls gilt:

$$\forall a, b \in H \; : \; a \cdot b = b \cdot a \qquad \text{(Kommutativgesetz, KG)}$$

1.7 Beispiel

Beispiele 1.5 a), e) sind kommutative Halbgruppen.
(hallo $\neq$ ollah, ab $\neq$ ba, Worthalbgruppe nicht kommutativ)

[1] $\bullet$ normale Multiplikation
[2] $+$ normale Addition
[3] $:$ normale Division

1.8 Definition

Sei $(H, \bullet)$ Halbgruppe, $\emptyset \neq U \subseteq H$

U heißt *Unterhalbgruppe* von H, falls $u \cdot v \in U \ \forall u, v \in U$ gilt.

$(U, \odot)$ ist dann selbst Halbgruppe.

1.9 Beispiel

$(\mathbb{Z}, +)$ Halbgruppe

G = Menge aller gerade ganzen Zahlen $\subseteq \mathbb{Z}$
$(G, +)$ ist Unterhalbgruppe von $(\mathbb{Z}, +)$

U = Menge aller ungerade Zahlen $\subseteq \mathbb{Z}$
$(U, +)$ ist keine Unterhalbgruppe!

1.10 Lemma

Eindeutigkeit des neutralen Elements:

Sei $(H, \bullet)$ Halbgruppe, $e_1, e_2 \in H$ mit $^{(*)} e_1 \cdot x = x \cdot e_1 = x$ und $^{(**)} e_2 \cdot x = x \cdot e_2 = x \ \forall x \in H$

Dann ist $e_1 = e_2$

Beweis. $e_1 \overset{(**)}{=} e_1 \cdot e_2 \overset{(*)}{=} e_2$ □

1.11 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *Monoid*, falls $e \in H$ existiert mit $e \cdot x = x \cdot e = x \ \forall x \in H$

e heißt *neutrales Element* / Einselement / Eins in H.
Schreibweise: $(H, \bullet, e)$

Für additive Verknüpfung oft 0 für e (Nullelement)
multiplikative 1

Nach 1.10 ist das neutrale Element eindeutig!

1.12 Beispiele

a) $(\mathbb{N}, \bullet)$ Monoid mit $e = 1$
$(\mathbb{N}, +)$ kein Monoid
$(\mathbb{N}_0, +)$ Monoid mit $e = 0$
$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ Monoide mit $e = 0$
$(\mathbb{Z}, \bullet), (\mathbb{N}_0, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ Monoide mit $e = 1$

b) $(\mathrm{Abb}(M, M), \circ)$ Monoid, $e = \mathrm{id}$

c) $(\mathbb{Z}_n, \oplus)$ Monoid, $e = 0$
$(\mathbb{Z}_n, \odot)$ Monoid, $e = 1$

d) $(A^*, \bullet)$ Monoid, $e = \lambda$ (halloλ = λhallo = hallo)

1.13 Definition

Sei $(M, \bullet, e)$ Monoid. Eine Teilmenge $\emptyset \neq U \subseteq M$ heißt *Untermonoid* von M, falls U mit $\bullet$ selbst ein Monoid mit neutralem Element e ist (also $e \in U$)

1.14 Lemma

Eindeutigkeit des inversen Elements:

Sei $(H, \bullet, e)$ Monoid und es gebe zu jedem Element $h \in H$ Elemente $x, y \in H$ mit $h \cdot x \overset{(*)}{=} e \overset{(**)}{=} y \cdot h$.

Dann ist $x = y$

Beweis. $y = y \cdot e \overset{(*)}{=} y \cdot (h \cdot x) \overset{(AG)}{=} (y \cdot h) \cdot x \overset{(**)}{=} e \cdot x = x$ □

1.15 Definition

(i) $(H, \bullet, e)$ Monoid, $h \in H$

Falls ein $x \in H$ existiert mit $hx = xh = e$, so nennt man h *invertierbar* und x das *Inverse* zu h, bez. h^{-1} (bei additiven Verknüpfungen oft auch $-h$)

Nach 1.14 ist h^{-1} eindeutig bestimmt!

Es gilt: e ist immer invertierbar, $e^{-1} = e$

(ii) Ein Monoid $(G, \bullet, e)$ heißt *Gruppe*, falls jedes Element in G invertierbar ist.

(iii) Für eine endliche Gruppe G heißt die Anzahl der Elemente in G die *Ordnung* von G, $|G|$

1.16 Bemerkung

$(H, \bullet, e)$ Monoid.

Sei G die Menge aller invertierbaren Elemente von H, dann ist $(G, \bullet, e)$ eine Gruppe.

Es gilt: e invertierbar $(e^{-1} = e)$

und falls g invertierbar, dann ist auch g^{-1} invertierbar: $(g^{-1})^{-1} = g$

falls g, h invertierbar, dann auch $g \cdot h$: $\quad (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

1.17 Beispiele

a) $(\mathbb{N}_0, +, 0)$ ist keine Gruppe aber $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0)$ sind Gruppen.

b) $(\mathbb{Z}, \bullet, 1)$ ist keine Gruppe.
Die Menge der invertierbaren Elemente ist $\{1, -1\}$, diese bilden eine Gruppe.

c) $(\mathbb{Q}, \bullet, 1)$ ist keine Gruppe, aber $(\mathbb{Q}\backslash\{0\}, \bullet, 1), (\mathbb{R}\backslash\{0\}, \bullet, 1)$ sind Gruppen.

d) A^* ist keine Gruppe, nur λ ist invertierbar.

1.18 Beispiele

a) $(\mathbb{Z}_n, \oplus, 0)$ ist Gruppe (was ist das Inverse zu $x \in \mathbb{Z}_n$? Siehe PÜ1, A9)

b) Sei $n \geq 2$. $(Z_n, \odot, 1)$ ist Monoid aber keine Gruppe.

Wann ist ein Element aus Z_n invertierbar bezüglich $\odot$?

$$\begin{aligned} z \in \mathbb{Z}_n \text{ invertierbar} &\Leftrightarrow \exists x \in \mathbb{Z}_n : z \odot x = 1 \\ &\Leftrightarrow \exists x \in \mathbb{Z} : (z \cdot x) \bmod n = 1 \\ &\Leftrightarrow \exists x, q \in \mathbb{Z} : z \cdot x = q \cdot n + 1 \\ &\Leftrightarrow \exists x, q \in \mathbb{Z} : z \cdot x + (-q \cdot n) = 1 \\ &\overset{\text{Mathe I}}{\Leftrightarrow} \operatorname{ggT}(z, n) = 1 \end{aligned}$$

also sind nur zu n teilerfremde Elemente invertierbar!

(vgl. $(Z_6, 0, 1)$: $0, 2, 3, 4$ nicht invertierbar, $1, 5$ invertierbar)

Bezeichnung:

$$Z_n^* = \{z \in \mathbb{Z}_n \mid \operatorname{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich $\odot$ (vgl. Bemerkung **??**) mit Ordnung $|Z_n^*| = \varphi(n)$ ("phi von n", Eulersche φ-Funktion) = Anzahl aller $z \in \mathbb{N}$, die teilerfremd zu n sind und $1 \leq z \leq n$.

$\varphi(3) = 2, \varphi(4) = 2, \varphi(7) = 6$

Wie berechnet man das Inverse von $z \in \mathbb{Z}_n^*$?

Mathe I, Erweiterter Euklidischer Algorithmus (WHK, S. 80/81) liefert zu z und n ($\operatorname{ggT}(z, n) = 1$) Zahlen $s, t \in \mathbb{Z}$ mit

$$\begin{aligned} & z \cdot s + n \cdot t = 1 \\ \Rightarrow\ & (z \cdot s) \bmod n = 1 \\ \Rightarrow\ & (z^{-1}) = s \bmod n \end{aligned}$$

Beispiel:

$n = 8$: $(\mathbb{Z}_8, \odot)$, $z = 5$ ist invertierbar, $\operatorname{ggT}(8, 5) = 1$

EEA: $5 \cdot (-3) + 8 \cdot 2 = 1 \Rightarrow z^{-1} = -3 \bmod 8 \Rightarrow z^{-1} = 5$

c) $\operatorname{Abb}(M, M)$: invertierbare Elemente sind genau die *bijektiven* Abbildungen auf M, $\operatorname{Bij}(M)$ (Mathe I)

Speziell: $M = \{1, 2, \ldots, n\}$, dann heißt $\operatorname{Bij}(M)$ die symmetrische Gruppe von Grad n, S_n

$|S_n| = n!$, Elemente heißen Permutationen.

Bsp: $n = 2$

$$S_2 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{\text{id}}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$n = 3$

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{\text{id}}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$

$\pi \circ \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ \varrho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ (nicht kommutativ!)

