1 Aussagenlogik

Eine Abb. $f\{1,0\}^n \to \{1,0\}$ heißt **Logikfunktion**.

Binäroperatortabele, n-äre Operatoren
- Es gibt genau 4 unäre (z.B. $\neq$)
- und 16 binäre Operatoren.

A	B	$*_1$	$*_2$	$*_3$	$*_4$	$*_5$
1	1	0	**1**	0	0	0
1	0	0	0	**1**	0	0
0	1	0	0	0	**1**	0
0	0	0	0	0	0	**1**
sprachliche Interpretation		0	AND $\wedge$	$\Rightarrow$ $A \wedge (\neg B)$	$\Leftarrow$ $(\neg A) \wedge B$	NOR $\vee$

A	B	$*_6$	$*_7$	$*_8$	$*_9$	$*_{10}$	$*_{11}$
1	1	**1**	**1**	**1**	0	0	0
1	0	**1**	0	0	**1**	**1**	0
0	1	0	**1**	0	**1**	0	**1**
0	0	0	0	**1**	0	**1**	**1**
sprachliche Interpretation		A	B	$\Leftrightarrow$	XOR $\oplus$	$\neg B$	$\neg A$

A	B	$*_{12}$	$*_{13}$	$*_{14}$	$*_{15}$	$*_{16}$
1	1	**1**	**1**	**1**	0	**1**
1	0	**1**	**1**	0	**1**	**1**
0	1	**1**	0	**1**	**1**	**1**
0	0	0	**1**	**1**	**1**	**1**
sprachliche Interpretation		OR $\vee$	$\Leftarrow$ $A \vee (\neg B)$	$\Rightarrow$ $(\neg A) \vee B$	NAND $\mid \wedge$	1

Äquivalenz:
$A \Leftrightarrow B :\equiv (A \Rightarrow B) \wedge ((B \Rightarrow A)) \equiv \overline{A} \vee B$
XOR:
$A \otimes B :\equiv A \text{ xor } B :\equiv \overline{A \Leftrightarrow B}$
Eine **Tautologie/Kontradiktion** ist eine Aussage, die für jede Variablenbelegung immer wahr/falsch ist.

einstellige Tautologien

Doppelte Verneinung: $\overline{\overline{A}} \Leftrightarrow A$
Ausgeschlossener Dritter: $A \vee \overline{A}$
Widerspruch: $\overline{A \wedge \overline{A}}$
Mit Idempotenzen:
$\bullet (A \vee A) \Leftrightarrow A$,
$\bullet (A \wedge A) \Leftrightarrow A$
Neutralität: $A \Leftrightarrow A \vee 0 \Leftrightarrow A \wedge 1$
Bsp.: Sei φ eine Tautologie, dann ist $\neg\varphi$ eine Kontradiktion
Subjunktion und Implikation: Eine wahre Subjunktion $\varphi :\equiv A \to B$ heißt **Implikation**.
Notation: $A \Rightarrow B$

Logikregeln
Kommutativgesetz:
$\bullet\ X \wedge Y \equiv Y \wedge X$
$\bullet\ X \vee Y \equiv Y \vee X$
Assoziativgesetz:
$\bullet\ X \wedge (Y \wedge Z) \equiv (X \wedge Y) \wedge Z$
$\bullet\ X \vee (Y \vee Z) \equiv (X \vee Y) \vee Z$
Distributivgesetz:
$\bullet\ X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$
$\bullet\ (X \vee Y)(X \vee Z) \equiv X \vee (Y \wedge Z)$
Idempotenz:
$\bullet\ X \equiv X \wedge X$;
$\bullet\ X \equiv X \vee X$
Absorption:
$\bullet\ X \wedge (X \vee Y) \equiv X$;
$\bullet\ X \vee (X \wedge Y) \equiv X$
0 und 1:
$\bullet\ X \wedge \overline{X} = 0$
$\bullet\ X \vee \overline{X} = 1$
$\bullet\ 0 \wedge X = 0$;
$\bullet\ 1 \wedge X \equiv X$
$\bullet\ 0 \vee X \equiv X$
$\bullet\ 1 \vee X = 1$
$\bullet\ \overline{0} = 1$;
$\bullet\ \overline{1} = 0$
De Morgan:
$\bullet\ \overline{X \wedge Y} \equiv \overline{X} \vee \overline{Y}$;
$\bullet\ \overline{X \vee Y} \equiv \overline{X} \wedge \overline{Y}$

Seien $(x_1,...,x_n)$ a.l. Variablen mit $i = 1,...,2^n$ Belegungen $(x_1^{(i)},...,x_n^{(i)})$, f eine Logikfunktion.
Konjunktive Normalform (KNF) :
Für $x_j^{(i)} = 1$: $(\neg)x_j^{(i)} = \overline{x_j^{(i)}}$,
Für $x_j^{(i)} = 0$: $(\neg)x_j^{(i)} = x_j^{(i)}$:
$f(x_1,...,x_n) = \bigwedge_i \left(\bigvee_j (\neg) x_j^{(i)} \right)$
Disjunkte Normalform (DNF) :
Für $x_j^{(i)} = 0$: $(\neg)x_j^{(i)} = \overline{x_j^{(i)}}$,
Für $x_j^{(i)} = 1$: $(\neg)x_j^{(i)} = x_j^{(i)}$. Dann gilt:
$f(x_1,...,x_n) = \bigvee_i \left(\bigwedge_j (\neg) x_j^{(i)} \right)$

In der Aussagenlogik sind **Junktoren** die logischen Operatoren.
Allquantor: $\forall$; Für alle x gilt die Eigenschaft E: $\forall x : E(x)$

Existenzquantor: $\exists$; Es existiert ein x, die Eigenschaft E erfüllt: $\exists x : E(x)$

Kombinationen mit beiden Quantoren:
- Zu jedem x gibt es ein y so dass Eigenschaft A gilt: $\forall x \exists y : A(x,y)$
- Ein x kann zu jedem y zugeteilt werden, so dass Eigenschaft A gilt: $\exists x \forall y : A(x,y)$

Verneinung der Quantoren:
$\bullet\ \neg(\forall x : A(x)) \Leftrightarrow \exists x : \neg A(x)$
$\bullet\ \neg(\exists x : A(x)) \Leftrightarrow \forall x : \neg A(x)$
Ausklammerungsregel:
$\bullet\ \forall x : A(x) \wedge B(x) \Leftrightarrow (\forall x : A(x)) \wedge (\forall x : B(x))$
$\bullet\ \exists x : A(x) \vee B(x) \Leftrightarrow ((\exists x : A(x)) \vee (\exists x : B(x))$

a.l. Fachausdrücke
- " Aussage A ist **genau dann** erfüllt **wenn** Aussage B erfüllt ist", bedeutet:
" Aussage A ist erfüllt"$\Leftrightarrow$ " Aussage B ist erfüllt".
- **Beliebige viele** x bedeutet **unendlich viele** x
- " Aussage A gilt **für fast alle** x"bedeutet:
" Aussage A wird von endlich vielen x nicht erfüllt".

