# Wie kann man die Normalform (bzgl. Affinen Transformationen) bestimmen, ohne die affine Abbildung bzw. Isometrie zu finden?

**Antwort in Dim 2:** Sei $Q$ eine Quadrik in $\mathbb{R}^2$ gegeben durch

$$(x_1 \ \cdots \ x_n) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + (a_1 \ \cdots \ a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + a = 0.$$

Bezeichnung $\Delta = det(Erw_Q)$, $\delta = det(A)$, $S = spur(A)$.

Bemerkung Man kann für $S$ immer $S \geq 0$ annehmen, indem man die Gleichung der Quadrik mit $-1$ multipliziert.

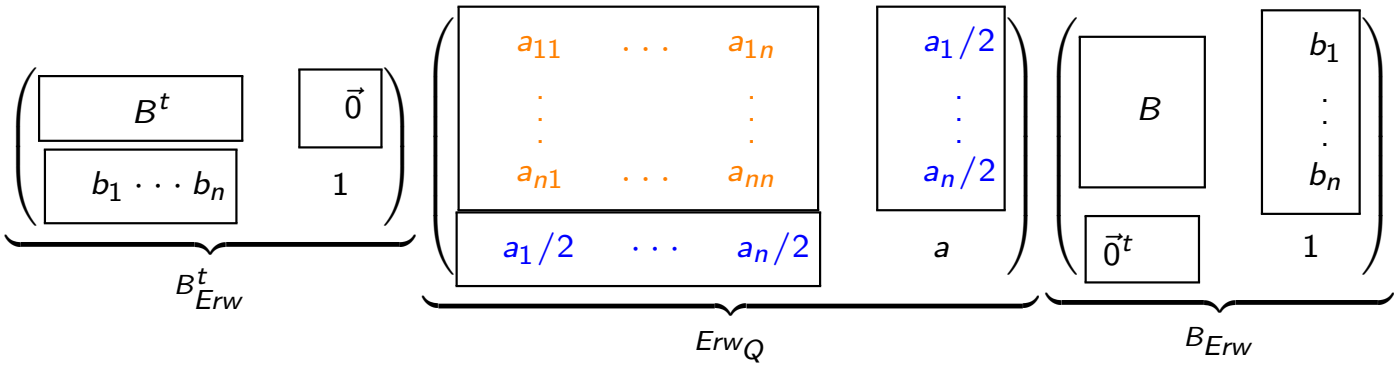
**Satz 20** *Angenommen $S \geq 0$. Es gilt:*

* *ist $\delta > 0$ und $\Delta < 0$, dann ist die Quadrik eine Ellipse,*
* *ist $\delta < 0$ und $\Delta \neq 0$, so ist die Quadrik eine Hyperbel.*
* *ist $\delta = 0$ und $\Delta \neq 0$, so ist die Quadrik eine Parabel.*
* *ist $\delta = 0$ und $\Delta = 0$, so ist die Quadrik ein paralleles Geradenpaar oder eine Gerade.*
* *ist $\Delta = 0$ und $\delta > 0$, so ist die Quadrik gleich $\varnothing$.*
* *ist $\Delta = 0$ und $\delta < 0$, so ist die Quadrik ein Geradenpaar mit Schnittpunkt.*

**Bemerkung** Nur die Vorzeichen von $\Delta$ und $\delta$ werden benutzt

**Frage** Was passiert mit $\Delta = det(Erw_Q)$ und $\delta = det(A)$ nach einer Isomertrie $F$?

Lemma 12: Sei $F^{-1} = b + Bx$ mit $B \in O(n)$. $Q_1 := Bild_F(Q)$. Dann ist $Erw_Q =$




Nach Lemma 12 ist $Erw_{Q_1} = B^t_{Erw} Erw_Q B_{Erw}$. Dann ist $det(Erw_{Q_1}) = det(B^t_{Erw}) det(Erw_Q) det(B_{Erw}) \overset{\text{Weil } det(C) = det(C^t)}{=} \underbrace{det(B_{Erw})^2}_{>0} \Delta$. Also wird das Vorzeichen von $\Delta$ nicht geändert.

Ähnlich: Weil $A_1 = B^t A B$ ist, ist $det(A_1) = \underbrace{det(B)^2}_{=1} \underbrace{\delta}_{det(A)}$. Also wird das Vorzeichen von $\delta$ nicht geändert.

Analog wird Spur von $A$ nicht geändert, weil $Spur(B^t A B) = Spur(B^{-1} A B) = Spur(A)$.

Dann genügt es, Satz 20 nur für Gleichungen, die bereits in Normalform sind, zu beweisen

Die Tabelle unten listet alle 2-Dimensionale Quadriken. Wir nehmen an, dass $\lambda > 0, \mu > 0$.

| Quadrik | $Erw_Q$ | $\Delta$ und $\delta$ |
|---|---|---|
| Ellipse | $\begin{pmatrix} \lambda & & \\ & \mu & \\ & & -1 \end{pmatrix}$ | $\Delta = -\lambda\mu,\ \delta = \lambda\mu$ |
| Hyperbel | $\begin{pmatrix} \lambda & & \\ & -\mu & \\ & & \pm 1 \end{pmatrix}$ | $\Delta = \mp\lambda\mu,\ \delta = -\lambda\mu$ |
| Parabel | $\begin{pmatrix} \lambda & & \\ & 0 & 1 \\ & 1 & \end{pmatrix}$ | $\Delta = \lambda,\ \delta = 0$ |
| paralleles Geradenpaar oder eine Gerade | $\begin{pmatrix} \lambda & & \\ & 0 & \\ & & -\mu \end{pmatrix}$ | $\Delta = 0,\ \delta = 0$ |
| $\varnothing$ | $\begin{pmatrix} \lambda & & \\ & \mu & \\ & & 1 \end{pmatrix}$ | $\Delta = \lambda\mu,\ \delta = \lambda\mu$ |
| Geradenpaar mit einem Schnittpunkt | $\begin{pmatrix} \lambda & & \\ & -\mu & \\ & & 0 \end{pmatrix}$ | $\Delta = 0,\ \delta = -\lambda\mu$ |

Wir sehen, dass die Vorzeichen von $\delta$ und $\Delta$ den Typ der Quadrik eindeutig bestimmt.

