Proseminar: Körpertheorie

Wantzels Satz zur Konstruierbarkeit

Ideale,
der größte gemeinsame Teiler
das kleinste gemeinsame Vielfache

Jelena Stjepanovic

25. April 2013

Prof. K. Wingberg, K. Hübner

WANTZELS SATZ ZUR KONSTRUIERBARKEIT

Def. 3.1. Sei F/E eine Körpererweiterung und $S \subset F$ eine Teilmenge von *F*. Dann nennt man $E[S]$ bzw. $E(S)$ **den kleinsten Teilring bzw. Teilkörper** von *F*, der *E* und *S* umfasst.
Man sagt auch, dass $E[S]$ und $E(S)$ aus E durch **Adjuktion** von *S* entstehen.
Ist $S=\{a\}$, so benutzt man auch die folgende Schreibweise $E[a]$ und $E(a)$.

Gibt es mehrere Teilringe von *F*, die *E* und *S* umfassen, findet man den kleinsten unter diesen, indem man ihren Durchschnitt bildet. Analog begründet man die Eindeutigkeit des Teilkörpers $E(S)$.

Satz 3.2.
Wantzels Satz

Sei *E* ein Teilkörper von **R**. Eine reelle Zahl *x* ist aus *E* konstruierbar, genau dann wenn es $n \in N_{0,}$ und einen Körperturm $E=E_0 \subset E_1 \subset E_2 \subset ... \subset E_n$ mit $[E_i : E_{(i-1)}]=2, \forall i \in \{1,...,n\}$ und $x \in E_n$ gibt.

Man nennt die Körpererweiterung F/E vom Grad 2 quadratisch, denn diese aus E durch Adjunktion der quadratischen Wurzel entstehen.

Proposition 3.3. Sei *E* ein Teilkörper von **R** (im Allg. char E ≠ 2). Sei F/E die Körpererweiterung vom Grad 2. Dann existiert $a \in F \setminus E$ mit $a^2 \in E$ und $F=E[a]$.

Beweis: Sei $x \in F \setminus E$. Das Vektorsystem (1, *x*) ist linear unabhängig, d.h. es existieren $p, q \in E$ mit $p+qx=0, p=q=0$ und damit wegen $\dim_E F = 2$ eine Basis von F ist. Nach der Definition ist eine Basis die maximale linear unabhängige Teilmenge in E-Vektorraum F. Daraus folgt, dass das Vektorsystem $(1,x,x^2)$ linear abhängig ist und es existieren $a, b, c \in E$, nicht alle gleich Null, mit $ax^2+bx+c=0$.
Wäre $a=0$, so ist $bx+c=0$ mit $b=c=0$. Das ist ein Widerspruch zur Annahme, dass $a, b, c \in E$ nicht alle gleich Null sind.
Es folgt $a \neq 0$, $x^2+\frac{b}{a}x+\frac{c}{a}=0$

$\Leftrightarrow x^2+\frac{b}{a}x+\left(\frac{b}{2a}\right)^2-\left(\frac{b}{2a}\right)^2+\frac{c}{a}=0$

$\Leftrightarrow \left(x+\frac{b}{a}\right)^2=\frac{b^2-4ac}{4a^2}$ (nach der 3. binomischen Formel) $\Leftrightarrow \left(\frac{2ax+b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$

Sei $\delta=2ax+b$. Dann gilt $\delta \notin E$ und $\delta^2=b^2-4ac$. Ferner ist $\delta^2 \in E$ wegen $a, b, c \in E$. Setzt man $x=\frac{\delta}{2a}-\frac{b}{2a}$ in $p \cdot 1+qx=0$ ein, so ist $p+\frac{\delta-b}{2a}q=0$ bzw. $2ap-bq+q\delta=0$ mit $p=q=0$.
Es folgt, dass das Vektorsystem $(1,\delta)$ linear unabhängig ist und wegen $\dim_E F = 2$ auch eine Basis von F ist. Mit anderen Worten entsteht F aus E durch Adjunktion von δ, d.h. $F=E[\delta]$.

□

Beweis des Wantzelts Satzes:

"=>" Sei *x* in *n* Schritten, $n \in N_{0,}$ mit dem Zirkel und Linear aus *E* konstruierbar.
Gilt $x \in E$, so ist *x* nach $n=0$ Schritten aus *E* konstruierbar.
Ist $x \notin E$, so betrachtet man zunächst die Form der Gleichungen der Geraden und Kreise und die Koordinaten ihrer Schnittpunkte, die sich aus den explizieten Lösungen dieser Gleichungen ergeben.
Sei K ein Teilkörper von **R**.
Die Gleichung der Gerade durch die Punkte $A=(a_1, b_1), A'=(a_2, b_2)$ mit Koordinaten aus *K* hat die Form $(b_2-b_1)(x-a_2)-(a_2-a_1)(y-b_2)=0$ bzw. $ax+by+c=0; a, b, c \in K$.

