Lineare Algebra I

Mitschrieb

Florian Kramer

23. November 2017

Inhaltsverzeichnis

1 Einführung

- Das Wort Algebra stammt aus dem arabischen äl-jabr".
- Allgemein ist Algebra die Lehre der mathematischen Symbole und deren Manipulation.
- Lineare Algebra: Insbesondere lineare Gleichungen

1.1 Aufbau der Vorlesung

1. Lineare Gleichungssysteme und der n-dimensionale reellen Raum
2. Grundlegende Objekte
3. Gruppen, Ringe, Körper
4. Vektorräume und lineare Abbildungen
5. Determinaten
6. Eigenwerte und Normalformen

1.2 Beispiel: Der Google Pagerank

Gegeben 4 Seiten, mit Verlinkungen zwischen den Seiten. Von einer nicht verlinkten Seite wechselt man zufl̈lig auf eine andere Seite. Der user startet an einer zufl̈ligen Stelle und folgt von dort einem zufälligen link auf eine andere Seite.Zusätzlich wird immer mit Wahrscheinlichkeit $(1-d), d \in [0,1]$ auf eine beliebige Website gewechselt.
Die wichtigste Site ist nun die, auf welcher ein Benutzer sich mit der höchsten Wahscheinlichkeit aufhält.
$p(\delta_1) = \frac{1-d}{N} + d(\frac{p(\delta_2)}{1}, \frac{p(\delta_5)}{4})$
$p(\delta_2) = \frac{1-d}{N} + d(\frac{p(\delta_1)}{3}, \frac{p(\delta_5)}{4})$
$\vdots$
Zur Berechnung von $p(\delta_j), j \in \{1..5\}$ gibt es Methoden aus der linearen Algebra.

2 Lineare Gleichungssyteme und der n-dimensionale reelle Raum

- Descartes führte "Koordinaten" ein in der Geometrie ein, also Zahlensysteme. Das führte dazu, das man nun leichter rechnen kann.
- Wir benutzen hier die reellen Zahlen (mit den üblichen Rechenregeln, also für die Addition :
  - $(x + y) + z = x + (y + z)$
  - $0 + x = x + 0 = x$
  - Es gibt für jedes x ein y mit $x + y = 0$, wir nennen dieses y das additiv inverse zu x ("-x").
  - $x + y = y + x$

  Und für multiplikation:
  - $\lambda(x + y) = \lambda x + \lambda y$
  - $(\lambda + \mu)x = \lambda x + \mu x)$
  - $\lambda(\rho\mu) = (\lambda\rho)\mu$
  - $1x = x$
- Weiteres brauchen wir die natürlichen Zahlen, die 1,2,3...

2.1 Der $\mathbb{R}^n$

Für gegebenes $n \in \mathbb{N}$ definieren wir:
$\mathbb{R}^n = \{x = (x_1, x_2, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{R}\}$
$(x_1, \ldots, x_n)$ ist dabei ein geordnetes n-Tupel, die Reihenfolge beim Vergleich Elemente dieser Art ist wichtig.
Für $x, y, \in \mathbb{R} : x = y \Leftrightarrow x_1 = y_1, x_2 = y_2, \ldots x_n, = y_n$
Wir nennen diese n-Tupel auch Vektoren im $\mathbb{R}^n$.

Mit $\mathbb{R}^0$ bezeichnen wir die Menge $\{0\}$, welche nur das Nullelement enthält.

Die Rechenregeln übertragen sich nun von $\mathbb{R}$. Wir schreiben

$x + y = (x_1 + y_1, \ldots, x_n + y_n)$ für $x, y \in \mathbb{R}^n$ (Vektoradition)

$\lambda x = (\lambda x_1, \ldots, \lambda x_n)$ (Skalarmultiplikation)

2.2 Lineare Gleichungssyteme

Eine lineare Gleichung ueber $\mathbb{R}$ist ein Ausdruck der Form:

$\alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n = \beta$

Fuer reele Zahlen $\beta, \alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Einen Vektor, $\xi = \{\xi_1, \ldots, \xi_n) \in \mathbb{R}^n$ nennen wir Loesung, wenn die reelen Zahleen , $\xi_1, \ldots, \xi_n$ eingesetzt in $x_1, \ldots, x_n$ die Gleichung erfüllen.

Ein lineares Gleichungssystem G ist ein System

$a_1 1 x_1 + a_1 2 + x_2 \ldots a_1 n x_n = b_1$

$a_2 1 x_1 + a_2 2 + x_2 \ldots a_2 n x_n = b_1$

$\vdots$

$a_m 1 x_1 + a_m 2 + x_2 \ldots a_m n x_n = b_1$

In Kurzform $= \sum_{j=1}^{n} a_{i,j} x_j = b_i \forall i \in \{1, \ldots, m\}$

oder, noch kürzer, in Matrixschreibweise

$Ax = b$

Wobei A eine Matrix ist mit Einträgen $a_{i,j}$, wir schreiben

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ & \vdots & \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}$$

Ax für $x \in \mathbb{R}^n$ ist dann eine Kurzform für $\sum_{i=1}^{n} a_{ij} x_j$ mit einem Vektor $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Das Ergebnis ist ein Vektor $b = (b_1, \ldots, b_m) \in \mathbb{R}^m$ für eine Matrix A mit m Zeilen und n Spalten.

Der Vektor b heißt rechte Seite des linearen Gleichungssystems, A heißt Koeffizienten Matrix des linearen Gleichungssystems. Eine Spalte / Zeile von A kann mit einem Vektor im $\mathbb{R}^m$ bzw. im $\mathbb{R}^n$ identifiziert werden. Wir sprechen von Spalten- / Zeilen Vektoren

der Matrix A.

Eine Matrix mit m Zeilen und n Spalten nennen wir $m \times n$ - Matrix. Fuer $x \in \mathbb{R}^n$, A eine $m \times n$ - Matix und B eine lxm - Matrix gilt die Rechenregel $BAx = B(Ax)$. Ein Gleichugnssystem $Ax = b$ heisst homogen, falls b der Nullvektor $(0, \ldots, 0)$ ist und quadratisch fuer $m = n$ (eine quadratische Matrix A).

2.2.1 Definition: Normalform

Ein Gleichungssytstem $Ax = b$ ist min Normalform, falss A die Gestalt

$$\begin{pmatrix} 1 & 0 & a_{1,k+1} & \ldots & a_{1,n} \\ 0 & 1 & a_{m,k+1} & \ldots & a_{m,n} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$ (fuer k=2)

fuer ein $k \in \mathbb{N}_0$

Beispiele:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$ Ist in Normalform für $k = 2$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ Ist in Normalform für $k = 3$.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$ Ist in Normalform für $k = 0$.

k heißt Rang der Matrix A (bzw. des Gleichungssytems). Es gilt

$0 \leq k \leq min(m, n)$

Ein Gleichungssystem ist genau dann Lösbar, wenn gilt:

$b_{k+1} = b_{k+2} = \cdots = b_m = 0$

In diesem Fall lässt sich eine Lösung $\xi \in \mathbb{R}^n$ bestimmen, indem man $\xi_{k+1}, \ldots, \xi_n$ beliebig

wählt, und danach $\xi_i = b_i - \sum_{j=k+1}^{n} a_{i,j}\xi_j \forall i \in \{1, \ldots, n\}$ wählt.

Denn für Zeile $i, i = k+1, \ldots, n$ lautet das Gleichungssystem $0x_1 + \cdots + 0x_n = b_i = 0$ und

Für Zeile $i, i = 1, \ldots, k$

$a_{i,i}x_i + \sum_{j=k+1}^{n} a_{i,j}x_j = b_i$

Beispiele: $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} x = b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

Wähle $x_3 = 1$. Dann folgt daraus $x_2 = -3$ und $x_1 = -2$

Wir sagen die Lösungsmenge ist

$\{(b_1 - \sum_{j=k+1}^{n} a_{1j}\xi_j), \ldots, (b_k - \sum_j = k + 1^n a_{kj}\xi_j), \xi_{k+1}, \ldots, \xi_n : \xi_{k+1}, \ldots, \xi_n \in \mathbb{R}\}$.

Wir nennen eine solche Mengen (n-k) parametrig.

2.2.2 Lemma 0.1

Sei A eine $m \times n$ -Matrix mit Rang k. Dann gilt $k = n$ genau dann, wenn alle Gleichungssysteme mit A höchstens eine Lösung haben, und k = m, genau dann, wenn alle Gleichungssyteme mit A lösbar sind.

Beweis: klar aus der Darstellung.

2.2.3 Zeilenoperationen

Eine Zeilenoperation macht aus dem Gleichungssystem ein neues Gleichungssytem durch Multiplikation der i-ten Zeile mit einer Zahl $\lambda \in \mathbb{R} \setminus 0$ oder durch addieren des λ-fachen der i-ten Zeile zur j-ten Zeile ($i \neq j$). Wir bezeichnen diese Operationen mit Z_i^λ bzw. $Z_{i,j}^\lambda$.

Bemerkung: Die Zeilenoperationen sind umkehrbar.

Die Umkehrung von $Z_i^\lambda = Z_i^{\frac{1}{\lambda}}$, die Umkehrung von $Z_{i,j}^\lambda = Z_{i,j}^{-\lambda}$

2.2.4 Lemma 0.2

Ein Gleichugnssystem G', welches aus einem Gleichungssytem G durch Zeilenoperationen hervorgeht besitzt die gleichen Lösungen wie G.