# Existenz einer Quadrik durch 5 Punkte

**Satz 21** *Seien $X_1, ..., X_5$ 5 verschiedene Punkte im $\mathbb{R}^2$. Dann existiert eine Quadrik $Q$, die diese 5 Punkte enthält.*

**Beweis.** Die Gleichung der Quadrik sieht wie folgt aus:

$$(x\ y)\begin{pmatrix} a_{11} & \frac{a_{12}}{2} \\ \frac{a_{12}}{2} & a_{22} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + a_1 x + a_2 y + a = 0 \iff$$

$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1 x + a_2 y + a = 0$ Wenn die 5 Punkte $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$,... ,$\begin{pmatrix} x_5 \\ y_5 \end{pmatrix}$ auf der Quadrik liegen, ist das folgende lineare Gleichungsystem erfüllt:

$$\underbrace{\begin{pmatrix} x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^2 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^2 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^2 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \end{pmatrix}}_{C} \begin{pmatrix} a_{11} \\ a_{12} \\ a_{22} \\ a_1 \\ a_2 \\ a_0 \end{pmatrix} = \vec{0}.$$ Nach der Dimensionsformel ist

$$dim(Kern_C) = 6 - \underbrace{dim(Bild_C)}_{\leq 5} \geq 1,$$ also gibt es eine Lösung. □

Man kann zeigen, durch Analyse des Gleichungssystems auf der vorherigen Folie, dass zwei verschiedene Quadriken in Dimension 2, von denen eine nicht ausgeartet ist, höchstens 4 Schnittpunkte haben können.
Ausgeartete Quadriken können mehr als 4 Schnittpunkte haben: etwa zwei Quadriken, gegeben durch die Gleichungen

$$(x-y)(x+2y) \quad \text{und} \quad (x-y)(x+3y)$$

haben unendlich viele gemeinsame Punkte.

# Warum sind Quadriken interessant

1. Vor 100 Jahren: Nach den Keplerschen Gesetzen sind die Bahnkurven von astronomischen Objekten Quadriken (z.B. sind Planetenorbits Ellipsen). Um die Koordinaten seines Schiffs (auf See) auszurechnen, konnte der Kapitän nur astronomische Objekte (+ präzise Uhr) benutzen. Die Geometrie der Quadriken spielte deshalb eine große Rolle in der Ausbildung von Kapitänen.

2. In der Analysis von Funktionen mehrerer Veränderlicher:
Mehrdimensionale Taylor-Reihe (Ana II/III)

**Satz (Taylorentwicklung, Ana II)** *Sei $f : \mathbb{R}^n \to \mathbb{R}$ eine glatte Funktion (z.B. existieren die* $\underbrace{\textit{dritten partiellen Ableitungen}}_{\textit{mehrdimensionale Verallgemeinerung der Ableitung, wird in Ana II erklärt}}$ *und sind stetig). Sei* $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ *ein Punkt. Dann gilt:*

$$f(x) := \underbrace{f(z)}_{a_0} + \underbrace{\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(z) \cdot (x_i - z_i)}_{a^t(x-z)} + \frac{1}{2} \underbrace{\sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_i \, \partial x_j}(z)(x_i - z_i)(x_j - z_j)}_{(x-z)^t A (x-z)} + \underbrace{Rest(x-z)}_{mit \ \frac{Rest(x-z)}{|x-z|^2} \ für \ x \to z \ \to 0}$$

Also, bis auf den $Rest(x-z)$ (welcher in der Nähe von $z$ klein ist), ist jede Funktion eine quadratische Funktion von $y := x - z$ mit $a_0 = f(z)$, $a_i = \frac{\partial f}{\partial x_i}(z)$ und $A_{ij} = \frac{1}{2} \frac{\partial^2 f}{\partial x_i \partial x_j}$.
Dann ist die Menge $\{x \in \mathbb{R}^n \mid f(x) = \text{const}\}$, für $x$ in der nähe des Punktes $z$ und für const, welche nah zu $a_0$ ist, "fast" eine Quadrik.

# Der projektive Raum $P(V)$ und projektive Transformationen

$(V, +, \cdot)$ sei ein Vektorraum (über $\mathbb{K}$).

**Def.** Der zu $V$ gehörige projektive Raum $P(V)$ ist definiert als die Menge aller 1-dimensionalen Untervektorräume von $V$ . Ist $dim(V) < \infty$, so setzt man $dim(P(V)) := dim(V) - 1$. (Nach Def. ist $P(\{\vec{0}\}) = \varnothing$ und $dim(P(\{\vec{0}\})) = -1$ – wir können damit leben.)

**Bemerkung.** Man hat eine kanonische Abbildung ("Projektion") $V \setminus \{\vec{0}\} \to P(V), v \mapsto \mathcal{L}_v := \{\lambda v | \lambda \in \mathbb{K}\}$.

# Homogene Koordinaten

Auf $\mathbb{K}^{n+1} \setminus \{\vec{0}\}$ betrachten wir die folgende Äquivalenzrelation:
$(v_0, ..., v_n) \sim (\tilde{v}_0, ..., \tilde{v}_n) \Leftrightarrow \exists \lambda \neq 0 \text{ sodass } (\lambda v_0, ..., \lambda v_n) = (\tilde{v}_0, ..., \tilde{v}_n)$.
**Bsp.** $\begin{pmatrix}1\\0\\2\end{pmatrix} \sim \begin{pmatrix}2\\0\\4\end{pmatrix} \sim \begin{pmatrix}-2\\0\\-4\end{pmatrix} \not\sim \begin{pmatrix}1\\2\\3\end{pmatrix}$.
Wir schreiben die Äquivalenzklasse des Elementes $(v_0, ..., v_n)$ wie folgt:

$$[(v_0, ..., v_n)] = (\ v_1 :\ v_2 : ... :\ v_n).$$

Für jeden Element von $P(\mathbb{K}^{n+1})$, also, für jede Gerade (durch $\vec{0}$)
$\mathcal{L}_v := \{\lambda(v_0, ..., v_n) \mid \lambda \in \mathbb{K}\}$ ordnen wir das Element $(v_1 : v_2 : ... : v_n)$
von $\left(\mathbb{K}^n \setminus \{\vec{0}\}\right) / \sim$.

Die Abbildung ist wohldefiniert, weil zwei Richtungsvektoren die gleiche Gerade definieren, genau dann wenn sie proportional sind.