2 Allgemeines

Die Zahl $n \in \mathbb{N}$ ist **gerade**: $\exists k \in \mathbb{N} : 2 \cdot k = n$
Die Zahl $n \in \mathbb{N}$ ist **ungerade**: $\exists k \in \mathbb{N}_0 : (2 \cdot k) + 1 = n$
Anmerkung: n ungerade $\Leftrightarrow$ n nicht gerade

Eine Teilmenge $M' \subset M$ ist **nach oben beschränkt**: $\exists a \in M \forall m \in M' : m \leqslant a$

Bzgl. natürliche Zahlen:
Jede nach oben beschränkte Teilmenge natürlicher Zahlen, hat ein eindeutige Maximum.

Schachtelung natürlicher Zahlen: $\forall n \in \mathbb{N}$: Es gibt kein $c \in \mathbb{N} : n < c < n+1$
(Un)Gerade Potenzen: Sei $n \in \mathbb{N}$
- n gerade $\Leftrightarrow$ n^2 gerade
- n ungerade $\Leftrightarrow$ n^2 ungerade.

ABC-Formel: Die Nullstellen von $p(x) = ax^2 + bx + c$ sind:
$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
p-q-Formel: Die Nullstellen von $f(x) = x^2 + px + q$ sind:
$$x_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{b^2}{4} - q}$$

3 Abbildungen & Mengenlehre

floor- und ceil-Funktion Sei $x \in \mathbb{R}$:
$\text{floor}(x) := \lfloor x \rfloor := \max\{n \in \mathbb{Z} | n \leqslant x\}$
$\text{ceil}(x) := \lceil x \rceil := \min\{n \in \mathbb{Z} | n \geqslant x\}$
Alternativdefinition:
$r = \lfloor x \rfloor :\Leftrightarrow r \in \mathbb{Z},\ \lfloor x \rfloor \leqslant r < \lfloor x \rfloor + 1$
$s = \lceil x \rceil :\Leftrightarrow s \in \mathbb{Z},\ \lceil x \rceil + 1 > s \geqslant \lceil x \rceil$

Ganzzahliger Anteil: $\{x\} := x - \lfloor x \rfloor$
Daraus folgt: $x = \lfloor x \rfloor + \{x\}$
Rechenregeln für floor und ceil
- $\lfloor x \rfloor = x \Leftrightarrow x \in \mathbb{Z} \Leftrightarrow \lceil x \rceil = x$
- $x - 1 < \lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil < x + 1$
- $\lfloor -x \rfloor = -\lceil x \rceil$ und $\lceil -x \rceil = -\lfloor x \rfloor$
- $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 \text{ falls } x \in \mathbb{Z} \\ 1 \text{ falls } x \notin \mathbb{Z} \end{cases}$
- $\forall\ k \in \mathbb{Z} : \lfloor x + k \rfloor = \lfloor x \rfloor + k$ und $\lceil x + k \rceil = \lceil x \rceil + k$
- $\lfloor x/2 \rfloor + \lceil x/2 \rceil = x \Leftrightarrow x \in \mathbb{Z}$

Eigenschaften von Mengen
- Mengen enthalten von jedem Element genau eines.
- Es gibt eine Menge ohne Elemente, die **leere Menge** $\emptyset$
- Die Elemente in einer Menge sind nicht geordnet. Es gilt: $\{1,2\} = \{2,1\}$
- Mengen können neben Zahlen auch Funktionen/Abbildungen und auch Mengen als Elemente enthalten:

Bsp.1: (Menge mit Abbildungen) Basis der Polynome n-ten Grades:
$\{1, x, x^2, ..., x^{n-1}, x^n\}$
Bsp: 2: (Menge mit Mengen) Potenzmenge $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$
- Um eine Aussagen zu treffen ob ein Element in der Menge **enthalten ist**: $2 \in \mathbb{N}$
Oder ob ein Element **nicht enthalten** ist: $\pi \notin \mathbb{N}$
wird das **Epsilon-Zeichen**, also $\in, \notin$, verwendet.

Mengenoperationen mit Aussagenlogik
- $x \in (A \cup B) \Leftrightarrow (x \in A) \vee (x \in B)$ heißt **Vereinigung**
- $x \in (A \cap B) \Leftrightarrow (x \in A) \wedge (x \in B)$ heißt **Schnitt**
- $x \in (A \setminus B) \Leftrightarrow (x \in A) \wedge (x \notin B)$ heißt **Differenz**
- $x \in (A \Delta B) \Leftrightarrow (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \notin B)$ heißt **symmetrische Differenz**

Für diese Aussagen verwenden wir nicht mehr das $\equiv \Leftrightarrow$

Zwei Mengen gelten als **disjunkt**, wenn sie sich nicht schneiden. Es gilt: $A \cap B = \emptyset$

Die Mengen $A_1,...,A_n$ heißen **paarweise disjunkt**, wenn gilt: $\forall i, j \in \{1,...,n\}, i \neq j : A_i \cap A_j = \emptyset$

Eine **Teilmenge** T von A ist eine Menge, das die Elemente enthält, die auch A enthält: $T \subseteq A :\Leftrightarrow (x \in T) \Rightarrow (x \in A)$
Anmerkung: Jede Menge ist zu sich selbst eine Teilmenge: $A \subseteq A$
Spezialfall: Die leere Menge, also $\emptyset$, ist von jeder Menge eine Teilmenge!

Eine **echte Teilmenge** R von A
ist immer ungleich A: $R \subset A :\Leftrightarrow (R \subseteq A) \wedge (R \neq A)$

Die **Potenzmenge** $\mathcal{P}$ einer Menge A ist die **Menge aller Teilmengen von** A: $2^A := \mathcal{P}(A) := \{A' \subseteq A\}$
Die **Mächtigkeit/Kardinalität** einer Menge ist die Anzahl ihrer Elemente:
Notation: $|A|$ oder $\#A$

Anmerkung: Die Mächtigkeit einer Potenzmenge $\mathcal{P}(A)$ ist immer $2^{|A|}$.

Summenregel zur Kardinalität:

Für zwei disjunkte Mengen A,B gilt: $|A \dot\cup B| = |A| + |B|$
Allgemeiner: Für paarweise disjunkte Mengen $A_1,...,A_n$ gilt: $\left|\dot\bigcup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i|$
Anmerkung: Sie ist ein Spezialfall der Inklusions-Exklusions-Formel!
Inklusion-Exklusions-Formel: Für zwei Mengen A,B gilt: $|A \cup B| = |A| + |B| - |A \cap B|$

Kartesisches Produkt: Seien M,N Mengen und $d \in \mathbb{N}$. Dann ist:
- $M \times N := \{(x,y) | x \in M, y \in N\}$
- $M^d := M \times ... \times M = \{(x_1,...,x_d) | x_1,...,x_d \in M\}$

Sei $f : A \to B$ eine Abbildung. Die Menge $f : D \subseteq A$ heißt **Definitionsmenge** von f, wenn es die größtmögliche Menge ist, auf der f definiert ist.

