Kapitel II: Algebraische Strukturen

Wir werden in diesem Kapitel folgende algebraische Strukturen betrachten:

- **Gruppen**
- **Ringe und Körper**
- **Vektorräume.**

2.1 Kapitel (II.1): Gruppen

2.1.1 Definition (II.1.a): Verknüpfungen

Sei M eine nicht leere Menge, (sei $M \times M = \{(a,b) | \, a, b \in M\}$). Eine Verknüpfung (Komposition) auf M ist eine Abbildung $f : M \times M \to M$.
Beispiele:

(a) $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, (a,b) \mapsto a + b$

(b) $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, (a,b) \mapsto a \cdot b$

(c) $f_1 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a,b) \mapsto a^b$

(d) $\mathbf{max} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a,b) \mapsto \mathbf{max}\,\{a,b\}$

(e) $\mathbf{min} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a,b) \mapsto \mathbf{min}\,\{a,b\}$

(f) $\mathbf{ggT} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a,b) \mapsto \mathbf{ggT}\,\{a,b\}$

(g) $\mathbf{kgV} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a,b) \mapsto \mathbf{kgV}\,\{a,b\}$

2.1.2 Definition (II.1.b): Abbildungen Abb (M, M)

Wir definieren: Abb $(M, M) = \{f : M \to M\}$ (Menge der Abbildungen von M nach M)
Hier ein Beispiel für Verknüpfungen:
$M \xrightarrow{f} N \xrightarrow{g} P$ **liefert** $g \circ f : M \to P$, $m \mapsto g(f(m))$.
Lies "$g \circ f$" als "Verknüpfung von f, g", "Komposition von f, g" oder als "Hintereinanderausführung von f, g".
Standardverknüpfung auf Abb (M, M):

$$\begin{aligned} \mathbf{Abb}\,(M,M) \times \mathbf{Abb}\,(M,M) &\to \mathbf{Abb}\,(M,M) \\ (f,g) &\mapsto g \circ f \end{aligned}$$

Beispiel: Sei $M = \mathbb{R}$ und f: $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ und g: $\mathbb{R} \to \mathbb{R}, x \mapsto (x+1)^2$
Nun gilt:

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g\left(x^3\right) = \left(x^3 + 1\right)^2 \\ (f \circ g)(x) &= f(g(x)) = f\left(x^2 + 1\right) = \left(x^2 + 1\right)^3 \end{aligned}$$

Wie man leicht sieht spielt die Reihenfolge eine Rolle.

2.1.3 Definition (II.1.c): Assoziativität

Eine Verknüpfung auf M heißt assoziativ, wenn gilt:

$$\forall a, b, c \in M : (ab)\, c = a\,(bc)$$

Anmerkung: Wir verwenden keine Operatoren im allgemeinen Fall, es gilt: $(a, b) \mapsto ab$**.**
Beispiel für Assoziativität: $+ : (a + b) + c = a + (b + c)$**.**
Sei f_1 **gegeben mit** $f_1\,(x, y) = x^y$
Nun wollen wir f_1 **auf Assoziativität untersuchen. Allgemein ergibt sich:**

- **für die linke Seite:** $f_1\,(f_1\,(a, b)\,, c) = \left(a^b\right)^c$**.**
- **für die rechte Seite:** $f_1\,(a, f_1\,(b, c)) = a^{b^c}$**.**

Wir vermuten, daß die Assoziativität nicht gegeben ist. Deshalb probieren wir aus:

$$\begin{aligned} \left(2^3\right)^4 &= 4096 \\ 2^{3^4} &= 2^{81} \approx 10^{0.3\cdot 81} \approx 10^{24.3} \ggg 4096 \end{aligned}$$

Wir haben ein Gegenbeispiel für eine Aussage gefunden die allgemein gültig sein soll. Also ist f_1 **nicht assoziativ.**
Wichtig: Verknüpfungen auf Abb (M, M) **sind assoziativ.**
Gegeben: $M \xrightarrow{f} N \xrightarrow{g} P \xrightarrow{h} Q$**. Nun gilt:** $h \circ (g \circ f) = (h \circ g) \circ f$**.**
Beweis: Auf der linken Seite:

$$h \circ (g \circ f)\,(m) \overset{\textbf{Def.}}{=} h\,((g \circ f)\,(m)) \overset{\textbf{Def.}}{=} h\,(g\,(f\,(m)))$$

Auf der rechten Seite ergibt sich:

$$((h \circ g) \circ f)\,(m) \overset{\textbf{Def.}}{=} (h \circ g)\,(f\,(m)) \overset{\textbf{Def.}}{=} h\,(g\,(f\,(m)))$$

2.1.4 Definition (II.1.d): Symmetrische Gruppe S_n, Permutation

Wir definieren die Gruppe S_n **als:**

$$\mathrm{S}_n = \{\textbf{invertierbare Abb}\,(\{1, \ldots, n\}\,, \{1, \ldots, n\})\,, \circ\}$$

Es gilt: $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$**, dabei stehen in der oberen Zeile die Elemente und in der unteren Zeile die Bilder.** σ **ist invertierbar** $:\Leftrightarrow \exists$ **Umkehrabbildung (**$\Leftrightarrow \sigma$ **ist bijektiv).**
Ist eine Abbildung bijektiv, so ist diese injektiv und surjektiv:

$$\begin{aligned} f : M \to N : \textbf{surjektiv} &:\Leftrightarrow \forall y \in N\, \exists x \in M : y = f\,(x) \\ f : M \to N : \textbf{injektiv} &:\Leftrightarrow \forall m_1, m_2 \in M : m_1 \neq m_2 \Rightarrow f\,(m_1) \neq f\,(m_2) \end{aligned}$$

σ **bijektiv** $\Leftrightarrow$ **alle** i_j **sind paarweise verschieden** $\Leftrightarrow$ **"2. Zeile ist eine Permutation der 1. Zeile".**

Definition und Notation:

$$\mathbf{S}_n \quad := \quad (\{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}, \sigma\, \textbf{bijektiv}\}, \circ)$$

$\mathbf{S}_n$ nennt man die symmetrische Gruppe von n Ziffern. Elemente von $\mathbf{S}_n$ werden als Permutationen bezeichnet.

Man benötigt für die Definition der symmetrischen Gruppe S_n folgende Tatsache: f, g bijektiv $\Rightarrow f \circ g$ bijektiv.

Genereller Sachverhalt:

$$\begin{aligned} f, g\, \textbf{injektiv} \quad &\Rightarrow \quad f \circ g\, \textbf{injektiv} \\ f, g\, \textbf{surjektiv} \quad &\Rightarrow \quad f \circ g\, \textbf{surjektiv} \end{aligned}$$

Anmerkung: Bei einer Komposition von Abbildungen zuerst immer die letzte Anwenden.

Beweis:

$$M \xrightarrow{g} N \xrightarrow{f} P$$

Zuerst die Injektivität: $\forall m_1, m_2 \in M : m_1 \neq m_2 \Rightarrow g(m_1) \neq g(m_2) \Rightarrow f(g(m_1)) \neq f(g(m_2)) \Leftrightarrow (f \circ g)(m_1) \neq (f \circ g)(m_2)$. Die erste Folgerung beruht auf der Injektivität von g, die zweite Folgerung beruht auf der Injektivität von f.

Nun die Surjektivität: Zu zeigen: $\forall p \in P\, \exists m \in M : p = (f \circ g)(m)$.

Sei $p \in P$ gegeben, dann gibt es wegen der Surjektivität von f ein $n \in N : p = f(n)$. Weil g surjektiv ist $\exists m \in M : n = g(m)$. Einsetzen liefert:

$$p = f(g(m)) \quad \overset{\textbf{Def.}}{=} \quad (f \circ g)(m)$$

Beispiel für $\mathbf{S}_n$, $n = 4$:

$$\underset{g}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}} \quad \underset{\circ}{\circ} \quad \underset{f}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}} \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$$

a, b, c, d ergeben sich nun folgendermaßen:

$$1 \xrightarrow{f} 4 \xrightarrow{g} 3 = a, \quad 2 \xrightarrow{f} 1 \xrightarrow{g} 2 = b, \quad 3 \xrightarrow{f} 3 \xrightarrow{g} 4 = c, \quad 4 \xrightarrow{f} 2 \xrightarrow{g} 1 = d$$

2.1.5 Definition (II.1.e): Halbgruppe, Neutrales Element

(i) Eine Menge mit assoziativer Verknüpfung heißt Halbgruppe.

(ii) Gegeben $(M, \circ)$. $e \in M$ heißt neutrales Element (Einselement, Nullelement, etc), wenn gilt: $\forall a \in M : a \cdot e = e \cdot a = a$.

Anmerkung: Bei "$\circ$" handelt es sich um eine Verknüpfung und nicht um die Multiplikation im Speziellen.

Beispiele:

- **$(\mathbb{Q}, +), (\mathbb{Z}, +)$: neutrales Element 0.**
- **$(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$: neutrales Element 1.**
- **$(\mathbf{Abb}(M, M), \circ)$: neutrales Element $e : M \to M$, $e \circ f = f \circ e = f = id_M$**

$\mathbf{id}_M$ ist die Identität. Sie besitzt folgende nützliche Eigenschaft:$\mathbf{id}_M(m) = m\, \forall m \in M$

Verknüpfung: $f : M \times M \to M$.
Abstrakt: $(a, b) \mapsto ab$. **Konkret für die Multiplikation:** $(a, b) \mapsto a \cdot b$.
Eigenschaften einer Halbgruppe:

(i) **Assoziativität:** $(ab)\,c = a\,(bc)$. **Beispiel:** $\mathbf{max}\,(\mathbf{max}\,(a, b), c) = \mathbf{max}\,(a, \mathbf{max}\,(b, c))$.

(ii) **neutrales Element** e **(auch "Nullelement" oder "Einselement")** $\forall a : ea = ae = a$.

Beispiele für Halbgruppen:

(a) $(\mathbb{Z}, +)$ **ist assoziativ,** 0 **ist neutrales Element.**

(b) $(\mathbb{N}, \cdot)$ **ist assoziativ,** 1 **ist neutrales Element.**

(c) $(\mathbf{Abb}\,(X, X), \circ)$ **ist assoziativ,** $\mathbf{id}_X$ **ist neutrales Element.**

(d) $\mathbf{S}_n = (\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} | \, \sigma$ **bijektiv** $, \circ)$ **ist assoziativ, id ist das neutrale Element.**

Spezielle Notation für σ**:**

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \quad \textbf{wird als Permutation bezeichnet}$$

Beispiel: $M = \{n \in \mathbb{N} | \, n \geq 2\}$. $(M, \cdot)$ **und** $(M, +)$ **sind assoziativ, enthalten aber kein neutrales Element.**

2.1.6 Satz (II.1.1): Eindeutigkeit des neutralen Elements in einer Halbgruppe

In einer Halbgruppe gibt es höchstens ein neutrales Element.
Beweis: Seinen e, e' **neutrale Elemente in der Halbgruppe** H.
Zu zeigen: $e = e'$.
Es ist:

$$e \overset{(*)}{=} e \cdot e' \overset{(**)}{=} e'$$

Anmerkung: $(*) : e'$ **ist neutrales Element,** $(**) : e$ **ist neutrales Element.**

2.1.7 Definition (II.1.f): Monoid, Invertierbarkeit

Definitionen:

(i) **Monoid** $:=$ **Halbgruppe mit neutralem Element.**

(ii) **Invertierbarkeit: Sei** H **eine Halbgruppe mit neutralem Element** e. **Dann heißt** $a \in H$ **invertierbar, wenn es** $b \in H$ **gibt mit** $ab = ba = e$.

Beispiele:

(a) **Gegeben sei** $(\mathbb{N}, \cdot)$. a **ist invertierbar (bezüglich der Multiplikation)**
$\Leftrightarrow \quad \exists b \in \mathbb{N} : a \cdot b = b \cdot a = 1$ **(in** $\mathbb{N}$ **ist** $a = 1$ **das einzig invertierbare Element).**

(b) **Gegeben sei** $(\mathbb{R}, \cdot)$. a **ist invertierbar**
$\Leftrightarrow \quad \exists b \in \mathbb{R} : a \cdot b = b \cdot a = 1 \quad \Leftrightarrow \quad a \neq 0$.

(c) **Gegeben sei** $(Abb\,(X, X), \circ)$. $f : X \to X$ **ist invertierbar**
$\Leftrightarrow \quad \exists g : X \to X$ **mit** $f \circ g = \mathbf{id}_X$ **und** $g \circ f = \mathbf{id}_X$.

Behauptung: f **ist invertierbar** $\Leftrightarrow f$ **ist bijektiv.**
Beweis:
"$\Leftarrow$":
f **ist bijektiv** $\Rightarrow$ **Es existiert die Umkehrfunktion** $f^{-1} : X \to X,\ f(x) \mapsto x$.
Setze $g := f^{-1}$**:** $(f \circ g)(x) = \left(f \circ f^{-1}\right)(x) \overset{\textbf{Def.}}{=} f\left(f^{-1}(x)\right) \overset{!}{=} x$.
Zum Beweis: Setze $x := f(a)$ **für ein** $a \in X$ **(**f **ist surjektiv), da** $f^{-1}(f(a)) = a$.
Weiter: $f\left(f^{-1}(x)\right) = f\left(f^{-1}(f(a))\right) = f(a) = x$.
Nun betrachten wir $(g \circ f)(x)$**:**
$(g \circ f)(x) = \left(f^{-1} \circ f\right)(x) = f^{-1}(f(x)) \overset{(*)}{=} x$. **Wir verwenden bei** $(*)$ **die Eigenschaften der Definition der Umkehrfunktion.**
Insgesamt haben wir bisher gezeigt: $f \circ f^{-1} = id$ **und** $f^{-1} \circ f = id$.
"$\Rightarrow$":
Zu zeigen: $f \circ g = id \overset{(1)}{\Rightarrow} f$ **surjektive,** $g \circ f = \mathbf{id} \overset{(2)}{\Rightarrow} f$ **injektive,**
<u>Beweis für (1)</u>:
Sei $y \in X$. **Zu zeigen:** $\exists x \in X : f(x) = y$.
Es ist $y = \mathbf{id}_X(y) = f \circ g(y) = f(g(y))$.
Also mit $g(y) = x$ **ergibt sich:** $f(g(y)) = f(x) = y$.
<u>Beweis für (2)</u>:
Zu zeigen: $x \neq x' \Rightarrow f(x) \neq f(x')$.
Kontraposition: $(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg B \Rightarrow \neg A)$.
In diesem Fall zu zeigen: $f(x) = f(x') \Rightarrow x = x'$.
Sei $f(x) = f(x') \Rightarrow g(f(x)) = g(f(x'))$.
Das heißt nach Definition: $(g \circ f)(x) = (g \circ f)(x')$.
Nach Voraussetzung gilt: $(g \circ f) = id_X$. **Daher:**

$$\begin{aligned} \mathbf{id}_X(x) &= \mathbf{id}_X(x') \\ x &= x' \end{aligned}$$

2.1.8 Satz (II.1.2)

Sei H **eine Halbgruppe mit neutralem Element. Dann gilt:**

$$ab = ab' = ba = b'a = e \Rightarrow b = b'$$

Umgangssprachlich: Das Inverse ist eindeutig.
Beweis:

$$b \overset{(N_\circ)}{=} b \circ e \overset{\textbf{Vor.}}{=} b \circ (a \circ b') \overset{(A_\circ)}{=} (b \circ a) \circ b' \overset{\textbf{Vor.}}{=} e \circ b' \overset{(N_\circ)}{=} b'$$

2.1.9 Definition (II.1.g): Das inverse Element

$ab = ba = e$. **Wir bezeichnen** b **als das Inverse zu** a.
Notation: $b = a^{-1}$.
Beispiele:

(a) $(\mathbb{R} \setminus \{0\}, \cdot)$ $a^{-1} = a^{-1} \doteqdot \frac{1}{a}$.

(b) $(\mathbf{Abb}(X,X), \circ)$. f^{-1} **ist das Inverse (**f^{-1} **ist die Umkehrfunktion).**

(c) $(\mathbb{Z}, +)$. **Das Inverse zu** a **ist** $-a$, **da** $a + (-a) = 0$.

(d) $\sigma \in \mathbf{S}_n$, σ **ist bijektiv, also existiert** σ^{-1}

Beispiel für $\sigma, \sigma^{-1} \in \mathbf{S}_5$ **:**

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \\ \sigma^{-1} &= \begin{pmatrix} 3 & 4 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \end{aligned}$$

Um σ^{-1} **zu erhalten haben wir die Werte und Bilder vertauscht und abschließend die neuen Werte der Größe nach sortiert.**

2.1.10 Definition (II.1.h): Gruppe

Eine Gruppe G **ist eine Halbgruppe mit neutralem Element, in der jedes Element invertierbar ist. Mit Quantoren:**

(i) Assoziativität: $\forall a, b, c \in G : (ab)\,c = a\,(bc)$.

(ii) Neutrales Element: $\exists e \in G\, \forall a \in G : ae = ea = a$.

(iii) Inverses Element: $\forall a \in G\, \exists b \in G : ab = ba = e$

Beispiele:

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ **sind Gruppen. Hier** $e = 0$, **Inverses Element** $-a$.

(b) $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$ **sind Gruppen. Hier** $e = 1$.
Inverses Element: $a^{-1} = \dfrac{1}{a}$.

(c) $(\{-1, 1\}, \cdot)$ **ist eine Gruppe mit zwei Elementen.**

(d) $(\{0\}, +)$ **ist eine Gruppe mit einem Element.**

2.1.11 Satz (**II**.1.3)

$\mathbf{S}_n$ ist eine Gruppe mit $n!$ Elementen.

Beweis: $\mathbf{S}_n$ ist Halbgruppe mit neutralem Element. Bereits bewiesen: jedes Element in $\mathbf{S}_n$ ist invertierbar weil die Elemente von S_n bijektiv sind.
Behauptung: $|\mathbf{S}_n| = n!$ ($|\mathbf{S}_n| :=$ Anzahl der Elemente in $\mathbf{S}_n$.)
Möglichkeiten für die Bilder einer Permutation: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$
Für den ersten Wert gibt es n Möglichkeiten für die Position von i_1.
Bei gewähltem i_1 gibt es $(n-1)$ Möglichkeiten für die Position von i_2. (σ injektiv $\Rightarrow i_2 = \sigma(2) \neq \sigma(1) = i_1$).
Bei gewählten i_1, i_2 gibt es $(n-2)$ Möglichkeiten für die Position von i_3.
Weiter so bis wir alle i_j durchlaufen haben.
Insgesamt: $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ verschiedene Möglichkeiten der Anordnung.

2.1.12 Notation: r-Zyklen

Es gilt: $\mathbf{S}_n = \left\{ \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \right\}, \quad |S_n| = n!$
Spezielle Permutationen: r-Zyklen (haben r Ziffern):

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_r \end{pmatrix}$$

Dies bedeutet:

(I) $i_1 \mapsto i_2 \mapsto \ldots \mapsto i_{r-1} \mapsto i_r \mapsto i_1$

(II) $k \neq i_1, \ldots, i_r \Rightarrow \sigma(k) = k$.

Man kann sich dies auch anhand eines Kreises vorstellen:

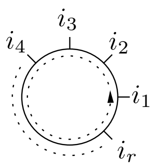

Abbildung II-1: ein r-Zyklus an einem Kreis

Hier nun ein Beispiel:

$$\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 1 & 6 \end{pmatrix} \\
\sigma^2 &= \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} \\
\sigma^3 &= \sigma \circ \sigma \circ \sigma = \sigma \circ \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 3 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 3 \end{pmatrix} \\
\sigma^4 &= \sigma \circ \sigma \circ \sigma \circ \sigma = \sigma \circ \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \mathbf{id}
\end{aligned}$$

Generell gilt: $\begin{pmatrix} i_1 & \dots & i_r \end{pmatrix}^r = \mathbf{id}$. **Nun gilt:**

$$\sigma^{7541} = \sigma^{4 \cdot 1885 + 1} = \left(\sigma^4\right)^{1885} \circ \sigma^1 = id^{1885} \circ \sigma = \sigma$$

2.1.13 Satz (II.1.4): Rechengesetze in Gruppen

In jeder Gruppe sind bei gegebenen $a, b \in$ G die folgenden Gleichungen eindeutig lösbar:

$$\mathbf{I}: a \cdot x = b \quad \mathbf{II}: y \cdot a = b \quad \textbf{und zwar} \quad \mathbf{I}: x = a^{-1} \cdot b \quad \mathbf{II}: y = b \cdot a^{-1}$$

Beweis für Gleichung I:
Wir müssen sowohl die Existenz als auch die Eindeutigkeit der Lösung zeigen.
Existenz: Wir setzen unsere Vermutung in die linke Seite ein und erhalten:

$$a \cdot x = a \cdot \left(a^{-1} \cdot b\right) \overset{\textbf{Ass.}}{=} \left(a \cdot a^{-1}\right) \cdot b \overset{\textbf{Inv.}}{=} e \cdot b = b$$

Wir erhalten die rechte Seite.
Eindeutigkeit der Lösung: Sei $x \in G$, das heißt $a \cdot x = b$. Nun multiplizieren wir mit a^{-1} auf beiden Seiten von links und erhalten: $a^{-1}(a \cdot x) = a^{-1} \cdot b$
Das heißt (Assoziativgesetz): $\left(a^{-1} \cdot a\right) \cdot x = a^{-1} \cdot b$
Das heißt (Neutrales Element): $e \cdot x = a^{-1} \cdot b \quad \Leftrightarrow \quad x = a^{-1} \cdot b$
Der Beweis für II erfolgt analog, wobei mir a^{-1} von rechts multipliziert wird.

