

Mitschriften der Vorlesung: “Lineare Algebra I”

von Prof G. Hein an der Universität Duisburg-Essen, Campus Essen

Inhaltsverzeichnis

1	Lineare Gleichungssysteme im \mathbb{R}^n	2
1.1	Die Vektorräume $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^3, \dots, \mathbb{R}^n$	2
1.1.1	\mathbb{R} – Der Körper der reellen Zahlen	2
1.1.2	\mathbb{R}^2 – Die reelle Ebene	3
1.2	Lineare Unabhängigkeit	6
1.3	Das Gaußsche Eliminationsverfahren	7
2	Mengen, Gruppen, Ringe und Körper	12
2.1	Mengen	12
2.2	Gruppen	16
2.3	Gruppenhomomorphismen	18
2.4	Nebenklassen, Normalteiler, Signum	19
2.5	Erzeuger und die Ordnung	25
2.6	Ringe und Körper	27
2.7	Der euklidische Algorithmus	30
2.8	\mathbb{C} – Der Körper der komplexen Zahlen	33
3	Anhang	34
3.1	Literaturangaben	34
3.2	Begriffserklärungen	34

Mitgeschrieben von Johannes Hölken unter verwendung von L^AT_EX
Online auf www.uni.johoelken.de – Fehlermeldungen: uni@johoelken.de

1 Lineare Gleichungssysteme im \mathbb{R}^n

1.1 Die Vektorräume $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^3, \dots, \mathbb{R}^n$

1.1.1 \mathbb{R} – Der Körper der reellen Zahlen

$$\begin{aligned}\mathbb{R}^n &= \text{Abb.}(\{1, \dots, n\}, \mathbb{R}) \\ &= \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R}\}\end{aligned}$$

Addition auf \mathbb{R}^n

$$x, y \in \mathbb{R}^n$$

$z = x + y$ ist definiert durch $[:=] z_i = x_i + y_i$,

wobei $x_i = \{x_1, \dots, x_n\}$; $y_i = \{y_1, \dots, y_n\}$ und $z_i = \{z_1, \dots, z_n\}$

Beispiel 1.1:

$$\begin{aligned}P_0 &= (2, 3); P_1 = (-3, -4) \\ P_0 + P_1 &= (-1, -1)\end{aligned}$$

Skalarmultiplikation auf \mathbb{R}^n

$$\lambda \in \mathbb{R}, x \in \mathbb{R}^n$$

$y = \lambda x$ ist definiert durch $[:=] y_i = \lambda x_i$

Es gilt offensichtlich für $x, y, z \in \mathbb{R}^n$; $\lambda, \mu \in \mathbb{R}$:

$$\begin{aligned}x + y &= y + x \\ (x + y) + z &= x + (y + z) \\ \lambda(x + y) &= \lambda \cdot x + \lambda \cdot y \\ (\lambda + \mu)x &= x \cdot \mu + x \cdot \lambda \\ (\lambda \cdot \mu)x &= \lambda(\mu \cdot x)\end{aligned}$$

Beispiel 1.2:

$$(-2) \cdot P_0 = (-2) \cdot (2, 3) = (-4, -6)$$

Schreibweise

$$0 \in \mathbb{R}^n \quad 0 := (0, \dotscolor, 0)$$

$$x, y \in \mathbb{R}^n \quad -x := (-1) \cdot x$$

$$\text{Es gilt: } x + (-x) = 0$$

$$x - y = x + (-y)$$

1.1.2 \mathbb{R}^2 – Die reelle Ebene

Die reelle Ebene \mathbb{R}^2 nennt man auch die x_1, x_2 bzw. x, y -Ebene
 $x \in \mathbb{R}^2$ x – Punkt oder Vektor

Geraden – Parameterform

Def. 1.1: Ein Richtungsvektor (R.V.) in \mathbb{R}^2 ist ein Vektor x mit $x \neq 0$

Def. 1.2: Eine Gerade (L) in \mathbb{R}^2 ist eine Menge von der Form:
 $L = \{x + \lambda y \mid \lambda \in \mathbb{R}\}$, wobei x und $y \in \mathbb{R}^2$ beliebige aber feste Richtungsvektoren sind.

Ist $L = \{x + \lambda y\}$ so nennt man dies eine *Parameter Beschreibung*.
(λ – Parameter, x – Stützpunkt, y – Richtungsvektor (R.V.))
In dieser Darstellung ist L das Bild der Abbildung $\varphi : \mathbb{R} \rightarrow \mathbb{R}^2$

Beispiel 1.3:

Die Gerade $L = \{(2, 0) + \lambda(1, 1) \mid \lambda \in \mathbb{R}\}$ ist gleich mit
 $G = \{(3, 1) + \lambda(\sqrt{2}, \sqrt{2}) \mid \lambda \in \mathbb{R}\}$
 \Rightarrow Die *Parameterdarstellung* ist nicht eindeutig!

LEMMA 1.1: Schneiden sich zwei Geraden L und L' in mehr als einem Punkt, dann gilt $L = L'$

Beweis: Sei $L = \{x + \lambda y \mid \lambda \in \mathbb{R}\}$ und $L' = \{x' + \mu y' \mid \mu \in \mathbb{R}\}$,
sei $z_1 \in L$ und $z_1 \in L'$ und sei $z_2 \in L$ und $z_2 \in L'$ mit $z_1 \neq z_2$

(i) $z_1 = x + \lambda_1 \cdot y$

(ii) $z_1 = x' + \mu_1 \cdot y'$

(iii) $z_2 = x + \lambda_2 \cdot y$

(iv) $z_2 = x' + \mu_2 \cdot y'$ mit $\lambda_1 \neq \lambda_2$ und $\mu_1 \neq \mu_2$

$$\vartheta = \frac{\lambda_1 - \lambda_2}{\mu_1 - \mu_2}$$

aus (i) und (ii) $x + \lambda_1 \cdot y = x' + \mu_1 \cdot y'$ (v)

aus (iii) und (iv) $x + \lambda_2 \cdot y = x' + \mu_2 \cdot y'$ (vi)

aus $\frac{(v)}{(vi)}$ $y(\lambda_1 - \lambda_2) = y'(\mu_1 - \mu_2)$

\Leftrightarrow $\vartheta \cdot y = y'$

aus (v) $x' = x + \lambda_1 \cdot y - \mu_1 \cdot y'$ $|y' = \vartheta \cdot y$
 $= x + \lambda_1 \cdot y - \mu_1 \cdot \vartheta \cdot y$
 $= x + (\lambda_1 - \mu_1 \cdot \vartheta) y$

$z' \in L'$ beliebig $\exists \mu' \in \mathbb{R}$

$$\begin{aligned}
z' &= x' + \mu' \cdot y' & | & \quad x' = x + (\lambda_1 - \mu_1 \cdot \vartheta) y \\
&= x + (\lambda_1 - \mu_1 \cdot \vartheta) y + \mu' \cdot y' & | & \quad y' = \vartheta \cdot y \\
&= x + (\lambda_1 - \mu_1 \cdot \vartheta) y + \mu' \cdot \vartheta \cdot y \\
&= x + (\lambda_1 - \mu_1 \cdot \vartheta + \mu' \cdot \vartheta) \cdot y \\
\Rightarrow z' \in L & \Rightarrow L' \subseteq L \text{ und analog: } L \subseteq L' \\
\Rightarrow L &= L'
\end{aligned}$$

q.e.d.

SATZ 1.1: Seien z_1 und z_2 zwei verschiedene Punkte im \mathbb{R}^2
so existiert genau eine Gerade (L) durch z_1 und z_2 .

Beweis: $y = z_1 - z_2 \neq 0$
 $L = \{z_1 + \lambda \cdot y \mid \lambda \in \mathbb{R}\}$
 $\lambda = 0 \Rightarrow z_1 \in L \quad \wedge \quad \lambda = 1 \Rightarrow z_2 \in L$
Wäre L' eine weitere Gerade, die z_1 und z_2 enthält, dann folgt nach
LEMMA 1.1 $L = L'$.

q.e.d.

Schnittpunkt zweier Geraden

Beispiel 1.4:

$$\begin{aligned}
L &= \{(2, 0) + \lambda(1, 1) \mid \lambda \in \mathbb{R}\} \\
L' &= \{(3, 3) + \mu(2, 1) \mid \mu \in \mathbb{R}\} \\
\text{Sei } z &\in L \cap L' \\
(2, 0) + \lambda(1, 1) &= z = (3, 3) + \mu(2, 1) & | & \text{Skalarmultiplikation} \\
\Leftrightarrow (2 + \lambda, \lambda) &= (3 + 2\mu, 3 + \mu) \\
\Leftrightarrow 2 + \lambda &= 3 + 2\mu & (i) \\
\wedge \quad \lambda &= 3 + \mu & (ii) \\
(i) - (ii): \Rightarrow 2 &= \mu \\
\text{d.h. } (3, 3) + 2(2, 1) &= (7, 5)
\end{aligned}$$

Beispiel 1.5:

$$\begin{aligned}
L &= \{(2, 0) + \lambda(1, 1) \mid \lambda \in \mathbb{R}\} \\
L' &= \{(3, 2) + \mu(2, 2) \mid \mu \in \mathbb{R}\} \\
\text{Sei } z &\in L \cap L' \\
\text{Analog zu Beispiel 1.4 kommen wir zu einem linearen Gleichungssystem (LGS):} \\
2 + \lambda &= 3 + 2\mu & (i) \\
\lambda &= 2 + 2\mu & (ii) \\
(i) - (ii) \Rightarrow 2 &= 1 & \text{falsch!} \\
\text{Schneiden sich zwei Geraden nicht, so nennt man sie auch parallel.}
\end{aligned}$$

Bemerkung: $L \cap L'$ kann folgendes sein:

- Eine leere Menge $\{\emptyset\}$
- Ein Punkt
- $L = L'$, wenn mehr als ein Schnittpunkt (*siehe* LEMMA 1.1)

Die Geradengleichung

Def. 1.3: Eine Gerade (L) ist die Lösungsmenge einer linearen Gleichung. $L = \{(x_1, x_2) | a_1x_1 + a_2x_2 = b\}$, mit (a_1, a_2) fix und $(a_1, a_2) \neq 0$ Diese Definition ist korrekt. D.h. gleichbedeutend mit Def. 1.2.

