Lineare Algebra 1

Daniele Agostini

3. Mai 2024

Vorwort

Diese Notizen basieren auf den Notizen des Kurses von Hannah Markwig. Unsere Notizen sind eher grob und ersetzen in keiner Weise ein gutes Buch über lineare Algebra. Falls Sie Fehler finden, teilen Sie mir diese (auch die offensichtlichen) bitte mit!

Inhaltsverzeichnis

Kapitel 1

Grundlagen

1.1 Aussagen

Siehe Analysis I.

1.2 Mengen

Das Konzept der Menge ist eines der grundlegenden Konzepte der Mathematik, und es gibt einen ganzen Zweig der Logik, die Mengenlehre, der sich mit ihren Studien beschäftigt. In diesem Kurs (und im Großteil der Mathematik) werden wir die naive Definition einer Menge verwenden:

Als Menge wird in der Mathematik ein abstraktes Objekt bezeichnet, das aus der Zusammenfassung einer Anzahl einzelner Objekte hervorgeht. Diese werden dann als die Elemente der Menge bezeichnet. (Wikipedia)

Man schreibt

$$\begin{aligned} x \in M &\iff x \text{ ein Element in } M \text{ ist }, \\ x \notin M &\iff x \text{ kein Element in } M \text{ ist }. \end{aligned}$$

Beispiel 1.2.1 (Mengen von Zahlen)**.** Die Menge von *natürliche Zahlen* ist

$$\mathbb{N} = \{0, 1, 2, \dots\}^1$$

Die Menge der *ganze Zahlen* ist

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Die Menge der *rationelle Zahlen* ist

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Die Menge der *reelle Zahlen* ist

$$\mathbb{R}.$$

[1] Vorsicht: manchmal ist die Menge von natürliche Zahlen als $\{1, 2, 3 \dots\}$ definiert. In unserem Kurs 0 ist eine natürliche Zahl.

Als Beispiel, sehen wir dass $-4 \in \mathbb{Z}$ aber $-4 \notin \mathbb{N}$. Man kann auch zeigen dass $\sqrt{2} \in \mathbb{R}$ aber $\sqrt{2} \notin \mathbb{Q}$.

Beispiel 1.2.2 (Viele andere Mengen)**.** Viele Beispiele von andere Mengen:

- Die zwei Mengen $\{1, 2, 3, 4\} = \{1, 1, 2, 3, 4\}$ sind gleich, weil sie die gleiche Elementen haben.
- Die menge von gerade natürliche Zahlen: $\{n \in \mathbb{N} \,|\, n \text{ gerade } \} = \{0, 2, 4, 6, \dots\}$.
- Die leere Menge $\emptyset$, die keine Elemente enthält.
- Die Menge M von alle Menschen auf der Erde: M hat circa 8.1 Milliarde Elementen. Die Menge $M_{>200} = \{m \in M \,|\, m \text{ ist mehr als 200 Jahre alt } \} = \emptyset$.

Definition 1.2.3 (Teilmenge)**.** Seien M_1, M_2 Mengen. Wir sagen dass M_1 eine *Teilmenge* von M_2 ist falls alle Elemente von M_1 auch Elemente von M_2 sind. Wir schreiben $M_1 \subseteq M_2$. Mit Symbole:

$$M_1 \subseteq M_2 \iff (x \in M_1 \implies x \in M_2)$$

Wir sagen dass M_1 eine *echte Teilmenge* ist, falls $M_1 \subseteq M_2$ und $M_1 \neq M_2$. Wir schreiben $M_1 \subsetneq M_2$.

Beispiel 1.2.4. Man kann zeigen dass $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

Bemerkung 1.2.5. Seien M_1, M_2 zwei Mengen, dann

$$M_1 = M_2 \iff M_1 \subseteq M_2 \text{ und } M_2 \subseteq M_1.$$

Definition 1.2.6 (Schnitt, Vereinigung, Differenz, Komplement)**.** Seien M_1, M_2 Mengen.

- Der *Schnitt* $M_1 \cap M_2$ enthalt alle Elemente, die sowohl in M_1 als auch in M_2 sind:

$$M_1 \cap M_2 = \{x \,|\, x \in M_1, x \in M_2\}.$$

- Die *Vereinigung* enthält alle Elemente die in M_1 oder in M_2 sind:

$$M_1 \cup M_2 = \{x \,|\, x \in M_1 \text{ oder } x \in M_2\}$$

- Die *Differenz* $M_1 \setminus M_2$ enthält alle Elemente in M_1 die nicht in M_2 enthält sind:

$$M_1 \setminus M_2 = \{x \in M_1 \,|\, x \notin M_2\}.$$

- Wenn $M_2 \subseteq M_1$, das *Komplement* von M_1 in M_2 ist

$$M_1^c = M_1 \setminus M_2$$

Bemerkung 1.2.7. Die Notation M^c ist immer abhängig vom Kontext: das Komplement von $\mathbb{N}$ in $\mathbb{Z}$ ist $\mathbb{N}^c = \{x \in \mathbb{Z} \,|\, x \notin \mathbb{N}\} = \{\dots, -3, -2, -1\}$, aber das Komplement von $\mathbb{N}$ in $\mathbb{N}$ ist $\mathbb{N}^c = \{x \in \mathbb{N} \,|\, x \notin \mathbb{N}\} = \emptyset$.

Wir können auch der Schnitt und der Vereinigung von beliebige viele Mengen $M_i, i \in I$ definieren:

$$\bigcap_{i\in I} M_i = \{x \,|\, x \in M_i \text{ für alle } i \in I\}, \qquad \bigcup_{i\in I} M_i = \{x \,|\, x \in M_i \text{ für ein } i \in I\}.$$

Definition 1.2.8. Zwei Mengen M_1, M_2 heißen *disjunkt*, falls $M_1 \cap M_2 = \emptyset$. Wenn M_1, M_2 disjunkt sind, wir schreiben manchmal die Vereinigung als $M_1 \sqcup M_2$ oder $M_1 \dot\cup M_2$.

Lemma 1.2.9 (Eigenschaften des Schnittes und der Vereinigung)**.** *Seien M_1, M_2, M_3 Mengen. Der Schnitt und der Vereinigung sind:*

- *Kommutativ:*

$$M_1 \cap M_2 = M_2 \cap M_1,$$
$$M_1 \cup M_2 = M_2 \cup M_1.$$

- *Associativ:*

$$(M_1 \cap M_2) \cap M_3 = M_1 \cup M_2 \cup M_3 = M_1 \cap (M_2 \cap M_3),$$
$$(M_1 \cup M_2) \cup M_3 = M_1 \cap M_2 \cap M_3 = M_1 \cap (M_2 \cap M_3).$$

- *Distributiv:*

$$(M_1 \cap M_2) \cup M_3 = (M_1 \cup M_3) \cap (M_2 \cup M_3),$$
$$(M_1 \cup M_2) \cap M_3 = (M_1 \cap M_3) \cup (M_2 \cap M_3).$$

Beweis. Als Beispiel, zeigen wir dass $(M_1 \cap M_2) \cup M_3 = (M_1 \cup M_3) \cap (M_2 \cup M_3)$. Wir zeigen die zwei Inklusionen:

- $\subseteq$: wir wollen zeigen, dass $(M_1 \cap M_2) \cup M_3 \subseteq (M_1 \cup M_3) \cap (M_2 \cup M_3)$. Sei $x \in (M_1 \cap M_2) \cup M_3$, dann $x \in M_1 \cap M_2$ oder $x \in M_3$. Wenn $x \in (M_1 \cap M_2)$ dann $x \in M_1 \cup M_3$ und $x \in M_2 \cup M_3$, so dass $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$. Wenn $x \in M_3$, dann $x \in M_1 \cup M_3$ und $x \in M_2 \cup M_3$, so dass $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$.

- $\supseteq$: wir wollen zeigen, dass $(M_1 \cap M_2) \cup M_3 \supseteq (M_1 \cup M_3) \cap (M_2 \cup M_3)$. Sei $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$, dann $x \in M_1 \cup M_3$ und $x \in M_2 \cup M_3$. Wenn $x \in M_3$, dann $x \in (M_1 \cap M_2) \cup M_3$ auch. Wenn $x \notin M_3$, wir wissen dass $x \in M_1 \cup M_3$, so dass $x \in M_1$. Wir wissen auch, dass $x \in M_2 \cup M_3$, so dass $x \in M_2$. Das zeigt dass $x \in M_1 \cap M_2$ und dann $x \in (M_1 \cap M_2) \cup M_3$.

□

Lemma 1.2.10 (Eigenschaften des Komplementes)**.** *Seien M_1, M_2, M_3 zwei Mengen so dass $M_1 \subseteq M_3, M_2 \subseteq M_3$. Die Komplementen in M_3 haben die Eigenschaften:*

- $M^1 \subseteq M_2 \iff M_1^c \supseteq M_2^c$.
- $(M_1 \cup M_2)^c = M_1^c \cap M_2^c$.
- $(M_1 \cap M_2)^c = M_1^c \cup M_2^c$.

- $(M_1^c)^c = M_1$.

Beweis. Im Repetitorium. □

Definition 1.2.11 (Kartesisches Produkt)**.** Seien M_1, M_2 Mengen. Das kartesisches Produkt von M_1 und M_2 ist die Menge definiert als

$$M_1 \times M_2 \colon = \{(x_1, x_2) \,|\, x \in M_1, x \in M_2\}$$

Hier (x_1, x_2) ist ein geordnetes Paar: d.h. $(x_1, y_1) = (x_2, y_2)$ genau dann, wenn $x_1 = y_1, x_2 = y_2$. Falls $M = N$ schreiben wir $M \times M = M^2$.

Beispiel 1.2.12. Seien $M_1 = \{1, 2, 3\}$ und $M_2 = \{4, 5\}$. Dann

$$M_1 \times M_2 = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}.$$

Beispiel 1.2.13. Die Menge $\mathbb{Z}^2 = \{(n, m) \,|\, n, m \in \mathbb{Z}\}$ ist eine Teilmenge von $\mathbb{R}^2 = \{(x, y) \,|\, x, y \in \mathbb{R}\}$

1.3 Funktionen

Definition 1.3.1 (Funktion, Abbildung)**.** Eine Funktion oder Abbildung $f \colon X \to Y$ von einer Menge X zu einer Menge Y ist eine Zuordnung, die jedem Element $x \in X$ ein Element $y = f(x) \in Y$ zuordnet. Wir schreiben

$$f \colon X \to Y, \qquad x \mapsto f(x)$$

Die Menge X heißt Definitionsbereich, die Menge Y heißt Zielbereich oder Wertemenge

Bemerkung 1.3.2. das Definitionsbereich und das Zielbereich sind teil von der Definition einer Abbildung. Das bedeutet dass zwei Abbildungen

$$f \colon X \to Y, \qquad g \colon X' \to Y'$$

gleich sind, genau dann, wenn $X = X', Y = Y'$ und $f(a) = g(a)$ für alle $a \in X$. Z.B. die zwei Abbildungen

$$f \colon \mathbb{N} \to \mathbb{N}, x \mapsto x + 1 \qquad g \colon \mathbb{N} \to \mathbb{Z}, x \mapsto x + 1$$

sind verschiedene Abbildungen, trotzdem $f(x) = g(x)$ für alle $x \in \mathbb{N}$.

Beispiel 1.3.3. Die Funktion $f \colon \{1, 2, 3\} \to \{4, 7\}$ so dass $f(1) = 7, f(2) = 4, f(3) = 4$

Beispiel 1.3.4. Die Funktion $f \colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$.

Andere Beispiele von Funktionen:

Definition 1.3.5 (Konstante Funktion)**.** Eine Funktion $f \colon X \to Y$ heißt konstant, wenn $k \in Y$ existiert so dass $f(x) = k$ für alle $x \in X$.

Definition 1.3.6 (Identität)**.** Sei X eine Menge. Die Identität von X ist die Abbildung

$$\mathrm{id}_X \colon X \to X, \qquad x \mapsto x$$

Definition 1.3.7 (Einschränkung)**.** Seien $f\colon X \to Y$ eine Funktion und $A \subseteq X$ eine Teilmenge. Die Einschränkung von f auf A ist die Funktion

$$f_{|A}\colon A \to Y, \qquad a \mapsto f(a)$$

Definition 1.3.8 (Bild)**.** Sei $f\colon X \to Y$ eine Funktion und $A \subseteq X$ eine Teilmenge. Das Bild von A unter f ist

$$f(A)\colon = \{f(a) \,|\, a \in A\} = \{y \in Y \,|\, y = f(a) \text{ für ein } a \in A\}$$

Das Bild von X unter f ist auch Bild von f genannt:

$$\operatorname{Im} f = f(X)$$

Definition 1.3.9 (Urbild)**.** Sei $f\colon X \to Y$ eine Funktion und $B \subseteq Y$ eine Teilmenge. Das Urbild von B unter f ist

$$f^{-1}(B)\colon = \{x \in X \,|\, f(x) \in B\}$$

Wenn $B = \{b\}$ nur ein Element enthält, schreiben wir auch $f^{-1}(b) = f^{-1}(\{b\})$.