2.1.14 Definition (II.1.i): Kommutative Verknüpfung

Eine Verknüpfung heißt kommutativ (abelsch) wenn gilt:

$$\forall a, b: \ ab = ba$$

Beispiele:

(a) $(\mathbb{Z}, +), (\mathbb{Z}, \cdot), \ldots, (\mathbb{R}, +), (\mathbb{R}, \cdot)$ **sind kommutativ.**

(b) $u, v \in \mathbb{R}: u, v \mapsto u \times v$ **ist nicht kommutativ.**

(c) $\mathbf{S}_1$, $\mathbf{S}_2$ **sind kommutativ .**

(d) $\mathbf{S}_n$, $n \geq 3$ **sind nicht kommutativ.**

Behauptung: $u \times v = -v \times u$
Beweis: $u = (a_1, a_2, a_3)\,,\ v = (b_1, b_2, b_3)$.

$$\begin{aligned} u \times v &= \left(\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right) \\ &= \left(- \begin{vmatrix} b_2 & b_3 \\ a_2 & a_3 \end{vmatrix}, - \begin{vmatrix} b_3 & b_1 \\ a_3 & a_1 \end{vmatrix}, - \begin{vmatrix} b_1 & b_2 \\ a_1 & a_2 \end{vmatrix} \right) \\ &= - \left(\begin{vmatrix} b_2 & b_3 \\ a_2 & a_3 \end{vmatrix}, \begin{vmatrix} b_3 & b_1 \\ a_3 & a_1 \end{vmatrix}, \begin{vmatrix} b_1 & b_2 \\ a_1 & a_2 \end{vmatrix} \right) \\ &= -v \times u \end{aligned}$$

Behauptung: $\mathbf{S}_n$ **fuer** $n \geq 3$ **ist nicht kommutativ.**
Das es sich um eine Aussage für alle handelt reicht ein Gegenbeispiel um zu zeigen, daß $S_n, n \geq 3$ nicht kommutativ ist.
Sei $\sigma, \tau \in \mathbf{S}_3$**:** $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
Nun gilt: $\sigma \circ \tau = \begin{pmatrix} 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \end{pmatrix} = \tau \circ \sigma$

2.1.15 Mehrfache Produkte von Gruppen (Halbgruppen)

Eine Verknüpfung ist binär. Das heißt: es können nur zwei Elemente auf einmal verknüpft werden.
Gegeben seien drei Elemente: $a, b, c \in G$. **Nun gibt es mehrere Möglichkeiten diese Elemente zu verknüpfen:** $(ab)\,c$, $a\,(bc)$, $(ba)\,c$, ...

Gegeben seien $a_1, \ldots, a_n \in G$. **Nun gilt:** $\prod_{i=1}^{n} a_i := (\ldots((a_1 \cdot a_2) \cdot a_3) \ldots \cdot a_{n-1}) \cdot a_n$

Als rekursiven Definition: $\prod_{i=1}^{1} a_i := a_1$ **und** $\prod_{i=1}^{n+1} a_i := \left(\prod_{i=1}^{n} a_i\right) \cdot a_{n+1}$

Wir wollen nun den Fall für $n = 4$ **betrachten:** $\prod_{i=1}^{4} a_i = ((a_1 \cdot a_2) \cdot a_3) \cdot a_4$

Es ist aber auch eine andere Klammerung möglich: $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4)$.

Behauptung: In einer Halbgruppe gilt: $\prod_{i=1}^{4} a_i = (a_1 \cdot a_2) \cdot (a_3 \cdot a_4)$

Beweis: $((\underbrace{a_1 \cdot a_2}_{x}) \cdot \underbrace{a_3}_{y}) \cdot \underbrace{a_4}_{z} \overset{A}{=} (\underbrace{a_1 \cdot a_2}_{x}) \cdot (\underbrace{a_3}_{y} \cdot \underbrace{a_4}_{z})$

Zudem gelten nach dem Assoziativgesetz auch:

$$((a_1 \cdot a_2) \cdot a_3) \cdot a_4 \overset{A}{=} (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) \overset{A}{=} a_1 \cdot (a_2 \cdot (a_3 \cdot a_4)) \overset{A}{=} a_1 \cdot ((a_2 \cdot a_3) \cdot a_4) \overset{A}{=} (a_1 \cdot (a_2 \cdot a_3)) \cdot a_4$$

2.1.16 Satz (II.1.5): Allgemeines Assoziativgesetz

Gegeben: H **sei Halbgruppe, mit** $a_1, \ldots, a_n, a_{n+1}, a_m \in H$. **Dann gilt:**

$$\prod_{i=1}^{n} a_i \cdot \prod_{j=1}^{m} a_{n+j} = \prod_{i=1}^{n+m} a_i$$

Beweis nun per vollständiger Induktion nach $n + m$.
Induktionsverankerung: $n + m = 2$. **Das heißt** $n = m = 1$, **da** $n, m \in \mathbb{N}$.

Betrachtung der linken Seite: $\prod_{i=1}^{1} a_i \cdot \prod_{j=1}^{1} a_{n+j} = a_1 \cdot a_2$

Betrachtung der rechten Seite: $\prod_{i=1}^{2} a_i = a_1 \cdot a_2$

Induktionsschluß: Es gibt zwei Möglichkeiten: $n + m \rightsquigarrow n + m + 1 = \begin{cases} (n+1) + m \\ n + (m+1) \end{cases}$

Hier wollen wir nur den unteren Fall betrachten:
$n + m \rightsquigarrow n + (m+1)$: **Wir starten auf der linken Seite:**

$$\begin{aligned} \prod_{i=1}^{n} a_i \cdot \prod_{j=1}^{m+1} a_{n+j} &= \left(\prod_{i=1}^{n} a_i\right) \cdot \left(\prod_{j=1}^{m+1} a_{n+j}\right) \overset{\textbf{Def.}}{=} \left(\prod_{i=1}^{n} a_i\right) \cdot \left(\left(\prod_{j=1}^{m} a_{n+j}\right) \cdot a_{n+m+1}\right) \\ &\overset{\textbf{Ass.}}{=} \left(\prod_{i=1}^{n} a_i \cdot \prod_{j=1}^{m} a_{n+j}\right) \cdot a_{n+m+1} \overset{\textbf{IA}}{=} \left(\prod_{i=1}^{n+m} a_i\right) \cdot a_{n+m+1} \overset{\textbf{Def.}}{=} \prod_{i=1}^{n+m+1} a_i \end{aligned}$$

2.1.17 Satz (II.1.6): Allgemeines Kommutativgesetz

Gegeben: H sei kommutative Halbgruppe, mit $a_1, \ldots, a_n \in H$, $\sigma \in S_n$. Dann gilt:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n \quad = \quad a_{\sigma(1)} \cdot a_{\sigma(2)} \cdot \ldots \cdot a_{\sigma(n)}$$

Hier kein Beweis. Es wird auf die Literatur verwiesen (Im Prinzip wie Beweis des allgemeinen Assoziativgesetz).

2.1.18 Anwendung: Potenzgesetze in Gruppen

Sei G eine Gruppe, $a \in G, n \in \mathbb{N}$ $a^n := \prod_{i=1}^{n} a_i$ **für** $a_i = a$ $\qquad a^0 := e$

Für $n \in \mathbb{Z}$ gilt: $n \geq 0$: siehe oben, $n < 0$: $a^n = \left(a^{|n|}\right)^{-1}$

2.1.19 Satz (II.1.7): Potenzgesetze

Sei G Gruppe, $a, b \in G, n, m \in \mathbb{Z}$. Dann gilt:

(i) Multiplikation:

$$\begin{aligned}
a^n a^m &= \prod_{i=1}^{n} a \cdot \prod_{i=1}^{m} a \overset{(\mathbf{II}.1.5)}{=} \prod_{i=1}^{n+m} a = a^{n+m} \\
(a^n)^m &= \prod_{j=1}^{m} a^n = a^n \cdot \ldots \cdot a^n = a^{\sum_{j=1}^{m} n} = a^{n \cdot m}
\end{aligned}$$

Beispiel:

$$\begin{aligned}
a^{10} \cdot a^{-14} &= a^{10} \cdot \left(a^{14}\right)^{-1} = \underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{14}}_{=a^{10}} \cdot \left(a^{14}\right)^{-1} \\
&= a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot \underbrace{a^{14} \cdot \left(a^{14}\right)^{-1}}_{=e} = a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot e \\
&= \left(a^1 \cdot a^1 \cdot a^1 \cdot a^1\right)^{-1} = \left(a^4\right)^{-1} = a^{-4} a^{-4}
\end{aligned}$$

(ii) Das Inverse Element einer Produktes: $(ab)^{-1} = b^{-1} a^{-1}$
Zu zeigen: $(ab)\left(a^{-1} b^{-1}\right) = \left(b^{-1} a^{-1}\right)(ab) = e$.
Nun gilt für die linke Seite: $(ab)\left(a^{-1} b^{-1}\right) = \left(abb^{-1}\right) a^{-1} = (ae)\, a^{-1} = aa^{-1} = e$
Auf der rechten Seite gilt: $\left(b^{-1} a^{-1}\right)(ab) = b^{-1}\left(a^{-1} ab\right) = b^{-1}(eb) = b^{-1} b = e$
Damit ist $\left(b^{-1} a^{-1}\right)$ **das inverse Element zu** (ab).

(iii) G abelsch: $(ab)^n = \prod_{i=1}^{n} (ab) \overset{\textbf{Kom.}}{=} \prod_{i=1}^{n} a \cdot \prod_{i=1}^{n} b = a^n b^n$

2.1.20 Definition (II.1.j): Äquivalenzrelation auf einer Menge M:

(i) $\forall x \in M : x \sim x$ **(Eigenschaft der Reflexivität)**

(ii) $\forall x, y \in M; x \sim y \Rightarrow y \sim x$ **(Eigenschaft der Symmetrie)**

(iii) $\forall x, y, z : x \sim y, y \sim z \Rightarrow x \sim z$ **(Eigenschaft der Transitivität)**

Die Äquivalenzrelation ist eine Abschwächung der Identitätsrelation.
Definition: Äquivalenzklasse: $[x] := \{ y \in M | \, y \sim x\}$
Es gilt: $M = \dot{\bigcup}$ **verschiedene Äquivalenzklassen**

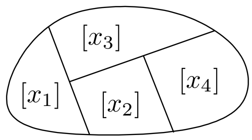

Abbildung II-2: Skizze für M

<u>Definition</u>: Menge der Äquivalenzklassen wird als $M/_\sim$ **bezeichnet. Die Elemente der Menge sind wiederum Mengen.**

2.1.21 Definition (II.1.k): Kongruenzrelation $\bmod n$ **auf** $\mathbb{Z}$**.**

Lies "modulo n **auf** $\mathbb{Z}$**". Für** $a, b \in \mathbb{Z}$ **und ein festes** $n \in \mathbb{N}$ **gilt:**$a \equiv b \bmod n \Leftrightarrow n|a - b$**Bemerkungen:**

- $n \in \mathbb{N}$, **Division mit Rest:** $a = q \cdot n + r$ **mit** $0 \leq r \leq n - 1$.
- $a \equiv b \bmod n \Leftrightarrow a, b$ **lassen bei Division mit Rest durch** n **denselben Rest.**

Definition für Teiler: $x|y \Leftrightarrow \exists z : x \cdot z = y$.

2.1.22 Satz (II.1.8): $\equiv \bmod n$ **ist eine Äquivalentrelation**

Beweis:
Reflexivität: $a \equiv a|n$, **denn** $n|a - a = 0$.
Symmetrie: Sei $a \equiv b \bmod n$, **Zu zeigen:** $b \equiv a \bmod n$. **Das heißt** $n|b - a$.
Nach Voraussetzung gilt: $n|a - b \Leftrightarrow a - b = k \cdot n \quad \Leftrightarrow \quad b - a = (-k) \cdot n \quad \Leftrightarrow \quad b - a = l \cdot n$
Transitivität: Sei $a \equiv b \bmod n$ **und** $b \equiv c \bmod n$.
Zu zeigen: $a \equiv b \bmod n$, $b \equiv c \bmod n \quad \Rightarrow \quad a \equiv c \bmod n$.
Es gilt: $a - c = (a - b) + (b - c) = k \cdot n + l \cdot n = (k + l) \cdot n$

2.1.23 Definition (II.1.l): $\overline{a}$

$\overline{a}$ =**Kongruenzklasse von** $a = \{ b \in \mathbb{Z} | \, a \equiv b \bmod n\} = \{ b \in \mathbb{Z} | \, (n|a - b)\}$.
Die Kongruenzklasse ist eigentlich eine Äquivalenzklasse.

2.1.24 Definition (II.1.m): Restklassenringe $\mathbb{Z}/_{n\mathbb{Z}}$

$\mathbb{Z}/_{n\mathbb{Z}}$:=**Menge der Kongruenzklassen** $\bmod n = \{ \overline{a} | \, a \in \mathbb{Z}\}$.

2.1.25 Satz (II.1.9):

Es gilt:

(i) $\overline{a} = a + n \cdot \mathbb{Z} = \{a, a+n, a-n, a+2n, a-2n, \ldots\}$

(ii) Es gibt genau $|n|$ verschiedene Kongruenzklassen für $n \neq 0$.

<u>Beweise</u>:

zu (i)**:** $b \in \overline{a} \overset{\textbf{Def.}}{\Leftrightarrow} a \equiv b \bmod n \Leftrightarrow \exists k \in \mathbb{Z} : a - b = k \cdot n$
$\Leftrightarrow \exists k \in \mathbb{Z} : b = a + (-k) \cdot n \Leftrightarrow l \in \mathbb{Z} : b = a + l \cdot n$

zu (ii)**:** $n = 0 : a \equiv b \bmod 0 \overset{\textbf{Def.}}{\Leftrightarrow} 0|a - b \Leftrightarrow \exists k \in \mathbb{Z} : 0 \cdot k = a - b \Leftrightarrow a = b$.
Also: $\equiv \text{mod} 0$ **ist die Identität. Das heißt** $\overline{a} = a$.
$n \neq 0$**: Division mit Rest bezüglich** $n : b = q \cdot n + r$ **für** $0 \leq r \leq |n| - 1$

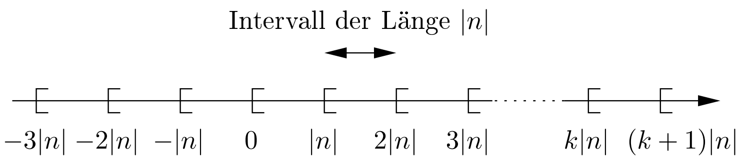

Abbildung II-3: Skizze für $n < 0$

Das heißt: $b \equiv r \bmod n$ **mit** $0 \leq r \leq |n| - 1 \Rightarrow \overline{b} = \overline{r}$ **für ein** $r \in \mathbb{N}_0$ **mit** $0 \leq r \leq |n| - 1$.
Es gibt also $|n|$ **viele Klassen.**
Noch zu zeigen: Die Klassen $\overline{r}$ **für** $0 \leq r \leq |n| - 1$ **sind paarweise verschieden.**
Sei $\overline{r} = \overline{s}$ **mit** $0 \leq s \leq |n| - 1$**. Das heißt** $r \equiv s \bmod n \Leftrightarrow n|s - r \Leftrightarrow s - r = k \cdot n \Rightarrow |s - r| = 0$ **oder** $|s - r| \geq |n|$**. Weil** $r, s \in [0, |n| - 1[$ **sind kann nur gelten:** $|s - r| = 0 \Rightarrow s = r$ $\square$.
Beispiele:

(a) $n = 2$: $\mathbb{Z}/_{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$. **Es gilt:**

$$\begin{aligned} \overline{0} &= \{x \in \mathbb{Z} \,|\, (2|x - 0)\} = \{\textbf{alle geraden Zahlen}\} \\ \overline{1} &= \{x \in \mathbb{Z} \,|\, (2|x - 1)\} = \{\textbf{alle ungeraden Zahlen}\} \end{aligned}$$

(b) $n = 3$: $\mathbb{Z}/_{3\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}\}$. **Es gilt:<u>t</u>**

$$\begin{aligned} \overline{0} &= \{x \in \mathbb{Z} \,|\, (3\,|x - 0)\} \\ &= \{\textbf{alle durch drei teilbaren Zahlen}\} \\ \overline{1} &= \{x \in \mathbb{Z} \,|\, (3\,|x - 1)\} \\ &= \{\textbf{Zahlen, die bei Division durch 3 Rest 1 zurücklassen}\} \\ \overline{2} &= \{x \in \mathbb{Z} \,|\, (3\,|x - 2)\} \\ &= \{\textbf{Zahlen, die bei Division durch 3 Rest 2 zurücklassen}\} \end{aligned}$$

(c) $n \in \mathbb{N}$**:** $\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

2.1.26 Rechengesetze auf $\mathbb{Z}/_{n\mathbb{Z}}$:

- $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$
- **Für** $n \neq 0$**:** $\mathbb{Z}/_{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\} = \{\overline{x} | \, x \in \mathbb{Z}\}$**.**

Gleichheit: $\overline{x} = \overline{y} \Leftrightarrow n|x - y \Leftrightarrow x \equiv y \bmod n$
Addition: $\overline{x} + \overline{y} = \overline{x + y}$
Multiplikation: $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$
Wohldefiniertheit: Ziel: "Klassen" zu addieren und multiplizieren.
Gegeben seinen K_1, K_2**. Nun:**

(a) **Wähle** x_1, x_2 **mit** $K_1 = \overline{x_1}$ **und** $K_2 = \overline{x_2}$

(b) **Addiere** $x_1 + x_2$

(c) **Definiere** $K_1 + K_2 := \overline{x_1 + x_2}$

Nun stellt sich das Problem der Wohldefiniertheit: Zeige, daß der Wert $K_1 + K_2$ **unabhängig von der Auswahl der** x_i **mit** $i = 1, 2$ **ist.**
Vor dem allgemeinen Beweis zuerst ein Beispiel:
Sei $n = 15$**. Nun gilt:** $\overline{1} = \overline{46}$ **und** $\overline{-6} = \overline{84}$ **(In beiden Fällen handelt es sich um Repräsentanten derselben Kongruenzklasse). Führen wie eine Addition durch, so ergibt sich:**

$$\overline{1 + (-6)} = \overline{-5} = \overline{10} = \overline{130} = \overline{46 + 84}$$

Die Auswahl spielt also in diesem Beispiel keine Rolle.
Allgemeiner Beweis: Sei $\overline{x_1} = \overline{x_1'}$ **und** $\overline{x_2} = \overline{x_2'}$**.**
Zu zeigen: $\overline{x_1 + x_2} = \overline{x_1' + x_2'}$**. Das heißt:** $n| \underbrace{(x_1 + x_2) - (x_1' + x_2')}_{\doteqdot \Delta}$

Bemerkung: In diesem Fall ist alles womit wir arbeiten können $n|x_1 - x_1'$ **und** $n|x_2 - x_2'$**.**
Nun gilt für Δ**:**

$$\Delta = (x_1 + x_2) - (x_1' + x_2') \quad \overset{\textbf{Vor.}}{=} \quad n \cdot l_1 + n \cdot l_2 = n \cdot (l_1 + l_2)$$

Also ist n **ein Teiler von** Δ**.**
Weiter ist zu zeigen: $\overline{x_1 \cdot x_2} = \overline{x_1' \cdot x_2'}$**. Das heißt** $n| \underbrace{x_1 \cdot x_2 - x_1' \cdot x_2'}_{\doteqdot \delta}$

Nun gilt für δ**:**

$$\begin{aligned} \delta &= x_1 \cdot x_2 - x_1' \cdot x_2' = x_1 \cdot x_2 \underbrace{-x_1' \cdot x_2 + x_1' \cdot x_2}_{=0} - x_1' \cdot x_2' \\ &= (x_1 - x_1') \cdot x_2 + x_1' \cdot (x_2 - x_2') = n \cdot l_1 \cdot x_2 + x_1' \cdot n \cdot l_2 = n \cdot (l_1 \cdot x_2 + l_2 \cdot x_1') \end{aligned}$$

Also ist n **ein Teiler von** δ**.**
Beispiele: Sei $n = 10$**:**

- $\overline{6} + \overline{9} = \overline{15} = \overline{5}$
- $\overline{6} \cdot \overline{9} = \overline{54} = \overline{4}$
- $\overline{4} \cdot \overline{5} = \overline{20} = \overline{0}$
- $\overline{7}^3 = \overline{343} = \overline{3}$
- $\overline{9}^{343461} = \left(\overline{9}^2\right)^{171730} \cdot \overline{9} = \left(\overline{1}\right)^{171730} \cdot \overline{9} = \overline{9}$

2.1.27 Satz (II.1.10)

Es gilt:

(i) $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ **ist abelsche Gruppe mit neutralem Element** $\overline{0}$. **Das additive Inverse zu** $\overline{a}$ **ist** $\overline{-a}$.

(ii) $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot)$ **ist eine kommutative Halbgruppe mit neutralem Element** $\overline{1}$.

Beweis:
zu (i): **Assoziativität. Zu zeigen:** $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$.

Linke Seite: $(\overline{a}+\overline{b})+\overline{c} \overset{\textbf{Def.}}{=} \overline{a+b}+\overline{c} \overset{\textbf{Def.}}{=} \overline{(a+b)+c}$.

Rechte Seite: $\overline{a}+(\overline{b}+\overline{c}) \overset{\textbf{Def.}}{=} \overline{a}+\overline{b+c} \overset{\textbf{Def.}}{=} \overline{a+(b+c)}$.

Da die Addition in $\mathbb{Z}$ **assoziativ ist folgt, daß die linke und die rechten Seite äquivalent sind.**
Betrachtung des neutralen Elements: $\overline{a}+\overline{0} = \overline{a+0} = \overline{a} = \overline{0+a} = \overline{0}+\overline{a}$

Betrachtung der Kommutativität: $\overline{a}+\overline{b} = \overline{a+b} \overset{\mathbb{Z}}{=} \overline{b+a} = \overline{b}+\overline{a}$

Betrachtung des inversen Elements: $\overline{a}+\overline{-a} \overset{\textbf{Def.}}{=} \overline{a+(-a)} \overset{\mathbb{Z}}{=} \overline{0}$

zu (ii): **Beweis erfolgt analog.**

2.1.28 Eigenschaften von $\mathbb{Z}/_{n\mathbb{Z}}$:

- $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ **ist abelsche Gruppe**
  - **Neutrales Element:** $\overline{0} = \overline{n} = \overline{-2n} = \ldots$
  - **Inverses Element:** $-(\overline{a}) = \overline{-a} = \overline{n-a} = \ldots$
- $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot)$ **ist kommutative Halbgruppe**
  - **Neutrales Element:** $\overline{1} = \overline{n+1} = \overline{-6n+1} = \ldots$
  - **Keine Gruppe, da** $\overline{0}\cdot\overline{x} = \overline{0\cdot x} = \overline{0} \neq \overline{1}$ **(Es existiert kein inverses Element für** $|n| > 1$**)**

Eine Anmerkung zur Notation: $\overline{a}-\overline{b} = \overline{a}+(\overline{-b}) = \overline{a-b}$.