Beweis:

Für Z_I^λ : betrachten wir nur die i-te Zeile.

$a_{i,1}x_1 + \cdots + a_{i,n}x_n = b_i$

Nach Z_i^λ: $\lambda a_{i,1}x_1 + \cdots + \lambda a_{i,n}x_n = \lambda b_i$

Diese besitzen eindeutig die selbe Lösungen $\xi_1, \ldots, \xi_n$

Für $Z_{i,j}^\lambda$ ebenso.

2.2.5 Satz 0.3

Jedes lineare Gleichungssytem lässt sich durch Zeilenoperationen und Vertauschungen von Variablen (d.h. Vertauschung von Spalten) in Normalform bringen.

Beweis:

Wir beweisen dies mittels eines expliziten Algorithmus (der Gauß=Jordan Elimination).

Aus praktischen Gruenden schreiben wir unser Gleichugnssystem als sogenannte erweiterte Koeffizientenmatrix. $\begin{pmatrix} a_11 & a_12 & \ldots & a_1n & | & b_1 \\ \vdots & & & & | & \\ a_m1 & a_m2 & \ldots & a_mn & | & b_m \end{pmatrix}$

Zunaechst vergewissern wir uns, dass wir durch nacheinander Anwendung von $Z_{i,j}^1, Z_{j,i}^{-1}, Z_{i,j}^1$und Z_i^{-1} die i-te und j-te Zeile vertauschen koennen.

Sei y die i-te Zeile, z die j-te Zeile.

$$\begin{pmatrix} y \\ z \end{pmatrix} \overset{Z_{i,j}^1}{\to} \begin{pmatrix} y \\ z+y \end{pmatrix} \overset{Z_{j,i}^{-1}}{\to} \begin{pmatrix} -z \\ z+y \end{pmatrix} \overset{Z_{i,j}^1}{\to} \begin{pmatrix} -z \\ y \end{pmatrix} \overset{Z_i^{-1}}{\to} \begin{pmatrix} z \\ y \end{pmatrix}$$

Algorithmus:

Schritt 1: Falls alle Koeffizienten $a_{i,j}$ Null sind, so ist die Matrix bereits in Normalform, und es ist nichts mehr zu tun.

Falls es einen von Null Verschiedenen Koeffizienten gibt, so können wir diesen in die linke obere Ecke bringen (durch Spalten und Zeilenvertauschungen). Damit ist nun

$a_{1,1} \neq 0$. Nach $Z_1^{\frac{1}{a_{1,1}}}$ gilt $a_{1,1} = 1$. Nun wenden wir $Z_{1,2}^{-a_{2,1}}, \ldots, Z_{1,m}^{-a_{m,1}}$ und erhalten $a_{2,1} = \cdots = a_{m,1} = 0$.

Die Matrix hat nun die Form $\begin{pmatrix} 1 & a_{1,2} & \ldots & a_{1,n} & | & b_1 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & & & \\ 0 & a_{m,2} & \ldots & a_{m,n} & | & b_m \end{pmatrix}$

Schritt 2: Falls $a_{i,j} = 0$ für $2 \leq i \leq m$ und $2 \leq j \leq n$, so ist die Matrix in Normalform für k=1 und wir sind fertig. Falls nicht, so existiert $i \geq 2, j \geq 2$ mit $a_{i,j} \neq 0$.

Wir vertauschen die i-te Zeile mit der zweiten Zeile, und die j-te Spalte mit der zweiten Spalte. Damit ist $a_{2,2} \neq 0$. Nun wenden wir $Z_2^{\frac{1}{a_{2,2}}}$ Damit ist $a_{2,2} = 1$. Danach wenden wir $Z_{2,1}^{-a_{1,2}}, \ldots, Z_{2,m}^{-a_{m,2}}$ an,

und erhalten die Form: $\begin{pmatrix} 1 & 0 & a_{1,3} & \ldots & a_{1,n} & | & b_1 \\ 0 & 1 & a_{2,3} & \ldots & a_{1,n} & | & b_2 \\ 0 & 0 & & & & & \\ \vdots & & & & & & \\ 0 & 0 & a_{m,3} & \ldots & a_{m,n} & | & b_m \end{pmatrix}$

$\vdots$

Wir verwandeln Damit der Reihe nach die Spalten der Matrix in Spalten, in welchen nur der Diagonaleintrag von Null verschieden ist (dieser Eintrag ist gleich 1).

Das Verfahren terminiert, wenn die Matrix in Normalform ist, oder wenn $min(n, m)$ Schritte vollzogen sind. Auch in diesem Fall ist die Matrix in Normalform.

2.2.6 Korolar 0.4

Sei A eine Matrix mit m Zeilen und n Spalten. Weiter sei k der Rang einer Normalform von A (d.h. einer Matrix in Normalform, welche aus A durch Zeilenoperationen und Spaltenvertauschungen hervorgeht). Ein Gleichungssystem mit Matrix A besitzt dann entweder keine Lösung, oder ein (n-k) Parametriges Lösungssytem. Es gilt $k = n$ genau dann wenn jedes Gleichungssystem $Ax = b$ höchstens eine Lösung besitzt und $k = m$

genau dann wenn jedes Gleichungssytem $Ax = b$ mindestens eine Lösung besitzt.

Beweis: Folgt aus Lemma 0.2 und daraus, dass Zeilen / Spaltenoperationen die Lösungsmenge (modulo Variablentausch) nicht ändern.

2.2.7 Korolar 0.5

Ein homogenes Gleichungssystem mit weniger Gleichungen als Variablen hat mindestens eine nicht triviale Lösung.

Beweis

Es gibt für homogene Gleichungssyteme immer die triviale Lösung. Der Rang der Matrix des Gleichungssystems in Normalform sei k. Damit existiert ein (n-k) parametriges Lösungssystem, aber $k \leq min(n, m) \leq m \leq (n-1)$. Somit existiert mindestens eine weitere Lösung.

2.2.8 Definition 0.6

Eine Kollektion $a_1, \ldots, a_n$ von Vektoren in $\mathbb{R}^m$ heißt linear unabhängig, wenn sich keiner der Vektoren als Linearkombination der anderen Vektoren schreiben lässt.

Bem: Als Linearkombination von $a_1, \ldots, a_n$ bezeichnen wir einen Ausdruck der Form $\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n = \sum_{j=1}^{n} \alpha_j a_j$ für $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$

2.2.9 Lemma 0.7

Vektoren $a_1, \ldots, a_n$ sind genau dann linear unabhängig, wenn für alle $\xi_1, \ldots, \xi_n \in \mathbb{R}$ gilt falls $\xi_1 a_1 + \cdots + \xi_n a_n = 0$ dann gilt $\xi_1 = \cdots = \xi_n = 0$

Beweis

1. Falls $0 = \xi_1 a_1 + \cdots + \xi_n a_n$, und oBdA. $\xi_1 \neq 0$ so folgt $a_1 = \sum_{j=2}^{n} -\frac{\xi_j}{\xi_1} a_j$. Somit habe ich a_1 als Linearkombination von $a_2, \ldots, a_n$ geschrieben.

2. Falls aber oBdA. $a_1 = \sum_{j=2}^{n} \lambda_j a_j$ so gilt: $0 = -a_1 = \sum j = 2^n$, damit ist ξ_1 (der erste Koeffizient) von Null verschieden.

2.2.10 Lemma 0.8

Es seien $a_1, \ldots, a_n \in \mathbb{R}^m$ linear unabhängig und es gelte $b = \lambda_1 a_1 + \cdots + \lambda_n a_n$, mit $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Dann ist diese Linearkombination eindeutig.

Beweis Es sei auch $b = \mu_1 a_1 + \cdots + \mu_n a_n$. Fuer Eindeutigkeit ist nun zu zeigen, dass $\mu_i = \lambda_i, 1 \leq i \leq n$.

Wir ziehen die Gleichungen voneinander ab, und erhalten:

$b - b = (\lambda_1 - \mu_1)a_1 + \cdots + (\lambda_n - \mu_n)a_n$

$\Leftrightarrow 0 = (\lambda_1 - \mu_1)a_1 + \cdots + (\lambda_n - \mu_n)a_n$

Mit Lemma 0.7 folgt die Aussage.

2.2.11 Satz 0.9

Wenn man ein Gleichungssystem durch Zeilenoperationen und Spaltenvertauschungen auf Normalform bringt, so erhält man immer denselben Rang.

Bemerkung Man kann damit vom Rang eines Gleichungssystems (bzw. einer Matrix) sprechen, auch wenn dieses nicht in Normalform ist.

Bemerkung Ein einzelner Vektor a gilt als linear unabhängig, solange $a \neq 0$. Die leere Kollektion von Vektoren (n=0) bezeichnen wir ebenfalls als linear unabhängig.

Vor dem Beweis des Satzes 0.9 noch ein paar Feststellungen.

Die Tatsache, dass $(\xi_1, \ldots, \xi_n$ Lösung eines linearen Gleichungssystems ist laesst sich als linaere Abhaengigkeit ausdruecken

$\xi_1 a_1 + \cdots + \xi_n a_n = b$, wobei a_i eine Spalte der Matrix des Gleichungssystems ist.