Beispiel 1.3.10. Sei $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. Das Bild von f ist

$$f(\mathbb{R}) = \{x^2 \,|\, x \in \mathbb{R}\}$$

Wir sehen dass $f(\mathbb{R}) \subseteq \mathbb{R}_{\geq 0} = \{y \in \mathbb{R} \,|\, y \geq 0\}$ weil jeder Quadrat in $\mathbb{R}$ nicht negativ ist. Aber wir wissen auch dass jedes $y \in \mathbb{R}_{\geq 0}$ ein Wurzel hat: es gibt $x \in \mathbb{R}$ so dass $y = x^2 = f(x)$. Das zeigt, dass

$$f(\mathbb{R}) = \mathbb{R}_{\geq 0};$$

Wir können auch manche Urbilder explizit bestimmen:

$$\begin{aligned} f^{-1}(0) &= \{x \in \mathbb{R} \,|\, x^2 \in \{0\}\} = \{x \in \mathbb{R} \,|\, x^2 = 0\} = \{0\} \\ f^{-1}(4) &= \{x \in \mathbb{R} \,|\, x^2 \in \{4\}\} = \{x \in \mathbb{R} \,|\, x^2 = 4\} = \{-2, +2\} \\ f^{-1}([-2,-1]) &= \{x \in \mathbb{R} \,|\, -2 \leq x \leq -1\} = \emptyset. \end{aligned}$$

Definition 1.3.11 (Injektiv, surjektiv, bijektiv)**.** Eine Funktion $f\colon X \to Y$ heißt

- Injektiv: falls verschiedene Elemente von X verschiedene Bilder haben: d.h. für alle $x_1, x_2 \in X$:

  $$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

  Das ist äquivalent zu

  $$f(x_1) = f(x_2) \implies x_1 = x_2.$$

- Surjektiv: falls alle Elemente von Y, Bilder von Elementen von X sind:

  $$\text{Für alle } y \in Y, \text{ existiert } x \in X \text{ s.d. } y = f(x).$$

  Das ist äquivalent zu $f(X) = Y$.

- Bijektiv: falls f injektiv und surjektiv ist. Das bedeutet dass

  $$\text{für alle } y \in Y \text{ existiert genau ein } x \in X \text{ s.d. } y = f(x).$$

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ **Ende Vorlesung 19.04.2024** ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

Beispiel 1.3.12. Die Abbildung $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist nicht injektiv, weil $f(1) = f(-1) = 1$ und ist nicht surjektiv, weil $f(x) = x^2 \geq 0$ für alle $x \in \mathbb{R}$ so dass kein $x \in \mathbb{R}$ existiert mit $f(x) = x^2 = -1$.

Die Abbildung $f_{|\mathbb{R}_{\geq 0}}\colon \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$ ist injektiv aber nicht surjektiv.

Die Abbildung $f_{|\mathbb{R}_{\geq 0}}\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist injektiv und surjektiv, d.h. bijektiv.

Lemma 1.3.13. *Sei $f\colon X \to Y$ eine Funktion. Dann gilt*

(a) f ist injektiv, genau dann, wenn $f^{-1}(y)$ entweder 1 oder 0 Elemente enthält, für alle $y \in Y$.

(b) f ist surjektiv, genau dann, wenn $f^{-1}(y) \neq \emptyset$ für alle $y \in Y$.

(c) f ist bijektiv, genau dann, wenn $f^{-1}(y)$ genau ein Element enthält, für alle $y \in Y$.

Beweis. (a) ($\Longrightarrow$) Sei $y \in Y$. Wir wollen zeigen, dass $f^{-1}(y)$ höchstens ein Element enthält. Seien $x_1, x_2 \in f^{-1}(y)$. Dann $f(x_1) = y = f(x_2)$. Da f injektiv ist, das zeigt dass $x_1 = x_2$.

($\Longleftarrow$) Seien $x_1, x_2 \in X$ so dass $f(x_1) = f(x_2) = y$. Dann $x_1, x_2 \in f^{-1}(y)$. Da $f^{-1}(y)$ höchstens ein Element enthält, es muss sein dass $x_1 = x_2$. Das zeigt dass f injektiv ist.

(b) Die Funktion f ist surjektiv, genau dann, wenn für alle $y \in Y$ ein $x \in X$ existiert, so dass $f(x) = y$. Die Gleichung $f(x) = y$ bedeutet genau dass $x \in f^{-1}(y)$. Das zeigt dass f surjektiv ist, genau dann, wenn $x \in X$ existiert so dass $xinf^{-1}(y)$. Äquivalent, genau dann, wenn $f^{-1}(y) \neq \emptyset$ für alle $y \in Y$.

(c) Die Funktion f ist bijektiv, genau dann, wenn f injektiv und surjektiv ist. Punkt (a) zeigt dass, f injektiv ist, genau dann, wenn $f^{-1}(y)$ höchstens ein Element enthält, für alle $y \in Y$. Punkt (b) zeigt dass f surjektiv ist, genau dann, wenn $f^{-1}(y)$ mindestens ein Element enthält, für alle $y \in Y$. Dann, ist f bijektiv, genau dann, wenn $f^{-1}(y)$ genau ein Element enthält, für alle $y \in Y$.

□

Definition 1.3.14 (Komposition)**.** Seien $f\colon X \to Y$ und $g\colon Y \to Z$ zwei Abbildungen. Ihre Komposition $g \circ f$ ist die Abbildung

$$g \circ f\colon X \to Z, \qquad x \mapsto g(f(x))$$

Beispiel 1.3.15. Seien $f\colon \mathbb{R} \to \mathbb{R}$ und $g\colon \mathbb{R} \to \mathbb{R}$ durch $f(x) = x + 2, g(x) = x^2$. Dann

$$f \circ g\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2 + 2,$$
$$g \circ f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto (x + 2)^2$$

Lemma 1.3.16. *(a) Sei $f\colon X \to Y$ eine Abbildung. Dann*

$$f \circ \mathrm{id}_X = f, \quad \mathrm{id}_Y \circ f = f.$$

(b) (Assoziativität) Seien $f\colon X \to Y, g\colon Y \to W, h\colon W \to Z$ Abbildungen. Dann gilt

$$h \circ (f \circ g) = (h \circ f) \circ g$$

Beweis. (a) Die zwei Abbildungen $f \circ \mathrm{id}_X$ und f haben Definitionsbereich X und Zielbereich X. Wir müssen zeigen dass $(f \circ \mathrm{id}_X)(x) = f(x)$ für alle $x \in X$. Aber $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x)$. Eine änliche Begrundung zeigt dass $\mathrm{id}_Y \circ f = f$.

(b) Die Zwei Abbildungen $h \circ (f \circ g)$ und $(h \circ f) \circ g$ haben Definitionsbereich X und Zielbereich Z. Sei $x \in X$: dann

$$\begin{aligned}(h \circ (f \circ g))(x) &= h((f \circ g)(x)) = h(f(g(x))) \\ &= (h \circ f)(g(x)) = ((h \circ f) \circ g))(x).\end{aligned}$$

□

Definition 1.3.17 (Invertierbare Funktion)**.** Eine Funktion $f\colon X \to Y$ heißt invertierbar oder umkehrbar, falls eine Funktion $g\colon Y \to X$ existiert so dass

$$(g \circ f) = \mathrm{id}_X, \qquad (f \circ g) = \mathrm{id}_Y$$

Die Funktion g heißt dann, Umkehrfunktion oder inverse Funktion von f. Wir schreiben auch f^{-1}.

Lemma 1.3.18. *Sei $f\colon X \to Y$ eine invertierbare Funktion. Dann ist die inverse Funktion eindeutig.*

Beweis. Seien $g_1\colon Y \to X$ und $g_2\colon Y \to X$ zwei inverse Funktionen von f. Dann gilt

$$g_1 = g_1 \circ \mathrm{id_Y} = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id_X} \circ g_2 = g_2.$$

□

Bemerkung 1.3.19. Die Gleichung $f^{-1} \circ f = \mathrm{id}_X$ zeigt dass $f^{-1}(f(x)) = \mathrm{id}_X(x) = x$ für alle $x \in X$. Die Gleichung $f \circ f^{-1} = \mathrm{id}_Y$ zeigt dass $f(f^{-1}(x)) = \mathrm{id}_Y(y) = y$ für alle $y \in Y$.

Definition 1.3.20 (Inverse Funktion)**.** Wenn $f\colon X \to Y$ eine invertierbare Funktion ist, schreiben wir die eindeutige inverse Funktion als $f^{-1}\colon Y \to X$.

Bemerkung 1.3.21 (**Vorsicht!**)**.** Sei $f\colon X \to Y$ eine Funktion. Das Urbild $f^{-1}(B)$ von einer Teilmenge $B \subseteq Y$ ist *immer* definiert, für *jede* Funktion. Die inverse Funktion $f^{-1}\colon Y \to X$ ist definiert *nur* wenn f invertierbar ist.

Wenn die Funktion invertierbar ist, stimmen diese beiden Begriffe wie folgt überein

Lemma 1.3.22. *Sei $f\colon X \to Y$ eine invertierbare Funktion mit inverse Funktion $f^{-1}\colon Y \to X$. Sei auch $B \subseteq Y$ eine Teilmenge. Das Urbild von B unter f, und das Bild von B unter f^{-1} sind gleich.*

Beweis. Wir schreiben die inverse Abbildung als $g\colon Y \to X$, um Verwirrung zwischen das Urbild und die inverse Funktion zu vermeiden. Wir wollen zeigen dass, das Bild $g(B)$ und das Urbild $f^{-1}(B)$ gleich sind:

$$g(B) = f^{-1}(B)$$

Wir zeigen zuerst dass $g(B) \subseteq f^{-1}(B)$: sei $y \in B$, dann $f(g(y)) = (f \circ g)(y) = \mathrm{id}_Y(y) = y$. Das bedeutet dass $g(y)$ im Urbild $f^{-1}(B)$ ist.

Wir zeigen jetzt dass $g(B) \supseteq f^{-1}(B)$: sei $x \in f^{-1}(B)$, sodass $y = f(x) \in B$. Dann $x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(y)$. Das zeigt dass $x \in g(B)$. □

Satz 1.3.1. *Eine Funktion $f\colon X \to Y$ ist invertierbar, genau dann, wenn f bijektiv ist.*

Beweis. Wir zeigen die zwei Implikationen:

($\Longrightarrow$) Wir zeigen dass, wenn f invertierbar ist, dann f auch bijektiv ist. Sei $f^{-1}\colon Y \to X$ die inverse Funktion von f.Wir zeigen zuerst dass f injektiv ist: seien $x_1, x_2 \in X$ so dass $f(x_1) = f(x_2)$. Dann $f^{-1}(f(x_1)) = f^{-1}(f(x_2)$. Da $f^{-1}(f(x)) = x$ für alle $x \in X$, sehen wir dass $x_1 = x_2$. Wir zeigen dass f surjektiv ist: sei $y \in Y$. Dann $f^{-1}(y) \in X$ und $f(f^{-1}(y)) = y$.

($\Longleftarrow$) Sei f bijektiv, und sei $y \in Y$. Lemma 1.3.13 shows that das Urbild $f^{-1}(y)$ genau ein Element enthält, wir nennen es $g(y)$. Das definiert eine Funktion $g\colon Y \to X$. Wir wollen zeigen, dass $f \circ g = \mathrm{id}_Y$ und $g \circ f = \mathrm{id}_X$. Sei $y \in Y$, dann $g(y) \in f^{-1}(y)$ so dass $f(g(y)) = y$. Das zeigt dass $f \circ g = \mathrm{id}_Y$. Sei $x \in X$, dann $x \in f^{-1}(f(x))$ so dass $x = g(f(x))$. Das zeigt, dass $g \circ f = \mathrm{id}_X$. □

1.4 Relationen

Siehe Analysis I.

1.5 Vollständige Induktion

Das Prinzip der Vollständige Induktion ist einfach, aber sehr wirkungsvoll

Prinzip der Vollständige Induktion. *Für jedes $n \in \mathbb{N}$ sei $\mathcal{A}(n)$ eine Aussage. Angenommen dass:*

- ***Induktionsanfang:*** *$\mathcal{A}(0)$ wahr ist,*
- ***Induktionsschritt:*** *für jedes $n \in \mathbb{N}$, wenn $\mathcal{A}(n)$ wahr ist, dann ist $\mathcal{A}(n+1)$ auch wahr:*

$$\mathcal{A}(n) \implies \mathcal{A}(n+1) \qquad \text{für alle } n \in \mathbb{N},$$

dann ist $\mathcal{A}(n)$ wahr für alle $n \in \mathbb{N}$. In dem Induktionsschritt die Annahme dass $\mathcal{A}(n)$ wahr ist heißt ***Induktionsvoraussetzung****.*

Wir zeigen jetzt mehrere Anwendungen und Beispielen:

Beispiel 1.5.1 (Summe der erste n Zahlen)**.** Wir zeigen dass

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \qquad \text{für alle } n \in \mathbb{N},$$

durch Induktion.

- **Induktionsanfang:** Für $n = 0$ die linke Seite ist 0, weil eine Summe von null Elemente, Null ist. Die rechte Seite ist auch 0, weil $\frac{0 \cdot 1}{2} = 0$. Die Aussage gilt für $n = 0$.

- **Induktionsschritt:** Nehmen wir an, dass die Aussage für n gilt. Wir wollen zeigen dass die Aussage für $n+1$ auch gilt:

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= (1+2+\cdots+n)+(n+1) \\ &= \frac{n(n+1)}{2}+(n+1) \qquad \text{(\textbf{Induktionsvoraussetzung})} \\ &= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+2)(n+1)}{2} \end{aligned}$$

  und das ist genau die Aussage für $n+1$.

Bemerkung 1.5.2. Es gibt Varianten des Prinzips der Vollständige Induktion. Z.B. für jedes $n \in \mathbb{N}$ sei $\mathcal{A}(n)$ eine Aussage. Angenommen dass

- $\mathcal{A}(n_0)$ gilt für ein $n_0 \in \mathbb{N}$,
- $\mathcal{A}(n) \implies \mathcal{A}(n+1)$ für alle $n \geq n_0$,

dann gilt $\mathcal{A}(n)$ für alle $n \geq n_0$.