2.1.29 Rechenbeispiele für Kongruenzklassen

Sei $n = 10$. **Berechnen Sie** $\overline{16}^3 - \overline{2}^6 + \overline{22}$. **Nun gilt:**
$\overline{16}^3 = \overline{16}^2\cdot\overline{16} = \overline{6}^2\cdot\overline{16} = \overline{(-4)}^2\cdot\overline{16} = \overline{16}\cdot\overline{16} = \overline{(-4)}^2 = \overline{16} = \overline{6}$
$\overline{2}^6 = \overline{2}^3\cdot\overline{2}^3 = \overline{8}\cdot\overline{8} = \overline{-2}\cdot\overline{-2} = \overline{4}$
$\overline{22} = \overline{2}$
Setzen wir nun ein, so erhalten wir: $\overline{16}^3 - \overline{2}^6 + \overline{22} = \overline{6}-\overline{4}+\overline{2} = \overline{8}-\overline{4} = \overline{4}$.
Sei $n = 10$. **Was ist** $\overline{9}^k$**?**
Der schlechte, da aufwendige Weg: $\overline{9}^k = \overline{9^k}$.
Der gute Weg: $\overline{9}^k = \overline{-1}^k$. **Nun gilt:**

$$\overline{-1}^k = \begin{cases} \overline{1} & k \textbf{ gerade} \\ \overline{-1} & k \textbf{ ungerade} \end{cases}$$

2.1.30 Invertierbarkeit von $\mathbb{Z}/_{8\mathbb{Z}}$

$\overline{a}$ ist invertierbar in $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot)$ $\Leftrightarrow$ $\exists \overline{b} \in \mathbb{Z}/_{n\mathbb{Z}} : \overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$
Sind die Klassen in $\mathbb{Z}/_{8\mathbb{Z}}$ invertierbar?

Element:	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
Dazugehöriges inverses Element	–	$\overline{1}$	–	$\overline{3}$	–	$\overline{5}$	–	$\overline{7}$

Die ungeraden Elemente sind leicht zu berechnen.
Warum gibt es keine inverses Element für $\overline{2}$?
Es gilt: $\overline{2} \cdot \overline{x} = \overline{2x} = \overline{y}$. $\overline{y}$ müßte nun $\overline{1}$ sein. Aber $\overline{y}$ ist gerade, weil $8|y - 2x$. Daher existiert für $\overline{2}$ kein inverses Element. Das Argument läßt sich analog auf alle anderen geraden Kongruenzklassen in $\mathbb{Z}/_{8\mathbb{Z}}$ anwenden.

2.1.31 Der ggT (a, b)

ggT (a, b) = größte natürliche Zahl, die a und b teilt.
Welche Inputs sind möglich: $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$.
Definition Teiler: $x|y \Leftrightarrow \exists k = k \cdot x = y$.
Anmerkung zur Null:

- **$x|0$, denn $0 \cdot x = 0$, wobei die erste Null k ist und die zweite Null y.**
- **$0|x \Rightarrow x = 0$.**

Wichtige Eigenschaften des ggT (a, b):

(i) **ggT** $(a, b) =$ **ggT** $(a, b - a \cdot q)$ **mit** $a \neq 0, q \in \mathbb{Z}$.

(ii) **ggT** $(a, 0) = |a|$

(iii) **ggT** $(a, b) =$ **ggT** (b, a)

Beweise:
Zu (iii): Klar, da a und b symmetrisch in die Definition eingehen.
Zu (ii): Klar, da alle Zahlen Null teilen. Der größte Teiler von a und Null ist $|a|$
Zu (i): Sei $d =$ ggT (a, b), $e =$ ggT $(a, b - q \cdot a)$. $d|a, b$.
Das heißt $a = x \cdot d$ und $b = y \cdot d \Rightarrow d|a, (b - a \cdot q = y \cdot d - (x \cdot d) \cdot q = (y - x \cdot q) \cdot d)$.
Das heißt: $d|a, a - b \cdot q \overset{\textbf{Def.}}{\Rightarrow} d \leq e$.
Nun bleibt zu zeigen: $e \leq d$ (dann folgt $e = d$).
Es ist $b = (b - a \cdot q) + a \cdot q = (b - a \cdot q) - a \cdot (-q)$. Also $b = b' - a \cdot (-q)$.
Hier noch einmal eine Verdeutlichung:

$$\begin{array}{ccccc} a, b & \rightarrow & a, b' & \rightarrow & a, b \\ d & \leq & e & \leq & d \end{array}$$

Division mit Rest: $a \neq 0, b = a \cdot q + r$ mit $0 \leq r \leq |a| - 1$. $r = b - a \cdot q$.
Nach Eigenschaft (i) folgt: ggT $(a, b) =$ ggT (a, r).

2.1.32 Euklidscher Algorithmus

Berechnen Sie den ggT $(196, 217)$**. Nun gilt:**

$$\begin{array}{rrcll}
 & \mathbf{ggT}\,(196, 217) & = & \mathbf{ggT}\,(196, ?) & ? \;:\; 217 = 196 \cdot 1 + 21 \\
\Rightarrow & \mathbf{ggT}\,(196, 217) & = & \mathbf{ggT}\,(196, 21) = \mathbf{ggT}\,(21, ?) & ? \;:\; 196 = 21 \cdot 9 + 7 \\
\Rightarrow & \mathbf{ggT}\,(196, 21) & = & \mathbf{ggT}\,(21, 7) = \mathbf{ggT}\,(7, ?) & ? \;:\; 21 = 7 \cdot 3 + 0 \\
\Rightarrow & \mathbf{ggT}\,(7, 21) & = & \mathbf{ggT}\,(7, 0) = |7| = 7 &
\end{array}$$

ggT (a, b) **liefert den größten gemeinesamen Teiler von** a **und** b**.**
Seien $a, b \in \mathbb{N}$**:**

$$\begin{array}{rll}
a_0 = b \cdot q_1 + a_2 & 0 \leq a_2 \leq b - 1 & \\
b = a_2 \cdot q_2 + a_3 & 0 \leq a_3 \leq a_2 - 1 & \\
a_2 = a_3 \cdot q_3 + a_4 & 0 \leq a_4 \leq a_3 - 1 & \\
a_3 = a_4 \cdot q_4 + a_5 & 0 \leq a_5 \leq a_4 - 1 & \\
\vdots & \vdots & \\
a_{i-1} = a_i \cdot q_i + a_{i+1} & 0 \leq a_{i+1} \leq a_i - 1 & a_{i+1} \neq 0 \\
a_i = a_{i+1} \cdot q_{i+1} + 0 & &
\end{array}$$

Dann ist a_{i+1} **der ggT** (a, b)**.**
Der Euklidische Algorithmus liefert $x, y \in \mathbb{Z}$ **mit ggT** $(a, b) = x \cdot a + y \cdot b$**.**

2.1.33 Beispiel: Berechnung von ggT $(471, 113)$

Es gilt:

$$\begin{array}{rcl}
471 & = & 113 \cdot 4 + 19 \\
113 & = & 19 \cdot 5 + 18 \\
19 & = & 18 \cdot 1 + 1 \\
18 & = & 1 \cdot 18 + 0 \\
 & & \\
\Rightarrow \mathbf{ggT}\,(471, 113) & = & 19 - 18 \cdot 1 \\
 & = & 19 - (113 - 19 \cdot 5) \cdot 1 \\
 & = & 19 \cdot 6 - 113 \cdot 1 \\
 & = & (471 - 113 \cdot 4) \cdot 6 - 113 \cdot 1 \\
 & = & 471 \cdot 6 - 113 \cdot 25
\end{array}$$

Damit ergibt sich: ggT $(471, 113) = 1 = 471 \cdot 6 - 113 \cdot 25$

2.1.34 Satz (II.1.11): Invertierbarkeit in $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot)$

Sei $\overline{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ **gegeben. Dann besitzt** $\overline{a}$ **ein (multiplikatives) Inverses genau dann, wenn ggT** $(a, n) = 1$**. Aus der Darstellung** $1 = x \cdot a + y \cdot n$ **ergibt sich:**

$$(\overline{a})^{-1} \quad = \quad \overline{x}$$

Nicht vollständiger Beweis:

$$1 = x \cdot a + y \cdot n \quad \Rightarrow \quad \overline{1} = \overline{x \cdot a + y \cdot n} = \overline{x \cdot a} + \underbrace{\overline{y \cdot n}}_{= 0} = \overline{x} \cdot \overline{a}$$

Also: $\overline{1} = \overline{x} \cdot \overline{a}$**.**

2.1.35 Erweiterter Euklidscher Algorithmus

ggT (a, b)**,** $a_1 = a, a_2 = b$**. Für** $i \geq 2 : a_{i-1} = a_i \cdot q_i + a_{i+1}$ **mit** $0 \leq a_{i+1} \leq |a_i| - 1$**.**
STOP: $a_{i+1} = 0$**. OUTPUT: ggT** $(a, b) = a_i$**.**
In der i**-ten Schleife: ggT** $(a_{i-1}, a_i) =$ **ggT** (a_{i+1}, a_i)**. Eventuell: ggT** $(a, 0) = |a|$**.**
Hier nun der erweiterte euklidische Algorithmus:

$$\begin{array}{rcl} a_1 & = & a_2 \cdot q_2 + a_3 \\ a_2 & = & a_3 \cdot q_3 + a_4 \\ \vdots & \vdots & \vdots \\ a_{i-3} & = & a_{i-2} \cdot q_{i-2} + a_{i-1} \\ a_{i-2} & = & a_{i-1} \cdot q_{i-1} + a_i \\ a_{i-1} & = & a_i \cdot q_i + 0 \end{array}$$

Aus der vorletzten Zeile folgt:

$$d = a_i = a_{i-2} + a_{i-1} \cdot (-q_{i-1})$$

Aus der drittletzten Zeile folgt:

$$\begin{array}{rcl} d & = & a_{i-2} + (a_{i-3} + a_{i-2} \cdot (-q_{i-2})) \cdot (-q_{i-1}) \\ & = & a_{i-3} + a_{i-2} \cdot (1 + q_{i-2} \cdot q_{i-1}) \end{array}$$

Eventuell erhalten wir:

$$\begin{array}{rcl} d & = & a_1 \cdot x + a_2 \cdot y \\ & = & a \cdot x + b \cdot y \end{array}$$

Noch eine Anmerkung zur Effizienz des erweiterten Euklidischen Algorithmus
$a, b < N \Rightarrow$ **dann läßt sich der ggT** (a, b) **in höchstens** $2 \cdot \ln N$ **Runden berechnen. Eine Runde ist dabei eine Division mit Rest.**
Annahme $N = 10^{100}$**. Nun müssen wir nur noch** $2 \cdot \ln 10^{100}$ **berechnen um die maximale Anzahl der Runden zu erhalten:**

$$2 \cdot \ln 10^{100} = 100 \cdot 2 \cdot \ln 2 \approx 200 \cdot 2.3 = 460$$

Man braucht also maximal 460 Divisionen mit Rest um den ggT zweier 100-stelliger Zahlen zu berechnen.
Behauptung: $\overline{a} \cdot \overline{b} = \overline{1} \Leftrightarrow$ **ggT** $(a, n) = 1$
"$\Leftarrow$**":** $1 = ax + ny \Rightarrow \overline{a} \cdot \overline{b} = \overline{1}$**.**
"$\Rightarrow$**":** $\overline{a} \cdot \overline{b} = \overline{1} \Rightarrow a \cdot b = 1 + l \cdot n$ **für ein** l**.** $d|a, n \Rightarrow d|1 \Rightarrow d = 1$**.**

2.1.36 $(\mathbb{Z}/_{n\mathbb{Z}})^*$ ist Gruppe bezüglich der Multiplikation

Es gilt: $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot) \supseteq \{\overline{a} | \, \overline{a} \,\text{ist invertierbar}\} \overset{(\mathbf{II}.1.11)}{=} \{\overline{a} | \, \mathbf{ggT}\,(a,n) = 1\}$
Nun definieren wir: $(\mathbb{Z}/_{n\mathbb{Z}})^* := \{\overline{a} \in \mathbb{Z}/_{n\mathbb{Z}} | \, \overline{a}$ **ist invertierbar**$\}$
Beweis:

- **Assoziativität: klar, denn die Multiplikation in** $\mathbb{Z}/_{n\mathbb{Z}}$ **ist assoziativ.**
- **neutrales Element:** $1 \in (\mathbb{Z}/_{n\mathbb{Z}})^*$, $\overline{1} \cdot \overline{a} = \overline{a} \cdot \overline{1} = \overline{a}$.
- **Inverses Element in** $(\mathbb{Z}/_{n\mathbb{Z}})^*$**: Zu** $\overline{a}$ **ist ein** $\overline{b}$ **zu finden mit** $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$.
  Nach Definition ($\overline{a}$ **ist invertierbar)** $\exists \overline{b}$ **mit** $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$.
  Nach Definition der Invertierbarkeit ist auch $\overline{b}$ **invertierbar.**
- **Noch zu zeigen: Multiplikation liefert Verknüpfung auf** $(\mathbb{Z}/_{n\mathbb{Z}})^*$.
  Zu zeigen: $\overline{a}, \overline{b}$ **sind invertierbar** $\overset{(*)}{\Rightarrow}$ $\overline{a} \cdot \overline{b}$ **ist invertierbar.**

Beweis von $(*)$**. Zu zeigen** $\exists \overline{c}$ **mit** $\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{c} \cdot \left(\overline{a} \cdot \overline{b}\right) = 1$.
[Uns steht zur Verfügung: $\overline{a}, \overline{b}$ **sind invertierbar:** $\overline{a} \cdot \overline{a_1} = \overline{a_1} \cdot \overline{a} = 1$ **und** $\overline{b} \cdot \overline{b_1} = \overline{b_1} \cdot \overline{b} = 1$**]**
Es folgt:

$$\begin{aligned} \left(\overline{a} \cdot \overline{b}\right) \cdot \left(\overline{a_1} \cdot \overline{b_1}\right) &= \left(\overline{a} \cdot \overline{a_1}\right) \cdot \left(\overline{b} \cdot \overline{b_1}\right) = 1 \cdot 1 = 1 \\ \left(\overline{a_1} \cdot \overline{b_1}\right) \cdot \left(\overline{a} \cdot \overline{b}\right) &= \left(\overline{a_1} \cdot \overline{a}\right) \cdot \left(\overline{b_1} \cdot \overline{b}\right) = 1 \cdot 1 = 1 \end{aligned}$$

Also $\overline{c} = \left(\overline{a_1} \cdot \overline{b_1}\right) = \left(\overline{b_1} \cdot \overline{a_1}\right)$.
Bemerkungen:

(i) $(\mathbb{Z}/_{n\mathbb{Z}})^*$ **ist eine abelsche Gruppe**

(ii) $\left|(\mathbb{Z}/_{n\mathbb{Z}})^*\right| =: \varphi(n)$. $\varphi(n)$ **ist die Eulersche** φ**-Funktion.**

2.1.37 Eulersche φ-Funktion

Für die Eulersche φ**-Funktion gilt:**

$$\varphi(n) = \prod_{p|n} p^{\alpha_p - 1}(p-1) \quad \textbf{bei} \;\; n = \prod_{p|n} p^{\alpha_p}$$

2.1.38 Zusammenfassung von Kapitel (II.1)

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ **sind abelsch.**
- $\mathbf{S}_n$ **mit** $|\mathbf{S}_n| = n!$ **ist nicht abelsch für** $n \geq 3$.
- $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ **mit** $|(\mathbb{Z}/_{n\mathbb{Z}}, +)| = n$ **ist abelsch.**
- $(\mathbb{Z}/_{n\mathbb{Z}})^*$ **mit** $\left|(\mathbb{Z}/_{n\mathbb{Z}})^*\right| = \varphi(n)$ **ist abelsch.**

2.2 Kapitel (II.2): Ringe und Körper

2.2.1 Definition (II.2.a): Ring

Eine Menge $(\mathbf{R}, +, \cdot)$ mit zwei Verknüpfungen ("+": Addition genannt, "·": Multiplikation genannt) heißt Ring, wenn sie folgende Axiome erfüllt sind:

- **$(\mathbf{R}, +)$ ist abelsche Gruppe**
- **$(\mathbf{R}, \cdot)$ ist Halbgruppe**
- **Die Distributivgesetze gelten: $\forall a, b, c \in \mathbf{R}$:**

$$a\,(b+c) = ab + ac \qquad (a+b)\,c = ac + bc$$

  (ausdrücklich: Nichtkommutativität von "·")

Anmerkungen zur Notation:

- **Neutrales Element bezüglich der Addition: 0, Nullelement mit**

$$0 + a = a + 0 = a$$

- **Inverses Element bezüglich der Addition: $(-a)$ mit**

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

- **Die Subtraktion ist die Addition des inversen Elements bezüglich der Addition:**

$$a - b := a + (-b)$$

- **Neutrales Element bezüglich der Multiplikation (falls vorhanden): 1, Einselement mit:**

$$1 \cdot a = a \cdot 1 = a$$

2.2.2 Beispiele für Ringe

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ **(aus der Schule bekannt)**
- $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ **(aus der Vorlesung bekannt)**

Nachweis, daß $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ ein Ring ist:

- **Additive Gruppe: schon erledigt.**
- **Multiplikative Halbgruppe: schon erledigt.**
- **Untersuchung ob die Distributivgesetze gelten:**

1. Distributivgesetz:

$$\overline{a} \cdot \left(\overline{b} + \overline{c}\right) = \overline{a} \cdot \left(\overline{b+c}\right) = \overline{a \cdot (b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

Der Trick: Wir führen Operationen in $\mathbb{Z}/_{n\mathbb{Z}}$ auf Operationen in $\mathbb{Z}$ zurück.
2. Distributivgesetz: Das 2. Distributivgesetz gilt, da die Multiplikation in $\mathbb{Z}$ kommutativ ist und das 1. Distributivgesetz gilt. $\square$
Einselemet: $\overline{1}$ ist das Einselement in $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$:

$$\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a} = \overline{a \cdot 1} = \overline{a} \cdot \overline{1}$$

2.2.3 Definition (II.2.b): kommutativer Ring mit 1

$(\mathbf{R}, +, \cdot)$ heißt kommutativer Ring mit 1 (Einselement) falls gilt:

- **$(\mathbf{R}, +, \cdot)$ ist ein Ring.**
- **Die Multiplikation ist kommutativ.**
- **$\exists 1$ (Es existiert ein Einselement)**

Es existiert aber ein kleines Problem: additive und multiplikative "Vielfachheit" eines Elements:
Sei $(\mathbf{H}, \cdot)$ eine Halbgruppe:
Multiplikative Vielfachheit: $a^n :=$ n-fache Verknüpfung von a mit sich selbst für $n \geq 1$.
Additive Vielfachheit:

- **Für** $n \in \mathbb{N}$ $\underbrace{a + \ldots + a}_{n - \text{mal}} =: n \cdot a$
- $n = 0$**:** $\underset{\in \mathbb{Z}}{0} \cdot a = \underset{\in \mathbb{R}}{0}$
- $n \in \mathbb{Z}$, $n < 0$**:** $n \cdot a := |n| \cdot (-a) = \underbrace{(-a) + \ldots + (-a)}_{|n|\,\textbf{-mal}}$

Es gelten die Vielfachengesetze (früher: Potenzgesetze siehe (II.1.7)) in Gruppen für $n, m \in \mathbb{Z}$:

$$\begin{aligned} n \cdot a + m \cdot a &= (n + m) \cdot a \\ n \cdot (m \cdot a) &= (n \cdot m) \cdot a \\ -(-a) &= a \\ -(a + b) &= (-a) + (-b) \\ n \cdot (a + b) &= n \cdot a + n \cdot b, \quad \textbf{falls} \quad a + b = b + a \end{aligned}$$

Die Vielfachengesetze bezüglich der Multiplikation mibt $n \in \mathbb{N}$:

$$a^n := \underbrace{a \cdot \ldots \cdot a}_{n\textbf{-mal}} \quad \textbf{mit} \quad n \geq 1 a^0, \qquad := 1 \quad \textbf{falls} \quad 1 \in \mathbf{R}$$

Es gelten die altbekannten Potenzgesetze bezüglich der Multiplikation:

$$a^n \cdot a^m = a^{n+m} \qquad (a^n)^m = a^{n \cdot m} = (a^m)^n$$

2.2.4 Satz (II.2.1): Rechenregeln auf Ringen

Sei $(\mathbf{R}, +, \cdot)$ Ring, $a, b, c \in \mathbf{R}$. Nun gilt:

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

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

(iii) $(a - b) \cdot c = a \cdot c - b \cdot c$**,** $a \cdot (b - c) = a \cdot b - a \cdot c$

Beweise:
Zu (i): Es gilt : $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$. Nun addieren wir $-(0 \cdot a)$ auf beiden Seiten der Gleichung und erhalten:

$$\begin{aligned} 0 \cdot a + \underbrace{0 \cdot a + (-(0 \cdot a))}_{=0} &= \underbrace{0 \cdot a + (-(0 \cdot a))}_{=0} \\ a \cdot 0 &= 0 \end{aligned}$$

Wir verfahren analog für $a \cdot 0 = 0$.
Zu (ii): Es gilt:

$$\begin{aligned} a \cdot (-b) + a \cdot (b) &= a \cdot \underbrace{((-b) + b)}_{=0} = a \cdot 0 = 0 \\ a \cdot (b) + a \cdot (-b) &= a \cdot \underbrace{(b + (-b))}_{=0} = a \cdot 0 = 0 \end{aligned}$$

Also folgt: $a \cdot (-b) = -a \cdot b$. Wir verfahren analog für $(-a) \cdot b = -a \cdot b$.
Wenden wir nun die obige Regel an, so erhalten wir für $(-a) \cdot (-b)$:

$$(-a) \cdot (-b) = [-(-a)] \cdot b = a \cdot b$$

Wir nutzen die Tatsache aus, daß $-(-a) = a$ ist. (Siehe Vielfachengesetze).
Zu (iii): Es gilt:

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

Wir verfahren analog für $a \cdot (b - c) = a \cdot b - a \cdot c$.

2.2.5 Definition (II.2.c): Körper

Bemerkung: R sei Ring mit 1. $x \in \mathbf{R}$ sei invertierbar wenn gilt: $\exists y \in \mathbf{R} : x \cdot y = y \cdot x = 1$.
Voraussetzung: $1 \neq 0$. Die Null ist nicht invertierbar, denn $0 \cdot x = 0 \neq 1$.
$\Rightarrow \{x \in \mathbf{R} | x$ ist invertierbar$\} \subseteq \mathbf{R} \setminus \{0\}$.

Definition: Eine kommutativer Ring mit $1 \neq 0$ heißt Körper, wenn jedes Element in $\mathbf{R} \setminus \{0\}$ invertierbar ist (bezüglich der Multiplikation).
Bemerkung (der pathologische Fall): Eine Ring mit $1 = 0 \Leftrightarrow \mathbf{R} = \{0\}$.

