Proseminar Körpertheorie

Konstruktionen mit Zirkel und Lineal

Lars Indus

18. April 2013

Prof. K. Wingberg, K. Hübner

1 Konstruierbarkeit

Eine den antiken griechischen Mathematikern bereits bekannte Fragestellung war die der Konstruierbarkeit von Zahlen beziehungsweise geometrischer Figuren mit Zirkel und Lineal, den sogenannten *euklidischen Werkzeugen*. Wenngleich es auch damals schon weitere Hilfsmittel gab, mit denen man kompliziertere Figuren konstruieren konnte, bezieht sich die klassische Fragestellung immer auf diese beiden Werkzeuge.

Im Folgenden werden wir die Ebene, in der die Konstruktion stattfindet, mit der komplexen Ebene identifizieren. Ein Punkt entspricht also einer komplexen Zahl.

Definition 1.1 *Es sei $S \subset \mathbb{C}$ eine Teilmenge. Üblicherweise wählt man $\{0,1\} \subset S$ als Voraussetzung. Nun bezeichnet man die Menge aller komplexen Zahlen, die man mit Zirkel und Lineal in endlich vielen Schritten aus S konstruieren kann, mit $K(S)$. Dabei sind die folgenden Schritte erlaubt:*

(i) *Zu $z_1, \ldots, z_4 \in K(S)$ bilde man den Schnittpunkt der Geraden $\overline{z_1 z_2}$ und $\overline{z_3 z_4}$.*

(ii) *Zu $z_1, \ldots, z_5 \in K(S)$ bilde man die Schnittpunkte der Geraden $\overline{z_1 z_2}$ mit dem Kreis um z_3 mit Radius $|z_5 - z_4|$.*

(iii) *Zu $z_1, \ldots, z_6 \in K(S)$ bilde man die Schnittpunkte der Kreise um z_1 mit Radius $|z_3 - z_2|$ und um z_4 mit Radius $|z_6 - z_5|$.*

Bemerkung: Um eine reelle Zahl x zu konstruieren, reicht es schon, eine Strecke der Länge x zu konstruieren, da man diese dann leicht auf die reelle Achse abtragen kann.

Weiterhin sieht man auch schnell ein, dass eine komplexe Zahl genau dann konstruierbar ist, wenn man sowohl ihren Real- als auch ihren Imaginärteil konstruieren kann.

Satz 1.2 *Es sei $\{0,1\} \subset S \subset \mathbb{C}$. Dann gilt für $K(S)$:*

(i) *Aus $x, y \in K(S)$ folgt $x \pm y \in K(S)$.*

(ii) *Für reelle $x, y \in K(S)$ gilt $xy \in K(S)$ und für $y \neq 0$ auch $\frac{x}{y} \in K(S)$.*

(iii) *Für reelles $x \in K(S)$ mit $x > 0$ gilt $\sqrt{x} \in K(S)$.*

Beweis: Punkt (i) macht man sich leicht mit der aus der Schule bekannten „Vektoraddition“ klar (Real- und Imaginärteil werden komponentenweise addiert).

Für (ii) betrachten wir die folgende Anordnung, die wir ohne größere Schwierigkeiten konstruieren können, da die Konstruktion von parallelen Geraden unmittelbar auf die von Mittelsenkrechten zurückgeführt werden kann:

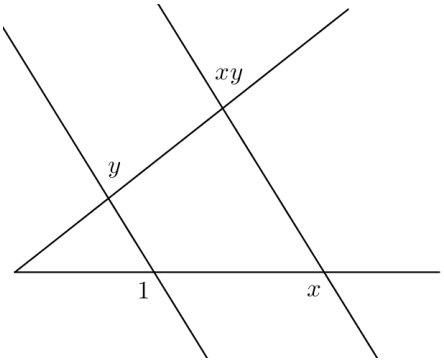

Abbildung 1: Strahlensatz

Mit den ebenfalls bekannten Strahlensätzen erhält man nun $\frac{x}{1} = \frac{xy}{y}$, das heißt wir können xy konstruieren. In der Abbildung ist hierbei $x > 1$ vorausgesetzt, aber auch für $x < 1$ erhält man durch eine einfache Umordnung die Behauptung. Ebenso liefert eine Umordnung auch die Konstruierbarkeit von $\frac{x}{y}$.