Satz 1.5.1 (Bernoullische Ungleichung)**.** *Seien $x \in \mathbb{R}, x \geq 1$ und $n \in \mathbb{N}$. Dann*

$$(1+x)^n \geq 1+nx.$$

Ist zusätzlich $n \geq 2$ und $x \neq 0$, so gilt sogar

$$(1+x)^n > 1+nx.$$

Beweis. Wenn $n = 0$ oder $n = 1$, es ist klar dass $(1+x)^n = 1+nx$. Das ist auch klar, wenn $x = 0$. Wir müssen dann zeigen dass

$$(1+x)^n \geq 1+nx \qquad \text{für alle } x \geq -1, x \neq 0, \text{ und } n = 2$$

und wir zeigen das durch Induktion:

- **Induktionsanfang:** Für $n = 2$ gilt

$$(1+x)^2 = 1+2x+x^2 > 1+2x$$

  weil $x^2 > 0$ (hier ist wichtig dass $x \neq 0$).

- **Induktionsschritt:** Angenommen dass die Ungleichung für ein $n \geq 2$ gilt, wollen wir zeigen dass die für $n+1$ auch gilt:

$$(1+x)^{n+1} = (1+nx)^n(1+x) \geq (1+nx)(1+x) = 1+x+nx+nx^2 > 1+(n+1)x.$$

  Hier haben wir die Induktionsvoraussetzung $(1+nx)^n \geq 1+nx$ benutzt.

□

1.6 Mächtigkeit

Beispiel 1.6.1. Wir betrachten die zwei Mengen $S = \{$ Studierende im Horsaal $\}$ und $P = \{$ Plätze im Horsaal $\}$. Wann haben diese zwei Mengen die gleiche Anzahl von Elemente? Wir können entweder die Studierende und die Plätze Anzahlen. Oder wir können auch sagen dass jede Studierende ein Platz hat, zwei Studierende sitzen nicht am gleichen Platz, und dass alle Platze voll sind. Mathematisch gesagt, es gibt eine bijektive Funktion

$$p\colon S \to P, \qquad s \mapsto p(s) = \text{ platz von Studierende } s$$

Dieses kleines Beispiel fuhrt zu einen sehr wichtiges Konzept in der Mathematik:

Definition 1.6.2 (Gleichmächtige Menge)**.** Zwei Mengen X, Y sind gleichmächtig wenn es eine bijektive Funktion $f\colon X \to Y$ existiert.

Lemma 1.6.3. *Zwei Mengen X, Y sind gleichmächtig, genau dann, wenn sie gleich viele Elemente besitzen.*

Beweis. Wir zeigen die zwei Implikationen:

($\implies$) Sei $f\colon X \to Y$ eine bijektive Abbildung. Wir schreiben $X = x_1, \ldots, x_n$, mit paarweise verschiedene x_i, so dass X genau n Elemente hat. Da f surjektiv ist, $Y = f(X) = \{f(x_1), \ldots, f(x_n)\}$, und da f injektiv ist, die $f(x_i)$ sind auch paarweise verschiedene. Das bedeutet dass Y genau n Elemente hat.

($\impliedby$) Wenn X und Y beide n Elemente haben, dann $X = \{x_1, \ldots, x_n\}$ mit paarweise verschiedene x_i und $Y = \{y_1, \ldots, y_n\}$ mit paarweise verschiedene y_i. Wir definieren zwei Funktionen

$$f\colon X \to Y, \quad x_i \mapsto y_i, \quad g\colon y_i \to x_i$$

und wir sehen dass $f \circ g = \mathrm{id}_Y$ und $g \circ f = \mathrm{id}_X$. Das bedeutet dass f invertierbar ist, und deswegen bijektiv. □

Definition 1.6.4 (Mächtigkeit)**.** Sei M eine endliche Menge. Der Anzahl von Elemente in M ist auch die **Machtigkeit** oder Kardinalität von M genannt. Man schreibt $|M|$ für die Mächtigkeit.

Eine Menge M heißt **abzählbar unendlich**, wenn M gleichmächtig zu $\mathbb{N}$ ist.

Eine Menge M heißt **überabzählbar** wenn sie weder endlich oder abzählbar unendlich ist.

Beispiel 1.6.5. Die Menge $A = \{1, \sqrt{2}, \pi\}$ hat 3 Elemente, so dass $|A| = 3$.

Beispiel 1.6.6. In der Mengenlehre zeigt man dass $\mathbb{Z}$ und $\mathbb{Q}$ unendlich abzählbar sind, und dass $\mathbb{R}$ unendlich überabzählbar ist.

1.6.1 Fakultät und Binomialkoeffizienten

Definition 1.6.7 (Fakultät)**.** Sei $n \in \mathbb{N}$. Das Fakultät $n!$ (sprich "n Fakultät") ist definiert als

$$n! \coloneqq \begin{cases} 1, & \text{falls } n = 0, \\ 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n, & \text{falls } n > 0 \end{cases}$$

Bemerkung 1.6.8. Eine nützliche Konvention in der Mathematik ist dass die leere Summe 0 ist und dass das leeres Produkt 1 ist. Dann können wir auch schreiben

$$n! = n \cdot (n-1) \cdot \cdots \cdot 1 \qquad \text{für alle } n \in \mathbb{N}$$

weil wenn $n = 0$, das Produkt an der rechte Seite ein leeres Produkt ist, und ein leeres Produkt ist 1.

Definition 1.6.9 (Binomialkoeffizient)**.** Seien $n, k \in \mathbb{N}$. Das Binomialkoeffizient $\binom{n}{k}$ (sprich "n über k" oder "k aus n") ist definiert als

$$\binom{n}{k} := \begin{cases} 0, & \text{falls } k > n. \\ \dfrac{n!}{k!(n-k)!}, & \text{falls } k \leq n. \end{cases}$$

Lemma 1.6.10 (Eigenschaften des Binomialkoeffizientes)**.** *Seien $n, k \in \mathbb{N}$ mit $k \leq n$. Dann gilt:*

(a) $\binom{n}{0} = 1$ *und* $\binom{n}{1} = n$ *für alle* n.

(b) $\binom{n}{k} = \dfrac{n(n-1) \cdot \ldots \cdot (n-k+1)}{k!}$

(c) $\binom{n}{k} = \binom{n}{n-k}$.

(d) $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$.

Beweis. (a) Wir berechnen

$$\binom{n}{0} = \frac{n!}{0!n!} = \frac{n!}{1 \cdot n!} = 1, \quad \binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n}{1} = n.$$

(b) Wir berechnen

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(n-k)! \cdot (n-k+1) \cdot \ldots \cdot (n-1)n}{k!(n-k)!} = \frac{(n-k+1) \cdot \ldots \cdot (n-1) \cdot n}{k!}.$$

(c) Wir berechnen

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}.$$

(d) Wir berechnen

$$\begin{aligned}\binom{n}{k+1}+\binom{n}{k} &= \frac{n!}{(k+1)!(n-k-1)!}+\frac{n!}{k!(n-k)!}\\ &= \frac{n!}{(k+1)k!(n-k-1)!}+\frac{n!}{k!(n-k-1)!(n-k)} =\\ &= \frac{n!}{k!(n-k-1)!}\cdot\left(\frac{1}{k+1}+\frac{1}{n-k}\right)\\ &= \frac{n!}{k!(n-k-1)!}\cdot\frac{n-k+k+1}{(k+1)(n-k)} = \frac{n!}{k!(n-k-1)!}\cdot\frac{n+1}{(k+1)(n-k)}\\ &= \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}.\end{aligned}$$

□

Bemerkung 1.6.11. Die letze Gleichung im vorherigen Lemma lässt sich gut anhand des Pascalsches Dreieck veranschaulichen. Siehe Tafel oder Wikipedia: `https://de.wikipedia.org/wiki/Pascalsches_Dreieck`.

Binomialkoeffizienten und Faktorzahlen sind in der Kombinatorik allgegenwärtig.Ganz informell ist dies der Teil der Mathematik, der sich mit dem Abzählen von Objekten beschäftigt. Wir werden hier nicht viele Objekte zählen, aber wir können ein sehr einfaches, aber sehr wichtiges Prinzip aufstellen

Lemma 1.6.12. *Sei $f\colon X \to Y$ eine Funktion, dann*

$$X = \bigsqcup_{y\in Y} f^{-1}(y).$$

Das heißt: $X = \cup_{y\in Y} f^{-1}(y)$ und die $f^{-1}(y)$ sind paarweise disjunkt.

Beweis. Wir zeigen zuerst dass $X = \bigcup_{y\in Y} f^{-1}(y)$: seien $x \in X$ und $y = f(x)$. Dann $x \in f^{-1}(y)$. Wir zeigen jetzt, dass die $f^{-1}(y)$ paarweise disjunkt sind: sei $x \in f^{-1}(y) \cap f^{-1}(y')$, dann $y = f(x) = y'$. □

Korollar 1.6.13. *Sei $f\colon X \to Y$ eine Funktion zwischen endliche Menge. Dann*

$$|X| = \sum_{y\in Y} |f^{-1}(y)|.$$

Beweis. Lemma 1.6.12 zeigt dass $X = \sqcup_{y\in Y} f^{-1}(y)$, sodass $|X| = \sum_{y\in Y} |f^{-1}(y)|$. □

Korollar 1.6.14. *Seien X, Y endliche Menge. Dann $|X \times Y| = |X| \times |Y|$.*

Beweis. Wir betrachten die Abbildung $\mathrm{p}_X\colon X \times Y \to X$. Für jedes $x \in X$, gilt $|f^{-1}(x)| = |\{(x, y) \mid y \in Y\}| = |Y|$.

$$|X \times Y| = \sum_{x\in X} |p_X^{-1}(x)| = \sum_{x\in X} |Y| = |X| \cdot |Y|$$

□

Proposition 1.6.15. *Sei A eine endliche Menge mit $|A| = n$ und sei $k \in \mathbb{N}, k \geq 1$. Die Anzahl von k-Tupeln,*

$$(a_1, a_2, \ldots, a_k), \qquad a_i \in A, \quad a_i \text{ paarweise verschiedene,}$$

ist $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$.

Beweis. Sei $T_k(A) = \{(a_1, \ldots, a_k) \,|\, a_i \in A, a_i \text{ paarweise verschiedene }\}$. Wir wollen zeigen, dass

$$|T_k(A)| = n \cdot (n-1) \cdot \cdots \cdot (n-k+1)$$

Wenn $k > n$, dann $|T_k(A)| = 0$, weil $T_k(A) = \emptyset$ und $n \cdot (n-1) \ldots \cdot (n-k+1) = 0$, weil eine der Faktoren gleich 0 ist. Wir müssen dann die Aussage beweisen für alle $1 \leq k \leq n$. Wir zeigen sie durch Induktion auf k:

- **Induktionsanfang:** Wenn $k = 1$, dann hat $T_1(A) = \{(a_1) \,|\, a_1 \in A\}$ genau n Elemente.
- **Induktionsschritt:** Wir nehmen an, dass die Aussage fur $1 \leq k \leq n-1$ gilt und wir wollen zeigen dass es für $k+1$ gilt. Wir betrachten die Funktion

  $$f \colon T_{k+1}(A) \to T_k(A), \quad (a_1, \ldots, a_{k+1}) \mapsto (a_1, \ldots, a_k)$$

  (Warum ist diese Funktion wohldefiniert?). Korollar 1.6.13 zeigt dass

  $$|T_{k+1}(A)| = \sum_{t \in T_k(A)} |f^{-1}(t)|$$

  Sei $t = (a_1, \ldots, a_k) \in T_k(A)$. Dann $f^{-1}(t) = \{(a_1, \ldots, a_k, a_{k+1}) \,|\, a_{k+1} \notin A \setminus \{a_1, \ldots, a_k\}\}$, so dass $|f^{-1}(t)| = |A \setminus \{a_1, \ldots, a_k\}| = (n-k)$. Dann haben wir

  $$|T_{k+1}(A)| = \sum_{t \in T_k(A)} (n-k) = |T_k(A)| \cdot (n-k)$$

  und die **Induktionsvoraussetzung** zeigt dass $|T_k(A)| = n(n-1) \cdot (n-k+1)$. Am Ende haben wir

  $$|T_{k+1}(A)| = n(n-1) \cdot \ldots \cdot (n-k)$$

  und das ist genau was wir zeigen wollten.

