PROSEMINAR LINEARE ALGEBRA SS10

Körper
und
Konstruktion mit Zirkel und Lineal

Neslihan Yikici

Mathematisches Institut
der
Heinrich-Heine Universität Düsseldorf
Juni 2010

Betreuung: Prof. Dr. Oleg Bogopolski

Inhaltsverzeichnis

§1 Beispiele von Körpern

1.1 Definition: Eine Teilmenge K eines Körpers L, die selbst mit dessen Operationen wieder einen Körper bildet, wird Unter- oder Teilkörper genannt. Das Paar K und L heißt *Körpererweiterung* $K \subset L$.

Beispielsweise ist der Körper $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$.

Ausführlich: Eine Teilmenge U eines Körpers K ist ein Teilkörper, wenn folgendes gilt:

* $1 \in U$
* $a, b \in U$
  $\Rightarrow a+b \in U, ab \in U$
  $\Rightarrow$ Abgeschlossenheit bezüglich Addition und Multiplikation
* $a \in U$
  $\Rightarrow -a \in U$
  $\Rightarrow$ Jedes Additive Inverse von U ist in U
* $a \in U \backslash \{0\}$
  $\Rightarrow a^{-1} \in U$
  $\Rightarrow$ Das multiplikative Inverse zu jedem Element aus U mit Ausnahme der Null ist in U

1.2 Beispiel: $Q(2) := \{q_1+\sqrt{2}q_2 \mid q_1, q_2 \in Q\} \subseteq \mathbb{C}$

neutrales Element zu $q_1+\sqrt{2}q_2$: $0+\sqrt{2}0$

inverses Element zu $q_1+\sqrt{2}q_2$ bezüglich Addition: $(-q_1-\sqrt{2}q_2)$

inverses Element zu $q_1+\sqrt{2}q_2$ bezüglich Multiplikation: $q_1/(q_1^2-2q_2^2) + \sqrt{2}(q_2/ q_1^2-2q_2^2)$

1.3 Definition: Ein Zahlkörper ist ein Teilkörper von $\mathbb{C}$.

Jeder Teilkörper von $\mathbb{C}$ enthält die Zahl 1 und damit den Körper $\mathbb{Q}$ der rationalen Zahlen.

Ein Zahlkörper ist also ein Erweiterungskörper von $\mathbb{Q}$.

Endliche Körper und Funktionenkörper werden wir nicht behandeln.

§2 Algebraische und transzendente Elemente

2.1 Definition: Sei $k \subseteq K$ eine Körpererweiterung.
Ein Element $\alpha \in K$ heißt *algebraisch über k*, wenn es ein Polynom $f \in k[X]\setminus\{0\}$ gibt, sodass $f(\alpha) = 0$.
Dagegen heißt $\alpha \in K$ *transzendent über k*, wenn es nicht algebraisch über k ist, d.h. wenn es nicht Nullstelle eines Polynoms von Grad $\geqq 0$ mit Koeffizienten in k ist.
Das Polynom sieht etwa so aus:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \quad a_i \in k$$

2.2 Definition: Sei $k \subseteq K$ eine Körpererweiterung, $K[x]$ der Polynomring zu K mit der Unbestimmten x und sei $\alpha \in L$ algebraisch, d.h. es existiert $0 \neq p(x) \in K[x]$ mit $p(\alpha) = 0$.
Dann existiert ein *Minimalpolynom* $m_\alpha(x) \in K[x]$ mit den Eigenschaften:

1) $m_\alpha(\alpha) = 0$.
2) $\mathrm{Grad}(m_\alpha)$ ist minimal, d.h für alle $g(x) \in K[x]$ mit $g(\alpha) = 0$ gilt $\deg(g) \geqq \deg(m_\alpha)$.
3) Hauptkoeffizient von $m_\alpha(x)$ ist 1.

2.3 Behauptung: 1) $m_\alpha(x)$ ist eindeutig und irreduzibel über dem Grundkörper K.
2) Jedes Polynom mit Koeffizienten im Grundkörper, das ein algebraisches Element α als Nullstelle hat, ist ein (Polynom-) Vielfaches des Minimalpolynoms von α.
3) Der Grad des Minimalpolynoms von α ist gleich dem Grad der einfachen Erweiterung $k \subseteq K(\alpha)$ (siehe Bezeichnung 2.5).