Um den letzten Punkt zu beweisen, betrachten wir erneut eine Abbildung:

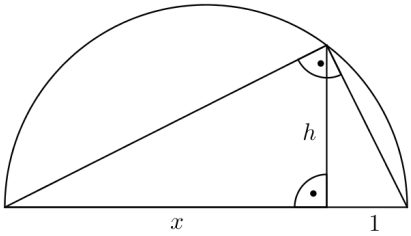

Abbildung 2: Höhensatz

Der Satz des THALES garantiert uns, dass das abgebildete Dreieck tatsächlich rechtwinklig ist. Nun können wir die Aussage leicht mit EUKLIDs Höhensatz beweisen, denn dieser liefert $h^2 = x \cdot 1$, also $h = \sqrt{x}$. □

2 Körpererweiterungen

Definition 2.1 *Ein Körperhomomorphismus $\varphi : K \to L$ heißt Körpererweiterung.*

Bemerkung: Man hat es fast immer mit dem Fall $K \subset L$ zu tun, wobei man φ dann als die kanonische Inklusionsabbildung wählen kann. Doch auch sonst lässt sich die Annahme $K \subset L$ auf folgende Art und Weise rechtfertigen:

Da ein Körperhomomorphismus immer injektiv ist, erhalten wir durch Einschränkung von L auf im φ die Isomorphie $K \cong$ im φ. Folglich können wir für einen beliebigen Körperhomomorphismus $\varphi : K \to L$ die Quelle K durch im φ ersetzen und φ dann wegen im $\varphi \subset L$ als die Inklusion auffassen.

Wir werden in Zukunft also immer vom Fall $K \subset L$ ausgehen. Häufig nennt man L eine Körpererweiterung von K oder man bezeichnet dieses Körperpaar als eine Körpererweiterung und notiert es in der Form L/K (lies „L über K“). Von nun an werden wir diese Notation verwenden.

Für eine beliebige Körpererweiterung L/K können wir L jetzt als K-Vektorraum auffassen, indem wir die Addition aus L übernehmen und durch $K \times L \to L,\ (x, y) \mapsto i(x) \cdot y$ eine Multiplikation definieren, wobei $i : K \to L$ die Inklusion ist.

Definition 2.2 *Es sei L/K eine Körpererweiterung. Man nennt*

$$[L : K] := \dim_K L$$

den Grad der Erweiterung. Ist $[L : K]$ endlich, so heißt die Körpererweiterung L/K endlich, andernfalls unendlich.

Bemerkung: Offenbar gilt genau dann $[L : K] = 1$, wenn $L = K$.

Beispiele:

- $\mathbb{C}/\mathbb{R}$ ist eine Erweiterung vom Grad 2, denn eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist gegeben durch $\{1, i\}$.
- Für einen beliebigen Körper K ist $K(X)/K$ eine unendliche Körpererweiterung, denn die Menge $\{1, X, X^2, \dots\}$ ist linear unabhängig.
- Es gilt $[\mathbb{R} : \mathbb{Q}] = \infty$, denn: $\mathbb{Q}$ ist abzählbar und aus der linearen Algebra ist bekannt, dass ein n-dimensionaler $\mathbb{Q}$-Vektorraum für ein $n \in \mathbb{N}$ isomorph zu $\mathbb{Q}^n$ ist. Außerdem weiß man, dass das kartesische Produkt abzählbarer Mengen wieder abzählbar ist. Somit erhält man, dass ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ebenfalls abzählbar ist. $\mathbb{R}$ ist jedoch nicht abzählbar.

Satz 2.3 (Gradsatz/Schachtelungsformel) *Es seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Insbesondere heißt das, M/K ist genau dann endlich, wenn M/L und L/K endlich sind.