□

Proposition 1.6.16. *Sei A eine endliche Menge mit n Elemente. Dann A hat genau $\binom{n}{k}$ Teilmenge mit k Elemente.*

Beweis. Für eine endliche Menge A schreibt man

$$\binom{A}{k} = \{B \subseteq A \,|\, B \text{ Teilmenge mit } k \text{ Elemente }\} = \{B \subseteq A \,|\, |B| = k\}\}$$

Wir wollen zeigen dass

$$\left|\binom{A}{k}\right| = \binom{n}{k}.$$

Wenn $k > n$, dann sind beide gleich 0. Wenn $k \leq n$, betrachten wir die Funktion

$$f\colon T_k(A) \to \binom{A}{k}, \quad (a_1, \ldots, a_k) \mapsto \{a_1, \ldots, a_k\}$$

(Warum ist die Funktion wohldefiniert?). Wir wollen Korollar 1.6.13 benutzen: sei $B \subseteq A$ eine Teilmenge mit $|B| = k$ Elemente. Dann $f^{-1}(B) = \{(b_1, \ldots, b_k) \,|\, b_i \in B \text{ paarweise verschiedene } \} = T_k(B)$, und Proposition 1.6.15 zeigt dass $|T_k(B)| = k!$. Dann Korollar 1.6.13 zeigt dass

$$|T_k(A)| = \sum_{B \in \binom{A}{k}} |f^{-1}(B)| = \sum_{B \in \binom{A}{k}} k! = \left|\binom{A}{k}\right| \cdot k!,$$

und dann

$$\begin{aligned} \left|\binom{A}{k}\right| &= \frac{|T_k(A)|}{k!} \\ &= \frac{n(n-1)\ldots(n-k+1)}{k!} && \text{(Prop. 1.6.15)} \\ &= \binom{n}{k} && \text{(Lemma 1.6.10.)} \end{aligned}$$

□

Bemerkung 1.6.17. Dieser Satz kann suggestiv wie folgt formuliert werden: sei A eine endliche Menge. Dann

$$\left|\binom{A}{k}\right| = \binom{|A|}{k}.$$

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ **Ende Vorlesung 23.04.2024** ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

Kapitel 2

Matrizen und das Gaußsches Verfahren

Wir haben zwei Beispiele von lineare Gleichungssysteme schon in der erste Vorlesung gesehen:

$$\begin{cases} h + k & = 40, \\ 2h + 4k & = 120. \end{cases}, \qquad \begin{cases} 2x + 3y - z + 4w - 5v = 10, \\ x - 2y + 3z - w + 2v = 5, \\ 3x + 2y - z + w - 4v = -3, \\ 4x - y + 2z + 3w + v = 8 \end{cases}$$

Man kann die einzige Lösung des erstes Systems relativ einfach berechnen: $h = 30, k = 10$. Was ist das bestes Weg, um das zweites System zu lösen? Gibt's uberhaupt Lösungen? In diesem Teil der Vorlesung, werden wir lineare Gleichungssysteme systematisch betrachten.

In diesem Kapitel werden wir das Symbol $\mathbb{K}$ für $\mathbb{R}$ verwenden, was bedeutet, dass $\mathbb{K} = \mathbb{R}$. Nachdem wir definiert haben, was ein Körper ist, werden wir sehen, dass die Ergebnisse des Kapitels für ein beliebiges Körper $\mathbb{K}$ gelten.

2.1 Gleichungssysteme, Vektoren, Matrizen

Die Gleichungssysteme oben sind bestimmt von den Koeffizienten von der Unbekannte und von den Werten das die Gleichungen. Wir organisieren diese Daten in Vektoren und Matrizen:

Definition 2.1.1 (Vektor)**.** Ein **Spaltenvektor** oder einfach **Vektor** in $\mathbb{K}^{m\times 1}$ ist ein Schema

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

mit **Koeffizienten** $b_i \in \mathbb{K}$. Die Koeffizienten b_i heißen auch **Koordinaten** von b.

Ein **Zeilenvektor** oder manchmal **Kovektor** in $\mathbb{R}^{1\times n}$ ist ein Schema

$$a = \begin{pmatrix} a_1 & a_2 & \dots & a_m \end{pmatrix}$$

mit Koeffizienten $a_j \in \mathbb{K}$. mit

Bemerkung 2.1.2. Beide Vektoren und Kovektoren sind Tupeln von Elementen in $\mathbb{K}$. Wir schreiben die Vektoren vertikal und die Kovektoren horizontal. In der Mathematik ist es üblich, die Elemente in $\mathbb{K}^m$ als Spaltenvektoren zu betrachten. **Ab jetzt, alle Elementen in $\mathbb{K}^m$ sind für uns Spaltenvektoren**:

$$b \in \mathbb{K}^m \iff b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \text{ mit } b_i \in \mathbb{K}.$$

Anders gesagt, $\mathbb{K}^m = \mathbb{K}^{m\times 1}$. Die Menge von Reihevektoren schreiben wir weiter als $\mathbb{K}^{1\times n}$.

Die **Summe** von zwei Vektoren $b, c \in \mathbb{K}^m$ ist definiert als

$$b + c = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} b_1 + c_1 \\ \vdots \\ b_m + c_m \end{pmatrix}$$

Fur jedes $\lambda \in \mathbb{K}$ und jeden Vektor $b \in \mathbb{K}^n$, definieren wir das Produkt $\lambda \cdot b$ als

$$\lambda \cdot b = \lambda \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} \lambda \cdot b_1 \\ \vdots \\ \lambda \cdot b_m \end{pmatrix}$$

Wir können auch die analogen Operationen für Zeilenvektoren definieren.

Definition 2.1.3 (Matrix)**.** Eine $m \times n$ Matrix mit Koeffizienten in $\mathbb{K}$ ist eine Schema $A \in \mathbb{K}^{m\times n} = \mathrm{Mat}(m \times n, \mathbb{K})$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad a_{ij} \in \mathbb{K}$$

mit m Zeilen und n Spalten.

Bemerkung 2.1.4. Vektoren sind Matrizen mit nur eine Spalte und Zeilenvektoren sind Matrizen mit nur eine Zeile.

Definition 2.1.5 (Matrix-Vektor-Produkt)**.** Seien $A \in \mathbb{K}^{m\times n}$ eine Matrix und $c \in \mathbb{K}^n$ ein Vektor. Wir definieren das Produkt $A \cdot c$ als

$$A \cdot c = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} a_{11} \cdot c_1 + a_{12} \cdot c_2 + \dots + a_{1n} \cdot c_n \\ a_{21} \cdot c_1 + a_{22} \cdot c_2 + \dots + a_{2n} \cdot c_n \\ \vdots \\ a_{m1} \cdot c_1 + a_{m2} \cdot c_2 + \dots + a_{mn} \cdot c_n \end{pmatrix}$$

Bemerkung 2.1.6. Um das Produkt $A \cdot c$ zu definiere, die Matrix A muss n Spalten haben und der Vektor c muss n Reihen haben: die Anzahl von Spalten von A und die Anzahl von Zeilen von c sind gleich. Z.B., das Produkt von einer 2×4 Matrix mit einem 3×1-Vektor ist nicht definiert.

Definition 2.1.7 (Lineares Gleichungssystem)**.** Seien $A = (a_{ij}) \in \mathbb{K}^{m\times n}$ eine Matrix und $b = (b_i) \in \mathbb{K}^m$ ein Vektor. Das lineares Gleichungssystem (LGS) von A und b ist besteht auf m lineare Gleichungen mit n Unbekannte oder Variablen:

$$LGS(A,b)\colon \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{cases}$$

mit $a_{ij}, b_i \in \mathbb{K}$. Wir köennen dieses System auch als

$$A \cdot x = b, \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

schreiben. Die Matrix A heißt **Koeffizientenmatrix** des Systems und die Matrix $(A|b) \in \mathbb{K}^{m\times(n+1)}$ heißt **erweiterte Koeffizientenmatrix**. Das LGS heißt **homogen** falls $b = 0$ und **inhomogen** falls $b \neq 0$.

Die **Menge von Lösungen** des Systems ist die Menge von alle Vektoren $x \in \mathbb{K}^n$ die alle Gleichungen erfüllen:

$$\mathrm{Los}(A,b) = \{x \in \mathbb{K}^n \mid Ax = b\}.$$

Bemerkung 2.1.8. Ein homogenes system hat immer die Lösung $x = 0$: $A \cdot 0 = 0$ für alle $A \in \mathbb{K}^{m\times n}$.

2.2 Die Zeilenstufenform

Beispiel 2.2.1. Wir wollen alle Lösungen des folgendes LGS bestimmen:

$$\begin{cases} x_1 + x_2 + 3x_5 &= -6 \\ x_3 + 5x_5 &= -10\,. \\ x_4 - x_5 &= 2 \end{cases} \tag{2.2.1}$$

Das ist sehr einfach: dieses System ist äquivalent zu

$$\begin{cases} x_1 &= -x_2 - 3x_5 - 6 \\ x_3 &= -5x_5 - 10 \\ x_4 &= x_5 + 2 \end{cases}$$

so dass die Menge von Lösungen des LGSs ist:

$$\mathrm{Los} = \left\{ \begin{pmatrix} -x_2 - 3x_5 - 6 \\ x_2 \\ -5x_5 - 10 \\ x_5 + 2 \\ x_5 \end{pmatrix} \mid x_2, x_5 \in \mathbb{K} \right\}$$

. Das nennt man eine **Parametrisierung** der Lösungsmenge: die Lösungen sind parametrisiert von den "freie" Variabeln x_2, x_5.

Beispiel 2.2.2. Wir betrachten jetzt das LGS

$$\begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_1 + x_2 + x_3 + 8x_5 & = -16 \\ x_1 + x_2 + x_3 + 2x_4 + 6x_5 & = -12 \end{cases}$$

Wir können dieses System nicht sofort lösen. Wenn wir jedoch die erste Gleichung von der zweiten und dritten Gleichung subtrahieren, erhalten wir

$$\begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_1 + x_2 + x_3 + 8x_5 & = -16 \\ x_1 + x_2 + x_3 + 2x_4 + 6x_5 & = -12 \end{cases} \iff \begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_3 + 5x_5 & = -10 \\ x_3 + 2x_4 + 3x_5 & = -6 \end{cases}$$

Dies ist eine Äquivalenz, denn um vom zweiten System zum ersten überzugehen, genügt es, die erste Gleichung mit der zweiten und der dritten zu addieren. Nun können wir Nun können wir die zweite Gleichung von der dritten subtrahieren (was ebenfalls eine umkehrbare Operation ist) und erhalten

$$\begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_3 + 5x_5 & = -10 \\ x_3 + 2x_4 + 3x_5 & = -6 \end{cases} \iff \begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_3 + 5x_5 & = -10 \\ 2x_4 - 2x_5 & = 4 \end{cases}$$

Nun können wir die dritte Gleichung mit $\frac{1}{2}$ multiplizieren (ebenfalls eine umkehrbare Operation) und erhalten

$$\begin{cases} x_1 + x_2 + 3x_5 & = -6 \\ x_3 + 5x_5 & = -10 \\ 2x_4 - 2x_5 & = 4 \end{cases} \iff \begin{cases} x_1 + x_2 - x_5 & = -4 \\ x_3 + 5x_5 & = -12 \\ x_4 - x_5 & = 2 \end{cases}$$

Wir haben das System (2.2.1) wieder gefunden. Wir hatten also ein erstes System, das sehr einfach zu lösen war, und ein weiteres System, das wir als äquivalent zum ersten System zeigen konnten. In diesem Kapitel werden wir sehen, dass jedes lineare System einem äquivalenten System entspricht, das sehr einfach zu lösen ist.

Die Tatsache, dass das erste lineare System sehr einfach zu lösen ist, ist auf seine Form zurückzuführen: die erweiterte Koeffizientenmatrix ist in reduzierter Zeilenstufenform:

$$(A \mid b) = \begin{pmatrix} 1 & 1 & 0 & 0 & 3 & -6 \\ 0 & 0 & 1 & 0 & 5 & -10 \\ 0 & 0 & 0 & 1 & -1 & 2 \end{pmatrix},$$

Definition 2.2.3 (Zeilenstufenform)**.** Eine Matrix $A = (a_{ij}) \in \mathbb{K}^{m \times n}$ hat **Zeilenstufenform**, falls es Zahlen r mit $0 \leq r \leq n$ und $j_1, j_2, \ldots, j_r$ mit $1 \leq j_1 < j_2 < \cdots < j_r \leq n$ gibt, so daß:

(a) $a_{ij} = 0$ für alle $i \leq r$ und $j < j_i$.

(b) $a_{ij} = 0$ für alle $i > r$ und alle j.

(c) $a_{ij_i} \neq 0$ für alle $i = 1, \ldots, r$.

Die Zahl r heißt der **Rang** der Matrix in Zeilenstufenform: wir schreiben $r = \mathrm{rk}(A)$. die Zahlen $a_{ij_i} \neq 0$ heißen **Pivots**.

$$A = \begin{pmatrix} 0 & \dots & 0 & a_{1j_1} & * & * & * & * & \dots & * & * & * & \dots & * & * & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & a_{2j_2} & * & \dots & * & * & * & \dots & * & * & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \dots & 0 & a_{3j_3} & * & \dots & * & \dots & * \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & a_{rj_r} & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

Die Matrix A hat **reduzierte Zeilenstufenform** wenn sie Zeilenstufenform hat, und außerdem

(d) alle Pivots sind 1: $a_{ij_i} = 1$ für alle $i = 1, \dots, r$.

(e) alle Koeffizienten oben die Pivots sind 0: $a_{hj_i} = 0$ für alle $i = 1, \dots, r$ und $h < i$.

$$A = \begin{pmatrix} 0 & \dots & 0 & 1 & * & * & 0 & * & \dots & * & * & 0 & \dots & * & 0 & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 1 & * & \dots & * & * & 0 & \dots & * & 0 & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \dots & 0 & 1 & * & \dots & 0 & \dots & * \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

Bemerkung 2.2.4. Jetz haben wir der Rang definiert nur für eine Matrix in Zeilenstufenform. Wir werden später der Rang für alle Matrizen definieren.

Proposition 2.2.5 (Lösungen von LGS in reduzierte Zeilenstufenform)**.** *Wir betrachten ein LGS* $\{Ax = b\}$ *mit erweiterte Koeffizientenmatrix* $(A|b)$ *in reduzierte Zeilenstufenform.*

(a) Die Koeffizientenmatrix A hat reduzierte Zeilenstufenform, und die Pivots von A sind auch Pivots von $(A|b)$*. Insbesondere* $\mathrm{rk}(A) \leq \mathrm{rk}(A|b) \leq \mathrm{rk}(A) + 1$.