Sei $f : X \to Y$ eine Abbildung und $D \subseteq X$ eine Teilmenge von X. Dann ist die **Abbildungsmenge** von X bezüglich f:
$f(D) := \{f(x) | x \in D\} = \{y \in Y | \exists x \in D\}$

Sei $D \subseteq A$ die Definitionsmenge der Abbildung $f : A \to B$. Dann ist $f(D) \subseteq B$ der **Wertebereich** von f in B.

Seien $f_a, f_b : X \to Y$ Abbildung von X nach Y. Eine **fallunterscheidente Abbildung** g mit den Eigenschaften A,B ist wie folgt definiert:

$$g : \begin{cases} X & \to Y \\ x & \mapsto \begin{cases} f_a(x), & \text{falls } A(x) \\ f_b(x), & \text{falls } B(x) \end{cases} \end{cases}$$

Die Abbildung $id : \begin{cases} M & \to N \\ x & \mapsto x \end{cases}$ heisst **Identitätsabbildung**.

Seien $f : A \to B$ und $g : B \to C$ Abbildung. Die ineinander Verschachtelung dieser Funktionen bzw. **Komposition** ist definiert als:

$$(g \circ f) : \begin{cases} A & \to C \\ x & \mapsto g(f(x)) \end{cases}$$

$f : X \to Y$ heisst **injektiv** wenn für $x_1, x_2 \in X$:
$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
Alternativ: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

$f : X \to Y$ heisst **surjektiv**:
$\forall y \in Y \exists x \in X : f(x) = y$
Alternativ:: $\exists D \subseteq X : f(D) = Y$ **bzw.** $f^{-1}(Y) = D$
Eine Abbildung ist **bijektiv**, wenn sie injektiv und surjektiv ist.
Zwei Mengen A,B heißen **gleichmächtig**, wenn es eine bijektive Abbildung $g : A \to B$ gibt.

Sei $f : B \to C$ eine Abbildung.
Eine Abbildung $f_r : A \to B$ heisst **rechtsinvers zur Abbildung** f, wenn $f \circ f_r = id$

Sei $g : A \to B$ eine Abbildung.
Eine Abbildung $g_l : B \to C$ heisst **linksinvers zur Abbildung** g, wenn $g_l \circ g = id$

Eine linksinverse Abbildung f_l zur Abbildung f heißt **Umkehrabbildung**, wenn f_l eindeutig ist. Hierbei wird f_l auch als f^{-1} bezeichnet.

Satz: Eine Abbildung f hat genau dann eine Umkehrabbildung, wenn sie bijektiv ist.

Sei $f : A \to B$ eine Abbildung, $C \subseteq B$. Das **Urbild** von C ist definiert als: $f^{-1}(C) = \{x \in A | f(x) \in C\}$ Ist $C = \{b\}$ einelementig, so heisst $f^{-1}(C) = f^{-1}(\{b\})$ **Faser** von b.

Mengen und Bilder mit Logik:
Sei $f : A \to B$ eine Abbildung und f^{-1} die dazugehörige Umkehrabbildung. Dann gilt für $A_1 \subseteq A$:
$y \in f(A_1) \Leftrightarrow \exists x \in A_1 : f(x) = y$
und für $B_1 \subseteq B$ gilt:
$x \in f^{-1}(B_1) \Leftrightarrow f(x) \in B_1$
Bilder von verknüpften Mengen: Seien $f : X \to Y$, $A,B \subseteq X$, $U,V \subseteq Y$, dann gilt:
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) = f(A) \cap f(B)$
- Falls f injektiv: $f(A \setminus B) = f(A) \setminus f(B)$
- $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$
- $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$
- $f^{-1}(U \setminus V) = f^{-1}(U) \setminus f^{-1}(V)$

Verknüpfung injektiver/surjektiver Abbildungen:
Seien $f : A \to B$ und $g : B \to C$:
- Für f injektiv und g injektiv $\Rightarrow$ $g \circ f$ injektiv
- Für $g \circ f$ injektiv $\Rightarrow$ f injektiv
- Für f surjektiv und g surjektiv $\Rightarrow$ $g \circ f$ surjektiv

4 Algebraische Strukturen & Zahlentheorie

Sei G eine Menge und $\circ$ ein Operator auf G. Das 2-Tupel $(G,\circ)$ heisst **Halbgruppe** wenn Assoziativität gilt, also: $\forall a,b,c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
Anmerkung Sei $\circ : \emptyset \times \emptyset \to \emptyset$ die leere Verknüpfung. Dann ist $(\emptyset,\circ)$ die **triviale Halbgruppe**

Sei $(G,\circ)$ eine Halbgruppe. Sie heißt **Gruppe** wenn zusätzlich gilt:
(i) $G \neq \emptyset$
(ii) Es existiert ein **neutrales Element** $e \in G$: $\forall a \in G : a \circ e = e \circ a = a$
(iii) Es existiert zu jedem Element $a \in G$ **ein inverses Element** $b \in G : \ a \circ b = b \circ a = e$
Notation: G wird als Gruppe bezeichnet, wenn es im Kontext klar ist, dass es sich um $(G,\circ)$ handelt.
Anmerkung: Das neutrale Element ist eindeutig und jede inverse Element in einer Gruppe ist eindeutig. Sonst wäre es keine Gruppe.

Eine Gruppe G heisst **abelsch** bzw. **kommutativ**, wenn für alle $a,b \in G : a \circ b = b \circ a$ gilt.

Eine Menge G heißt **additive Gruppe**, wenn $(G,+)$ eine Gruppe, und **multiplikative Gruppe**, wenn $(G,\cdot)$ eine Gruppe ist.
Bsp.: $\mathbb{Q}$ ist eine multiplikative Gruppe bzw. $\mathbb{Z}$ ist eine additive Gruppe.

Inverse verknüpfter Elemente: Sei G eine Gruppe, dann gilt für $a,b \in G : (a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Seien $a,b \in \mathbb{Z}$. Die Zahl a ist ein **Teiler** von b wenn es ein $c \in \mathbb{Z}$ gibt mit der Eigenschaft: $a \cdot c = b$. Man schreibt auch $a|b$.

Bemerkung: Seien $a,b,p \in \mathbb{Z}$, dann gilt:
1) $(p|a \wedge p|b) \Rightarrow p|(a+b)$
2) $(p|a \wedge p|a+b) \Rightarrow p|b$

Zwei Zahlen $a,b \in \mathbb{Z}$ sind **kongruent** bezüglich eines modulo $p \in \mathbb{Z}$, wenn gilt: $p|(a-b)$.
Notation: $a \equiv b \mod p$

Bemerkung: Sei $i \in \mathbb{N}_0$ und $p \in \{3,9\}$, dann gilt: $10^i \equiv 1 \mod p$.