Nachweis: Sei L in Parameterform gegeben:

$$L = \{(x_1, x_2) + \lambda(y_1, y_2) | \lambda \in \mathbb{R}\}$$

Behauptung: Es gilt $L = \{(X_1, X_2) | y_2X_1 - y_1X_2 = y_2x_1 - y_1x_2\}$

$$X_1 = x_1 + \lambda \cdot y_1$$

$$X_2 = x_2 + \lambda \cdot y_2$$

$\Rightarrow (X_1, X_2)$ erfüllt die Geradengleichung.

Ohne Beschränkung der Allgemeinheit (O.B.d.A.) sei angenommen, dass $y_2 \neq 0$ ist und (X_1, X_2) die Geradengleichung erfüllen, dann ist:

$$\begin{aligned} X_1 &= \frac{y_1 X_1}{y_2} = \frac{1}{y_2} \cdot (y_2 x_1 - y_1 x_2) \\ &= x_1 + \frac{y_1 X_1 - y_1 x_2}{y_2} \\ &= x_1 + \frac{y_1 (X_1 - x_2)}{y_2} = x_1 + \frac{X_1 - x_2}{y_2} \cdot y_1 \end{aligned}$$

(X_1, X_2) erfüllt die Geradengleichung.

$$\begin{aligned} (X_1, X_2) &= (x_1, x_2) + (X_1 - x_1, X_2 - x_2) \\ &= (x_1, x_2) + \left(\frac{X_1 - x_2}{y_2} \cdot y_1, X_2 - x_2\right) \\ &= (x_1, x_2) + \frac{X_1 - x_2}{y_2} (y_1, y_2) \end{aligned}$$

Sei L durch $L = \{(x_1, x_2) | a_1x_1 + a_2x_2 = b\}$ gegeben.

Sei o.B.d.A. $a_1 \neq 0$

$$(X_1, X_2) \in L \Leftrightarrow x_1 = \frac{b - a_2 x_2}{a_1} = \lambda$$

dann folgt daraus:

$$L = \left\{ \left(\frac{b}{a_1}, 0\right) + \lambda \left(\frac{-a_2}{a_1}, 1\right) \mid \lambda \in \mathbb{R} \right\}$$

q.e.d.

1.2 Lineare Unabhängigkeit

Def. 1.4: Seien x_1, \dots, x_m Vektoren im \mathbb{R}^n
nennen wir diese Vektoren linear Unabhängig, genau dann wenn
aus:

$$\sum_{i=1}^m a_i \cdot x_i = 0 \quad \Rightarrow \quad a_i := a_1 = \dots = a_m = 0$$

Beispiel 1.6: $x_1 := (1, 1)$
 $x_2 := (2, 1)$
 $x_3 := (3, 2)$
Es gilt: $1 \cdot x_1 + 1 \cdot x_2 + (-1) \cdot x_3 = 0$
 $\Rightarrow x_1, x_2$ und x_3 sind linear Abhängig.

Beispiel 1.7: $x_1 := (1, 1)$
 $x_2 := (2, 1)$
ist: $a_1 \cdot x_1 + a_2 \cdot x_2 = 0$ | Skalarmultiplikation
 $\Rightarrow (a_1, a_1) + (2a_2, a_2) = 0$
 $\Rightarrow a_1 + 2a_2 = 0$ | (i)
 $\wedge a_1 + a_2 = 0$ | (ii)
(i) - (ii) $\Rightarrow a_2 = 0$ | (iii)
(ii) - (iii) $\Rightarrow a_1 = 0$
 $\implies a_1 = a_2 = 0$

Bemerkung: Ist $x_1 = 0$ so ist jeder m - Tupel linear Abhängig
 $a_1 = 1$; $a_2 = a_3 = \dots = a_m = 0$

$$\sum_{i=1}^m a_i \cdot x_i = 0$$

„Zwei Vektoren heißen linear unabhängig, wenn beide von 0 verschieden sind und auf unterschiedlichen Geraden durch den 0-Punkt liegen.“

1.3 Das Gaußsche Eliminationsverfahren

Def. 1.5: 1. Eine lineare Gleichung (LG) mit den Unbekannten: x_1, \dots, x_n ist eine Gleichung der Form:

$$\sum_{i=1}^n a_i x_i = b$$

d.h: ($a_1 x_1 + a_2 x_2 + \dots + a_n x_n = b$).

2. Ein Lineares Gleichungssystem (LGS) mit den Unbekannten: x_1, \dots, x_n ist eine Menge von m LGS.

Beispiel 1.8:

$$1x_1 + 3x_2 = 7 \quad (1)$$

$$2x_1 + 7x_2 = 8 \quad (2)$$

$$(1) - (2) \Rightarrow \quad x_2 = -6$$

Schreib:

$$\begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$$

(*Matritzenschreibweise eines LGS*)

Verallgemeinert sieht das ganze dann so aus:

$$\sum_{i=1}^n a_{ji} x_{ji} = b_j; j = 1, \dots, m$$

dieses LGS schreiben wir:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1n} \\ a_{2,1} & a_{2,2} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{mi} & a_{mi} & \dots & a_{jn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

Beispiel. 1.9:

$$\begin{pmatrix} 1 & 2 & 3 & 8 & 1 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Man kann den treppenartigen Verlauf der “Nullen” in diesem Beispiel sehr gut erkennen. Diese Form eines LGS nennen wir “Zeilenstufenform”.

Schreibe man die Variablen unter eine jede Spalte so nennt man die Variablen unter jedem Absatz gebundene – , die anderen freie Variablen.

In unserem Beispiel wären x_1, x_3 sowie x_4 gebundene Variablen, x_2 und x_5 hingegen wären freie Variablen.

daraus ergibt sich:

$$x_4 = 3 + x_5 \tag{3}$$

$$x_3 = 2 - 2x_5 \tag{4}$$

$$\begin{aligned} x_1 &= 1 - 2x_2 - 3x_3 - 8x_4 - x_5 && | \text{Zeile 1} \\ &= 1 - 2x_2 - 3(2 - 2x_5) - 8(3 + x_5) - x_5 && | \text{einsetzen von (3) und (4)} \\ &= -29 - 2x_2 - 5x_5 \end{aligned}$$

⇒ Die Lösungsmenge ist gegeben durch das Bild $\mathbb{R}^2 \rightarrow \mathbb{R}^5$

Wähle: $\lambda = x_2 \wedge \mu = x_5$, dann ergibt sich aus Zeile 1:

$(\lambda, \mu) \mapsto (-29 - 2\lambda - 5\mu, \lambda, 2 - 2\mu, 3 + \mu, \mu)$ Bemerkung: Es ist leicht ein LGS in dieser Zeilenstufenform (Z.St.F.) zu lösen. Die Kunst besteht darin es in o.g. Form umzustellen.

Def. 1.6: Zeilenstufenform (Z.St.F.)

eine $m \times n$ - Matrix mit reellen Koeffizienten ist eine Menge

$\{a_{ji} | a_{ji} \in \mathbb{R}\}$ mit $i = 1 \dots m; j = 1 \dots n$

(m - Zeilen der Matrix und n - Spalten der Matrix)

$$A = \{a_{ji}\} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_{n'} \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \rightarrow A \cdot x = b$$

Die Matrix A ist in Zeilenstufenform, wenn

- $\exists r \in \mathbb{N}$, so dass
 - $\forall k > r$ gilt: die k te Zeile von A enthält nur Nullen
 - $\forall k \leq r$ gilt: die k te Zeile von A enthält nicht nur Nullen
- $\forall k \leq r \quad i_k := \min \{i | a_{ik} \neq 0\}$
- $i_1 < i_2 < \dots < i_r$

LEMMA: 1.2

Sei A eine $m \times n$ - Matrix (lies: m kreuz n) und $A \cdot x = b$ ein LGS.

Lösungsmenge (Lös.) $(A, b) = \{x = \begin{pmatrix} x_1 \\ \vdots \\ x_{n'} \end{pmatrix} | A \cdot x = b\}$.

