Def. 3 Wir sagen, dass A mächtige 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 2^A bezeichnet und Potenzmenge heißen.

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

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

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 nach binäre 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 3 Für eine beliebige Menge A gilt: $|A| < |2^A|$.

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 2 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 ist, und 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 4 $|2^{\mathbb{N}}| = |\mathbb{R}|$.

Beweis. Z.z.: (i) Es gibt eine injektive Abbildung $f : \mathbb{R} \to 2^{\mathbb{Q}}$.
Da $|\mathbb{N}| = |\mathbb{Q}|$, ist $|2^{\mathbb{N}}| = |2^{\mathbb{Q}}|$. Deswegen genügend 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 α_i von Null verschieden sind, ist die Zahl rational.
Wir ordnen den 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 $|2^{\mathbb{Q}}| \leq |\mathbb{R}|$, folglich $|2^{\mathbb{Q}}| = |\mathbb{R}|$. □

Beweis vom Satz 1

Satz 1. $\mathbb{R}$ ist keine endliche Erweiterung 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,

$$\left.\begin{array}{l} |\mathbb{Q}| \overset{\text{gestern bewiesen}}{=} |\mathbb{N}| \Longrightarrow |2^{\mathbb{Q}}| \overset{\text{Satz 2}}{=} |2^{\mathbb{N}}| \overset{\text{Satz 4}}{=} |\mathbb{R}| \\ |\mathbb{Q}| \overset{\text{gestern bewiesen}}{=} |\mathbb{N}| \overset{\text{Folgerung}}{=} |\mathbb{N}^k| \overset{\text{Satz 2}}{=} |\mathbb{Q}^k| \\ |2^{\mathbb{Q}}| \overset{\text{Satz 3}}{>} |\mathbb{Q}| \end{array}\right\} \Longrightarrow |\mathbb{R}| > |\mathbb{Q}^k|$$

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

Komplexifizierung von $\mathbb{R}$-Vektorräumen

Komplexifizierung ist eine Operation, die einem $\mathbb{R}$- Vektorraum einen $\mathbb{C}$-Vektorraum zuordnet, der sehr ähnliche Eigenschaften hat.

Es sei $(V, +, \cdot)$ ein $\mathbb{R}$-Vektorraum.

Wir konstruieren ein $\mathbb{C}$-Vektorraum $V_{\mathbb{C}}$.
Die Menge: $V_{\mathbb{C}} := \{u + i \cdot v \mid \ u, v \in V\}$ der formalen Ausdrucken der Form $u + i \cdot v$ (also ist $V \times V$ als die Menge).
Verknüpfungen:
$+ : V_{\mathbb{C}} \times V_{\mathbb{C}} \to V_{\mathbb{C}}, \ (u_1 + i \cdot v_1) + (u_2 + i \cdot v_2) = (u_1 + u_2) + (v_1 + v_2) \cdot i.$
$\bullet : \mathbb{C} \times V_{\mathbb{C}} \to V_{\mathbb{C}}, (\alpha + \beta \cdot i) \cdot (u + i \cdot v) = \underbrace{(\alpha u - \beta v)}_{\in V} + \underbrace{(\alpha v + \beta u)}_{\in V} \cdot i.$

Bsp. $(\alpha + \beta \cdot i)(u + \vec{0} \cdot i) = \alpha u + \beta u \cdot i.$

Bsp. $\alpha(u + v \cdot i) = \alpha u + \alpha v \cdot i.$

Aussage. $(V_{\mathbb{C}}, +, \cdot)$ ist ein $\mathbb{C}-$Vektorraum.

Beweis. Direkt nach Definition: man muss die Axiomen (V1 – V4) überprüfen. □

Basis und Dimension der Komplexifizierten Vekrotrraum

Sei $(b_1, ..., b_n)$ eine Basis von V. Dann ist $(b_1 + \vec{0} \cdot i, ..., b_n + \vec{0} \cdot i)$ eine Basis in $V_{\mathbb{C}}$. Daraus folgt, dass $Dim(V) = Dim(V_{\mathbb{C}})$.

