

Kapitel 7: Quadratische Zahlkörper

Algebraische Zahlen

Def: Eine komplexe Zahl $\alpha \in \mathbb{C}$ heisst algebraisch wenn es ein normiertes Polynom

$$f(x) \in \mathbb{Q}[X] \quad \left(x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0 \right. \\ \left. \text{gibt, sodass } f(\alpha) = 0 \quad a_i \in \mathbb{Q} \right)$$

Die Menge der algebraischen Zahlen bezeichnen wir mit $\bar{\mathbb{Q}}$

α heisst ganz-algebraisch wenn sogar $f(x) \in \mathbb{Z}[X]$ (d.h. f ganzzahlig) gewählt werden kann.

Die Menge der ganz-algebraischen Zahlen bezeichnen wir mit $\mathcal{O}$

Eine nicht-algebraische komplexe Zahl heisst transzendent.

Beispiele: Ganz-algebraisch: $\dots, -2, -1, 0, 1, 2, \dots$

$$\sqrt{2}, i, \sqrt[3]{7} \quad [x^2-2, x^2+1, x^3-7]$$

$$\sqrt{3-\sqrt[3]{5}} \quad [(x^2-3)^3+5]$$

$$\begin{array}{l} \text{Algebraisch} : \frac{1}{2}, \frac{\sqrt{5}}{3} \\ \text{(aber nicht ganz-alg.)} \\ \frac{1+\sqrt{3}i}{7} \end{array}$$

Transzendent: $e, \pi, 2\pi i, e^2, \dots$

$\frac{\pi}{e}, e + \pi$: unbekannt ob transzendent
oder sogar irrational.

Bemerkung: Es gibt abzählbar viele algebraische Zahlen (Aufgabe)
überabzählbar viele transzendente Zahlen

Satz 7.1: (i) Sei $\alpha \in \mathbb{Q}$. Dann gilt

$$\alpha \in \mathcal{O} \Leftrightarrow \alpha \in \mathbb{Z}$$

(beachten: gilt nicht
für $\alpha \in \mathbb{R}$ allgemein)

(ii) Sei $\alpha \in \mathbb{C}$. Dann gilt

$$\alpha \in \bar{\mathbb{Q}} \Leftrightarrow \exists m \in \mathbb{N}^+ \text{ sodass } m\alpha \in \mathcal{O}$$

Beweis: (i) $\Leftarrow$: Klar α ist eine Nullstelle von $X - \alpha$

$\Rightarrow$: Sei $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$

$$\alpha = \frac{a}{b}, \quad a, b \in \mathbb{Z}$$

$$b > 1$$

$$(a, b) = 1$$

Angenommen: $f(\alpha) = 0$

mit $f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$ $c_i \in \mathbb{Z}$

$$\Rightarrow \frac{a^n}{b^n} + c_{n-1} \frac{a^{n-1}}{b^{n-1}} + \dots + c_0 = 0$$

$$\Rightarrow a^n + b c_{n-1} a^{n-1} + \dots + b^n c_0 = 0$$

$$\Rightarrow b \mid a^n \quad \downarrow \quad (a, b) = 1, \quad b > 1$$

also ist $\alpha \notin \mathbb{O}$

(ii) $\Rightarrow$: Sei $f(x) = X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Q}[X]$
mit $f(\alpha) = 1$

Wähle $m \in \mathbb{N}^+$ sodass $ma_i \in \mathbb{Z} \quad \forall 1 \leq i \leq n-1$

(m existiert da $a_i \in \mathbb{Q}$ und es nur endlich viele a_i gibt)

$$\text{Sei } g(x) = X^n + (ma_{n-1})X^{n-1} + \dots + (m^n a_0)$$

Dann ist $g(x) \in \mathbb{Z}[X]$

~~und~~

$$\begin{aligned} \text{und } g(m\alpha) &= (m\alpha)^n + (ma_{n-1})(m\alpha)^{n-1} + \dots + m^n a_0 \\ &= m^n f(\alpha) \\ &= 0 \end{aligned}$$

Also ist $m\alpha \in \mathbb{O}$

$\Leftarrow$: Sei $f(x) = X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$
mit $f(m\alpha) = 0 \quad (m \in \mathbb{N}^+)$

$$\text{Sei } g(x) = X^n + \frac{a_{n-1}}{m} X^{n-1} + \dots + \frac{a_0}{m^n}$$

Dann ist $g(x) \in \mathbb{Q}[x]$

$$\text{und } g(x) = x^n + \frac{a_{n-1}}{m} x^{n-1} + \dots + \frac{a_0}{m^n}$$

$$= \frac{1}{m^n} \left((mx)^n + a_{n-1} (mx)^{n-1} + \dots + a_0 \right)$$

$$= \frac{1}{m^n} f(mx)$$

$$= 0$$

also ist $\alpha \in \overline{\mathbb{Q}}$

□

Bemerkung

und Def: Für eine (ganz-)algebraische Zahl $\alpha \in \overline{\mathbb{Q}}$ (bzw. $\mathbb{C}$) existiert ein eindeutiges normiertes Polynom $m(x) \in \mathbb{Q}[x]$ (bzw. $\mathbb{Z}[x]$) des kleinsten Grades sodass $m(\alpha) = 0$