1. Sei A' eine Matrix, die durch vertauschen zweier Zeilen aus A entsteht
 \rightarrow Lös. $(A', b') =$ Lös. (A, b) , wobei b' durch Vertauschen der selben Spalten aus b entsteht.
2. Sei $\lambda \in \mathbb{R}$; A' entsteht aus A durch Ersetzen der i ten Zeile durch die l te Zeile $+ \lambda \cdot (i$ te - Zeile) und b' entsteht analog für $i \neq l$.
 $b'_i = b_i + \lambda \cdot b_l \rightarrow$ Lös. $(A', b') =$ Lös. (A, b) .

Beweis:

1. trivial, da die Reihenfolge der Gleichungen egal ist.

2.

$$\begin{aligned}
 & \sum_{k=1}^n a_{i,k}x_k = b_i \quad \wedge \quad \sum_{k=1}^n a_{j,k}x_k = b_j \\
 \Rightarrow & \sum_{k=1}^n a_{i,k}x_k = b_i \wedge \sum_{k=1}^n a_{j,k}x_k = b_j \wedge \left(\sum_{k=1}^n a_{i,k}x_k \right) + \lambda \cdot \left(\sum_{k=1}^n a_{j,k}x_k \right) = b_i + \lambda b_j \\
 \Rightarrow & \left(\sum_{k=1}^n (a_{i,k} + \lambda a_{j,k})x_k = b_i + \lambda b_j \wedge \sum_{k=1}^n a_{j,k}x_k = b_j \right) \quad (5)
 \end{aligned}$$

durch multiplizieren mit dem λ -fachen der j -ten Zeile zu (5) erhält man wieder die Ausgangsgleichung.

q.e.d.

SATZ 1.2: Jede Matrix A lässt sich durch endlich viele Schritte (d.h. Zeilen vertauschen oder Addition vom λ -Fachen einer Zeile zu einer anderen) in Zeilenstufenform bringen.

Beweis: Sei A eine $m \times n$ - Matrix.

A ist bis zur k -ten Spalte in Zeilenstufenform, wenn die Matrix:
 $A(k) = \{a_{j,i} \mid j = 1, \dots, m \text{ und } i = 1, \dots, k\}$ in Zeilenstufenform ist.

- (i) ist A bereits in Zeilenstufenform \checkmark
- (ii) ist A hingegen nicht in Zeilenstufenform, dann gibt es ein minimales k , so dass $A(k)$ nicht in Zeilenstufenform ist. D.h. $A(k-1)$ ist in Zeilenstufenform, mit $r_{k-1} \in \mathbb{N}$

$\Rightarrow \exists$ ein $l > r_{k-1}$ mit $a_{lk} \neq 0$

Wir vertauschen jetzt die l -te und die $(r_{k-1} + 1)$ - Zeile und können nun annehmen $\lambda := a_{r_{k-1} + 1, k} = 0$, jetzt addieren wir $\forall l > r_{k-1}$, zur l -ten Zeile das $(-\frac{a_{l,k}}{\lambda})$ -fache der $(r_{k-1} + 1)$ -Zeile.

\Rightarrow Es stehen in der k -ten Spalte nur Nullen.

Genauer: $a'_{l,k} = 0 \quad \forall l > r_{k-1} + 1$

und da die Anzahl der Spalten endlich ist folgt:

q.e.d.

Beispiel 1.10:

$$\left(\begin{array}{cccccc|c} 1 & 0 & 1 & 0 & 3 & \vdots & 4 \\ 2 & 1 & 6 & 2 & 7 & \vdots & 15 \\ -1 & 3 & 11 & 7 & -1 & \vdots & 25 \end{array} \right)$$

↓

$$\left(\begin{array}{cccccc|c} 1 & 0 & 1 & 0 & 3 & \vdots & 4 \\ 0 & 1 & 4 & 2 & 1 & \vdots & 7 \\ -0 & 3 & 12 & 7 & 2 & \vdots & 29 \end{array} \right)$$

↓

$$\left(\begin{array}{cccccc|c} 1 & 0 & 1 & 0 & 3 & \vdots & 4 \\ 0 & 1 & 4 & 2 & 1 & \vdots & 7 \\ 0 & 0 & 0 & -1 & -1 & \vdots & 8 \end{array} \right)$$

Somit ist das LGS in Zeilenstufenform, und damit leicht lösbar.

2 Mengen, Gruppen, Ringe und Körper

2.1 Mengen

Mengen – sind bestimmt durch die Gesamtheit ihrer Elemente.

Die Menge M mit den Elementen x_1, \dots, x_n schreibt man: $M = \{x_1, \dots, x_n\}$

Schreibweisen: $x \in M$ – x ist Element von M

$N \subset M$ – N ist Teilmenge von $M \Leftrightarrow (x \in N \Rightarrow x \in M)$

$N \subseteq M$ – Teilmengen mit möglicher Gleichheit.

$N \subsetneq M, N \subset M \Rightarrow \exists x \in M, x \notin N$

ist eine Teilmenge ohne mögliche Gleichheit

$N \cup M$ – Vereinigung

$N \cap M$ – “geschnitten”, Menge aller x die sowohl in N als auch in M sind.

$N \setminus M = \{x \in N \mid x \notin M\}$

$f: M \rightarrow N$ Abbildung von M nach N

$m \mapsto f(m)$

$m \in M, f(m) \in N$

$imf = \{f(m) \mid m \in M\} \subset N$

$P(M) = \{N \mid N \supset M\}$ – Potenzmenge

Bsp.: $M = \{O, I\}$

$P(M) = \{\emptyset, \{O\}, \{I\}, \{O, I\}\}$

M, N seien Mengen

$M \times N = \{(x, y) \mid x \in M, y \in N\}$ – Kreuzprodukt von M und N

$\bar{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ M – Menge mit $m \in \mathbb{N}$ Elementen

$card.(M) = m$ oder $\#(M) = m$

ist M unendlich, so setzen wir $card(M) = \infty$

Zur Cardinalität $\langle card(M) \rangle$

Multiplikationen

$$\bar{\mathbb{N}}, \infty \cdot n = \begin{cases} 0 & \text{für } n = 0 \\ \infty & \text{für } n > 0 \end{cases}$$

$$card(M \times N) = card(M) \cdot card(N)$$

Zur Abbildung $\langle M \rightarrow N \rangle$
 M, N und P seien Mengen

$$\begin{aligned} \text{Abb.}(N, P) \times \text{Abb.}(M, N) &\longrightarrow \text{Abb.}(M, P) \\ (f, g) &\longmapsto f \circ g \\ &f \circ g(m) = f(g(m)) \end{aligned}$$

- Def. 2.1:** Eine Abbildung $\langle f : M \rightarrow N \rangle$ heißt
- injektiv $\Leftrightarrow m \neq m', m \in M; m' \in M$
 $\Rightarrow f(m) \neq f(m')$
 - surjektiv $\Leftrightarrow \text{im}(f) = N$
d.h. jedes Element in M hat ein Element in N
 - bijektiv \Leftrightarrow injektiv und surjektiv

- Beispiel 2.1: – $f : M \rightarrow \mathbb{N}$
 $n \mapsto$ Anzahl der Primzahlen bis einschließlich n .
 $f(0) = f(1) = 0$
 $f(2) = 1$
 $f(3) = f(4) = 2$
 f ist surjektiv
- $f : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto n^2$
 f ist injektiv
- $f : \mathbb{R} \rightarrow \mathbb{R}_{>0}$
 $t \mapsto \exp(t)$
 f ist injektiv und surjektiv \Rightarrow bijektiv

Ist $f : M \rightarrow N$ bijektiv, dann existiert eine eindeutig bestimmte Umkehrabbildung (inverse Abb.) $g : N \rightarrow M$ mit $f \circ g = \text{id}_M$ und $g \circ f = \text{id}_N$.

N sei eine Menge.
 $\text{id}_N \in \text{Abb.}(N, N)$
 $\text{id}_N(n) = n$
 g ist die inverse Abb. zu $f, g := f^{-1}$
Zur Definition von $g: n \in N$ Abb. surjektiv
 $\Rightarrow \exists m \in M$ mit $f(m) = n$
 m ist eindeutig, da die Abb. injektiv ist.
 $\Rightarrow g(n) = m$

Bemerkung: Es existiert eine natürliche Bijektion zwischen:
 $P(M)$ und $Abb.(M, \{0, 1\})$
 $f : P(M) \rightarrow Abb.(M, \{0, 1\})$
 $N \mapsto \chi_N$ mit $\chi_N(m) = 0 \iff m \notin N \vee 1 \iff m \in N$
 $f^{-1} : Abb.(M, \{0, 1\}) \rightarrow P(M)$
 $g \mapsto \text{supp}(g)$ | $\text{supp} = \text{support}$
 $\text{supp}(g) = \{m \in M \mid g(m) \neq 0, g(m) = 1\}$

Def. 2.2: Eine Relation auf einer Menge M ist eine Teilmenge $R \subset M \times M$
 $x, y \in M$
 $x \sim_R y \Leftrightarrow (x, y) \in R$
 R heißt \circ reflexiv $\Leftrightarrow x \sim_R x \quad \bigwedge x \in M$
 \circ symmetrisch $\Leftrightarrow x \sim_R y \Rightarrow y \sim_R x$
 \circ transitiv $\Leftrightarrow x \sim_R y \wedge y \sim_R z \Rightarrow x \sim_R z$
 \circ äquivalent \Leftrightarrow reflexiv, symmetrisch und transitiv ist.