Die Abbildung heisst Koordinatenabbildung und Bild des Elements $\mathcal{L} \in P(\mathbb{K}^{n+1})$ heisst der (homogene) Koordinatenvektor von $\mathcal{L}$.

# Affines Koordinatensystem auf $P(V)$

Wir betrachten eine Hyperebene $H$ in $V$, $H = \{a_0 + u \mid u \in V_H\}$, $dim(V_U) = dim(V) - 1$, die nicht den $\vec{0}$-Punkt erhält. Dann wählen wir ein affines Koordinatensystem auf der Hyperebene (d.h. $n+1$ Punkte $a_0, ..., a_n$ s.d. die Vektoren $\overrightarrow{a_0 a_1}, ..., \overrightarrow{a_0 a_1}$ eine Basis in $V_H$ bilden).

Als Koordinaten der Geraden $\mathcal{L}(\vec{0}, x) \in P(V)$ mit $x \in H$ definieren wir die Koordinaten von $x$.

Diese Koordinaten sind dann für alle Punkte in $P(V)$ ( = Geraden in $V$) definiert, die nicht zur Hyperebene $H$ parallel sind. Die Richtungsvektoren der Geraden ( = Punkte von $P(V)$), für die die affinen Koordinaten nicht definiert sind, sind dann die Vektoren von $V_H$. Die Menge dieser Punkte von $P(V)$ heißt unendliche Hyperebene (bzgl. dieses Koordinatensystems).

# Bsp.

Als Hyperebene in $\mathbb{R}^{n+1}$ nehmen wir $\{(x_0, ..., x_n) \mid x_0 = 1\}$. Als affine Basis auf $H$ nehmen wir die Punkte $a_0 = (1, 0, ..., 0)^t$, $a_1 = (1, 1, 0, ..., 0)^t$, ... , $a_n = (1, 0, ..., 0, 1)^t$. In diesem Koordinatensystem sind die Koordinaten von $(1, x_1, ..., x_n) \in H$ gleich $(x_1, ..., x_n)$. Dann sind die affinen Koordinaten des Punktes $(x_0 : ... : x_n) \in P(\mathbb{R}^{n+1})$ gleich $\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right)$. Die unendliche Hyperebene besteht dann aus den Punkten von $P(\mathbb{R}^{n+1})$ der Form $(0 : x_1 : ... : x_n)$.

Eine Funktion $f : \mathbb{K}^{n+1} \to \mathbb{K}$ heißt homogen mit Grad $k \in \mathbb{Z}$, falls $f(\lambda x_0, ..., \lambda x_n) = \lambda^k f(x_0, ..., x_n)$ für alle $(x_0, ..., x_n) \in \mathbb{K}^{n+1}$ und $\lambda \in \mathbb{K}$.

**Bsp.** Eine lineare Funktion $f \in (\mathbb{K}^{n+1})^*$ ist 1-homogen.
$f^2$ ist $2-$homogen.

**Bemerkung.** Sei $f$ eine homogene Funktion. Liegt $(x_0, ..., x_n)$ in der Lösungsmenge der Gleichung $f(x) = 0$, so liegen alle Punkte der Gerade $\mathbb{K}(x_0, ..., x_n) = \{\lambda(x_0, ..., x_n) \mid \lambda \in \mathbb{K}\}$ in der Lösungsmenge der Gleichung $f(x) = 0$.
Die Gleichung $f(x) = 0$ kann man also als eine Gleichung auf $P(\mathbb{K}^{n+1})$ verstehen.

# Quadriken in $P(\mathbb{K}^{n+1})$

In homogene Koordinaten sind sie die Lösungen von homogenen quadratischen Gleichungen

$$\sum_{i,j=0}^{n} a_{ij} x_i x_j = 0,$$

wobei $A = (a_{ij})$ eine von 0 verschiedene symmetrische $(n+1) \times (n+1)$-Matrix ist.
Die Gleichung ist homogen, deswegen wenn wir für einen Punkt $(x_0, ..., x_n)$ der Lösung liegt der Punkt $(\lambda x_0, ..., \lambda x_n)$ auch in der Lösung.

# Wie sieht die Gleichung einer projektiven Quadrik in der affinen Koordinaten?

Lass uns es in den affinen Koordinaten aus Bsp. oben ausrechnen: die Zuordnung ist wie folgt:
das Tupel $(x_0, x_1, ..., x_n)$ entspricht das Tupel $\left(1, \frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right) \in H$. Die Zuordnung ist keine Abbildung, weil sie für die Tupel der Form $(0, x_1, ..., x_n)$ nicht definiert ist. Sie ist eine bijektive Abbildung auf $P(\mathbb{K}^{n+1}) \setminus H_0$, wobei $H_0 = \{(0 : x_1 : ... : x_n) \mid x_1, ..., x_n \in \mathbb{K}\}$. $H_0$ haben wir unendlich ferne Hyperebene (bezüglich dieses Koordinatensystem) genannt.
Die Gleichung $\sum_{i,j=0}^{n} a_{ij} x_i x_j = 0$, wird nach diese Zuordnung die Gleichung $\sum_{i,j=1}^{n} a_{ij} x_i x_j + 2 \sum_{i=1}^{n} a_{0i} x_i + a_{00} = 0$.
Dass ist aber eine Gleichung der Quadrik in $\mathbb{K}^n$.
**Bemerkung.** Die Bedingung dass die Matrix $(a_{ij})_{i,j=1,...,n}$ nicht null ist ignorieren wir einfach.
**Bemerkung.** Die Berechnung haben wir in der folgenden affinen Koordinaten gemacht: die affine Hyperebene ist $\{(1, x_1, ..., x_n)\}$ und die affine Basis ist $(a_0 = (1, 0, ..., 0), a_1 = (1, 1, 0, ...0), ...)$. Es ist aber nicht wesentlich.