Sei G eine Menge und $M \subseteq G \times G$ mit folgenden Eigenschaften:
- (Reflexivität) Für $a \in G : (a,a) \in M$
- (Symmetrie) $a,b \in G : (a,b) \in M$, dann auch $(b,a) \in M$.
- (Transzendenz) $a,b,c \in G : ((a,b) \in M \wedge (b,c) \in M) \Rightarrow (a,c) \in M$

Dann ist auf M eine **Äquivalenzrelation** definiert, die sich wie folgt dargestellt wird:
$\forall a,b \in G : a \sim_M b :\Leftrightarrow (a,b) \in M$

Die Menge $[a]_{\sim_M} := \{b \in G | b \sim_M a\}$ wird als **Äquivalenzklasse** definiert.

Anmerkung: Die Elemente aus $\mathbb{Z}/n\mathbb{Z}$ sind Äquivalenzklassen, da sie Mengen von zueinander kongruenten Zahlen bzgl. des Modulo n sind.

Sei G eine multiplikative Gruppe und $a \in G$ mit $a \neq 0$. Die Zahl $b \in G$ mit $b \neq 0$ heißt **Nullteiler**, wenn $ab = 0$ gilt.
Anmerkung: Somit wäre auch b ein Nullteiler

Eine Gruppe ohne Nullteiler heißt **nullteilerfrei**.

Sei $(G,\circ)$ eine Gruppe, dann wird ein Element $c \in G$ **Einheit** genannt,
wenn es bezüglich $\circ$ ein (inverses) Element $b \in G$ gibt mit: $b \circ c = c \circ b = e$

Die Menge $G^\times := \{a \in G | \ a \text{ ist eine Einheit in } G\} \subseteq G$ ist die **Menge aller Einheiten** von G.

Sei $(G,\circ)$ eine Gruppe, $a \in G$. Die Potenz von a bezüglich $\circ$ ist:
$\forall n \in \mathbb{N} : a^n := \underbrace{a \circ ... \circ a}_{n\text{-mal}}$
Das **Erzeugnis** von a bezüglich $\circ$ ist:
$\langle a \rangle := \{a^n | n \in \mathbb{N}\} = \{a, a^2, a^3, ..., a^n\}$
Eine Gruppe $(G,\circ)$, mit G endlich, heißt **endlich erzeugt** oder **zyklisch**, wenn es ein $a \in G$ gibt mit $\langle a \rangle = G$.

Zwei Zahlen a,b **sind teilerfremd**, wenn kein Teiler von a die Zahl b nicht teilt und umgekehrt.
Anmerkung: Insbesondere sind Primzahlen zu allen Zahlen teilerfremd.

Der **größte gemeinsame Teiler** von a,b , ist die größte natürliche Zahl t mit $t|a$ und $t|b$.
in kurz: $\text{ggT}(a,b) = t$
Bei Teilerfremdheit:
- Zwei Zahlen $c,d \in \mathbb{Z}$ sind teilerfremd genau dann, wenn $ggT(c,d) = 1$.
- Für eine Primzahl p und $a \in \mathbb{Z} \setminus \{0,p\}$ ist $ggT(p,a) = 1$.

(Erweiterter) Euklidischer Algorithmus: Seien $a,b \in \mathbb{Z}$ mit $a < b$. Der $ggT(a,b)$ lässt sich wie folgt algorithmisch ermitteln:
(1) Berechne die ganzzahlige Division $b/a = c$ und die Restedivision $b\%a = r = b \mod a$.
(2) Falls $r = 0$, dann stoppe die Routine. Dann ist $a = ggT(a,b)$.
Sonst wiederhole Schritt 1. mit $b := a$ und $a := r$.
Erweiterung: Setze bei jeden Schritt von 1. das $r = b - c * a$ dar. In jedem r müssen die ursprünglichen Zahlen a,b vom Anfang enthalten sein.
Anmerkung 1: Auch Reste können negativ werden, z.B. $119 : 4 = 29$ Rest3 oder $119 : 4 = 30$ Rest -1.

Anmerkung 2: Mithilfe des erweiterten euklidischen Algorithmus lässt sich jeder $ggT(a,b)$ als Linearkombination von a und b darstellen. Es gibt also $\lambda,\mu \in \mathbb{Z} : ggT(a,b) = \lambda a + \mu b$.
Somit lassen sich multiplikativ inverse Zahlen berechnen (bzgl. eines Modulos b).

ggT-Rechenregeln:
- $\forall a \in \mathbb{Z} : ggT(a,1) = 1$
- $\forall a \in \mathbb{Z} : ggT(a,0) = a$
- $\text{ggT}(a,b) = c :\Leftrightarrow [c|a] \wedge [c|b] \wedge [\forall t : (t|a \wedge t|b) \Rightarrow t|c]$
- $\text{ggT}(a,b) = \text{ggT}(b,a)$
- $\forall k \in \mathbb{Z} : \text{ggT}(a,b) = \text{ggT}(b, a-kb)$
- $\text{ggT}(a,b) = \text{ggT}(b, \mod(a,b))$

Eulersche Phi-Funktion: Anzahl aller zu n teilerfremden Zahlen, die $\leqslant n$ sind.
$\phi(n) := |\{a \in \mathbb{N} | 1 \leqslant a \leqslant n \wedge \text{ggT}(a,n) = 1\}|$
Sonderfall: Sei p_k die k-te Primzahl. Dann gilt: $\phi(p_k) = k - 1$
Bei Primzahlpotenzen: Sei p eine Primzahl. Dann gilt: $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$
Berechnungsformel: $\phi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$
Multiplikativität: Seien m,n teilerfremd. Dann gilt: $\phi(n \cdot m) = \phi(n)\phi(m)$

Satz von Euler: Seien $a,b \in \mathbb{Z}$ und zueinander teilerfremd. Dann gilt für $a < b : a^{\phi(b)} \equiv 1 \mod b$

Kleiner Satz von Fermat: Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}_p^\times$, dann gilt: $a^{p-1} \equiv 1 \mod p$ bzw. $a^p \equiv a \mod p$
Anmerkung: Für $p \in \mathbb{P}$ ist $(\mathbb{Z}_p,+)$ eine abelsche

Gruppe und $(\mathbb{Z}_p^\times,\cdot)$ eine abelsche Gruppe. Man nennt hier $(\mathbb{Z},+,\cdot)$ auch Körper (da auch die beidseitigen Distributivgesetze gelten).

Sei G eine endliche Gruppe. Die **Ordnung von** G ist die Mächtigkeit von G. Also $\text{ord}(G) := |G|$.

Sei G eine endliche multiplikative Gruppe und $a \in G$. Die **Ordnung von** a ist die kleinste Potenz $n \in \mathbb{N}$, sodass $a^n = e$ ist. Also $\text{ord}(a) := n$.

Folgerung aus dem Satz von Lagrange: Sei $(G,\circ)$ eine Gruppe und G endlich, dann teilt die Ordnung jedes Elementes $x \in G$ die Mächtigkeit von G.
In kurz: Nach Lagrange gilt, dass die Elementordnung die Mächtigkeit der zugehörigen Gruppe teilt.

Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Für $a \in G$ wird die Menge $aH := \{ah | h \in H\}$ als **Linksnebenklasse** in G zur Untergruppe H bezeichnet, und $Ha := \{ha | h \in H\}$ als **Rechtsnebenklasse** in G zur Untergruppe H bezeichnet.