Beweis:
"$\Rightarrow$": $x = x \cdot 1 = x \cdot 0 = 0$
"$\Leftarrow$": $\mathbf{R} = \{0\} : 0 + 0 = 0,\ 0 \cdot 0 = 0$ ist Ring mit $1 = 0$.
Von nun an soll für alle betrachteten Ringe gelten $1 \neq 0$.

2.2.6 Beispiele für Körper

Beispiele:

(a) **$(\mathbb{Z}, +, \cdot)$ ist kein Körper, da es inverse Elemente gibt, die nicht in $\mathbb{Z}$ enthalten sind.**

(b) **$(\mathbb{Q}, +, \cdot)$ ist ein Körper. Es ist der kleinste Körper $\supseteq \mathbb{Z}$.**

(c) **$(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind Körper.**

(d) **$(\mathbb{Z}/_{p\mathbb{Z}}, +, \cdot)$ ist Körper, wenn p Primzahl ist Beweis siehe (II.2.2).**

2.2.7 Satz(II.2.2): $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ ist Körper $\Leftrightarrow n$ ist Primzahl.

“$\Rightarrow$” Sei $n = r \cdot s$, $1 < r, s < n$. Es folgt: $\overline{n} = \overline{r} \cdot \overline{s}$. Also $\overline{r} \cdot \overline{s} = \overline{0}$. Es ist $\overline{r} \neq 0$.
Wäre $\overline{r}$ invertierbar, so $\exists \overline{t} : \overline{t} \cdot \overline{r} = \overline{1}$. Es folgt: $\underbrace{\overline{t} \cdot \overline{0}}_{=\overline{0}} = \underbrace{\overline{t} \cdot \overline{r}}_{=\overline{1}} \cdot \overline{s} = \overline{1} \cdot \overline{s}$. Also: $n|s \Rightarrow$ Widerspruch zur Annahme $\overline{n} = \overline{r} \cdot \overline{s}$. Also ist n eine Primzahl.

“$\Leftarrow$”: Schon früher bewiesen: $\overline{a}$ ist invertierbar $\Leftrightarrow$ ggT $(a, n) = 1$. Betrachtung der Elemente in $\mathbb{Z}/_{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$. Für $a = 1, 2, \ldots, n-1$ ist der ggT $(a, n) = 1$, da n eine Primzahl ist. Damit ist jedes Element in $\mathbb{Z}/_{n\mathbb{Z}} \setminus \{0\}$ invertierbar.

2.2.8 Definition (II.2.c): Alternative Definition für Körper

$(\mathbf{R}, +, \cdot)$ heißt Körper $:\Leftrightarrow$

- **(i)** $(\mathbf{R}, +)$ **ist abelsche Gruppe** (0 **ist neutrales Element)**
- **(ii)** $(\mathbf{R} \setminus \{0\}, \cdot)$ **ist abelsche Gruppe**
- **(iii)** $\forall a, b, c \in \mathbf{R} : a \cdot (b + c) = ab + ac$

Bemerkung: 1. Definition $\Leftrightarrow$ 2. Definition
Beweis:
“$\Rightarrow$” Noch zu zeigen:

- **(a)** $\forall a, b \in \mathbf{R} \setminus \{0\} : a \cdot b \neq 0$ **(Wohldefiniertheit)**
- **(b) Assoziativität**
- **(c) Einselement**
- **(d) Invertierbarkeit**

Zu (a): Angenommen: $a \cdot b = 0, a \neq 0$. Multiplikation von links mit a^{-1} ergibt:

$$\begin{aligned} a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot 0 \\ \left(a^{-1} \cdot a\right) \cdot b &= 0 \\ 1 \cdot b &= 0 \\ b &= 0 \end{aligned}$$

Aber: $b = 0$ ist ein Widerspruch zur Voraussetzung.
Zu (b): klar, weil $(\mathbf{R}, \cdot)$ assoziativ.
Zu (c): $1 \neq 0$, also $1 \in \mathbf{R} \setminus \{0\}$: $1 \cdot a = a = a \cdot 1$
Zu (d): $a \neq 0$. Zu zeigen: $\exists b \neq 0$ mit $a \cdot b = 1$
$\exists b$ mit $a \cdot b = 1$ nach der 1. Definition. $b \neq 0$, sonst $a \cdot b = a \cdot 0 = 0 \neq 1$.
“$\Leftarrow$”: Selbst oder nie.

Der Körper $\mathbb{C}$

2.2.9 Gründe für ein Studium weiterer Körper:

(a) $\mathbb{Q} \to \mathbb{R}$:

- **Gleichungen lösen wie zum Beispiel:** $x^2 - 2 = 0$.
- **Längen in der Geometrie: Nach den Vorstellungen der Griechen sind alle Strecken kommensummerable (haben ein rationales Streckenverhältnis). Nach Pythagoras ist aber die Hypothenuse eines rechtewinkligen Dreiecks mit den Katheten der Länge Eins nicht kommensummerable, da die Hypothenuse die Länge** $\sqrt{2}$ **hat.**
- **Kreisumfang:** πr^2. **Es gibt keine algebraische Gleichung der Form**
$$\pi^k + \alpha_1 \cdot \pi^{k-1} + \ldots + \alpha_k = 0$$
mit $\alpha_i \in \mathbb{Q}$. **Eine andere transzendentale Zahl ist zum Beispiel** e.

(b) Endliche Körper:

- **Teilbarkeitslehre (**$\Rightarrow$ **Kongruenzrelation)**
- **Kodierungstheorie**
- **Kryptographie**

(c) $\mathbb{R} \to \mathbb{C}$:

- **Studium <u>weiterer</u> Gleichungen. Zum Beispiel:**
$$\begin{aligned} x^2 + 1 &= 0 \\ x^2 + 4x + 9 &= 0 \\ x^{27} + 22x^{13} + x^6 - 1 &= 0 \end{aligned}$$

2.2.10 Herleitung von $\mathbb{C}$

Angenommen $\mathbb{K} \supseteq \mathbb{R}, \exists i : i^2 + 1 = 0$. $\mathbb{R} \subseteq \mathbb{K} \quad \Rightarrow \quad a + ib \in \mathbf{K}\, \forall a, b \in \mathbb{R}$.
Gleichheit zweier Elemente:
Behauptung: $a + bi = a' + b'i$ **mit** $a, a', b, b' \in \mathbb{R} \Rightarrow a = a', b = b'$.
Beweis:
$$\begin{aligned} (a - a') &= (b' - b) \cdot i && \mid \textbf{quadrieren} \\ (a - a')^2 &= (b' - b)^2 \cdot i^2 \\ (a - a')^2 &= -(b' - b)^2 \\ (a - a')^2 + (b' - b)^2 &= 0 && \textbf{in } \mathbb{R} \end{aligned}$$
Daher: $(a' - a)^2 = 0 \wedge (b' - b)^2 = 0 \Rightarrow a = a' \wedge b = b'$
Multiplikation zweier Elemente:
$$\begin{aligned} (a + bi) \cdot (c + di) &\overset{D}{=} a \cdot (c + di) + bi \cdot (c + di) \\ &\overset{D}{=} ac + adi + bic + bidi \\ &\overset{A+K}{=} ac + adi + bci + bdi^2 \\ &\overset{A+K}{=} (ac - bd) + i \cdot (ad + bc) \end{aligned}$$
Aus der Annahme $\mathbb{R} \subseteq \mathbb{K}$, **Körper,** $i^2 + 1 = 0, i \in \mathbb{K}$ **folgt:** $\mathbb{K} \supseteq \{a + bi \mid a, b \in \mathbb{R}\}$ **ist Ring.**

Behauptung: $a + bi \neq 0 \Rightarrow a + bi$ **ist invertierbar.**
Ohne dies jetzt im Detail herzuleiten glauben wir:

$$(a + bi)^{-1} = \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} \cdot i \right)$$

Beweis:

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} \cdot i \right) = \frac{(a + bi) \cdot (a - bi)}{a^2 + b^2} = \frac{a^2 - (bi)^2}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

$\Rightarrow \mathbf{K} \supseteq \{ a + bi | \, a, b \in \mathbb{R} \}$ **ist sogar Körper.**

2.2.11 Konstruktion von $\mathbb{C}$

$\mathbb{C} = \left(\mathbb{R}^2, +, \cdot \right)$
Addition: $(a, b) + (c, d) = (a + c, b + d)$ **(komponentenweise)**
Multiplikation: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

2.2.12 Satz (II.2.3)

$\mathbb{C}$ **ist ein Körper:**

- **Nullelement:** $(0, 0)$
- **Einselement:** $(1, 0)$
- **Inverses Element für** $(a, b) \neq (0, 0)$**:**

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right)$$

Beweise: Nachrechnen. Beispiele dazu:
Assoziativität bezüglich der Multiplikation: Seinen $a, b, c, d, e, f \in \mathbb{R}$**:**
Behauptung: $[(a, b) \cdot (c, d)] \cdot (e, d) = (a, b) \cdot [(c, d) \cdot (e, f)]$**.**
Auf der linken Seite ergibt sich:

$$\begin{aligned} [(a, b) \cdot (c, d)] \cdot (e, d) &= (ac - bd, ad + bc) \cdot (e, f) \\ &= ((ac - bd) \cdot e - (ad + bc) \cdot f, (ac - bd) \cdot f + (ad + bc) \cdot e) \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce) \end{aligned}$$

Auf der rechten Seite ergibt sich:

$$\begin{aligned} (a, b) \cdot [(c, d) \cdot (e, f)] &= (a, b) \cdot (ce - df, cf + de) \\ &= (a \cdot (ce - df) - b \cdot (cf + de), a \cdot (cf + de) + b \cdot (ce - df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) \end{aligned}$$

Da in $\mathbb{R}$ **Addition und Multiplikation kommutativ sind, erhalten wir dasselbe Ergebnis für die linke und rechte Seite.**
Neutrales Element:

$$\begin{aligned} (1, 0) \cdot (a, b) &= (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b) \\ (a, b) \cdot (1, 0) &= (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b) \end{aligned}$$

Inverses Element:

$$\begin{aligned}
(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right) &= \left(a\cdot\frac{a}{a^2+b^2}-b\cdot\frac{-b}{a^2+b^2},a\cdot\frac{-b}{a^2+b^2}+b\cdot\frac{a}{a^2+b^2}\right)\\
&= \left(\frac{a^2+b^2}{a^2+b^2},\frac{-a\cdot b+a\cdot b}{a^2+b^2}\right)\\
&= (1,0)\\
\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)\cdot(a,b) &= \left(\frac{a}{a^2+b^2}\cdot a-\frac{-b}{a^2+b^2}\cdot b,\frac{a}{a^2+b^2}\cdot b+\frac{-b}{a^2+b^2}\cdot a\right)\\
&= \left(\frac{a^2+b^2}{a^2+b^2},\frac{a\cdot b-a\cdot b}{a^2+b^2}\right)\\
&= (1,0)
\end{aligned}$$

Nun wollen wir die Lösung der Gleichung: $x^2+1=0$ **untersuchen.**
Genauer: $\exists\,(a,b)$ **mit** $(a,b)^2+(1,0)=(0,0)$**?**
Das heißt: $\left(a^2-b^2+1,2a\cdot b\right)=(0,0)$**. Wir erhalten also ein Gleichungssystem in** $\mathbb{R}$**:**

$$\begin{aligned}
a^2-b^2+1 &= 0\\
\wedge\qquad 2ab &= 0
\end{aligned}$$

Die zweite Gleichung liefert: $a=0$ **oder** $b=0$**.**
Für $a=0$ **ergibt sich:** $-b^2+1=0\Rightarrow b=\pm1$**.**
Für $b=0$ **ergibt sich:** $a^2+1=0$**. Diese Gleichung hat keine Lösung in** $\mathbb{R}$**.**
Falls eine Lösung vorhanden ist muß gelten: $a=0,b=\pm1$**.**
Nachrechnen liefert $(0,\pm1)$ **als die beiden Lösungen.**
Die Gleichung $x^2+1=0$ **hat also genau zwei Lösungen in** $\mathbb{C}$**.**

2.2.13 Einbettung von $\mathbb{R}$ in $\mathbb{C}$

Wir konstruieren nun eine Funktion φ **mit:** $\varphi:\mathbb{R}\to\mathbb{C}:a\mapsto(a,0)$**.**
Eigenschaften von φ**:**

$$\varphi(a+b)=\varphi(a)+\varphi(b)\qquad \varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$$

$\varphi:\mathbb{R}\to\{(a,0)\,|\,a\in\mathbb{R}\},\varphi$ **ist bijektiv.**
Stichwort: Isomorphismus.
Beweise (hier nur für "$\cdot$", "$+$" ist analog):

$$\begin{aligned}
\varphi(a\cdot b) &= (a\cdot b,0)\\
\varphi(a)\cdot\varphi(b) &= (a,0)\cdot(b,0)=(a\cdot b-0\cdot0,a\cdot0+0\cdot b)=(a\cdot b,0)
\end{aligned}$$

Die geometrische Bedeutung: $\mathbb{R}^2$ ist eine Ebene:

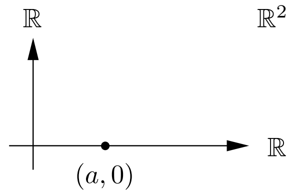

Abbildung II-4: $\mathbb{R}$ eingebettet als "x-Achse"

Anmerkung: Bei der "x-Achse" spricht man auch von der reellen Achse.
Nun die komplexe 1 und 0; i und $-i$ im $\mathbb{C}$:

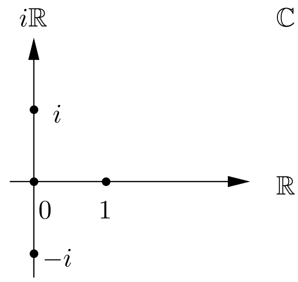

Abbildung II-5: Komplexe 1 und 0, i und $-i$ im Körper $\mathbb{C}$

Wichtig: $(a,b) = (a,0) + (b,0) \cdot i$**, da**

$$(a,0) + (b,0) \cdot (0,1) = (a,0) + (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (a,0) + (0,b) = (a,b)$$

Also folgt: $(a,b) \mapsto a + ib$**. Dies läßt sich geometrisch folgendermaßen darstellen:**

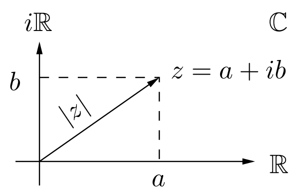

Abbildung II-6: geometrische Darstellung von $a + ib$

2.2.14 Rechenregeln für komplexe Zahlen

- **Gleichheit zweier komplexer Zahlen:** $a + ib = a' + ib' \Leftrightarrow a = a' \wedge b = b'$
- **Addition zweier komplexer Zahlen:** $(a + ib) + (c + id) = (a + c) + i \cdot (b + d)$
- **Multiplikation:** $(a + ib) \cdot (c + id) = (ac - bd) + i \cdot (ad + bc)$
- **Inverse Element:** $a + bi \neq 0 \Rightarrow (a + ib)^{-1} = \dfrac{a}{a^2 + b^2} - i \cdot \dfrac{b}{a^2 + b^2}$
- **Zusätzlich gilt:** $i^2 = -1$

2.2.15 Beispiele für das Rechnen mit komplexen Zahlen

Berechnen Sie alle Lösungen der Gleichung $x^4 - 4 = 0$ in $\mathbb{C}$.
Nun gilt:

$$(1+i)^4 = \left((1+i)^2\right)^2 = \left(1+2i+i^2\right)^2 = (1-1+2i)^2 = (2i)^2 = 4i^2 = -4$$

Das heißt $(1+i)^4$ ist eine Lösung der Gleichung $x^4 - 4 = 0$. Wieviele Lösungen hat nun die Gleichung $x^4 + 4 = 0$ in $\mathbb{C}$?

Sei $x^4 + 4 = 0$, dann $\left(\frac{x^2}{2}\right)^2 + 1 = 0 \quad \Rightarrow \quad \frac{x^2}{2} = \pm i$. **Also** $x^2 = 2i \vee x^2 = -2i$.

Anmerkung: $y^2 = 1 \Rightarrow (y+1)\cdot(y-1) = 0 \Rightarrow y = \pm 1$.

Aus $x^2 = 2i$ folgt: $x^2 = (1+i)^2 \quad \Rightarrow \quad \left(\frac{x}{1+i}\right)^2 = 1 \quad \Rightarrow \quad x = \pm(1+i)$.

Aus $x^2 = -2i$ folgt: $x^2 = -(1+i)^2 \quad \Rightarrow \quad \left(\frac{x}{1+i}\right)^2 = -1 \quad \Rightarrow \quad \frac{x}{1+i} = \pm i$. **Nun gilt:**

$$\begin{aligned} & x = i\cdot(1+i) = i - 1 = -1 + i \\ \vee \quad & x = -i\cdot(1+i) = 1 - i \end{aligned}$$

Also ergeben sich folgende Kandidaten für Lösungen der Gleichung $x^4 + 4 = 0$:

$$\pm(1+i), -1+i, 1-i$$

Durch einsetzen und ausrechnen ergibt sich, daß alle vier Kandidaten Lösungen sind.

2.2.16 Satz (II.2.4): Fundamentalsatz der Algebra (ohne Beweis)

Seien $n \in \mathbb{N}$, $a_0, \ldots, a_n \in \mathbb{C}$.
Dann besitzt $f(x) = a_0 + a_1 \cdot x^1 + a_2 \cdot x^2 + \ldots + x_n \cdot x^n$ mindestens eine Nullstelle in $\mathbb{C}$.

2.2.17 Satz (II.2.5): Rechenregeln für komplexe Zahlen

Seien $z, w \in \mathbb{C}$. Dann gilt:

(i) $z \in \mathbb{R} \quad \Leftrightarrow \quad z = \overline{z}$

(ii) $z \cdot \overline{z} = |z|^2$, $|z| = \sqrt{z \cdot \overline{z}}$

(iii) $\overline{z+w} = \overline{z} + \overline{w}$, $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$

(iv) $z \neq 0 \quad \Rightarrow \quad z^{-1} = \frac{1}{|z|^2} \cdot \overline{z}$

(v) $\overline{w} \neq 0 \quad \Rightarrow \quad \overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$

(vi) $\overline{\overline{z}} = z$

Beweise: Seien $z = a + i\cdot b$, $w = c + i \cdot d$ **mit** $a, b, c, d \in \mathbb{R}$
Zu (i):

$$z = \overline{z} \quad \Leftrightarrow \quad a + ib = a - ib \quad \Leftrightarrow \quad ib = -ib \quad \Leftrightarrow \quad b = 0 \quad \Leftrightarrow \quad z \in \mathbb{R}$$

Zu (ii):

$$z \cdot \overline{z} = (a+ib)\cdot(a-ib) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2 \quad \textbf{da} \quad |z| = \sqrt{a^2+b^2}$$

$|z| = \sqrt{z \cdot \overline{z}}$ **folgt direkt, indem wir die Wurzel ziehen.**

Zu (iii)**: Für die Addition:**

$$\begin{aligned}\overline{z+w} &= \overline{(a+ib)+(c+id)} = \overline{(a+c)+i\cdot(b+d)} \\ &= (a+c)-i\cdot(b+d) = (a-ib)+(c-id) = \overline{z}+\overline{w}\end{aligned}$$

Für die Multiplikation:

$$\begin{aligned}\overline{z\cdot w} &= \overline{(a+ib)\cdot(c+id)} = \overline{ac-bd+i\cdot(bc+ad)} \\ &= ac-bd-i\cdot(bc+ad) = ac-bd-ibc-iad \\ &= (a-ib)\cdot(c-id) = \overline{(a+ib)}\cdot\overline{(c+id)} = \overline{z}\cdot\overline{w}\end{aligned}$$

Zu (iv)**: folgt aus** (ii)**.**

Zu (v): $\overline{w}\neq 0$. $\overline{\left(\frac{z}{w}\right)}\cdot\overline{w} = \overline{\frac{z}{w}\cdot w} = \overline{z} \quad\Rightarrow$ **Behauptung.**

Zu (vi)**:** $\overline{\overline{z}} = \overline{\overline{a+ib}} = \overline{a-ib} = a+ib = z$

2.2.18 Satz (II.2.6)

Seien $z, w \in \mathbb{C}$**. Dann gilt:**

(i) $|z| \geq 0$, $|z| = 0 \quad\Leftrightarrow\quad z = 0$

(ii) $|z\cdot w| = |z|\cdot|w|$

(iii) $|z+w| \leq |z|+|w|$ **(Dreiecksungleichung)**

(i) **und** (iii) **folgen aus den entsprechenden Sätzen für die Normen im** $\mathbb{R}^2$**.**
Beweis zu (ii)**: Seien** $z = a+i\cdot b$, $w = c+i\cdot d$ **mit** $a,b,c,d\in\mathbb{R}$
Nun gilt:

$$\begin{aligned}|z\cdot w| &= |(a+ib)\cdot(c+id)| = |ac-bd+i\cdot(ab+cd)| = \sqrt{(ac-bd)^2+(ab+cd)^2} \\ &= \sqrt{a^2c^2-2abcd+b^2d^2+a^2b^2+2abcd+c^2d^2} \\ &= \sqrt{a^2c^2+b^2d^2+a^2b^2+c^2d^2} = \sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} = |z|\cdot|w|\end{aligned}$$

2.2.19 Die Polarkoordinatendarstellung komplexer Zahlen

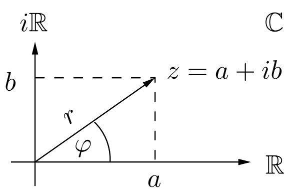

Abbildung II-7: Polarkoordinatendarstellung komplexer Zahlen

Die Polarkoordinatendarstellung für $z\neq 0$ **ist bestimmt durch** (r,φ)**.**
Dabei $r\in\mathbb{R}_+$, $\varphi\in[0,2\pi[$**. Es ist** $r = |z|$**.**
Definition: $\varphi = \arg(z)$ **(Lies "das Argument von** z**")**

2.2.20 Satz (II.2.7): Umrechnungsformeln

(i) Sei $z \in \mathbb{C}$ gegeben durch $r \in \mathbb{R}_+$, $\varphi \in [0, 2\pi[$. Dann ist $z = a + ib = r \cdot (\cos\varphi + i \cdot \sin\varphi)$

(ii) Sei $z = a + ib \in \mathbb{C} \setminus \{0\}$ gegeben. Dann ist $r = |z| = \sqrt{a^2 + b^2}$, $\cos\varphi = \frac{a}{r}$, $\sin\varphi = \frac{b}{r}$

Beweise sollten in der Analysis erfolgen.

