1.2 Mengen

Potenzmenge: $P(M) = \{X|X\subseteq M\}$, $|P(M)| = 2^{|M|}$

1.3 Abbildungen

$f(z)$ heißt **Bild von z** unter f, $f^{-1}(z)$ heißt **Urbild von z**.

Eingeschränkte Abbildung: $f|_{X'}: X'\to Y$ mit $f|_{X'}(x)=f(x)\ \forall x\in X'$

Eine Abb. $f: X\to Y$ heißt

- **injektiv** $\Leftrightarrow \forall x,x'\in X, x\neq x': f(x)\neq f(x')$ (versch. El. haben versch. Bilder)
- **surjektiv** $\Leftrightarrow f(X)=Y$ (jedes $y\in Y$ hat mind. ein Urbild)
- **bijektiv** $\Leftrightarrow$ inj. und surj. (jedes $y\in Y$ hat genau ein Urbild) oder falls $f^{-1}: Y\to X$ existiert mit $f^{-1}(f(x))=x\ \forall x\in X$. f^{-1} ist dann eindeutig, bijektiv und heißt **inverse Abb.** zu f, $(f^{-1})^{-1}=f$.

Für $f: X\to Y$ und $g: Y'\to Z$ mit $Y\subseteq Y'$ heißt $g\circ f: X\to Z$ mit $g\circ f(x)=g(f(x))\ \forall x\in X$ **Komposition**. Falls f und g inj./surj./bij., so auch $g\circ f$ inj./surj./bij.

$h\circ(g\circ f)=(h\circ g)\circ f$ (assoziativ). $id_X: X\to X$ mit $id_X(x)=x\ \forall x\in X$ heißt **identische Abb.**, $f\circ id_X=id_X\circ f=f$. $f^{-1}\circ f=id_X$. Falls f und g bijektiv, $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

1.4 Mächtigkeit von Mengen

Seien X und Y endliche Mengen. Es existiert $f: X\to Y$, so dass: f ist surjektiv $\Leftrightarrow |X|\geq|Y|$, f ist injektiv $\Leftrightarrow |X|\leq|Y|$, f ist bijektiv $\Leftrightarrow |X|=|Y|$.

Unendliche Mengen sind **gleichmächtig**, wenn es eine bijektive Abb. zwischen den beiden gibt; **abzählbar** dann, wenn es eine bij. Abb. von $\mathbb{N}$ in die Menge gibt, sonst **überabzählbar** ($\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ abz., $\mathbb{R}$ überabz.).

1.5 Relationen

$xRy \Leftrightarrow (x,y)\in R$, wobei $R\subseteq M\times M$. R ist

- **reflexiv** $\Leftrightarrow \forall x\in M: xRx$
- **symmetrisch** $\Leftrightarrow \forall x,y\in M: xRy \Rightarrow yRx$
- **antisymmetrisch** $\Leftrightarrow \forall x,y\in M: xRy \wedge yRx \Rightarrow x=y$
- **transitiv** $\Leftrightarrow \forall x,y,z\in M: xRy \wedge yRz \Rightarrow xRz$

Eine ref., sym. und trans. Relation $\sim$ heißt **Äquivalenzrelation**. Für $x\in X$ heißt $[x]_\sim=\{y\in M|x\sim y\}$ **Äquivalenzklasse** von x, die Menge der Äquivalenzklassen ist eine **Partition** von M. Eine ref., antisym. und trans. Relation heißt **Halbordnung**. Für eine **totale Ordnung** gilt zudem $\forall x,y\in M: xRy \vee yRx$.

2.1 Vollständige Induktion und Rekursion

$\forall n\in\mathbb{N}$ sei A eine Aussage, dann gilt: $A(1) \wedge (\forall n\in\mathbb{N}: A(n) \Rightarrow A(n+1)) \Rightarrow (\forall n\in\mathbb{N}: A(n))$.

(Kann auf $n\geq n_0$ und $(A(n_0), \ldots, A(n)) \Rightarrow A(n+1)$ verallgemeinert werden.)