(b) Wenn $\mathrm{rk}(A) \neq \mathrm{rk}(A|b)$*, dann* $\mathrm{Los}(A, b) = \emptyset$.

(c) Wenn $\mathrm{rk}(A) = \mathrm{rk}(A|b)$*, dann hat* $\mathrm{Los}(A, b)$ *eine Parametrisierung, bei der die Variablen, die den Spalten der Pivots entsprechen, durch die Variablen der anderen Spalten ausgedrückt werden können.*

Beweis. (a) Hausaufgabe.

(b) Wenn $\mathrm{rk}(A) \neq \mathrm{rk}(A|b)$, dann $\mathrm{rk}(A|b) = \mathrm{rk}(A) + 1$. Sei $r = \mathrm{rk}(A)$. Dann ist die $(r+1)$-te Zeile von A Null aber die $(r+1)$-te Zeile von $(A|b)$ ist nicht Null. Dann ist die $(r+1)$-te Gleichung

$$0 \cdot x_1 + \dots + 0 \cdot x_n = b_{r+1}$$

mit $b_{r+1} \neq 0$. Diese Gleichung hat keine Lösungen.

(c) Wenn $\mathrm{rk}(A) = \mathrm{rk}(A|b)$, dann sind alle Pivots von $(A|b)$ auch Pivots von A. Sei $A \in \mathbb{K}^{m\times n}$ und seien $a_{1j_1}, \ldots, a_{rj_r}$ die Pivots von A, mit $1 \leq j_1 < \cdots < j_r \leq n$. Das LGS von $(A|b)$ ist:

$$\begin{cases} a_{1j_1}x_{j_1} + \sum_{k=j_1+1}^{n} a_{1k}x_k & = b_1 \\ a_{2j_2}x_{j_2} + \sum_{k=j_2+1}^{n} a_{2k}x_k & = b_2 \\ \vdots & \\ a_{rj_r}x_{j_r} + \sum_{k=j_r+1}^{n} a_{rk}x_k & = b_r \end{cases}$$

Da $(A|b)$ reduzierte Zeilenstufenform hat, $a_{ij_i} = 1$ für alle $i = 1, \ldots, r$, und $a_{hj_i} = 0$ für alle $i = 1, \ldots, r$ und $h < i$. Sei $F = \{\{1, \ldots, n\} \setminus \{j_1, j_2, \ldots, j_r\}$. Wir können das LGS wie folgt schreiben:

$$\begin{cases} x_{j_1} & = -\sum_{k\in F}^{n} a_{1k}x_k + b_1 \\ x_{j_2} & = -\sum_{k\in F}^{n} a_{2k}x_k + b_2 \\ \vdots & \\ x_{j_r} & = -\sum_{k\in F}^{n} a_{rk}x_k + b_r \end{cases}$$

und das ist eine Parametrisierung der Menge der Lösungen $\mathrm{Los}(A, b)$.

□

Bemerkung 2.2.6. Diese Proposition zeigt, dass es sehr einfach ist, die Lösung eines Systems in reduzierter Zeilenstufenform zu parametrisieren. Wenn wir also ein lineares System in reduzierte Zeilenstufenform bringen können, können wir es auch lösen. Dies ist immer möglich,und wir sehen das in der nächsten Sektion.

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ **Ende Vorlesung 26.04.2024** ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

2.3 Elementare Zeilenunformungen und das Gauß-Verfahren

Definition 2.3.1 (Elementare Zeilenumformungen)**.** Die elementare Zeilenumformungen in einer Matrix sind:

(GZ_1) Vertauschen zweier Zeilen.

(GZ_2) Addition des λ-fachen einer Zeile zu einer andere, verschiedene Zeile, $\lambda \in \mathbb{K}$.

(GZ_3) Multiplikation einer Zeile mit $\lambda \in \mathbb{K}, \lambda \neq 0$.

Proposition 2.3.2. *Entsteht $(A'|b')$ aus $(A|b)$ durch endlich viele elementare Zeilenunformungen, so ist*

$$\mathrm{Los}(A, b) = \mathrm{Los}(A', b')$$

Beweis. Dank der Induktion, es genugt, die Aussage für eine einzelne elementare Zeitumformung zu Zeigen. Wir nehmen also an, $(A'|b')$ entsteht aus $(A|b)$ durch eine elementare Zeilenumformung vom Typ:

(GZ_1) Die zwei Systeme $\{Ax = b\}$ und $\{A'x = b'\}$ haben die selbe Gleichungen, nur in einer anderen Reihenfolge.

(GZ_2) Nehmen wir an, dass die h-te Zeile von $(A'|b')$ die Summe des h-te Zeile von $(A|b)$ und des λ-fachen der k-te Zeile von $(A|b)$ ist. Alle Zeilen außer h und k bleiben unverändert. Es genugt, daher, zu zeigen, daß die Lösungsmengen von

$$\begin{cases} a_{h1}x_1 + \cdots + a_{hn}x_n &= b_h \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= b_k \end{cases}, \quad \text{und} \quad \begin{cases} (a_{h1} + \lambda a_{k1})x_1 + \cdots + (a_{hn} + \lambda a_{kn})x_n &= b_h + \lambda b_k \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= b_k \end{cases},$$

gleich sind. Addiert man ein λ-Vielfaches der zweiten Gleichung links zur ersten Gleichung links, so erhält man das System rechts. Somit ist jede Lösung des linken Systems auch eine Lösung des rechten Systems. Umgekehrt erhält man das linke System, wenn man ein λ-Vielfaches der zweiten Gleichung auf der rechten Seite von der ersten Gleichung auf der rechten Seite subtrahiert. Somit ist jede Lösung des rechten Systems auch eine Lösung des linken Systems.

(GZ_3) Nehmen wir an, dass die h-te Zeile von $(A'|b')$ das λ-Vielfaches der h-the Zeile von $(A|b)$ ist, mit $\lambda \in \mathbb{K}, \lambda \neq 0$. Dann, analog zu ($GZ_2$), müssen wir zeigen dass die zwei Gleichungen

$$a_{h1}x_1 + \cdots + a_{hn}x_n = b_h, \quad \text{und} \quad \lambda a_{h1}x_1 + \cdots + \lambda a_{hn}x_n = \lambda b_h$$

die gleiche Lösungen haben. Multipliziert man jedoch die erste Gleichung mit λ, erhält man die erste Gleichung, und multipliziert man die zweite Gleichung mit λ^{-1} (existiert weil $\lambda \neq 0$), erhält man die erste Gleichung. Dann haben die beiden Gleichungen die gleichen Lösungen.

□

Das folgende Satz ist grundlegend für die lineare Algebra

Satz 2.3.1 (Gaußches Eliminationsverfahren)**.** *Jede Matrix A läßt sich durch endliche viele elementare Zeilenumformungen vom Typ (GZ_1) und (GZ_2) auf Zeilenstufenform bringen, mit (GZ_1),(GZ_2) und (GZ_3) sogar auf reduzierte Zeilenstufenform.*

Beweis. Der Beweis ist konstruktiv, durch das Gaußsches Eliminationsverfahren. Sei $A \in \mathbb{K}^{m\times n}$ eine Matrix. Ist $A = 0$, so ist A schon auf reduzierte Zeilenstufenform. Für den allgemeinen Fall beweisen wir zunächst, dass die Matrix in die Zeilenstufenform gebracht werden kann. Wenn $m = 1$ so das A nur eine Zeile hat, so ist A schon in Zeilenstufenform. Wenn $m > 1$, führen wir die Schritte des **Gaußsches Eliminationsverfahren** durch:

- **Schritt 1.**: Die Spalten von links nach rechts durchgehen, bis die erste Spalte A^{j_1} , die nicht Null ist, gefunden wird.
- **Schritt 2.**: Zwei Zeilen vertauschen (Zeilenumformung (GZ_1)), so dass das Element am Anfang der Spalte A^{j_1} ungleich Null ist. Sei A' die neue Matrix. Dann $a'_{1j_1} \neq 0$.

$$A \longrightarrow A' = \begin{pmatrix} 0 & 0 & \dots & 0 & a'_{1j_1} & * & * & \dots & * \\ 0 & 0 & \dots & 0 & a'_{2j_1} & * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & a'_{mj_1} & * & * & \dots & * \end{pmatrix}$$

- **Schritt 3.**: Für alle $i > 1$, subtrahiere von der i-ten Zeile von A' das $\frac{a_{ij_1}}{a_{1j_1}}$-Vielfache der ersten Zeile (GZ_2), so dass alle Einträge unter a_{1,j_1} zu Null werden. Sei A'' die neue Matrix:

$$A' \longrightarrow A'' = \begin{pmatrix} 0 & 0 & \dots & 0 & a'_{1j_1} & * & * & \dots & * \\ 0 & 0 & \dots & 0 & 0 & * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & * & * & \dots & * \end{pmatrix}$$

Sei A_1 die $(m-1) \times (n-j_1+1)$ Matrix unter rechts von a_{1j_1} (siehe Tafel). Wenn A_1 in Zeilenstufenform ist, dann ist die ganze Matrix A'' in Zeilenstufenform auch. Wenn A_1 nicht in Zeilenstufenform ist, das Gauß-verfahren wiederholen. Da die erste Matrix m Zeilen hat, müssen wir den Algorithmus höchstens $m-1$ mal wiederholen, bis wir fertig sind (eine Matrix mit nur einer Zeile ist bereits in Zeilenstufenform).

Sobald die Matrix in Zeilstufenform ist, können wir die Zeile des Pivots a_{ij_i} mit $a_{ij_1}^{-1}$ multiplizieren (dies ist möglich, weil $a_{ij_i} \neq 0$), so dass die Pivots eins werden. Danach können wir Schritt 3 wiederholen, aber diesmal mit den Zeilen oberhalb der Pivots. Dadurch wird die Matrix von einer Zeilenstufenform zu einer reduzierten Zeilenstufenform □

Beispiel 2.3.3. Wir wenden den Algorithmus auf die folgende Matrix an:

$$\begin{pmatrix} 0 & 0 & 2 & 3 \\ 0 & 1 & 4 & 5 \\ 0 & 2 & 6 & 7 \end{pmatrix} \xrightarrow{Z1 \leftrightarrow Z2} \begin{pmatrix} 0 & 1 & 4 & 5 \\ 0 & 0 & 2 & 3 \\ 0 & 2 & 6 & 7 \end{pmatrix} \xrightarrow{Z3 \to Z3 - 2 \cdot Z1} \begin{pmatrix} 0 & 1 & 4 & 5 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & -2 & -3 \end{pmatrix} \xrightarrow{Z3 \to Z3 + Z2} \begin{pmatrix} 0 & 1 & 4 & 5 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Dies bringt die Matrix in Zeilenstufenform. Um es in reduzierte Zeilstufenform zu bringen gehen wir weiter:

$$\begin{pmatrix} 0 & 1 & 4 & 5 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{Z2 \to \frac{1}{2} \cdot Z2} \begin{pmatrix} 0 & 1 & 4 & 5 \\ 0 & 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{Z1 \to Z1 - 4 \cdot Z2} \begin{pmatrix} 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Dank dieses Algorithmus haben wir eine allgemeine Methode zur Lösung linearer Systeme: Wir bringen die erweiterte Koeffizientenmatrix in eine reduzierte Zeilenstufenform und verwenden dann die Proposition 2.2.5. Wenn wir nur wissen wollen, ob ein System Lösungen hat oder nicht, reicht es eigentlich aus, eine Zeilenstufenform zu berechnen:

Lemma 2.3.4. *Ein LGS mit erweiterte Koeffizientenmatrix $(A|b)$ in Zeilenstufenform hat eine Losung genau dann, wenn* $\mathrm{rk}(A) = \mathrm{rk}(A|b)$.

Beweis. Der gleiche Beweis (Aufgabe) wie in Satz 2.2.5 zeigt, dass wenn $(A|b)$ Zeilenstufenform hat, dann hat auch A Zeilenstufenform, so dass es sinnvoll ist, von ihren Rängen zu sprechen[1]. Wir können den Algorithmus von Gauß verwenden, um die Matrix $(A|b)$ in eine andere Matrix (A'—b') in reduzierter Zeilenstufenform zu bringen. Betrachtet man den Algorithmus, so sieht man, dass die Pivots von $(A|b)$ die gleichen sind wie die Pivots von $(A'|b')$, also $\mathrm{rk}(A) = \mathrm{rk}(A')$ und $\mathrm{rk}(A|b) = \mathrm{rk}(A'|b')$. Proposition 2.3.2 zeigt, dass $\mathrm{Los}(A,b) \neq \emptyset$ genau dann, wenn $\mathrm{Los}(A',b') \neq \emptyset$, und Satz 2.2.5 zeigt, dass $\mathrm{Los}(A',b') \neq \emptyset$ genau dann, wenn $\mathrm{rk}(A') = \mathrm{rk}(A'|b')$. Da $\mathrm{rk}(A') = \mathrm{rk}(A)$ und $\mathrm{rk}(A|b) = \mathrm{rk}(A'|b')$, ist dies äquivalent zu $\mathrm{rk}(A|b) = \mathrm{rk}(A'|b')$. □

[1]In der Zukunft werden wir sehen, wie man den Rang einer beliebigen Matrix definiert, aber im Moment haben wir ihn nur für die Matrizen in Zeilenstufenform definiert

Bemerkung 2.3.5 (Lösung eines LGS)**.** Wir fassen zusammen, wie man ein lineares System mit dem Gauß-Algorithmus löst:

- Schritt 1.: Die erweiterte Koeffizientenmatrix $(A|b)$ in Zeilenstufenform bringen.
- Schritt 2.: Wenn $\mathrm{rk}(A) \neq \mathrm{rk}(A|b)$, dann $\mathrm{Los}(A|b) = \emptyset$.
- Schritt 3.: Wenn $\mathrm{rk}(A) = \mathrm{rk}(A|b)$, dann die erweiterte Koeffizientenmatrix $(A|b)$ in reduzierte Zeilenstufenform bringen, und die Lösungen durch Proposition 2.2.5 bestimmen.