$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi, \ \varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

1.19 Satz (Gleichungen lösen in Gruppen)

Sei G Gruppe, $a, b \in G$

(i) Es gibt genau ein $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$)

(ii) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)

(iii) Ist $\underset{ya=yb}{ax = bx}$ für ein $\underset{y \in G}{x}$, dann gilt $a = b$ (Kürzungsregel)

Beweis. (i)
- $x = a^{-1}$ ist Lösung (prüfe $ax = b$):
  $a \cdot \underbrace{a^{-1}b}_{x} \overset{\text{AG}}{=} (a \cdot a^{-1}) \cdot b = e \cdot b = b$
- Es gibt genau eine Lösung:
  Es gelte $ax = b$
  $\Rightarrow x = ex = (a^{-1}a)x \overset{\text{AG}}{=} a^{-1}(ax) = a^{-1}b$

(ii) analog

(iii) Multipliziere von rechts mit $\underset{\text{links}}{x^{-1}}$ $\underset{y^{-1}}{}$

□

1.20 Beispiel

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ - Was ist x?

$a \cdot x = b \Leftrightarrow x = a^{-1} \cdot b$

$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

1.21 Definition

$(G, \cdot)$ Gruppe, $\varnothing \neq U \subseteq G$ Teilmenge.

U heißt *Untergruppe* von G ($U \leqslant G$), falls U bzgl. $\cdot$ selbst eine Gruppe ist.

Insbesondere gilt dann: $\forall u, v \in U$ ist $u \cdot v \in U$.
e von G ist auch neutrales Element in U. (*)
Inversen in U sind die gleichen wie in G.

(*) Angenommen e ist neutrales Element in G, aber f neutrales Element in U, f^{-1} Inverses von f in G.
Dann ist $f^{-1} \cdot f = f \cdot f^{-1} = e$ und $f \cdot f = f$.
$\Rightarrow f = e \cdot f = (f^{-1} \cdot f) \cdot f = f^{-1} \cdot (f \cdot f) = f^{-1} \cdot f = e$

1.22 Beispiele

a) $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +)$

b) $(\{-1, 1\}, \cdot) \leqslant (\mathbb{Q}\backslash\{0\}, \cdot) \leqslant (\mathbb{R}\backslash\{0\}, \cdot)$

c) $(e, \cdot)$ ist Untergruppe jeder beliebigen Gruppe mit Verknüpfung $\cdot$ und neutralem Element e.

d) $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$, $\pi^{-1} = \pi, \pi^{-1} \circ \pi = \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\Rightarrow (\pi, \mathrm{id}) \leqslant S_3$

1.23 Satz und Definition

G Gruppe, $U \leqslant G$

(i) Durch $x \sim y \Leftrightarrow x \cdot y^{-1} \in U$
$x + (-y) \in U$ (bei additiver Verknüpfung)
wird auf G eine Äquivalenzrelation definiert

Beweis

$\sim$ ist reflexiv: $x \sim x$ gilt $\forall x \in G$, denn $x \cdot x^{-1} = e \in U$ ✓

$\sim$ ist symmetrisch: $x \sim y \Rightarrow y \sim x$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ (zzg.: $y \sim x$, also $y \cdot x^{-1} \in U$)
dann ist $y \cdot x^{-1} = (x \cdot y^{-1})^{-1} \in U$, da auch $x \cdot y^{-1} \in U$.

$\sim$ ist transitiv: $x \sim y, y \sim z \Rightarrow x \sim z$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ und $y \sim z$, also $y \cdot z^{-1} \in U$ (zzg.: $x \sim z$, d.h. $x \cdot z^{-1} \in U$)
$x \cdot z^{-1} = xez^{-1} = x(y^{-1}y)z^{-1} = (\underbrace{x \cdot y^{-1}}_{\in U}) \cdot (\underbrace{y \cdot z^{-1}}_{\in U}) \in U$, also $x \sim z$. □

(ii) Für $x \in G$ ist $Ux = \{u \cdot x \mid u \in U\}$ die Äquivalenzklasse von x bzgl. $\sim$ und heißt *Rechtsnebenklasse* von U in G.

Also (Eigenschaften von Äquivalenzklassen siehe Mathe I):

(a) $Ux = Uy \Leftrightarrow x \sim y$, also $x \cdot y^{-1} \in U$

(b) $x, y \in G$, dann ist entweder $Ux = Uy$ oder $Ux \cap Uy = \varnothing$

Beweis

(a) Sei $x \sim y \Rightarrow y \sim x \Rightarrow y \cdot x^{-1} \in U \Rightarrow y = y(x^{-1} \cdot x) = \underbrace{(y \cdot x^{-1})}_{\in U} x \in Ux$

(b) Sei $y \in Ux$, dann zeige: $x \sim y$
$y \in Ux \Rightarrow y = u \cdot x$ für ein $u \in U$
$\Rightarrow x \cdot y^{-1} = x \cdot (ux)^{-1} = x \cdot x^{-1} \cdot u^{-1} = u^{-1} \in U$
Es wurde gezeigt, dass $x \sim y$ gilt.

□

1.24 Beispiel

$G = (\mathbb{Z}, +), 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$
$U = (3\mathbb{Z}, +) \leqslant G$ (ÜA, Blatt 2)
Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$.
$x \sim y \Leftrightarrow \underset{\text{bzw.: } x-y \in U}{x \cdot y^{-1} \in U}$

$x = 0 : U + 0 = \{u + 0 \mid u \in U\} = \{\dots, -3, 0, 3, 6, \dots\} = U = 3\mathbb{Z}$

$x = 1 : U + 1 = \{u + 1 \mid u \in U\} = \{\dots, -2, 1, 4, 7, 10, \dots\} = 3\mathbb{Z} + 1$

$x = 2 : U + 2 = \{u + 2 \mid u \in U\} = \{\dots, -1, 2, 5, 8, 11, \dots\} = 3\mathbb{Z} + 2$

$x = 3 : U + 3 = U + 0 = 0$

...

1.25 Lemma

G Gruppe, U endliche Untergruppe von G, $x \in G$

Dann ist $|U| = |Ux|$

Beweis

$$\begin{array}{rccc} \text{Abb } \varphi : & U & \to & Ux \\ & u & \mapsto & ux \end{array}$$

ist surjektiv und injektiv (falls $u_1 x = u_2 x$, dann ist $u_1 = u_2$ (Satz 1.19 (iii), Kürzungsregel))

Also ist φ bijektiv, also U, Ux gleich mächtig.

1.26 Theorem (Satz von Lagrange)

G endliche Gruppe, $U \leqslant G$

Dann gilt $|U|$ ist Teiler von $|G|$ und $q = \frac{|G|}{|U|}$ ist die Anzahl der Rechtsnebenklassen von U in G

Beweis

Seien $Ux_1, \ldots, Ux_q$ die q verschiedenen Rechtsnebenklassen von U in G

$$\text{Mathe I \& ?? } \Rightarrow G = \bigcup_{i=1}^{q} Ux_i \text{ (disjunkte Vereinigung der Äquivalenzklassen)}$$

$$\Rightarrow |G| = \sum_{i=1}^{q} \underbrace{|Ux_i|}_{|U|} \overset{1.25}{=} q \cdot |U|$$

1.27 Definition

$(G, \bullet, e)$ Gruppe, $a \in G$

Definiere
$$\begin{aligned} a^0 &:= e \\ a^1 &:= a \\ a^m &:= a^{m-1} \cdot a \quad \text{für } m \in \mathbb{N} \\ a^m &:= (a^m)^{-1} \quad \text{für } m \in \mathbb{Z}^- \end{aligned}$$

(Potenzen von a)

Bei additiver Schreibweise:
$$\begin{aligned} 0 \cdot a &= e \\ 1 \cdot a &= a \\ m \cdot a &= \begin{cases} (m-1) \cdot a + a & \text{für } m \in \mathbb{N} \\ (-m) \cdot (-a) & \text{für } m \in \mathbb{Z}^- \end{cases} \end{aligned}$$

1.28 Satz

G, a wie oben

(i) $(a^{-1})^m = (a^m)^{-1} = a^{-m} \quad \forall m \in \mathbb{Z}$

(ii) $a^m \cdot a^n = a^{m+n} \quad \forall m, n \in \mathbb{Z}$

(iii) $(a^m)^n = a^{m \cdot n} \quad \forall m, n \in \mathbb{Z}$

Beweis

(i) $m \in \mathbb{N}: (a^{-1})^m \cdot a^m = \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{m \text{ mal}} \cdot \underbrace{a \cdot \cdots \cdot a \cdot a}_{m \text{ mal}} = e$

$\Rightarrow (a^{-1})^m = (a^m)^{-1}$ (Inverses von a^m)

nach Definition ist $a^{-m} = (a^{-1})^m$

$\Rightarrow$ (i) gilt $\forall m \in \mathbb{N}$

$m = 0: \; e = e = e\checkmark$

$m \in \mathbb{Z}^-$: dann ist $-m \in \mathbb{N}$

Wende den bewiesenen Teil an auf a^{-1} statt a und $-m$ statt m, Behauptung folgt.