2.2.21 Geometrische Bedeutung der Addition in $\mathbb{C}$

Seien z_1, z_2 in der Form $z_k = a_k + ib_k$, $k = 1, 2$ gegeben.
Die Adiition in $\mathbb{C}$ geht auf die Vektoraddition im $\mathbb{R}^2$ zurück.

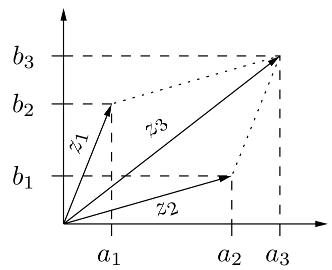

Abbildung II-8: Vektoraddition im $\mathbb{R}^2$

2.2.22 Satz (II.2.8) Multiplikation in $\mathbb{C}$

Seien zwei komplexe Zahlen in Polarkoordinaten gegeben mit $|z_j| = r_j \cdot (\cos\varphi_j + i \cdot \sin\varphi_j)$ für $j = 1, 2$. Dann gilt: $z_1 \cdot z_2 = r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2))$

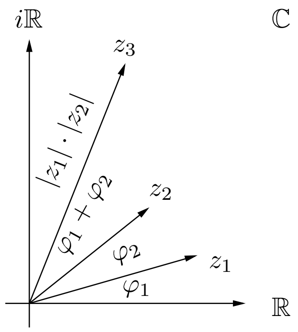

Abbildung II-9: Multiplikation zweier komplexer Zahlen

Beweis: Vorgriff auf die Analysis:
Es gilt:

$$\begin{aligned}\cos(\varphi_1 + \varphi_2) &= \cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \cdot \sin\varphi_2 \\ \sin(\varphi_1 + \varphi_2) &= \cos\varphi_1 \cdot \sin\varphi_2 + \sin\varphi_1 \cdot \cos\varphi_2\end{aligned}$$

Also gilt für $z_1 \cdot z_2$:

$$\begin{aligned}z_1 \cdot z_2 &= r_1 \cdot r_2 \cdot [(\cos\varphi_1 + i \cdot \sin\varphi_1) \cdot (\cos\varphi_2 + i \cdot \sin\varphi_2)] \\ &= r_1 \cdot r_2 \cdot [(\cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \cdot \sin\varphi_2) + i \cdot (\cos\varphi_1 \cdot \sin\varphi_2 + \sin\varphi_1 \cdot \cos\varphi_2)] \\ &= r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2))\end{aligned}$$

2.2.23 Satz (II.2.9): Formel von De Moivre

Ist $z = r \cdot (\cos\varphi + i \cdot \sin\varphi)$ **und** $n \in \mathbb{N}$**, so ist** $z^n = r^n \cdot (\cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi))$**.**
Beachte: $n \cdot \varphi$ **oder** $\varphi_1 + \varphi_2$ **ist immer als** $\bmod 2\pi$ **beziehungsweise Modulo** 360^0 **zu verstehen.**
In der Analysis: $\cos\varphi + i \cdot \sin\varphi = e^{i\varphi}$ **(komplexe Exponentialfunktion)**
Dann: $\exp(x+y) = \exp(x) \cdot \exp(y)$, $z = r \cdot e^{i\varphi} \Rightarrow z^n = r^n \cdot e^{n \cdot i\varphi}$
Anwendung: Ziehen der n**-ten Wurzel aus einer komplexen Zahl**
(Vergleiche Aufgabe ? auf Übungsblatt 7)
Fazit: 3 Deutungen von $\mathbb{C}$**:**

(1) $(a,b) \in \mathbb{R}^2$**. Nützlich für Addition, Betrag, etc.**

(2) $a + ib$**. Nützlich für Rechnungen** $\left(i^2 = -1\right)$**.**

(3) Polarkoordinaten. Nützlich für Multiplikation, Wurzel ziehen, etc.

Warnung: Oft wird geschrieben: $i = \sqrt{-1}$**.**
Zum einen: $i = \left\{z \in \mathbb{C} : z^2 = -1\right\}$**. Wenn** $i = \sqrt{-1}$**, so ist auch** $-i = \sqrt{-1}$**, aber** $i \neq -i$**.**
Zum Beispiel:

$$-1 = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1) \cdot (-1)} = \sqrt{1} = 1$$

Wir erhalten einen Widerspruch.

2.2.24 Definition (II.2.d): Charakteristik eines Körpers $\mathbb{K}$

Sei $\mathbb{K}$ **ein Körper. Die Charakteristik eines Körpers** $\mathbb{K}$ **ist endlich, falls** $\exists n \in \mathbb{N}$**, so daß**

$$n \times 1_{\mathbb{K}} = \underbrace{1_{\mathbb{K}} + 1_{\mathbb{K}} + \ldots + 1_{\mathbb{K}}}_{n - \textbf{mal}} = 0_{\mathbb{K}}$$

Beispiele:

(a) Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ **haben keine Charakteristik.**

(b) Der endliche Körper $\mathbb{Z}/_{p\mathbb{Z}} = \mathbb{F}_p$ **hat die Charakteristik** p**.**

Allgemein gilt für endliche Körper: char $(\mathbb{K}) = \min\{n \in \mathbb{N} : n \times 1_{\mathbb{K}} = 0_{\mathbb{K}}\} \overset{!}{=}$ **Primzahl**
Anmerkungen:

- **char** $(\mathbb{K}) = 1 \quad \Rightarrow \quad 1 \times 1_{\mathbb{K}} = 0$ **(pathologischer Fall - geht nicht)**
- **char** $(\mathbb{K}) = 2 \quad \Rightarrow \quad 2 \times 1_{\mathbb{K}} = 1_{\mathbb{K}} + 1_{\mathbb{K}} = 0_{\mathbb{K}} \quad \Rightarrow \quad \forall a \in \mathbb{K}\text{:}\ a + a = 0 \quad \Leftrightarrow \quad a = -a.$
  Ein Beispiel: $\mathbb{Z}/_{2\mathbb{Z}} = \mathbb{F}_2$
- **Umgekehrt:** $\forall a \in \mathbb{K}$**:** $a + a = 0 \quad \Rightarrow \quad$ **char** $(\mathbb{K}) = 2$

2.3 Kapitel (II.3): Vektorräume

2.3.1 Definition (II.3.a): Vektorraum:

$\mathbb{K}$ sei ein Körper. $\mathbf{V} = (\mathbf{V}, +, \cdot)$ mit:

- **Addition:** $+ : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$
- **skalare Multiplikation:** $\cdot : \mathbb{K} \times \mathbf{V} \to \mathbf{V}$.

Das Tripel $(\mathbf{V}, +, \cdot)$ wird als $\mathbb{K}$-Vektorraum ($\mathbb{K}$-VR) bezeihnet.
Nun müssen folgende Axiome erfüllt sein:

(V1) $(\mathbf{V}, +)$ **ist abelsche Gruppe, das neutrale Element 0 heißt Nullvektor.**

(V2) Für alle $v, w \in \mathbf{V}, \alpha, \beta \in \mathbb{K}$ soll gelten (Distributivgesetze)

(a) $(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$ **(Verträglichkeit der Multiplikation)**
(b) $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$
(c) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
(d) $1 \cdot v = v$

2.3.2 Beispiele für Vektorräume

(a) Standard n-dimensionaler Vektorraum:
$\mathbb{K}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{K}\}$ **ist $\mathbb{K}$-Vektorraum mit**

$$\begin{aligned} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n) \\ \alpha \cdot (x_1, \ldots, x_n) &= (\alpha x_1, \ldots, \alpha x_n) \end{aligned}$$

Nun prüfen wir nach, ob die Axiome erfüllt sind:
Abelsche Gruppe (Stichworte):

- **Assoziativität: auf $+$ in $\mathbb{K}$ zurückführen**
- $0 = (0, \ldots, 0)$
- **Inverses Element bezüglich der Addition:** $-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n)$

Anmerkung: Man muß sich von der Vorstellung verabschieden, daß die Elemente eines Vektorraums ("Vektoren") eine Richtung und Länge haben, wie zum Beispiel der $\mathbb{R}^n$. Ein Beispiel für einen Vektorraum, dessen Objekte keine Länge oder Richtung mehr haben ist $\mathbb{Z}/_{2\mathbb{Z}}$.
(b) $M \neq \phi, \mathbf{V} = \{f : M \to \mathbb{K}\}$. **Nun müssen Addition und skalare Multiplikation erklärt sein. Deshalb definieren wir:**

$$(f + g)(m) = f(m) + g(m) \qquad (\alpha \cdot f)(m) = \alpha \cdot f(m)$$

Für die Null gilt: $0_{\mathbf{V}} : \begin{cases} M \to \mathbb{K} \\ m \mapsto 0_{\mathbb{K}} \end{cases}$
Für das additive Inverse in $\mathbf{V}$ gilt: $(-f)(m) = -f(m)$.
Beweis: Zu zeigen: $f + (-f) = 0_{\mathbf{V}}$.
Genauer zu zeigen: $\forall m \in \mathbf{M} : (f + (-f))(m) = 0_{\mathbf{V}}(m) = 0_{\mathbb{K}}$.
Linke Seite: $(f + (-f))(m) \overset{\textbf{Def.}}{=} f(m) + (-f)(m) \overset{\textbf{Def.}}{=} f(m) - f(m) = 0_{\mathbb{K}}$
Rechte Seite: $0_{\mathbf{V}}(m) \overset{\textbf{Def.}}{=} 0_{\mathbb{K}}$. **Es folgt die Behauptung.**

(c) $\mathbf{M} = \mathbb{R}$, $\mathbb{K} = \mathbb{R}$, $\mathbf{V} = \{f : \mathbb{R} \to \mathbb{R}\}$
(d) $\mathbf{M} = \{1, \ldots, n\}$, $\mathbb{K} = \mathbb{R}$, $\mathbf{V} = \{f : \{1, \ldots, n\} \to \mathbb{R}\}$.
Nun gilt: $\mathbf{V} = \{f : \{1, \ldots, n\} \to \mathbb{R}\} = \{(x_1, \ldots, x_n) : x_i \in \mathbb{R}\} = \mathbb{R}^n$.
Also: $f \leftrightarrow \{x_i = f(i), i = 1, \ldots, n\}$. **Wir definieren:**

$$(f+g)(i) = f(i) + g(i) \qquad (\alpha \cdot f)(i) = \alpha \cdot f(i)$$

Ergebnis: $\{f : \{1, \ldots, n\} \to \mathbb{R}\}$ **ist Standardvektorraum** $\mathbb{R}^n$. **Anstatt** $\mathbb{R}$ **wird auch oft** $\mathbb{K}$ **verwendet.**
(e) $\mathbb{R}$ **ist auf natürliche Art und Weise** $\mathbb{Q}$**-Vektorraum mit:**

$$\mathbb{K} = \mathbb{Q} \qquad + : \mathbb{R} \times \mathbb{R} = \mathbb{R} \qquad \cdot : \mathbb{Q} \times \mathbb{R} = \mathbb{R}$$

Hier nun der Nachweiß in Stichworten:

- $(\mathbb{R}, +)$ **ist Abelsche Gruppe (klar)**
- $(\alpha \cdot \beta) \cdot r = \alpha \cdot (\beta \cdot r)$: **Assoziativität der Multiplikation in** $\mathbb{R}$
- $\alpha \cdot (r + s) = \alpha \cdot r + \alpha \cdot s$ **und** $(\alpha + \beta) \cdot r = \alpha \cdot r + \beta \cdot r$: **Distributivität in** $(\mathbb{R}, +, \cdot)$
- $1 \cdot r = r$ **(die Eins in** $\mathbb{R}$**)**

2.3.3 Satz (II.3.1): Rechenregeln über Vektorräumen

Rechenregeln: Sei $v \in \mathbf{V}$, $\alpha \in \mathbb{K}$. **Es gelten:**

(i) $0_{\mathbb{K}} \cdot v = 0_{\mathbf{V}}$

(ii) $\lambda \cdot 0_{\mathbf{V}} = 0_{\mathbf{V}}$

(iii) $\lambda \cdot v = 0_{\mathbf{V}} \quad \Rightarrow \quad \lambda = 0_{\mathbb{K}} \vee v = 0_{\mathbf{V}}$

(iv) $(-1) \cdot v = -v$

(v) $\lambda \cdot (-v) = (-\lambda) \cdot v = -(\lambda \cdot v)$

Die Beweise erfolgen wie in der Ringtheorie.
Hier als Beispiel (i) **und** (iii)
Zu (i)**: Es gilt:**

$$0_{\mathbb{K}} \cdot v + 0_{\mathbb{K}} \cdot v = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot v = 0_{\mathbb{K}} \cdot v$$

Nun addieren wir das Inverse zu $0_{\mathbb{K}} \cdot v$**:**

$$\begin{aligned}(-0_{\mathbb{K}} \cdot v) + (0_{\mathbb{K}} \cdot v + 0_{\mathbb{K}} \cdot v) &= (-0_{\mathbb{K}} \cdot v)(0_{\mathbb{K}} \cdot v) \\ (-0_{\mathbb{K}} \cdot v + 0_{\mathbb{K}} \cdot v) + (0_{\mathbb{K}} \cdot v) &= 0_{\mathbf{V}} \\ 0_{\mathbf{V}} + (0_{\mathbb{K}} \cdot v) &= 0_{\mathbf{V}} \\ 0_{\mathbb{K}} \cdot v &= 0_{\mathbf{V}}\end{aligned}$$

Zu (iii)**: Zu zeigen** $\lambda \cdot v = 0 \Rightarrow \lambda = 0 \vee v = 0$.
Sei $\lambda \neq 0$. **Dann multiplizieren wir die Gleichung mit** λ^{-1} **von links.**
$\Rightarrow \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0$.
Nun ergibt sich auf der linken Seite: $\lambda^{-1} \cdot (\lambda \cdot v) = \left(\lambda^{-1} \cdot \lambda\right) \cdot v = 1 \cdot v = v$.
Für die rechte Seite gilt: $\lambda^{-1} \cdot 0 = 0$
Also $\Rightarrow v = 0$. **Analog ergibt sich** $\lambda = 0$.

2.3.4 Satz (II.3.2)

Allgemeines Distributivgesetze

$$(i)\ \left(\sum_{i=1}^{n}\lambda_i\right)\cdot v=\sum_{i=1}^{n}\lambda_i\cdot v \quad \textbf{und} \quad (ii)\ \lambda\cdot\left(\sum_{i=1}^{n}v_i\right)=\sum_{i=1}^{n}\lambda\cdot v_i$$

Die Beweise für (i) und (ii) erfolgen per Induktion. Für den Induktionsschritt gilt:

$$\sum_{i=1}^{n}\lambda_i=\left(\sum_{i=1}^{n-1}\lambda_i\right)+\lambda_n, \qquad \sum_{i=1}^{n}v_i=\left(\sum_{i=1}^{n-1}v_i\right)+v_n$$

Der Rest des Beweises ist klar, da die Axiome für binäre Summen gelten.

2.3.5 Definition (II.3.b): Untervektorraum

U heißt Untervektorraum von V (Notation: U $<$ V) wenn U bezüglich der Einschränkung der Addition und skalaren Multiplikation ein Vektorraum ist.

2.3.6 Beispiel für Untervektorräume

Beispiele:
(a) U $=\{x,y,0\}$ bezüglich der Einschränkung der Addition und skalaren Multiplikation ist ein Vektorraum. Damit ist U ein Untervektorraum: U $=\{(x,y,0):x,y\in\mathbb{K}\}<\mathbb{K}^3$

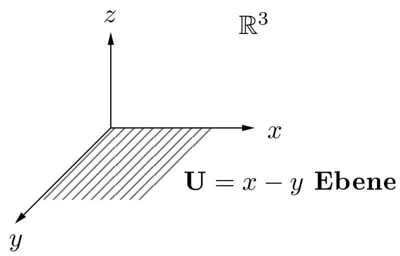

Abbildung II-10: Beispiel für einen Untervektorraum

(b) U $:=\{(x,1):x\in\mathbb{R}\}\subseteq\mathbb{R}^2$

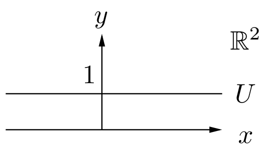

Abbildung II-11: **U** im $\mathbb{R}^2$

Ist $+|_{\mathbf{U}}$ eine Verknüpfung auf U?
Nein, denn $(x,1)+(y,1)=(x+y,1+1)=(x+y,2)\notin$ **U**
(c) U $:=\left\{(x,y):x,y\in\mathbb{Z}/_{3\mathbb{Z}},\ x^3+y^3=0\right\}\subseteq\left(\mathbb{Z}/_{3\mathbb{Z}}\right)^2$
Nun wenden wir einen Trick an: Für $\mathbb{Z}/_{3\mathbb{Z}}$ gilt: $x^3=x\,\forall x$.
Beweis: Durch Ausprobieren ergibt sich:

$$\overline{0}^3=\overline{0} \qquad \overline{1}^3=\overline{1} \qquad \overline{2}^3=\overline{2}$$

Damit ergibt sich für U:

$$\mathbf{U} = \{(x, y) : x, y \in \mathbb{Z}/_{3\mathbb{Z}},\ x + y = 0\}$$

Nun gilt für x und y: $y = -x$. Damit ergibt sich endgültig für U:

$$\mathbf{U} = \{(x, -x) : x \in \mathbb{Z}/_{3\mathbb{Z}}\}$$

Abschließend müssen wir zeigen, daß U bezüglich der Einschränkungen von Addition und skalarer Multiplikation ein Vektorraum ist.
Addition: $(x, -x) + (y, -y) = (x + y, -x + (-y)) = (x + y, -(x + y))$. **Anmerkung: In der Gruppentheorie haben wir folgende Rechenregel kennengelernt:** $-(a + b) = -a + (-b)$.
Skalare Multiplikation: $\alpha \cdot (x, -x) = (\alpha \cdot x, \alpha \cdot (-x)) = (\alpha \cdot x, -\alpha \cdot x)$. **Anmerkung: In der Ringtheorie haben wir folgende Rechenregel kennengelernt:** $a \cdot (-b) = -a \cdot b = (-a) \cdot b$.
Damit gilt:

$$\begin{aligned} + &: \mathbf{U} \times \mathbf{U} \to \mathbf{U} \\ \cdot &: \mathbb{Z}/_{3\mathbb{Z}} \times \mathbf{U} \to \mathbf{U} \end{aligned}$$

Alle anderen Axiome sind schon in $\left(\mathbb{Z}/_{3\mathbb{Z}}\right)^2$ erfüllt. Damit ist U ein Untervektorraum.
(d) $\mathbb{L}$ sei der Lösungsraum des linearen Gleichungssystems:

$$\begin{array}{ccccccccccc} a_{11} \cdot x_1 & + & a_{12} \cdot x_2 & + & a_{13} \cdot x_3 & + & \dots & + & a_{1n} \cdot x_n & = & b_1 \\ a_{21} \cdot x_1 & + & a_{22} \cdot x_2 & + & a_{23} \cdot x_3 & + & \dots & + & a_{2n} \cdot x_n & = & b_2 \\ a_{31} \cdot x_1 & + & a_{32} \cdot x_2 & + & a_{33} \cdot x_3 & + & \dots & + & a_{3n} \cdot x_n & = & b_3 \\ \vdots & & \vdots & & \vdots & & \ddots & & \vdots & \vdots & \vdots \\ a_{m1} \cdot x_1 & + & a_{m2} \cdot x_2 & + & a_{m3} \cdot x_3 & + & \dots & + & a_{mn} \cdot x_n & = & b_m \end{array}$$

$x_1, \dots, x_n$ **sind die Unbekannten. Die a_{ij} sind (bekannte) Koeffizienten des Gleichungssystems. $(b_1, \dots, b_m)$ ist die Lösungsspalte.**
Nun gilt für den Lösungsraum:

$$\mathbb{L}(a_{ij}, b_k) = \left\{ (x_1, \dots, x_n) \in \mathbb{K}^n : \sum_{j=1}^{n} a_{ij} \cdot x_j = b_i \right\}$$

wobei $i = 1 \dots m$, $j = 1 \dots n$, $k = 1 \dots m$.
Zu zeigen: $\mathbb{L}(a_{ij}, b_k) < \mathbb{K}^n$.