Beispiel 2.3.6. Wir anwenden das Algorithmus fürs LGS

$$\begin{cases} x + 2y - 2z &= -15 \\ 2x + y - 5z &= -21 \\ x - 4y + z &= 18 \end{cases}$$

Wir bringen die erweiterte Koeffizientenmatrix in Zeilenstufenform:

$$(A|b) = \left(\begin{array}{ccc|c} 1 & 2 & -2 & -15 \\ 2 & 1 & -5 & -21 \\ 1 & -4 & 1 & 18 \end{array}\right) \xrightarrow[Z3 \to Z3 - Z1]{Z2 \to Z2 - 2\cdot Z1} \left(\begin{array}{ccc|c} 1 & 2 & -2 & -15 \\ 0 & -3 & -1 & 9 \\ 0 & -6 & 3 & 33 \end{array}\right)$$
$$\xrightarrow{Z3 \to Z3 - 2\cdot Z2} \left(\begin{array}{ccc|c} 1 & 2 & -2 & -15 \\ 0 & -3 & -1 & 9 \\ 0 & 0 & 5 & 15 \end{array}\right)$$

Die erweiterte Koeffizientenmatrix ist jetzt in Zeilenstufenform und hat Rang 3. Die Koeffizientenmatrix hat auch Rang 3, sodass Lösungen existieren. Um alle Lösungen zu bestimmen, bringen wir die erweiterte Koeffizientenmatrix in reduzierte Zeilenstufenform:

$$\left(\begin{array}{ccc|c} 1 & 2 & -2 & -15 \\ 0 & -3 & -1 & 9 \\ 0 & 0 & 5 & 15 \end{array}\right) \xrightarrow{Z3 \to \frac{1}{5} Z3} \left(\begin{array}{ccc|c} 1 & 2 & -2 & -15 \\ 0 & -3 & -1 & 9 \\ 0 & 0 & 1 & 3 \end{array}\right) \xrightarrow[Z1 \to Z1 + 2\cdot Z3]{Z2 \to Z2 + Z3} \left(\begin{array}{ccc|c} 1 & 2 & 0 & -9 \\ 0 & -3 & 0 & 12 \\ 0 & 0 & 1 & 3 \end{array}\right)$$
$$\xrightarrow{Z2 \to -\frac{1}{3} Z2} \left(\begin{array}{ccc|c} 1 & 2 & 0 & -9 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 3 \end{array}\right) \xrightarrow{Z1 \to Z1 - 2\cdot Z2} \left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Das LGS hat jetzt reduzierte Zeilenstufenform

$$\begin{cases} x_1 &= -1 \\ x_2 &= -4 \\ x_3 &= 3. \end{cases}$$

sodass das System eine einzige Lösung hat:

$$\mathrm{Los} = \left\{ \begin{pmatrix} -1 \\ -4 \\ 3 \end{pmatrix} \right\}$$

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ **Ende Vorlesung 30.04.2024** ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

Beispiel 2.3.7. Für welche $b \in \mathbb{R}^3$ hat das LGS

$$\begin{cases} x + 2y + 3z &= b_1 \\ 4x + 5y + 6z &= b_2 \\ -2x - y &= b_3 \end{cases}$$

eine Lösung? Wir können diese Frage mit Hilfe des Gauß-Algorithmus beantworten: Wir bringen zuerst die erweiterte Koeffizientenmatrix in Zeilenstufenform

$$\begin{pmatrix} 1 & 2 & 3 & | & b_1 \\ 4 & 5 & 6 & | & b_2 \\ -2 & -1 & 0 & | & b_3 \end{pmatrix} \xrightarrow[Z3 \mapsto Z3+2\cdot Z1]{Z2 \mapsto Z2-4\cdot Z1} \begin{pmatrix} 1 & 2 & 3 & | & b_1 \\ 0 & -3 & -6 & | & b_2 - 4b_1 \\ 0 & 3 & 6 & | & b_3 + 2b_1 \end{pmatrix}$$
$$\xrightarrow{Z3 \to Z3+Z2} \begin{pmatrix} 1 & 2 & 3 & | & b_1 \\ 0 & -3 & -6 & | & b_2 - 4b_1 \\ 0 & 0 & 0 & | & b_3 + b_2 - 2b_1 \end{pmatrix}$$

Diese Matrix hat Zeilenstufenform, und wir sehen dass die Koeffizientenmatrix hat Rang 2. Die erweiterte Koeffizientenmatrix hat Rang 2 genau dann, wenn $b_3 + b_2 - 2b_1 = 0$. Hence, das LGS hat eine Lösung genau dann, wenn $b_3 + b_2 - 2b_1 = 0$.

In diesem Fall können wir auch alle Lösungen beschreiben: wir bringen die erweiterte Koeffizientenmatrix in reduzierte Zeilenstufenform (die dritte Zeile ist Null und wir koennen sie ignorieren)

$$\begin{pmatrix} 1 & 2 & 3 & | & b_1 \\ 0 & -3 & -6 & | & -4b_1 + b_2 \end{pmatrix} \xrightarrow{Z2 \mapsto -\frac{1}{3} Z2} \begin{pmatrix} 1 & 2 & 3 & | & b_1 \\ 0 & 1 & 2 & | & \frac{4}{3}b_1 - \frac{1}{3}b_2 \end{pmatrix}$$
$$\xrightarrow{Z1 \mapsto Z1-2\cdot Z2} \begin{pmatrix} 1 & 0 & -1 & | & -\frac{5}{3}b_1 + \frac{2}{3}b_2 \\ 0 & 1 & 2 & | & \frac{4}{3}b_1 - \frac{1}{3}b_2 \end{pmatrix}$$

Das System hat jetzt die Form

$$\begin{cases} x &= z - \frac{5}{3}b_1 + \frac{2}{3}b_2 \\ y &= -2z + \frac{4}{3}b_1 - \frac{1}{3}b_2 \end{cases}$$

und die Lösungsmenge ist

$$\text{Los} = \left\{ \begin{pmatrix} z - \frac{5}{3}b_1 + \frac{2}{3}b_2 \\ -2z + \frac{4}{3}b_1 - \frac{1}{3}b_2 \\ z \end{pmatrix} \mid z \in \mathbb{R} \right\}$$

Bemerkung 2.3.8. Wir haben gesehen, dass wir jedes lineare Gleichungssystem über $\mathbb{R}$ mit dem Gauß-Algorithmus lösen können, insbesondere mithilfe der drei Zeilenoperationen. Gibt es etwas Besonderes an den reellen Zahlen? Wenn wir uns die Zeilenoperationen ansehen, stellen wir fest, dass was wir brauchen ist das wir zwei reelle Zahlen a, b addieren und multiplizieren können, um andere reelle Zahlen $a + b$ und $a \cdot b$ zu erhalten. Außerdem, brauchen wir dass jede von null verschiedene reelle Zahl $a \neq 0$ eine multiplikative Inverse $\frac{1}{a}$ besitzt, die wiederum eine reelle Zahl ist. Diese Eigenschaften gelten auch für die rationalen Zahlen $\mathbb{Q}$, aber zum Beispiel gilt die letzte nicht für die ganzen Zahlen $\mathbb{Z}$. Die allgemeine Struktur, die diese Eigenschaften ermöglicht, ist die eines Körpers, den wir im nächsten Kapitel kennenlernen werden.

Kapitel 3

Vektorräume

3.1 Abelsche Gruppe, Ringe, Körpern

Definition 3.1.1 (Abelsche Gruppe)**.** Eine abelsche Gruppe ist eine Menge A zusammen mit einer Verknüpfung

$$+ \colon A \times A \to A, \qquad (a, b) \mapsto a + b$$

mit den folgenden Eigenschaften:

- **Assoziativität:** $a + (b + c) = (a + b) + c$ für alle $a, b, c \in A$.
- **Neutrales Element:** Es gibt ein Element $0 \in A$ so, dass $a + 0 = 0 + a = a$ für alle $a \in A$ gilt.
- **Inverses Element:** Für jedes $a \in A$ gibt es ein Element $a' \in A$ so, dass $a + a' = a' + a = 0$ gilt. Man schreibt $a' = -a$.
- **Kommutativität:** $a + b = b + a$ für alle $a, b \in A$.

Wir bezeichnen eine solche Gruppe mit $(A, +)$ oder manchmal nur mit A, wenn die Verknüpfung $+$ klar ist.

Bemerkung 3.1.2. Eine Menge A mit einer Verknüpfung, die die ersten drei Eigenschaften erfüllt, nennt man eine Gruppe. Eine abelsche Gruppe ist eine Gruppe, deren Verknüpfung kommutativ ist.

Bemerkung 3.1.3. Wenn $(A, +)$ eine abelsche Gruppe ist, sagt uns die Assoziativität, dass $(a + b) + c = a + (b + c)$ für alle $a, b, c \in A$. Insbesondere können wir dieses Element einfach als $a + b + c$ bezeichnen. Auf die gleiche Weise können wir $a_1 + a_2 + \cdots + a_n$ für jede endliche Sammlung von Elementen $a_i \in A, i = 1 \ldots, n$ definieren. Als weitere Notation schreiben wir $a - b$ für $a + (-b)$.

In der Definition der Gruppe fragen wir nach der Existenz eines neutralen Elements und eines inversen Elements. Tatsächlich sind diese Elemente, falls sie existieren, eindeutig bestimmt:

Lemma 3.1.4. *Sei $(A, +)$ eine abelsche Gruppe.*

1. *Das neutrale Element ist eindeutig bestimmt: Wenn $0, 0' \in A$ zwei neutrale Elemente sind, dann gilt $0 = 0'$.*

2. *Das inverse Element ist eindeutig bestimmt: Wenn a', a'' zwei inverse Elemente von $a \in A$ sind, dann gilt $a' = a''$.*

Beweis. 1. Nach der Definition eines neutralen Elements: $0 = 0 + 0' = 0'$.

2. Wir nutzen die Eigenschaften einer Gruppe:

$$\begin{aligned} a' &= a' + 0 && \text{(Neutrales Element)} \\ &= a' + (a + a'') && \text{(Inverses Element)} \\ &= (a' + a) + a'' && \text{(Assoziativität)} \\ &= 0 + a'' && \text{(Inverses Element)} \\ &= 0 + a'' = a''. && \text{(Neutrales Element)} \end{aligned}$$

Hier haben wir explizit erwähnt, wo wir die Eigenschaften der Gruppenoperation verwendet haben. In Zukunft werden wir nicht so explizit sein und die Eigenschaften nicht mehr explizit erwähnen.

□

Beispiel 3.1.5. Die Mengen der ganzen Zahlen $\mathbb{Z}$, rationalen Zahlen $\mathbb{Q}$ und reellen Zahlen $\mathbb{R}$ mit der üblichen Addition bilden abelsche Gruppen $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$. Die Menge der natürlichen Zahlen $\mathbb{N}$ mit der üblichen Addition bildet keine Gruppe, da es kein additives Inverses gibt: z.B. $-1 \notin \mathbb{N}$.

Beispiel 3.1.6. Die Mengen der nicht nullen reellen Zahlen $\mathbb{R}^\times = \mathbb{R} \setminus 0$ mit der Multiplikation $(\mathbb{R}^\times, \cdot)$ und die Menge der nicht nullen rationalen Zahlen $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ mit der Multiplikation $(\mathbb{Q}^\times, \cdot)$ bilden ebenfalls abelsche Gruppen. Die Menge der nicht nullen ganzen Zahlen mit der Multiplikation ist jedoch keine Gruppe: Es fehlt das inverse Element, z.B. $\frac{1}{2} \notin \mathbb{Z}$.

Bemerkung 3.1.7. Wie das vorherige Beispiel zeigt, ist das Symbol + für die Operation in einer abelschen Gruppe nur eine Konvention. Manchmal kann die Operation durch andere Symbole angegeben werden, wie z.B. in $(\mathbb{Q}^\times, \cdot)$. Wenn wir von einer allgemeinen abelschen Gruppe sprechen, werden wir weiterhin die Notation + verwenden, aber wenn wir mit expliziten Beispielen umgehen, ist es wichtig zu beachten, was die Operation ist.

Wir geben einige grundlegende Eigenschaften abelscher Gruppen an, die zeigen, dass sie sich in vielen Aspekten wie die Gruppe der ganzen Zahlen $\mathbb{Z}$ verhalten.

Lemma 3.1.8. *Sei $(A, +)$ eine abelsche Gruppe.*

1. *Für alle $a, b \in A$ gilt $-(a + b) = -a - b$ und $-(-a) = a$.*
2. *Für alle $a, b, c \in A$ gilt $a + b = c$ genau dann, wenn $a = c - b$. Insbesondere gilt $a + c = b + c$ genau dann, wenn $a = b$.*
3. *Für jedes $n \in \mathbb{N}$ und $a \in A$ definieren wir*

$$n \cdot a = a + a + \cdots + a \quad (n \text{ mal}), \quad (-n) \cdot a = (-a) + (-a) + \cdots + (-a) \quad (n \text{ mal})$$

Dann gilt

$$(-1) \cdot a = (-a), \quad (n + m) \cdot a = n \cdot a + m \cdot a, \quad n \cdot (m \cdot a) = (n \cdot m) \cdot a$$

Beweis. 1. Um zu zeigen, dass $-(a+b) = -a-b$ gilt, müssen wir beweisen, dass $(a+b)+(-a-b) = 0$, aber $a+b-a-b = a-a+b-b = 0+0 = 0$. Um zu zeigen, dass $-(-a) = a$ gilt, müssen wir beweisen, dass $-a+a = 0$, was klar ist.