(ii), (iii) per Induktion und mit (i) □

1.29 Satz und Definition

G endliche Gruppe, $g \in G$

(i) Es existiert eine kleinste natürliche Zahl n mit $g^n = e$, diese heißt die *Ordnung* $\mathrm{o}(g)$ von G

(ii) Die Menge $\left\{g^0 = e, g^1 = g, g^2, \ldots, g^{n-1}\right\}$ ist eine Untergruppe von G, die von g erzeugte zyklische Gruppe $< g >$

Es gilt $\mathrm{o}(g) = |< g >| = n$ teilt $|G|$

(iii) $g^{|G|} = e$

Bemerkung: Eine endliche Gruppe heißt *zyklisch*, falls sie von einem Element erzeugt werden kann.

Beweis

(i) G endlich $\Rightarrow \exists i, j \in \mathbb{N}, i > j$ mit $g^i = g^j$ (Schubfachschluss -*Editor*)

Dann ist $g^{i-j} \overset{1.28 ii)}{=} g^i \cdot g^{-j} \overset{1.28}{=} \underbrace{g^i}_{=g^j} \cdot (g^j)^{-1} = e$

(ii) Das Produkt zweier Elemente aus $< g >$ liegt wieder in $< g >$

Neutrales Element ist $g^0 = e$

Inverses Element zu g^i ist $(g^i)^{-1} = g^{n-i}$

$\Rightarrow < g > \leqslant G$

(iii) Satz von Lagrange (1.26): $n = \mathrm{o}(g) = |< g >| \;\Big|\; |G|$

Also ist $|G| = n \cdot k$ für ein $k \in \mathbb{N}$

$g^{|G|} = g^{n \cdot k} = (g^n)^k = e^k = e$

□

1.30 Beispiel

$(\mathbb{Z}_3 \backslash \{0\}, \odot, 1)$

$g = 1$: $< 1 >= \left\{g^0 = 1^0 = 1\right\}$, $\mathrm{o}(1) = 1$

$g = 2$: $< 2 >= \left\{g^0 = 1, g^1 = 2\right\}$, $\mathrm{o}(2) = 2$

$(\mathbb{Z}_5 \backslash \{0\}, \odot, 1)$

$g = 2$: $< 2 >= \left\{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3\right\}$, $\mathrm{o}(2) = 4$

1.31 Korollar

(i) Satz von Euler

Sei $n \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a,n) = 1$
Dann ist

$$a^{\varphi(n)} \equiv 1(\text{ mod } n)$$

(ii) Kleiner Satz von Fermat

Ist p eine Primzahl, $a \in \mathbb{Z}, p \nmid a$, dann gilt

$$a^{p-1} \equiv 1(\text{ mod } p)$$

1.32 Beweis

a) Wir können annehmen, dass $1 \leq a < n$ (denn $a^{\varphi(n)} \text{ mod } n = (a \text{ mod } n)^{\varphi(n)}$)
wegen $\text{ggT}(a,n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist eine endliche Gruppe.
$\overset{??(iii)}{\Rightarrow} a^{|\mathbb{Z}_n^*|} = 1(= e)$ $\quad a \odot a \odot \ldots$
$\Rightarrow a^{\varphi(n)} \equiv 1(\text{ mod } n)$ $\quad a \cdot a \cdot \ldots$

b) Folgt aus (i) ($n = p,\ \varphi(p) = -1$)

2 Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper

2.1 Definition

Sei $R \neq \varnothing$ eine Menge mit zwei Verknüpfungen + und $\bullet$.

(i) Wir nennen $(R,+,\cdot)$ einen *Ring*, falls gilt:

(a) $(R,+)$ ist eine abelsche Gruppe (Eselsbrücke: KAIN)
Das neutrale Element bezeichnen wir hier mit 0, das zu $a \in \mathbb{R}$ Inverse mit $-a$
(schreibe auch $a - b$ für $a + (-b)$).

(b) $(R,\cdot)$ ist eine Halbgruppe.

(c) Es gelten die Distributivgesetze:
$a \cdot (b + c) = (a \cdot b) + (a \cdot c) = ab + ac$
$(a + b) \cdot c = (a \cdot c) + (b \cdot c) = ac + bc \qquad \forall a,b,c \in R$

(ii) Ein Ring $(R,+,\cdot)$ heißt *kommutativ* falls $\cdot$ ebenfalls kommutativ ist, also falls $\forall a,b \in \mathbb{R} : a \cdot b = b \cdot a$

(iii) Ein Ring $(R,+,\cdot)$ heißt *Ring mit Eins*, falls $(R,\cdot)$ ein Monoid ist mit neutralen Element $1 \neq 0$ $(\forall a \in R : a \cdot 1 = 1 \cdot a = a)$.

(iv) Ist $(R,+,\cdot)$ Ring mit Eins, dann heißen die bezüglich $\cdot$ invertierbaren Elemente *Einheiten*. Das zu a bezügliche $\cdot$ invertierbare Element bezeichnen wir mit a^{-1}.
R^* := Menge der Einheiten in R.

2.2 Beispiel

a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins (1)
$\mathbb{Z}^* = \{1, -1\}$, $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ ebenso
$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}$.

b) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne Eins

c) trivialer Ring $(\{0\}, +, \cdot)$ ohne Eins

d) $n \in \mathbb{N}, n \geq 2, (\mathbb{Z}_n, \oplus, \odot)$ kommutativer Ring mit Eins

e) $(\mathbb{R}^n, \underbrace{+, \cdot}_{\text{Komponentenweise}})$; allgemein: $R_1, \ldots, R_n$ Ringe, dann $R_1, \times \cdots \times R_n$ Ring.

f) $M_n(\mathbb{R})$ - Menge aller $n \times n$-Matrizen über $\mathbb{R}$, mit Matrixaddition und -multiplikation ist Ring mit Eins ($=E_n$), nicht kommutativ für $n \geq 2$.

2.3 Satz (Rechnen mit Ringen)

Sei $(R, +, \cdot)$ ein Ring, $a, b, c \in R$. Dann gilt:

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot b$

Beweis

(i) $a \cdot 0 = a \cdot (0 + 0) \underset{2.1(3)}{=} a \cdot 0 + a \cdot 0$
addiere $-(a \cdot 0)$ (Inverses von $a \cdot 0$) auf beiden Seiten, erhalte $0 = a \cdot 0$
Analog $0 \cdot a = 0$

(ii) $(-a) \cdot b + a \cdot b \underset{2.1(3)}{=} (-a + a) \cdot b = 0 \cdot b \overset{(i)}{=} 0$
also ist $(-a \cdot b)$ Inverses zu $a \cdot b$, also $= -(a \cdot b)$.
Analog $a \cdot (-b) = -(a \cdot b)$

(iii) $(-a) \cdot (-b) \underset{(ii)}{=} -(a \cdot (-b)) \underset{(ii)}{=} -(-(a \cdot b)) = a \cdot b$

□

2.4 Bemerkung

a) In jedem Ring mit Eins sind 1 und -1 Einheiten (denn $(-1) \cdot (-1) = 1$, siehe 2.3(iii))
Es kann mehr geben (z.B. in $\mathbb{Z}_5$ usw.). Es kann auch $-1 = 1$ gelten (z.B. in $(\mathbb{Z}_2, \oplus, \odot)$)

b) 0 kann nach 2.3(i) nie Einheit sein (da $1 \neq 0$)

c) In einem kommutativen Ring R gilt der *Binomialsatz*,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \quad (n \in \mathbb{N}, a, b \in \mathbb{R})$$

2.5 Definition

Ein kommutativer Ring $(K, +, \cdot)$ heißt *Körper*, wenn jedes Element $0 \neq x \in K$ eine Einheit ist, also wenn

$$K^* = K \backslash \{0\}$$

2.6 Beispiele

a) $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind Körper. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

b) vgl. Beispiel 1.18 b)

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \text{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich $\odot$

$\Rightarrow (\mathbb{Z}_n, \oplus, \odot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

2.7 Satz (Rechnen im Körper, Nullteilerfreiheit)

Sei $(K, +, \cdot)$ ein Körper, $a, b \in K$

Dann gilt

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ oder } b = 0$$

Gegenbeispiel: $(\mathbb{Z}_6, \oplus, \odot)$ ist kein Körper. Hier gilt $2 \odot 3 = 0$, aber weder $2 = 0$, noch $3 = 0$

Beweis

"$\Leftarrow$": klar: $0 \cdot b = 0$ oder $a \cdot 0 = 0$ (Satz 2.3 (i), Rechenregeln für Ringe)

"$\Rightarrow$": Sei $a \cdot b = 0$. Angenommen $a \neq 0$ (d.h. a hat Inverses)

Dann ist
$$\begin{aligned} b &= 1 \cdot b = (a^{-1} \cdot a) \cdot b \\ &= a^{-1} \cdot (a \cdot b) \\ &= a^{-1} \cdot 0 \\ &\overset{2.3(i)}{=} 0 \end{aligned}$$

□

2.8 Definition

Seien $(R, +\cdot)$ und $(\tilde{R}, \boxplus, \boxdot)$ Ringe.