Konstruktion 2.3:

Surjektionen sind das gleiche wie Äquivalenzrelationen (ÄR)

$f : M \rightarrow N$ surjektion

$m, m', m'' \in M$

$m \sim_f m' \Leftrightarrow f(m) = f(m')$

Beweis: \sim_f ist reflexiv, da $f(m) = f(m) \Rightarrow m \sim_f m$

\sim_f ist symmetrisch, da

$$\begin{aligned} m \sim_f m' &\Rightarrow f(m) = f(m') \\ &\Rightarrow f(m') = f(m) \\ &\Rightarrow m' \sim_f m \end{aligned}$$

\sim_f ist transitiv, da $m' \sim_f m$ und $m \sim_f m'$ und $m' \sim_f m''$
 $\Rightarrow f(m) = f(m') = f(m'')$

q.e.d.

Äquivalenzklassen

Sei \sim eine ÄR auf M . $m \in M$

$[m] = \{m' \in M \mid m \sim m'\}$

\diamond Es gilt $m \in [m]$, da \sim reflexiv ist.

$\diamond [m] \cap [m'] \ni m' \Rightarrow [m] = [m']$

Zu beweisen ist: $[m] \subset [m'] \wedge [m'] \subset [m]$

Sei $n \in [m]$; $m' \in [m]$; $m'' \in [m] \wedge m'' \in [m']$

$m \sim n \Rightarrow m \sim m'' \Rightarrow n \sim m''$

da aber auch $m' \sim m'' \Rightarrow m' \sim n \Rightarrow n \in [m'] \Rightarrow [m] \subset [m']$

und $[m'] \subset [m]$ analog.

q.e.d.

$M / \sim :=$ Menge aller Äquivalenzklassen von \sim

$M \rightarrow M / \sim$

$m \mapsto [m]$

SATZ 2.1: A, B, C seien Mengen

$$f \in \text{Abb.}(A, B)$$

$$g \in \text{Abb}(B, C) \text{ Es gilt:}$$

- (i) f, g injektiv $\Rightarrow g \circ f$ injektiv
- (ii) f, g surjektiv $\Rightarrow g \circ f$ surjektiv
- (iii) f, g bijektiv $\Rightarrow g \circ f$ bijektiv und
- (iv) $g \circ f$ bijektiv $\Rightarrow f$ injektiv und g surjektiv.

Beweis zu (i) [f und g injektiv]

$$\text{zu zeigen: } a_1 \neq a_2 \Rightarrow g \circ f(a_1) \neq g \circ f(a_2)$$

$$f \text{ injektiv} \Rightarrow f(a_1) \neq f(a_2)$$

$$g \text{ injektiv} \Rightarrow g(f(a_1)) \neq g(f(a_2))$$

$$\Rightarrow g \circ f(a_1) \neq g \circ f(a_2)$$

aus (i) und (ii) folgt (iii).

q.e.d.

SATZ 2.2: (i) Es seien $f : A \rightarrow B$ und $f' : A' \rightarrow B$
zwei injektive Abbildungen mit $\text{im}(f) = \text{im}(f')$, dann existiert
eine eindeutig bestimmte Bijektion $g : A \rightarrow A'$ mit $f' \circ g = f$

- (ii) Seien $f : A \rightarrow B$ und $f' : A \rightarrow B'$ zwei
Surjektionen mit $\sim_f = \sim_{f'}$, dann existiert
eine Bijektion $g : B \rightarrow B'$ mit $g \circ f = f'$
 $f : A \rightarrow B$
 \sim_f auf A $a_1 \sim a_2 \Leftrightarrow f(a_1) = f(a_2)$

Beweis zu (i): $a \in A, f(a) \in B$ ($-\text{im}(f) = \text{im}(f')$)
Es existiert ein $g(a) \in A'$ mit $f'(g(a)) = f(a)$,
da f' injektiv $\Rightarrow g(a)$ ist eindeutig bestimmt, da
 f injektiv $\Rightarrow g$ injektiv, da $-\text{im}(f) = \text{im}(f')$ ist g
surjektiv.

zu (ii): $b \in B' \rightarrow f^{-1}(b) = \{a \in A | f(a) = b\}$
 $a \in f'(b)$ beliebig $g(b) = f'(a)$
die Äquivalenzklasse von a bezüglich $\sim_f = f^{-1}(b)$
die Äquivalenzklasse von a bezüglich $\sim_{f'} = f^{-1}(b)$
 $g(b)$ ist injektiv $b_1 \neq b_2$
 $f^{-1}(b_1) \cap f^{-1}(b_2)$, da dies die Äquivalenzklassen
von $\sim_{f'}$ sind ist $f'(f^{-1}(b_1)) \cap f'(f^{-1}(b_2))$ surjektiv
 $b' \in B$ $a \in f'(f^{-1}(b')) \neq \emptyset$ $f(a') \in B$
 $g(f(a')) = b$

q.e.d.

Def. 2.4: Sei \sim eine ÄR auf M
 eine Teilmenge $S \subset M$ heißt vollständiges Repräsentantensystem, wenn die
 Abb. $\Pi \circ \iota$ eine Bijektion ist
 $\iota : S \rightarrow M$
 $\Pi : M \rightarrow M / \sim$

2.2 Gruppen

Def. 2.5: Eine Gruppe ist eine Menge G mit einer
 Abb. $\circ : G \times G \rightarrow G \quad (g_1, g_2) \mapsto g_1 \circ g_2$,
 so dass gilt:

(I) Assoziativgesetz:

$$\bigwedge_{g_1, g_2, g_3 \in G} (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

(II) Neutrale Elemente:

$$\bigwedge_{g \in G} \exists e \in G \text{ mit } e \circ g = g$$

(III) Inverse Elemente:

$$\bigwedge_{g \in G} \exists g' \in G \text{ mit } g' \circ g = e$$

Beispiele 2.2:

1. $(\mathbb{Z}, +) \quad e = 0 \quad k' = -k$
2. $(\mathbb{R}_+, \cdot) \quad e = 1, \quad r' = \frac{1}{r}$
3. $(M \neq \emptyset)$ eine beliebige Menge
 $e = id_M \quad f = f^{-1}$
 $G = \text{Bijektiv } (M, M)$
 $G = \{f : M \rightarrow M \text{ mit } f \text{ bij.}\}$
 $M = [3] = \{1, 2, 3\}$
 $G = \text{Bijektiv } (M) \quad f \in G$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\implies f \circ g \neq g \circ f$$

Def. 2.6: Die Gruppe (G, \circ) ist kommutativ (Abelsch),
falls $g_1 \circ g_2 = g_2 \circ g_1$ für alle $g_1, g_2 \in G$

PROPOSITION 2.3: Sei (G, \circ) eine Gruppe, und $g_1, g_2, h \in G$, dann gilt:

- (i) $e \in G$ aus Def.2.5 (II) ist eindeutig bestimmt und erfüllt:
 $g \circ e = e \circ g = g$, für alle $g \in G$
 - (ii) $g' \in G$ aus Def.2.5 (III) ist eindeutig bestimmt, wird mit g^{-1} bezeichnet, und erfüllt: $g^{-1} \circ g = g \circ g^{-1} = e$
 - (iii) $(g^{-1})^{-1} = g$
 $(g_1 \circ g_2)^{-1} = g_1^{-1} \circ g_2^{-1}$
 - (iv) $g_1 \circ h = g_2 \circ h \Rightarrow g_1 = g_2$
 $h \circ g_1 = h \circ g_2 \Rightarrow g_1 = g_2$
- $g \in G$ beliebig
 $\text{II} \Rightarrow \exists g' \in G \quad g' \circ g = e$
 $\text{II} \Rightarrow \exists g'' \in G \quad g'' \circ g' = e$
 $g \circ g' = e \circ (g \circ g') = (g'' \circ g') \circ (g \circ g')$
 $= g'' \circ ((g' \circ g) \circ g') = g'' \circ (e \circ g')$
 $= g'' \circ g = e$

Beweis zu (i): $g \circ e = g \circ (g' \circ g) = (g \circ g') \circ g = e \circ g = g$
 Sei e' ein zweites neutrales Element
 $\tilde{e} \circ e = e$, da \tilde{e} neutral
 $\tilde{e} \circ e = \tilde{e} \Rightarrow \tilde{e} = e$

- (ii): Sei \tilde{g}' ein zweites inverses Element zu g
 $\tilde{g}' = \tilde{g}' \circ e = \tilde{g}' \circ g \circ g'$
 $= e \circ g' = g'$

Das inverse Element zu g ist g^{-1}
 $g \circ g^{-1} = e = g^{-1} \circ g$

- (iii): $g \circ g^{-1} = e \Rightarrow g = (g^{-1})^{-1}$
 $(g_1^{-1} \circ g_2^{-1}) \circ (g_1 \circ g_2)$
 $g_2^{-1} \circ (g_1^{-1} \circ g_1) \circ g_2$
 $g_2^{-1} \circ g_2 = e$
 $(g_1 \circ g_2)^{-1} = g_2^{-1} \circ g_1^{-1}$

- (iv): $g_1 \circ h = g_2 \circ h \quad | \circ h^{-1}$
 $\Leftrightarrow g_1 \circ h \circ h^{-1} = g_2 \circ h \circ h^{-1}$
 $\Leftrightarrow g_1 = g_2$

q.e.d.