Tatsächlich, die Vektoren $(b_1 + \vec{0} \cdot i, ..., b_n + \vec{0} \cdot i)$ sind linear unabhängig: ist
$\vec{0} + \vec{0} \cdot i = (\alpha_1 + \beta_1 \cdot i)(b_1 + \vec{0} \cdot i) + ... + (\alpha_n + \beta_n \cdot i)(b_1 + \vec{0} \cdot i)$, so ist
$\vec{0} + \vec{0} \cdot i = (\alpha_1 b_1 + \beta_1 b_1 \cdot i) + ... + (\alpha_n b_n + \beta_n b_n \cdot i)$.
Die letzte Gleichung ist äquivalent zu den folgenden zwei Gleichungen:
$\vec{0} = \alpha_1 b_1 + ... + \alpha_n b_n \qquad (*)$
$\vec{0} = \beta_1 b_1 + ... + \beta_n b_n \qquad (**)$
Wir sehen, dass die beide Gleichungen die Gleichungen in V sind; da $(b_1, ..., b_n)$ eine Basis in V ist, sind $\alpha_i = \beta_i = 0$ folglich $\alpha + \beta \cdot i = 0$ folglich die Menge $\{b_1 + \vec{0} \cdot i, ..., b_n + \vec{0} \cdot i\}$ ist linear unabhängig.
Die Menge ist auch erzeugend: wir betrachten einen Vektor $u + v \cdot i \in V_{\mathbb{C}}$. Da u bzw. v Vektoren aus V sind, kann man sie als Linearkombinationen von Basisvektoren darstellen:
$u = \alpha_1 b_1 + ... + \alpha_n b_n$, $v = \beta_1 b_1 + ... + \beta_n b_n$. Dann ist
$u + v \cdot i = (\alpha_1 + \beta_1 \cdot i)(b_1 + \vec{0} \cdot i) + ... + (\alpha_n + \beta_n \cdot i)(b_n + \vec{0} \cdot i)$. Also, die Menge ist linear unabhängig und erzeugend folglich ist $(b_1 + \vec{0} \cdot i, ..., b_n + \vec{0} \cdot i)$ eine Basis.

Komplexifizierung von linearen Abbildungen

Sei $f : V \to W$ eine lineare Abbildung von $\mathbb{R}-$ Vektorraum V nach $\mathbb{R}-$ Vektorraum W.
Frage: Kann man die Abbildung f linear auf $V_{\mathbb{C}}$ verlängern? Gibt es eine Abbildung $f_{\mathbb{C}}$ sodass $f_{\mathbb{C}}(u + \vec{0} \cdot i) = f(u) + \vec{0} \cdot i$?

Antwort: Ja!

Die folgende Abbildung $f_{\mathbb{C}} : V_{\mathbb{C}} \to W_{\mathbb{C}}$: $f_{\mathbb{C}}(u + v \cdot i) = f(u) + f(v) \cdot i$ hat offensichtlich diese Eigenschaft (weil $f(\vec{0}) = \vec{0}$), und ist linear:

$f_{\mathbb{C}}(u_1 + v_1 \cdot i + u_2 + v_2 \cdot i) = f(u_1 + u_2) + f(v_1 + v_2) \cdot i =$
$f(u_1) + f(u_2) + (f(v_1) + f(v_2)) \cdot i = f_{\mathbb{C}}(u_1 + v_1 \cdot i) + f_{\mathbb{C}}(u_2 + v_2 \cdot i)$.

Ähnlich bzgl. Multiplizieren mit Skalaren.

Sei A die Matrix der Abbildung f bzgl. Basen $(b_1, ..., b_n)$ in V und $(c_1, ...c_m)$ in W.
Frage: Welche Matrix hat die Abbildung $F_{\mathbb{C}}$ bzgl. der Basen $(b_1 + \vec{0} \cdot i, ..., b_n + \vec{0} \cdot i)$ in $V_{\mathbb{C}}$ und $(c_1 + \vec{0} \cdot i, ...c_m + \vec{0} \cdot i)$ in $W_{\mathbb{C}}$?

Antwort: Dieselbe Matrix A.