Ist das Gleichungssystem in Normalform, so sind die ersten k Spaltenvektoren linear unabhängig. Die folgenden n-k Spaltenvektoren lassen sich aber als Linearkombination der ersten k darstellen, also

$\lambda_{1,i} a_1 + \cdots + \lambda_{k,i} a_k = a_i$ fuer $k < i \leq n$

mit $\lambda_{1,i} = a_{1,i}, \ldots$.

Falls das Gleichungssystem lösbar ist, kann man dank $\xi_1 a_1 + \cdots + \xi_n a_n = b$ auch b als

solche Linearkombination schreiben.
Wegen Lemma 0.8 sind diese Linearkombinationen auch eindeutig.

Beweis von Satz 0.9

Wir bemerken zunächst, dass Zeilenoperationen und Spaltenvertauschung die Anzahl linear unabhängiger Spaltenvektoren nicht ändern.
Wir überlegen uns nun, dass der Rang eines linearen Gleichungssystems nichts anderes als die maximale Anzahl linear unabhängiger Spaltenvektoren der Matrix ist.

Die ersten k Spalten sind linear unabhängig, da die Matrix in Normalform.
Seien also $a_{i_1}, \ldots, a_{i_{k+1}}$ beliebige Spaltenvektoren der Matrix des Gleichungssystems. Nachdem in diesen Vektoren alle Einträge ab dem k+1-ten Eintrag Null sind, hat das Gleichungssystem
$x_1 a_{i_1} + \cdots + x_{k+1} a_{i_{k+1}} = 0$
nur k mögliche Gleichungen. (Die Zeilen k+1 bis m in diesem Gleichungssystem sind $0 = 0$)
Nach Korolar 0.5 hat dieses homogene Gleichungssystem mir k Gleichungen und k+1 Unbekannten aber mindestens eine nicht triviale Lösung. Die Vektoren $a_{i_1}, \ldots a_{i_{k+1}}$ sind somit nicht linear unabhängig.

2.2.12 Korolar 0.10

Wird ein Gleichungssystem *nur* durch Zeilenoperationen (also ohne Variablentausch) auf Normalform gebracht, so ist die Matrix die man erhält immer die gleiche. Falls das Gleichungssystem lösbar ist, so ist auch das erhaltene b immer das gleiche.

2.3 Ein wenig euklidische Geometrie

2.3.1 Geraden und Ebenen

2.3.2 Def 0.11

1. Sei v != 0 ein Vektor in $\mathbb{R}^n$. Mit $\mathbb{R}v$ bezeichnen wir die Menge an Vektoren in $\mathbb{R}^n$der Form $\mathbb{R}v = \{\lambda v : \lambda \in \mathbb{R}\}$

2. Sei $a \in \mathbb{R}^n, v \in \mathbb{R}^n, v \neq 0$. Als (affine) Gerade bezeichnen wir die Menge der Vektoren der Form $g = \{a + \lambda v : \lambda \in \mathbb{R}\} = a + \mathbb{R}v$

Bemerkung: Der Richtungsraum $\mathbb{R}v$ einer Geraden g ist durch diese eindeutig bestimmt als Menge der Differenzen $x - y$ aus Vektoren in g.

2.3.3 Lemma 0.12

Zwei Geraden $a+\mathbb{R}v, b+\mathbb{R}w$ sind genau dann gleich, wenn gilt $\mathbb{R}v = \mathbb{R}w$ und $a-b \in \mathbb{R}v$.

Beweis

Sei also $x = a + \mathbb{R}v$, dh. $x = a + \lambda v$ für ein $\lambda \in \mathbb{R}$. Nach Annahme gilt $\mathbb{R}v = \mathbb{R}w$. Damit existiert ein $\mu \in \mathbb{R}$ mit $\lambda v = \mu w$ und somit $x = a+\mu w$. Weiteres haben wir nach Annahme, dass $a-b \in \mathbb{R}v$, also existiert ein $\xi \in \mathbb{R}$ mit $a-b = \xi w$, also $x = a-(a-b)+\xi w+\mu w$ und sommit $x = b + (\xi + \mu)w$.

Es ist also $x \in b + \mathbb{R}w$.

Die Umkehrung, also die Behauptung, dass sich ein Punkt $y \in b + \mathbb{R}w$ auch als Punkt in $a + \mathbb{R}v$ schreiben lässt, folgt analog.

2.3.4 Lemma 0.13

Durch zwei verschiedene Punkte in $\mathbb{R}^n$geht genau eine Gerade.

Beweis: Übung

2.3.5 Definition 0.14

Zwei Geraden heißen parallel, wenn sie die gleichen Richtungsgäume haben.

2.3.6 Definition 0.15

Eine (affine) Ebene ist eine Menge der Form $a+\mathbb{R}v+\mathbb{R}w$ für linear unabhängige Vektoren v, w.

Bemerkung: Auch hier gilt, das der Raum $\mathbb{R}v + \mathbb{R}w$ eindeutig bestimmt ist als Menge aller Differenzen von Punkten in der Ebene.

2.3.7 Lemma 0.16

Zwei nicht-parallele Geraden, die in einer Ebene liegen, schneiden sich.

Beweis:

Es sei $E = c + \mathbb{R}v_1 + \mathbb{R}v_2$, $g_1 = a_1 + \mathbb{R}b_1$, $g_2 = a_2 + \mathbb{R}b_2$ zwei Geraden in E.

Wir suchen ξ_1, ξ_1, so dass $a_1 + \xi_1 w_1 = a_2 + \xi_2 w_2$.

Nun schreiben wir $a_i = c + \beta_{1,i}v_1 + \beta_{2,i}v_2$ und $w_i = \alpha_{1,i}v_1 + \alpha_{2,i}v_2$ für $i = 1, 2$.

Das führt auf das Gleichungssystem

$\alpha_{1,1}\xi_1 - \alpha_{1,2}\xi_2 = -\beta_{1,1} + \beta_{1,2}$

$\alpha_{2,1}\xi_1 - \alpha_{2,2}\xi_2 = -\beta_{2,1} + \beta_{2,2}$

Nachdem g_1, g_2 nicht parallel sind, sind w_1, w_2 linear unabhängig. Damit sind aber die Spaltenvektoren der Matrix $\begin{pmatrix} \alpha_{1,1} & -\alpha_{1,2} \\ \alpha_{2,1} & -\alpha_{2,2} \end{pmatrix}$ ebenfalls linear unabhängig. Damit besitzt das Gleichungssystem eine Lösung (da $k = m$) nach Satz 0.9.

2.3.8 Das Skalarprodukt

Es seien $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ zwei Vektoren in $\mathbb{R}^n$.

2.3.9 Def 0.17

Das Skalarprodukt von a und b ist definiert als $(a, b) = \sum_{j=1}^{n} a_j b_j$.

2.3.10 Lemma 0.18

Das Skalarprodukt zweier Vektoren a und b in $\mathbb{R}^n$ist eine sogennante symmetrische, positiv definite Bilinearform, das heißt.

1. $(a, b) = (b, a)$ (symmetrisch)
2. $(a + b, c) = (a, c) + (b, c)$ (linear)
3. $\lambda a, b = \lambda(a, b)$ (linear)
4. $(a, a) \geq 0$ (positiv definit)
5. $(a, a) = 0$ genau dann, wenn $a = 0$

für alle Vektoren $a, b, c \in \mathbb{R}^n$, alle $\lambda \in \mathbb{R}$.
Bemerkung: aus 1 und 2 folgt $(a, b + c = (a, b) + (a, c)$ und $(a, \lambda b) = \lambda(a, b)$ (bilinearität).
Beweis: 1, 2, 3 sind klar aus der Definition.
4 und 5 folgen daraus, dass $(a, a) = a_1^2, \ldots, a_n^2$.

2.3.11 Def. 0.19 Norm eines Vektors

Die Norm (oder Länge) von a ist $\sqrt{(a, a)} = ||a||$.

2.3.12 Def. 0.20 Winkel zweier Vektoren

1. Der Winnkel α zwischen zwei Vektoren $a, b \neq 0$ ist definiert durch $0 \leq \alpha \leq \pi$ und $cos(\alpha) = \frac{|(a,b)|}{||a|| \cdot ||b||}$.
2. Zwei Vektoren $a, b \in \mathbb{R}^n$ heißen orthogonal, falls gilt $(a, b) = 0$.

2.3.13 Lemma 0.21 Cauchy-Schwarz'sche Ungleichung

Es gilt $|(a,b)| \leq ||a||||b||$.

Beweis:

Es gilt für jedes beliebiges $\lambda \in \mathbb{R}$:

$0 \leq (a+\lambda b, a+\lambda b) = (a,a) + 2(\lambda a, b) + \lambda^2 (b,b)$

Für $\lambda = -\frac{(a,b)}{(b,b)}$ ergibt sich

$0 \leq (a,a) - 2\frac{(a,b)^2}{(b,b)} + \frac{(a,b)^2}{(b,b)}$

Für $b = 0$ ist die Aussage des Lemmas klar. Angenommen $b \neq 0$. Es folgt:

$(a,b)^2 \leq (a,a)(b,b)$

Bemerkung: Falls a und b linear unabhängig sind so folgt $|(a,b)| < ||a||||b||$, denn dann ist $a + \lambda b \neq 0$ (für jedes $\lambda \in \mathbb{R}$) und die Ungleichung ist strikt (d.h. mit "<").

