Algebraische Zahlen und Minimalpolynome

Gliederung:

Was sind algebraische Zahlen?

Algebraische Zahlen

- sind aus der Menge der reellen und komplexen Zahlen
- addiert, subtrahiert, multipliziert oder dividiert man sie, entstehen wieder algebraische Zahlen
- unterteilt in ganzalgebraische Zahlen und reell-algebraische Zahlen
- abzählbar
- Menge der Zahlen bilden einen Körper
- nicht algebraisch → transzendent

Definition:

Eine Zahl heißt algebraisch, wenn es zu x ein Polynom p(x) mit rationalen oder ganzzahligen Koeffizienten gibt, wobei mindestens eine von Null verschieden ist, so dass x eine Nullstelle dieses Polynoms ist.

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0$$

Um also eine algebraische Zahl zu finden, bzw. nachzuweisen dass sie algebraisch ist, muss doch „nur“ eine geeignete Funktion

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0$$

gefunden werden, die beim Einsetzen der Zahl den Wert Null liefert.

Nach der Definition kann man also sagen, jede rationale Zahl, welche in den reellen Zahlen zu finden ist, ist eine Algebraische Zahl!

Eine rationale Zahl r können wir doch als Bruch r = m/n darstellen, wobei m und n ganze Zahlen sind, dann ist r Nullstelle von

$$n*x-m$$

→ also algebraisch

Ebenso ist die n-te Wurzel (n ϵ N) einer rationalen Zahl algebraisch, denn für r ϵ Q erfüllt $\sqrt[n]{r}$ die Gleichung

$$x^n - r = 0$$

Algebraische Zahlen sind abzählbar denn:

- wir betrachten eine natürliche Zahl *n*
- Dann gibt es nur abzählbar viele Polynome *n*-ten Grades mit ganzen Koeffizienten, denn man hat für jeden der *n* Koeffizienten nur abzählbar viele Wahlmöglichkeiten
- Also gibt es auch insgesamt nur abzählbar viele Polynome mit ganzen Koeffizienten
- Jedes dieser abzählbar vielen Polynome hat nur endlich viele Nullstellen

d.h. es gibt nur abzählbar viele algebraische Zahlen

Körpererweiterungen

$x^2 - 2 \in Q[x]$ ist Irreduzibel

→daher erweist sich $Q[x]/(x^2-2)$ als Körper

$Q(\sqrt{2})$ ist eine Körpererweiterung von Q
d.h. zu Q wird das neue Element $\sqrt{2}$ adjungiert

$Q(\sqrt{2})$ bildet einen Q-Vektorraum der Dimension 2

Analog dazu

$x^2+1 \in R[x] \rightarrow R[x]/(x^2+1)$ als Körper

Für diesen Körper schreiben wir $C=R(i)$

C ist eine Körpererweiterung von R

Zu R haben wir also die imaginäre Einheit i adjungiert

$R(i)$ bildet einen R-Vektorraum der Dimension 2

Allg.

$p(x) \in K[x]$ irreduzibel
vom Grad n
$K(\alpha) = K[x]/(p(x))$,

so enthält $K(\alpha)$ als Körper den Vektorraum V über K, welcher von den Potenzen von α erzeugt wird

Diese *einfachen Körpererweiterungen*, welche durch Adjunktion eines Elementes α zu K erzeugt werden, haben folgende Form :

$$K(x) := \{c_0 + c_1\alpha + \ldots + \mathrm{c}_{\text{n-1}}\alpha^{n-1} \mid c_k \in K, k = 0..n-1\}$$

Bspl: $Q(\sqrt[3]{5})$

$$a + b\sqrt[3]{5} + c\sqrt[3]{25}$$

Endliche Körpererweiterung

Ein Körper E heißt endliche Körpererweiterung des Körpers E über K vom Grad n.

Jede einfache Körpererweiterung K(α)=K[x]/p(x) ist endlich

Ist n der Grad des irreduziblen Polynoms, so bilden die Elemente α^{n-1} eine Basis von K(α) über K

$$[K(\alpha):K] = n$$

Eine Mehrfache Körpererweiterung $K(\alpha,\beta)$, bei welcher α vom Grad n und β vom Grad m ist, bildet einen n*m dimensionalen Vektorraum über K.