2.2 Modulare Arithmetik

$a\neq 0$ ist **Teiler** von b $(a|b)$, falls q existiert mit $b=a\cdot q$ $(a,b,q\in\mathbb{Z})$, 1 und b sind **triviale Teiler**. $a|b \Rightarrow a|b\cdot c$, $a|b \wedge b|c \Rightarrow a|c$, $a|b \wedge a|c \Rightarrow a|(s\cdot b+t\cdot c)$, $a|(b+c) \wedge a|b \Rightarrow a|c$, $a|b \Leftrightarrow a\cdot c|b\cdot c$ falls $c\neq 0$, $a|b \wedge b|a \Rightarrow a=\pm b$. Für $a,b\in\mathbb{Z}$, $b\neq 0$ gibt es $q,r\in\mathbb{Z}$ so dass $a=q\cdot b+r$ und $0\leq r<|b|$, q und $r=$**a mod b** sind eindeutig.

Dann heißt die größte nat. Zahl n mit $n|a \wedge n|b$ **ggT(a,b)**, a und b **teilerfremd** $\Leftrightarrow$ $ggT(a,b) = 1$, $ggT(a,b)=ggT(b,a)=ggT(-a,b)=ggT(a,-b)=ggT(-a,-b)=ggT(a+m\cdot b,b)=ggT(a \bmod b,b)$.

Für $a,b\in\mathbb{N}$ und $a\geq b$ ist $ggT(a,b)$: Berechne $r=a \bmod b$; ist $r=0$, dann $ggT(a,b)=b$ (Stop); berechne $ggT(b, a \bmod b)$.

a und b sind **kongruent mod m** ($a\equiv b \pmod m$), falls $a \bmod m=b \bmod m$.

$(a+b) \bmod m = ((a \bmod m)+(b \bmod m)) \bmod m$
$(a\cdot b) \bmod m = ((a \bmod m)\cdot(b \bmod m)) \bmod m$

2.3 Gruppen, Ringe, Körper

Eine Verknüpfung $\circ$ auf M ist
- **kommutativ** $\Leftrightarrow a\circ b=b\circ a$
- **assoziativ** $\Leftrightarrow \forall a,b,c\in M: (a\circ b)\circ c=a\circ(b\circ c)$

Für einen Ring mit Eins $(R,+,\cdot)$ heißt $x\in R$ **Einheit**/invertierbar, falls ein $y\in R$ existiert mit $x\cdot y=y\cdot x=1$. R^* enthält alle Einheiten in R, $(R^*,\cdot)$ ist eine Gruppe, $x\in\mathbb{Z}_m$ ist Einheit $\Leftrightarrow ggT(x,m)=1$.
Für einen kom. Ring mit Eins $(R,+,\cdot)$ und eine Unbestimmte x ist ein Ausdruck der Form $a_0x^0+\ldots+a_nx^n=\sum_{i=0}^{n}a_ix^i$ mit $n\in\mathbb{N}_0$ und $a_i\in R$ ein **Polynom** über R. Falls $a_i=0$, **Grad(P)**$=-\infty$, sonst $Grad(P)=\max_i\{a_i\neq 0\}$. R[x] enthält alle Polynome über R.

2.4 Komplexe Zahlen

Man schreibt $a=(a,0)$, $i=(0,1)$ (**imaginäre Einheit** $i^2=-1$), $b\cdot i=(0,b)$, $a+b\cdot i=(a,b)$. Für $z=a+b\cdot i$ ist $Re(z)=a$ **Realteil** und $Im(z)=b$ **Imaginärteil**. **Betrag**: $|z|=\sqrt{a^2+b^2}$.
Konjugiert-komplexe Zahl: $\overline{z}$=a-b·i. $\overline{z+w}=\overline{z}+\overline{w},\ \overline{z\cdot w}=\overline{z}\cdot\overline{w},\ |z|^2=z\cdot\overline{z},\ z^{-1}=\overline{z}/|z|^2,\ z\neq 0$.
$|z|\geq 0$, $|z|=0\Leftrightarrow z=0$, $|z\cdot w|=|z|\cdot|w|$, $|z+w|\leq|z|+|w|$.
Jedes $z\in\mathbb{C}$, $z\neq 0$ kann eindeutig dargestellt werden als $z=r\cdot(\cos\varphi+i\cdot\sin\varphi)=r\cdot e^{\varphi i}$, $r\in\mathbb{R}_{\geq 0}$, $\varphi\in[0,2\pi]$, $r=|z|$ und φ der Winkel zwischen z und der reellen Achse.
$\cos\phi=\frac{Re(z)}{|z|},\ \sin\phi=\frac{Im(z)}{|z|}$, $e^{\pi i}=-1$, $z\cdot z'=r\cdot r'\cdot(\cos(\varphi+\varphi')+i\cdot\sin(\varphi+\varphi'))$
Quadratwurzel: $\sqrt[n]{z}=\sqrt[n]{r}\cdot(\cos\frac{\varphi}{n}+i\cdot\sin\frac{\varphi}{n})$ bzw. allgemein: $c_k=\sqrt[n]{r}\cdot(\cos\frac{\varphi}{n}+i\cdot\sin\frac{\varphi}{n})\cdot\omega_n^k$ so dass $c_k^n=z$ mit $k=0,\ldots,n-1$ und n-ter Einheitswurzel $\omega_n^k=\cos\frac{2k\pi}{n}+i\cdot\sin\frac{2k\pi}{n},\ \omega_n^0=1$.
Für ein Polynom $f\in\mathbb{C}[x]$ gibt es $c_1,\ldots,c_n\in\mathbb{C}$ so dass $f(x)=a\cdot(x-c_1)\cdot\ldots\cdot(x-c_n)$, $a\in\mathbb{C}$.