2. Wenn $a+b = c$, dann $a+b-b = c-b$, sodass $a = a+0 = c-b$. Umgekehrt, wenn $a = c-b$, dann $a+b = c-b+b = c$.

3. Übung.

□

Definition 3.1.9 (Ring)**.** Ein kommutativer Ring mit Eins ist eine Menge A zusammen mit zwei Operationen, Addition und Multiplikation

$$+\colon A \times A \to A, \qquad \cdot\colon A \times A \to A$$

so dass

- $(A, +)$ eine abelsche Gruppe ist.
- **Assoziativität der Multiplikation**: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in A$.
- **Multiplikative Eins**: Es existiert ein Element $1 \in A$ so dass $a \cdot 1 = 1 \cdot a = a$ für alle $a \in A$.
- **Kommutativität der Multiplikation**: $a \cdot b = b \cdot a$ für alle $a, b \in A$.
- **Distributivität**: $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(a+b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in A$.

Definition 3.1.10. Wenn die Multiplikation nur assoziativ und distributiv bezüglich der Addition ist, erhalten wir einen Ring. Ein Ring, in dem die Multiplikation kommutativ ist, wird als kommutativer Ring bezeichnet, ein Ring mit einer multiplikativen Eins wird als Ring mit Eins bezeichnet.

Definition 3.1.11 (Körper)**.** Ein Körper ist ein kommutativer Ring mit Eins $(\mathbb{K}, +, \cdot)$, in dem $1 \neq 0$ ist und jedes nicht null Element ein multiplikatives Inverses hat:

- **Multiplikatives Inverses**: Für jedes $a \in \mathbb{K}, a \neq 0$ gibt es ein Element $a^{-1} \in \mathbb{K}$ so dass $aa^{-1} = 1$.

Wir sagen auch, dass jedes nicht null Element bezüglich der Multiplikation invertierbar ist. Wir schreiben auch $\frac{1}{a} = a^{-1}$ und $\frac{b}{a} = ba^{-1}$.

Beispiel 3.1.12. Die Menge $\mathbb{Z}$ mit der üblichen Addition und Multiplikation ist ein kommutativer Ring mit Eins, aber kein Körper, da wir z.B. kein multiplikatives Inverses für 2 haben. Die Menge der rationalen Zahlen $\mathbb{Q}$ und die Menge der reellen Zahlen $\mathbb{R}$ sind Körper.

Lemma 3.1.13. *Sei $(A, +, \cdot)$ ein Ring.*

1. *Wenn die multiplikative Eins existiert, ist sie eindeutig.*
2. *Wenn das multiplikative Inverse eines Elements $a \in A$ existiert, ist es eindeutig.*

Außerdem gilt für alle $a, b, c, d, e \in A$:

3. $a \cdot 0 = 0 \cdot a = 0$.
4. $(-a) \cdot b = a \cdot (-b) = -(ab)$.
5. $(-a) \cdot (-b) = ab$.
6. $a \cdot (b - c) = ab - ac$ *und* $(a - b)c = ac - bc$.
7. $a \cdot (n \cdot b) = (n \cdot a) \cdot b = n \cdot (ab)$ *für alle* $n \in \mathbb{Z}$.

Außerdem, wenn A ein Körper ist, gilt:

8. $(a^{-1})^{-1} = a$ *für jedes* $a \neq 0$.
9. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, *für jedes* $b, d \neq 0$.
10. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, *für jedes* $b, d \neq 0$.
11. $ab = 0$ *genau dann, wenn* $a = 0$ *oder* $b = 0$.
12. $ab = ac$ *genau dann, wenn* $a = 0$ *oder* $b = c$.

Beweis.

1. Seien $1, 1'$ zwei multiplikative Einheiten. Dann $1 = 1 \cdot 1' = 1'$.
2. Seien a', a'' zwei multiplikative Inversen von a. Dann $a' = a' \cdot 1 = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = 1 \cdot a'' = a''$.
3. Wir sehen, dass $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, also $a \cdot 0 = 0$. Etwas Ähnliches gilt für $0 \cdot a$.
4. Um zu zeigen, dass $(-a) \cdot b = -(ab)$ gilt, müssen wir zeigen, dass $(-a) \cdot b + ab = 0$, und wir können dies wie folgt tun: $(-a) \cdot b + ab = (-a + a) \cdot b = 0 \cdot a = 0$. Eine ähnliche Argumentation beweist die andere Gleichheit.
5. Aus dem zuvor Bewiesenen folgt: $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-a \cdot b) = a \cdot b$.
6. Aus dem zuvor Bewiesenen folgt: $a \cdot (b - c) = a \cdot b + a \cdot (-c) = a \cdot b - a \cdot c$.
7. Übung.
8. Da $aa^{-1} = 1$, muss $a = (a^{-1})^{-1}$ sein.
9. Wir sehen, dass $\frac{a}{b} \cdot \frac{c}{d} = ab^{-1}cd^{-1} = acb^{-1}d^{-1}$, also reicht es zu beweisen, dass $b^{-1}c^{-1} = (bc)^{-1}$. Dies ist einfach, weil $b^{-1}c^{-1}bc = b^{-1}bc^{-1}c = 1 \cdot 1 = 1$.
10. Wir sehen, dass $\frac{ad+bc}{bd} = (ad + bc) \cdot (bd)^{-1} = (ad) \cdot (bd)^{-1} + (bc) \cdot (bd)^{-1} = adb^{-1}d^{-1} + bcb^{-1}d^{-1} = ab^{-1} + cd^{-1} = \frac{a}{b} + \frac{c}{d}$.
11. Wenn $ab = 0$ und $b \neq 0$, dann $0 = 0 \cdot b^{-1} = ab \cdot b^{-1} = a$.
12. Wir sehen, dass $ab = ac$ genau dann, wenn $a(b - c) = 0$. Dann folgt die Schlussfolgerung aus dem vorherigen Punkt.

□

Bemerkung 3.1.14. Die vorherigen Eigenschaften zeigen, dass wenn $\mathbb{K}$ ein Körper ist, dann die Menge der nicht null Elemente $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ mit der Multiplikation

$$\mathbb{K}^\times \times \mathbb{K}^\times \to \mathbb{K}^\times, \qquad (a, b) \mapsto ab$$

eine abelsche Gruppe ist. Sie können diese Aussage als Übung beweisen..

3.1.1 Vektoren, Matrizen und lineare Gleichungssysteme über einem Körper

Die zuvor gegebenen Definitionen von Vektoren und Matrizen können über einem beliebigen Körper $\mathbb{K}$ anstelle von nur über $\mathbb{R}$ gegeben werden. Daher können wir von Vektoren $b \in \mathbb{K}^m$ und von Matrizen $A \in \mathbb{K}^{m\times n}$ sprechen. Wir können auch von dem entsprechenden linearen Gleichungssystem und Lösungsraum sprechen

$$A \cdot x = b, \qquad \mathrm{Los}(A, b) = \{x \in \mathbb{K}^n \mid A \cdot x = b\}$$

Die Algorithmen, die wir zuvor über $\mathbb{R}$ vorgestellt haben, übertragen sich ohne Änderungen auf jeden Körper $\mathbb{K}$: Tatsächlich basierten diese Algorithmen auf den drei elementaren Zeilenumformungen auf einer Matrix, die über einem beliebigen Körper $\mathbb{K}$ durchgeführt werden können. Insbesondere kann der Gauß-Eliminationsverfahren über einem beliebigen Körper verwendet werden, um eine Matrix in (reduzierte) Zeilenstufenform zu bringen, und dies kann verwendet werden, um die Menge der Lösungen $\mathrm{Los}(A, b)$ über einem beliebigen Körper $\mathbb{K}$ zu bestimmen.

3.1.2 Endliche Körper

Die bisher gesehenen Beispiele von Körpern sind unendliche Körper: $\mathbb{Q}, \mathbb{R}$. Nicht alle Körper sind unendlich:

Beispiel 3.1.15. Betrachten Sie eine Menge $\mathbb{F}_2 = \{[0], [1]\}$ mit zwei verschiedenen Elementen $[0], [1]$. Wir definieren eine Summe und eine Multiplikation auf $\mathbb{F}_2$ wie folgt

$$\begin{aligned} [0] + [0] &= [0], & [0] \cdot [0] &= [0], \\ [0] + [1] &= [1], & [0] \cdot [1] &= [0], \\ [1] + [0] &= [1], & [1] \cdot [0] &= [0], \\ [1] + [1] &= [0], & [1] \cdot [1] &= [1]. \end{aligned}$$

Dann ist $\mathbb{F}_2$ mit diesen Operationen ein Körper. Um ein Gefühl für diesen Körper zu bekommen, ersetzen Sie $[0]$ durch "gerade" und $[1]$ durch "ungerade".

Allgemein kann bewiesen werden, dass wenn $\mathbb{K}$ ein endlicher Körper ist, dann muss er p^n Elemente haben, wobei p eine Primzahl ist und $n \geq 1$. Umgekehrt gibt es für jede Primzahl p und jedes $n \geq 1$ einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen.

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ **Ende Vorlesung 3.05.2024** ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

3.1.3 Die komplexen Zahlen

Ein wichtiges Beispiel für einen Körper sind die komplexen Zahlen:

Definition 3.1.16 (Komplexe Zahlen)**.** Eine komplexe Zahl ist ein formaler Ausdruck der Form

$$z = a + ib, \qquad a, b \in \mathbb{R}$$

Die reelle Zahl a wird als der Realteil von z bezeichnet und die reelle Zahl b wird als der Imaginärteil von z bezeichnet:

$$a = \Re(z), \qquad b = \Im(z)$$

Zwei komplexe Zahlen sind gleich, genau dann, wenn sie den gleichen Real- und Imaginärteil haben. Die komplexe Zahl $i \coloneqq 0 + i \cdot 1$ wird als die imaginäre Einheit bezeichnet. Die Menge aller komplexen Zahlen wird durch $\mathbb{C}$ bezeichnet, und $\mathbb{R}$ kann als eine Teilmenge von $\mathbb{C}$ betrachtet werden durch die injektive Abbildung

$$\mathbb{R} \hookrightarrow \mathbb{C}, \qquad a \mapsto a + i \cdot 0$$

so dass $\mathbb{R} = \{z \in \mathbb{C} \mid \Im(z) = 0\}$.

Bemerkung 3.1.17. Der Real- und Imaginärteil bilden Bijektionen

$$\mathbb{R}^2 \to \mathbb{C}, \quad (a, b) \mapsto a + ib, \qquad \mathbb{C} \to \mathbb{R}^2, \quad z \mapsto (\Re(z), \Im(z))$$

so dass $\mathbb{C}$ auch als $\mathbb{R}^2$ betrachtet werden kann. In diesem Sinne nennt man $\mathbb{C}$ die komplexe Ebene. Die Teilmenge $\mathbb{R} = \{z \in \mathbb{C} \mid \Im(z) = 0\}$ wird als die reale Achse bezeichnet und $\{z \in \mathbb{C} \mid \Re(z) = 0\}$ wird als die imaginäre Achse bezeichnet (siehe Tafel).

Definition 3.1.18 (Addition und Multiplikation von komplexen Zahlen)**.** Die Addition und Multiplikation auf $\mathbb{C}$ sind definiert durch

$$\begin{aligned} +\colon \mathbb{C} \times \mathbb{C} &\to \mathbb{C} & (a + ib, c + id) &\mapsto (a + c) + i(b + d) \\ \cdot\colon \mathbb{C} \times \mathbb{C} &\to \mathbb{C} & (a + ib, c + id) &\mapsto (ac - bd) + i(ad + bc) \end{aligned}$$

Bemerkung 3.1.19. Die Art und Weise, wie man diese Operationen betrachtet, ist, dass man die Ausdrücke $a + ib$ wie erwartet multipliziert, jedoch mit der zusätzlichen Bedingung, dass $i^2 = -1$. Tatsächlich überprüfen wir zunächst, dass $i^2 = -1$ ist:

$$i \cdot i = (0 + i \cdot 1)(0 + i \cdot 1) = -1 + i \cdot 0 = -1$$

Jetzt, wenn wir $(a + ib)$ und $(c + id)$ wie üblich addieren und multiplizieren, erhalten wir

$$(a + ib) + (c + id) = a + ib + c + id = a + c + ib + id = (a + c) + i(b + d).$$
$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = ac + iad + ibc - bd = (ac - bd) + i(ad + bc).$$

Proposition 3.1.20. *Die Menge der komplexen Zahlen mit diesen beiden Operationen ist ein Körper.*

Beweis. Die Überprüfung der Eigenschaften eines Körpers bleibt als Übung. Wir zeigen nur, wie man das Inverse eines von Null verschiedenen Elements $z = a + ib$ berechnet. Wir beobachten, dass

$$(a + ib) \cdot (a - ib) = a^2 - (ib)^2 = a^2 - (i)^2b^2 = a^2 - (-1)b^2 = a^2 + b^2$$

Insbesondere, wenn $z \neq 0$, dann $a \neq 0$ oder $b \neq 0$, so dass $a^2 + b^2$ reell und positiv ist und wir sein Inverses $(a^2 + b^2)^{-1}$ nehmen können. Dies zeigt, dass

$$(a + ib) \cdot \frac{a - ib}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1.$$