Falls $aG = Ga$ ist, so ist $G/aG := \{g(aG) | g \in G\}$
Für $(\mathbb{Z},+)$ ist das $\mathbb{Z}/n\mathbb{Z} = \{\{k+ng | g \in \mathbb{Z}\} : k \in \mathbb{Z}\}$

Die Elemente $\{k+ng | g \in \mathbb{Z}\}$ werden auch als die **Kongruenzklassen** $[k]$ bezeichnet (Alternative Schreibweise: $\bar{k}$) und $\mathbb{Z}/n\mathbb{Z}$ als **Restklassenring**.

Zahlentheoretische Aussagen und Tricks Sei G eine Gruppe und H eine Untergruppe von G
- Sei $(\mathbb{Z}_m^\times,\cdot)$ eine zyklische Gruppe. Die **Anzahl der Erzeuger** ist gleich $\phi(m)$.
- Die Nebenklassen zur Untergruppe H in G lassen sich schrittweise durch finden aller aH ermitteln.
- Alle Nebenklassen sind entweder paarweise disjunkt oder gleich.
- Die Vereinigung aller Nebenklassen ergibt die Gruppe $(G,\cdot)$.

Sei $(G,\circ)$ eine abelsche Gruppe und $(G,*)$ eine Halbgruppe. Dann wird $(G,\circ,*)$ als **Ring** bezeichnet, wenn zusätzlich das links- und rechtsseitige Distributivgesetz gilt:
$[a*(b\circ c) = a*b\circ a*c] \wedge [(a\circ b)*c = a*c\circ b*c]$

Sei $(G,\circ,*)$ ein Ring. Es ist ein **Körper**, wenn $(G,*)$ ebenfalls eine abelsche Gruppe ist.

5 Komplexe Zahlen

Die Gleichung $x^2+1=0$ hat in $\mathbb{R}$ keine Lösung.
Definiere hierfür eine Obermenge von $\mathbb{R}$, die $\sqrt{-1}$ enthält.
Die Menge $\mathbb{C} := \mathbb{R} + i\mathbb{R} = \{x+iy | x,y \in \mathbb{R} \wedge i^2 = -1\}$ heißt **Menge der komplexe Zahlen**.

Darstellungen der **komplexen Zahlen**. Für ein $z \in \mathbb{C}$
Vektorschreibweise: Sei $z = \binom{a}{b} \in \mathbb{C}$:
- **Addition:** $\binom{a}{b} + \binom{c}{d} = \binom{a+c}{b+d}$
- **Multiplikation:** $\binom{a}{b} \cdot \binom{c}{d} = \binom{ac-bd}{ad+bc}$

Summenschreibweise: (die eigentlich gängige): Sei $z = a+ib \in C$:
Addition: $(a+ib)+(c+id) = a+c+ib+id = (a+c)+i(b+d)$
Multiplikation: $(a+ib)\cdot(c+id) = ac+iad+ibc-bd = (ac-bd)+i(ad+bc)$
Hierbei werden bei einer komplexen Zahl $z = a+ib$ die Zahl $a \in \mathbb{R}$ als **Realanteil** und die Zahl $b \in \mathbb{R}$ als **Imaginäranteil** bezeichnet.
Notation:
$\text{Re}(z) = \text{Re}(a+ib) := a \qquad \text{Im}(z) = \text{Im}(a+ib) := b$
$(\mathbb{C},+,\cdot)$ ist ein Körper, also $(\mathbb{C},+)$ und $(\mathbb{C}\setminus\{0\},\cdot)$ sind abelsche Gruppen und es gelten die beidseitigen Distributivgesetze.

Die reellen Zahlen $\mathbb{R}$ sind eine echte Teilmenge von $\mathbb{C}$, da jede reelle Zahl $r \in R$, eine komplexe Zahl mit Imaginäranteil gleich 0 ist. Also $r = r+i0$.

Das **additive Inverse** einer Zahl $z = a+ib$ ist $-z = -a-ib$.
Das **multiplikativ Inverse** einer Zahl $z = a+ib \neq 0$ ist $\frac{1}{z} = z^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} = \frac{a-ib}{a^2+b^2}$

Das **komplex konjugierte** einer Zahl $z = a+ib$ ist $\overline{z} := a+ib$.

Der **Betrag** einer komplexen Zahl $z = a+ib$ ist $|z| = \sqrt{a^2+b^2}$

Rechenregeln: Sei $z = (a+ib)$
- $z^2 = (a+ib)^2 = (a^2+b^2)+i(2ab)$
- $\overline{z}^2 = (a-ib)^2 = (a^2+b^2)-i(2ab)$
- $z\overline{z} = (a+ib)(a-ib) = a^2+b^2$
- $\left(\sqrt{\frac{1}{2}}+i\sqrt{\frac{1}{2}}\right)^2 = i$

Anmerkung: $\forall a,b \in \mathbb{R}_0^+ : \sqrt{a}\cdot\sqrt{b} = \sqrt{ab}$

6 Lineare Algebra

Vektorräume Sei $(K,+_K,\cdot_K)$ ein Körper bzw. $(K,+_K)$ und $(K\setminus\{0\},\cdot_K)$ jeweils abelsche Gruppen, wo das links- und rechtsseitige Distributivgesetz gilt.
Gegeben sei eine Menge V mit den Verknüpfungen:
Vektoraddition:
$+ : V\times V \to V, (v,w) \mapsto v+w$ Vektoraddition
Skalarmultiplikation:
$\cdot : K\times V \to V, (\lambda,v) \mapsto \lambda\cdot v$
Zusätzlich mit den Eigenschaften:
V1 $(V,+)$ ist eine abelsche Gruppe, mit 0 als neutrales Element und $(-v) \in V$ als Inverses von $v \in V$.
V2 Folgende Rechenregeln:
$\forall \lambda,\mu \in K$ und $v,w \in V$:
a) $(\lambda+\mu)\cdot v = \lambda\cdot v + \mu\cdot v$
b) $\lambda\cdot(v+w) = \lambda\cdot+\lambda\cdot w$
c) $\lambda\cdot(\lambda\cdot v) = (\lambda\cdot\mu)\cdot v$
d) $1\cdot v = v$
Dann heißt die Struktur $(V,+,\cdot)$ K**-Vektorraum** (kurz: K-VR).

Notation: Ist - anhand der Zahlen und aus welcher Menge sie stammen - im Kontext klar, welche Operation zu welcher Menge gehört, so kann anstatt $+,\cdot$ bzw. $+,\cdot$ auch als $+,\cdot$ geschrieben werden.

Anmerkung: Sei $(K,+,\cdot)$ ein Körper. Dann ist $V := K^n = \underbrace{K\times\ldots\times K}_{n\text{-mal}}$ ein $K-Vektorraum$.

