

Mathematik III - Wintersemester 14/15

2. Dezember 2014

Inhaltsverzeichnis

1	Algebraische Strukturen mit einer Verknüpfung	4
1.1	Definition: Verknüpfung	4
1.2	Beispiel	4
1.3	Definition: Halbgruppe	4
1.4	Bemerkung	4
1.5	Beispiel	5
1.6	Definition: kommutative Halbgruppe	5
1.7	Beispiel	5
1.8	Definition: Unterhalbgruppe	6
1.9	Beispiel	6
1.10	Lemma: Eins eindeutig	6
1.11	Definition: Monoid	6
1.12	Beispiele	6
1.13	Definition: Untermonoid	7
1.14	Lemma: Inverses eindeutig	7
1.15	Definition: Gruppe, Inverse, Ordnung	7
1.16	Bemerkung	7
1.17	Beispiele	7
1.18	Beispiele	8
1.19	Satz: Gleichungen lösen in Gruppen	9
1.20	Beispiel	9
1.21	Definition: Untergruppe	9
1.22	Beispiele	10
1.23	Satz und Definition: Rechtsnebenklassen	10
1.24	Beispiel	11
1.25	Lemma: Mächtigkeit von Untergruppen	11
1.26	Theorem: Satz von Lagrange	11
1.27	Definition: Potenzen	12
1.28	Satz: Potenzgesetze	12
1.29	Satz und Definition: Ordnung, zyklische Gruppe	13
1.30	Beispiel	13
1.31	Korollar	14
1.32	Beweis	14
2	Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper	14
2.1	Definition: Ring	14
2.2	Beispiel	15
2.3	Satz: Rechnen mit Ringen	15
2.4	Bemerkung	15
2.5	Definition: Körper	16
2.6	Beispiele	16
2.7	Satz: Rechnen im Körper, Nullteilerfreiheit	16
2.8	Definition: Homomorphismus, Isomorphismus	16
2.9	Beispiel	17
2.10	Satz: Chinesischer Restsatz	17
2.11	Beispiel	17

2.12	Bemerkung	18
2.13	Korollar: Phi-Funktion berechnen	18
2.14	Definition: Polynom	18
2.15	Beispiel	19
2.16	Satz und Definition: Polynomring	19
2.17	Bemerkung	20
2.18	Beispiel	20
2.19	Definition: Grad eines Polynoms	20
2.20	Satz	20
2.21	Korollar	21
2.22	Definition	21
2.23	Definition	21
2.24	Definition (Division mit Rest)	21
2.25	Beispiel	22
2.26	Korollar	22
2.27	Definition	23
2.28	Bemerkung	23
2.29	Satz (von Bezout)	23
2.30	Satz	24
2.31	Satz	24
2.32	Beispiel	24
2.33	Definition	24
2.34	Beispiel	24
2.35	Abschlussbemerkung	24
3	Der Körper der \mathbb{C} der Komplexen Zahlen	25
3.1	Definition	25
3.2	Beispiel	25
3.3	Bemerkung: komplexe Zahlenebene	26
3.4	Satz (Eigenschaften)	26
3.5	Bemerkung	26
3.6	Polarkoordinaten	27
3.7	Beispiel	27
3.8	Definition/Schreibweise	27
3.9	Bemerkung	27
3.10	Beispiele	28
3.11	Bemerkung	28
4	Wiederholung und Erweiterung der linearen Algebra aus Mathe II	28
4.1	Beispiel	28
4.2	Definition	29
5	Lineare Abbildungen	29
5.1	Definition	29
5.2	Bemerkung	30
5.3	Beispiel	30
5.4	Satz	30
5.5	Satz	31

5.6	Definition	32
5.7	Definition/Satz	32
5.8	Beispiel	32
5.9	Satz	33
5.10	34
5.11	Satz (Dimensionsformel)	34
5.12	Korollar	35
5.13	Zusammenhang lin. Abb. und hom. LGS, Matrizen, Rang	35

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

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

$a \bullet b$ 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 Multiplikationstabellen.