# Projektivitäten

Sei $f : \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$ eine lineare Abbildung. Dann bildet sie die Geraden durch $\vec{0}$ auf Geraden durch $\vec{0}$ ab und deswegen induziert sie eine Abbildung von $P(\mathbb{K}^{n+1})$ nach $P(\mathbb{K}^{n+1})$. Solche Abbildungen heissen Projektivitäten. In homogenen Koordinaten siehen sie wie folgt aus:

$$f(x_0 : \ldots : x_n) = \left( \sum_{j=0}^{n} a_{0j} x_j : \ldots : \sum_{j=0}^{n} a_{nj} x_j \right)$$

(d.h. wir multiplizieren $A$ mit dem Vektor $(x_0, \ldots, x_n)^t$ und dann "homogenisieren" wir das Ergebnis).
In affinen Koordinaten aus dem Bsp. oben sieht die Abbildung wie folgt:

$$f(x_1, \ldots, x_n) = \left( \frac{a_{10} + \sum_{j=1}^{n} a_{1j} x_j}{a_{00} + \sum_{j=1}^{n} a_{0j} x_j}, \ldots, \frac{a_{n0} + \sum_{j=1}^{n} a_{nj} x_j}{a_{00} + \sum_{j=1}^{n} a_{0j} x_j} \right).$$

Selbstverständlich ist die Abbildung nicht für alle $(x_1, \ldots, x_n)$ definiert, weil der Nenner $a_{00} + \sum_{j=1}^{n} a_{0j} x_j$ gleich null sein kann. Die Punkte sodass $a_{00} + \sum_{j=1}^{n} a_{0j} x_j = 0$ entsprechen dann den Punkten, die auf unendlich ferne Gerade abgebildet sind.

# Frage: Was machen die Projektivitäten mit Quadriken?

**Antwort.** Da lineare nichtausgeartete lineare Abbildungen Quadriken auf Quadriken abbilden und die Eigenschaft einer Funktion, homogen zu sein, erhalten, bilden Projektivitäten (projektiven) Quadriken auf (projektiven) Quadriken ab.

**Beispiel.** Sei $Q = \{(x_0 : x_1 : x_2) \in P(\mathbb{R}^3) \mid -x_0^2 + x_1^2 + x_2^2 = 0\}$.
(1) Sei $H = \{(x_0 : x_1 : x_2) \in P(\mathbb{R}^3) | x_0 = 0\}$ und

$$\psi : \mathbb{R}^2 \to P(\mathbb{R}^2) \setminus H, \quad (x_1, x_2) \mapsto (1 : x_1 : x_2).$$

Dann ist $Q \cap H = \varnothing$ und $\mathit{Urbild}_\psi(Q) = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + x_2^2 - 1 = 0\}$ ist ein Kreis.
(2) Sei $H = \{(x_0 : x_1 : x_2) \in P(\mathbb{R}^3) | x_1 = 0\}$. Dann besteht $Q \cap H$ aus zwei Punkten und für
$\psi : \mathbb{R}^2 \to P(\mathbb{R}^3) \setminus H,\ (x_0, x_2) \mapsto (x_0 : 1 : x_2)$ ist
$\mathit{Urbild}_\psi(Q) = \{(x_0, x_2) \in \mathbb{R}^2 \mid x_0^2 - x_2^2 - 1 = 0\}$ eine Hyperbel.
(3) Sei $H = \{(x_0 : x_1 : x_2) \in P(\mathbb{R}^3) | x_0 + x_1 = 0\}$. Dann ist $Q \cap H$ ein Punkt und für
$\psi : \mathbb{R}^2 \to P(\mathbb{R}^3) \setminus H,\ (x_1, x_2) \mapsto ((1 - x_1) : x_1 : x_2)$ ist
$\mathit{Urbild}_\psi(Q) = \{(x_1, x_2) \in \mathbb{R}^2 | x_2^2 + 2x_1 - 1 = 0\}$ eine Parabel. (Die Substitution $x_1 = -z_1 + \frac{1}{2}$ ergibt $\frac{1}{2}x_2^2 - z_1 = 0$.)

Wir haben gesehen: Je nachdem, was man als unendlich ferne Hyperebene auszeichnet, erhält man aus $Q$ folgende drei affine Kurven: Kreis, Hyperbel, Parabel. D.h.: Kreis, Hyperbel und Parabel sind projektiv äquivalent.)

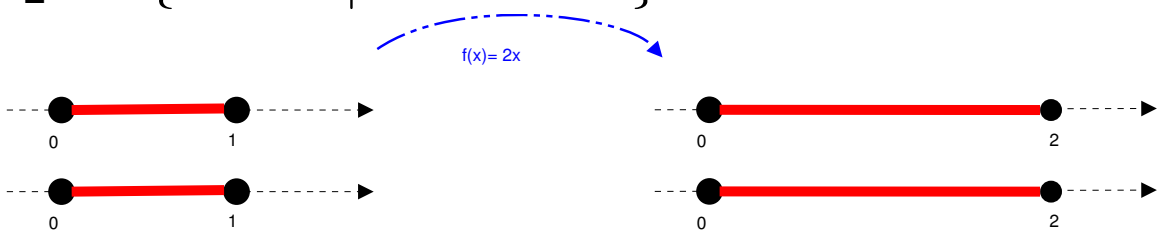
# Neues Thema: Mengenlehre: Mächtigkeit (Ordnung) einer Menge

**Def.** Seien $A, B$ Mengen. Wir sagen, dass $A$ höchstens gleichmächtig zu $B$ ist, falls es eine injektive Abbildung $f : A \to B$ gibt. Schreibweise: $|A| \leq |B|$. Wir sagen, dass $A$ und $B$ gleichmächtig sind, falls $|A| \geq |B|$ und $|B| \geq |A|$ ist. Schreibweise: $|A| = |B|$.

**Bsp.** Die Mengen $A, B$ seien endlich, $|A| := a$, $|B| := b$. Dann gilt:
$|A| \geq |B| \iff a \geq b$, folglich $|A| = |B| \iff a = b$.

**Bemerkung. Gibt es eine Bijektion $f : A \to B$, so gilt:**
$|A| = |B|$.
**Beweis.** $f$ ist bijektiv, deswegen injektiv, deswegen $|A| \leq |B|$. Da $f$ bijektiv ist, gibt es eine inverse Abbildung $g : B \to A$, die auch bijektiv (folglich injektiv) ist. Also $|A| \geq |B|$. □

**Bsp.** $I_1 := \{x \in \mathbb{R} \mid 0 < x < 1\}$ ist gleichmächtig mit $I_2 := \{x \in \mathbb{R} \mid 0 < x < 2\}$.