2.3.14 Lemma 0.22 Dreiecksungleichung

Es gilt $||a+b|| \leq ||a|| + ||b||$.

Beweis:

$||a+b||^2 = (a+b, a+b) = ||a||^2 + 2(a,b) + ||b||^2 \leq ||a||^2 + 2||a||||b|| + ||b||^2 = (||a|| + ||b||)^2$

2.3.15 Korollar 0.23 $||x-y||$ ist eine Metrik

Der $\mathbb{R}^n$mit dem Abstand $d(x,y) = ||x-y||$ ist ein sogennanter metrischer Raum. D.h.

1. $d(x,y) \geq 0$
2. $d(x,y) = 0 \Leftrightarrow x = y$
3. $d(x,y) = d(y,x)$
4. $d(x,z) \leq d(x,y) + d(y,z)$

für alle x, y, z in $\mathbb{R}^n$.

Wir nennen d einen Abstand.

3 Grundlegende Objekte

3.1 Elementare Aussagenlogik

Aussagen (in der Mathematik) sind sprachliche Gebilde, welche entweder wahr (w) oder falsch (f) sind.

Darstellung mittels Wahrheitstabelle:

	Aussage	
Beispiele:	A: es sind am 2.11.2017 mehr als fünf Personen im Hörsaal Rundbau.	w
	B = Der Dozent der LA in FR im WS 17/18 heißt Peter	f

3.1.1 Definition 1.1 Logische Operatoren

A, B seien Aussagen.

1. "$\neg A$", oder "nicht A" ist die Negation von A

A	$\neg A$
w	f
f	w

2. Junktoren

   $A \vee B$, "A oder B" ist wahr, wenn mindestens eine der Aussagen wahr A, B ist.

   $A \wedge B$, "A und B" ist wahr, wenn beide wahr sind.

A	b	$A \vee B$	$A \wedge B$
w	w	w	w
f	w	w	f
w	f	w	f
f	f	f	f

3. Implikationen

   $A \Rightarrow B$ ist wahr, wenn A die Aussage B impliziert.

   $A \Leftrightarrow B$ ist wahr, wenn A genau dann wahr ist, wenn B wahr ist.

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w
f	w	w	f
w	f	f	f
f	f	w	w

Beispiel Sei G ein lineares Gleichungssystem mit m Zeilen, n Spalten und Grad k. Dann gilt

$k = n \quad \Rightarrow$ Lösung immer eindeutig.

$A \quad \Rightarrow \quad B$

Um die Aussage $A \Rightarrow B$ zu zeigen, können wir annehmen, das A richtig ist und müssen folgern, das B auch richtig ist.

Bemerkung (De Morgan)

1. $(\neg A \vee \neg B) = \neg(A \wedge B)$
2. $(\neg A \wedge \neg B = \neg(A \vee B)$

3.2 Mengen und Abbildungen

Problem: Der Begriff der Menge ist sehr schwer zu definieren. (Die Menge aller Mengen die sich nicht selbst enthalten, ist zwar naiv eine Menge, macht aber keinen Sinn, da die Definition dieser Menge zum Widerspruch geführt werden kann. Objekte wie dieses machen die Definition schwer.)

Endliche Mengen kann man durch Auflistung aller Elemente angeben.

z.B. $X = \{x_1, x_2, x_3\}$

x_1, x_2, x_3 heißen dann Elemente von X und wir scheiben $x_1 \in X$.

Reihenfolge der Elemente und Mehrfachauflistung sind nicht relevant. Die Mächtigkeit einer Menge ist die Anzahl paarweise verschiedener Elemente.

$\{1, 2, 2, 3\}$ hat Mächtigkeit 3.

Die leere Menge $\{\}$ oder $\emptyset$ enthält kein Element.

3.2.1 Definition 1.2 Teilmengen und Gleichheit

1. Eine Menge Y heißt Teilmenge von X, wenn aus $x \in y$ immer folgt $x \in X$. Wir schreiben $Y \subset X$.

2. Wir sagen $X = Y$ genau dann, wenn $X \subset Y$ und $Y \subset X$
   (d.h. zwei Mengen sind gleich, wenn sie die gleichen Elemente enthalten. ("Extensenalitästsprinzip"?))

Bemerkungen

1. $\emptyset \subset M$, für jede Menge M

2. $M \subset M$, für jede Menge M

3. Wenn gilt $M \subset N$, aber nicht $M = N$, dann heißt M "echte Teilmenge" von N, wir schreiben dann $M \subsetneq N$ (Die ISO vorschrift sieht hier $\subset$ für "echte Teilmenge" und $\subseteq$ für "Teilmenge" vor, dies wird jedoch selten bentuzt.)

3.2.2 Die Natürliche Zahlen

Die einfachste unendliche Menge ist die, der natürlichen Zahlen
$\mathbb{N} = \{1, 2, 3, \dots\}$, deren Existenz wir annehmen, zusammen mit den üblichen Rechenregeln.
Die natürlichen Zahlen genügen dem Prinzip der vollständigen Induktion.
Sei $M \subset \mathbb{N}$ und es gelte:

1. $1 \in M$

2. falls $m \in M$, so ist auch $n + 1 \in M$

Dann gilt $M = \mathbb{N}$.

Durch Erweiterung von Zahlbereichen können wir aus $\mathbb{N}$auch die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$ sowie die reellen Zahlen $\mathbb{R}$konstruieren.

(ebenso die komplexen Zahlen $\mathbb{C}$)

Bemerkung

Es gilt $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

3.2.3 Teilmengen mit Eigenschaften

Aus einer Menge können wir Teilmengen Auswählen, welche durch bestimme Eigenschaften charakterisiert werden. Wir schreiben
$X' = \{x \in X : x \text{ hat Eigenschaft E}\}$ (aucch $\{x \in X | x \text{ hat Eigenschaft}\}$ ist verbreitet)

3.2.4 Definition 1.3 Mengenoperationen

Sind X, Y Mengen, so können wir bilden:

1. Die Vereinigung $X \cup Y$, ist die Menge aller Elemente, welche in X sind oder welche in Y sind.
2. Der Schnitt $X \cap Y = \{x \in X : x \in Y\}$, ist die Menge aller Elemente, die sowohl in X als auch in Y sind.
3. Für $Y \subset X$ schreiben wir $X \setminus Y$ sprich "X ohne Y" für die Menge $\{x \in X : x \notin Y\}$
4. Das "kartesische Produkt" $X \times Y$ ist die Menge aller geordneten Tupel $\{(x, y) : x \in X, y \in Y\}$

Beispiele

1. $\{1, 2, 4\} \cap \{2, 3\} = \{2\}$
2. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
3. Die Elemente der Menge $\{1, \{1\}, 2\}$ sind genau $1, \{1\}, 2$

3.2.5 Definition 1.4 Abbildungen

Seien X, Y Mengen. Als Abbildung von X nach Y bezeichnen wir eine Vorschrift f, welche jedem Element x in X genau ein Element y in Y zuordnet. Wir schreiben
$f : X \to Y,\ x \mapsto f(x)$

3.2.6 Definition 1.5 Gleichheit von Abbildungen

Zwei Abbildungen $f : X \to Y, g : X \to Y$ heißen gleich, wenn für alle $x \in X$ gilt $f(x) = g(x)$.

3.2.7 Definition 1.6 Bild und Urbild

Sei $f : X \to Y, M \subset X, N \subset Y$

1. Wir schreiben $f(M) = \{y \in Y : \text{es existiert } x \in M \text{ mit } f(x) = y\} \subset Y$ Bild von M
2. $f^{-1}(N) = \{x \in X : f(x) \in N\} \subset X$ Urbild von N

Beispiel:

1. $X = \{1, 2, 3\}$
   $Y = \{3, 4, 5, 6\}$
   $f(1) = 4, f(2) = 5, f(3) = 5$
   $M = \{1, 2\} \subset X$
   $f(M) = \{4, 5\} \subset Y$
   $f(\emptyset) = \emptyset \subset Y$
   $f(X) = \{4, 5\}$
   $N = \{3, 4, 5\}$
   $f^{-1}(N) = \{1, 2, 3\}$
   $f^{-1}(\emptyset) = \emptyset$
   $f^{-1}(\{6\}) = \emptyset$
   $f^{-1}(\{5\}) = \{2, 3\}$

2. $X = \mathbb{R}., Y = \mathbb{R}$

   $f : X \to Y, x \mapsto f(x) = x^2$

   $f([1,2]) = [1,4] \subset Y$

   $f^{-1}(\{0\}) = \{0\}$

   $f^{-1}(\{1\}) = \{-1,1\}$

   $f^{-1}(\{-1\}) = \emptyset$

Achtung: $f^{-1}(N)$ ist nur definiert für Mengen $N \subset Y$. Insebesundere ist f^{-1} (zumindest jetzt) keine Abbildung von Y nach X.

3.2.8 Definition 1.7 Einschränkung von Funktionen

Es sei $f : X \to Y$ eine Abbildung, $M \subset X$.

Die Einschränkung von f auf M ist die Abbildung $f|_M = M \to Y, x \mapsto f(x)$

Bemerkung

Der Unterschied zu f ist nur der eingeschränkte Definitionsbereich.