2.3 Gruppenhomomorphismen

Gruppentafeln

Def. 2.7: Sei (G, \circ) eine endliche Gruppe, mit den Elementen $G = \{e, g_2, g_3, \dots, g_n\}$ dann lässt sich die Abb $\circ: G \times G \rightarrow G$ durch die folgende Tafel (Tabelle) darstellen:

$h \setminus g$	e	g_2	g_3
e	e	g_2	g_3
g_2	g_2		
g_3	g_3		

Beispiel 2.3:

$$\text{card}(G) = 2 \quad G = \{e, a\} = (\{\pm 1\}, \cdot)$$

\circ	e	a
e	e	a
a	a	e

Beispiel 2.4:

$$\text{card}(G) = 3 \quad G = \{e, a, b\} = (\{0, 1, 2\}, +)$$

\circ	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

LEMMA 2.4 ist (G, \circ) eine Gruppe, und $g \in G$, so sind

die Abb $\tau_g: G \rightarrow G$

$$h \mapsto h \circ g$$

und Abb ${}_g\tau: G \rightarrow G$

$$h \mapsto g \circ h, \text{ bijektiv.}$$

Beweis zu τ_g :

$$\begin{aligned} \text{– injektiv:} \quad & \tau_g(h_1) = \tau_g(h_2) \\ & \Rightarrow h_1 \circ g = h_2 \circ g \quad | \circ g^{-1} \\ & \Rightarrow h_1 = h_2 \end{aligned}$$

$$\begin{aligned} \text{– surjektiv:} \quad & h \in G \text{ beliebig} \\ \text{gesucht:} \quad & f \in G \text{ mit } \tau_g(f) = h \\ & f = h \circ g^{-1} \\ & \Rightarrow \tau_g(f) = h \circ g^{-1} \circ g = h \end{aligned}$$

Der Beweis zu ${}_g\tau$ folgt analog, daher:

q.e.d.

Def 2.8 Gruppenhomomorphismen

Seien (G, \circ_G) und (H, \circ_H) zwei Gruppen.

Ein Gruppenhomomorphismus $\varphi : (G, \circ_G) \rightarrow (H, \circ_H)$ ist die Abb $\varphi : G \rightarrow H$ mit: $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$.

Eqimorphismus := surjektiver Gruppenhomomorphismus

Monomorphismus := injektiver Gruppenhomomorphismus

Isomorphismus := bijektiver Gruppenhomomorphismus

Beispiel 2.5:

$$G = (\mathbb{Z}, +)$$

$$H = (\mathbb{R}, +)$$

$$\varphi : G \rightarrow H$$

$$m \mapsto m \cdot \pi$$

Ist ein Monomorphismus.

$$\tau : G \rightarrow H$$

$$m \mapsto m + 1$$

Ist kein Gruppenhomomorphismus, da

$$\tau(0, 0) = 1 \text{ aber } \tau(0) + \tau(0) = 2 \text{ ist.}$$

$$\chi : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{\geq 1}, \cdot)$$

$$a \mapsto \exp(a) = e^a$$

Ist ein Isomorphismus.

2.4 Nebenklassen, Normalteiler, Signum

Linksnebenklassen

Konstruktion 2.9: Sei $U \subset (G, \circ)$ eine Untergruppe, und \sim_u eine Relation auf U so dass gilt:

$$g_1 \sim_u g_2 \Leftrightarrow g_1 = g_2 \circ u \text{ f\u00fcr ein } u \in U$$

Behauptung: \sim_u ist eine \u00c4R

(1) \sim_u ist reflexiv, da $e \in U$

(2) \sim_u ist transitiv, da $g_1 \sim_u g_2 \wedge g_2 \sim_u g_3$

$$\text{d.h. } g_1 = g_2 \circ u \wedge g_2 = g_3 \circ u'$$

$$g_1 = (g_3 \circ u') \circ u$$

$$= g_3 \circ (u' \circ u) \quad | u' \circ u \in U$$

$$= g_3 \circ u''$$

$$\Rightarrow g_1 \sim_u g_3$$

(3) \sim_u ist symmetrisch, da $g_1 \sim_u g_2 \Rightarrow g_1 = g_2 \circ u$

$$\Rightarrow g_1 \circ u^{-1} = g_2$$

$$\Rightarrow g_2 \sim_u g_1$$

q.e.d.

Def 2.10 : $G/U := G/\sim_u$

Wie sieht die Äquivalenzklasse von $g \in G$ aus?

$$g \circ U = \{g \circ u \mid u \in U\}.$$

Annahme: $\text{card}(G) < \infty \Rightarrow \text{card}(U) < \infty$

Def 2.11 : $(G \div U) = \text{card}(G/U)$

Jede Äquivalenzklasse von $g \in G$ hat $\text{card}(U)$ – Elemente, denn

$$U \rightarrow g \circ U$$

$u \mapsto g \circ u$ ist bijektiv.

SATZ 2.6: (kleiner FERMAT)

$$\text{card}(G) = (G \div U) \cdot \text{card}(U)$$

Rechtsnebenklassen erhalten wir durch die Relation $u \sim$

$$u \sim := g_1 u \sim g_2 \Leftrightarrow g_1 \circ u = g_2$$

$$[g] := U \circ g = \{u \circ g \mid u \in U\}$$

Achtung: Im Allgemeinen $u \sim \neq \sim_u$

$$\begin{aligned} U &= \left\{ e = \begin{pmatrix} 123 \\ 123 \end{pmatrix}, u = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \right\} \wedge g = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \\ U \circ g &= \left\{ g, f \circ g := \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\} \\ g \circ U &= \left\{ g, g \circ f := \begin{pmatrix} 123 \\ 231 \end{pmatrix} \right\} \\ &\Rightarrow g \circ U \neq U \circ g \end{aligned}$$

Normalteiler

Def 2.12 : $U \subset (G, \circ)$ heißt normalteiler, wenn

$$\begin{aligned} \bigwedge_{g \in G} g \circ U &= U \circ g \\ \Leftrightarrow U &= g^{-1} \circ U \circ g \end{aligned}$$

Schreibweise: $U \triangleleft G$

- Def. 2.13:** Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus, dann ist
- $im(f) = \{h \in H \mid h = f(g), g \in G\}$
 - $ker(f) = \{g \in G \mid f(g) = e\}$

PROPOSITION 2.7 Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus, dann gilt:

- (i) $f(e_G) = e_H$
- (ii) $f(g^{-1}) = f(g)^{-1}$
- (iii) $f : injektiv \Leftrightarrow ker(f) = \{e\}$

Beweis zu (i): $f(e_G) = f(e_g \circ_G e_G)$
 $= f(e_G) \circ_H f(e_G) \quad | \circ f(e_g)^{-1}$
 $e_H = f(e_G)$

zu (ii): $e_H = f(g \circ_G g^{-1})$
 $= f(g) \circ_H f(g^{-1}) \quad | f(g)^{-1} \circ_H$
 $f(g)^{-1} = f(g^{-1})$

zu (iii): „ \Rightarrow “ $f^{-1}(e_H) = ker(f) = \{e_G\}$
 „ \Leftarrow “ $f(g_1) = f(g_2)$
 $\Rightarrow f(g_1) \circ f(g_2)^{-1} = e_H$
 $\Leftrightarrow f(g_1) \circ f(g_2^{-1}) = e_H$
 $\Rightarrow f(g_1 \circ g_2^{-1}) = e_H$
 $\Rightarrow g_1 \circ g_2 \in ker(f)$
 $\Rightarrow g_1 \circ g_2^{-1} = e_G \quad | \circ g_2$
 $\Rightarrow g_1 = g_2$

q.e.d.

PROPOSITION 2.8: Ist $\tau : G \rightarrow H$ ein Gruppenhomomorphismus, dann gilt:

- (i) $img(\tau)$ ist eine Untergruppe;
- (ii) $ker(\tau)$ ist Normalteiler.

Beweis zu (i): $img(\tau) \neq \emptyset \quad h_1, h_2 \in img(\tau)$
 zu zeigen: $h_1 \circ h_2^{-1} \in img(\tau)$
 $\exists g_1, g_2 \in G$ mit $\tau(g_i) = h_i$
 $\Rightarrow g_1 \circ g_2^{-1} \in G \quad \Rightarrow \tau(g_1 \circ g_2^{-1}) \in img(\tau)$
 $= \tau(g_1) \circ \tau(g_2^{-1}) = h_1 \circ h_2^{-1}$

zu (ii): $g_1, g_2 \in ker(\tau) \Rightarrow \tau(g_1) = e = \tau(g_2)$
 $\Rightarrow \tau(g_1^{-1}) = \tau(g_2^{-1}) = e$
 $\Rightarrow \tau(g_1 \circ g_2^{-1}) = e$
 $\Rightarrow g_1 \circ g_2^{-1} \in ker(\tau)$

d.h. $ker(\tau)$ ist eine UGR, weiterhin zu zeigen bleibt

$ker(\tau)$ ist Normalteiler:

Sei $g \in G$ beliebig und $u \in ker(\tau)$

$$ker(\tau) = g^{-1} \circ ker(\tau) \circ g$$

$$\begin{aligned}
\tau(g^{-1} \circ u \circ g) &= \tau(g^{-1} \circ \tau(u) \circ \tau(g)) \\
&= \tau(g^{-1}) \circ e \circ \tau(g) \\
&= \tau(g^{-1} \circ \tau(g)) \\
&= \tau(e) = e \in \ker(\tau) \\
\Rightarrow g^{-1} \circ \ker(\tau) \circ g &\in \ker(\tau) \\
\text{Analog folgt: } g \circ \ker(\tau) \circ g^{-1} &\in \ker(\tau) \\
&\text{daher: q.e.d.}
\end{aligned}$$

PROPOSITION 2.9: Ist U Normalteiler von G [$U \triangleleft G$], dann existiert eine Gruppenstruktur auf G/U , so dass $G \rightarrow G/U$ ein Gruppenhomomorphismus ist, mit: $\ker(\Pi) = U$.