Beweis. Die j-te Spalte der Matrix $f_{\mathbb{C}}$ ist der Koordinatenvektor von $f_{\mathbb{C}}(b_j)$ in der Basis c_i, also die Zahlen $\begin{pmatrix} \lambda_1 + \mu_1 \cdot i \\ \vdots \\ \lambda_m + \mu_m \cdot i \end{pmatrix}$ sodass

$f_{\mathbb{C}}(b_j + \vec{0} \cdot i) = (\lambda_1 + \mu_1 \cdot i)(c_1 + \vec{0} \cdot i) + ... + (\lambda_m + \mu_m \cdot i)(c_m + \vec{0} \cdot i)$ $(*)$
Die Gleichung $(*)$ ist äquivalent zu zwei Gleichungen:
$\vec{0} = \mu_1 c_1 + ... + \mu_m c_m \implies \text{alle } \mu_i = 0.$
$f(b_j) \overset{\text{Weil } \mu_i = 0}{=} \lambda_1 c_1 + ... + \lambda_m c_m.$
Aber diese Gleichung hat nur eine Lösung, und zwar die Einträge der $j-$te Spalte der Matrix von f sind die Lösung. Also, die Matrizen von $f_{\mathbb{C}}$ und von f sind gleich.

Konjugieren

$V_{\mathbb{C}}$ sein die komplexifizierung des $\mathbb{R}-$Vektorraums V. Dann heißt die Abbildung $u + v \cdot i \mapsto u - v \cdot i$ konjugieren, und wird wie übliche Konjugation mit „quer“ oben bezeichnet $\overline{u + v \cdot i} := u - v \cdot i$. Ferner gilt: $\overline{u + v \cdot i} = u + v \cdot i \iff v = \vec{0}$.

Rechnenregeln für Konjugieren:

- $\overline{f_{\mathbb{C}}(u + v \cdot i)} = f_{\mathbb{C}}(u - v \cdot i)$.
- $\overline{(\alpha + \beta \cdot i)(u + v \cdot i)} = (\alpha - \beta \cdot i)(u - v \cdot i)$.

(Beweis: nachrechnen)

Anwendung von Komplexifizierung

Satz 5 *Sei $f : V \to V$ ein Endomorphismus von $n-$dimensionalen $\mathbb{R}-$Vektorraum V. Angenommen, die Komplexifizierung $f_{\mathbb{C}}$ von f ist diagonalisierbar (als Endomorphismus von $\mathbb{C}$-Vektorraum $V_{\mathbb{C}}$.) Dann gibt es ein Basis B in V sodass die Matrix von f die folgende Form hat*

$$\begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_k & & & \\ & & & \begin{matrix} \alpha_1 & \beta_1 \\ -\beta_1 & \alpha_1 \end{matrix} & & \\ & & & & \ddots & \\ & & & & & \begin{matrix} \alpha_m & \beta_m \\ -\beta_m & \alpha_m \end{matrix} \end{pmatrix}$$

, wobei $\beta_j \neq 0$ ist.

(k oder m können auch gleich 0 sein. Selbstverständlich gilt $2 \cdot m + k = dim(V)$.)

Bemerkung. Beweis enthält auch einen Algorithmus, wie man die Basis finden kann.

Bemerkung. In LAAG I hatten wir zwei Diagonalisierbarkeitkriterien, Sätze 55, 58.

Exkurs: Haupsatz der Algebra

Warum ist $\mathbb{C}$ oft besser als $\mathbb{R}$? Weil in $\mathbb{C}$ der Haupsatz der Algebra gilt.

Hauptsatz der Algebra (Beweis in Analysis – Vorlesungen oder in Funktionentheorie) *Jedes* $P \in \mathbb{C}[x]$ *mit* $Grad(P) \geq 1$ *hat mind. eine Nulstelle*

Bsp. In $\mathbb{R}[x]$ ist die Aussage falsch: z.B. $x^2 + 1$ hat keine Nulstell in $\mathbb{R}$. (wenn wir das Polynom als Polynom über Komplexe koeffizienten auffassen, hat das Polynom die Nullstellen $x_1 = i$, $x_2 = -i$.)