$f : \mathbb{R} \to \mathbb{R}, x \mapsto f(x) = x^2$

$M = R_0^+ = \{x \in \mathbb{R} : x \geq 0\}$

$(f|_M)^{-1}(\{1\}) = \{1\}$

3.2.9 Def 1.8 Injektiv und surjektiv

Es sei $f : X \to Y$ eine Abbildung.

1. f heißt injektiv, falls gilt

   $(x, x' \in X, f(x) = f(x') \Rightarrow x = x')$

2. f heißt surjektiv, falls gilt

   $f(X) = Y$

3. f heißt bijektiv, falls f injektiv und surjektiv ist.

Beispiel

$f : \mathbb{R} \to \mathbb{R}, x \mapsto f(x) = x^2$

ist nicht injektiv, da $f(-1) = f(1), 1 \neq -1$. f ist auch nicht surjektiv, da $f(x) \geq 0$.
$f|_{\mathbb{R}_0^+} : \mathbb{R}_0^+ \to \mathbb{R}$ ist injektiv, aber nicht surjektiv
$f|_{\mathbb{R}_0^+} : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ ist injektiv, und surjektiv, also bijektiv

3.2.10 Definition 1.9 f^{-1}

Es sei $f : X \to Y$ bijektiv. Wir schreiben dann $f^{-1} : Y \to X, f^{-1}(y) = x$ mit dem eindeutig definierten $x \in X$, sodass gilt $f(x) = y$.

Bemerkung

Die Sinnhaftigkeit der Definition 1.9 folgt sofort aus der Definition von bijektivität.

3.2.11 Satz 1.10

Sei X eine endliche Menge, so sind für $f : X \to X$ äquivalent:

1. f ist injektiv
2. f ist surjektiv
3. f ist bijektiv

Bemerkung Für nicht endliche Mengen haben wir einfache Gegenbeispiele:
$f : \mathbb{N} \to \mathbb{N}, x \mapsto f(x) = 2x$

Beweis

X ist eine endliche Menge, wir schreiben $X = \{x_1, \ldots, x_n\}$ mit paarweise verschiedenen x_j.

1. Wir zeigen zunächst 1. $\Rightarrow$ 2.. Zu zeigen ist also falls f injektiv ist, so ist f auch surjektiv. Dies wird impliziert durch die Aussage "Ist f *nicht* surjektiv, so ist f auch *nicht* injektiv", welche wir zeigen.
   Sei f also nicht surjektiv. Also $f(X) \neq X$. Damit besteht $f(X)$ aus $m < n$ Elementen. Verteilt man aber n Elemente in $m < n$ Schubladen, so muss eien Schublade existieren, in der mehr als ein Element ist. Damit kann f nicht injektiv sein (es existiert $x \neq x'$ mit $f(x') = f(x)$).

2. 2. $\Rightarrow$ 1.. Sei f also nicht injektiv, dann existieren nach Definition $x, x' \in X, x' \neq x$ aber $f(x) = f(x')$. Damit kann aber $f(X)$ höchstens n-1 Elemente enthalten und f ist auch nicht surjektiv.

3. 3. $\Rightarrow$ 1. trivial nach der Definition der Bijektivität

4. 3. $\Rightarrow$ 2. ebenso

5. 1. $\Rightarrow$ 3. Aus Injektivität folgt bereits Surjektivität und damit auch Bijektivität.

6. 2. $\Rightarrow$ 3. Aus Surjektivität folgt bereits Injektivität und damit auch Bijektivität.

3.2.12 Definition 1.11 Komposition von Abbildungen

Es seien X, Y, Z Mengen, $f : X \to Y, g : Y \to Z$ Abbildungen.
Dann definiert $g \circ f : X \to Z, x \mapsto g(f(x)) = (g \circ f)(x)$ die Komposition von Abbildungen.

Bemerkung
Es gilt Assoziativität: $(h \circ g) \circ f = h \circ (g \circ f)$ für $f : X \to Y, g : Y \to Z, h : Z \to A$
aber *nicht* Kommutativität, d.h. im Allgemeinen gilt nicht $f \circ g = g \circ f$ für $f : X \to X, g : X \to X$, denn
$f : \mathbb{R} \to R, f(x) = x + 1$
$g : \mathbb{R} \to \mathbb{R}, f(x) = x^2$
ist ein Gegenbeispiel, denn im Allgemeinen gilt *nicht*, dass $(x + 1)^2 = x^2 + 1$.

3.2.13 Definition 1.12 Identität

Mit $Id_X : X \to X$ bezeichnen wir die identische Abbildung $x \mapsto x$

3.2.14 Lemma 1.13 Identität und Surjektivität bzw. Injektivität

Es sei $f : X \to Y$ eine Abbildung, $X, Y \neq \emptyset$. Dann gilt:

1. f ist genau dann injektiv, wenn eine Abbildung $g : Y \to X$ existiert, mit $g \circ f = Id_X$

2. f ist genau dann surjektiv, wenn $g : Y \to X$ existiert, mit $f \circ g = Id_Y$

3. f ist genau dann bijektiv, falls $g : Y \to X$ existiert, so dass sowohl $g \circ f = Id_X$ und $f \circ g = Id_Y$. Es gilt dann $g = f^{-1}$

Beweis

1. Sei f injektiv. Dann existiert zu jedem $y \in f(X)$ genau ein $x \in X$ mit $f(x) = y$. Wir setzen $g(y) = x$ für ebensolche $y = f(x)$. Nun wählen wir $x_0 \in X$ beliebig und setzen $g(y') = x_0$ für alle $y' \in \backslash f(X)$. Dieses g erfüllt die Bedingung.
   Sei nun $g : Y \to X$ mit $g \circ f = Id_X$. Seien $x, x' \in X$ mit $f(x) = f(x')$. Es gilt $x = Id_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = Id_X(x') = x'$. Also ist f injektiv.

2. Sei f surjektiv. Zu jedem $y \in Y$ wählen wir ein $x \in X$ mit $f(x) = y$ und setzen $g(y) = x$. Damit gilt $f \circ g = Id_Y$.
   Ungekehrt, sei $g : Y \to X$, so dass $f \circ g = Id_Y$. Sei $y \in Y$, dann gilt $y = f(g(y))$. Sei $x' = g(y)$. Damit ist $y = f(x'), x' \in X$ und $y \in f(X)$. Damit ist f surjektiv.

3. Sei f bijektiv. Die nun definierte Abbildung $f^{-1} : Y \to X$ erfüllt die Voraussetzung an g.
   Falls aber g existiert, mit $g \circ f = Id_x$ und $f \circ g = Id_Y$. Damit erfüllt g die Voraussetzungen von 1. und 2. und f ist sowohl injektiv als auch surjektiv. Es gilt dann auch $g = f^{-1}$.

3.2.15 Definition 1.14 Menge aller Abbildungen

Seien X, Y Mengen. Mit $Abb(X, Y)$ bezeichnen wir die Menge aller Abbildungen von X nach Y.

Bemerkung

$\{f \in Abb(X, Y) : f \text{ surjektiv}\}$ ist nun ebenfalls definiert.

3.2.16 Definition 1.15 Mächtigkeit von Mnegen

Es seien X, Y Mengen. Wir sagen X ist gleichmächtig wie Y, falls eine bijektive Abbildung von X nach Y existiert.

Bemerkung

Für endliche Mengen M gilt $\#M = m$ genau dann, wenn M gleichmächtig wie $\{1, 2, \ldots, m\}$ ist.

3.2.17 Definition 1.16 Potenzmenge

Sei M eine Menge. Die Menge aller Teilmengen von M heißt Potenzmenge von M, kurz 2^M.

Bemerkung

Für eine (beliebige nicht notwendigerweise bijektive) Abbildung $f : X \to Y$ ist f^{-1} eine Abbildung von 2^Y nach 2^X.

3.2.18 Satz 1.17 Mächtigkeit von 2^M

Sei M eine endliche Menge mit $\#M = m$, $m \in \mathbb{N} \cup \{0\}$. Dann gilt $\#2^M = 2^m$.

Beweis

Für m = 0 gilt $M = \emptyset$ und die Aussage ist klar. (denn $2^\emptyset = \{\emptyset\}$, und diese Menge besitzt ein Element).

Rest des Beweises mittel Induktion.

Wir nennen $K \subset \mathbb{N}$ die Menge der natürlichen Zahlen m, für welche die Aussage gilt, und zeigen:

1.) $1 \in K$

2.) falls $m \in K$ so ist auch $m + 1 \in K$.

Damit folgt (nach dem Induktionsprinzip), dass K = $\mathbb{N}$ und der Satz ist gezeigt.

Zu 1.) Die einelementige Menge M schreiben wir als $\{x\}$, die Teilmengen sind $\emptyset, \{x\}$. Somit ist $2^M = \{\emptyset, \{x\}\}$ mit $\#2^M = 2 = 2^1$.

Zu 2.) Es sei also $\#M = m + 1$ und M_m eine Menge mit $\#M_m = m$. Wir dürfen annehmen, dass gilt $\#2^{M_m} = 2^m$. Wir schreiben M als $M_m \cup \{x\}, x \notin M_m$. Wir scheiben

$2^M = \{$Menge aller Teilmengen von M, welche x nicht enthalten$\} \cup \{$Menge aller Teilmengen von M, welche x enthalten$\} = A \cup B$ und es gilt $\#2^M = \#A + \#B$.

$\#A = \#2^{M_m} = m$, da $A = 2^{M_m}$.