1.2 Beispiel

$$\begin{array}{c|cc} \bullet & a & b \\ \hline a & b & b \\ b & a & a \end{array}$$

$$(a \bullet a) \bullet a = b \bullet a = a$$

$$a \bullet (a \bullet a) = a \bullet b = b \quad \rightarrow \text{nicht assoziativ}$$

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

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:

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

1.4 Bemerkung

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

$$(a \cdot b) \cdot (c \cdot d) = ((a \cdot b) \cdot c) \cdot d = (a \cdot (b \cdot c)) \cdot d \quad (\text{usw.})$$

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) $(\mathbb{Q} \setminus \{0\}, :)$ ³ ist *keine* Halbgruppe, denn z.B. $(12 : 6) : 2 = 1$
 $12 : (6 : 2) = 4$

- c) vgl. Vorlesung Theoretische Informatik

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

$A^+ = \bigcup_{n \in \mathbb{N}} A^n$ = 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: $\lambda \cdot w = w \cdot \lambda = w \quad \forall w \in A^*$

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

- d) $M \neq \emptyset$ Menge, $\text{Abb}(M, M)$: Menge aller Abbildungen $M \rightarrow M$ mit \circ (Komposition) ist Halbgruppe.

- e) (WICHTIG)

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

Verknüpfung: $\oplus : a \oplus b := (a + b) \bmod n$
 $\odot : a \odot b := (a \cdot b) \bmod n$

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

1.6 Definition

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

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

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. $e_1 \stackrel{(**)}{=} e_1 \cdot e_2 \stackrel{(*)}{=} e_2$

□

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) $(\text{Abb}(M, M), \circ)$ Monoid, $e = \text{id}$
- c) (\mathbb{Z}_n, \oplus) Monoid, $e = 0$
 (\mathbb{Z}_n, \odot) Monoid, $e = 1$
- d) (A^*, \bullet) Monoid, $e = \lambda$ (hallo $\lambda = \lambda$ hallo = 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 $h \cdot x \stackrel{(*)}{=} e \stackrel{(**)}{=} y \cdot h$.

Dann ist $x = y$

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

□

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 $g \cdot h$: $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

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 $(\mathbb{Q} \setminus \{0\}, \bullet, 1), (\mathbb{R} \setminus \{0\}, \bullet, 1)$ 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 $n \geq 2$. $(\mathbb{Z}_n, \odot, 1)$ ist Monoid aber keine Gruppe.

Wann ist ein Element aus \mathbb{Z}_n invertierbar bezüglich \odot ?

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

also sind nur zu n teilerfremde Elemente invertierbar!

(vgl. $(\mathbb{Z}_6, 0, 1)$: 0, 2, 3, 4 nicht invertierbar, 1, 5 invertierbar)

Bezeichnung:

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

ist Gruppe bezüglich \odot (vgl. Bemerkung ??) mit Ordnung $|\mathbb{Z}_n^*| = \varphi(n)$ ("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 ($\text{ggT}(z, n) = 1$) 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, $\text{ggT}(8, 5) = 1$

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

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

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

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

Bsp: $n = 2$

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

$n = 3$

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

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

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

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

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 $ax = bx$ für ein $x \in G$, dann gilt $a = b$ (Kürzungsregel)

Beweis. (i) • $x = a^{-1}$ ist Lösung (prüfe $ax = b$):

$$a \cdot \underbrace{a^{-1}b}_x \stackrel{\text{AG}}{=} (a \cdot a^{-1}) \cdot b = e \cdot b = b$$

- Es gibt genau eine Lösung:

$$\text{Es gelte } ax = b$$

$$\Rightarrow x = ex = (a^{-1}a)x \stackrel{\text{AG}}{=} a^{-1}(ax) = a^{-1}b$$

(ii) analog

(iii) Multipliziere von rechts mit x^{-1}
links y^{-1}

□

1.20 Beispiel

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

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

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

1.21 Definition

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

U heißt *Untergruppe* von G ($U \leq G$), 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) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

b) $(\{-1, 1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$

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

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

1.23 Satz und Definition

G Gruppe, $U \leq G$

- (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. $x \cdot z^{-1} \in U$)

$$x \cdot z^{-1} = x e z^{-1} = x (y^{-1} y) z^{-1} = \underbrace{(x \cdot y^{-1})}_{\in U} \cdot \underbrace{(y \cdot z^{-1})}_{\in U} \in U, \text{ also } x \sim z. \quad \square$$

- (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 $Ux \cap Uy = \emptyset$

Beweis

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

$$(b) \text{ Sei } y \in Ux, \text{ dann zeige: } x \sim y$$

$$y \in Ux \Rightarrow y = u \cdot x \text{ für ein } u \in U$$

$$\Rightarrow x \cdot y^{-1} = x \cdot (ux)^{-1} = x \cdot x^{-1} \cdot u^{-1} = u^{-1} \in U$$

Es wurde gezeigt, dass $x \sim y$ gilt.