3.1 Lineare Gleichungssysteme und Matrizen

Ein lin. GS heißt **homogen**, wenn die letzte Spalte der erw. Koeff.-Mat. 0 ist, ein hom. GS hat immer die triviale Lösung 0.
Elementare Zeilenumformungen auf $\mathbb{K}^{m\times n}$ sind $V_{k,l}$: $\mathbb{K}^{m\times n}\to\mathbb{K}^{m\times n}$ und $A_{k,l}(c)$: $\mathbb{K}^{m\times n}\to\mathbb{K}^{m\times n}$ und $M_k(c)$: $\mathbb{K}^{m\times n}\to\mathbb{K}^{m\times n}$ für $c\neq 0$, diese sind darstellbar als **Elementarmatrizen**:
El_{ij} wie E_n, aber $(i,i)=(j,j)=0$ und $(i,j)=(j,i)=1$.
$El_i(\lambda)$ wie E_n, aber $(i,i)=\lambda$.
$El_{ij}(\lambda)$ wie E_n, aber $(j,i)=\lambda$.
$El_{ij}^{-1}=El_{ij}$, $El_i(\lambda)^{-1}=El_i(\lambda^{-1})$, $El_{ij}(\lambda)^{-1}=El_{ij}(-\lambda)$.
Für $A\in\mathbb{K}^{m\times n}$, $B,C\in\mathbb{K}^{n\times l}$ gilt $A\cdot B$="Spalte mal Zeile" mit $A\cdot B\in\mathbb{K}^{m\times l}$ und $A\cdot(B+C)=A\cdot B+A\cdot C$.

3.2 Vektorräume

In VR gilt $\forall v\in V\ \forall\alpha\in\mathbb{K}$: $0\cdot v=0$, $\alpha\cdot 0=0$, $\alpha\cdot v=0\Leftrightarrow\alpha=0\ \vee\ v=0$, $(-\alpha)\cdot v=-(\alpha\cdot v)$.
Für $A\in\mathbb{K}^{m\times n}$ ist die Lösungsmenge $\{x\in\mathbb{K}^n|A\cdot x=0\}$ des hom. LGS $A\cdot x=0$ Teilraum von $\mathbb{K}^n$.
Für V $\mathbb{K}$-VR und $U_1,U_2\leq V$ sind $U_1\cap U_2$ und $U_1+U_2=\{u_1+u_2|u_1\in U_1,u_2\in U_2\}$ Unterräume von V.
$v\in V$ ist **Linearkombination** von $u_1,\ldots,u_n$, wenn $\exists\alpha_i\in\mathbb{K}$: $\alpha_1u_1+\ldots+\alpha_nu_n=v$.
Für $M\subseteq V$ ist $\langle M\rangle=\{v\in V|v$ ist Lin.komb. endlich vieler El. aus M$\}$ das **Erzeugnis** von M, $\langle\{\}\rangle=\{0\}$, $\langle M\rangle\leq V$. M ist **linear unabhängig**, wenn $\forall v\in M$: $\langle M\backslash\{v\}\rangle\neq\langle M\rangle$ bzw. für jede endliche Teilmenge $\{v_1,\ldots,v_n\}\subseteq M$ gilt: $\alpha_1v_1+\ldots+\alpha_nv_n=0\Rightarrow\alpha_i=0$.
M ist **Basis** von V, falls jedes $v\in V$ eindeutig als Lin.komb. aus M darstellbar ist, also falls $\langle M\rangle=V$ und M lin. unabh. $\{\}$ ist Basis für $\{0\}$. Für eine Basis $B=\{b_1,\ldots,b_n\}$ und $v\in V$, $v\neq 0$ gibt es ein b_iB s.d. $\{b_1,\ldots,b_{i-1},v,b_{i+1},\ldots,b_n\}$ auch Basis ist. n heißt **Dimension** von V,