2.4 Beispiel: $K = \mathbb{Q}[i]$, $\alpha = \sqrt{2}/2*(1+i) \subseteq \mathbb{C}$, $\alpha \notin K$

$\alpha^2 = (\sqrt{2}/2)^2*(1+2i+i^2) = i \in K$

$\alpha^2 - i = 0$

$m_\alpha(x) = x^2 - i \in K[x]$

$m_\alpha(\alpha) = \alpha^2 - i = 0$

2.5 Bezeichnung: Der von einem Element $\alpha \in K$ erzeugte Erweiterungskörper von k wird mit $k(\alpha)$ bezeichnet. $k(\alpha)$ ist der kleinste Körper, der k und α enthält.

$$k[\alpha]=\{ a_n\alpha^n+\ldots+a_0 \mid a_i \in k \} \subset k(\alpha)=\{ (a_n\alpha^n+\ldots+a_0)/(b_m\alpha^m+\ldots+b_0) \mid a_i, b_j \in k, b_m\alpha^m+\ldots+b_0 \neq 0 \}$$

2.6 <u>Satz:</u> Seien $\alpha_1,...,\alpha_n$ algebraische Elemente eines Erweiterungskörpers k von K.

Dann ist $k[\alpha_1,...,\alpha_n] = k(\alpha_1,...,\alpha_n)$

2.7 <u>Beispiel:</u> $Q(\sqrt{2}) = \{(q_1+\sqrt{2}q_2)/(q_1'+\sqrt{2}q_2') \mid q_i, q_i' \in Q, (q_1', q_2') \neq (0,0)\}$

$Q[\sqrt{2}] = \{q_1+\sqrt{2}q_2 \mid q_1,q_2 \in Q\}$

$1/(q_1'+\sqrt{2}q_2') = (q_1'+\sqrt{2}q_2')/((q_1'+\sqrt{2}q_2')*(q_1'-\sqrt{2}q_2'))$

$= (q_1'-\sqrt{2}q_2')/(q_1'^2+2q_1'*q_2')$

$= (q_1'/(q_1'^{2-}2q_1'*q_2'))-(q_2'/(q_1'^{2-}2q_1'*q_2'))*\sqrt{2} \in Q[\sqrt{2}]$

2.8 <u>Satz:</u> Sei α algebraisches Element über K mit Minimalpolynom f(x).

Angenommen f(x) habe den Grad n.

Dann ist $(1,\alpha, \alpha^2,...,\alpha^{n-1})$ eine Basis für $K[\alpha]$ als Vektorraum über K.

<u>Beweis:</u> 1) $\beta \in K(\alpha)= K[\alpha]$

$\beta = a_m \alpha^m+a_{m-1} \alpha^{m-1}+...+a_0$

$f(x) = a_m x^m+a_{m-1} x^{m-1}+...+a_0 \in K[x]$

$f(x)=q(x)*m_\alpha(x)+r(x)$

$\beta = f(\alpha) = q(\alpha)*m_\alpha(\alpha)+r(\alpha) = r(\alpha)$

$\beta = r(\alpha)$ mit Grad $(r(x))<n$

$r(\alpha)=b_{n-1} \alpha^{n-1}+...+b$ mit $b_i \in K$

Damit ist $\beta \in L$ als eine Linearkombination von $1, \alpha, \alpha^2,...,\alpha^{n-1}$ dargestellt.

2) $1,\alpha, \alpha^2,...,\alpha^{n-1}$ sind linear unabhängig

$\lambda_1+\lambda_2\alpha+...+ \lambda_{n-1}\alpha^{n-1} = 0$

$f(x) = \lambda_1+ \lambda_2x+...+ \lambda_{n-1}x^{n-1}$

$f(\alpha) = 0$

Damit ein Widerspruch zum Minimalpolynom.

§3 Der Grad einer Körpererweiterung

3.1 Definition: Seien $k \subseteq K$ zwei Körper .
Dann betrachten wir k als Vektorraum über K.
$[k:K]$= Dimension von k als Vektorraum über K.

3.2 Satz: Ist a algebraisch über k, so ist $[k(a):K]$ der Grad des Minimalpolynoms von a über k.

3.3 Hauptsatz: Gradsatz
Seien $K \subset L \subset M$ Körper.
Dann gilt für die Körpergrade:
$$[M:K] = [M:L][L:K]$$

3.4 Beispiel: $Q(\sqrt[3]{2}, \sqrt[4]{5})$
$n = 3r = 4s = 12$
$12 \mid n$
$Q(\sqrt[3]{2}) \subseteq Q(\sqrt[3]{2}, \sqrt[4]{5})$
d.h. x^4-5 annulliert das Element $\sqrt[4]{5}$ und hat Koeffizient in $Q(\sqrt[3]{2})$
$\Rightarrow$ Grad $m_\alpha(x) \leqq 4$ für $\alpha = \sqrt[4]{5}$
$\Rightarrow r \leqq 4 \Rightarrow n \leqq 3r \leqq 12 \Rightarrow n = 12$

§4 Konstruktion mit Zirkel und Lineal

Regeln:

1) Zwei Punkte in der Ebene mit Abstand 1 werden als Ausgangspunkte vorgegeben. Diese Punkte gelten als *konstruiert.*

2) Sind zwei Punkte konstruiert, so darf man ihre Verbindungsgerade ziehen oder um einen der Punkte einen Kreis schlagen, der durch den anderen Punkt geht.
Solche Geraden und Kreise werden auch als *konstruiert* betrachtet.