2.3.7 Konstruktion von Vektorräumen

(a) $\mathbf{U}_1, \mathbf{U}_2 < \mathbf{V} \Rightarrow \mathbf{U}_1 \cap \mathbf{U}_2 < \mathbf{V}$. Wir definieren:

$$\mathbf{U}_1 + \mathbf{U}_2 := \{u_1 + u_2 : u_1 \in \mathbf{U}_1, u_2 \in \mathbf{U}_2\} < \mathbf{V}$$

Warnung: im allgemeinen: $\mathbf{U}_1 \cup \mathbf{U}_2 \not< \mathbf{V}$
(b) $\mathbf{V}_1, \mathbf{V}_2$ seinen $\mathbb{K}$-Vektorräume $\Rightarrow \mathbf{V}_1 \times \mathbf{V}_2 = \{(v_1, v_2) : v_i \in \mathbf{V}_i\}$ ist $\mathbb{K}$-Vektorraum bezüglich:

$$\begin{aligned} (v_1, v_2) + (v_1', v_2') &= (v_1 + v_1', v_2 + v_2') \\ \alpha \cdot (v_1, v_2) &= (\alpha \cdot v_1, \alpha \cdot v_2) \end{aligned}$$

Allgemein: $\mathbf{U}_i < \mathbf{V}_i \Rightarrow \mathbf{U}_1 \times \mathbf{U}_2 < \mathbf{V}_1 \times \mathbf{V}_2$

2.3.8 Satz (II.3.3):

Sei $(\mathbf{V}, +, \cdot)$ ein $\mathbb{K}$-Vektorraum.
$\mathbf{U} \subseteq \mathbf{V}$ heißt Untervektorraum, wenn gilt:

(i) $\mathbf{U} \neq \phi$

(ii) $\forall u, v \in \mathbf{U} : u + v \in \mathbf{U}$

(iii) $\forall \alpha \in \mathbf{K}, \forall u \in \mathbf{U} : \alpha \cdot u \in \mathbf{U}$

Bedeutung: $(\mathbf{U}, +, \cdot)$ ist ein Vektorraum über $\mathbb{K}$.
Beweis: Selbst oder Buch
Diese drei Kriterien werden im Allgemeinen für den Nachweis verwandt. Die anderen Axiome sind in der Regel für U erfüllt, da diese Axiome schon für V erfüllt sind.
Es gibt mindestens zwei Untervektorräume für einen Vektorraum V: $\mathbf{V} < \mathbf{V}$ $\quad \{0\} < \mathbf{V}$

2.3.9 Beispiele für Untervektorräume und deren Konstruktion

(a) Gegeben sei der $\mathbb{R}^3$. Eine Ebene ist gegeben durch $\mathbf{E} : ax + by + cz = d$.
Behauptung: $\mathbf{E} < \mathbb{R}^3 \Leftrightarrow d = 0$
Beweis:
"$\Leftarrow$": Gegeben: $ax + by + cz = 0$.
Zu Zeigen: $(i) - (iii)$ gelten.
Zu (i): $(0, 0, 0) \in \mathbf{E}$ (klar)
Zu (ii): Addition ist abgeschlossen:
Sei $ax + by + cz = 0$ und $ax' + by' + cz' = 0 \Leftrightarrow (x, y, z) + (x', y', z') \in \mathbf{E}$.
Addition der Gleichungen liefert:

$$ax + by + cz + ax' + by' + cz' = a \cdot (x + x') + b \cdot (y + y') + c \cdot (z + z')$$

Also: $(x, y, z) + (x', y', z') \in \mathbf{E}$.
Zu (iii): Multiplikation mit einem Skalar ist abgeschlossen:
Sei $ax + by + cz = 0$ und $\alpha \in \mathbb{R} \Leftrightarrow \alpha \cdot (x, y, z) \in \mathbf{E}$. Nun gilt:

$$0 = \alpha \cdot (ax + by + cz) = \alpha \cdot ax + \alpha \cdot by + \alpha \cdot cz = a \cdot (\alpha x) + a \cdot (by) + a \cdot (cz) \quad \Rightarrow \quad \alpha \cdot (x, y, z) \in \mathbf{E}$$

(b): Wir befinden uns im $\mathbb{R}^3$. Wir betrachten folgende Konstruktion:

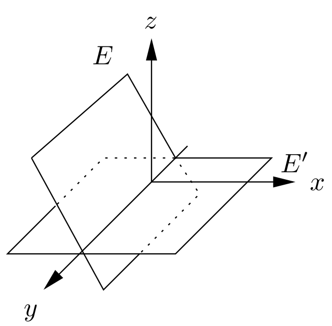

Abbildung II-12: Zwei Ebenen im $\mathbb{R}^3$

$E \cap E'$ ist eine Gerade durch den Ursprung.
(c): Weitere Konstruktionen für Untervektorräume sind: $\mathbf{U}_1 \cap \mathbf{U}_2$, $\mathbf{U}_1 + \mathbf{U}_2$, $\mathbf{U}_1 \times \mathbf{U}_2$.

(d): Welche Geraden sind Untervektorräume im $\mathbb{R}^3$?
Eine Gerade g im $\mathbb{R}^3$ sei gegeben durch:

$$\begin{aligned} ax + by + cz &= d \\ a'x + b'y + c'z &= d' \end{aligned}$$

Behauptung: $g < \mathbb{R}^3 \Leftrightarrow d = d' = 0$.
(e): Seien $\mathbf{U}_1 = \mathbb{R}v_1$ und $\mathbf{U}_2 = \mathbb{R}v_2$.
Nun gilt:

$$\mathbf{U}_1 + \mathbf{U}_2 = \{u_1 + u_2 : u_1 \in \mathbf{U}_1, u_2 \in \mathbf{U}_2\}$$

Hier in diesem Fall gilt: $\mathbf{U}_1 + \mathbf{U}_2 = \{\alpha v_1 + \beta v_2 : \alpha, \beta \in \mathbb{R}\} = E_{0;v_1,v_2}$
Wir spannen also eine Ebene durch den Nullpunkt mit den Richtungsvektoren v_1 und v_2 auf:

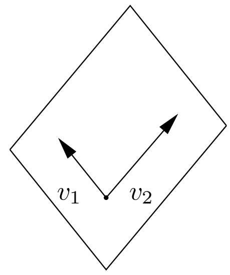

Abbildung II-13: Ebene durch den Nullpunkt mit Richtungsvektoren v_1 und v_2

(f) $\mathbb{R} \times \mathbb{R}^2 = \{(x, (y, z)) : x, y, z \in \mathbb{R}\} \overset{(*)}{=} \{(x, y, z) : x, y, z \in \mathbb{R}\} = \mathbb{R}^3$
Anmerkung zu $(*)$: Strenggenommen sind die beiden Terme nicht gleich, sie sind aber so zu identifizieren.
$\mathbf{U} = \mathbb{R} < \mathbb{R}$ **und** $\mathbf{V} = ((a, 0) : a \in \mathbb{R}) < \mathbb{R}^2$. **Genauer:** $\mathbf{V} = \{a \cdot (1, 0) : a \in \mathbb{R}\} = \mathbb{R}\,(1, 0)$.

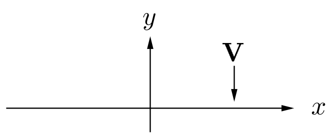

Abbildung II-14: $\mathbf{V}$ in der Ebene

$\mathbf{U} \times \mathbf{V} = \{(x, y, 0) : x, y \in \mathbb{R}\} = xy$**-Ebene im** $\mathbb{R}^3$.

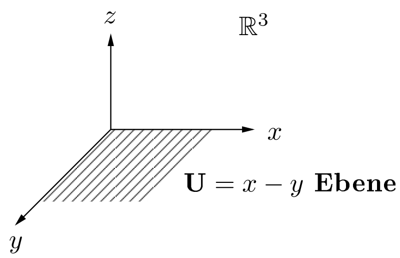

Abbildung II-15: $\mathbf{U} \times \mathbf{V}$ in der Ebene

2.3.10 Erzeugung von Untervektorräumen

Nun wollen wir für einen endlichen Vektorraum alle Unterräume bestimmen:
Sei

$$\begin{aligned}\mathbf{V} = (\mathbb{Z}/_{2\mathbb{Z}})^2 &= \{(x,y) : x,y \in \mathbb{Z}/_{2\mathbb{Z}}\} \\ &= \left\{\left(\overline{0},\overline{0}\right), \left(\overline{0},\overline{1}\right), \left(\overline{1},\overline{0}\right), \left(\overline{1},\overline{1}\right)\right\}\end{aligned}$$

Die trivialen Fälle für die Untervektorräume sind: $\left(\overline{0},\overline{0}\right)$ **und V.**
Gibt es weitere Untervektorräume?
Jeder weitere Untervektorraum von V muß mindestens das Element $\left(\overline{0},\overline{0}\right)$ **enthalten.**
Also raten wir:
Behauptung: $\mathbf{U} = \left\{\left(\overline{0},\overline{0}\right), \left(\overline{0},\overline{1}\right)\right\}$ **seien ein Untervektorraum. Nun müssen wir die Eigenschaften** $(i) - (iii)$ **überprüfen:**
Zu (i): $\left\{\left(\overline{0},\overline{0}\right), \left(\overline{0},\overline{1}\right)\right\} \neq \phi$ **(klar)**
Zu (ii): Abgeschlossenheit bezüglich der Addition. Es treten drei Fälle auf:

$$\begin{aligned}\left(\overline{0},\overline{0}\right) + \left(\overline{0},\overline{0}\right) &= \left(\overline{0},\overline{0}\right) \in \mathbf{U} \\ \left(\overline{0},\overline{0}\right) + \left(\overline{0},\overline{1}\right) &= \left(\overline{0},\overline{1}\right) \in \mathbf{U} \\ \left(\overline{0},\overline{1}\right) + \left(\overline{0},\overline{1}\right) &= \left(\overline{0},\overline{0}\right) \in \mathbf{U}\end{aligned}$$

Die Addition ist also abgeschlossen.
Zu (iii) Abgeschlossenheit bezüglich der skalaren Multiplikation. Es treten vier Fälle auf:

$$\begin{aligned}0 \cdot \left(\overline{0},\overline{0}\right) &= \left(\overline{0},\overline{0}\right) \in \mathbf{U} \qquad & 0 \cdot \left(\overline{0},\overline{1}\right) &= \left(\overline{0},\overline{0}\right) \in \mathbf{U} \\ 1 \cdot \left(\overline{0},\overline{0}\right) &= \left(\overline{0},\overline{0}\right) \in \mathbf{U} & 1 \cdot \left(\overline{0},\overline{1}\right) &= \left(\overline{0},\overline{1}\right) \in \mathbf{U}\end{aligned}$$

Auch bezüglich der skalaren Multiplikation ist U abgeschlossen.
Es folgt: $\mathbf{U} = \left\{\left(\overline{0},\overline{0}\right), \left(\overline{0},\overline{1}\right)\right\} < \mathbf{V}$.
Analog zeigen wir, daß $\mathbf{U} = \left\{\left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{0}\right)\right\} < \mathbf{V}$ **und** $\mathbf{U} = \left\{\left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{1}\right)\right\} < \mathbf{V}$.
Gibt es nun auch Untervektorräume in V, die nun mindestens drei Elemente haben?:
Sei $\mathbf{U} < \mathbf{V}$ **und** $|\mathbf{U}| \geq 3$. **Es gilt:** $\left(\overline{0},\overline{0}\right) \in \mathbf{U}$ **(Ansonsten ist es garantiert kein Untervektorraum). Nun treten drei Fälle auf:**
1. Fall: $\left(\overline{0},\overline{1}\right), \left(\overline{1},\overline{0}\right) \in \mathbf{U} \quad \Rightarrow$ **Auch** $\left(\overline{1},\overline{1}\right) \in \mathbf{U}$ **(sonst nicht abgeschlossen)** $\Rightarrow \mathbf{U} = \mathbf{V}$.
2. Fall: $\left(\overline{0},\overline{1}\right), \left(\overline{1},\overline{1}\right) \in \mathbf{U} \quad \Rightarrow$ **Auch** $\left(\overline{1},\overline{0}\right) \in \mathbf{U}$ **(sonst nicht abgeschlossen)** $\Rightarrow \mathbf{U} = \mathbf{V}$.
3. Fall: $\left(\overline{1},\overline{0}\right), \left(\overline{1},\overline{1}\right) \in \mathbf{U} \quad \Rightarrow$ **Auch** $\left(\overline{0},\overline{1}\right) \in \mathbf{U}$ **(sonst nicht abgeschlossen)** $\Rightarrow \mathbf{U} = \mathbf{V}$.
Damit haben wir eine Liste aller Untervektorräume von V gefunden:

$$\left(\overline{0},\overline{0}\right), \mathbf{V}, \left\{\left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{0}\right)\right\}, \left\{\left(\overline{0},\overline{0}\right), \left(\overline{0},\overline{1}\right)\right\}, \left\{\left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{1}\right)\right\}$$

Diesen Vektorraum können wir auch graphisch darstellen:

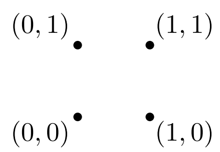

Abbildung II-16: graphische Darstellung von **V**

Für die graphische Darstellung der Untervektorräume von V gilt nun:

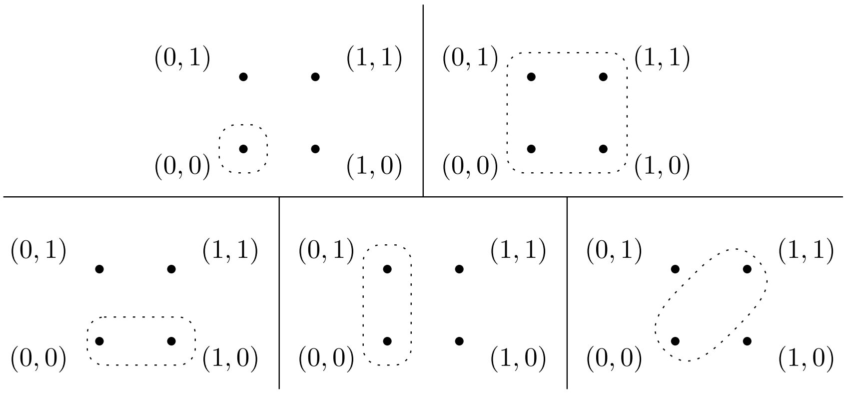

Abbildung II-17: graphische Darstellung der Untervektorräume

Gegeben: $v_1, \ldots, v_k \in \mathbf{V}$. **Suche alle Untervektorräume** $\mathbf{U} \ni v_1, \ldots, v_k$.
Es ergeben sich folgende notwendigen Bedingungen:
Aus (iii): $\forall \alpha_1, \ldots, \alpha_k \in \mathbb{K}: \ \alpha_1 v_1, \ldots, \alpha_k v_k \in \mathbf{U}$
Aus (ii): $\forall \alpha_1, \ldots, \alpha_k \in \mathbb{K}: \ \alpha_1 v_1 + \ldots + \alpha_k v_k \in \mathbf{U}$
Also: $\Rightarrow \quad \mathbf{U} \supseteq \left\{ \textbf{alle Linearkombinationen } \sum_{i=1}^{k} \alpha_i v_i \right\}$

2.3.11 Satz (II.3.4)

Gegeben seien $v_1, \ldots, v_k \in \mathbf{V}$. **Dann ist** $\left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in \mathbb{K},\, i = 1, \ldots, k \right\}$ **der kleinste Untervektorraum von V, der die Vektoren** $v_1, \ldots, v_k$ **enthält.**
Beweis:
Nach der Vorüberlegung genügt es zu zeigen, daß $\left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in \mathbb{K},\, i = 1, \ldots, k \right\} < \mathbf{V}$

Nun sei: $\mathbf{U} := \left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in \mathbb{K},\, i = 1, \ldots, k \right\}$
Wir müssen die Eigenschaften $(i) - (iii)$ **überprüfen:**
Zu (i): $\mathbf{U} \neq \phi$, **denn** $v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_k \in \mathbf{U}$
Zu (ii): Abgeschlossenheit bezüglich der Addition:

$$\sum_{i=1}^{k} \alpha_i v_i + \sum_{i=1}^{k} \beta_i v_i = \sum_{i=1}^{k} (\alpha_i v_i + \beta_i v_i) = \sum_{i=1}^{k} (\alpha_i + \beta_i) \cdot v_i \in \mathbf{U}$$

Zu (iii): Abgeschlossenheit bezüglich der skalaren Multiplikation:

$$\alpha \cdot \sum_{i=1}^{k} \alpha_i v_i = \sum_{i=1}^{k} \alpha \cdot (\alpha_i v_i) = \sum_{i=1}^{k} (\alpha \cdot \alpha_i) \cdot v_i \in \mathbf{U}$$

Da alle Eigenschaften erfüllt sind ist U < V. Die anderen Axiome sind schon in V erfüllt und übertragen sich damit auf U.

2.3.12 Definition (II.3.c): Spann und Erzeugendensystem

(i) $\langle v_1, \ldots, v_k\rangle$ **wir definiert als** $\langle v_1, \ldots, v_l\rangle := \left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_1 \ldots \alpha_k \in \mathbf{K} \right\}$
$\langle v_1, \ldots, v_k\rangle$ **ist der von** $v_1, \ldots, v_k$ **erzeugte oder aufgespannte Vektorraum oder Span** $(v_1, \ldots, v_k)$**.**

(ii) Ist $\mathbf{U} = \langle v_1, \ldots, v_k\rangle$**: U wird von** $v_1, \ldots, v_k$ **erzeugt oder aufgespannt.** $v_1, \ldots, v_k$ **wird als Erzeugendensystem von U bezeichnet.**

2.3.13 Beispiele für Spann

Gerade im $\mathbb{R}^2$**:** $g_{P,v} = P + \mathbb{R} \cdot v = P + \langle v\rangle$**.**
Ebene im $\mathbb{R}^3$**:** $E_{P,v_1,v_2} = P + \mathbb{R}v_1 + \mathbb{R}v_2 = P + \langle v_1, v_2\rangle$**.**
Man nennt ein solches System: Affiner Unterraum des $\mathbb{K}^n$**:** $P + \langle v_1, \ldots, v_k\rangle$**.**
Nun ist es oft gefordert für einen Untervektorraum ein Erzeugendensystem zu finden.
Hier nun eine Beispiel:
Gegeben sei $\mathbb{K}$ **und** $\mathbf{U} = \{(x_1, \ldots, x_n) \in \mathbb{K}^n : a_1x_1 + \ldots + a_nx_n = 0\} < \mathbb{K}^n$**.**
1. Fall $a_i = 0, i = 1, \ldots, n \quad \Rightarrow \quad \mathbf{U} = \mathbb{K}^n = \langle e_1, \ldots, e_n\rangle$ **mit** $e_i = (0, \ldots, 1, \ldots, 0)$ **wobei die** 1 **an der** i**-ten Stelle steht un** $(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i e_i$
2. Fall: ein $a_i \neq 0$**, etwa** $a_1 \neq 0$**. Nun gilt:**

$$\begin{aligned} a_1x_1 + \ldots + a_nx_n = 0 \quad &\Leftrightarrow \quad x_1 = -\frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n \\ &\Leftrightarrow \quad (x_1, \ldots, x_n) = \left(-\frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n, x_2, \ldots, x_n\right) \end{aligned}$$

Nun gilt:

$$\begin{aligned} (x_1, \ldots, x_n) &= \left(-\frac{a_2}{a_1}x_2 - \ldots - \frac{a_n}{a_1}x_n, x_2, \ldots, x_n\right) \\ &= x_2 \cdot \left(-\frac{a_2}{a_1}x_2, 1, 0, \ldots, 0\right) + x_3 \cdot \left(-\frac{a_3}{a_1}x_3, 0, 1, 0, \ldots, 0\right) \\ &\quad + x_i \cdot \left(-\frac{a_i}{a_1}x_i, \ldots, 1, \ldots, 0\right) + x_n \cdot \left(-\frac{a_n}{a_1}x_n, 0, \ldots, 1\right) \end{aligned}$$

Damit: $x \in \mathbf{U} \Leftrightarrow$

$$\exists x_2, \ldots, x_n \in \mathbb{K} : x = x_2 \cdot \left(-\frac{a_2}{a_1}, 1, 0, \ldots, 0\right) + \ldots + x_i \cdot \left(-\frac{a_i}{a_1}x_i, \ldots, 1, \ldots, 0\right) + x_n \cdot \left(-\frac{a_n}{a_1}x_n, 0, \ldots, 1\right)$$

Also: $\mathbf{U} = \left\langle \ldots, \left(-\frac{a_i}{a_i}, 0, \ldots, 1, \ldots, 0\right), \ldots \right\rangle$ **für** $i = 2, \ldots, n$ **sind Lösungen, denn**

$$a_1 \cdot \left(-\frac{a_i}{a_1}\right) + 1 \cdot a_i = 0$$

2.4 Kapitel (II.4): Basis und Dimension

2.4.1 Ziel dieses Paragraphen: Haupsatz für Basen

Der Hauptsatz für Basen lautet:

(i) **Jeder endlich erzeugte Vektorraum hat eine Basis.**
Das heißt: jeder endlich erzeugte Vektorraum besitzt ein linear unabhängiges Erzeugendensystem.

(ii) **Je zwei Basen haben dieselbe Länge (Anzahl der Vektoren)**

2.4.2 Definition (II.4.a): Lineare Unabhängigkeit von Vektoren

$v_1, \ldots, v_n$ **heißen linear unabhängig, wenn gilt:**

$$\forall \alpha_1, \ldots, \alpha_k \in \mathbb{K} : \sum_{i=1}^{k} \alpha_i v_i = 0 \quad \Rightarrow \quad \alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$$

2.4.3 Definition (II.4.b): Basis

$v_1, \ldots, v_k$ **heißen eine Basis von V** $\quad :\Leftrightarrow \quad \mathbf{V} = \langle v_1, \ldots, v_k \rangle = \left\{ \sum_{i=1}^{k} \alpha_i v_i \,\middle|\, : \alpha_i \in \mathbb{K} \right\}$.
Dabei sind $v_1, \ldots, v_k$ **linear unabhängig.**

2.4.4 Beispiele für Basen

(a) $\mathbb{K}^n$ **hat die Standardbasis** $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ **mit** $\mathbf{e}_i$ **als dem** i**-ten Einheitsvektor. Der** i**-te Einheitsvektor hat als** i**-te Komponente eine Eins und ansonsten Nullen:** $(0, \ldots, 1, \ldots, 0)$.
Ein Vektor x **läßt sich dann darstellen als** $x = (x_1, \ldots, x_n) = x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n$.
(b) $\mathbb{R}^2$ **hat die Basen** $\{\mathbf{e}_1, \mathbf{e}_2\}$ **und** $\{(1,1), (7000163, -14201660)\}$.
Zu zeigen: $\forall a, b$: $(a, b) = \alpha \cdot (1,1) + \beta \cdot (7000163, -14201660)$. **Wir müssen also folgendes Gleichungssystem lösen:**

$$\begin{aligned} a &= \alpha \cdot 1 + \beta \cdot 7000163 \\ b &= \alpha \cdot 1 + \beta \cdot (-14201660) \end{aligned}$$

(c) Sei $\mathbf{U} = \left\{ x | \sum_{i=1}^{n} a_i x_i = 0 \right\}$ **mit** $a_1 \neq 0$. $\mathbf{U} = \langle u_2, \ldots, u_n \rangle$**, also** $u_2, \ldots, u_n$ **sind ein Erzeugendensystem von U.**
Behauptung: $u_2, \ldots, u_n$ **sind linear unabhängig.**
Beweis: Sei $\alpha_2 u_2 + \ldots + \alpha_n u_n = 0$.
Wegen der Gestalt von u_i **folgt:** $\sum_{i=1}^{n} \alpha_i u_i = (*, \alpha_2, \ldots, \alpha_n)$ **wobei** $*$ **irgendeinen Produkt ist. Also:**

$$\sum_{i=1}^{n} \alpha_i u_i = 0 \quad \Rightarrow \quad \alpha_2 = \alpha_3 = \ldots = \alpha_n = 0$$

2.4.5 Basen und Dimensionen

Familie von Vektoren : $(v_i)_{i\in I}$, wobei I eine (Index)menge ist: $I \to \mathbf{V}, i \mapsto v_i$. Nicht notwendigerweise: $v_i \neq v_j$ für $i \neq j$. $v_1, \ldots, v_n$ sind eine endliche Familie, das heißt $\{1, \ldots, n\} \to \mathbf{V}$, $i \mapsto v_i$.

Notation $\langle E\rangle$: Bisher $\langle v_1, \ldots, v_n\rangle$. Auf Übungsblatt 9 zu zeigen: $\langle E\rangle \subseteq \mathbf{V}$. Allgemeinste Verwendung: $E = (v_i)_{i\in I}$ Familie von Vektoren. $\langle E\rangle =$ der kleinste Untervektorraum von V, der alle $v_i, i \in I$ enthält.