Eindeutigkeit: Wären $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$
 $\neq g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$

mit $f(\alpha) = g(\alpha) = 0$

Dann ist $(f-g)(x) = (a_{n-1}-b_{n-1})x^{n-1} + \dots + (a_0-b_0) \neq 0$

mit $(f-g)(\alpha) = 0$

in $\mathbb{Q}[x]$ normieren wir. $\hookrightarrow$ zur Minimalität

für $\alpha \in \mathbb{C}$ muss man etwas mehr arbeiten
um zu zeigen, dass $m(x)$ stets ganzzahlig ist
(siehe Schmidt)

Das Polynom $m(x)$ heisst das Minimalpolynom von α

Der Grad von α ist der Grad von $m(x)$

$m(x)$ ist irreduzibel in $\mathbb{Q}[x]$

sonst wäre α eine Nullstelle mindestens einer der
Faktoren, im Widerspruch zur Minimalität.

Satz 7.2: Für $\alpha \in \mathbb{C}$ sind folgende Aussagen äquivalent:

- (i) $\alpha \in \overline{\mathbb{Q}}$
- (ii) Der $\mathbb{Q}$ -Vektorraum $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_r\alpha^r : r \in \mathbb{N}, a_i \in \mathbb{Q}\}$
ist endlichdimensional
- (iii) Es gibt einen endlichdimensionalen $\mathbb{Q}$ -Vektorraum
 $V \subseteq \mathbb{C}$ mit $V \neq \{0\}$ und $\alpha V \subseteq V$

Beweis: (i) $\Rightarrow$ (ii): Sei $m(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$
das Minimalpolynom von α .

Es gilt

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \dots + a_0)$$

$$\Rightarrow \alpha^{n+1} = -(a_{n-1}\alpha^n + \dots + a_0\alpha)$$

$$= -a_{n-1}(-a_{n-1}\alpha^{n-1} + \dots + a_0) - (a_{n-2}\alpha^{n-1} + \dots + a_0\alpha)$$

$$= b_{n-1}\alpha^{n-1} + \dots + b_0 \quad \text{mit } b_i \in \mathbb{Q}$$

Setzen wir dieses Verfahren fort, so sehen wir,
dass jede Potenz α^k eine $\mathbb{Q}$ -Linearkombination
in $1, \alpha, \dots, \alpha^{n-1}$ ist, also ist

$$\mathbb{Q}[\alpha] = 1 \cdot \mathbb{Q} + \alpha \cdot \mathbb{Q} + \dots + \alpha^{n-1} \mathbb{Q}$$

$$= \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}$$

(ii) $\Rightarrow$ (iii): Wähle $V = \mathbb{Q}[\alpha]$

(iii) $\Rightarrow$ (i): Sei $V \subseteq \mathbb{C}$ wie in (iii) und $v_1, \dots, v_n$ eine Basis von V über $\mathbb{Q}$.

Für $j = 1, \dots, n$ ist $v_j \in V$

$$\Rightarrow \alpha v_j \in \alpha V \subseteq V$$

$$\Rightarrow \alpha v_j = a_{j1} v_1 + a_{j2} v_2 + \dots + a_{jn} v_n$$

mit $a_{ji} \in \mathbb{Q}$

Schreiben wir diese Gleichungen in Matrixform:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \alpha \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

also ist α ein Eigenwert der Matrix $(a_{ij})_{ij}$

$\Rightarrow \alpha$ ist eine Nullstelle des charakteristischen Polynoms

und da $a_{ij} \in \mathbb{Q} \forall i, j$, ist das charakteristische Polynom in $\mathbb{Q}[X]$

also ist $\alpha \in \overline{\mathbb{Q}}$



Satz 7.3: Sei $\alpha \in \bar{\mathbb{Q}}$ mit Grad n

Dann hat der $\mathbb{Q}$ -Vektorraum $\mathbb{Q}[\alpha]$ die Dimension n
und $\mathbb{Q}[\alpha]$ ist ein Körper.

Beweis: Nächstes Mal.

Def: $\mathbb{Q}[\alpha]$ heisst ein algebraischer Zahlkörper

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$$

Wenn α Grad 2 hat, heisst $\mathbb{Q}[\alpha]$ ein
quadratischer Zahlkörper