(i) $\varphi : R \to \tilde{R}$ heißt (Ring-)*Homomorphismus*, falls gilt:

$$\varphi(\underbrace{x+y}_{\in R}) = \underbrace{\varphi(x)}_{\in \tilde{R}} \boxplus \underbrace{\varphi(y)}_{\in \tilde{R}} \quad \text{und} \quad \varphi(x \cdot y) = \varphi(x) \boxdot \varphi(y) \quad \forall x, y \in R$$

2.9 Beispiel

$\varphi(\mathbb{Z},+,\cdot) \to (\mathbb{Z}_n,\oplus,\odot)$
$x \mapsto x \bmod n$ ist Ringhomomorphismus (kein Isomorphismus), da φ nicht injektiv ist, z.B. $n = 5 : \varphi(1) = \varphi(6) = \varphi(11) \ldots$

2.10 Satz (Chinesischer Restsatz)

Seien $m_1,\ldots,m_n \in \mathbb{N}$ paarweise teilerfremd, $M := m_1 \cdot \cdots \cdot m_n$, $a_1,\ldots,a_n \in \mathbb{Z}$

Dann existiert ein x, $0 \le x < M$ mit

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Beweis

Für jedes $i \in \{1,\ldots,n\}$ sind die Zahlen m_i und $M_i := \frac{M}{m_i}$ teilerfremd.

$\Rightarrow$ EEA liefert s_i und $t_i \in \mathbb{Z}$ mit $t_i \cdot m_i + s_i \cdot M_i = 1$

Setze $e_i := s_i \cdot M_i$, dann gilt:

$$\begin{aligned} e_i &\equiv 1 \pmod{m_i} \\ e_i &\equiv 0 \pmod{m_j} \quad (j \neq i) \end{aligned}$$

Die Zahl $x := \sum_{i=1}^{n} a_i e_i \pmod{M}$ ist dann die Lösung der simultanen Kongruenz. □

2.11 Beispiel

a) Finde $0 \le x < 60$ mit $x \equiv \begin{cases} 2 \pmod 3 \\ 3 \pmod 4 \\ 2 \pmod 5 \end{cases}$

$M = 3 \cdot 4 \cdot 5 = 60$

$$\begin{aligned} M_1 = \tfrac{60}{3} = 20 \quad & 7 \cdot 3 + (-1) \cdot 20 = 1 \quad \Rightarrow e_1 = -20 \\ M_2 = \tfrac{60}{4} = 15 \quad & 4 \cdot 4 + (-1) \cdot 15 = 1 \quad \Rightarrow e_2 = -15 \\ M_3 = \tfrac{60}{5} = 12 \quad & 5 \cdot 5 + (-2) \cdot 12 = 1 \quad \Rightarrow e_3 = -24 \end{aligned}$$

$x = (2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24)) \bmod 60 = 47$

b) Was ist $2^{1000} \bmod \underbrace{1155}_{3\cdot5\cdot7\cdot11}$

(a) Berechne $2^{1000} \bmod 3,5,7,11$

$$\begin{aligned} 2^{1000} \bmod 3 &= (-1)^{1000} \bmod 3 = 1 \\ 2^{1000} \bmod 5 &= 4^{500} \bmod 5 = (-1)^{500} \bmod 5 = 1 \\ 2^{1000} \bmod 7 &= 2^{3\cdot333+1} \bmod 7 = (8^{333} \cdot 2) \bmod 7 = (1 \cdot 2) \bmod 7 = 2 \\ 2^{1000} \bmod 11 &= 2^{5\cdot200} \bmod 11 = 32^{200} \bmod 11 = (-1)^{200} \bmod 11 = 1 \end{aligned}$$

(b) Suche $0 \leq x < 1155$ mit $x \equiv \begin{cases} 1 & (\bmod 3) \\ 1 & (\bmod 5) \\ 2 & (\bmod 7) \\ 1 & (\bmod 11) \end{cases}$

Der chinesische Restsatz liefert $x = 331$

2.12 Bemerkung

Man kann auch zeigen, dass die Lösung x aus Satz 2.10 eindeutig ist:

Durch $\psi : \mathbb{Z}_M \to Z_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$
$x \mapsto (x \bmod m_1, \ldots, x \bmod m_n)$

wird ein Ringisomophismus definiert:

ψ ist surjektiv (zu jedem n-Tupel aus $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ gibt es eine Lösung x, siehe Restsatz) und es gilt:

$$\underbrace{|\mathbb{Z}_M|}_{M} = \underbrace{|\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}|}_{m_1 \cdot \cdots \cdot m_n = M}$$

also ist ψ bijektiv, also auch injektiv, also ist Lösung x eindeutig.

2.13 Korollar

$M = m_1 \cdot \cdots \cdot m_n$, m_i paarweise teilerfremd.
Dann ist $\varphi(M) = \varphi(m_1) \cdot \ldots \varphi(m_n)$, insbesondere:
$n = p_1^{a_1} \cdot \cdots \cdot p_k^{a_k}$ (p_i Primzahlen, $a_1 > 0, p_i \neq p_j$ für $i \neq j$)

Beweis

Nach 2.12 ist $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ mittels ψ
$\Rightarrow x$ Einheit $\Leftrightarrow \psi(x) = (x \bmod m_1, \ldots, x \bmod m_n)$ Einheit
$\Leftrightarrow x \bmod m_i$ Einheit $\forall i = 1 \ldots n$
$\Rightarrow \varphi(M) = \varphi(m_1) \cdot \cdots \cdot \varphi(m_n)$
$\varphi(p^a) \underbrace{=}_{\text{Überlegen}} p^a - p^{a-1} = p^{a-1}(p-1)$

2.14 Definition

Sei K Körper mit Nullelement 0 und Einselement 1:

(i) Ein *Polynom über K* ist Ausdruck $f = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$, $n \in \mathbb{N}_0, a_i \in K$.
a_i heißen *Koeffizienten* des Polynoms.

(a) Ist $a_i = 0$, so kann man $0 \cdot x^i$ bei der Beschreibung weglassen.

(b) Statt $a_0 x^0$ schreibt auch a_0

(c) Sind alle $a_i = 0$, so schreibt man $f = 0$, das Nullpolynom.

(d) Ist $a_i = 1$, so schreibt man x^i statt $1 \cdot x^i$

(e) Die Reihenfolge der $a_i x^i$ kann verändert werden, ohne dass das Polynom sich verändert ($x^4 + 2x^3 + 3 = 2x^3 + 3 + x^4$)

(ii) Zwei Polynome f und g sind *gleich*, wenn ($f = 0$ und $g = 0$) oder ($f = a_0 + a_1 x^1 + \cdots + a_n x^n$, $g = b_0 + b_1 x^1 + \cdots + b_m x^m, a_n \neq 0, b_m \neq 0$ und $n = m$, $a_i = b_i$ für $i = 0, \ldots, n$) gilt.

(iii) Die Menge aller Polynome über K bezeichnet man als $K[x]$

2.15 Beispiel

a) $\underbrace{f}_{f(x)} = 3x^2 + \frac{1}{2}x - 1 \in \mathbb{Q}[x] \wedge f \in \mathbb{R}[x]$

b) $g = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$

Wir wollen in $K[x]$ wie in einem Ring rechnen können. Wir brauchen dazu + und $\cdot$ für Polynome.

2.16 Satz und Definition

K Körper, dann wird $K[x]$ zu einem kommutativen Ring mit Eins durch folgende Verknüpfungen:

$$f = \underbrace{\sum_{i=0}^{n} a_i x^i}_{\text{z.B. } x+2}, \quad g = \underbrace{\sum_{j=0}^{m} b_j x^j}_{x^3+2x+1},$$

dann

$$f + g = \underbrace{\sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i}_{x^3+3x+3}$$

$$f \cdot g = \sum_{i=0}^{n+m} c_i x^i$$

$$\text{mit } c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0 = \sum_{j=0}^{i} a_j b_{i-j} \qquad \text{(Faltungsprodukt)}$$

(setze a_i mit $i > n$ bzw. b_j mit $j > m$ gleich 0)

- Einselement: $f = 1$ ($a_0 = 1, a_j = 0$ für $j \geq 1$)
- Nullelement: $f = 0$

$K[x]$ heißt der *Polynomring* in einer Variablen über K.
Beweis: Ringeigenschaften nachrechnen.