Haben zwei endliche Körpererweiterungen $K \subset E \subset F$ den Grad $[E:K]=n$ und $[F:E]=m$, so ist die Körpererweiterung $K \subset F$ ebenfalls endlich und hat den Grad $[F:K]=n*m$

Algebraische Körpererweiterung

Eine Körpererweiterung E $\supset$ K heißt algebraisch, wenn jedes Element von E algebraisch über K ist

→Endliche Körpererweiterung algebraisch

1.

Jede endliche Körpererweiterung E $\supset$ K ist algebraisch und lässt sich durch Adjunktion endlich vieler algebraischer Elemente erzeugen

2.

Jede Körpererweiterung E $\supset$ K, welche durch Adjunktion endlich vieler algebraischer Elemente entsteht, ist endlich
→Und somit algebraisch

+,-,*, / algebraische Zahlen sind wieder algebraisch

Minimalpolynome

Sei α ϵ E algebraisch über K
Dann gibt es genau ein irreduzibles normiertes Polynom p(x) ϵ K[x], dessen Nullstelle α ist.
Dieses Polynom heißt Minimalpolynom der algebraische Zahl α über K und wird mit $m_a(\alpha, x)$ bezeichnet.
Sein Grad n heißt der Grad der algebraischen Zahl α über K

Das Minimalpolynom ist dasjenige normierte Polynom kleinsten Grades in K[x], welche α als Nullstelle besitzt

$Q(\sqrt{2})$

Nullstelle: $\alpha = \sqrt{2}$

Polynom : $x^2 - 2$

Das Polynom ist normiert und irreduzibel

→ Minimalpolynom

minipol ($\sqrt{2}$, x) = $x^2-2 \in Q[x]$.

$\sqrt{2}$ ist also algebraisch über Q vom Grad 2

Das Minimalpolynom von $i \in R(i) = C$ ist

$minpol_R(i,x) = x^2 + 1 \in R[x]$
$minpol_Q(i,x) = x^2 + 1$

i ist also algebraisch über Q und R jeweils vom Grad 2.

Minimalpolynome sind wichtig um algebraische Zahlen zu charakterisieren

Bspl.: $\alpha = \sqrt{2}$ gilt minpol(α,x) = x^2 -2 und grad(α) = 2

Diese Aussage beinhaltet die Irrationalitätsaussage für $\sqrt{2}$

Wäre $\sqrt{2}$ rational, dann hätte das Minimalpolynom den Grad 1.

Bspl.:

$\beta = \sqrt{4}$

$p(x) = x^2 - 4$

Dieses Polynom kann man aber leicht über Q faktorisieren

$$p(x) = x^2 - 4 = (x-2)(x+2)$$

$$p(x) = x^2 - 4 = (x-2)(x+2)$$

Da es nur ein irreduzibles normiertes Polynom $p(x) \in K[x]$ gibt, dessen Nullstelle x ist, muss eines der Polynome das Minimalpolynom sein

$$\mathrm{Minpol}(\beta,x) = x - 2, \text{ d.h. } \beta = 2$$

Beispiel für kompliziert geschachtelte Wurzeln

α	$= \sqrt{4+2\sqrt{3}}$	/quad.
α^2	$= 4+2\sqrt{3}$	
$\alpha^2 - 4$	$= 2\sqrt{3}$	
$(\alpha^2 - 4)^2$	$= 12$	

$$p(x) = x^4 - 8x^2 + 4 = 0$$

$$p(x) = x^4 - 8x^2 + 4 = 0$$

Minimalpolynom von α ?

Nein denn p(x) ist reduzibel

$p(x) = (x^2 - 2x - 2)(x^2 + 2x - 2)$

Das Minimalpolynom für $\sqrt{4+2\sqrt{3}}$ ist

$(x^2 - 2x - 2) \rightarrow (\alpha^2 - 2\alpha - 2) = 0$

Bestimmung des Minimalpolynoms von Produkten und Summen algebraischer Zahlen

α und β seinen zwei algebraische Zahlen über K, mit den Polynomen p(x), q(x) $\in$ K[x]

$\alpha + \beta$, $\alpha * \beta$ → Ergebnis wieder algebraisch über K

Grad des Minimalpolynoms <= grad(α) * grad(β)

Vorgehensweise für das Bspl.: α + β :

1.
Berechne sämtliche Potenzen $\gamma^k = (\alpha + \beta)^k$, 1 < k <= m*n

Ersetze dabei auftretende Terme mit $\alpha^n \beta^m$, gemäß den MP d.h. die Potenzen γ^k sich als Linearkombination der m*n Terme a_{ij} ausdrücken

$$a_{ij} = \alpha^i \beta^i (i = 0,\ldots,n-1, j = 0,\ldots,m-1)$$

2.