Jede Menge in B ist aber eine Menge in 2^{M_m} vereinigt mit $\{x\}$ und $\#B = 2^m$. Somit gilt $\#2^M = 2^m + 2^m = 2^{m+1}$.
Damit gilt die Aussage für $m + 1$.

Wir kennen bereits das direkte (bzw. kartesische) Produkt zweier Mengen $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

3.2.19 Definition 1.18 Graph einer Funktion

Es sei $f : X \to Y$ eine Abbildung. Die Menge $\Gamma_f = \{(x, f(x)) \in X \times Y\}$ nennen wir Graph von f.

Noch nützlicher ist das direkte Produkt um eine sogenannte Relation zu definieren.

Beispiele

$x \underset{\text{(Steht in Relation zu)}}{\sim} y \Leftrightarrow x \leq y$

3.2.20 Definition 1.19 Relationen

Eine Relation R auf einer Menge X ist eine Teilmenge von $X \times X$.
Wir sagen für $x, y \in X$, dass $x \sim y$ genau dann, wenn $(x, y) \in R$.

Für das Beispiel gilt $R = \{(x, y) \in X \times X : x \leq y\}$

3.2.21 Definition 1.20 Äquivanlenzrelation

Eine Relation $\sim$ auf X heißt Äquivalenzrelation, falls gilt:

1. $x \sim x$ (Reflexivität)
2. $x \sim y \Rightarrow y \sim x$ (Symmetrie)

3. $x \sim y \wedge y \sim z \Rightarrow x \sim z$ (Transitivität)

für alle $x, y, z \in X$

Beispiele:

"=" auf Zahlensystemen.

$X = 2^N$. Für $x, y \in X$ gelte $x \sim y$ falls endliche Teilmengen A, B von x und y mit $x \setminus A = y \setminus B$

3.2.22 Definition 1.21 Äquivalenzklassen

Sei X eine Menge mit Äquivalenzrelation "$\sim$". Eine Menge $A \subset X$ heißt Äquivalenzklasse bezüglich "$\sim$", falls gilt:

1. $A \neq \emptyset$
2. falls $x, y \in A \Rightarrow x \sim y$
3. $x \in A, y \in X, x \sim y \Rightarrow y \in A$

3.2.23 Proposition 1.22 Partitionierung in Äquivalenzklassen

Sei X eine Menge mit Äquivalenzrelation "$\sim$". Dann gehört jedes $a \in X$ zu genau einer Äquivalenzklasse A bezüglich "$\sim$".
Für zwei Äquivalenzlkassen A, A' gilt entweder $A = A'$ oder $A \cap A' = \emptyset$.

Beweis

Für $a \in X$ definieren wir die Menge $A = \{x \in X : a \sim x\}$.
Nachdem $a \sim a$ gilt $a \in A$, somit ist $A \neq \emptyset$. Sind nun $x, y \in A$, so gilt $a \sim x \wedge a \sim y$. Damit folgt $x \sim a$ und $a \sim y$ und somit $x \sim y$.
Für $x \in A, y \in X$ mit $x \sim y$. gilt $a \sim x, x \sim y$ also $a \sim y$ und somit $y \in A$.
Somit ist A eien Äquivalenzklasse und a ist in *mindestens* einer Äquivalenzklasse enthalten.
Es ist noch zu zeigen, dass zwei Äquivalenzklassen entweder gleich oder disjunkt sind.
Seien also A, A' Äquivalenzklassen mit $A \cap A' \neq \emptyset$. Also existiert $b \in A \cap A'$. Falls nun

$x \in A$, so gilt $x \sim b$. Nachdem b auch in A' ist, folgt aber $x \in A'$. Damit folgt $a \subset A'$. Die Umkehrung, also $A' \subset A$ folgt ebenso.

3.2.24 Definition 1.23 Quotientenmenge

Es sei X eine Menge mit Äquivalenzrelation "$\sim$". Die Menge der Äquivalenzklassen in X bezeichnen wir als Quotientenmenge und schreiben für diese Menge $X/\sim$

Bemerkung

Wir können eine Abbildung definieren, welche jedem $a \in X$ dessen Äquivalenzklasse zuordnet:

$X \to x/\sim, a \mapsto A_a$ (nach Prop 1.22 eindeutig zugeorndete Äquivalenzklasse).

Ein solches a heißt dann Repräsentant der Äquivalenzklasse A_a.

Beispiel

Sei X = $\mathbb{N}$. Wir schreiben $X \sim y$, falls sowohl x als auch y gerade bzw. ungerade Zahlen sind.

Sei $a \in X$. Die zughörige Äquivalenzklasse ist gegeben durch:

Die Menge aller geraden Zahlen, falls a gerade ist.

Die Menge aller ungeraden Zahlen, falls a ungerade ist.

3.3 Gruppen

3.3.1 Definition 1.24 Verknüpfungen

Es sei G eine Menge. Eine Verknüpfung $*$ auf G ist eine Abbildung:

$* : G \times G \to G$.

$(a, b) \mapsto *(a, b)$

Bemerkung Oft schreiben wir einfach $a * b$ für $*(a, b)$.

Beispiele

$G = \mathbb{N}, *(a, b) = a \cdot b$

$G = \mathbb{N}, *(a,b) = a + b$

X Menge, $G = Abb(X,X), *(f,g) = f \circ g$

Definition 1.25 Gruppen

Eine Menge G mit Verknüpfung $*$ heißt Gruppe, falls gilt:

1. $(a * b) * c = a * (b * c)$ (Assoziativgesetzt)
2. Es existiert ein Element $e \in G$, so dass gilt:
   a) $a * e = a$ für alle $a \in G$
   b) Für alle $a \in G$ existiert $a' \in G$ mit $a' * a = e$

Die Gruppe heißt abelsch, falls zusätzlich gilt $a * b = b * a$ für alle $a, b \in G$.

e aus 2. a.) heißt neutrales Element.

a' ais 2. b.) heißt inverses Element.

Bemerkung

Wir schreiben oft einfach $a \cdot b$ bzw. ab für $a * b$.

Beispiele

1. $G = \mathbb{Z}, *(a,b) = a + b$ $(e = 0, a' = -a)$
2. $G = \mathbb{Q} \setminus \{0\}, *(a,b) = a \cdot b$ $(e = 1, a' = \frac{1}{a})$
3. $G = \{f \in Abb(X,X), f \text{ bijektiv}\}, *(f,g) = f \circ g$ $(e = Id_X, f^{-1}$ als inverses)

Achtung: 1 und 2 sind abelsch, 3 nicht notwendigerweise.

3.3.2 Propostition 1.26 Eindeutigkeit neutrales und inverses

Es sei G eine Gruppe. Dann gilt

1. Das neutrale Element ist eindeutig bestimmt, und es gilt auch $a * e = a$
2. Das inverse Element a' ist zu jedem $a \in G$ eindeutig bestimt und es gilt auch $a * a' = e$

Beweis

Wir betrachten ein $e \in G$ und ein $a \in G$, wobei e ein neutrales Element ist. Es sei a' ein Inverses zu a. Es folgt:

$aa' = e(aa') = (a''a')(aa') = a''(a'(aa')) = a''((a'a)a') = a''(ea') = a''a' = e$

Somit gilt $ae = a(a'a) = (aa')a = a$.

Sei $\hat{e}$ ein anderes neutrales Element. Dann gilt $e\hat{e} = e$ und $e\hat{e} = \hat{e}$. Damit folgt $e = \hat{e}$.

Sei nun $\hat{a}'$ ein weiteres inverses Element, dann folgt:

$\hat{a}' = \hat{a}'e = \hat{a}'(aa') = (\hat{a}'a)a' = ea' = a'$

Bemerkungen

1. Wir schreiben a^{-1} für das (nun) eindeutig bestimmte inverse Element zu a.
   Es gilt also $a^{-1}a = aa^{-1} = e$ sowie $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$
   (denn $b^{-1}a^{-1})(ab) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$

2. Es folgen auch die Kürzungsregeln:
   $a\hat{x} = ax \Rightarrow x = \hat{x}$
   und $\hat{y}a = ya \Rightarrow y = \hat{y}$

3.3.3 Definition 1.27 Rechts- und Linkstranslation

Für $a \in G$, G eine Gruppe, schreiben wir

$\tau_a : G \to G, x \mapsto xa$ (Rechtstranslation)

${}_a\tau : G \to G, x \mapsto ax$ (Linkstanslation)

3.3.4 Lemma 1.28

1. Falls G eine Gruppe ist, so sind τ_a und ${}_a\tau$ bijektiv.

2. Sei G eine Menge mit assoziativer Verknüpfung. Dann folgt Def 1.25 2. aus surjektivität von t_a und ${}_a\tau$

Beweis

1. Bijektivität folgt aus $(\tau_a)^{-1}$ gegeben durch $(\tau_a)^{-1}(x) = xa^{-1}$, denn $(tau_a)^{-1}(\tau_a(y)) = \tau_a(y)a^{-1} = (ya)a^{-1} = y$ für jedes $y \in G$.

2. Seien also τ_a und ${}_a\tau$ surjektiv. Dann existiert für jedes $b \in G$ eine Lösung für:
   $xa = b$ sowie $ay = b$.
   Damit existiert aber zu $a \in G$ ein e mit $ea = a$. Für beliebiges $b \in G$ folgt dann $eb = e(ay) = (ea)y = ay = b$
   Durch Lösen von $xa = e$ bekommen wir analog das Inverse Element zu a.