2.17 Bemerkung

Die +-Zeichen in der Beschreibung der Polynome entsprechen der Ring-Addition der *Monome* $a_0, ax, a_2x^2, \ldots, a_nx^n$

2.18 Beispiel

a) in $\mathbb{Q}[x], \mathbb{R}[x]$ Addition, Multiplikation klar

b) in $\mathbb{Z}_3[x]$: $f = 2x^3 + 2x + 1$, $g = 2x^3 + x$

$$\begin{aligned} f + g &= x^3 + 1 \\ f \cdot g &= (2x^3 + 2x + 1)(2x^3 + x) \\ &= x^6 + 2x^4 + x^4 + 2x^2 + 2x^3 + x \\ &= x^6 + 2x^3 + 2x^2 + x \end{aligned}$$

c) in $\mathbb{Z}_2[x]$: $f = x^2 + 1$, $g = x + 1$

$$\begin{aligned} f + g &= x^2 + x \\ f + f &= 0 \\ g \cdot g &= x^2 + 1 \end{aligned}$$

2.19 Definition

Sei $0 \neq f \in K[x]$

$f = a_0 + a_1x + \cdots + a_nx^n$ mit $a_n \neq 0$

Dann heißt n der *Grad* von f $\mathrm{Grad}(f)$

$\mathrm{Grad}(0) := -\infty$
$\mathrm{Grad}(f) = 0$ *für konstante Polynome* $\neq 0$

2.20 Satz

K Körper, $f, g \in K[x]$

Dann ist $\mathrm{Grad}(f \cdot g) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$

(Konvention: $-\infty + (-\infty) = -\infty + n = -\infty$)

Beweis

Stimmt für $f = 0$ oder $g = 0$

$$\begin{aligned} f &= a_0 + a_1x^1 + \ldots + a_nx^n && \text{mit} \quad a_n \neq 0 \\ g &= b_0 + b_1x^1 + \ldots + b_mx^m && \text{mit} \quad b_m \neq 0 \\ f \cdot g &= (\ldots) \cdot (\ldots) = \ldots + \underbrace{(a_nb_n)}_{\neq 0,} \cdot x^{n+m} \end{aligned}$$

(siehe Satz 2.7 Nullteilerfreiheit in Körpern)

Höhere Potenzen mit Koeffizienten $\neq 0$ gibt es nicht

$\Rightarrow \text{Grad}(f \cdot g) = n + m$

2.21 Korollar

K Körper, dann $K[x]^* = \{f \in K[x] \mid \text{Grad}(f) = 0\}$,

d.h. nur die konstanten Polynome $\neq 0$ sind in $K[x]$ bezüglich $\cdot$ invertierbar.

$$\underbrace{f}_{\text{Grad } n} \cdot \underbrace{f^{-1}}_{\text{müsste Grad } -n \text{ haben}} = \underbrace{1}_{\text{Grad } 0} \leftarrow \text{geht nicht}$$

2.22 Definition

Sei $b \in K$

$\varphi_b : K[x] \to K, f := \sum_{i=0}^{n} a_i x^i \mapsto f(b) := \sum_{i=0}^{n} a_i b^i$

ist ein surjektiver Ringhomomorphismus, der sogenannte *Auswertungshomomorphismus* an der Stelle b.

(setze b für x ein)

2.23 Definition

K Körper, $f, g \in K[x]$

f teilt g, $f|g$, falls ein $q \in K[x]$ existiert mit $g = q \cdot f$

(Nach 2.20 ist dann $\text{Grad}(f) \leq \text{Grad}(g)$, falls $g \neq 0$)

2.24 Definition (Division mit Rest)

K Körper, $0 \neq f \in K[x],\ g \in K[x]$

Dann existieren eindeutig bestimmte Polynome $q, r \in K[x]$ mit $g = q \cdot f + r$ und $\text{Grad}(r) < \text{Grad}(f)$.

Bezeichnung:

$$r =: g \bmod f$$
$$q =: g \operatorname{div} f$$

Beweis

Vgl. Mathe I für $\mathbb{Z}$, siehe z.B. WHK Satz 4.69

2.25 Beispiel

a)

$$g = x^4 + 2x^3 - x + 2 \quad \in \mathbb{Q}[x]$$
$$f = 3x^2 - 1 \quad \in \mathbb{Q}[x]$$

Rechne:

$$\begin{array}{l} \left(\; x^4 + 2x^3 \qquad - x \;\; + 2\right) : \left(3x^2 - 1\right) = \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} + \dfrac{-\frac{1}{3}x + \frac{19}{9}}{3x^2 - 1} \\ \underline{-x^4 \qquad + \frac{1}{3}x^2} \\ \qquad 2x^3 + \frac{1}{3}x^2 \;\; - x \\ \qquad \underline{-2x^3 \qquad + \frac{2}{3}x} \\ \qquad\qquad \frac{1}{3}x^2 - \frac{1}{3}x \;\; + 2 \\ \qquad\qquad \underline{-\frac{1}{3}x^2 \qquad + \frac{1}{9}} \\ \qquad\qquad\qquad -\frac{1}{3}x + \frac{19}{9} \end{array}$$

b)

$$g = x^4 + x^2 + 1 \qquad f = x^2 + x \quad \in \mathbb{Z}_2[x]$$

Rechne:

$$(x^4 + x^2 + 1) : x^2 + x = \underbrace{x^2 + x}_{q}$$

2.26 Korollar

K Körper, $a \in K$

$f \in K[x]$ ist genau dann durch $(x - a)$ teilbar, wenn $f(a) = 0$ ist (d.h. a ist Nullstelle von f).

Beweis

"⇒" sei f durch $(x - a)$ teilbar, d.h.

$$f = q \cdot (x - a) \Rightarrow f(a) = q(a) \cdot (\underbrace{a - a}_{0}) = 0 \quad q \in K$$

"⇐" Division mit Rest: $f = q(x - a) + r$, wobei $\text{Grad}(r) < \underbrace{\text{Grad}(x - a)}_{1}$

$\Rightarrow r$ ist konstantes Polynom (Grad 0) oder Nullpolynom (Grad $(-\infty)$) also $r \in K$

$$0 = f(a) = q(a) \cdot 0 + r \Rightarrow r = 0$$

□

2.27 Definition

K Körper

(i) Ein Polynom dessen höchster von 0 verschiedener Koeffizient gleich 1 ist, heißt normiert.

(ii) $g, h \in K[x]$, nicht beide 0

$f \in K[x]$ heißt *größter gemeinsamer Teiler* von g und h ($f = \mathrm{ggT}(g,h)$), falls f normiertes Polynom von maximalem Grad ist, das g und h teilt.

(iii) $g, h \in K[x] \setminus \{0\}$ beide nicht 0

$f \in K[x]$ heißt *kleinstes gemeinsames Vielfaches* von g und h
($f = kgV(g,h)$), falls f normiertes Polynom von kleinstem Grad ist, das von g und h geteilt wird.

2.28 Bemerkung

a) $f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$, dann ist $a_n^{-1} f = x^n + \ldots$ normiertes Polynom.

(z.B.: $f = 3x^2 + x + 7 \in \mathbb{R}[x]$)

dann $\frac{1}{3} f = x^2 + \frac{x}{3} + \frac{7}{3}$ normiert.

In $\mathbb{Z}_{11}[x]$: $\underbrace{4}_{\text{Inverses von 3, denn } 3 \cdot 4 = 12 \equiv 1 \pmod{11}} f = x^2 + 4x_6$ normiert.

b) $\mathrm{kgV}(g,h)$ existiert und ist eindeutig:

$$\begin{aligned} &\text{sei } f_1 = \mathrm{kgV}(g,h),\ f_2 = \mathrm{kgV}(g,h) \\ &\Rightarrow g,h|f_1, \quad g,h|f_2 \\ &\Rightarrow g,h|(f_1 - f_2) \end{aligned}$$

c) $\mathrm{ggT}(g,h)$ existiert. Beweis Eindeutigkeit wie in $\mathbb{Z}$ (Mathe I), folgt aus.

2.29 Satz (von Bezout)

K Körper, $g, h \in K[x]$, nicht beide 0.

Dann existieren $s,t \in K[x]$, sodass

$$f = s \cdot g + t \cdot h$$

ein ggT von g und h ist.

(Beweis: EEA in $K[x]$, später)

2.30 Satz

Euklidischer Algorithmus in $K[x] \rightarrow$ siehe „Blatt"

2.31 Satz

EEA in $K[x] \rightarrow$ siehe „Blatt"

2.32 Beispiel

$g = x^4 + x^3 + 2x^2 + 1, h = x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$
... TBD ...

2.33 Definition

k Körper. Ein Polynom $p \in K[x]$, $\text{Grad}(p) \geq 1$ (d.h. $p \neq 0$, p nicht konst., also keine Einheit) heißt *irreduzibel*, falls gilt:

Ist $p = f \cdot g$ $(f, g \in K[x])$, so ist $\text{Grad}(f) = 0$ oder $\text{Grad}(g) = 0$ (d.h. f oder g ist konst. Polynom).