Tatsächlich, die Abbildung $f : x \mapsto 2 \cdot x$ ist eine Bijektion zwischen $I_1$ und $I_2$.

**Bsp.** $|\mathbb{Z}| = |\mathbb{N}|$. **Beweis.** Die Abbildung $f : \mathbb{N} \to \mathbb{Z}$ ,

$$f(n) = \begin{cases} (n-1)/2 & \text{falls } n \text{ ungerade ist} \\ -n/2 & \text{falls } n \text{ gerade ist} \end{cases}$$

ist eine Bijektion

# Ein kurioses Beispiel

**Hilberts Hotel** (Hilbert:  1862 –1943) besteht aus unendlich vielen Zimmern (mit natürlichen Zahlen nummeriert), die leider alle belegt sind. Es kommen aber noch unendlich viele Gäste (auch mit natürlichen Zahlen durchnummeriert). Kann man Sie unterbringen, ohne die Zimmer doppelt zu belegen?

**Antwort:** Ja!

Der Gast aus Zimmer $k$ geht in das Zimmer $2k$

Der Neuankömmling mit Nummer $k$ geht in das Zimmer $2k - 1$.

Keine Doppelbelegung: Die alten Gäste sind jetzt in Zimmern mit geraden Nummern, die neuen in Zimmern mit ungeraden Nummern. Alle sind untergebracht.

# Bitte üben

**Aufgabe** Finden Sie eine Bijektion zwischen $[0,1]$ und $[0,1] \cup [2]$

**Eine mögliche Lösung.** Wir betrachten eine unendliche Folge in $[0,1]$, z.B. $x_1 = 1$, $x_2 = \frac{1}{2}$, $x_3 = \frac{1}{3}$, $x_4 = \frac{1}{4}$, $x_5 = \frac{1}{5}$,... ,
Die Menge der Elementen der Folge bezeichnen wir mit $X$,
$X := \{x_i \mid i \in \mathbb{N}\}$ (in unserem Bsp. ist $X = \{\frac{1}{i} \mid i \in \mathbb{N}\}$ ).
Wir definieren die Abbildung $f : [0,1] \to [0,1] \cup [2]$ wie folgt:
Für $x \in X$ sodass $x \neq 1$ setzen wir $f(x_i) = x_{i-1}$. (Vgl. mit Hilbert-Hotel)
Für $x = 1$ setzen wir $f(1) = 2$.
Für $x \notin X$ setzen wir $f(x) = x$.
Die Abbildung ist eine Bijektion.

**Wicht. Bsp.** $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

**Beweis:** Die injektive Abbildung $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ ist einfach zu finden: $n \mapsto (1, n)$.

Wir konstruieren eine injektive Abbildung $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Sei $p_n$ die $n-$te Primzahl. Z.B., $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.

- Wir benutze hier (ohne Beweis) die bekannte Aussage, dass die Anzahl von Primzahlen unendlich ist. Wir haben diese Aussage fast bewiesen in Vorl. I von LA I; wenn wir die Widerspruchsbeweismethode eingeführt haben.
- Dabei haben wir ohne Beweis die folgende Aussage benutzt: die Zahl $p_1 p_2 ... p_n + 1$ ist nicht durch $p_1, p_2, ..., p_n$ teilbar, also Primzahlzerlegung von $p_1 p_2 ... p_n + 1$ soll enthält eine grossere Primzahl.
- Diese derzeit nicht bewiesene Aussage, und auch Exitenz und eindeutigkeit von Primzahlzehrlegung, könnten Sie jetzt selbst als einfache Übung beweisen, mit Hilfe von Körper $Z_{p_i}$.

Wir definieren $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n, m) = p_n^m$.

Die Abbildung ist injektiv: ist $f(n, m) = f(n', m')$, so ist $p_{n'}^{m'} = p_n^m$

folglich $p_{n'}^{m'} \equiv p_n^m \pmod{p_n}$

folglich $p_{n'}^{m'} \equiv 0 \pmod{p_n}$,

was unmöglich ist, weil $\mathbb{Z}_n$ ein Körper ist und $p_{n'} \not\equiv 0 \pmod{p_n}$ ist

Daraus folgt insbesondere, dass $|\mathbb{N}| = |\mathbb{Q}|$.
In der Tat, $|\mathbb{Q}| \geq |\mathbb{N}|$, weil die Abbildung $I : \mathbb{N} \to \mathbb{Q}$, $I(n) = n$ eine Injektion ist.

Um zu zeigen, dass $|\mathbb{Q}| \leq |\mathbb{N}|$, benutzen wir die Abbildung
$f \circ g : \mathbb{Q} \to \mathbb{N}$, wobei
$f$ die injektive Abbildung : $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ aus dem Wicht. Bsp. ist,
und $g : \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$ ist die folgende injektive Abbildung:

$$g(p/q) = \begin{cases} (|p|, |q|) & \text{falls } p/q \geq 0 \\ (2 \cdot |p|, 2 \cdot |q|) & \text{falls } p/q < 0 \end{cases} \in \mathbb{N} \times \mathbb{N}.$$

(Wir nehmen an, dass $p$ und $q$ Teilfremd sind. )
Da die Verkettung von injektiven Abbildungen injektiv ist, ist
$f \circ g : \mathbb{Q} \to \mathbb{N}$ auch injektiv, folglich $\mathbb{Q} \leq \mathbb{N}$. Dann $|\mathbb{Q}| = |\mathbb{N}|$. $\square$

**Satz 22.** Zwei Mengen $A, B$ sind genau dann gleichmächtig, wenn es eine Bijektion $h\colon A \to B$ gibt.

**Beweis.** $\Longleftarrow$ ist trivial (und bereits oben bewiesen. wir wiederholen den Beweis): $h$ ist injektiv, deswegen $|A| \leq |B|$. Die inverse Abbildung $h^{-1}$ ist auch eine Bijektion, folglich injektiv, folglich $|A| \geq |B|$.

Es gelte jetzt $|A| = |B|$, und zwar seien $f\colon A \to B$ und $g\colon B \to A$ injektiv. Wir definieren jetzt eine Abbildung $h\colon A \to B$ wie folgt:Sei $A_1 = A \setminus Bild_g(B)$ und dann rekursiv $A_{n+1} = Bild_{g\circ f}(A_n)$. Sei $C = \bigcup_{n\geq 1} A_n$.