Beweis: Sollte einer der Grade $[M : L]$ und $[L : K]$ unendlich sein, ist diese Gleichung symbolisch zu verstehen und $[M : K]$ ist ebenfalls unendlich. Deshalb seien nun $[M : L]$ und $[L : K]$ endlich. Wir wählen eine Basis $x_1, \dots, x_n$ von L über K und eine Basis $y_1, \dots, y_m$ von M über L und werden zeigen, dass durch die Elemente $x_i y_j$, $i = 1, \dots, n$, $j = 1, \dots, m$, eine Basis von M über K gegeben ist. Zunächst weisen wir nach, dass diese Elemente ein Erzeugendensystem bilden:

Jedes $z \in M$ lässt sich darstellen als $z = \sum_{j=1}^{m} a_j y_j$ mit Koeffizienten $a_j \in L$. Allerdings findet man auch für jedes a_j eine Darstellung $a_j = \sum_{i=1}^{n} a_{ij} x_i$ mit Koeffizienten $a_{ij} \in K$. Insgesamt erhält man

$$z = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} x_i y_j,$$

also bilden die $x_i y_j$ tatsächlich ein Erzeugendensystem.

Nun müssen wir noch die lineare Unabhängigkeit der Elemente nachweisen:

Es seien also Koeffizienten $a_{ij} \in K$ mit $\sum_{i,j} a_{ij} x_i y_j = 0$ gegeben. Wir schreiben diese Gleichung in der Form

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} x_i \right) y_j = 0.$$

Aus der linearen Unabhängigkeit der y_j folgt $\sum_{i=1}^{n} a_{ij} x_i = 0$ für alle j. Genauso erhält man dann aus der linearen Unabhängigkeit der x_i schon $a_{ij} = 0$ für alle i und j. Damit sind die $x_i y_j$ linear unabhängig über K und bilden folglich eine Basis von M über K. Man sieht leicht ein, dass diese Basis aus nm vielen Elementen besteht. □

Korollar 2.4 *Ist $[M : K] = p$ für eine Primzahl p, so gilt $M = L$ oder $L = K$. Insbesondere hat eine Körpererweiterung von primem Grad keinen echten Zwischenkörper.*

Beweis: Nach dem Gradsatz gilt

$$p = [M : K] = [M : L] \cdot [L : K],$$

also $[M : L] = 1$ und $[L : K] = p$ oder umgekehrt. Wie bereits bemerkt folgt dann $M = L$ oder $L = K$. □

Definition 2.5 *Es sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt algebraisch über K, wenn es ein vom Nullpolynom verschiedenes $f \in K[X]$ gibt, sodass $f(\alpha) = 0$ ist. Existiert nur das Nullpolynom mit dieser Eigenschaft, heißt α transzendent.*

Ist jedes $\alpha \in L$ algebraisch über K, so heißt die Körpererweiterung L/K algebraisch, ansonsten nennt man sie transzendent.

Beispiele:

- Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn es ist Nullstelle des Polynoms $X^2 - 2 \in \mathbb{Q}[X]$.
- $\mathbb{C}/\mathbb{R}$ ist algebraisch, denn eine beliebige komplexe Zahl $a + bi$ ist Nullstelle des Polynoms $X^2 - 2aX + \left(a^2 + b^2\right) \in \mathbb{R}[X]$.
- π ist transzendent über $\mathbb{Q}$ (Lindemann, 1882).
- $e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$ ist transzendent über $\mathbb{Q}$ (Hermite, 1873).

Definition 2.6 *Es sei L/K eine Körpererweiterung und $\alpha \in L$. Das Bild des Ringhomomorphismus'*

$$\varphi_\alpha : K[X] \to L, \quad f \mapsto f(\alpha)$$

heißt der von α über K erzeugte Unterring von L und wird mit $K[\alpha]$ bezeichnet. φ_α ist außerdem auch ein Vektorraumhomomorphismus, sodass $K[\alpha]$ auch ein Untervektorraum von L ist.

Bemerkung: $K[\alpha]$ ist der kleinste Unterring von L, der α enthält.

Satz 2.7 *Es sei L/K eine Körpererweiterung und $\alpha \in L$. Dann gilt:*

(i) *Ist α transzendent über K, so ist φ_α injektiv und es gilt $\dim_K K[\alpha] = \infty$.*

(ii) *Ist α algebraisch über K, so existiert ein eindeutig bestimmtes normiertes Polynom minimalen Grades $f \in K[X]$ mit $f(\alpha) = 0$. f ist sogar irreduzibel und es gilt $\dim_K K[\alpha] = \deg f$. Schließlich wird jedes andere Polynom $g \in K[X]$ mit $g(\alpha) = 0$ von f geteilt.*