Beweis: Auf G/U definieren wir eine Gruppenstruktur $[\times]$ durch
 $(g \circ U) \times (g' \circ U) = (g \circ g') \circ U$
Die Nebenklasse ist nicht von der Wahl von g bzw. g' abhängig
Normalteiler := Rechtsnebenklasse = Linksnebenklasse
 $g'_1 \sim g' \Rightarrow g'_1 = g' \circ u \quad u \in U$
 $(g \circ g'_1) \circ U = g \circ g' \circ u \circ U$
da $u \circ U = U$, folgt $g \circ g' \circ U = g \circ g'_1 \circ U$
 $g \sim g_1 \Leftrightarrow g_1 = g \circ u$
 $g_1 \circ g' \circ U = g \circ u \circ g' \circ U$
 $= g \circ u \circ U \circ g'$
 $= g \circ U \circ g'$
 $= g \circ g' \circ U$
Das neutrale Element ist in $U = e \circ U$
Die inverse Klasse von $g \circ u$ ist $g^{-1} \circ u$.
 $\Pi : G \rightarrow U$
 $g \mapsto g \circ u$
 $\Pi(g \circ g') = (g \circ g') \circ U$
 $= (g \circ U) \times (g' \circ U)$

q.e.d.

Def. 2.14 Transposition

$$S_n = \text{Bij}([n])$$

$$[n] = \{1, 2, \dots, n\}$$

$\tau \in S_n$ heißt Transposition (von i und j) mit $i \neq j, i \in [n], j \in [n]$

$$\tau = (k) \begin{cases} k & k \notin \{i, j\} \\ j & k = i \\ i & k = j \end{cases}$$

$$\tau = \tau_{ij}$$

Da τ eine Transposition ist, ist τ zu sich selbst invers: $\tau = \tau^{-1}$

Bemerkung: Jedes Element von S_n ist Darstellbar als eine Komposition (hintereinander Ausführung) von Transpositionen.

Beweis: $\sigma \in S_n$
 $fix(\sigma) = card(k \in [n])$ mit $\sigma(k) = k$

q.e.d.

Beispiel 2.6:

$$fix\left(\begin{smallmatrix} 12345 \\ 23145 \end{smallmatrix}\right) = 2$$

$$fix(id_{[n]}) = n$$

SATZ 2.10 ist $\sigma \in S_n$ und $\sigma \neq (id_{[n]})$ dann existiert eine Transposition $\tau \in S_n$ mit $fix(\tau \circ \sigma) > fix(\sigma)$

Beweis: $\sigma \in S_n$ beliebig

1. Fall: $\sigma = id_{[n]} \Rightarrow \sigma = \tau \circ \tau$

2. Fall: $\sigma \neq id_{[n]}$

Es existiert eine Transposition τ_i , so dass

$$fix(\sigma) < fix(\tau_1 \circ \sigma) < fix(\tau_1 \circ \tau_2 \circ \sigma) < fix(\tau_1 \circ \tau_2 \circ k \circ \sigma)$$

$$\Rightarrow \tau_1 \circ \tau_2 \circ \dots \circ \tau_k \circ \sigma = id_n$$

$$\Rightarrow \tau_1 \circ \dots \circ \tau_k = \sigma^{-1}$$

q.e.d.

Das Signum

Def. 2.15 Anzahl der Fehlstände [*inv* - Inversionen]

$$\sigma \in S_n$$

$$inv(\sigma) = card\{(i, j) \left[\begin{array}{l} - \quad i, j \in [n] \\ - \quad i < j \\ - \quad \sigma(i) > \sigma(j) \end{array} \right. \}$$

$$sgn(\sigma) := (-1)^{inv(\sigma)}$$

SATZ 2.11: $sgn : S_n \rightarrow (\pm 1, \circ)$ ist ein Gruppenhomomorphismus

Beweis: τ ist eine Transposition

Behauptung: $inv(\tau \circ \sigma) - inv(\sigma) =: \delta$ ist ungrade.

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

τ vertauscht $\sigma(k)$ mit $\sigma(l)$

Sei o.B.d.A. $k < l$

Die Differenz der Anzahl der Fehlstände berücksichtigt
offenbar nur Paare (i, j) mit $(i, j) \cap (k, l) \neq \emptyset$

	1	2	...	k	...	l	...	n
$\sigma \downarrow$	$\sigma(1)$	$\sigma(2)$...	$\sigma(k)$...	$\sigma(l)$...	$\sigma(n)$
$\tau \downarrow$	$\sigma(1)$	$\sigma(2)$...	$\sigma(l)$...	$\sigma(k)$...	$\sigma(n)$
Abschn.		A		B		C		

In B liegen $l - k - 1$ Elemente

$a_1 :=$ Elemente in B $> \sigma(k)$

$a_2 :=$ Elemente in B $> \sigma(l)$

$a_3 :=$ Elemente in B $< \sigma(k)$

$a_4 :=$ Elemente in B $< \sigma(l)$

$$\Rightarrow a_1 + a_3 = l - k - 1 \quad (1)$$

$$\Leftrightarrow a_3 = l - k - 1 - a_1$$

und $\Rightarrow a_2 + a_4 = l - k - 1 \quad (2)$

$$\Leftrightarrow a_4 = l - k - 1 - a_2$$

$$\delta := a_4 - a_2 + a_3 - a_1 \pm 1$$

$$= (l - k - 1) - 2a_2 + (l - k - 1) - 2a_1 \pm 1$$

$$\Rightarrow \delta \text{ ist ungrade.}$$

$\sigma, \sigma' \in S_n$ beliebig

$$\sigma = \tau_1 \circ \dots \circ \tau_k$$

$$\Rightarrow sgn(\sigma) = (-1)^k$$

$$\sigma' = \tau'_1 \circ \dots \circ \tau'_{k'}$$

$$\Rightarrow sgn(\sigma') = (-1)^{k'}$$

$$\Rightarrow sgn(\sigma \circ \sigma') = (-1)^{k+k'}$$

q.e.d.

2.5 Erzeuger und die Ordnung

KOROLLAR 2.12: Sei G eine Gruppe und A eine Teilmenge $A \subset G$ mit $A \neq \emptyset$, dann ist der Erzeuger

$$\text{erz}(A) = \{g \in G \mid G = a_1 \circ a_2 \circ \dots \circ a_n; n \in \mathbb{N}; a_i, a_i^{-1} \in A\}$$

eine Untergruppe von G .

Beweis: Durch die Untergruppenkriterien

$$\text{zu zeigen: } g, g' \in \text{erz}(A) \Rightarrow g \circ g'^{-1} \in \text{erz}(A)$$

$$g = a_1 \circ a_2 \circ \dots \circ a_n$$

$$g' = a'_1 \circ a'_2 \circ \dots \circ a'_{n'}$$

$$g \circ g'^{-1} = a_1 \circ a_2 \circ \dots \circ a_n \circ a'_{n'} \circ a'_{n'-1} \circ \dots \circ a'_1$$

$$\Rightarrow g \circ g'^{-1} \in \text{erz}(A)$$

q.e.d.

Bemerkung:

$\text{erz}(A)$ - die von A erzeugte Untergruppe

- die kleinste A enthaltende Untergruppe

$$\text{erz}(\emptyset) = \{e\}$$

Einelementige erz :

$$\text{Sei } A = \{g\}$$

$$\text{erz}(A) = \{g^k \mid k \in \mathbb{Z}\}$$

$$k \geq 0, \quad g^0 = e, \quad g^k := g^{k-1} \circ g$$

Def. 2.16: Wir nennen die Kardinalität von $\text{erz}(\{g\})$ die Ordnung von g .

Beispiel 2.7: - $G = (\mathbb{Z}, +)$

$$- \text{ord}(4) = \infty$$

$$- G = \mathbb{Z}/4\mathbb{Z}$$

$$G = \{[0], [1], [2], [-1]\}$$

$$\text{ord}([0]) = 1 \quad \text{ord}([2]) = 2$$

$$\text{ord}([1]) = 4 \quad \text{ord}([-1]) = \text{ord}([3]) = 4$$

LEMMA 2.13: ist G eine endliche Gruppe, dann gilt:

$$\text{ord}(g) < \infty \text{ für alle } g \in G$$

Beweis: $\text{card}(g) = n$

$$M = \{g, g^2, g^3, \dots, g^{n+1}\}$$

$$\Rightarrow \exists l, k > 0 \quad g^l = g^{l+k} \quad | \circ g^{-l}$$

$$e = g^k$$

Sei nun k die kleinste natürliche Zahl mit $g^k = e$

Behauptung: $erz(\{g\}) = \{g, g^2, \dots, g^k = e\}$

Beweis: $g^a \in erz(\{g\})$
 $g^b \in erz(\{g\})$
 $g^a \circ b^{-b} = g^{a-b}$
 $= g^{a-b} \circ e$
 $= g^{a-b} \circ g^k$
 $= g^{a-b+k}$

$\implies ord(g) = \min\{k \in \mathbb{N}_+ \mid g^k = e\}$

q.e.d.