Der Kreis mit dem Mittelpunkt $O=(a'',b'')$ und Radius MM' , wobei $M=(a,b), M'=(a',b')$ die Punkte mit Koordinaten aus *K* sind, hat die Gleichung $(x-a'')^2+(y-b'')^2=(a-a')^2+(b-b')^2$ bzw. $x^2+y^2+dx+ey+f=0; d,e,f\in K$.

Nach der Anwendung des Gauß-Eliminationsverfahrens ist der Schnittpunkt zweier nicht-parallenen Geraden $\overline{AA'}$ und $\overline{BB'}$ ein Punkt mit der Koordinaten aus *K*, wenn *A, A', B, B'* die Punkte mit der Koordinaten aus *K* sind.

Der Schnittpunkt eines Kreises und einer Gerade ist die Lösung eines Gleichungssystem, das aus einer quadratischen $x^2+y^2+dx+ey+f=0$ und einer linearen Gleichung $ax+by+c=0$ besteht. Es gilt entweder $a\neq 0$ oder $b\neq 0$, denn sonst kann man nicht die obige lineare Gleichung als die Gleichnung einer Gerade betrachten.
O.B.d.A. sei $b\neq 0$. Löst man die lineare Gleichung nach y auf, d.h. $y=\frac{-(c+ax)}{b}$ und setzt dieses in der Gleichung des Kreises ein, bekommt man die quadratische Gleichung in einer Unbestimmte *x* mit Koeffizienten aus *K*. Die Diskriminate Δ dieser quadratischen Gleichung gehört zu K. Dann gehört *x* zu dem aus *K* durch Adjuktion von $\sqrt{\Delta}$ entstandenen Körper $K(\sqrt{\Delta})$. Wegen $y=\frac{-(c+ax)}{b}$ liegt die y-Koordinate des Schnittpunktes auch in $K(\sqrt{\Delta})$. .

Analog bestimmt man den Schnittpunkt zweier Kreise, denn nach der Substraktion ihrer Gleichungen ist das Gleichungssystem, das aus einer quadratischen und einer linearen Gleichung besteht, zu lösen.

Also nach $n-1$ Schritten bei der Konstruktion von *x*, ist der Folge $E=E_0\subset E_1\subset ...\subset E_{(n-1)}$ der quadratischen Erweiterüngen vorhanden und der Körper E_n mit $x\in E_n$ entsteht aus $E_{(n-1)}$ durch Adjunktion der Diskriminante einer quadratischen Gleichnung, deren Lösung dem Schnittpunkt einer Geraden und eines Kreis bzw. dem Schnittpunkt zweier Kreise.

"<=" Sei $E=E_0\subset E_1\subset E_2\subset ...\subset E_n$ einer Körperturm mit $[E_i:E_{(i-1)}]=2, \forall i\in\{1,...,n\}$ und $x\in E_n$ gegeben. Es genügt zu zeigen, dass für jede quadratische Körpererweiterung L/K gilt, dass jedes Element aus *L* konstruierbar aus *K* ist.
Nach der Prop.3.3. gibt es ein $\delta\in L\setminus K$ mit $\delta^2\in K$ *und* $L=K[\delta]$. Dann ist $\delta=\pm\sqrt{\delta^2}$ aus K konstruierbar. Da $\{1,\delta\}$ eine Basis von *L* ist, läßt sich dann jedes Element aus *L* als die Linearkombination $x+y\delta$ darstellen und damit aus *K* konstruieren.
Dass jedes Element aus E_n aus *E* konstruierbar ist, zeigt man dann mittels Induktion über n.

□

Folgerung 3.4 Sei *E* ein Teilkörper von **R** und *x* eine reelle Zahl, die aus *E* konstruierbar ist. Dann ist *x* algebraisch über *E* und sein Grad über *E* ist eine zweier Potenz.

Beweis: Da *x* konstruierbar aus *E* ist, folgt nach dem Wantzels Satz, dass es $n\in N_{0,}$ und eine Folge quadratischer Körpererweiterungen $E=E_0\subset E_1\subset E_2\subset ...\subset E_n$ mit $x\in E_n$ gibt.

Für die Körpererweiterung E_n/E gilt nach dem Gradsatz
$[E_n:E]=[E_n:E_1][E_1:E]=2[E_n:E_1]=...=2^n$.
Da jede endliche Körpererweiterung algebraisch ist, so ist x algebraisch über *E*.

Da $E\subset E[x]\subset E_n$ eine Komposition von Körpererweiterungen ist, gilt
$[E_n:E]=[E_n:E[x]][E[x]:E]=2^n$. Somit ist der Grad von *x* über E eine zweier Potenz, denn $[E[x]:E]$ teilt 2^n .

□

Ideale, der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache

Def 4.1. Eine Untergruppe I von einem Ring $(R,+)$ heißt ein **Ideal** von R, wenn gilt
$$a\in R,\ b\in I \Rightarrow ab,\ ba\in I.$$
Gilt nur $ba\in I$ *bzw.* $ab\in I$ für eine Untergruppe I von R, so nennt man I ein Links- bzw. Rechtsideal von R.
I heißt ein Hauptideal, wenn es von nur einem Element $a\in R$ erzeugt wird. Bez. $I=(a)$
Ein Integritätsring heißt ein **Hauptidealring**, wenn jedes seiner Ideale ein Hauptideal ist.