jede Basis von V hat n Elemente (also B Basis ⇔ |B|=dim V und B lin. unabh.), dim {0}=0. Für eine geordnete Basis $(b_1,\dots,b_n)$ sind $x_1,\dots,x_n\in\mathbb{K}$ mit $v=x_1b_1+\dots+x_nb_n$ **Koordinaten** von v bzgl. der Basis B.

3.3 Lineare Abbildungen

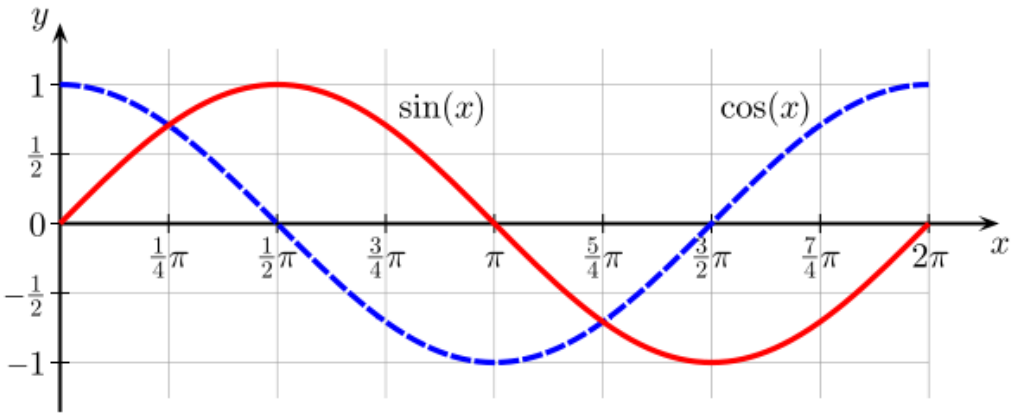
Für $\mathbb{K}$-VR U,V heißt f: U→V **linear**, falls $\forall u_1,u_2\in U\ \forall\lambda\in\mathbb{K}$:
- $f(u_1+u_2) = f(u_1)+f(u_2)$
- $f(\lambda\cdot u_1) = \lambda\cdot f(u_1)$

bzw. wenn $\exists A\in\mathbb{K}^{m\times n}$: $f(x)=A\cdot x$ (A mit den Spalten s_i).
U und V sind **isomorph**, wenn es einen **Isomorphismus** (bij. lin. Abbildung f: U→V) gibt bzw. wenn dim U=dim V. Ist f Isomorphismus, so auch f^{-1}. Sind f(x)=A·x und g(x)=B·x linear, so auch $g\circ f(x)=(B\cdot A)\cdot x$.
Rang(A) ist die max. Anzahl lin. unabh. Spalten-/Zeilenvektoren in A:
$\text{Rang}(A) = \dim \langle s_1,\dots,s_n\rangle$
Kern(f) $= \{u\in U \mid f(u)=0\} = \{x\in\mathbb{K}^n \mid A\cdot x=0\} \leq U$
Bild(f) $= \{v\in V \mid \exists u\in U: f(u)=v\} = \langle s_1,\dots,s_n\rangle \leq V$
dim Kern(f) + dim Bild(f) = dim U
dim Bild(f) = Rang(A)
dim Kern(f) = dim U - Rang(A)
Für quadratische Matrizen $A\in\mathbb{K}^{n\times n}$ gilt:
- f(x)=A·x bij.
- ⇔ Spalten/Zeilen von A sind lin. unabh.
- ⇔ Rang(A)=n
- ⇔ $\exists A^{-1}\in\mathbb{K}^{n\times n}$: $A\cdot A^{-1}=A^{-1}\cdot A=E_n$, dann ist A invertierbar und A^{-1} die **inverse Matrix** von A.

$(A^{-1})^{-1}=A$, $(A_1\cdot A_2)^{-1}=A_1^{-1}\cdot A_2^{-1}$.
Berechnen von A^{-1}: $(A|E_n)$ in die Form $(E_n|A^{-1})$ bringen; falls nicht möglich, ist A nicht invertierbar. (Falls $A\cdot A^T=E_n$, A orthogonal und $A^{-1}=A^T$.)