Macht man nun den Ansatz

$$F(\gamma) = \sum_{k=0}^{m*n} c_k \gamma^k = 0$$

mit den noch zu bestimmenden Koeffizienten c_k , so lassen sich die Potenzen γ^k in $F(\gamma)$ wieder als Linearkombination der m*n Terme ausdrücken

$$\sqrt{3} - \sqrt[3]{2}$$

Das Minimalpolynom $\sqrt{3}$ ist 2.Grades

Das Minimalpolynom $\sqrt[3]{2}$ ist 2.Grades

Also muss man bis zur 6. Potenz ausrechnen (2*3)

$$(\sqrt{3}-\sqrt[3]{2})^6$$

$$=\sqrt{3}^6$$

$$-6*\sqrt{3}^5*\sqrt[3]{2}$$

$$+15*\sqrt{3}^4*\sqrt[3]{2}^2$$

$$-20*\sqrt{3}^3*\sqrt[3]{2}^3$$

$$+15*\sqrt{3}^2*\sqrt[3]{2}^4$$

$$-6*\sqrt{3}*\sqrt[3]{2}^5$$

$$+\sqrt[3]{2}^6$$

$$= 27 - 54\sqrt{3}\sqrt[3]{2} + 135\sqrt[3]{4} - 120\sqrt{3} + 90\sqrt[3]{2} - 12\sqrt{3}\sqrt[3]{4} + 4$$

$$= 31 - 120\sqrt{3} + 90\sqrt[3]{2} + 135\sqrt[3]{4} - 54\sqrt{3}\sqrt[3]{2} - 12\sqrt{3}\sqrt[3]{4}$$

...

$$(\sqrt{3} - \sqrt[3]{2})^2 = 3 + \sqrt[3]{4} - 2 * \sqrt{3} * \sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^1 = \sqrt{3} - \sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^0 = 1$$

$$\begin{pmatrix} 31 \\ -120 \\ 90 \\ 135 \\ -54 \\ -12 \end{pmatrix} = a \begin{pmatrix} -60 \\ 9 \\ -45 \\ -2 \\ 15 \\ 30 \end{pmatrix} + b \begin{pmatrix} 9 \\ -8 \\ 2 \\ 18 \\ -12 \\ 0 \end{pmatrix} + c \begin{pmatrix} -2 \\ 3 \\ -9 \\ 0 \\ 0 \\ 3 \end{pmatrix} + d \begin{pmatrix} 3 \\ 0 \\ 0 \\ 1 \\ -2 \\ 0 \end{pmatrix} + e \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + f \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$
\left|\begin{array}{r:r:r:r:r:r}
-60 & 9 & -2 & 3 & 0 & 1 \\
9 & -8 & 3 & 0 & 1 & 0 \\
-45 & 2 & -9 & 0 & -1 & 0 \\
-2 & 18 & 0 & 1 & 0 & 0 \\
15 & -12 & 0 & -2 & 0 & 0 \\
30 & 0 & 3 & 0 & 0 & 0
\end{array}\right| * \begin{array}{c} a \\ b \\ c \\ d \\ e \\ f \end{array} = \left|\begin{array}{r} 31 \\ -120 \\ 90 \\ 135 \\ -54 \\ 12 \end{array}\right|
$$

Das System wird gelöst durch

a = 0,
b = −9,
c = 4,
d = 27,
e = 36,
f = −23,

so dass wir $x^6 - 9x^4 + 4x^3 + 27x^2 + 36x - 23$

als Minimalpolynom von $\sqrt{3} - \sqrt[3]{2}$ gefunden haben

Transzendente Zahlen

Schwierig ist es jedoch Nachzuweisen, dass eine Zahl x nicht Algebraisch ist. Noch so komplizierte Funktionen der Form

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0$$

dürfen beim Einsetzen von x niemals Null ergeben.

- die Eulersche Zahl
- die Kreiszahl pi

Die ursprünglichen Beweise der Transendenz von

der Eulerschen Zahl *e*
und der Kreiszahl π

stammen von Charles Hermite. Diese sind allerdings nur sehr schwer nachzuvollziehen.
Einen sehr „eleganten Beweis“ veröffentlichte der David Hilbert im Jahre 1893.

Vielen Dank

.

.

.

.

Fragen?