Satz 4.2. Für jedes Ideal I von $K[X]$ existiert ein Polynom $P\in K[X]$ *mit* $I=(P)$.

Beweis: Ist $I=\{0\}$ so ist das gesuchte Polynom $P=0$.

"$\supset$" Sonst sei $P\in I, P\neq 0$ ein Polynom vom Grad d wober $d\geqslant 0$ der kleiste Grad aller Polynome im Ideal I ist. Ferner gilt $PQ\in I$ für jedes $Q\in K[X]$. Damit ist $(P)\subset I$.

"$\subset$" Sei $A\in I$. Nach der Euklidischen Division des Polynoms A mit Polynom P gilt $A=PQ+R$ bzw. $R=A-PQ$ mit $deg\ R<d$. Aus $PQ, A\in I$ folgt $R\in I$. Da d der kleinste Grad aller von Null verschiedenen Polynome in I ist, folgt $R=0$ und $A=PQ\in(P)$. □

Bem. 4.3. Der Erzeuger eines von Null verschiedenen Ideals I von $K[X]$ ist nach dem obigen Satz nicht eindeutig. Sind $P, Q\in K[X]$ zwei Erzeuger von I, so gilt $P=RQ\ und\ Q=SP$, wobei $R, S\in K[X]$ die von Null verschiedenen konstanten Polynomen sind, denn $deg\ P=deg\ Q$ ist. D.h. P und Q teilen einander und unterscheiden sich in einer Konstante $\lambda\in K^x$. Aus $P=\lambda Q$ folgt, dass der Erzeuger von I eindeutig ist, wenn er ein normiertes Polynom ist.

Folgerung 4.4.
Satz vom Bézout

Seien A,B zwei Polynome. Die Menge $I=(A, B)$, die alle $AP+BQ$ mit $P, Q\in K[X]$ enthält, ist ein Ideal in $K[X]$. Erzeugt D dieses Ideal, dann:
(i) existieren $U, V\in K[X]$, sd. $D=AU+BV$;
(ii) D teilt A und B;
(iii) jedes Polynom, das A und B teilt, teilt auch D.

Dann ist ***D* der größte gemeinsame Teiler von A und B**.

Zwei Polynome A und B heißen **teilerfremd**, wenn ihr gemeinsamer Teiler ein konstantes Polynom ist. D.h. es existieren $U, V\in K[X]$ mit $AU+BV=1$.

Beweis: I ist ein Ideal in $K[X]$, denn:
1) I ist nicht leer, da $A\cdot 0+B\cdot 0=0\in I$ gilt.
2) Für belibige $P, P', Q, Q'\in K[X]$ sind $AP+BQ, AP'+BQ'\in I$. Also ist ihre Summe auch das Element des Ideals I, denn $(AP+BQ)+(AP'+BQ')=A\cdot(P+P')+B\cdot(Q+Q')$.
3) Sei $M\in K[X], AP+BQ\in I$ gegeben. Wegen $(AP+BQ)M=A\cdot MP+B\cdot MQ=(AP+BQ)M$ ist $M(AP+BQ),(AP+BQ)M\in I$.

Da $D\in I$ ist, es existieren $U, V\in K[X]$ mit $D=AU+BV$. Damit ist *(i)* gezeigt.
Aus $A=A\cdot 1+B\cdot 0$ und $B=A\cdot 0+B\cdot 1$ folgt, dass $A, B\in I$ gilt. Damit existierten $P, Q\in K[X]$ mit $A=PD$ und $B=QD$. Also die Aussage *(ii)* D teilt A und B gilt.
Sei C ein weiteres Polynom, dass A und B teilt, d.h. $A=PC$ und $B=QC$ wobei $P, Q\in K[X]$
Aus der Relation $D=AU+BV$ folgt $D=PCU+QCV=C(PU+QV)$. Damit ist C durch D teilbar.

□

Bemerkung 4.5. Sind A und B zwei von Null verschiede Polynome, so ist dann das Ideal (A, B) auch nicht Null und nach der Bemerkung 4.3. und Folgerung 4.4 *iii)* ist D eindeutig bestimmt.

Def. 4.6. Für $A, B, P, Q \in K[X]$ ist die Menge (A, B), die alle $AP+BQ$ enthält, ein Ideal in $K[X]$. Man nennt $T \in K[X]$ **kleinstes gemeinsames Vielfaches von *A* und *B***, falls:

(i) A teilt T und B teilt T;
(ii) jedes Polynom, das A oder B teilt, teilt auch T.

Literatur:

- Christian Karpfinger, Kurt Meyberg – Algebra - 2. Auflage, Spektrum Verlag 2010
- Chambert-Loir – A field guide to algebra – Springer Verlag 1999
- Falko Lorenz – Einführung in die Algebra- 3. Auflage, Spektrum Verlag 1996