* Ist $a \in C$, so setze $h(a) = f(a)$.
* Ist $a \notin C$, so folgt insbesondere $a \in Bild_g(B)$, wir können somit $h(a) = g^{-1}(a)$ setzen (wobei $g^{-1}$ eine Linksinverse zu $g$ ist).

Diese Abbildung $h$ ist injektiv: Es gelte $h(a_1) = h(a_2)$ für zwei Elemente $a_1, a_2 \in A$.

* Ist $a_1 \in C$ und $a_2 \notin C$, so ergibt sich mit $a_2 = g(h(a_2)) = g(h(a_1)) = g(f(a_1)) \in A_{n+1}$ ein Widerspruch.
* Der Fall $a_2 \in C$ und $a_1 \notin C$ ist ebenso ausgeschlossen.
* Ist $a_1 \in C$ und $a_2 \in C$, so folgt $f(a_1) = h(a_1) = h(a_2) = f(a_2)$, also $a_1 = a_2$.
* Ist sowohl $a_1 \notin C$ als auch $a_2 \notin C$, so folgt $a_1 = g(h(a_1)) = g(h(a_2)) = a_2$.

Die Abbildung ist aber auch surjektiv: Sei $b \in B$ beliebig.

* Ist $g(b) \in A_n$ für ein $n \geq 1$, so folgt nach Definition von $A_1$, dass sogar $n > 1$ gilt.Folglich ist $g(b) = g(f(a))$ für ein $a \in A_{n-1}$ und $h(a) = f(a) = b$.
* Ansonsten gilt $h(g(b)) = g^{-1}(g(b)) = b$.

Folglich ist $h\colon A \to B$ eine Bijektion. □

**Folgerung.** $|\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k \text{ Stück}}| = \mathbb{N}$.

**Beweis für $k = 3$.** Wir haben im Wicht. Bsp. gezeigt, dass $|\underbrace{\mathbb{N} \times \mathbb{N}}| = \mathbb{N}$. Nach Satz 22 gibt es dann eine Bijektion $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Wir konstruieren eine Bijektion $\Phi : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Wir setzen $\Phi(n_1, n_2, n_3) := \phi(\phi(n_1, n_2), n_3) \in \mathbb{N}$.

$\Phi$ ist injektiv: gilt $\Phi(n_1, n_2, n_3) = \Phi(m_1, m_2, m_3)$, so ist $\phi(\phi(n_1, n_2), n_3) = \phi(\phi(m_1, m_2), m_3)$. Da $\phi$ bijektiv ist, folgt daraus, dass $\phi(n_1, n_2) = \phi(m_1, m_2)$ und $n_3 = m_3$. Da $\phi$ bijektiv ist, folgt aus $\phi(n_1, n_2) = \phi(m_1, m_2)$, dass $n_1 = m_1$ und $n_2 = m_2$. Also ist $\Phi$ ist injektiv.

$\Phi$ ist surjektiv: Es sei $n \in \mathbb{N}$. Da $\phi$ surjektiv ist, gibt es $n_1, n_2$ mit $\phi(n_1, n_2) = n$. Da $\phi$ surjektiv ist, gibt es $m_1, m_2$ mit $\phi(m_1, m_2) = n_1$. Dann ist $\Phi(m_1, m_2, n_2) = \phi(\phi(m_1, m_2), n_2) = \phi(n_1, n_2) = n$. □

**Bemerkung:** Der Beweis für ein beliebiges $k$ erfolgt durch Induktion (im Beweis für $k = 3$ haben wir praktisch den Induktionsschritt gemacht).

**Def.** Wir sagen, dass $A$ mächtiger als $B$ ist, falls $|A| \geq |B|$, aber $|A| \neq |B|$. Schreibweise: $|A| > |B|$.
Sei $A$ eine Menge. Die Menge aller Teilmengen von $A$ wird mit $2^A$ bezeichnet und Potenzmenge genannt.

**Bsp.** Für $A = \varnothing$ ist $2^A = \{\varnothing\} \neq \varnothing$.

**Bsp.** Sei $A = \{1, 2\}$. Dann ist $2^A = \big\{\varnothing, \{1\}, \{2\}, \{1, 2\}\big\}$.
Sei $A = \{0, 1, 2\}$. Dann ist
$2^A = \big\{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{1, 2\}, \{0, 2\}, \{0, 1, 2\}\big\}$.

**Bemerkung.** Sei $A$ endlich. Dann gilt: $|2^A| = 2^{|A|}$.

Beweis. Angenommen $A = \{0, ..., n\}$ (d.h. $|A| = n + 1$).
Wir ordnen jeder Teilmenge $A'$ die folgende binäre Zahl $\alpha_n\alpha_{n-1}...\alpha_0$ zu: $\alpha_i = \begin{cases} 1 & \text{falls } i \in A' \\ 0 & \text{falls } i \notin A' \end{cases}$.

**Z.B.** $\{1, 2\} \mapsto 110_2$.
$\{0, 2\} \mapsto 101_2$.
Diese Abbildung (von $2^A$ in die binären Zahlen aus höchstens $n + 1$ Ziffern) ist injektiv und surjektiv. Dann ist
$|2^A| = \#\{\text{Binäre Zahlen von 0 bis } \underbrace{1...1}_{n+1}\} = 2^{n+1}$.

**Satz 23** Für eine beliebige Menge $A$ gilt: $|A| < |2^A|$.

**Bemerkung.** Der Satz wird auch oft in der Vorlesungen Analysis besprochen.

**Beweis.** Es sind die folgenden beiden Aussagen zu zeigen:

(i) Es gibt eine Injektion $f : A \to 2^A$ (daraus folgt, dass $|A| \leq |2^A|$)
(ii) Es gibt keine Bijektion zwischen $A$ und $2^A$ (gibt es eine Injektion von $2^A$ nach $A$, so gibt es nach Satz 22 eine Bijektion zwischen $A$ und $2^A$.)

(i) offensichtlich: die Abbildung $f : a \mapsto \{a\}$ leistet das Verlangte.