Bemerkungen

1. Falls die Gefahr der Verwechslung besteht, scheiben wir gerne $(G, *)$ Ffür eine Gruppe G mit Verknüpfung $*$.
   Beispielsweise $(\mathbb{Q}, +)$ für $\mathbb{Q}$mit Addition, oder $(\mathbb{Q}\setminus 0, \cdot)$ für $\mathbb{Q}\setminus 0$ mit Multiplikation.

2. Bei der Verknüpfung + gehen wir immer von kommutativität aus.

3. Endliche Gruppen kann man mit einer (Gruppen-) Tafel darstellen

$*$	e	$\cdots$	a_i
e	e		a_i
$\vdots$			
a_j	a_j		$a_i * a_j$

4. Es gibt nur eine zweielementige Gruppe:

$*$	e	a
e	e	a
a	a	e

3.3.5 Definition 1.29 Untergruppen

Es sei $(G, \cdot)$ eine Gruppe, $G' \subset G$. G' heißt Untergruppe von G, falls für $a, b \in G'$ auch gilt $ab \in G'$ und $a^{-1} \in G'$.

3.3.6 Definition 1.30 Homo- und Isomorphismen auf Gruppen

Seien $(G, \cdot), (H, *)$ Gruppen, und $\varphi : G \to H$ eine Abbildung.

1. Die Abbildung φ heißt Homomorphismus, falls gilt, dass
   $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ für alle $a, b \in G$
2. φ heißt Isomorphismum, falls φ zusätzlich bijektiv ist.

3.3.7 Proposition 1.31 Untergruppen sind Gruppen

Es sei $(G, \cdot)$ eine Gruppe, G' eine Untergruppe von G. Dann ist $(G', \cdot)$ selbst eine Gruppe.

Beweis

Assoziativität folgt sofort. Es ex a^{-1} in G', somit auch $e = aa^{-1} \in G'$.

3.3.8 Proposition 1.32 Eigenschaften von Homomorphismen

Sei $\varphi : G \to H$ ein Homomorphismus von Gruppen $(G, \cdot), (H, *)$. Dann gilt

1. $\varphi(e) = \hat{e}$ mit neutralen Elementen $e \in G, \hat{e} \in H$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für alle $a \in G$
3. Für einen Isomorphismus φ ist auch φ^{-1} ein Homomorphismus

Beweis

1. $\hat{e} * \varphi(e) = \varphi(e) = \varphi(e \cdot e) = \varphi(e) * \varphi(e)$
   Nach der Kürzungsregel folgt $\hat{e} = \varphi(e)$
2. Aus 1. gilt $\hat{e} = \varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1}) * \varphi(a)$ also ist $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. Wir betrachten $c, d \in H$ mit $c = \varphi(a), d = \varphi(b)$. Dann gilt
   $\varphi(ab) = \varphi(a) * \varphi(b) = c * d$
   also $\varphi^{-1}(c * d) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(c)\varphi^{-1}(d)$

Beispiele

1. $G = (\mathbb{R}, +), H = (\{x \in \mathbb{R} : x > 0\}, \cdot)$

   $exp : \mathbb{R} \to \mathbb{R}_*^+, x \mapsto e^x$

   ist ein Isomorphismus, denn $e^{x+y} = e^x e^y$.

2. Wir betrachten $(\mathbb{Z}, +)$. Sei $m \in \mathbb{Z}$. Dann ist $\varphi_m : \mathbb{Z} \to \mathbb{Z}, a \mapsto ma$ ein Homomorphismus, denn $m(a + b) = ma + mb$.

   Das Bild $\phi_m(\mathbb{Z}) = m\mathbb{Z} = \{ma : a \in \mathbb{Z}\} \subset \mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Z}, +)$, denn $ma + mb = m(a + b) \in m\mathbb{Z}$ und $-(ma) = m(-a) \in m\mathbb{Z}$.

   Dazu betrachten wir die Menge $r + m\mathbb{Z}$ (für $r \in \{0, 1, \ldots, m - 1\}$) mit $r + m\mathbb{Z} = \{r + ma : a \in \mathbb{Z}\}$. Dann gilt $\mathbb{Z} = (0 + m\mathbb{Z}) \cup (1 + m\mathbb{Z}) \cup \cdots \cup (m - 1 \cup m\mathbb{Z})$ und die Vereinigung ist disjunkt.

   Für $a \in \mathbb{Z}$ gilt $\frac{a}{m} = k + \frac{r}{m}$ für $k \in \mathbb{Z}, r \in \{0, \ldots, m - 1\}$ (Division mit Rest).

   Dann gilt $a \in r + m\mathbb{Z}$. (denn $a = km + r$).

   Wir beseichnen die Mengen $r + m\mathbb{Z}$ auch als sogenannte "*Restklassen modulo* m".

   Falls a, a' in derselben Klasse $r + m\mathbb{Z}$ sind, gilt $\frac{a-a'}{r} \in \mathbb{Z}$, und wir schreiben $a \equiv a'$ mod m (ist kongruent zu).

   Zu $a \in \mathbb{Z}$ schreiben wir $\bar{a} = a + m\mathbb{Z}$, die zu a gehörige Restklasse und wir definieren eine Addition $\bar{a} + \bar{b} = \overline{a + b}$.

   Wir müssen sicherstellen, dass die Definition nicht von der Auswahl des Repräsentanten abhängt, das ist aber leicht zu sehen.

   $\bar{a} = \bar{a'}, \bar{b} = \bar{b'}$, dann folgt auch schon, dass gilt $\overline{a + b} = \overline{a' + b'}$.

Satz

Für $m \in \mathbb{N}$ sei $Z/m\mathbb{Z} = \{\bar{0}, \ldots, \overline{m - 1}\}$.

Dann gilt, dass $\mathbb{Z}/m\mathbb{Z}, +$ (+ def. wie oben) eine abelsche Gruppe ist.

Die Abbildung $Z \to Z/m\mathbb{Z}, a \mapsto \bar{a} = a + m\mathbb{Z}$ ist ein surjektiver Homomorphismus.

Beweis: Übung.

Wir nennen diese Gruppen die zyklischen Gruppen der Ordnung m.

3.4 Ringe und Körper

3.4.1 Def 1.33 Ringe

Es sei R eine Menge, $+ : R \times R \to R$ und $\cdot : R \times R \to R$ Verknüpfungen. $(R, +, \cdot)$ heißt Ring, falls:

1. $(R, +)$ ist eine abelsche Gruppe
2. Die Multiplikation $\cdot$ assoziativ ist.
3. Das Distributivgesetz gilt:
   $a \cdot (b + c) = ab + ac$
   $(b + c) \cdot a = ba + ca$

Ein Ring heißt kommutativ, falls gilt $a \cdot b = b \cdot a$ für alle $a, b \in R$.
Falls ein Element $1 \in R$ existiert mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$, dann nennen wir dieses Element Einselement.
Das neutrale Element der Addition + heißt Nullelement (oder 0).

3.4.2 Proposition 1.34 Absorption durch Nullelement

Es gilt $0 \cdot a = a \cdot 0 = 0$.

Beweis

Wir erinnern uns an die Kürzungsregel: $\alpha + \xi = \beta + \xi \Rightarrow \alpha = \beta$.
Wir schreiben $0 + 0a = 0a = (0 + 0)a = 0a + 0a \Rightarrow 0 = 0a$
Ebenso folgt $0 = a0$.

Beispiele

1. $(\mathbb{Z}, +\cdot)$, $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +\cdot)$.
2. $\mathbb{Z}.m\mathbb{Z}$ mit + wie bisher und $\bar{a} \cdot \bar{b} = \overline{ab}$ (Nach Überprüfung der Unabhängigkeit von der Wahl des Repräsentanten)

Beispiel

Die 2x2-Matrizen $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bilden einen Ring mit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ac+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Die gewünschten Eigenschaften folgen sofort. Es gilt aber:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

3.4.3 Definition 1.35 Unterring und Ringhomomorphismus

1. Es sei $(R, +, \cdot)$ ein Ring, $R' \subset R$. $(R', +, \cdot)$ heißt Unterring, falls $(R', +)$ eine Untergruppe von $(R, +)$ ist und gilt $a, b \in R' \Rightarrow ab \in R'$

2. Es seien $(R, +, \cdot)$, $(S, \hat{+}, \hat{\cdot})$ Ringe, $\varphi : R \to S$ eine Abbildung. φ heißt Ringhomomorphismus, falls gilt $\varphi(a + b) = \varphi(a)\hat{+}\varphi(b)$ und $\varphi(ab) = \varphi(a)\hat{\cdot}\varphi(b)$ für alle $a, b \in R$.

3.4.4 Definition 1.36 Körper

Es sei K eine Menge, $+ : K \times K \to K, \cdot : K \times K \to K$ Verknüpfungen. $(k, +, \cdot)$ heißt Körper, falls gilt:

1. $(K, +)$ ist eine abelsche Gruppe

2. K^* sei gegeben durch $K \setminus \{0\}$. Dann gilt $(K^*, \cdot)$ ist eine abelsche Gruppe.

3. Für $a, b, c \in K$ gilt $a(b + c) = ab + bc$ und $(b + c)a = ba + ca$

Bemerkung

Das neutrale Element der Multiplikation bezeichnen wir mit Eins (= 1), das Inverse zu a bezüglich der Multiplikation mit a^{-1} oder $\frac{1}{a}$, bezüglich der Addition mit $-a$.