3) Die Schnittpunkte der konstruierten Geraden und Kreise gelten ebenfalls als *konstruiert.*

4.1 Satz: Ist a eine konstruierbare reelle Zahl, so ist sie algebraisch und ihr Grad über $\mathbb{Q}$ ist eine Zweierpotenz.

4.2 Satz: Unmöglichkeit der Winkeldreiteilung.
Werden einen bestimmten Winkel Θ mit folgenden Eigenschaften angeben:

i) Θ ist konstruierbar
ii) $^1/_3\Theta$ ist nicht konstruierbar

Der Winkel $\Theta = 60°$ erfüllt die Eigenschaften.
Aus Satz 4.1 folgt, dass cos20° nicht konstruierbar ist und man daher 60° nicht dreiteilen kann.

In der Tat:
Mit Additionstheorem für Sinus und Kosinus kann man folgende Gleichung zeigen:

$$\cos 3\Theta = 4\cos^3\Theta - 3\cos\Theta$$

Für $\Theta = 20°$ und $\alpha = \cos 20°$ erhält man die Gleichung:

$$½ = 4\alpha^3 - 3\alpha$$

$\Rightarrow$ Dieses Polynom $f(x) = 4x^3-3x- ½ \in \mathbb{Q}[x]$ besitzt keine Nullstelle in $\mathbb{Q}$. Somit ist das Polynom irreduzibel über $\mathbb{Q}$, weil sich das Produkt nicht in zweier nicht invertierbaren Polynome schreiben lässt und somit nicht in „einfachere“ Polynome zerfällt.

Beweis: Das Polynom $f(x) = 4x^3-3x- ½ \in \mathbb{Q}[x]$ besitzt keine Nullstelle in $\mathbb{Q}$.

$(x-p/q)f(x) \Rightarrow$ p/q ist eine Nullstelle des Polynoms.
Für x = p/q in das Polynom einsetzen:

$$4(p/q)^3 - 3(p/q) - ½ = 0 \qquad |*q^3$$
$$4p^3 - 3pq^2 – ½\, q^3 = 0 \qquad |*2$$
$$8p^3 - 6pq^2 - q^3 = 0$$

1.Fall: $q|8p^3$
somit ist der ggt(q,p) = 1
$\Rightarrow q|8 \quad \Rightarrow q \in \{-1, 1, -2, 2, -4, 4, -8, 8\}$

2.Fall: $p|q^3$ $\quad \Rightarrow p \in \{-1, 1\}$, weil der ggt(q,p) = 1 ist, kann p nur -1,1 sein.

Somit ist $p/q \in \{-1, 1, -½, ½, -¼, ¼, -^1/_8, ^1/_8\}$

<u>Rechnung:</u>

Für **x = -1** in das Polynom f(x) einsetzen
$4(-1)^3 - 3(-1) – ½ = -1½ \neq 0$
Für **x = 1** in das Polynom f(x) einsetzen
$4(1)^3 - 3(1) – ½ = ½ \neq 0$
Für **x = -½** in das Polynom f(x) einsetzen
$4(-½)^3 - 3(-½) – ½ = ½ \neq 0$

Für **x = ½** in das Polynom f(x) einsetzen

$4(½)^3 - 3(½) – ½ = -1½ \neq 0$

Für **x = -¼** in das Polynom f(x) einsetzen

$4(-¼)^3 - 3(-¼) – ½ = ^3/_{16} \neq 0$

Für **x = ¼** in das Polynom f(x) einsetzen

$4(¼)^3 - 3(¼) – ½ = -^{19}/_{16} \neq 0$
Für **x = -$^1/_8$** in das Polynom f(x) einsetzen
$4(-^1/_8)^3 - 3(-^1/_8) – ½ = -^{15}/_{128} \neq 0$
Für **x = $^1/_8$** in das Polynom f(x) einsetzen
$4(^1/_8)^3 - 3(^1/_8) – ½ = -^{111}/_{128} \neq 0$

Damit wurde gezeigt, dass das Polynom $f(x) = 4x^3-3x- ½ \in \mathbb{Q}[x]$ keine Nullstelle in $\mathbb{Q}$ besitzt.

Literaturverzeichnis

S. Schröer, Skript Alegbra 2010

M. Artin, Algebra 1998