Definition 2.8 *Das oben erwähnte eindeutig bestimmte Polynom $f \in K[X]$ heißt das Minimalpolynom von α über K. Sein Grad heißt der Grad von α über K.*

Beweis: Es sei zunächst α transzendent über K. Dann existiert kein nicht-triviales Polynom in $K[X]$ mit der Nullstelle α. Somit folgt $\ker \varphi_\alpha = \{0\}$, also ist φ_α injektiv. Schränkt man nun den Zielbereich L auf $K[\alpha]$ ein, ist φ_α per Konstruktion sogar surjektiv und wir erhalten $K[X] \cong K[\alpha]$, woraus $\dim_K K[\alpha] = \infty$ folgt, da die Menge $\{1, X, X^2, \dots\}$ linear unabhängig ist. Damit ist (i) gezeigt.

Es sei nun α algebraisch über K und $f \in K[X]$ ein normiertes Polynom minimalen Grades mit $f(\alpha) = 0$. Sei weiterhin $g \in K[X]$ ein beliebiges Polynom mit $g(\alpha) = 0$. Der euklidische Algorithmus liefert

$$g = fq + r, \quad \deg r < \deg f.$$

Somit ergibt sich

$$r(\alpha) = g(\alpha) - f(\alpha)q(\alpha) = 0.$$

Für $r \neq 0$ erhält man mittels Division durch den Leitkoeffizienten von r ein normiertes Polynom $\tilde{r}$ mit $\tilde{r}(\alpha) = 0$ und $\deg \tilde{r} < \deg f$. Dies widerspricht jedoch der Minimalität von f, also folgt $r = 0$ und somit $f|g$. Nehmen wir nun an, es gäbe ein weiteres Polynom $\tilde{f} \in K[X]$ mit den Eigenschaften von f. Da f und $\tilde{f}$ vom selben Grad sind und beide die Nullstelle α haben, teilen sie sich gegenseitig. Dann müssen sie, da sie normiert sind, allerdings schon gleich sein und f ist somit eindeutig bestimmt.

Nun sei $d = \deg f$ und $K[X]_{<d}$ der K-Vektorraum aller Polynome vom Grad kleiner als d. Wir betrachten den Homomorphismus

$$\varphi_{\alpha,d} : K[X]_{<d} \to K[\alpha], \quad g \mapsto g(\alpha).$$

Dieser ist injektiv, denn nach dem bereits Gezeigten wissen wir, dass in $K[X]_{<d}$ nur das Nullpolynom α als Nullstelle besitzen kann. Mit dem euklidischen Algorithmus schreiben wir für ein beliebiges $g \in K[X]$ erneut $g = fq + r$ mit $\deg r < d$. Es folgt

$$g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = \varphi_{\alpha,d}(r),$$

also $g(\alpha) \in \text{im } \varphi_{\alpha,d}$. Damit ist $\varphi_{\alpha,d}$ surjektiv, also sogar ein Isomorphismus, und es gilt $K[X]_{<d} \cong K[\alpha]$. Da die Elemente $1, X, \ldots, X^{d-1}$ offensichtlich eine Basis von $K[X]_{<d}$ über K bilden, gilt demnach $\dim_K K[\alpha] = d$.

Zuletzt zeigen wir, dass f irreduzibel ist. Wir schreiben $f = gh$ mit $g, h \in K[X]$. Es gilt dann

$$0 = f(\alpha) = g(\alpha)h(\alpha).$$

Wegen der Nullteilerfreiheit von L können wir ohne Einschränkung $g(\alpha) = 0$ annehmen, folglich $f|g$ und $\deg f \leq \deg g$. Allerdings gilt wegen der Zerlegung $f = gh$ auch $g|f$ und somit $\deg g = \deg f$, also $\deg h = 0$. Das heißt aber gerade $h \in K\backslash\{0\} = K[X]^\times$, weswegen f irreduzibel ist. □

Literatur

[Bos] S. Bosch, *Algebra*, Springer, 7. Auflage (November 2008)

[Cha] A. Chambert-Loir, *A Field Guide to Algebra*, Springer, 1. Auflage (Oktober 2004)

[MK] F. Modler und M. Kreh, *Tutorium Algebra*, Springer Spektrum, 1. Auflage (Juli 2012)