Weitere Rechenregeln: Aus den Vektorraum-Eigenschaften lassen sich weitere Rechenregel herleiten (sei V ein K-VR und $v \in V$):
a) $0\cdot v = 0$
b) $\lambda\cdot 0 = 0$
c) $[\lambda\cdot v = 0] \Rightarrow [(\lambda = 0)\vee(v=0)]$
d) $(-1)\cdot v = -v$
Anmerkung: Falls klar ist, dass $(V,+,\cdot)$ ein K-VR ist, so schreibt man nur: V ist ein K-VR.

Sei V ein K-VR und $U \subseteq V$. Falls für die Struktur $(U,+,\cdot)$ gilt:
a) $\forall u,v \in U : (u+v) \in U$
b) $\forall \lambda \in K, u \in U : (\lambda u) \in U$
Dann heißt $(U,+,\cdot)$ ein **Untervektorraum** von V.
(Abkürzung: U ist ein UVR von V)

Anmerkung: Jeder K-VR ist zu sich selbst ein UVR.
Sei K ein Körper. Dann ist K^n ein K-VR. Des weiteren seien $\lambda \in K$, $x,y \in V$ mit $x = (x_1,\ldots,x_n)$ und $y = (y_1,\ldots,y_n)$. Für $i \in \{1,\ldots,n\}$ heißt x_i bzw. y_i der i**-te Eintrag** bzw. i**-te Komponente** von Vektor x bzw. y.

Zur Vektoraddition:
$x+y = (x_1,\ldots,x_n)+(y_1,\ldots,y_n) = (x_1+y_1,\ldots,x_n+y_n)$

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

Anmerkung: Ein Körper K kann selbst als eindimensionaler K-VR aufgefasst werden.

Lineare Gleichungssysteme: Seien $i = 1,\ldots,n$, $j = 1,\ldots,m$, $a_{ij} \in K$, $b_i \in$ Ein **lineares Gleichungssystem (LGS)** mit n Zeilen und m Spalten bzw. Unbekannten x_m:
$\forall i : a_{i1}+\ldots+a_{im} = b_i$
Falls $b_1 = b_2 = \ldots = b_n = 0$, dann ist das LGS **homogen**
Ist mind. ein $b_i \neq 0$, dann ist das LGS **inhomogen.**

Lösbarkeit eines LGS:
- Das LGS kann via **Gauß-Algorithmus** gelöst werden.
- Ein homogenes LGS ist **immer mehrdeutig lösbar.**
- Die **triviale Lösung** eines homogenen LGS ist $x_1 = \ldots = x_m = 0$
- Ein inhomogenes LGS ist **entweder eindeutig, mehrdeutig oder nicht lösbar.**
- Hat das inhomogene LGS **mind. genausoviele Zeilen wie Spalten**, so ist es entweder eindeutig oder nicht lösbar.
- Hat das inhomogene LGS **mehr Spalten als Zeilen**, so ist es entweder mehrdeutig oder nicht lösbar.

Sei V ein K-VR, $v_1,v_2,\ldots,v_r \in V$. Die Vektoren $v_1,v_2,\ldots,v_r$ sind **linear unabhängig**:
$[\lambda_1v_1+\lambda_2v_2+\ldots+\lambda_rv_r = 0] \Rightarrow [\lambda_1 = \lambda_2 = \ldots = \lambda_r = 0]$
Andernfalls sind die Vektoren $v_1,v_2,\ldots,v_r$ **linear abhängig**.

Sei V ein K-VR und $T \subseteq V$ mit $T = \{v_1,\ldots,v_n\}$. Für $\lambda_1,\ldots,\lambda_n \in K$ wird der Vektor $w \in V$:
$w := \sum_{i=1}^n \lambda_i a_i$ als **Linearkombination** der Vektoren aus T bezeichnet.

Anmerkung: Jeder Vektor aus T ist ebenfalls eine Linearkombination von Vektoren aus T, da $a_i = 0\cdot a_1+0\cdot a_2+\ldots+0\cdot a_{i-1}+1\cdot a_i+0\cdot a_{i+1}+\ldots+0\cdot a_n$.

Sei V ein K-VR und $A = \{a_1,\ldots,a_n\} \subseteq V$.
Die **Lineare Hülle** von A ist:
$span(A) := \{\sum_{i=1}^n \lambda_i a_i | \lambda_i \in K, a_i \in A, n \in \mathbb{N}\}$
Es ist die Menge aller Linearkombinationen der Vektoren aus A
Anmerkung: Jeder K-VR V ist zu sich selbst die lineare Hülle, also $span(V) = V$.

Sei V ein K-VR und $\mathcal{A} \subseteq V$. $\mathcal{A}$ heißt **erzeugendes System** von V, falls jeder Vektor aus V als Linearkombination von Vektoren aus $\mathcal{A}$ dargestellt werden kann.
Also $V = span(\mathcal{A})$.
Anmerkung: Wird die Menge $\mathcal{A}$ in einem Tupel geschrieben, so gilt die Reihenfolge der Vektoren im Gegensatz zur Mengenstruktur.

$\mathcal{A}$ heißt **Basis**, wenn zusätzlich gilt, dass alle Vektoren in $\mathcal{A}$ linear unabhängig sind.

Die **Dimension** von V ist gleich der Mächtigkeit seiner Basis.

Anmerkung: Eines K-VR V kann eventuell mehrere Basen haben, jedoch haben alle Basen die gleiche Mächtigkeit.

Für $V = K^n$ wird die Basis $\{e_1,..,e_n\}$ mit:
$e_1 := (1,0,\ldots,0)^T$, $e_2 := (0,1,0,\ldots,0)^T$,..., $e_n := (0,\ldots,0,1)^T$
als **kanonische Basis** bezeichnet.

Austauschlemma von Steinitz: Sei V ein K-VR, $B \subseteq V$ eine Basis von V und $v_1,\ldots v_k \in V$ linear unabhängig.
Die Vektoren aus B können mit den Vektoren $v_1,\ldots,v_k$ ausgetauscht werden. B bleibt weiterhin eine Basis von V.

Basisergänzungs-Satz: Sei V ein K-VR. Jede Menge $E \subseteq V$ mit linear unabhängigen Vektoren, lässt sich durch hinzufügen weiterer Vektoren aus V zu einer Basis von V ergänzen.

Kürzen von Erzeugenden Systemen: Sei V ein K-VR und $E \subseteq V$ ein erzeugendes System von V. Falls die Vektoren in E linear abhängig sind, so kann E zu einer Basis umgewandelt werden, indem Vektoren aus E entfernt werden.

Mengenaddition: Seien M,N Mengen.
$N+M := \{x+y | x \in N, y \in M\}$

Mit der Mengenaddition, dem Basisergänzungs-Satz und Linearkombinationen, lässt sich ein K-VR V als Summe von UVR von V, darstellen.

Seien $U_1,...,U_n$ UVR von V und es gilt:
$[U_1+U_2+...+U_n = V] \quad \wedge \quad [U_1 \cap U_2 \cap ... \cap U_n = \{0_V\}]$
Dann ist: $V = U_1 \oplus U_2 \oplus ... \oplus U_n$ und wird als **direkte Summe** bezeichnet.