3.4.5 Proposition 1.37 Rechenregeln für Körper

Sei $(K, +, \cdot)$ ein Körper. Dann gilt

1. $1 \neq 0$
2. $0a = a0 = 0$
3. $ab = 0 \Rightarrow a = 0 \vee b = 0$
4. $a(-b) - (ab)$ und $(-a)(-b) = ab$
5. $xa = \hat{x}a$ und $a \neq 0 \Rightarrow x = \hat{x}$

Beweis

1. Folgt sofort, denn $(K^*, \cdot)$ ist eine Gruppe.
2. Folgt analog zu Ringen.
3. Folgt aus Gruppeneigenschaft von $(K^*, \cdot)$, da $(K^*, \cdot)$ unter der Multiplikation abgeschlossen ist, und somit a oder b nicht in K^* sein kann (also 0 ist)
4. Wir rechnen
   $ab + a(-b) = a(b - b) = a0 = 0$
   und
   $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$
5. Die Regel gilt für $x, \hat{x}$ beide in K^*. Ist aber $\hat{x} = 0$, so gilt $\hat{x}a = 0$ nach 2. und mit 3. folgt die Aussage.

Beispiele

1. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$.
2. Die komplexen Zahlen $\mathbb{C}$, wie folgt definiert. Für $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ sei
   $(a, b) + (c, d) = (a + c, b + d)$ und
   $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Mit $(0,0)$ als Nullelement und $(1,0)$ als Einselement.

Das additive Inverse zu (a,b) ist dann $(-a,-b)$, das Multiplikative Inverse ist $(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$

Wir bezeichnen den so konstruierten Körper mit $\mathbb{C}$.

Die Abbildung $\mathbb{R} \to \mathbb{C}, a \mapsto (a,0)$ ist injektiv. Wir sehen, dass zwischen $\mathbb{R} \times \{0\}$ und $\{(a,b) \in \mathbb{C} : b = 0\}$ nicht unterschieden werden muss, denn

$(a,0)(b,0) = (ab,0)$

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

Wir schreiben $i = (0,1) \in \mathbb{C}$ und $(a,b) = (a,0) + (0,b) = a + ib$.

Es gilt $i^2 = ii = -1$. Weiterhin schreiben wir für $z = (a,b) \in \mathbb{C}, \bar{z} = (a,-b)$. (bzw. $z = a + ib, \bar{z} = a - ib$). (Komplex konjugiertes)

Für komplexe Zahlen λ, μ gilt dann $\overline{\lambda + \mu} = \bar{\lambda} + \bar{\mu}$ sowie $\overline{\lambda\mu} = \bar{\lambda}\bar{\mu}$ und $\lambda \in R \Leftrightarrow lb = \bar{\lambda}$

Für $\lambda = a + ib \in \mathbb{C}$ sehen wir $\lambda\bar{\lambda} = (a+bi)(a-bi) = a^2 + b^2 \in \mathbb{R}$ und wir definieren den Absolutbetrag $|\lambda| = \sqrt{\lambda\bar{\lambda}}$.

Damit gilt, dass $d(\lambda,\mu) = |\lambda - \mu|$ ein Metrik im Sinne von Kap 0 darstellt. (denn

$d(\mu,\lambda) = d(\lambda,\mu)$,

$d(\mu,\lambda) = 0 \Leftrightarrow \lambda = \mu$,

$d(\mu,\lambda) + d(\lambda,\kappa) \geq d(\mu,\kappa)$)

(Das ist die selbe Metrik, die bereits im $\mathbb{R}^2$ eingeführt wurde.)

$d(x,y) = \sqrt{(x-y, x-y)} = \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2}$ mit $((\xi,\eta) = \xi_1\eta_1 + \xi_2\eta_2)$.

Neu ist die Identität $|\lambda \cdot \mu| = |\lambda||\mu|$

Wir betrachten noch eine geometrische Anschauung der komplexen Zahlen. Es sei $\lambda \in \mathbb{C}$ mit $|\lambda| = 1$. Dann gilt, dass $\lambda^{-1} = |\frac{1}{\lambda}| = 1$ (folgt aus der Formel für das Inverse bezgl. Multiplikation in $\mathbb{C}$).

In der Analysis lernen wir, dass gilt:

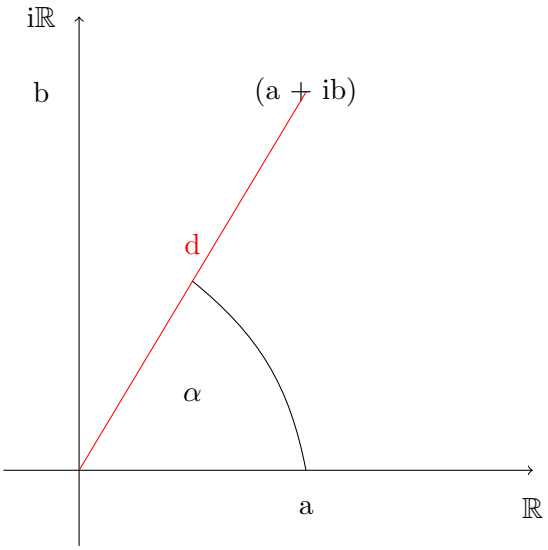
- es existiert ein eindeutiges $\alpha \in [0, 2\pi)$, so dass $\lambda = cos(\alpha) + i\sin(\alpha) = e^{i\alpha}$ für $\lambda \in \mathbb{C}, |\lambda| = 1$.

Wir bezeichnen α als Argument von λ, also $\alpha = \arg\lambda$.

Sei nun $\lambda \in \mathbb{C} \setminus 0$ beliebig (d.h. ohne die Einschänkung, dass $|\lambda| = 1$). Dann schreiben wir $\arg \lambda = \arg \frac{\lambda}{|\lambda|}$, denn $|\frac{\lambda}{|\lambda|}|$.

Damit gilt $\lambda = |\lambda| e^{i \arg \lambda}$ (für jedes $\lambda \in \mathbb{C}$).

In der komplexen Ebene $\mathbb{C} = \mathbb{R}^2$ gilt dann:



mit $d = |\lambda|, \alpha = \arg \lambda$.

Wir sehen nun, dass gilt $\lambda\mu = |\lambda| e^{i \arg \lambda} \cdot |\mu| e^{i \arg \mu} = |\lambda||\mu| e^{e \arg \lambda} e^{i \arg \mu} = |\lambda||\mu| e^{i(\arg \lambda + \arg \mu)}$.

D.h. Beträge werden multipliziert, Argumente addiert bei der Multiplikation in $\mathbb{C}$.

3.4.6 Definition 1.38 Nullteilerfreiheit von Ringen

Ein Ring $(R, +, \cdot)$ heißt Nullteilerfrei, falls für $a, b \in R$ gilt $ab = 0 \Rightarrow a = 0 \vee b = 0$.

Bemerkung

Wir sehen, dass jeder Körper bereits ein nullteilerfreier Ring ist.

Beispiele

Auf $\mathbb{Z}/m\mathbb{Z}$ ist bereits eine Addition definiert, mit der $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe wird. Mit der Multiplikation

$\bar{a} \cdot \bar{b} = \overline{ab}$

für $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ und Repräsentanten a und b wird $\mathbb{Z}/m\mathbb{Z}$ zu einem Ring

Wie für die Addition zeigen wir unabhängigkeit von der Wahl der Repräsentanten.

(Assoziativität und Distributivgesetz sind leicht Nachzurechnen.) Der Ring ist kommutativ.

3.4.7 Satz 1.39 Nullteilerfreiheit des Restklassenrings

Der Restklassenring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann nullteilerfrei, wenn m eine Primzahl ist.

Beweis

Falls m nicht prim ist, gilt $m = k \cdot l$ mit $1 < k, l < m$. Damit gilt $\bar{k} \neq \bar{0}, \bar{l} \neq \bar{0}$, aber $\bar{k}\bar{l} = \overline{kl} = \bar{m} = \bar{0}$.

Umgekehrt: Sei m prim und $\bar{k}\bar{l} = 0$. Dann gilt $k \cdot l = r \cdot m$, für ein $r \in \mathbb{Z}$. Damit gilt aber, dass mindestens einer der Faktoren k, l einen Faktor m enthält. Also ist $\bar{k} = 0$ oder $\bar{l} = 0$.

3.4.8 Satz 1.40

Ein nullteilerfreier, kommutativer Ring K mit endlich vielen Elementen und Eins ist ein Körper.

Beweis

Nach Lemma 1.28 reicht es zu zeigen, dass die Abbildung ${}_a\tau : K^* \to K^* : {}_a\tau(x) = ax$ für jedes $a \in K^*$ surjektiv ist. K^* ist eine endliche Menge, also folgt surjektivität aus injektivität. Sei also ${}_a\tau(x) = {}_a\tau(y)$, für x, y aus K^*. Es folgt $ax = ay$, also $a(x - y) = 0$. Damit gilt aber (wegen Nullteilerfreiheit und $a \in K^*$, also $a \neq 0$), dass $x - y = 0$, also $x = y$.