Folgerung A *Jedes $P \in \mathbb{C}[x]$, $P \neq 0$,kann man in lineare Faktoren zehrlegen (d.h. in der Form $P = a(x - x_1)(x - x_2)...(x - x_n)$ schreiben,wobei $a, x_i \in \mathbb{C}$ sind). Diese Zerlegung ist eindeutig bis zum umstellen von Faktoren.*

Beweis Existenz: Sei P ein Polynom des Grades $n \geq 1$. Nach Hauptsatz der Algebra hat er eine Nulstelle x_1. Nach Lemma 6 ist dann $P = (x - x_1)g$, wobei $Grad(g) = Grad(P) - 1$.Ist $Grad(g) = 0$, so ist $g = a \in \mathbb{C}$,und wir sind fertig. Sonst hat g eine Nulstelle x_2, und deswegen (Lemma 6) ist $g = (x - x_2)h$, wobei $Grad(h) = Grad(g) - 1 = Grad(P) - 2$,also $P = (x - x_1)(x - x_2)h$, U.S.W. Nach n Schritte bekommen wir $P = a(x - x_1)...(x - x_n)$.
Eindeutigkeit Induktion nach n. I.A. ist trivial: hat P Grad 0,so ist $P = a = b$,also $a = b$. I.V.: Angenommen, jedes Polynom des Grades $n - 1$ kann man Eindeutig in der Form $P = a(x - x_1)(x - x_2)...(x - x_n)$ darstellen. I.S. Z.z.: die Eindeutigkeit gilt auch für Polynome des Grades n. Sei $P = a(x - x_1)...(x - x_n) = b(x - y_1)...(x - y_n)$, wobei $a \neq 0 \neq b$. Da x_1 eine Nulstelle des Polynoms $a(x - x_1)...(x - x_n) = b(x - y_1)...(x - y_n)$ ist,ist $b(x_1 - y_1)(x_1 - y_2)...(x_1 - y_n) = 0$, und deswegen ist ein von y_i gleich x_1. OBdA ist $y_1 = x_1$. Dividieren des Polynoms durch $(x - x_1)$ gibt $a(x - x_2)...(x - x_n) = b(x - y_2)...(x - y_n)$. Nach I.V. ist $a = b$ und die Faktoren $(x - x_i)$ sind die Faktoren $(x - y_i)$ $(i \geq 2)$, möglicherweise in andere Reihenfolge.

Ist $P \in \mathbb{R}[x]$, so ist $P \in \mathbb{C}[x]$, weil $\mathbb{R} \subseteq \mathbb{C}$.

Folgerung B Jedes $P \in \mathbb{R}[x]$, $Grad(P) > 0$, kann man in Produkt von lineare und quadratrischen Faktoren $g_i \in \mathbb{R}[x]$ zerlegen: $P := g_1 g_2 ... g_m$, wobei $Grad(g_i) \in \{1, 2\}$.

Hilfsaussage. Es sei $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$. Dann gilt für jedes $z \in \mathbb{C}$: $P(\overline{z}) = \overline{P(z)}$ (wobei $\bar{z}$ komplexe Konjugation ist)

Wiederholung: Für $z = a + ib$ ist $\bar{z} = a - ib$.

Wir erinnern zunächst an folgende Eigenschaften komplexer Zahlen:

$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

(Konjugieren ist ein Autoisomorphismus des Körpers $\mathbb{C}$)

Deswegen ist $\overline{z^k} = \overline{z}^k$ für alle $k \in \mathbb{N}$. Damit erhalten wir wegen $a_k \in \mathbb{R}$

$\overline{P_n(z)} = \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} =$

$\overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0} = a_n \overline{z}^n + a_{n-1} \overline{z}^{n-1} + \cdots + a_1 \overline{z} + a_0 = P_n(\overline{z})$.

Hilfsaussage ist bewiesen. Daraus folgt insbesondere, daß für ein $P \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$ zusammen mit $P_n(c) = 0$ stets auch $P_n(\overline{c}) = 0$ gilt.

Damit ist eine Nullstelle von P_n entweder reell oder die zu ihr komplex konjugierte Zahl ist ebenfalls eine Nullstelle.