□

1.24 Beispiel

$$G = (\mathbb{Z}, +), 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$$

$$U = (3\mathbb{Z}, +) \leq G \text{ (ÜA, Blatt 2)}$$

Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$.

$$x \sim y \Leftrightarrow x \cdot y^{-1} \in U$$

bzw.: $x - y \in U$

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

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

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

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

...

1.25 Lemma

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

Dann ist $|U| = |Ux|$

Beweis

$$\text{Abb } \varphi : U \rightarrow Ux$$

$$u \mapsto ux$$

ist surjektiv und injektiv (falls $u_1x = u_2x$, 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, $U \leq G$

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, \dots, Ux_q die q verschiedenen Rechtsnebenklassen von U in G

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

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

1.27 Definition

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

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

(Potenzen von a)

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

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

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

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

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

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

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

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

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* $o(g)$ von G
- (ii) Die Menge $\{g^0 = e, g^1 = g, g^2, \dots, g^{n-1}\}$ ist eine Untergruppe von G , die von g erzeugte zyklische Gruppe $\langle g \rangle$
Es gilt $o(g) = |\langle g \rangle| = n$ 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 $g^{i-j} \stackrel{1.28ii)}{=} g^i \cdot g^{-j} \stackrel{1.28}{=} \underbrace{g^i}_{=g^j} \cdot (g^j)^{-1} = e$
- (ii) Das Produkt zweier Elemente aus $\langle g \rangle$ liegt wieder in $\langle g \rangle$
Neutrales Element ist $g^0 = e$
Inverses Element zu g^i ist $(g^i)^{-1} = g^{n-i}$
 $\Rightarrow \langle g \rangle \leq G$
- (iii) Satz von Lagrange (1.26): $n = o(g) = |\langle g \rangle| \mid |G|$
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

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

$g = 1$: $\langle 1 \rangle = \{g^0 = 1^0 = 1\}$, $o(1) = 1$

$g = 2$: $\langle 2 \rangle = \{g^0 = 1, g^1 = 2\}$, $o(2) = 2$

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

$g = 2$: $\langle 2 \rangle = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3\}$, $o(2) = 4$

1.31 Korollar

(i) Satz von Euler

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

Dann ist

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

(ii) Kleiner Satz von Fermat

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

$$a^{p-1} \equiv 1 \pmod{p}$$

1.32 Beweis

- a) Wir können annehmen, dass $1 \leq a < n$ (denn $a^{\varphi(n)} \pmod{n} = (a \pmod{n})^{\varphi(n)}$)
wegen $\text{ggT}(a, n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist eine endliche Gruppe.

$$\begin{aligned} \stackrel{?(iii)}{\Rightarrow} a^{|\mathbb{Z}_n^*|} &= 1 (= e) & a \odot a \odot \dots \\ \Rightarrow a^{\varphi(n)} &\equiv 1 \pmod{n} & a \cdot a \cdot \dots \end{aligned}$$

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

2 Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper

2.1 Definition

Sei $R \neq \emptyset$ eine Menge mit zwei Verknüpfungen $+$ und \cdot .

- (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 $a \in R$ Inverse mit $-a$
(schreibe auch $a - b$ für $a + (-b)$).

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

- (c) Es gelten die Distributivgesetze:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) = ab + ac \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) = ac + bc \quad \forall a, b, c \in R \end{aligned}$$

- (ii) Ein Ring $(R, +, \cdot)$ heißt *kommutativ* falls \cdot ebenfalls kommutativ ist, also falls $\forall a, b \in R : a \cdot b = b \cdot a$
- (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
 $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
- 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, \dots, R_n Ringe, dann $R_1 \times \dots \times R_n$ 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) $a \cdot 0 = a \cdot (0 + 0) \stackrel{2.1(3)}{=} a \cdot 0 + a \cdot 0$
 addiere $-(a \cdot 0)$ (Inverses von $a \cdot 0$) auf beiden Seiten, erhalte $0 = a \cdot 0$
 Analog $0 \cdot a = 0$
- (ii) $(-a) \cdot b + a \cdot b \stackrel{2.1(3)}{=} (-a + a) \cdot b = 0 \cdot b \stackrel{(i)}{=} 0$
 also ist $(-a \cdot b)$ Inverses zu $a \cdot b$, also $= -(a \cdot b)$.
 Analog $a \cdot (-b) = -(a \cdot b)$
- (iii) $(-a) \cdot (-b) \stackrel{(ii)}{=} -(a \cdot (-b)) \stackrel{(ii)}{=} -(-(a \cdot b)) = a \cdot b$