□

Definition 3.1.21 (Komplexe Konjugation und Betrag)**.** Die komplexe Konjugierte einer komplexen Zahl $z = a + ib$ ist

$$\bar{z} = a - ib.$$

Der Betrag einer komplexen Zahl $z = a + ib$ ist

$$|z| = \sqrt{a^2 + b^2}$$

Lemma 3.1.22 (Eigenschaften der komplexen Konjugation und des Betrags)**.** *Für alle $z, w \in \mathbb{C}$ gilt:*

1. $\overline{z + w} = \overline{z} + \overline{w}$ *und* $\overline{zw} = \overline{z} \cdot \overline{w}$.
2. $\overline{\overline{z}} = z$.
3. $z + \overline{z} = 2\Re(z)$ *und* $z - \overline{z} = 2\Im(z)$.
4. $z = \bar{z}$ *genau dann, wenn* $z \in \mathbb{R}$.
5. $z \cdot \overline{z} = |z|^2$.
6. $|z| \geq 0$ *und* $|z| = 0$ *genau dann, wenn* $z = 0$
7. $z^{-1} = \frac{\overline{z}}{|z|^2}$ *falls* $z \neq 0$.
8. $|\overline{z}| = |z|$.
9. $|zw| = |z| \cdot |w|$.
10. $\Re(z) \leq |z|, \Im(z) \leq |z|$
11. $|z + w| \leq |z| + |w|$ *(Dreiecksungleichung).*

Beweis. Wir beweisen nur die Dreiecksungleichung und lassen den Rest als Übung. Wir sehen, dass

$$\begin{aligned} |z + w|^2 &= (z + w)\overline{(z + w)} = (z + w)(\overline{z} + \overline{w}) = z \cdot \overline{z} + z \cdot \overline{w} + \overline{z} \cdot w + w \cdot \overline{w} \\ &= |z|^2 + |w|^2 + z \cdot \overline{w} + \overline{z} \cdot w = |z|^2 + |w|^2 + 2\Re(z \cdot \overline{w}) \leq |z|^2 + |w|^2 + |z \cdot \overline{w}| \\ &= |z|^2 + |w|^2 + 2|z| \cdot |w| = (|z| + |w|)^2. \end{aligned}$$

Dies zeigt, dass $|z + w|^2 \leq (|z| + |w|)^2$ ist, und durch Ziehen von Wurzeln sehen wir, dass $|z + w| \leq |z| + |w|$. □

3.1.4 Polynome

Ein wichtiges Beispiel eines Rings ist der Ring der Polynome mit Koeffizienten in einem Körper.

Definition 3.1.23 (Polynom)**.** Sei $\mathbb{K}$ ein Körper. Ein Polynom mit Koeffizienten in $\mathbb{K}$ in der Variablen x ist eine formale Summe

$$f = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n = \sum_{i=0}^{n} a_i x^n, \qquad a_i \in \mathbb{K}$$

Die a_i werden als Koeffizienten des Polynoms bezeichnet. Der Grad eines nicht nullen Polynoms f ist

$$\deg(f) = \max\{i \mid a_i \neq 0\}$$

Wir setzen auch den Grad des Nullpolynoms auf $\deg(0) = -\infty$. Wenn $\deg(f) = n$, dann wird a_n als der Leitkoeffizient bezeichnet. Ein Polynom mit Leitkoeffizienten 1 wird monisch genannt. Der Koeffizient a_0 wird als der konstante Koeffizient bezeichnet. Ein Polynom heißt konstant, falls $f = a_0$. Die Menge aller Polynome mit Koeffizienten in $\mathbb{K}$ und in der Variablen x wird mit $\mathbb{K}[x]$ bezeichnet.

Bemerkung 3.1.24. Manchmal werden wir ein Polynom wie oben als $f(x)$ bezeichnen, um zu betonen, dass es von der Variablen x abhängt. Es sollte jedoch nicht als Funktion betrachtet werden, es ist nur ein formaler Ausdruck. Wir werden jedoch später sehen, dass es manchmal als Funktion betrachtet werden kann.

Definition 3.1.25 (Summe und Produkt von Polynomen)**.** Für zwei Polynome $f, g \in \mathbb{K}[x]$

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{i=0}^{m} a_i x^i$$

definieren wir ihre Summe und ihr Produkt als

$$f + g \coloneqq \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i, \qquad f \cdot g = \sum_{i=0}^{nm} \left(\sum_{j=0}^{i} a_i b_{j-i} \right) x^i$$

Hier verwenden wir die Konvention, dass $a_k = 0$ für alle $k > \deg(f)$ und $b_h = 0$ für alle $h > \deg(g)$.

Bemerkung 3.1.26. Die Definition des Produkts mag kompliziert aussehen, aber es ist genau das, was wir erhalten, wenn wir das Produkt

$$(a_0 + a_1 x + \cdots + a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_m x^m)$$

auf die erwartete Weise ausmultiplizieren. Zum Beispiel

$$\begin{aligned}(a_0 + a_1 x) \cdot (b_0 + b_1 x + b_2 x^2) &= a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + a_1 b_0 x + a_1 b_1 x^2 + a_1 b_2 x^3 \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1) x^2 + (a_1 b_2) x^3.\end{aligned}$$

Insbesondere können wir berechnen, dass $x^n \cdot x^m = x^{n+m}$.

Proposition 3.1.27. *Die Menge $\mathbb{K}[x]$ zusammen mit der obigen Addition und Multiplikation ist ein kommutativer Ring mit Eins. Weiterhin gilt für $f, g \in \mathbb{K}[x]$, dass* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Beweis. Die Tatsache, dass $\mathbb{K}[x]$ ein Ring ist, wird als Übung überlassen. Wir beweisen die Aussage über die Grade. Wenn $f = 0$, dann $0 \cdot g = 0$, so dass $\deg(0 \cdot g) = \deg(0) = -\infty = \deg(0) + \deg(g)$. Das Gleiche gilt, wenn $g = 0$. Wenn $f, g \neq 0$, dann $\deg(f) = n, \deg(g) = m$ und

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{i=0}^{m} b_i x^i$$

mit $a_n, b_m \neq 0$. Dann ist $a_n b_m \neq 0$ (da $\mathbb{K}$ ein Körper ist) und die Formel für das Produkt zeigt, dass $\deg(f \cdot g) = n + m$. □

Lassen Sie $f \in \mathbb{K}[x]$ ein Polynom sein, $f = \sum_{i=0}^{n} a_i x^i$. Wir können eine entsprechende Polynomfunktion definieren:

$$f\colon \mathbb{K} \to \mathbb{K}, \qquad x_0 \mapsto f(x_0) = \sum_{i=0}^{n} a_i x_0^i$$

die wir immer noch mit demselben Zeichen bezeichnen, auch wenn es mehrdeutig ist.

Definition 3.1.28 (Nullstelle eines Polynoms)**.** Sei $f \in \mathbb{K}[x]$ ein Polynom. Ein Element $x_0 \in \mathbb{K}$ ist eine Nullstelle des Polynoms, wenn die entsprechende Polynomfunktion an dem Element Null ist: $f(x_0) = 0$.

Beispiel 3.1.29. Nehmen Sie $f(x) = x^2 - 3x + 2 \in \mathbb{Q}[x]$. Dann ist $f(2) = 2^2 - 3 \cdot 2 + 2 = 4 - 6 + 2 = 0$, so dass 2 eine Nullstelle von f ist.

Proposition 3.1.30 (Abspalten von Nullstellen)**.** *Sei $f(x) \in \mathbb{K}[x]$. Dann gilt $f(x_0) = 0$ genau dann, wenn wir schreiben können*

$$f(x) = (x - x_0) \cdot g(x)$$

für ein Polynom $g(x) \in \mathbb{K}[x]$.

Bevor wir dies beweisen, benötigen wir ein Lemma:

Lemma 3.1.31. *Sei A ein kommutativer Ring mit Eins. Für jedes $a, b \in A$ und $n \in \mathbb{N}, n \geq 2$ gilt*

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

Beweis. Wir können explizit berechnen

$$\begin{aligned}(a - b) \cdot (a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) &= a\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right) + b\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right) \\ &= \sum_{i=0}^{n-1} a^{i+1} b^{n-1-i} - \sum_{i=0}^{n-1} a^i b^{n-i} \\ &= a^n + \sum_{i=1}^{n-1} a^i b^{n-i} - \sum_{i=1}^{n-1} a_i b^{n-i} - b^n = a^n - b^n.\end{aligned}$$

□

Nun können wir die Proposition beweisen:

Beweis der Proposition 3.1.30. Wenn $f(x) = (x - x_0) \cdot g(x)$, dann $f(x_0) = 0 \cdot g(x_0) = 0$. Umgekehrt, nehmen Sie an, $f(x_0) = 0$. Wenn wir $f(x) = \sum_{i=0}^{n} a_i x^i$ schreiben, erhalten wir $f(x_0) = \sum_{i=0} a_i x_0^i = 0$. Dann

$$f(x) = f(x) - 0 = \sum_{i=0}^{n} a_i x^i - \sum_{i=0}^{n} a_i x_0^i = \sum_{i=0}^{n} a_i (x^i - x_0^i) = \sum_{i=0}^{n} a_i (x - x_0) \cdot g_i(x)$$

wobei $g_i(x) = \sum_{h=0}^{i-1} x_0^h x^{i-1-h}$ aus dem vorherigen Lemma stammt. Dann können wir schreiben

$$f(x) = \sum_{i=0}^{n} a_i (x - x_0) \cdot g_i = (x - x_0) \cdot (\sum_{i=0}^{n} a_i g_i) = (x - x_0) \cdot g(x)$$

□

Korollar 3.1.32. *Sei $f \in \mathbb{K}[x]$ ein Polynom.*

1. *Für $x_1, \ldots, x_m \in \mathbb{K}$ paarweise verschieden gilt $f(x_1) = \cdots = f(x_n) = 0$ genau dann, wenn*

$$f(x) = (x - x_1) \cdot \cdots \cdot (x - x_m) \cdot g(x)$$

   für ein bestimmtes $g(x) \in \mathbb{K}[x]$.

2. *Wenn f nicht null und vom Grad n ist, kann es höchstens n Nullstellen haben.*

Beweis. 1. Induktion über m. Wenn $m = 1$, haben wir das bereits zuvor bewiesen. Wenn $m > 1$, dann ist $f(x_m) = 0$, so dass

$$f(x) = (x - x_m) \cdot h(x)$$

Für $i = 1, \ldots, m-1$ muss $0 = f(x_i) = (x_i - x_m) \cdot h(x_i)$ sein. Da $x_i \neq x_m$ sein muss, muss $h(x_i) = 0$ sein. Nach Induktionshypothese $h(x) = (x - x_1) \cdot (x - x_{m-1}) \cdot g(x)$ und $f(x) = (x - x_1) \cdot (x - x_m) \cdot g(x)$.

2. Seien $x_1, \ldots, x_m$ die verschiedenen Nullstellen von f. Dann haben wir bewiesen, dass $f(x) = (x - x_1) \ldots (x - x_m) g(x)$, so dass $n = \deg(f) = \sum_{i=1}^{m} \deg(x - x_i) + \deg(g) = m + \deg(g)$. Dies zeigt $m \leq n$.

□

Korollar 3.1.33. *Sei $\mathbb{K}$ ein unendlicher Körper und seien $f, g \in \mathbb{K}[x]$. Dann gilt $f = g$ in $\mathbb{K}[x]$ genau dann, wenn $f(x_0) = g(x_0)$ für alle $x_0 \in \mathbb{K}$ gilt. Anders ausgedrückt, sind zwei Polynome gleich, wenn ihre Polynomfunktionen gleich sind.*

Beweis. Betrachten Sie das Polynom $h(x) = f(x) - g(x)$. Wir wissen, dass $h(x_0) = 0$ für alle $x_0 \in \mathbb{K}$. Das bedeutet, dass h unendlich viele Nullstellen hat, und das vorherige Lemma zeigt, dass h das Nullpolynom sein muss. □

3.1.5 Algebraisch abgeschlossene Körper

Definition 3.1.34 (Algebraisch abgeschlossener Körper)**.** Ein Körper $\mathbb{K}$ heißt algebraisch abgeschlossen, wenn jedes nichtkonstante Polynom $f \in \mathbb{K}[x]$ eine Nullstelle hat.

Proposition 3.1.35. *Wenn $\mathbb{K}$ algebraisch abgeschlossen ist, dann zerlegt sich jedes nichtkonstante Polynom als Produkt von linearen Faktoren: D.h. für jedes nichtkonstante $f(x) \in \mathbb{K}[x]$ gibt es $x_1, \ldots, x_m \in \mathbb{K}$ zusammen mit Exponenten $e_1, \ldots, e_m \in \mathbb{N}$ und $a \in \mathbb{K}^\times$, sodass*

$$f(x) = a \cdot (x - x_1)^{e_1} \cdot \cdots \cdot (x - x_m)^{e_m}$$

Beweis. Durch Induktion über den Grad von f. Wenn $\deg(f) = 1$, dann ist $f(x) = a_1 x + a_0$ mit $a_1 \neq 0$ und $f(x) = a_1 \cdot (x - (-\frac{a_0}{a_1}))$. Wenn $\deg(f) > 1$ dann hat f eine Nullstelle, da $\mathbb{K}$ algebraisch abgeschlossen ist. Dann können wir $f(x) = (x - x_1) \cdot g(x)$ für ein Polynom $g(x)$ schreiben. Da $\deg(g) = \deg(f) - 1$ zeigt die Induktionshypothese, dass g ein Produkt von linearen Faktoren ist. Dann ist f auch ein Produkt von linearen Faktoren. □

Satz 3.1.1 (Fundamentalsatz der Algebra)**.** *Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.*