Seien $A = \begin{pmatrix} | & & | \\ v_1 & ... & v_k \\ | & & | \end{pmatrix}$,

Durch Zeilenoperationen wird A in die Matrix A' überführt, die in Gauß-Jordan-Form vorliegt. Die Anzahl der " Zeilenabstufungen"ist der **Rang von** A (und somit auch von A' und jeder Matrix, die aus Zeilenoperationen von A resultiert).

Lineare Abbildungen Seien V,W K-VR und $f: V \to W$. Die Abb. f heißt **linear** wenn:
1. $\forall a,b \in V : f(a+b) = f(a) + f(b)$ (f ist also ein Vektorraum-Homomorphismus)
2. $\forall \lambda \in K, a \in V : f(\lambda a) = \lambda f(a)$

Eigenschaften von linearen Abbildungen:
1. Sei $H = \{f \in Abb(V,W) | f \text{ linear}\}$ die Menge aller linearen Abbildungen. mit der Addition von Funktionen und der Skalarmultiplikation bildet H einen K-VR.
Anmerkung: Für $V = K$ mit K Körper bzw. ein K-VR über sich selbst, wird H auch als **Dualraum** bezeichnet mit $V^* := H$.
2. Sei $F: V \to W$, $G: U \to V$ jeweils linear. Dann ist $F \circ G$ auch linear.
3. Sei die lineare Abbildung f invertierbar. Dann ist auch f^{-1} linear.
4. Sei $F: V \to W$ linear und $\mathcal{A} = (a_1,...,a_n)$ Basis von V. F ist bereits eindeutig festgelegt, wenn bereits die Werte $F(a_1),...,F(a_n)$ bekannt sind.

Bild und Kern:
Seien V,W K-VR und $f: V \to W$ eine lineare Abbildung:
$Im(f) := f(V) := \{f(v) | v \in V\}$
$Ker(f) := \{v \in V | f(v) = 0_W\}$
Anmerkung: $Im(f)$ ist ein UVR von W und $Ker(f)$ ist ein UVR von V

Bild-Kern-Formel (Rangsatz):
Seien V,W K-VR und $f: V \to W$ linear.
$\dim(V) = \dim(Im(f)) + \dim(Ker(f))$

Dimensionsformel:
Sei V ein K-VR und U_1, U_2 UVR von V. Dann gilt:
$\dim(U_1+U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2)$
Anmerkung: Die Dimensionsformel hat eine starke Ähnlichkeit mit der Summenregel für die Mächtigkeit von Mengen.

Matrizen Sei K ein Körper, $n,m \in \mathbb{N}$. Dann ist $K^{n \times m}$ die Menge aller Matrizen, mit n Zeilen und m Spalten.
Notation: Sei $A \in K^{n \times m}$, mit Einträgen a_{ij} für $i \in \{1,...,n\}$, $j \in \{1,...,m\}$.
Dann ist: $(a_{ij})_{\substack{i=1,...,n \\ j=1,...,m}} := A$
Ist der Kontext klar, so kann auch $(a_{ij})_{i,j} = A$ geschrieben werden.
Spezialfall Vektor:
Ein Vektor aus K^n kann als $n \times 1$-Matrix aufgefasst werden: $x \in K^{n \times 1}$, bzw. x^T als $1 \times n$-Matrix (also $x^T \in K^{1 \times 1}$)

Sei $l,m,n \in \mathbb{N}$, und K ein Körper. Dann ist die **Matrixmultipliation** "·"wie folgt definiert:
$K^{l \times m} \times K^{m \times n} \to K^{l \times n}$, $(A,B) \mapsto C$
mit $c_{ik} = \sum_{j=1}^{m} a_{ij} \cdot b_{jk}$
Wichtig: Die Spaltenanzahl der linken Matrix muss mit der Zeilenanzahl der rechten Matrix übereinstimmen.
Anmerkung: Mit dem Multiplikationstableau ist es wesentlich schneller zu rechnen, als die Formel in der Definition zu verwenden!

Ausnahme: Seien $x,y \in K^n$ zwei Vektoren. Dann ist $x \cdot y^T$ eine Matrix, die durch die 2 Vektoren im Prinzip der Verknüpfungstabelle äufgespannt"wird.

Seien V,W K-VR und $f: V \to W$ linear. Des weiteren sei $\mathcal{B} = \{b_1,...,b_n\}$ Basis von V und $\mathcal{C} = \{c_1,...,c_m\}$ Basis von W. Für $k \in \{1,...,n\}$ gilt:
$f(b_k) = \lambda_1^{(k)} c_1 + ... \lambda_m^{(k)} c_m$
Dabei ist (k) ein zweiter Index (keine Potenz!).

Die **Abbildungsmatrix von** f **bezüglich den Basen** $\mathcal{B},\mathcal{C}$ ist definiert als:
$M_{\mathcal{C}}^{\mathcal{B}}(f) := \begin{pmatrix} \lambda_1^{(1)} & ... & \lambda_1^{(n)} \\ \vdots & ... & \vdots \\ \lambda_m^{(1)} & ... & \lambda_m^{(n)} \end{pmatrix}$

Lineare Abbildung als Matrixmultiplikation:
Sei V,W K-VR und $f: V \to W$ linear. Des weiteren sei $\mathcal{E}_n$ kanonische Basis von V und $\mathcal{E}_m$ kanonische Basis von W. Dann gilt:
$\forall v \in V : f(v) = M_{\mathcal{E}_m}^{\mathcal{E}_n}(f) \cdot v$

Abbildungsverknüpfung als Matrixmultiplikation:
Seien V,W,Z jeweils K-VR und $f: V \to W$; $g: W \to Z$ jeweils linear. Des weiteren ist $\mathcal{B} = \{b_1,...,b_n\}$ Basis von V, $\mathcal{C} = \{c_1,...,c_m\}$ Basis von W und $\mathcal{D} = \{d_1,...,d_p\}$ Basis von Z
Für die Abbildungsmatrix $g \circ f$ bzgl. den Basen $\mathcal{B}$ und $\mathcal{D}$ gilt:
$M_{\mathcal{D}}^{\mathcal{B}}(g \circ f) = M_{\mathcal{C}}^{\mathcal{B}}(g) \cdot M_{\mathcal{D}}^{\mathcal{C}}(f)$

Spezielle Matrizen:
Sei $A \in K^{n \times m}$. Die Matrix $C \in K^{m \times n}$ heißt **Linksinverse von** A, wenn gilt: $C \cdot A = E_n$
A ist hierbei die **Rechtsinverse von** C und E_n die **Einheitsmatrix**. Letztere ist immer quadratisch und eine spezielle **Diagonalmatrix**!
$\text{diag}(a_1,...,a_n) := \begin{pmatrix} a_1 & 0 & ... & 0 \\ 0 & a_2 & ... & 0 \\ \vdots & & & \vdots \\ 0 & 0 & ... & a_n \end{pmatrix}$,
$E_n = \text{diag}(\underbrace{1,...,1}_{n\text{-mal}})$
Bei einer quadratischen Matrix A, also $A \in K^{n \times n}$, ist die Linksinverse C von A gleichzeitig die Rechtsinverse, und ist zudem eindeutig bestimmt!
Diese (allgemeine) **Inverse** C ist ebenfalls Element in $K^{n \times n}$ und wird als A^{-1} bezeichnet.
Anmerkung: Ein LGS $Ax = b$ lässt sich mithilfe der Inversen A^{-1} lösen, da:
$A^{-1}Ax = A^{-1}b \Rightarrow E_n x = x = A^{-1}b$