(ii) Angenommen, irgendeine Abbildung $f : A \to 2^A$ wäre bijektiv. Dies wird nun zum Widerspruch geführt.
Die Teilmenge $M \subseteq A$ wird definiert als $M := \{a \in A \mid a \notin f(a)\}$.
Da $f$ bijektiv und deswegen surjektiv istund da $M \in 2^A$ ist, hat $M$ ein Element $a \in A$ mit $f(a) = M$. Nun gilt:
$a \in M \Longleftrightarrow a \notin f(a) \Longleftrightarrow a \notin M$.
(Die erste Äquivalenz beinhaltet die Definition von $M$, die zweite Äquivalenz benutzt nur die Urbildeigenschaft.)
Damit ist der gewünschte Widerspruch vorhanden. □

**Satz 24** $|2^{\mathbb{N}}| = |\mathbb{R}|$.

**Beweis.** Z.z.: (i) Es gibt eine injektive Abbildung $f : \mathbb{R} \to 2^{\mathbb{N}}$.
Da $|\mathbb{N}| = |\mathbb{Q}|$, ist $|2^{\mathbb{N}}| = |2^{\mathbb{Q}}|$. Deswegen genügt es, eine injektive Abbildung $f : \mathbb{R} \to 2^{\mathbb{Q}}$ zu konstruieren.

(ii) Es gibt eine injektive Abbildung $g : 2^{\mathbb{N}} \to \mathbb{R}$.

**(i): Konstruktion von $f$:** Man kann jede Zahl $a \in \mathbb{R}$ in der dezimalen Form schreiben: $a = \alpha_k\alpha_{k-1}...\alpha_0, \alpha_{-1}\alpha_{-2}... = \sum_{i=k}^{-\infty} \alpha_i \cdot 10^i$, wobei $\alpha_i \in \{0, .., 9\}$.
Z.B. ist
$\pi = 3.14159... = 3 + 1/10 + 4/100 + 1/1000 + 5/10000 + 9/100000 + ....$
Falls nur endlich viele $\alpha_i$ von Null verschieden sind, ist die Zahl rational.
Wir ordnen der Zahl $a = \alpha_k\alpha_{k-1}...\alpha_0, \alpha_{-1}\alpha_{-2}...$, die folgende Teilmenge von $\mathbb{Q}$ zu:$\{\alpha_k \cdot 10^k, \alpha_{k-1} \cdot 10^{k-1}, ..., \alpha_0, \alpha_{-1} \cdot 10^{-1}, ...\}$.
Die Abbildung ist offensichtlich injektiv. Also, $|2^{\mathbb{Q}}| \geq |\mathbb{R}|$.

**(ii) Konstruktion von $g$ :** Man ordne der Teilmenge $A = \{...a_i...\} \subseteq \mathbb{N}$ die Zahl $\sum_i 10^{-a_i}$ zu.
Z.B., falls $A = \{1, 3\}$, dann ist $g(A) = 0, 101$. Die Abbildung ist offensichtlich injektiv. Dann $|2^{\mathbb{N}}| \leq |\mathbb{R}|$, folglich $|2^{\mathbb{N}}| = |\mathbb{R}|$. □

# Anwendung: $\mathbb{R}$ ist keine endliche Körpererweiterung von $\mathbb{Q}$

Zwei Körper $(\mathbb{K}_1, +_1, \cdot_1)$ und $(\mathbb{K}_2, +_2, \cdot_2)$ sind isomorph, falls es eine Bijektion $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ gibt, die die Verknüpfungen erhält: $\phi(x \cdot_1 y) = \phi(x) \cdot_2 \phi(y)$, $\phi(x +_1 y) = \phi(x) +_2 \phi(y)$.

**Def (Wiederholung).** Ein Körper $\mathbb{H}$ heißt eine Körpererweiterung von einem Körper $\mathbb{K}$, falls es einen Unterkörper $\mathbb{H}' \subseteq \mathbb{H}$ gibt, der zu $\mathbb{K}$ isomorph ist.

(In den Beispielen unten wird $\mathbb{K}$ immer ein Unterkörper von $\mathbb{H}$ sein. In dem Fall ist der Isomorphismus die Identitetsabbildung.)

**Bsp.** $\mathbb{C}$ ist eine Körpererweiterung von $\mathbb{R}$.

**Bsp.** $\mathbb{R}$ ist eine Körpererweiterung von $\mathbb{Q}$.

**Wicht. Bsp.** Quadratische Körpererweiterung von $\mathbb{Q}$.
Sei $s \in \mathbb{Q}_{\geq 0}$ sodass $\sqrt{s} \notin \mathbb{Q}$ (Z.B. $s = 2$).
Setze $\mathbb{Q}(\sqrt{s}) := \{x + y\sqrt{s} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{R}$.
**Wiederholung:** $\mathbb{Q}(\sqrt{s})$ ist eine Körpererweiterung von $\mathbb{Q}$.
**Beweis.** Offensichtlich ist $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{s})$. Nach Def. müssen wir zeigen, dass $\mathbb{Q}(\sqrt{s})$ ein Körper ist.

Es genügt z.z. (s. Bemerkung oben), dass $\mathbb{Q}(\sqrt{s})$ ein Unterkörper von $\mathbb{R}$ ist. Wir müssen zeigen, dass $\mathbb{Q}(\sqrt{s})$ und $\mathbb{Q}(\sqrt{s}) \setminus \{0\}$ Untergruppen von $\mathbb{R}$ sind, d.h. $\mathbb{Q}(\sqrt{s})$ abgeschlossen bzgl. „$+$“ , „$\cdot$“ und Invertieren ist.

Addition: $x_1 + y_1\sqrt{s} + x_2 + y_2\sqrt{s} = \underbrace{x_1 + x_2}_{x \in \mathbb{Q}} + \underbrace{(y_1 + y_2)}_{y \in \mathbb{Q}}\sqrt{s}$.

Invertieren bzgl. „$+$“: $x + y\sqrt{s} + (-x - y\sqrt{s}) = 0$.