□

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

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

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)

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

□

2.8 Definition

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

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

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

2.9 Beispiel

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

2.10 Satz (Chinesischer Restsatz)

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

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

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

Beweis

Für jedes $i \in \{1, \dots, n\}$ 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

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

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

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

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

$$\text{b) Was ist } 2^{1000} \bmod \underbrace{1155}_{3 \cdot 5 \cdot 7 \cdot 11}$$

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

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

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

Der chinesische Restsatz liefert $x = 331$

2.12 Bemerkung

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

$$\text{Durch } \psi : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ x \mapsto (x \bmod m_1, \dots, x \bmod m_n)$$

wird ein Ringisomorphismus 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:

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

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

2.13 Korollar

$M = m_1 \cdots m_n$, m_i paarweise teilerfremd.

Dann ist $\varphi(M) = \varphi(m_1) \cdots \varphi(m_n)$, insbesondere:

$$n = p_1^{a_1} \cdots p_k^{a_k} \quad (p_i \text{ Primzahlen, } a_1 > 0, p_i \neq p_j \text{ für } i \neq j)$$

Beweis

Nach 2.12 ist $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ mittels ψ

$$\Rightarrow x \text{ Einheit} \Leftrightarrow \psi(x) = (x \bmod m_1, \dots, x \bmod m_n) \text{ Einheit}$$

$$\Leftrightarrow x \bmod m_i \text{ Einheit } \forall i = 1 \dots n$$

$$\Rightarrow \varphi(M) = \varphi(m_1) \cdots \varphi(m_n)$$

$$\varphi(p^a) \underbrace{=}_{\text{Überlegen}} p^a - p^{a-1} = p^{a-1}(p-1)$$

Überlegen

2.14 Definition

Sei K Körper mit Nullelement 0 und Einselement 1:

(i) Ein *Polynom über K* ist Ausdruck $f = a_0x^0 + a_1x^1 + \cdots + a_nx^n$, $n \in \mathbb{N}_0, a_i \in K$.
 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_0x^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 ($f = a_0 + a_1 x^1 + \dots + a_n x^n$, $g = b_0 + b_1 x^1 + \dots + b_m x^m$, $a_n \neq 0, b_m \neq 0$ und $n = m$, $a_i = b_i$ für $i = 0, \dots, n$) 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

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

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

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

(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* $a_0, ax, a_2x^2, \dots, a_nx^n$

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

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

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

$\text{Grad}(0) := -\infty$

$\text{Grad}(f) = 0$ für konstante Polynome $\neq 0$

2.20 Satz

K Körper, $f, g \in K[x]$

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

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

Beweis

Stimmt für $f = 0$ oder $g = 0$

$$\begin{aligned} f &= a_0 + a_1x^1 + \dots + a_nx^n && \text{mit } a_n \neq 0 \\ g &= b_0 + b_1x^1 + \dots + b_mx^m && \text{mit } b_m \neq 0 \\ f \cdot g &= (\dots) \cdot (\dots) = \dots + \underbrace{(a_nb_n)}_{\neq 0} \cdot x^{n+m} \\ &&& \text{(siehe Satz 2.7 Nullteilerfreiheit in Körpern)} \end{aligned}$$

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 $b \in K$

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

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:

$$r =: g \bmod f$$

$$q =: g \text{ div } f$$

Beweis

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

2.25 Beispiel

a)

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

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

Rechne:

$$\begin{array}{r} (x^4 + 2x^3 - x + 2) : (3x^2 - 1) = \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} + \frac{-\frac{1}{3}x + \frac{19}{9}}{3x^2 - 1} \\ \underline{-x^4} + \frac{1}{3}x^2 \\ 2x^3 + \frac{1}{3}x^2 - x \\ \underline{-2x^3} \phantom{+ \frac{1}{3}x^2} + \frac{2}{3}x \\ \frac{1}{3}x^2 - \frac{1}{3}x + 2 \\ \underline{-\frac{1}{3}x^2} \phantom{- \frac{1}{3}x} + \frac{1}{9} \\ -\frac{1}{3}x + \frac{19}{9} \end{array}$$

b)