SATZ 2.14: (kleiner FERMAT')

Ist G eine endliche Gruppe, so gilt:

$$\bigwedge_{g \in G} ord(g) \mid card(G)$$

Def. 2.17: G heißt zyklische, wenn g heißt Erzeuger von G :

$$G = erz(\{g\})$$

Beispiel 2.9: $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$g \setminus h$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

...ist nicht zyklisch.

2.6 Ringe und Körper

Def. 2.18 Ringe

$(R, +, \cdot)$ ist ein Ring, wenn

$$- + : R \times R \rightarrow R$$

$$- \cdot : R \times R \rightarrow R$$

mit $(R, +)$ - ist eine abelsche Gruppe mit neutralem Element 0.

- (R, \cdot) - ist assoziativ, d.h.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$$

Weiterhin gilt das Distributivgesetz:

$$a \cdot (b + c) = ab + ac$$

$$(a + b) \cdot c = ac + bc$$

Beispiel 2.10: $\circ (\mathbb{Z}, +, \cdot)$ ist ein Ring.

$\circ (4\mathbb{Z}, +, \cdot)$ ist ein Ring.

$\circ I = [0, 1] \quad R = \text{Abb}(I, \mathbb{Z})$

$$f + g(x) := f(x) + g(x)$$

$$f \cdot g(x) := f(x) \cdot g(x)$$

$\circ \mathbb{Q}, \mathbb{R}$ sind Ringe.

$\circ \mathbb{N}$ ist kein Ring, denn $(\mathbb{N}, +)$ ist nicht abelsch.

Beispiel 2.11: $R = (\mathbb{Z}/m\mathbb{Z}, +, \cdot) \quad m \in \mathbb{N}$

$$[R = \{[0], [1], [2], \dots, [m-1]\}]$$

$(\mathbb{Z}/m\mathbb{Z}, +)$ ist eine Gruppe.

$$[k] + [l] := [k + l] \quad [k] = k + m \cdot \mathbb{Z}$$

$(\mathbb{Z}/m\mathbb{Z}, \cdot)$ ist eine Gruppe.

$$[k] \cdot [l] := [k \cdot l]$$

Zu zeigen: $[k] = [k'] \Rightarrow [k \cdot l] = [k' \cdot l]$

$$k' = k + n \cdot m$$

$$[k' \cdot l] = k \cdot l + n \cdot m \cdot l + m \cdot \mathbb{Z}$$

$$= k \cdot l + m(n \cdot l + \mathbb{Z})$$

$$|(n \cdot l + \mathbb{Z}) = \mathbb{Z}$$

$$= k \cdot l + m \cdot \mathbb{Z}$$

Analog folgt: $[l] = [l'] \Rightarrow [k \cdot l] = [k \cdot l']$

Def. 2.19: Kommutativer Ring, Einselement und Nullteiler

Sei R ein Ring.

- R ist kommutativ, wenn

$$a \cdot b = b \cdot a \quad \text{für alle } a, b \in R$$

- R ist ein Ring mit Einselement, wenn $1 \in R$, mit

$$a \cdot 1 = 1 \cdot a = a \quad \text{für alle } a \in R \text{ existiert.}$$

- a und b heißen Nullteiler, wenn

$$a \cdot b = 0 \quad \text{mit } a, b \neq 0 \text{ für alle } a, b \in R$$

- R heißt Nullteilerfrei (NTF), wenn R keine Nullteiler enthält.

	\mathbb{Z}	$4\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/17\mathbb{Z}$	\mathbb{R}
kommut.	✓	✓	✓	✓	✓
1-Elem.	1	/	[1]	[1]	1
0-Teiler	/	/	[2] · [2] = 0	/	/

Def. 2.20: Körper

Ein Körper ist ein kommutativer Ring (K) , mit $(K \setminus \{0\}, \cdot)$ ist eine Gruppe.

Beispiele 2.12: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p \cdot \mathbb{Z}$ mit $p \in \text{Primzahlen}$

PROPOSITION 2.15: Sei R ein endlicher, kommutativer Ring mit *Einselement*, dann gilt: R ist Nullteilerfrei $\Leftrightarrow R$ ist ein Körper.

Beweis:

“ \Leftarrow “ trivial

“ \Rightarrow “ $a \in R \setminus \{0\}$

ges. $b \in R \setminus \{0\}$ mit $a \cdot b = 1$

$\Pi_a : R \setminus \{0\} \rightarrow R \setminus \{0\}$

$b \mapsto a \cdot b$

1. Fall: $1 \in \text{im}(\Pi_a) \Rightarrow \exists b$ mit $a \cdot b = 1$

2. Fall: $1 \notin \text{im}(\Pi_a)$

$\exists b \neq b' \in R \setminus \{0\}$ mit $a \cdot b = a \cdot b'$

$a \cdot b + (-a \cdot b') = 0$

$a(a - b') = 0$ Widerspruch zur NTF(!)

q.e.d.

Bemerkung (zu $+$, $-$ und 0) :

- $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$
 $0 = 0 \cdot a$

- $a - b := a + (b)^{-1} \text{bzgl. } +$
 $\Rightarrow -b := (b)^{-1} \text{bzgl. } +$

- $1 \in R \quad -1 := 1 + (-1) = 0$

- $1 + (-1) = 0 \quad | \cdot a$
 $1 \cdot a + (-1) \cdot a = 0 \quad \Rightarrow a^{-1} := (-1) \cdot a = -a$

Bemerkung: Was passiert, wenn $1 = 0$ ist?

$a \in \mathbb{R} \quad 1 \cdot a = a \quad 0 \cdot a = 0$, ist also

$1 = 0$ so folgt daraus, dass $a = 0$, also jedes Element des Ringes $= 0$ ist.

Daher die Konvention: $\mathbf{1} \neq \mathbf{0}$

Def. 2.21: Einheitengruppe

Sei R ein Ring mit *Einselement*.

$R^* := \{u \in R \mid \exists u' \in R \text{ mit } u' \cdot u = 1\}$

R^* nennt man die "Einheitengruppe" des Ringes R

Behauptung: (R^*, \cdot) ist eine Gruppe.

Beweis: $- u_1, u_2 \in R^* \Rightarrow \exists u'_1 u'_2 \text{ mit } u'_1 \cdot u_1 = 1 = u'_2 \cdot u_2$

$\Rightarrow u'_1 \cdot u'_2 \cdot (u_2 \cdot u_1) = 1$

$\Rightarrow u'_1 \cdot u'_2 \in R^*$

$- (R, \cdot)$ ist assoziativ $\Rightarrow (R^*, \cdot)$ ist assoziativ.

$- 1$ ist das neutrale Element.

$-$ Das inverse Element existiert nach der Definition.

q.e.d.

Beispiel 2.13:

Ring R	R^*	$char(R)$
\mathbb{Z}	$(\pm 1, \cdot)$	0
$\mathbb{Z}/7\mathbb{Z}$	$[1], [2] - [4],$ $[3] - [5], [6]$	7
$\mathbb{Z}/8\mathbb{Z}$	$[1], [3], [5],$ $[7]$	8
Körper K	$K \setminus \{0\}$?

2.7 Der euklidische Algorithmus

Def. 2.22: Ein euklidischer Ring ist ein Ring R , der

- NTF
- $h : R \setminus \{0\} \rightarrow \mathbb{N}$
- für alle $a, b \in R \setminus \{0\}$ $h(ab) \geq h(a)$
- für alle $a, b \in R \setminus \{0\}$ $\exists c \in R$ mit $\begin{cases} a = b \cdot c \\ h(a - bc) < h(b) \end{cases}$ ist.

Beispiel 2.14: \mathbb{Z}

$$h : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$$

$$a \mapsto |a|$$

$$a = 12, b = 5, c = 2$$

$$h(12 - 2 \cdot 5) < h(5)$$

SATZ 2.16 Ist R ein euklidischer Ring und $a, b \in R \setminus \{0\}$ und $d, f, g, h \in R$, dann existiert ein Element $e \in R$ mit:

- $e = a \cdot d + b \cdot f$ (Linearkombination)
- $a = e \cdot g$
- $b = e \cdot h$

Die Gültigkeit des Satzes ändert sich nicht, wenn man a und b vertauscht.