Existenz: In der Vorlesung: Existenz von endlichen Familien gezeigt. Auf Übungsblatt 9: Für beliebige Familien:

$$\langle E\rangle = \left\{ \sum_{j\in J} \lambda_j v_j \,\middle|\, J \subseteq I, J \text{ endlich}, \lambda_j \in \mathbb{K} \right\}$$

Basis von V: Familien von Vektoren mit

(i) $v_1, \ldots, v_n$ **sind linear unabhängig**

(ii) $\langle v_i, \ldots, v_n\rangle = \mathbf{V}$

Bemerkung: Aus (i) folgt: $r \neq s \quad \Rightarrow \quad v_r \neq v_s$
Beweis: Sei $v_r = v_s$ mit $r \lneqq s$.
Also existiert eine nicht triviale Darstellung der Null:

$$0 = 0 \cdot v_1 + \ldots + 0 \cdot v_{r-1} + 1 \cdot v_r + 0 \cdot v_{r+1} + \ldots + 0 \cdot v_{s-1} + (-1) \cdot v_s + 0 \cdot v_{s+1} + \ldots + 0 \cdot v_n$$

Wir erhalten einen Widerspruch zur linearen Unabhängigkeit.
Nun noch eine Notation der Linearkombination: $\sum \lambda_j v_j$:

$$0 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3 + 0 \cdot v_4 = \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3$$

Beide Terme sind eine Linearkombination von $v_1, \ldots, v_4$, wobei alle Faktoren mit $\lambda_j = 0$ auf der rechten Seite weggelassen worden sind.
Lineare Unabhängigkeit:
$v_1, \ldots, v_n$ sind linear unabhängig $\quad \Leftrightarrow \quad \forall i = 1 \ldots n : v_i \notin \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\rangle$.
Für $n = 2$: v_1, v_2 sind linear unabhängig $\quad \Leftrightarrow \quad v_1 \notin \mathbb{K}v_2$ und $v_2 \notin \mathbb{K}v_1$.
Anmerkung zur Notation: Um Schreibarbeit zu sparen sind äquivalent:

$$\langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\rangle \doteqdot \langle v_1, \ldots, v_{i-1}, \hat{v}_i, v_{i+1}, \ldots, v_n\rangle$$

Der Vektor, der nicht Element des Erzeugendensystems ist wird mit einem Dach bezeichnet.
Beweis: Angenommen $v_i \in \langle v_1, \ldots, v_{i-1}, \hat{v}_i, v_{i+1}, \ldots, v_n\rangle$.
"$\Rightarrow$": Zu zeigen

$$\begin{array}{rrcl} & v_i & = & \lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \ldots + v_n \lambda_n \\ \Rightarrow & 0 & = & \lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + (-1) \cdot v_i + \lambda_{i+1} v_{i+1} + \ldots + v_n \lambda_n \end{array}$$

Also muß mindestens ein $\lambda_j \neq 0$ für $j \neq i$. Dies ist eine Widerspruch zur Voraussetzung, daß die Vektoren linearen Unabhängigkeit sind.
"$\Leftarrow$": Sei $\sum_{i=1}^{n} \lambda_i v_i = 0$ wobei ein $\lambda_i \neq 0$. OE: $\lambda_1 \neq 0$ (Ansonsten sortieren wir um). Dann

$$\lambda_1 v_1 + \sum_{i=2}^{n} \lambda_i v_i = 0 \quad \Rightarrow \quad v_1 = \sum_{i=2}^{n} \left(-\frac{\lambda_i}{\lambda_1}\right) v_i$$

Also $v_1 \in \langle v_2, \ldots, v_n\rangle$

2.4.6 Hauptsatz (II.4.1)

Sei V ein endlich erzeugter $\mathbb{K}$-Vektorraum. Dann gelten:

(1) V besitzt eine Basis

(2) Je zwei Basen haben dieselbe Länge (Sprich: dieselbe Anzahl von Vektoren)

Beweis: Voraussetzung: V $= \langle v_1, \ldots, v_n \rangle$. **Konstruktion einer Basis aus** $v_1, \ldots, v_n$.
Erste Konstruktion: (Idee: behalte Erzeugenden-Eigenschaften):
Nun unterscheiden wir zwei Fälle:
1. Fall: $v_1, \ldots, v_n$ **sind linear unabhängig: Fertig, da wir Basis damit haben.**
2. Fall: $v_1, \ldots, v_n$ **sind linear abhängig. Das heißt** $0 = \sum \lambda_i v_i$ **wobei nicht alle** $\lambda_i \neq 0$.
Dann $v_1 \in \langle v_2, \ldots, v_n \rangle \quad \Rightarrow \quad v_1, \ldots, v_n \in \langle v_2, \ldots, v_n \rangle$.
$\langle w_1, \ldots, w_k \rangle$ **ist der kleinste Unterraum** $\ni w_1, \ldots, w_k$
$\Rightarrow \quad \mathbf{V} = \langle v_1, \ldots, v_n \rangle \subseteq \langle v_2, \ldots, v_n \rangle \subseteq \mathbf{V} \quad \Rightarrow \quad \mathbf{V} = \langle v_2, \ldots, v_n \rangle$
Iteration liefert ein Teilsystem $v_{i_1}, \ldots, v_{i_r}$ **von** $v_1, \ldots, v_n$ **mit den Eigenschaften:**

- $\mathbf{V} = \langle v_{i_1}, \ldots, v_{i_r} \rangle$
- $v_{i_r}, \ldots, v_{i_r}$ **sind linear unabhängig, das heißt Basis**

Achtung: $r = 0$ **kann auftreten. Das heißt V** $= \{0\}$.

2.4.7 Satz (II.4.1.a): Basisauswahlsatz

In jedem Erzeugendensystem ist eine Basis erhalten, die man durch sukzessive Elimination von Vektoren erhalten kann. Eliminiert wird mittels einer nicht trivialen Darstellung der Null. (siehe oben: Fall (2)**)**
Zweite Konstruktion: (Idee: behalte Eigenschaft der linearen Unabhängigkeit)
Sei $B_0 \subseteq \{v_1, \ldots, v_n\}$ **eine linear unabhängige Teilfamilie. Eventuell kann sein:** $B_o = \phi$.
Es gibt maximale Teilfamilie B **von** $v_1, \ldots, v_n$ **mit:**

(i) B **ist linear unabhängig**

(ii) $B_0 \subseteq B$

Beweis:
Zu (i)**: lineare Unabhängigkeit: klar, da nach Voraussetzung** B_0 **linear unabhängig.**
Zu (ii)**:** $\langle B \rangle = \mathbf{V}$.
Zu zeigen: $v_1, \ldots, v_n \in \langle B \rangle$: $\quad \Rightarrow \quad \mathbf{V} = \langle v_1, \ldots, v_n \rangle \subseteq \langle B \rangle \subseteq \mathbf{V} \quad \Rightarrow \quad \langle B \rangle = \mathbf{V}$
Nun betrachten wir v_i. **Wir unterscheiden zwei Fälle:**
1. Fall: $v_i \in B \quad \Rightarrow \quad v_i \in \langle B \rangle$
2. Fall: $v_i \notin B$, **dann ist** $B \cup \{v_i\}$ **eine echte größere Teilfamilie von** $v_1, \ldots, v_n$. **Nach Wahl von** B **ist** $B \cup \{v_i\}$ **linear abhängig, das heißt es gilt :** $0 = \sum_{v \in B} \lambda_v v + \mu v_i$ **wobei nicht alle Koeffizienten gleich Null sind.**
Angenommen: $\mu = 0$, **dann** $0 = \sum_{v \in B} \lambda_v v$. **Nun folgt aus den Eigenschaften von** B **und der linearen Unabhängigkeit:** $\lambda_v = 0$, **daß heißt: alle Koeffizienten sind gleich Null. Dies ist eine Widerspruch zu unserer Annahme. Also: für** $\mu = 0 \quad \Rightarrow \quad v_i \in \langle B \rangle$

2.4.8 Satz (II.4.1.b): Basisergänzungssatz

Hier zwei Fassungen des Basisergänzungssatz:

(i) Ist B_0 eine linear unabhängige Familie, E ein endliches Erzeugendensystem von $\mathbf{V}, B_0 \subseteq E$, dann läßt sich B_0 innerhalb von E zu einer Basis ergänzen.

(ii) Sei V ein endlich erzeugter $\mathbb{K}$-Vektorraum und B_0 eine linear unabhängige Familie, dann läßt sich B_o zu einer Basis von V ergänzen.

Beweis: $(i) \quad \Rightarrow \quad (ii)$**:**
Sei $\mathbf{V} = \langle v_1, \ldots, v_n \rangle$ **nach Voraussetzung, wähle Familie** B_0**,** $v_1, \ldots, v_n =: E$**.**
Dann offenbar: $B_0 \subseteq E, \langle E \rangle = \mathbf{V}$**.**
Hier eine Beispiel im $\mathbb{R}^4$**:**
Behauptung: $(1,2,0,4), (3,0,4,6), (0,117,2133,-6), (0,0,1,4), (6,7,8,0), (1,2,3,4)$ **erzeugen** $\mathbb{R}^4$**.**
Die lineare Abhängigkeit sagt aus:

$$\begin{aligned} \lambda_1 + 3\lambda_2 + 0\lambda_3 + 0\lambda_4 + 6\lambda_5 + \lambda_6 &= 0 \\ \vdots \quad &\quad \vdots \\ 4\lambda_1 + 6\lambda_2 + -6\lambda_3 + 4\lambda_4 + 0\lambda_5 + 4\lambda_6 &= 0 \end{aligned}$$

Wir erhalten als ein Gleichungssystem mit 4 **Gleichungen und** 6 **Unbekannten.**
Nachrechnen liefert, daß wir die Vektoren $(0,0,1,4)$ **und** $(1,2,3,4)$ **eliminieren können. Die anderen** 4 **Vektoren ergeben eine Basis.**
Konstruktion eines Erzeugendensystem für $\mathbb{R}^4$ **nach Satz (II.4.1.b):**
Gegeben seien die linear unabhängigen Vektoren $(1,704,603,502)$ **und** $(2,401,300,199)$**.**
Auf jeden Fall: Die vier Einheitsvektoren $(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$ **sind ein Erzeugendensystem für den** $\mathbb{R}^4$**.**
Nachrechnen liefert:
$(1,704,603,502), (2,401,300,199), (1,0,0,0), (0,1,0,0)$ **ist eine Basis im** $\mathbb{R}^4$ **.**
Für den Beweis des Satzes (II.4.1.b) brauchen wir den Austauschsatz von Steinitz:

2.4.9 Satz (II.4.1.c): Austauschsatz von Steinitz

Sei B eine linear unabhängige Familie von Vektoren in V.
Dann gibt es zu jedem $v \in B$ ein $w \in E$, so daß $(B \setminus \{v\}) \cup \{w\}$ wieder linear unabhängig ist.
Beweis: Wähle $v \in B$, weil $\langle E \rangle = \mathbf{V}$ gilt:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

Zu zeigen: Es gibt ein i: $(B \setminus \{v\}) \cup \{v_i\}$ ist linear unabhängig.
Beweis durch Widerspruch: Angenommen $\forall i$: $(B \setminus \{v\}) \cup \{v_i\}$ ist linear abhängig, daraus folgt analog zum Beweis der 2. Konstruktion: $v_i \in \langle B \setminus \{v\} \rangle$, $\forall i$. Daraus:

$$v = \sum \lambda_i v_i \in \langle B \setminus \{v\} \rangle \quad \textbf{und} \quad v = \sum_{\substack{w \neq v \\ w \in B}} \lambda_w \cdot w$$

Dies ist ein Widerspruch zur Annahme der linearen Unabhängigkeit.
Folgerung: B_1, B_2 sind Basen von V $\quad \Rightarrow \quad |B_1| = |B_2|$.
Beweisschema: Zunächst: $|B_1| \leq |B_2|$. Dito: $|B_2| \leq |B_1| \quad \Rightarrow \quad |B_1| = |B_2|$.
Sei $B_1 := \{v_1, \ldots, v_r\}$, $B_1 := \{w_1, \ldots, w_s\}$.
Nun wenden wir den Austauschsatz mehrfach an.
B_1 ist linear unabhängig, B_2 sei ein Erzeugendensystem.
Nun ersetze v_1 durch einen passenden Vektor w_i. OE: $i = 1$, ansonsten sortieren wir um.
Dann: $B_1 = \{w_1, v_2, \ldots, v_r\}$ ist linear unabhängig und B_2 ist eine Erzeugendensystem.
Nun v_2 ersetzen durch w_i. $i = 1$ ist unmöglich, da ansonsten $w_1, w_1, v_3, \ldots, v_r$ linear abhängig sind.
Also $i \geq 2$. OE: $i = 2$, dann $B_1 = \{w_1, w_2, v_3, \ldots, v_r\}$ ist linear unabhängig und B_2 ist ein Erzeugendensystem.
Sukzessive werden $v_1, \ldots, v_r$ durch r verschiedene Vektoren aus B_2 ersetzt, daher $r \leq s$.
Dito: $s \leq r$. Also $r = s$.
Als Konsequenz aus den drei Sätzen ergibt sich (schon gezeigt):

- **Existenz einer Basis**
- **Gleichmächtigkeit von Basen**

2.4.10 Definition (II.4.c): dim(V)

Sei V endlich erzeugter Vektorraum. Die Dimension von V: $\dim(\mathbf{V}) := |B|$, wobei B Basis von V ist.

2.4.11 Konsequenzen aus $\dim(\mathbf{V}) := |B|$

Als Konsequenzen ergeben sich:

(i) $\dim(\mathbf{V}) = n$, **wobei** $v_1, \ldots, v_n$ **linear unabhängig** $\Rightarrow$ $v_1, \ldots, v_n$ **bilden eine Basis**

(ii) Basen = minimale Erzeugendensysteme

(iii) Basen = maximal unabhängige Familien

Stichworte zu den Beweisen:

Zu (i)**:** $v_1, \ldots, v_n$ **sind linear unabhängig. Nach dem Basisergänzungssatz folgt, daß** $v_1, \ldots, v_n$ **zu einer Basis ergänzt werden kann. Nach dem Austauschsatz folgt unmittelbar, daß** $v_1, \ldots, v_n$ **eine Basis sind, also eine Ergänzung nicht notwendig sind.**

Zu (ii)**: B sei eine Basis. Aus der Definition der Basis folgt: B ist Erzeugendensystem. Sei** $\mathbf{B}_0 \subseteq \mathbf{B}$ **und** $\mathbf{B}_0$ **Erzeugendensystem.**

Zu zeigen: $\mathbf{B}_0 = \mathbf{B}$**.**

Sei $\mathbf{B}_0 \subseteq \mathbf{B}$**. Es existiert ohne Einschränkung** $v_1 \in \mathbf{B} \setminus \mathbf{B}_0$

$$v_1 = \lambda_2 v_2 + \ldots + \lambda_r v_r \quad \textbf{mit} \quad v_2, \ldots, v_r \in \mathbf{B}_0$$

Daher sind $v_1, \ldots, v_r$ **linear abhängig. Dies ist eine Widerspruch zur Eigenschaft der Basis.**

Es folgt, daß B ein minimales Erzeugendensystem ist.

Bisher haben wir bewiesen: B ist minimales Erzeugendensystem.

Es bleibt zu zeigen: Ein minimales Erzeugendensystem ist Basis.

Sei E ein Erzeugendensystem, dann existiert $\mathbf{B} \subseteq \mathbf{E}$**, B sei Basis (nach Basisauswahlsatz). B ist Erzeugendensystem, E war minimal** $\Rightarrow$ $\mathbf{B} = \mathbf{E}$**. Also ist E Basis.**

Zu (iii)**: Analog zu** (ii)

2.4.12 Anwendung:

(i) $\dim(\mathbb{K}^n) = n$, $B := \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ **Basis von** n**-Vektoren (Standardbasis).** $v_1, \ldots, v_n$ **seien linear unabhängig** $\Rightarrow$ $v_1, \ldots, v_n$ **ist Basis von** $\mathbb{K}^n$ **(mittels Basisergänzungssatz, Standardbasis, Satz (II.4.1.b))**

(ii) lineares Gleichungssysteme $\sum_{j=1}^{n} a_{ij} x_j = 0$ **für** $i = 1, \ldots, n$
Lösungsmenge ist Untervektorraum des $\mathbb{K}^n = \mathbb{L}$**. Später:** $\mathbb{L}$ **Basis von** $v_1, \ldots, v_r$ **mit** $r \leq n$**:**

$$\mathbb{L} = \left\{ \sum_{i=1}^{r} \lambda_i v_i : \lambda_i \in \mathbb{K} \right\}$$

2.4.13 Darstellung durch Basen

$v_1, \ldots v_n$ **sei eine Basis,** $v \in \mathbf{V}$**. Nun läßt sich** v **als Linearkombination darstellen:**

$$v = \sum_{i=1}^{n} \lambda_i v_i \quad \textbf{für gewisse } \lambda_1, \ldots, \lambda_n \in \mathbb{K}$$

2.4.14 Satz (II.4.2)

Die Darstellung von Vektoren bezüglich einer Basis ist eindeutig.

Beweis: Sei v dargestellt durch: $v = \sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \mu_i v_i$

Zu zeigen $\lambda_i = \mu_i \ \forall i$.
Sei ein $\lambda_{i_0} \neq \mu_{i_0}$. Nun gilt:

$$\sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \mu_i v_i \quad \Leftrightarrow \quad \sum_{i=1}^{n} \lambda_i v_i - \sum_{i=1}^{n} \mu_i v_i = 0 \quad \Leftrightarrow \quad \sum_{i=1}^{n} (\lambda_i - \mu_i) \cdot v_i = 0$$

Für einen Koeffizienten, $i = i_0$, ist die Summe der λ, μ nicht Null. Damit erhalten wir einen Widerspruch zur linearen Abhängigkeit.
Hier nun ein anschauliches Beispiel für den $\mathbb{R}^3$:
Sei v gegeben durch: $v = v_1 + 2v_2 - 3v_3$ **und** $v = v_1 + 2,1 \cdot v_2 - 4v_3$
Subtrahieren wir die beiden Gleichungen, so erhalten wir:

$$0 \quad = \quad 0,1 \cdot v_2 + (-1) \cdot v_3$$

Damit erhalten wir einen Widerspruch zur linearen Unabhängigkeit.
Formale Konsequenz: Gegeben sei ein $\mathbb{K}$-Vektorraum mit den Basis $v_1, \ldots, v_n$. Dann ist ein Vektor durch genau einen $n-$Tupel eindeutig darstellbar:$v = \sum_{i=1}^{n} \lambda_i v_i$

2.4.15 Bemerkungen zu nicht endlich erzeugten Vektorräumen

1. Existieren Sie? Ja!
$\mathbb{R}$ ist ein $\mathbb{Q}$-Vektorraum:

- $(\mathbb{R}, +)$ **ist abelsche Gruppe**
- $\mathbb{Q} \times \mathbb{R} \to \mathbb{R} : (\alpha, v) \mapsto \alpha \cdot v$ **(skalare Multiplikation)**
- $(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$ **(Assoziativität)**
- $(\alpha + \beta) \cdot v = \alpha v + \beta v$, $\alpha \cdot (u + v) = \alpha u + \alpha v$, **und** $1 \cdot v = v$

Aber $\mathbb{R}$ ist nicht endlich erzeugt.
Angenommen: $\mathbb{R}$ wäre als $\mathbb{Q}$-Vektorraum endlich erzeugt. Dann hätte $\mathbb{R}$ eine $\mathbb{Q}$-Basis $v_1, \ldots, v_n$, dann gäbe es eine Bijektion $\mathbb{R} \tilde{\to} \mathbb{Q}^n$. Aber $\mathbb{Q}^n$ ist gleich mächtig wie $\mathbb{Q}$ (nach Cantor), dann folgt: $\mathbb{R} \tilde{\to} \mathbb{Q}$ (gleiche Mächtigkeit von $\mathbb{R}$ und $\mathbb{Q}$). Wir erhalten einen Widerspruch zu Cantor. Also ist $\mathbb{R}$ nicht endlich erzeugter $\mathbb{Q}$-Vektorraum.
Gibt es nun einen Körper jenseits von $\mathbb{C}$, wobei $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{K}^2$ mit $\dim_{\mathbb{C}} \mathbb{K} < \infty$.
$\mathbb{C} = \{a + ib : a.b \in \mathbb{R}\}$, wobei $1, i$ ist $\mathbb{R}$-Basis.
Es gibt solche $\mathbb{K}$ nicht, da man zeigen kann, daß eine Kugeloberfläche "Löcher" hat, da man bestimmte Kurven nicht zusammenziehen kann.
2. Haben auch nicht-endlich erzeugte Vektorräume Basen?
Sei $(v_i)_{i \in I}$ Basis:

(i) jeder Vektor ist eine endliche Linearkombination von einigen der v_i.

(ii) je endlich viele v_i sind linear unabhängig (im bisherigen Sinne)

2.4.16 Mengentheorie: Zermelo-Fraenkle

Zur Mengentheorie nach Cantor lassen sich Widersprüche konstruieren:
Wir betrachten die Menge M aller Mengen, die sich nicht selbst enthalten:
$M := \{m | m\,\textbf{Menge}, m \notin m\}$

(1) Annahme: M enthält M als Element $(M \in M)$. Dann ist nach Definition $M \notin M$.

(2) Annahme: M enthält sich nicht als Element $(M \notin M)$. Also erfüllt M die geforderte Eigenschaft und ist somit in M enthalten

Ausweg aus diesem Dilemma: Einschränkung des Mengenbildungsprozeß.
Das System, das am häufigsten angewendet wird ist das von Zemelo-Fraenkle (ZF).
Aber aus ZF folgt nicht, daß jeder Vektorraum eine Basis hat.
Zum Glück folgt aus ZF + Auswahlaxiom: Jeder Vektorraum hat eine Basis.