Bemerkung: $p = a \cdot a^{-1} \cdot p$ für $a \in K \backslash \{0\}$ geht immer.

2.34 Beispiel

a) $ax + b$ $(a \neq 0)$ ist irreduzibel in $K[x]$ für jeden Körper K

b) $x^2 - 2 \in \mathbb{Q}[x]$ ist irreduzibel:
angenommen nicht, dann $(x^2 - 2) = (ax + b)(cx + d)$ mit $a, b, c \in \mathbb{Q} \wedge a, c \neq 0$
$(ax + b)$ hat Nullstelle $-\frac{b}{a}$, also müsste auch $(x^2 - 2)$ Nullstelle $-\frac{b}{a}$ $(\in \mathbb{Q})$ haben.
Nullstellen von $(x^2 - 2)$ sind aber nur $\sqrt{2}$ und $-\sqrt{2}$, beide nicht in $\mathbb{Q}$!

c) $x^2 - 2 \in \mathbb{R}[x]$ ist nicht irreduzibel.
$x^2 - 2 = \underbrace{(x + \sqrt{2})}_{\in \mathbb{R}[x]} \cdot \underbrace{(x - \sqrt{2})}_{\in \mathbb{R}[x]}$

d) $x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel

e) $x^2 + 1 \in \mathbb{Z}_5[x]$ ist nicht irreduzibel:
$(x^2 + 1) = (x + 2) \cdot (x + 3) = (x^2 + 3x + 2x + 1) = (x^2 + 1)$
$2 \Rightarrow (x^2 + 1)$ ist teilbar durch $(x - 2) \hat{=} (x + 3)$

2.35 Abschlussbemerkung

a) Irreduzibel Polynome in $K[x]$ entsprechen den Primzahlen in $\mathbb{Z}$. Man kann zeigen:
$f = \sum_{i=0}^{n} a_i x^i \in K[x]$, $a_n \neq 0, n \geq 1$.
Dann existieren eindeutig bestimmte irreduzibel Polynome $p_1, \ldots, p_e$ und natürlichen Zahlen $m_1, \ldots, m_e \in \mathbb{N}$ mit $f = a_n \cdot p_1^{m_1} \cdot \ldots \cdot p_e^{m_e}$

b) Gegeben: Primzahl p, dann gibt es Körper mit p Elementen:
$(\mathbb{Z}_p, \oplus, \odot)$

Man kann zeigen: zu jeder Primzahlpotenz p^a gibt es Körper mit p^a Elementen, diesen konstruiert man über irreduzible Polynome in $\mathbb{Z}_p[x]$.

3 Der Körper der $\mathbb{C}$ der Komplexen Zahlen

3.1 Definition

Eine komplexe Zahl $\mathbb{Z}$ ist von der Form $z = x + i \cdot y$ mit $x, y \in \mathbb{R}$ und einer „Zahl" i mit $i^2 = -1$ („imaginäre Einheit"). x heißt Realteil von z, x =Re z
y heißt Imaginärteil, y =In z.

Die Menge aller komplexen Zahlen bezeichnen wie mit $\mathbb{C}$ und definieren auf $\mathbb{C}$ Addtition und Multiplikatio wie folgt:

Für $z = x + iy$ und $w = a + ib$ ist
$z + w := (x + a) + i(y + b)$,
$z - w := (x - a) + i(y - b)$ und
$z \cdot w := (xa - yb) + i(xb + ya)$.

Erläuterung zur Multiplikation: $((x + iy)(a + ib) = xa + xib + iya + i^2yb = (xa - yb) + i(xb + ya)$.

Mit diesen Verknüpfungen ist $\mathbb{C}$ ein Körper:

a) AG, kG, DG: nachrechnen

b) $0 = 0 + i \cdot 0$

c) additiv Inverses: $-z = -x - iy$

d) $1 = 1 + i \cdot 0$

e) multiplikativ Inverses: $z^{-1} = \frac{1}{z} = \frac{1}{x+y} = \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy} = \frac{x-iy}{x^2+y^2} = \underbrace{\frac{x}{x^2+y^2}}_{\in\mathbb{R}} + i \cdot \underbrace{\frac{-y}{x^2+y^2}}_{\in\mathbb{R}}$

Man nennt für $z = x + iy$ die Zahl $\overline{z} = x - iy$ die zu z *konjugiert komplexe Zahl* und $|z| := \sqrt{x^2 + y^2}$ den *Betrag* von z.

3.2 Beispiel

a) $z = 2 + 3i$ mit $\mathrm{Re}(z) = 2$ und $\mathrm{Im}(z) = 3$.
$\overline{z} = 2 - 3i, |z| = \sqrt{2^2 + 3^2} = \sqrt{13}$
$z \cdot \overline{z} = (2 + 3i) \cdot (2 - 3i)$
$= 4 - 6i + 6i - 9i^2 = 4 + 9 = 13$

b) $w = 1 + i = 1 + 1i$ mit $\mathrm{Re}(w) = 1$, $\mathrm{Im}(w) = 1$, $\overline{w}1 - i, |w| = \sqrt{1^2 + 1^2} = \sqrt{2}$

c) Selbst nachrechnen: $u = 7 = 7 + 0 \cdot i$, $v = 5i = 0 + 5i$

d) $u + w + z = 7 + (1 + i) + (2 + 3i) = 10 + 4i$
$u \cdot w = 7 \cdot (1 + i) = 7 + 7i$
$\frac{w}{z} = \frac{1+i}{2+3i} = \frac{(1+i)\cdot(2-3i)}{4+9} = \frac{2-3i+2i=3i^2}{13} = \frac{5-i}{13} = \frac{5}{13} - \frac{1}{13}i$

3.3 Bemerkung: komplexe Zahlenebene

Man kann $\mathbb{C}$ veranschaulichen in der „Gaußschen Zahlenebene":
Betrachte $z = x + iy$ als Punkt $(x|y)$ in $\mathbb{R}^2$:

3.4 Satz (Eigenschaften)

a)
$$\left.\begin{array}{ll} \overline{w+z} & = \overline{w} + \overline{z} \\ \overline{w \cdot z} & = \overline{w} \cdot \overline{z} \\ \overline{\frac{w}{z}} & = \frac{\overline{w}}{\overline{z}} \quad (z \neq 0) \\ \overline{\overline{z}} & = z \end{array}\right\} \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z} \text{ ist Körperisomorphismus}$$

b) $Re(z) = \frac{z+\overline{z}}{2}, Im(z) = \frac{z-\overline{z}}{2i}$

c) $|z| \geq 0$, $|z| = 0$ nur für $z = 0$

d) $|z| = |\overline{z}| = \sqrt{z \cdot \overline{z}}$

e) $|w \cdot z| = |w| \cdot |z|$

f) $|w + z| \leq |w| + |z|$ (Dreiecksungleichung)
$|w + z| \geq \Big||w| - |z|\Big|$

Beweis

z.B.: d) sei $z = x + iy \quad x, y \in \mathbb{R}$
$\Rightarrow \overline{z} = x - iy, \quad |z| = \sqrt{x^2 + y^2}$
$|\overline{z}| = \ldots$

3.5 Bemerkung

a) In $\mathbb{C}$ existiert $\sqrt{-1} : \pm i$, d.h. $x^2 + 1 = 0$ ist lösbar in $\mathbb{C}$, das Polynom $x^2 + 1$ ist nicht irreduzibel in $\mathbb{C}[x]$: $x^2 + 1 = (x + i)(x - i)$

b) Mann kann jede quadratische Gleichung $ax^2 + bx + c$ $(a, b, c \in \mathbb{R})$ in $\mathbb{C}$ lösen:
$x_{1|2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$
Jedes $b^2 - 4ac < 0$ ist, schreibe:
$\frac{-b \pm \sqrt{4ac-b^2}\cdot i}{2a}$

c) Es gilt sogar: Fundamentalsatz der Algebra:
Jedes Polynom $f \in \mathbb{C}[x]$ vom Grad $n \geq 1$ hat genau n Nullstellen in $\mathbb{C}$.