Beweis: O.B.d.A. sei $h(a) \geq h(b)$

Beweis durch Induktion über $K := h(a) + h(b)$

IND-ANFANG ($K = 0$) $\Rightarrow h(a) = 0 = h(b)$

Da $h(b)$ das Minimum an nimmt existiert ein $c \in R$, mit $a = b \cdot c$

$e = b$; $e = a \cdot 0 + b \cdot 1$; $a = b \cdot c$; $b = 1c$

IND-SCHRITT ($K \rightsquigarrow K + 1$)

IND-ANNAHME: $h(a) + h(b) \leq K$

IND-BEHAUPTUNG: $h(a) + h(b) \leq K + 1$

$\exists c$ mit:

- Fall 1: $a - bc$

- Fall 2: $h(a - bc) < h(b)$

im 1. Fall $\rightarrow e = b$; $e = a \cdot 0 + b \cdot 1$; $a = b \cdot c$; $b = 1c$

im 2. Fall $\rightarrow h(a - bc) < h(b)$

$a' := a - bc \Rightarrow h(a') < h(b) \leq h(a)$ für $h(a, b)$ gilt IND-ANN.

d.h. $\exists e = a' \cdot d + b \cdot f'$ (1)

$a' = e \cdot g'$ (2)

$b = e \cdot h$ (3)

(1) $\Rightarrow e = a' \cdot d + b \cdot f'$
 $= (a - bc) \cdot d + b \cdot f'$ (1')

(2) $\Rightarrow a = bc + e \cdot g'$ (2')

(3) $\Rightarrow b = e \cdot h$ (3)

(1') $\Rightarrow e = a \cdot d + b(f' - cd)$

(2') $\Rightarrow a = e \cdot h \cdot c + e \cdot g' = e(hc + g')$

$b = e \cdot h$ q.e.d.

Wir nennen e den größten gemeinsamen Teiler von a und b [$g.g.T.(a, b)$]

Der euklidische Algorithmus

Beispiel 2.15: $p \in \text{Primzahl}$

- $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ist ein Körper.
 - $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$
 - $\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$
 - $\mathbb{F}_{101} := \mathbb{Z}/101\mathbb{Z} = \{[0], [1], \dots, [62], \dots, [100]\}$
- $$\begin{array}{rcl}
 101 \div 62 = 1 & R39 & 101 = 62 \cdot 1 + 39 \\
 62 \div 39 = 1 & R23 & 62 = 39 \cdot 1 + 23 \\
 39 \div 23 = 1 & R16 & 39 = 23 \cdot 1 + 16 \\
 23 \div 16 = 1 & R7 & 23 = 16 \cdot 1 + 7 \\
 16 \div 7 = 2 & R2 & 16 = 7 \cdot 2 + 2 \\
 7 \div 2 = 3 & R1 & 7 = 2 \cdot 3 + 1 \\
 \Rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3(16 - 2 \cdot 7) = 7 \cdot 7 - 3 \cdot 16 \\
 2 = 16 - 2 \cdot 7 = \dots = a \cdot 62 + b \cdot 101
 \end{array}$$

Beispiel 2.16: $\mathbb{F}_{997} = \mathbb{Z}/997\mathbb{Z}$

$$\begin{array}{rcl}
 997 \div 240 & = & 4 \quad R \ 37 \quad (3) \\
 240 \div 37 & = & 6 \quad R18 \quad (2) \\
 37 \div 18 & = & 2 \quad R \ 1 \quad (1) \\
 18 \div 1 & = & 18 \quad R0 \\
 (1) \Rightarrow & 1 & = 37 - 2 \cdot 18 \\
 (2) \Rightarrow & 18 & = 240 - 6 \cdot 37 \\
 (3) \Rightarrow & 37 & = 997 - 4 \cdot 240 \\
 1 & = & 27 - 2(240 - 6(997 - 4 \cdot 240)) \\
 & = & 13(997 - 4 \cdot 240) - 2 \cdot 240 \\
 \Rightarrow & 1 & = 13 \cdot 997 - 54 \cdot 240 \\
 \Rightarrow & 1 & = [-54] \cdot [240] \\
 & \frac{1}{[240]} & = [-54]
 \end{array}$$

Def. 2.23: Ringhomomorphismen

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ zwei Ringe.

Ein Ringhomomorphismus (Ringhom.) ist eine Abbildung:

$\omega : R \rightarrow S$, mit:

$$- \omega(a +_R b) = \omega(a) +_S \omega(b)$$

$$- \omega(a \cdot_R b) = \omega(a) \cdot_S \omega(b)$$

Konvention: Sind R und S Ringe mit *eins*, dann

$$- \omega : 1 \rightarrow 1$$

Beispiel 2.17: Sei R ein Ring mit *eins*, dann existiert genau ein Ringhomomorphismus $\chi : \mathbb{Z} \rightarrow R$, mit:

$$- \chi(1) \rightarrow 1_R$$

$$- a \in \mathbb{Z} \quad a > 0 \quad a := 1 + 1 + \dots + 1$$

$$\Rightarrow \chi(a) = 1_R + 1_R + \dots + 1_R$$

$$= a \cdot 1_R$$

$$\chi(-a) = -\chi(a)$$

Es gilt offenbar:

$$\chi(a \cdot b) = \chi(a) \cdot \chi(b) \text{ sowie,}$$

$$\chi(a \cdot b) \cdot 1_R = \chi(a \cdot 1_R) \cdot (b \cdot 1_R).$$

Def. 2.24: Charakter von R $\text{char}(R)$

Sei R ein Ring mit *eins*, dann existiert genau ein Ringhomomorphismus $\chi : \mathbb{Z} \rightarrow R$, mit

$$\chi(1) = 1$$

1. Fall: χ ist injektiv.

$$\text{char}(R) := 0$$

2. Fall: χ ist nicht injektiv.

$$\Rightarrow \ker(\chi) \text{ ist Untergruppe von } (\mathbb{Z}, +)$$

$$\text{char}(R) := \min\{c \in \mathbb{N}_{>0} \mid \chi(c) = 0\}$$

Beispiele siehe Tabelle in Beispiel 2.13.

2.8 \mathbb{C} – Der Körper der komplexen Zahlen

Def. 2.25: $\mathbb{C} := \mathbb{R}^2$ mit folgenden Körperaxiomen:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

$$\Rightarrow (0, 1)^2 = (0, 1) \cdot (0, 1) = (-1, 0)$$

$$(a, 0) \cdot (c, 0) = (ac, 0)$$

$$(a, 0) + (c, 0) = (a + c, 0)$$

Beobachtungen:

$$\iota : \mathbb{R} \rightarrow \mathbb{C}$$

$$a \mapsto (a, 0)$$

$$\iota(a \cdot c) = \iota(a) \cdot \iota(c)$$

$$\iota(a + c) = \iota(a) + \iota(c)$$

$$\text{Negative Quadrate: } i := (0, 1) \quad i^2 = \iota(-1) = -1$$

$$\text{Schreibweise: } a + bi =: (a, b)$$

Abbildungen von \mathbb{C} nach \mathbb{R} :

$$Re : \mathbb{C} \rightarrow \mathbb{R}$$

$$(a, b) \mapsto a \quad \text{'Realteil'}$$

$$IM : \mathbb{C} \rightarrow \mathbb{R}$$

$$(a, b) \mapsto b \quad \text{'Imaginärteil'}$$

Behauptung: \mathbb{C} ist ein Körper.

Wie wir oben bereits gezeigt haben ist $(\mathbb{C}, +)$ eine Gruppe. Es bleiben also noch die folgenden Körperaxiome für (\mathbb{C}, \circ) zu zeigen:

(i) (\mathbb{C}, \circ) ist assoziativ und

(ii) ein kommutativer Ring

(iii) mit Einselement

(iv) und Distributivgesetz

(v) sowie $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$

zu (i) $((a, b) \cdot (c, d)) \cdot (e, f) = (a, b) \cdot ((c, d) \cdot (e, f))$

3 Anhang

3.1 Literaturangaben

Die Vorlesung basiert auf dem Buch:

Gerd Fischer **ISBN 3-8348-0031-7**
Lineare Algebra ca. 20,00 EUR

Diese Mitschrift hält sich in der Gliederung weitestgehend an die Zusammenfassung von Herrn Prof. G. Hein, welche online unter <http://www.uni-due.de/hm0019/~lehre/pdf/das-ist-kein-skript.pdf> verfügbar ist.

3.2 Begriffserklärungen

- | | |
|------------------------|--|
| Lemma | – Hilfsatz im Beweis eines wichtigeren Satzes |
| Korollar | – Sammlung von Feststellungen oder Folgerungen, die sich aus einem Satz oder einer Definition ohne großen Aufwand ergeben. |
| Proposition | – logische Aussage |
| Satz oder auch Theorem | – Lehr- und Grundsatz. Theorem ist ein veraltender Ausdruck, im Englischen sowie im Russischen oder bei seit langem bekannten Sätzen aber noch gebräuchlich. |
| O.B.d.A. | – Ohne Beschränkung der Allgemeinheit
Eine Einschränkung wird nur zur Vereinfachung vorausgesetzt ohne, dass die Gültigkeit der im Anschluss getroffenen Aussagen in bezug auf die Allgemeinheit darunter leidet. Dies geschieht unter der Bedingung, dass die anderen Fälle in analoger Weise bewiesen werden können |
| q.e.d. | – quod erat demonstrandum (<i>lat.</i>) - Was zu beweisen / zeigen war.
Wird oft durch \square oder \blacksquare ersetzt. |
| Konvention | – (v. lat.: conventio = Übereinkunft, Zusammenkunft)
ist eine nicht formal festgeschriebene Regel. |