2.4.17 Satz (II.4.3)

Sei $\mathbf{dim}\,(\mathbf{V}) = n$, $\mathbf{U} < \mathbf{V}$, dann gilt:

(i) U ist endlich erzeugt, $\mathbf{dim}\,(\mathbf{U}) \leq \mathbf{dim}\,(\mathbf{V})$

(ii) $\mathbf{dim}\,(\mathbf{U}) = \mathbf{dim}\,(\mathbf{V}) \quad \Leftrightarrow \quad \mathbf{U} = \mathbf{V}$

Beweis:
(i) Seien $u_1, \ldots, u_k \in \mathbf{U}$ linear unabhängig. Dann $k \leq n$ (folgt aus Basisergänzungssatz). Sei k maximal mit dieser Eigenschaft, das heißt: $u_1, \ldots, u_k$ ist ein maximales unabhängiges System in U (Warnung: "Basen = maximal unabhängige Familien" ist hier nicht anwendbar, weil wir noch nicht nachgewiesen haben, daß U endlich erzeugt wird). Sei $u \in \mathbf{U}$ und $u \neq u_1, \ldots, u_k$. Somit ist u Linearkombination von $u_1, \ldots, u_k$:

$$u = \sum_{i=1}^{k} \lambda_i u_i$$

Wegen der Maximalität sind $u_1, \ldots, u_k, u$ linear abhängig. Das heißt: es existiert eine nicht triviale Darstellung der Null:

$$0 = \sum_{i=1}^{k} \lambda_i u_i + \mu u$$

wobei nicht alle Koeffizienten Null sind.
Es folgt: Für $\mu \neq 0$ ist u Linearkombination von $u_1, \ldots, u_k$.
Also zusätzlich: $u_1, \ldots, u_k$ erzeugen $u \Rightarrow u_1, \ldots, u_k$ sind eine Basis.
(ii) "$\Leftarrow$": klar
"$\Rightarrow$": $\mathbf{dim}\,(\mathbf{U}) = \mathbf{dim}\,(\mathbf{V}) = n$. $u_1, \ldots, u_n$ sind eine Basis von U. Nach (i) folgt unmittelbar: $u_1, \ldots, u_n$ sind eine Basis von $\mathbf{V} \Rightarrow \mathbf{U} = \mathbf{V}$.

2.4.18 Satz (II.4.4): Dimensionsformel für Unterräume

Sei V endlich dimensionaler Vektorraum und seien U_1, U_2 Untervektorräume, dann gilt:

$$\mathbf{dim}\,(\mathbf{U}_1 \cap \mathbf{U}_2) + \mathbf{dim}\,(\mathbf{U}_1 + \mathbf{U}_2) = \mathbf{dim}\,(\mathbf{U}_1) + \mathbf{dim}\,(\mathbf{U}_2)$$

Hier ein Beispiel für den $\mathbb{R}^3$
Sei U_1 eine Gerade durch den Nullpunkt, U_2 eine Ebene durch den Nullpunkt.
Wir unterscheiden zwei Fälle:
1. Fall:

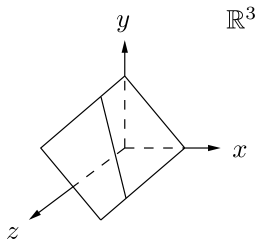

Abbildung II-18: 1. Fall: Die Gerade liegt in der Ebene

Die Gerade ist in der Ebene enthalten: $\mathbf{U}_1 \subseteq \mathbf{U}_2$
Nun gilt: $\mathbf{U}_1 \cap \mathbf{U}_2 = \mathbf{U}_1$ und $\mathbf{U}_1 + \mathbf{U}_2 = \mathbf{U}_2$
Damit ist die Dimensionsformel für Untervektorräume erfüllt.
2. Fall:

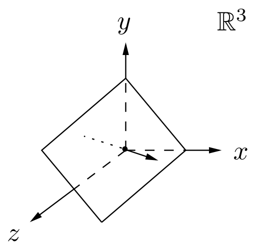

Abbildung II-19: 2. Fall: Die Gerade schneidet die Ebene nur im Nullpunkt

Nun gilt: $\mathbf{U}_1 \not\subseteq \mathbf{U}_2$, $\mathbf{U}_1 \cap \mathbf{U}_2 = \{0\}$.
Aber: $\mathbb{R}^3 \supseteq \mathbf{U}_1 + \mathbf{U}_2 \supseteq \langle v_1, v_2, v_3 \rangle = \mathbb{R}^3$, wobei v_1 der Richtungsvektor der Geraden und v_2, v_3 die beiden Richtungsvektoren der Ebene sind.
Damit ist die Dimensionsformel für Untervektorräume auch in diesem Fall erfüllt.
Für den Beweis haben wir nun folgendes Schema im Kopf:

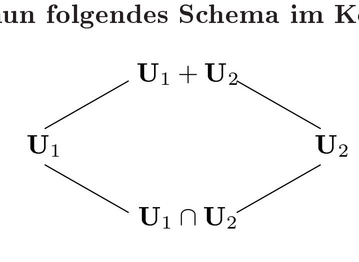

Abbildung II-20: Schema für den Beweis von Satz (II.4.4)

<u>Beweis</u>: Sei $u_1, \ldots, u_k$ eine Basis von $\mathbf{U}_1 \cap \mathbf{U}_2$. Nun ergänze $u_1, \ldots, u_k$ zu einer Basis $u_1, \ldots, u_k, v_1, \ldots, v_l$ von $\mathbf{U}_1$. Zudem ergänze $u_1, \ldots, u_k$ zu einer Basis $u_1, \ldots, u_k, w_1, \ldots, w_m$ von $\mathbf{U}_2$ (Ergänzungen mittels Basisergänzungssatz)

Behauptung: $u_1, \ldots, u_k, v_1, \ldots, v_l, w_1, \ldots, w_m$ **ist eine Basis von** $\mathbf{U}_1 + \mathbf{U}_2$
(Nach der Formel ergibt sich für die linke Seite: $k + (k + l + m)$ **und für die rechte Seite:** $(k + l) + (k + m)$**)**
Beweis: Erzeugendensystem $v = z_1 + z_2$ **mit** $z_i \in \mathbf{U}_i$**.**
Sei:

$$
\begin{aligned}
z_1 &= \sum_{i=1}^{k} \lambda_i u_i + \sum_{j=1}^{l} \mu_j v_j \\
z_2 &= \sum_{i=1}^{k} \lambda_i u_i + \sum_{k=1}^{m} \varphi_k w_k
\end{aligned}
$$

Es folgt unmittelbar, daß $z_1 + z_2$ **Linearkombination von** $u_1, \ldots, u_k, v_1, \ldots, v_l, w_1, \ldots, w_m$ **ist.** $z_1 + z_2 \in \langle u_1, \ldots, u_k, v_1, \ldots, v_l, w_1, \ldots, w_m \rangle$
Noch zu zeigen: Lineare Unabhängigkeit. Sei

$$
\underbrace{\sum_{i=1}^{k} \lambda_i u_i}_{u} + \underbrace{\sum_{j=1}^{l} \mu_j v_j}_{v} + \underbrace{\sum_{k=1}^{m} \varphi_k w_k}_{w} = 0
$$

Nun ist zu zeigen: Alle $\alpha_i, \beta_j, \gamma_r$ **sind gleich Null.**
Wir wissen:

$$
\underbrace{u}_{\mathbf{U}_1 \cap \mathbf{U}_2} + \underbrace{v}_{\mathbf{U}_1} + \underbrace{w}_{\mathbf{U}_2} = 0
$$

Also gilt:

$$
w = -u - v \in \mathbf{U}_1 \cap \mathbf{U}_2
$$

da $u, v \in \mathbf{U}_1$**.**
Es ergibt sich:

$$
w = \sum_{r=1}^{m} \gamma_r w_r = \sum_{s=1}^{k} \delta_s u_s = u
$$

Bringen wir nun beide Terme auf eine Seite, so erhalten wir eine nicht triviale Darstellung der Null:

$$
\sum_{r=1}^{m} \gamma_r w_r - \sum_{s=1}^{k} \delta_s u_s = 0
$$

Weil u_s, w_r **eine Basis von** $\mathbf{U}_2$ **bilden folgt: Alle Koeffizienten sind gleich Null und damit insbesonders alle** γ_r **sind gleich Null.**
Einsetzen in die Ausgangsgleichung liefert:

$$
\sum_i \alpha_i u_i + \sum_j \beta_j v_j = 0
$$

Weil u_i, v_j **eine Basis von** U_1 **bilden, folgt, daß alle Koeffizienten** $\alpha_i, \beta_j = 0$ **sind.**
Damit: $\mathbf{dim}\,(\mathbf{U}_1 + \mathbf{U}_2) = k + l + m = (k + l) + (k + m) - l = \mathbf{dim}\,(\mathbf{U}_1) + \mathbf{dim}\,(\mathbf{U}_2) - \mathbf{dim}\,(\mathbf{U}_1 \cap \mathbf{U}_2)$

2.4.19 Anwendung auf lineare Gleichungssysteme

Ein lineares Gleichungssystem ist von folgender Gestalt

$$\begin{array}{ccccccc} a_{11}\cdot x_1 & + & \dots & + & a_{1n}\cdot x_n & = & 0 \\ a_{21}\cdot x_1 & + & \dots & + & a_{2n}\cdot x_n & = & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ a_{m1}\cdot x_1 & + & \dots & + & a_{mn}\cdot x_n & = & 0 \end{array}$$

Gegeben sind alle $a_{ij} \in \mathbb{K}$, gesucht sind $x_1, \dots, x_n$.
Wir können einen Lösungsraum angeben:

$$\mathbb{L} = \left\{ (x_1, \dots, x_n) \in \mathbb{K}^n : \sum_{j=1}^{n} a_{ij} \cdot x_j = 0 \quad \textbf{wobei} \quad i = 1, \dots, m \right\}$$

Der Lösungsraum ist auch auf die folgende Art darzustellen:

$$\mathbb{L} = \bigcap_{i=1}^{m} \underbrace{\left\{ (x_1, \dots, x_n) \in \mathbb{K}^n : \sum_{j=1}^{n} a_{ij} \cdot x_j = 0 \right\}}_{\doteqdot\, u_i}$$

Hier noch eine kleine Auffrischung: $a_1 \cdot x_1 + \ldots + a_n \cdot x_n = 0$

OBdA: Sei $a_1 \neq 0$, dann läßt sich x_1 als LK von $x_2, \dots, x_n$ darstellen: $x_1 = \sum_{j=2}^{n} -\frac{a_j}{a_1} \cdot x_j$

Daraus folgt unmittelbar: $(x_1, \dots, x_n) = \sum_{j=2}^{n} x_j \cdot \left(-\frac{a_j}{a_1}, 0, \dots, 0, 1, 0, \dots, 0 \right)$ **wobei die** 1 **an der** j**-ten Stelle steht. Also:**

$$\left\{ (x_1, \dots, x_n) : \sum_{j=1}^{n} a_i \cdot x_i = 0 \right\} = \left\langle \dots, \left(-\frac{a_j}{a_i}, 0, \dots, 0, 1, 0, \dots, 0 \right), \dots \right\rangle \quad \textbf{mit} \quad j = 2, \dots, n$$

Für die Dimension des Lösungsraumes gilt:

$$\mathbf{dim} \left\{ (x_1, \dots, x_n) : \sum_{j=1}^{n} a_i \cdot x_i = 0 \right\} = n - 1 \quad \textbf{falls } a_i = 0$$

Sind alle $a_i = 0$ so folgt unmittelbar, daß $\left\{ x : \sum_{i=1}^{n} a_i \cdot x_i = 0 \right\} = \mathbb{K}^n$ **wobei der $\mathbb{K}^n$ natürlich n-dimensional ist. Wir können also Aussagen über die Dimension des Lösungsraumes machen.**
Wählen wir $m = 2$ so gilt:

$$\begin{array}{rcl} \mathbb{L} & = & \mathbb{L}_1 \cap \mathbb{L}_2 \\ \mathbf{dim}\,(\mathbb{L}) & = & \mathbf{dim}\,(\mathbb{L}_1) + \mathbf{dim}\,(\mathbb{L}_2) - \mathbf{dim}\,(\mathbb{L}_1 + \mathbb{L}_2) \geq (n-1) + (n-1) - n = n - 2 \end{array}$$

Damit können wir eine Aussage für $m = 3$ treffen:

$$\begin{array}{rcl} \mathbb{L} & = & (\mathbb{L}_1 \cap \mathbb{L}_2) \cap \mathbb{L}_3 \\ \mathbf{dim}\,(\mathbb{L}) & = & \mathbf{dim}\,(\mathbb{L}_1 \cap \mathbb{L}_2) + \mathbf{dim}\,(\mathbb{L}_3) + \mathbf{dim}\,(\mathbb{L}_1 \cap \mathbb{L}_2 + \mathbb{L}_3) \geq (n-2) + (n-1) - n = n - 3 \end{array}$$

Per Induktion nach m folgt: $\mathbf{dim}\,(\mathbb{L}_1 \cap \mathbb{L}_2 \cap \ldots \cap \mathbb{L}_m) \geq n - m$
Die interessanten Fälle sind: $m \leq n - 1 \Rightarrow \mathbf{dim}\,(\mathbb{L}) \geq 1$ **(In diesen Fällen haben wir mindestens eine Gleichung weniger als Variablen)**

2.4.20 Studium von Unterräumen

Gegeben seien U_1, U_2 mit $U_1 \cap U_2 = \{0\}$. Hier ein anschauliches Beispiel für den $\mathbb{R}^3$
I. U_1 ist der $\mathbb{R}^3$, $U_2 = \{0\}$

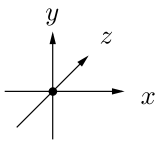

Abbildung II-21: 1. Beispiel für Untervektorräume

II. Sei U_1 eine Ebene und U_2 eine Gerade, wobei $U_2 \notin U_1$ (Die Gerade ist nicht in der Ebene enthalten)

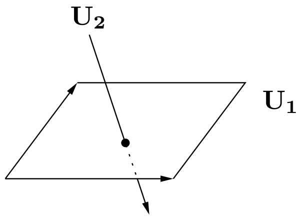

Abbildung II-22: 2. Beispiel für Untervektorräume

Andere Untervektorräume: $\mathbb{R}^3 \subseteq U_1, U_2$, $\dim(U_i) \geq 2$
Behauptung: $\dim(U_1 \cap U_2) \geq 1$
Beweis: $\dim(U_1 \cap U_2) \geq \dim(U_1) + \dim(U_2) - \dim(U_1 + U_2) = 2 + 2 - 3 = 1$
Sei $\dim(U_1 \cap U_2) = 2$, $\dim(U_i) = 2$
Behauptung: $\Rightarrow \quad U_1 = U_2$. **Dazu: Ist** $U < V$ **und** $\dim(U) = \dim(V) \quad \Rightarrow \quad U = V$

2.4.21 Satz (II.4.5)

Seien $U_1, U_2 < V$, wobei $U_1 \neq U_2$. Folgende Aussagen sind äquivalent:

- **(i)** $U_1 \cap U_2 = \{0\}$
- **(ii)** $\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$
- **(iii)** $0 = u_1 + u_2$, $u_i \in U_i \Rightarrow u_1 = u_2 = 0$
- **(iv)** **Jedes** $v \in U_1 + U_2$ **hat eine eindeutige Darstellung der Form** $v = u_1 + u_2$ **mit** $u_i \in U_i$

Beweise:
$(i) \Rightarrow (ii)$: **Dimensionsformel:** $\dim\{0\} = 0$
$(ii) \Rightarrow (iii)$: **Angenommen:** $0 = u_1 + u_2$, **ein** $u_i \neq 0$ **(nicht beide** u_i **können Null sein). Damit sind beide** u_i **ungleich Null:** $u_1 = -u_2 \neq 0$. $u_1 \in U_1$, **da** $u_1 = -u_2 \neq 0 \Rightarrow u_1 \in U_2 \Rightarrow U_1 \cap U_2 \neq \{0\} \Rightarrow \dim(U_1 \cap U_2) \geq 1$. **Damit erhalten wir einen Widerspruch zur Annahme:** $\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$
$(iii) \Rightarrow (iv)$: **Annahme: Sei** $v = u_1 + u_2 = u_1' + u_2'$ **wobei** $u_i, u_i' \in U_i$. **Zu zeigen:** $u_1 = u_1'$, $u_2 = u_2'$. **Es gilt:** $0 = v - v = u_1 + u_2 - u_1' - u_2' = \underbrace{(u_1 - u_1')}_{\in U_1} + \underbrace{(u_2 - u_2')}_{\in U_2}$. **Nach** (iii) **folgt:** $u_1 = u_1'$ **und** $u_2 = u_2'$.
$(iv) \Rightarrow (i)$ **Sei** $v \in U_1 \cap U_2$ **und** $0 = \underbrace{v}_{\in U_1} + \underbrace{(-v)}_{\in U_2}$. $0 \in U_1 + U_2$ **und** $0 = \underbrace{0}_{\in U_1} + \underbrace{0}_{\in U_2}$.
Da es nur eine eindeutige Darstellung gibt, folgt: $v = 0$.

2.4.22 Definition (II.4.d): Komplement eines Untervektorraums

$\mathbf{U}_2$ heißt Komplement oder komplementärer Vektorraum zu $\mathbf{U}_1 < \mathbf{V}$, wenn gilt:

$$\mathbf{U}_2 < \mathbf{V}, \quad \mathbf{U}_1 \cap \mathbf{U}_2 = \{0\}, \quad \mathbf{U}_1 + \mathbf{U}_2 = \mathbf{V}$$

Achtung: Die Definition unterscheidet sich von dem Mengentheoretrischen Komplement.

2.4.23 Satz (II.4.6)

Jeder Untervektorraum eines endlich erzeugten Vektorraums besitzt ein Komplement.
Beweis: Sei $\mathbf{U} < \mathbf{V}$, wobei $\mathbf{V}$ ein endlich erzeugter Vektorraum ist. Dann hat $\mathbf{U}$ eine Basis $u_1, \ldots, u_k$. Nach dem Basisergänzungssatz bildet $u_1, \ldots, u_k, u_{k+1}, \ldots, u_n$ eine Basis von $\mathbf{V}$. Setze nun $\mathbf{U}' := \langle u_{k+1}, \ldots, u_n \rangle$
Behauptung: $\mathbf{U} \cap \mathbf{U}' = \{0\}$ beziehungsweise $\mathbf{U} + \mathbf{U}' = \mathbf{V}$
Beweis: $\mathbf{U}+\mathbf{U}' = \mathbf{V}$, weil $\mathbf{U}+\mathbf{U}'$ die Basis von $u_1, \ldots, u_k, u_{k+1}, \ldots, u_n$ enthält. Weiterhin:

$$\mathbf{dim}\,(\mathbf{U} + \mathbf{U}') = n = k + (n-k) = \mathbf{dim}\,(\mathbf{U}) + \mathbf{dim}\,(\mathbf{U}')$$

Nach Satz (II.4.5) (ii) folgt: $\mathbf{U} \cap \mathbf{U}' = \{0\}$
Bemerkung:

(i) Notation: $\mathbf{V} = \mathbf{U} \oplus \mathbf{U}$: $\mathbf{V}$ ist die direkte Summe von $\mathbf{U}$ und $\mathbf{U}'$

$$\mathbf{V} = \mathbf{U} \oplus \mathbf{U} :\Leftrightarrow \mathbf{U} \cap \mathbf{U}' = \{0\}, \quad \mathbf{U} + \mathbf{U}' = \mathbf{V}$$

(ii) Es gibt im Allgemeinen mehrere Komplemente: Beispiele (siehe (iii)) oder: Basisergänzung ist nicht eindeutig.

(iii) Beispiel:

$$\mathbf{V} = \left(\mathbb{Z}/_{3\mathbb{Z}}\right)^2$$

Hier die Darstellung von

$$\mathbf{U}_1 = \left\{ \left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{0}\right), \left(\overline{2},\overline{0}\right) \right\} = \mathbb{Z}/_{3\mathbb{Z}} \cdot \left(\overline{1},\overline{0}\right)$$

und

$$\mathbf{U}_2 = \left\{ \left(\overline{0},\overline{0}\right), \left(\overline{1},\overline{2}\right), \left(\overline{2},\overline{1}\right) \right\} = \mathbb{Z}/_{3\mathbb{Z}} \cdot \left(\overline{1},\overline{2}\right)$$

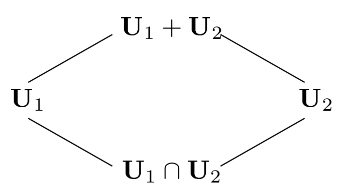

Abbildung II-23: Darstellung von $\mathbf{U}_1$ und $\mathbf{U}_2$

Behauptung: $\mathbf{U}_2$ ist das Komplement zu $\mathbf{U}_1$.
Zu zeigen: $\mathbf{U}_1 \cap \mathbf{U}_2 = \{0\}$ und $\mathbf{U}_1 + \mathbf{U}_2 = \mathbf{V}$.
Beweis: Man sieht leicht:

$$\begin{aligned}\mathbf{U}_1 \cap \mathbf{U}_2 &= \left\{\left(\overline{0},\overline{0}\right),\left(\overline{1},\overline{0}\right),\left(\overline{2},\overline{0}\right)\right\} \cap \left\{\left(\overline{0},\overline{0}\right),\left(\overline{1},\overline{2}\right),\left(\overline{2},\overline{1}\right)\right\} \\ &= \left\{\left(\overline{0},\overline{0}\right)\right\}\end{aligned}$$

$\mathbf{V} = \left(\mathbb{Z}/_{3\mathbb{Z}}\right)^2 = \left\{\left(\overline{0},\overline{0}\right),\left(\overline{1},\overline{0}\right),\left(\overline{0},\overline{1}\right)\right\}$ **Es reicht diese drei Paare zu betrachten, da wir alle anderen als Linearkombinationen darstellen können.**
Da es sich um einen endlichen Körper handelt können wir alle Kombinationen ausrechnen:

$$\mathbf{U}_1 + \mathbf{U}_2 = \left\{\left(\overline{0},\overline{0}\right),\left(\overline{1},\overline{0}\right),\left(\overline{2},\overline{0}\right),\left(\overline{1},\overline{2}\right),\left(\overline{2},\overline{1}\right)\right\}$$

$\left(\overline{0},\overline{0}\right)$ **ist zwingend erforderlich, also brauchen wir nur noch zwei lineare unabhängige Vektoren zu wählen und zeigen, daß sie V erzeugen. z.B.** $\left(\overline{2},\overline{0}\right),\left(\overline{1},\overline{2}\right)$. **In** $\left(\mathbb{Z}/_{3\mathbb{Z}}\right)^2$ **ist** $\overline{2}\cdot\left(\overline{2},\overline{0}\right) = \left(\overline{4},\overline{0}\right) = \left(\overline{1},\overline{0}\right) \in \mathbf{V}$ **und** $\overline{2}\cdot\left(\overline{1},\overline{2}\right) - \left(\overline{2},\overline{0}\right) = \left(\overline{2},\overline{1}\right) - \left(\overline{2},\overline{0}\right) = \left(\overline{0},\overline{1}\right) \in \mathbf{V}$
Beweis: $(ii) \quad \Rightarrow \quad (i)$**: ?**