Spezielle lineare Abbildungen:
Seien V,W K-VR und $f: V \to W$ linear. Falls $W = V$, also $f: V \to V$, dann ist f ein **Endomorphismus**. **Notation:** $f \in \textbf{End}(V)$
Ist f zusätzlich bijektiv, dann ist f **automorph**.
Notation: $f \in \text{Aut}(V)$.
Anmerkung: Da id eine lineare, bijektive und endomorphe Abbildung ist, gilt: $id \in \text{Aut}(V)$

Sei V ein K-VR, $f \in \text{End}(V)$, $\mathcal{B} = \{b_1,...,b_n\}$,$\mathcal{C} = \{c_1,...,c_n\}$ jeweils Basen von V. Die Matrix $M_{\mathcal{C}}^{\mathcal{B}}(id)$ heißt **Transformationsmatrix** von der Basis $\mathcal{B}$ zur Basis $\mathcal{C}$. Es gilt:
$M_{\mathcal{C}}^{\mathcal{B}}(id) = \left(M_{\mathcal{B}}^{\mathcal{C}}(id)\right)^{-1}$ bzw.
$M_{\mathcal{B}}^{\mathcal{C}}(id) = \left(M_{\mathcal{C}}^{\mathcal{B}}(id)\right)^{-1}$

Basiswechsel/-transformation: Sei V ein K-VR, $f \in \text{End}(V)$, $\mathcal{B} = \{b_1,...,b_n\}$,$\mathcal{C} = \{c_1,...,c_n\}$, und $\mathcal{A} = \{a_1,...,a_n\}$ jeweils Basen von V. Dann gilt:
$M_{\mathcal{C}}^{\mathcal{B}}(f) = M_{\mathcal{C}}^{\mathcal{A}}(id) \cdot M_{\mathcal{A}}^{\mathcal{A}}(f) \cdot M_{\mathcal{A}}^{\mathcal{B}}(id)$ bzw.
$M_{\mathcal{C}}^{\mathcal{B}}(f) = \left(M_{\mathcal{A}}^{\mathcal{C}}(id)\right)^{-1} \cdot M_{\mathcal{A}}^{\mathcal{A}}(f) \cdot M_{\mathcal{A}}^{\mathcal{B}}(id)$

Sei K Körper und $A \in K^{n \times m}$,
mit $n > 1, m > 1$. Die Matrix $A_{[i,j]} \in K^{(n-1) \times (m-1)}$ heißt **Streich/Untermatrix** von A. Sie entsteht durch das Entfernen/Löschen/Streichen der i-ten Zeile und der j-ten Spalte.

Sei $A \in K^{n \times n}$ eine Matrix. Die **Determinante** einer Matrix lässt sich wie folgt bestimmen:
1) Falls A eine 1×1-Matrix ist, dann $\det(A) = a_1 1$ die Determinante.
2) Falls $n > 1$, so wende den **Laplaceschen Entwicklungssatz** an:
$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{[i,j]})$
$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{[i,j]})$
WARNUNG: Die Sarrus-Regel gilt nie für 4×4 oder größer!

Determinantenregeln:
- Jede Zeilen und/oder Spaltenoperation ändert die Determinante nicht.
- Die Multiplikation von entweder einer Zeile oder einer Spalte mit $\lambda \in K$, multipliziert die ganze Determinante mit λ. $\Rightarrow \det(\lambda A) = \lambda^n A$
- Das Vertauschen von entweder einer Zeile oder einer Spalte ändert das Vorzeichen der Determinante.

Zusammenfassung LGS:
Sei $f \in End(V)$, $\mathcal{A},\mathcal{B}$ Basen von V und $A = M_{\mathcal{B}}^{\mathcal{A}}(f)$.
Dann sind folgende Aussagen äquivalent:
- A ist invertierbar
- A hat den vollen Rang. Also $rang(A) = n$
- A ist invertierbar
- Das homogene LGS $Ax = 0$ ist eindeutig lösbar.
- $\det(A) \neq 0$
- f ist surjektiv
- f ist injektiv

Sei $v \in K^n, A \in K^{n \times n}, \lambda \in K$. Falls die Gleichung $Av = \lambda v$ erfüllt ist, so heißt λ **Eigenwert** von A und v **Eigenvektor** von A.

Sei $\lambda \in K, A \in K^{n \times n}$. Das Polynom: $\det(A - \lambda E_n)$ heißt **Charakteristisches Polynom**. Die Nullstellen dieses Polynom sind die **Eigenwerte von** A.

Sei $A \in \mathbb{K}^{n \times n}$. Sei $p(X) = a_0 E_n + a_1 X + ... + a_n X^n$ ein Polynom mit matrixwertigen Unbekannten. Das Polynom p heißt **Minimalpolynom** von A, wenn für kleinstmöglichstes n gilt: $p(A) = 0_{K^{n \times n}}$
Anmerkung: Sei n^* das minimalste n des Minimalpolynoms p von A. Die Nullstellen des Polynoms $p^*(x) = a_0 + a_1 x + ... + a_{n^*} x^{n^*} \in K[t]$ sind die Eigenwerte von A und zugleich die Nullstellen des charakteristischen Polynoms.
Das Polynom p^* hat also die selbe Gestalt wie das Minimalpolynom p.
Anmerkung: Das Minimalpolynom ist ein Teil des charakteristischen Polynoms.

Sei $f \in \text{End}(V)$, A Abbildungsmatrix von f und λ Eigenwert von A.
Der Raum $\text{Eig}(f,\lambda) := ker(f - \lambda id)$ heißt **Eigenraum** von A bzgl. λ. Jeder Eigenvektor v bzgl. λ liegt in $\text{Eig}(f,\lambda)$.
Die Vorkommen von λ als Nullstelle von $\det(A - \lambda E_n)$ heißt **algebraische Vielfachheit**, die Dimension von $\text{Eig}(f,\lambda)$ ist die **geometrische Vielfachheit** von λ.

Die Matrix $A \in K^{n \times n}$ heißt **diagonalisierbar**, wenn es eine Diagonalmatrix D und invertierbare Matrix S gibt: $SAS^{-1} = D$
Anmerkung: A ist genau dann diagonalisierbar, wenn für jeden Eigenwert λ von A jeweils in ihrer algebraischen und geometrischen Vielfachheit entsprechen. Dann ist $S = (\text{Eig}(A,\lambda_1),...,\text{Eig}(A,\lambda_n))$ und $D = \text{diag}(\lambda_1,....,\lambda_n)$