3.4 Gleichungssysteme "aus Expertensicht"

Für $A\in\mathbb{K}^{m\times n}$, $b\in\mathbb{K}^m$ hat das LGS A·x=b
- keine Lösung ⇔ Rang(A)<Rang(A|b) (b ist nicht aus A erzeugbar)
- eine Lösung ⇔ Rang(A)=n (Lösungen $L_b=w+\text{Kern}(A)$, $w\in L_b$)
- viele Lösungen ⇔ Rang(A)=Rang(A|b)<n (n-Rang(A) freie Variablen)



Algebraische Strukturen

Notation	Struktur	Bedingungen
$(M,\circ)$	**Halbgruppe**	$\circ$ assoziativ
	Monoid	Halbgruppe + $\exists e \forall x \in M: e\circ x=x\circ e=x$
	Gruppe	Monoid + $\forall x \exists x^{-1} \in M: x\circ x^{-1}=x^{-1}\circ x=e$
	kom. Gruppe	Gruppe + $\circ$ kommutativ
	Untergruppe	$M \subseteq M'$, $e_{(M',\circ)} \in M$, $\forall a,b \in M: a\circ b \in M$, $a^{-1} \in M$
$(R,+,\cdot)$	**Ring**	$(R,+)$ kom. Gruppe, $(R,\cdot)$ Halbgruppe, $\forall x,y,z \in R: x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
	Ring mit 1	Ring + $(R,\cdot)$ Monoid, $e_{(R,\cdot)} \neq e_{(R,+)}$
	kom. Ring	Ring + $\cdot$ kommutativ
	Unterring	$R \subseteq R'$, $(R,+)$ Untergruppe von $(R',+)$, $\forall x,y \in R: x\cdot y \in R$
$(\mathbb{K},+,\cdot)$	**Körper**	Ring + jedes $x\neq 0$ hat ein $x^{-1}_{(\mathbb{K},\cdot)}$ *oder* $(\mathbb{K},+)$ und $(\mathbb{K}\setminus\{0\},\cdot)$ kom. Gruppen, Distributivität
$(V,\oplus,\odot,(\mathbb{K},+,\cdot)$	**$\mathbb{K}$-Vektorraum**	$(V,\oplus)$ kom. Gruppe, $\forall v,w \in V\ \forall \alpha,\beta \in \mathbb{K}: 1\odot v=v$, $(\alpha\cdot\beta)\odot v=\alpha\odot(\beta\odot v)$, $(\alpha+\beta)\odot v=\alpha\odot v\oplus\beta\odot v$, $\alpha\odot(v\oplus w)=\alpha\odot v\oplus\alpha\odot w$
	Unterraum	$V \subseteq V'$, $0 \in V$, $\forall v,w \in V\ \forall \alpha \in \mathbb{K}: (\alpha\cdot v)+w \in V$

Beispiele für Strukturen

Menge	Struktur	Verknüpfungen
$R[x]$	kom. Ring mit 1	$+,\cdot$ intuitiv
$\mathbb{Z}_m$	kom. Ring mit 1	$+_m,\cdot_m$ (Modulo-Rechnen), $m \in \mathbb{N}$, $m \geq 2$
$\mathbb{Z}_p$	Körper	$+_m,\cdot_m$ (Modulo-Rechnen), $m \in \mathbb{N}$, m prim
$\mathbb{C}=\mathbb{R}\times\mathbb{R}$	Körper	$(a,b)\oplus(a',b')=(a+a',b+b')$ $(a,b)\odot(a',b')=(a\cdot a'-b\cdot b',a\cdot b'+a'\cdot b)$ $e_\oplus=(0,0)$, $x^{-1}{}_\oplus=(-a,-b)$, $e_\odot=(1,0)$, $x^{-1}{}_\odot=(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2})$
$\mathbb{K}^{n\times n}$	Ring mit 1	+ ist Matrixadd., $\cdot$ ist Matrixmult.
$\mathbb{K}^{m\times n}$	$\mathbb{K}$-Vektorraum	+ ist Matrixadd., $\cdot$ ist Skalarmult.

	0°	30°	45°	60°	90°	120°	135°	150°	180°
sin	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
cos	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{\sqrt{2}}{2}$	$-\frac{\sqrt{3}}{2}$	-1
arc	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{3\pi}{4}$	$\frac{5\pi}{6}$	π

$\sin^2 x+\cos^2 x=1$