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

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

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

$$f = q \cdot (x - a) \Rightarrow f(a) = q(a) \cdot \underbrace{(a - a)}_0 = 0 \quad q \in K$$

" \Leftarrow " 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 ($f = \text{ggT}(g, h)$), 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 ($f = \text{kgV}(g, h)$), 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 $a_n^{-1} f = x^n + \dots$ 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 $\mathbb{Z}_{11}[x] : \underbrace{4}_4 f = x^2 + 4x_6$ normiert.

Inverses von 3, denn $3 \cdot 4 = 12 \equiv 1 \pmod{11}$

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

$$\text{sei } f_1 = \text{kgV}(g, h), f_2 = \text{kgV}(g, h)$$

$$\Rightarrow g, h | f_1, \quad g, h | f_2$$

$$\Rightarrow g, h | (f_1 - f_2)$$

- c) $\text{ggT}(g, h)$ 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 $a \in K \setminus \{0\}$ 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, \dots, p_e und natürlichen Zahlen $m_1, \dots, m_e \in \mathbb{N}$ mit $f = a_n \cdot p_1^{m_1} \cdot \dots \cdot p_e^{m_e}$

- 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 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 , $x = \operatorname{Re} z$
 y heißt Imaginärteil, $y = \operatorname{Im} z$.

Die Menge aller komplexen Zahlen bezeichnen wie mit \mathbb{C} und definieren auf \mathbb{C} Addition und Multiplikation wie folgt:

Für $z = x + iy$ und $w = a + ib$ ist

$$z + w := (x + a) + i(y + b),$$

$$z - w := (x - a) + i(y - b) \text{ und}$$

$$z \cdot w := (xa - yb) + i(xb + ya).$$

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

Man nennt für $z = x + iy$ die Zahl $\bar{z} = x - iy$ 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 $\operatorname{Re}(z) = 2$ und $\operatorname{Im}(z) = 3$.

$$\bar{z} = 2 - 3i, |z| = \sqrt{2^2 + 3^2} = \sqrt{13}$$

$$z \cdot \bar{z} = (2 + 3i) \cdot (2 - 3i)$$

$$= 4 - 6i + 6i - 9i^2 = 4 + 9 = 13$$

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

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

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

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)

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

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

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

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

$$\text{e) } |w \cdot z| = |w| \cdot |z|$$

$$\text{f) } |w + z| \leq |w| + |z| \text{ (Dreiecksungleichung)}$$

$$|w + z| \geq \left| |w| - |z| \right|$$

Beweis

z.B.: d) sei $z = x + iy \quad x, y \in \mathbb{R}$

$$\Rightarrow \overline{z} = x - iy, \quad |z| = \sqrt{x^2 + y^2}$$

$$|\overline{z}| = \dots$$

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) Man 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 $r \geq 0$ und ein $\varphi \in \mathbb{R}$ mit

$z = r(\cos \varphi + i \cdot \sin \varphi)$ (Polarkoordinatendarstellung von z) und zwar ist $r = |z| = \sqrt{x^2 + y^2}$
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):

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

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 Definition 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

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

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

3.10 Beispiele

- a) $1 \cdot e^{i \cdot 0} = 1$
- b) $e^{i\pi} = -1$ (und: $e^{i\pi} + 1 = 0 \odot$)
- c) $2 \cdot e^{2\pi} = 2$
- d) \dots

3.11 Bemerkung

\mathbb{C} hat alle algebraischen und analytischen 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: $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
 $\mathcal{O} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, d.h. $-\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
 $\forall v \in V : 0 \cdot v = \mathcal{O} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $1 \cdot v = v$
- b) $K = \mathbb{Z}_5, V_2 = \mathbb{Z}_5^3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \right\}$
 $v = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, w = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \in \mathbb{Z}_5^3$
 $-v = \begin{pmatrix} 0 \\ 4 \\ 3 \end{pmatrix}, -w = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, v + w = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$
 $1 \cdot w = w, 2 \cdot w = \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, 3 \cdot w = \dots$
 $|V| = 5 \cdot 5 \cdot 5 = 125$
- 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. $u_1 \oplus u_2 = 0$

$$\Rightarrow \text{für } \lambda \cdot u = \begin{pmatrix} \lambda u_1 \\ \lambda u_2 \end{pmatrix} \text{ gilt } \lambda u_1 \oplus \lambda u_2 = \lambda \cdot \underbrace{(u_1 \oplus u_2)}_0 = 0$$

d) \mathbb{Z}_3^3 :