3.6 Polarkoordinaten

Eine andere Möglichkeit, komplexe Zahlen zu beschreiben:

Angabe von Winkel (φ) und Abstand r zum Nullpunkt.
Zu jedem $z \in \mathbb{C}$ gibt es ein eindeutig bestimmtes $r \leq 0$ und ein $\varphi \in \mathbb{R}$ mit
$z = r(\cos\varphi + i \cdot \sin\varphi)$ (Polarkoordinatendarstellung von z) und zwar ist $r = |z| = \sqrt{x^2 + x^2}$
für $z = x + iy$, $\frac{x}{r} = \cos\varphi$, $\frac{y}{r} = \sin\varphi$:

$$\begin{aligned} z &= x + iy \\ &= r \cdot \cos\varphi + i \cdot r \cdot \sin\varphi \\ &= r \cdot (\cos\varphi + i \cdot \sin\varphi) \end{aligned}$$

Aus den Additionstheoremen für sin, cos folgt (PÜ6):

$$\begin{aligned} z_1 \cdot z_2 &= |z_1| \cdot |z_2| \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)) \\ z^2 &= |z|^2 \cdot (\cos(2\varphi) + i \cdot \sin(2\varphi)) \\ \pm\sqrt{z} &= \sqrt{|z|} \cdot (\cos(\frac{\varphi}{2}) + i \cdot \cos(\frac{\varphi}{2})) \end{aligned}$$

3.7 Beispiel

a) $z_1 = 1,\ r_1 = 1,\ \varphi_1 = 0 \Rightarrow z_1 = 1 \cdot (\cos 0 + i \cdot \sin 0)$

b) $z_2 = i,\ r_2 = 1,\ \varphi_2 = \frac{\pi}{2} \Rightarrow z_2 = 1 \cdot (\cos\frac{\pi}{2} + i \cdot \sin\frac{\pi}{2})$

c) $z_3 = 1 + i,\ r_2 = \sqrt{2},\ \varphi_2 = \frac{\pi}{4} \Rightarrow z_3 = \sqrt{2} \cdot (\cos\frac{\pi}{4} + i \cdot \sin\frac{\pi}{4})$

3.8 Definition/Schreibweise

$e^{i\varphi} := \cos\varphi + i \cdot \sin\varphi$

$z = \underbrace{r}_{\text{Betrag}} \cdot e^{i\varphi}$

3.9 Bemerkung

Statt Defintion 3.8:

Man kann auch die Definition von Folgen, Konvergenz, Grenzwert von $\mathbb{R}$ auf $\mathbb{C}$ übertragen, alles aus Mathe II (Analysis!), u.a. auch Potenzreihen, insbesondere die Exponentialfunktion definieren.

Für alle $z \in \mathbb{C}$ konvergiert $\sum_{k=0}^{\infty} \frac{z^k}{k!} := \exp(z),\ e^z$

Mit den Methoden aus Mathe II - „2. Teil" kann man dann zeigen, dass

$$e^i t = \cos t + i \cdot \sin t \ \forall t \in \mathbb{R} \text{ (Eulersche Formel)}$$

$$z_1 \cdot z_2 = (r_1 \cdot r_2) \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)) = \underline{(r_1 \cdot r_2) \cdot e^{i(\varphi_1 + \varphi_2)}}$$

3.10 Beispiele

a) $1 \cdot e^{i \cdot 0} = 1$

b) $e^{i\pi} = -1$ (und: $e^{i\pi} + 1 = 0$ ☺)

c) $2 \cdot e^{2\pi} = 2$

d) ...

3.11 Bemerkung

$\mathbb{C}$ hat alle algrebraischen und analystischen Eigenschaften wie $\mathbb{R}$ (oder besser), außer:

Es gibt auf $\mathbb{C}$ keine vollständige Ordnung $\leq$, die mit + und $\cdot$ verträglich ist, d.h. für die gelten würde:

$$a \leq b, c \leq d \Rightarrow a + c \leq b + d$$
$$a \leq b, r \geq 0 \Rightarrow ra \leq rb$$

4 Wiederholung und Erweiterung der linearen Algebra aus Mathe II

4.1 Beispiel

a) $K = \mathbb{Z}, V_1 = \mathbb{Z}_2^2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : x_1, x_2 \in \mathbb{Z}_2 \right\}$

V_1 hat 4 Elemente: $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$O = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, d.h. $- \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\forall v \in V : 0 \cdot v = O = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $1 \cdot v = v$

b) $K = \mathbb{Z}_5, V_2 = \mathbb{Z}_5^3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \right\}$

$v = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, w = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \in \mathbb{Z}_5^3$

$-v = \begin{pmatrix} 0 \\ 4 \\ 3 \end{pmatrix}, -w = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, v + w \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$

$1 \cdot w = w, 2 \cdot w = \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, 3 \cdot w = \cdots$

$|V| = 5 \cdot 5 \cdot 5 = 125$

c) $U = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in V_1 : x_1 \oplus x_2 = 0 \right\}$ ist UR von V_1

- $U = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\} \neq \emptyset$
- Sei $u = \begin{pmatrix}u_1\\u_2\end{pmatrix} \in U$, d.h. $u_1 \oplus u_2 = 0$

$\Rightarrow$ für $\lambda \cdot u = \begin{pmatrix}\lambda u_1\\\lambda u_2\end{pmatrix}$ gilt $\lambda u_1 \oplus \lambda u_2 = \lambda \cdot \underbrace{(u_1 \oplus u_2)}_{0} = 0$

d) $\mathbb{Z}_3^3$:

$\begin{pmatrix}0\\0\\0\end{pmatrix}$ l.a.; $\begin{pmatrix}0\\1\\2\end{pmatrix}$ l.u.; $\begin{pmatrix}0\\1\\2\end{pmatrix}, \begin{pmatrix}0\\2\\1\end{pmatrix}$ sind l.a.

e) Kanonische Basis von V_2 (Bsp. b)):

$B_1 = \underbrace{\left\{e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}\right\}}_{\text{geordnete Basis}}$, $\dim V_2 = 3$

z.B.: $\begin{pmatrix}2\\3\\1\end{pmatrix} = \alpha \cdot e_1 + \beta \cdot e_2 + \gamma \cdot e_3$ mit $\alpha = 2,\ \beta = 3,\ \gamma = 1$ und $\alpha,\ \beta,\ \gamma$ sind die kartesischen Koordinaten.

Eine andere (geordnete) Basis, z.B.:

$B_2 = \left\{\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\2\\3\end{pmatrix}\right\}$

Zeige Vektoren sind linear unabhängig:

$\alpha \cdot \begin{pmatrix}2\\0\\0\end{pmatrix} + \beta \cdot \begin{pmatrix}0\\1\\1\end{pmatrix} + \gamma \cdot \begin{pmatrix}1\\2\\3\end{pmatrix} = O$

$\Rightarrow \cdots \Rightarrow \cdots \Rightarrow \alpha = \beta = \gamma = 0$

Koordinaten von $\begin{pmatrix}2\\3\\1\end{pmatrix}$ in B_2?

Stelle LGS auf und löse es ...

4.2 Definition

$A \in M_{n,n}(K)$ heißt *invertierbar*, falls $\exists A^{-1} \in M_{n,n}(K)$ mit $A^{-1} \cdot A = A \cdot A^{-1} = E_n$

5 Lineare Abbildungen

5.1 Definition

Seien V, W K-Vektorräume.

a) $\varphi : V \to$ heißt *lineare* Abbildung (VR-Homomorphismus), falls:

- $\forall v_1, v_2 \in V : \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ (Additivität)
- $\forall v \in V, \forall \lambda \in K : \varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ (Homogenität)

b) Ist die lineare Abbildung $\varphi : V \to W$ bijektiv, so heißt φ *Isomorphismus*, V und W heißen dann *isomorph*, $V \cong W$.

5.2 Bemerkung

$\varphi : V \to W$ ist eine lineare Abbildung:

a) $\varphi(O) = O$

b) $\varphi\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{i=1}^{n} \lambda_i \varphi(v_i)$

5.3 Beispiel

a) Nullabbildung:
$\varphi : V \to W, v \mapsto O$

b) $\varphi : V \to V, v \mapsto \lambda v$ für jedes festes $\lambda \in K$ ist lineare Abbildung ($\lambda = 1 : \varphi = \mathrm{id}_V$)

c) $\varphi : \mathbb{R}^3 \to \mathbb{R}^3, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ z_3 \end{pmatrix}$ ist eine lineare Abbildung (Spiegelung an x_1, x_2-Ebene)

d) $\varphi : \mathbb{R}^2 \to R^2, \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} (x_1)^2 \\ x_2 \end{pmatrix}\right)$ ist nicht linear

$v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \lambda = 3 :$

$\varphi(3v) = \varphi\left(\begin{pmatrix} 3 \\ 6 \end{pmatrix}\right) = \begin{pmatrix} 9 \\ 6 \end{pmatrix} \neq \begin{pmatrix} 3 \\ 9 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 3 \cdot \varphi\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = 3 \cdot \varphi(v)$

5.4 Satz

$A \in M_{m,n}(K)$

Dann ist $\varphi : K^n \to K^m, x \mapsto Ax$

eine lineare Abbildung

Beweis

folgt aus Rechenregeln für Matrizen:

$$\varphi(x+y) = A(x+y) = Ax + Ay$$
$$= \varphi(x) + \varphi(y)$$

$$\varphi(\lambda \cdot x) = A(\lambda x) = \lambda Ax$$
$$= \lambda\varphi(x)$$

□

Alle bisherigen Beispiele waren von dieser Form!