Multiplikation: $(x_1 + y_1\sqrt{s}) \cdot (x_2 + y_2\sqrt{s}) = \underbrace{x_1x_2 + y_1y_2s}_{x \in \mathbb{Q}} + \underbrace{(x_1y_2 + x_2y_1)}_{y \in \mathbb{Q}}\sqrt{s}$

Invertieren bzgl. „$\cdot$“:

$$(x + y\sqrt{s}) \cdot \left( \underbrace{\frac{x}{x^2 - y^2s}}_{\in \mathbb{Q}} - \underbrace{\frac{y}{x^2 - y^2s}}_{\in \mathbb{Q}}\sqrt{s} \right) = \frac{(x+y\sqrt{s})(x-y\sqrt{s})}{x^2-y^2s} = 1. \qquad \square$$

**Bemerkung:** Für $x + y\sqrt{s} \neq 0$ ist der Nenner $x^2 - y^2s \neq 0$, weil sonst $\frac{x^2}{y^2} = s$ ist, also $\sqrt{s} = \frac{|x|}{|y|} \in \mathbb{Q}$, was den Voraussetzungen widerspricht.

Im Beweis oben kann man $\mathbb{Q}$ durch jeden Unterkörper $\mathbb{K} \subseteq \mathbb{R}$ (oder sogar $\mathbb{K} \subseteq \mathbb{C}$) ersetzen (die Zahl $s$ erfüllt dann die Bedingung $\sqrt{s} \notin \mathbb{K}$). Der Beweis wird buchstäblich wiederholt. Also gilt:

**Wicht. Bsp. in einer stärkeren Form:** *Sei $\mathbb{K}$ ein Unterkörper von $\mathbb{R}$ (bzw. $\mathbb{C}$), und $s \in \mathbb{K}$ mit $\sqrt{s} \notin \mathbb{K}$. Dann ist die Menge $\mathbb{K}(\sqrt{s}) := \{x + y\sqrt{s} \mid x, y \in \mathbb{K}\} \subseteq \mathbb{R}$ (falls zusätzlich $s \geq 0$ , sonst $\subseteq \mathbb{C}$) auch ein Unterkörper von $\mathbb{R}$ (bzw. $\mathbb{C}$).*

Dieser Unterkörper heißt eine quadratische Erweiterung von $\mathbb{K}$.

**Bsp.** $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Tatsächlich, jede Zahl $z \in \mathbb{C}$ kann man in der Form $\underbrace{x}_{\in\mathbb{R}} + \underbrace{y}_{\in\mathbb{R}} \cdot i$ darstellen.

# Endliche Körpererweiterungen

**Wiederholung (Eine Serie von Hausaufgaben in LA I)** Sei $\mathbb{K}'$ ein Unterkörper des Körpers $(\mathbb{K}, +, \cdot)$. Dann ist $(\mathbb{K}, +, \cdot)$ ein $\mathbb{K}'$-Vektorraum.

**Beweis.** $(\mathbb{K}', +, \cdot)$ ist ein Körper. Wir müssen die Körperaxiomen I – VIII aus der Definition des Vektorraums nachweisen: für $\lambda, \mu \in \mathbb{K}'$ und $v, u \in \mathbb{K}$ sollte gelten:

$$\left.\begin{array}{l} [I]\ (u+v)+w = u+(v+w) \\ [II]\ \ \mathrm{u}+\mathrm{v}=\mathrm{v}+\mathrm{u} \\ [III]\ \exists \vec{0} \in V, \text{ s. d. } \vec{0}+v = v \\ [IV] \forall v \in V\ \exists -v \in V \text{ s. d. } -v+v = \vec{0} \end{array}\right\} \text{folgen aus den Körpereigenschaften von } \mathbb{K}.$$

[V] $(\lambda\mu)v = \lambda(\mu v)$ Körpereigenschaft von $\mathbb{K}$.
[VI] $(\lambda+\mu)v = (\lambda v + \mu v)$ Körpereigenschaft von $\mathbb{K}$.
[VII] $\lambda(u+v) = \lambda u + \lambda v$ Körpereigenschaft von $\mathbb{K}$.
[VIII] $1v = v$ (Wobei 1 das neutrale Element in $(\mathbb{K}, \cdot)$ ist.) Das Element 1 in $\mathbb{K}'$ fällt mit dem Element 1 in $\mathbb{K}$ zusammen.

Eine Körpererweiterung $\mathbb{K}' \subseteq \mathbb{K}$ heißt endlich, falls die Dimension von $(\mathbb{K}, +, \cdot)$ ein endlichdimensionaler $\mathbb{K}'$-Vektorraum ist.

**Bsp.** $\mathbb{Q}(\sqrt{s})$ ist eine endliche Erweiterung von $\mathbb{Q}$ (weil jedes Element die Form $x + y \cdot \sqrt{s}$ hat, also die Menge $\{1, \sqrt{s}\}$ erzeugend ist.)

**Bsp.** $\mathbb{C}$ ist eine endliche Erweiterung von $\mathbb{R}$, weil die Menge $\{1, i\}$ erzeugend ist.

**Satz 25.** $\mathbb{R}$ ist keine endliche Erweiterung von $\mathbb{Q}$.

# Beweis vom Satz 25

**Satz 25.** $\mathbb{R}$ ist keine endliche Körpererweiterung von $\mathbb{Q}$.

**Beweis.** Laut Definition ist jede endliche Körpererweiterung $\mathbb{K}$ von $\mathbb{Q}$ ein endlichdimensionaler Vektorraum über $\mathbb{Q}$. Dann ist er zu $\mathbb{Q}^k$ isomorph. Dann gibt es eine Bijektion zwischen $\mathbb{Q}^k$ und $\mathbb{K}$.
Wir haben jedoch gezeigt, dass es keine Bijektion zwischen $\mathbb{Q}^k$ und $\mathbb{R}$ gibt. In der Tat,

$$\left.\begin{array}{l} |\mathbb{Q}| \overset{\text{heute bewiesen}}{=} |\mathbb{N}| \Longrightarrow |2^{\mathbb{Q}}| = |2^{\mathbb{N}}| \overset{\text{Satz 24}}{=} |\mathbb{R}| \\ |\mathbb{Q}| \overset{\text{heute bewiesen}}{=} |\mathbb{N}| \overset{\text{Folgerung}}{=} |\mathbb{N}^k| \overset{\text{Satz 22}}{=} |\mathbb{Q}^k| \\ |2^{\mathbb{Q}}| \overset{\text{Satz 23}}{>} |\mathbb{Q}| \end{array}\right\} \Longrightarrow |\mathbb{R}| > |\mathbb{Q}^k|$$

Nach Definition von “$>$“ gibt es keine Bijektion zwischen $\mathbb{R}$ und $\mathbb{Q}^k$.