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

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 α, β, γ 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:

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

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

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) $\varphi : V \rightarrow W$ 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 $\varphi : V \rightarrow W$ bijektiv, so heißt φ *Isomorphismus*, V und W heißen dann *isomorph*, $V \cong W$.

5.2 Bemerkung

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

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

5.3 Beispiel

- Nullabbildung:
 $\varphi : V \rightarrow W, v \mapsto O$
- $\varphi : V \rightarrow V, v \mapsto \lambda v$ für jedes festes $\lambda \in K$ ist lineare Abbildung ($\lambda = 1 : \varphi = \text{id}_V$)
- $\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}^3, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ -x_3 \end{pmatrix}$ ist eine lineare Abbildung (Spiegelung an x_1, x_2 -Ebene)
- $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} (x_1)^2 \\ x_2 \end{pmatrix}$ 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 $\varphi : K^n \rightarrow K^m, x \mapsto Ax$

eine lineare Abbildung

Beweis

folgt aus Rechenregeln für Matrizen:

$$\begin{aligned}\varphi(x + y) &= A(x + y) = Ax + Ay \\ &= \varphi(x) + \varphi(y)\end{aligned}$$

$$\begin{aligned}\varphi(\lambda \cdot x) &= A(\lambda x) = \lambda Ax \\ &= \lambda \varphi(x)\end{aligned}$$

□

Alle bisherigen Beispiele waren von dieser Form!

5.3

a) $A = 0 = \text{Nullmatrix}$

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 (\rightarrow später):

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

5.5 Satz

$\varphi : V \rightarrow W$ 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, \dots, v_k Basis von U
 $\Rightarrow \varphi(u_1), \dots, \varphi(u_k)$ ist Erzeugendensystem von $\varphi(U)$
 \Rightarrow enthält Basis (Mathe II)
 \Rightarrow Behauptung

□

5.6 Definition

$\varphi : V \rightarrow W$ lineare Abbildung, V endlich dimensional

Dann heißt die $\dim(\varphi(V))$ der Rang von φ , $\text{rg}(\varphi)$.

5.7 Definition/Satz

$\varphi : V \rightarrow W$ 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) $\varphi : \text{injektiv} \Leftrightarrow \ker(\varphi) = \{O\}$

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

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

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

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

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

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

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

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

5.9 Satz

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

$\{v_1, \dots, v_n\}$ Basis von V

w_1, \dots, w_n Vektoren aus W (nicht notwendig verschieden)

Dann $\exists!$ lineare Abbildung

$$\varphi : V \rightarrow W \text{ mit } \varphi(v_i) = w_i \quad (i = 1, \dots, n)$$

und zwar:

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

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

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

$$\text{Dann ist } \psi\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i (\psi(v_i)) = \sum_{i=1}^n \lambda_i w_i = \varphi\left(\sum_{i=1}^n \lambda_i v_i\right) \quad \square$$

5.10 Beispiel

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

φ ist lin. Abb.:

$$\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2)$$

$$\varphi(\lambda\alpha) = \lambda\varphi(\alpha)$$

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

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

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

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

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

5.11 Satz (Dimensionsformel)

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

Dann gilt:

$$\dim(V) = \dim(\ker(\varphi)) + \underbrace{\text{rg}(\varphi)}_{\dim(\varphi(V))}$$

Beweis

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

Ergänze zu Basis u_1, \dots, u_n von V (Mathe 2, Basisergänzungssatz)

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

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

Außerdem ist $\varphi(U) = \varphi(V)$

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

□

5.12 Korollar

V, W endlich. dim. K -VR mit $\dim V = \dim W$,
 $\varphi : V \rightarrow W$ 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:

$$n = \dim(\ker(\varphi)) + \operatorname{rg}(\varphi)$$

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

\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 $Ax = \mathcal{O}$
- lin. Abb. dazu:
 $\varphi : K^n \rightarrow K^m, x \mapsto Ax$

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