5.3

a) $A = 0 = Nullmatrix$

b) $A = \begin{pmatrix} \lambda & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda \end{pmatrix} = \lambda \cdot E_n$

c) $A = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$

Es gilt (→ später):

alle lineare Abbildungen $K^n \to K^m$ sind von der Form in 5.4

5.5 Satz

$\varphi : V \to W$ lineare Abbildung

(i) $U \subseteq V$ UR von V
$\Rightarrow \varphi(U) \subseteq W$ UR von W und $\varphi(V)$ (Bild von V) ist UR von W

(ii) falls $\dim(U)$ endlich : $\dim(\varphi(U)) \leq \dim(U)$

Beweis

(i) $U \subseteq V$ Unterraum, d.h. für $u, v \in U$ ist $\lambda u + \mu v \in U$
$\varphi(U) = \{\varphi(u) | u \in U\}$ ist auch UR:
für $\varphi(u), \varphi(v) \underset{\text{lin. Abb.}}{=} \varphi(\lambda u + \mu v) \in \varphi(U)$
außerdem ist $\varphi(U) \neq \emptyset$, da $\varphi(O) = O$

(ii) $v_1, \ldots, v_k$ Basis von U
$\Rightarrow \varphi(u_1), \cdots, \varphi(u_k)$ ist Erzeugendensystem von $\varphi(U)$
$\Rightarrow$ enthält Basis (Mathe II)
$\Rightarrow$ Behauptung □

5.6 Definition

$\varphi : V \to W$ lineare Abbildung, V endlich dimensional
Dann heißt die $\dim(\varphi(V))$ der Rang von φ, $\operatorname{rg}(\varphi)$.

5.7 Definition/Satz

$\varphi : V \to W$ lineare Abbildung

(i) $\ker(\varphi) := \{v \in V \mid \varphi(v) = O\}$
(alle Vektoren die von φ auf O abgebildet werden)
heißt der Kern von φ und ist ein UR von V.

(ii) φ : injektiv $\Leftrightarrow \ker(\varphi) = \{O\}$

Beweis

(i) $\ker(\varphi)$ ist UR:

- $\ker(\varphi) \neq \emptyset$, da $\varphi(O) = O$
- seien $u, v \in \ker(\varphi)$, d.h. $\varphi(u) = O, \varphi(v) = O$, seien $\lambda, \mu \in K$
  $\Rightarrow \lambda u + \mu v \in \ker(\varphi)$, dann:
  $\varphi(\lambda u + \mu v) \underset{\text{lin. Abb.}}{=} \lambda \cdot \underbrace{\varphi(u)}_{O} + \mu \cdot \underbrace{\varphi(v)}_{O} = O$

(ii) "$\Rightarrow$"
$\varphi(O) = O$, wegen Injektivität kann kein weiteres Element auf O abgebildet werden.
"$\Leftarrow$"
Angenommen es gibt $v_1, v_2 \in V$ mit $\varphi(v_1) = \varphi(v_2)$, dann ist $O = \varphi(v_1) - \varphi(v_2)$
$= \varphi(v_1 - v_2)$ (lineare Abbildung!)
$\Rightarrow v_1 - v_2 = O$ (nur O wird auf O abgebildet)
$\Rightarrow v_1 = v_2$
$\Rightarrow \varphi$ injektiv

□

5.8 Beispiel

$\varphi : \mathbb{R}^3 \to \mathbb{R}^3, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \to \begin{pmatrix} x_1 \\ 2x_1 \\ x_1 + x_2 + 2x_3 \end{pmatrix}$ ist lineare Abbildung

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}$$

$U = \langle e_2, e_3 \rangle, \quad \dim(U) = 2$

$\varphi(U),\ dim(\varphi(U)),\ ker(\varphi)$?

$$\varphi(U) = \langle \varphi(e_2), \varphi(e_3) \rangle = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle = x_3\text{-Achse}$$

$$\varphi(e_2) = \varphi(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \varphi(e_3) = \varphi(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

$\dim(\varphi(U)) = 1$

5.9 Satz

V, W K-VR, $\dim(V) = n$

$\{v_1, \ldots, v_n\}$ Basis von V
$w_1, \ldots, w_2$ Vektoren aus W (nicht notwendig verschieden)

Dann $\exists!$ lineare Abbildung

$\varphi : V \to W$ mit $\varphi(v_i) = w_i \ (i = 1, ..., n)$

und zwar:

$$\left.\begin{array}{l} \varphi : V \to W \\ v = \sum_{i=1}^{n} \lambda_i v_i \mapsto \sum_{i=i}^{n} \lambda_i w_i \end{array}\right\} *$$

D.h.: wenn man weiß, wie die Basisvektoren abgebildet werden, dann kennt man die lineare Abbildung vollständig.

Beweis

Für φ aus * gilt:

- φ ist linear
- $\varphi(v_i) = w_i$
  $\varphi(v_1) = \varphi(1 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_n) = 1 \cdot w_1 + 0 \cdot w_2 + \ldots + 0 \cdot w_n = 1 \cdot w_1 = w_1$ usw.
- φ ist eindeutig.

  Angenommen $\exists\ \psi : V \to W$ lin. Abb. mit $\psi(v_i) = w_i\ \forall i = 1 \ldots n$

  Dann ist $\psi(\sum_{i=1}^{n} \lambda_i v_i) = \sum_{i=1}^{n} \lambda_i (\psi(v_i)) = \sum_{i=1}^{n} \lambda_i w_i = \varphi(\sum_{i=1}^{n} \lambda_i v_i)$ □

5.10 Beispiel

$V = \mathbb{R}^2, \varphi$ Drehung um Winkel α $(0 \leq \alpha < 2\pi)$ um Nullpunkt gegen den Uhrzeigersinn.

φ ist lin. Abb.:
$\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2)$
$\varphi(\lambda\alpha) = \lambda\varphi(\alpha)$

$\varphi : e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$

$e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$

allg. Vektor $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\begin{aligned} \varphi : x &\mapsto x_1 \cdot \varphi(e_1) + x_2 \cdot \varphi(e_2) \\ &= x_1 \cdot \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + x_2 \cdot \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} \\ &= \begin{pmatrix} x_1 \cdot \cos\alpha - x_2 \cdot \sin\alpha \\ x_1 \cdot \sin\alpha + x_2 \cdot \cos\alpha \end{pmatrix} \\ &= A \cdot x \end{aligned}$$

mit $A = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$

5.11 Satz (Dimensionsformel)

V endl. dim. K-VR, $\varphi : V \to W$ lin. Abb.

Dann gilt:
$\dim(V) = \dim(\ker(\varphi)) + \underbrace{\mathrm{rg}(\varphi)}_{\dim(\varphi(V))}$

Beweis

Sei $u_1, ..., u_k$ Basis von $\ker(\varphi)$

Ergänze zu Basis $u_1, ..., u_n$ von V (Mathe 2, Basisergänzungssatz)

Setze $U := \langle u_{k+1}, ..., u_n \rangle$

Dann ist $\ker(\varphi) \cap U = \{O\}$,
d.h. kein Element außer O liegt in U,
also hat die Abb. $\varphi|_U$ den

$\ker(\varphi|_U) = \{O\}$,

ist damit nach Satz 5.7 (ii) injektiv.
Deshalb ist dim(U) = dum($\varphi(U)$).

Außerdem ist $\varphi(U) = \varphi(V)$
$\Rightarrow \dim(V) = \dim(\ker(\varphi)) + \underbrace{\dim(U)}_{\dim(\varphi(U))=\dim(\varphi(V))=\mathrm{rg}(\varphi)}$

□

5.12 Korollar

V, W endlich. dim. K-VR mit $\dim V = \dim W$,
$\varphi : V \to W$ lin. Abb.

Dann sind folgende Aussagen äquivalent:

(i) φ ist surjektiv

(ii) φ ist injektiv

(iii) φ ist bijektiv

Beweis

$\dim V = \dim W = n$

Nach 5.11 gilt:
$n = \dim(\ker(\varphi)) + \operatorname{rg}(\varphi)$

Also: $\underbrace{\operatorname{rg}(\varphi) = n}_{\varphi \text{ surjektiv}} \Leftrightarrow \underbrace{\dim(\ker(\varphi))}_{\varphi \text{ injektiv (Satz 5.7)}} = 0$
$\Rightarrow$ Beh. □

5.13 Zusammenhang lin. Abb. und hom. LGS, Matrizen, Rang

- homogenes LGS: $A \in M_{m,n}(K)$ gesucht:
  Menge aller $x \in K^n$ mit $Ax = O$
- lin. Abb. dazu:
  $\varphi : K^n \to K^m, x \mapsto Ax$

Dann ist der Lösungsraum des homogenen LGS = $\ker(\varphi)$