Die Klassischen Probleme der Algebra

JProf.-Dr. Christoph Wockel

10. April 2012

Die Algebra wurde in ihrer Entstehung von der Suche nach einer Lösung der folgenden Probleme maßgeblich beeinflusst:

- Konstruierbarkeit mit Zirkel und Lineal:
  - Würfelverdopplung (Delisches Problem): Konstruiere zu einem Würfel einen Würfel mit doppeltem Inhalt (also $\sqrt[3]{2}$)!
  - Winkeldrittelung: Konstruiere zu einem Winkel der Größe φ einen Winkel der Größe $\frac{\varphi}{3}$!
  - Quadratur des Kreises: Konstruiere zu einem Quadrat (mit Kantenlänge a) einen Kreis mit gleichem Flächeninhalt (also mit Radius $a/\sqrt{\pi}$)
  - Konstruktion regelmäßiger n-Ecke: Konstruiere den Winkel $\frac{2\pi}{n}$!
- Auffinden exakter Lösungsformeln für polynomiale Gleichungen: Zu einem Polynom $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$, finde einen (iterierten) Ausdruck in dem nur $a_0, ..., a_{n-1}$, deren Summen, Produkte, Differenzen, Quotienten oder Wurzelausdrücke solcher vorkommen, so dass diese Ausdrücke genau die Nullstellen von P sind!

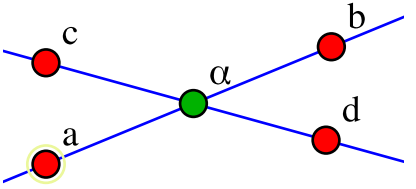
Diese Probleme (Konstruierbarkeit und Existenz exakter Lösungsformeln) kann man mit den Werkzeugen der modernen Algebra elegant und effektiv lösen. Wir werden dies (zunächst) an der Frage nach der Konstruierbarkeit mit Zirkel und Lineal illustrieren.

Zentral hierbei ist es, das Problem der Konstruierbarkeit (welches ja ein anschaulich/geometrisches zu sein scheint) zunächst in ein algebraisches Problem zu übersetzen. Diesen Prozess nennt man **Algebraisierung**, den wir hier im Weiteren kennen lernen werden.

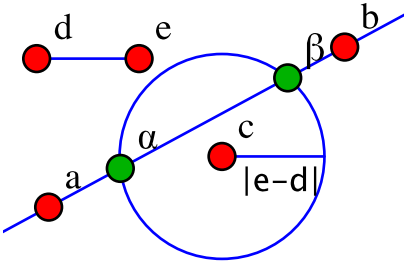
Für die Entwicklung der modernen Algebra ist die Frage nach der Konstruierbarkeit eher zweitrangig, die Frage nach der Existenz exakter Lösungsformeln für Polynomgleichungen war hier viel entscheidender. Da die Thematik bei diesem Problem etwas komplizierter ist werden wir (wenn überhaupt) erst am Ende der Vorlesung hierauf eingehen können.

Definition: Sei $S \subseteq \mathbb{C} \cong \mathbb{R}^2$ eine Teilmenge. Dann bezeichnet $\measuredangle(S)$ die Menge der Punkte, die durch Iteration der folgenden Konstruktionen aus S konstruiert werden können:

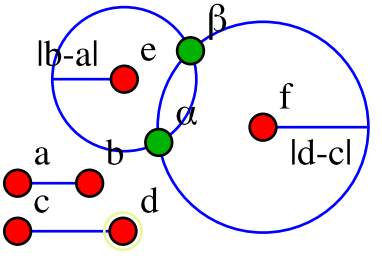
- Sei $\mathrm{Ge}(S)$ die Menge der Geraden durch mindestens zwei verschiedene Punkte $a \neq b$ aus S. Dann ist $\gamma \cap \eta \in \measuredangle(S)$ für $\gamma, \eta \in \mathrm{Ge}(S)$ mit $\gamma \neq \eta$.



- Sei $\mathrm{Kr}(S)$ die Menge der Kreise mit Mittelpunkt $c \in S$ und Radius $|e-d|$ für $d, e \in S$. Dann ist $\gamma \cap \kappa \subseteq \measuredangle(S)$ für $\gamma \in \mathrm{Ge}(S)$ und $\kappa \in \mathrm{Kr}(S)$.



- Für $\kappa, \lambda \in \mathrm{Kr}(S)$ mit $\kappa \neq \lambda$ ist $\kappa \cap \lambda \subseteq \measuredangle(S)$.



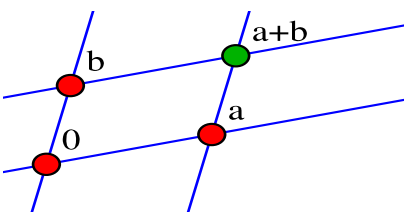
Im Folgenden wird es wichtig sein, dass die Menge $\measuredangle(S)$ eine algebraische Struktur trägt, die es erlaubt diese zu analysieren.
Aus den o.g. Konstruktionen leiten sich in bekannter Weise weitere Konstruktionen ab, wie Lot durch einen Punkt, Mitte zwischen Punkten, Parallele durch gegebenen Punkt, Winkelhalbierende. Damit beweisen wir

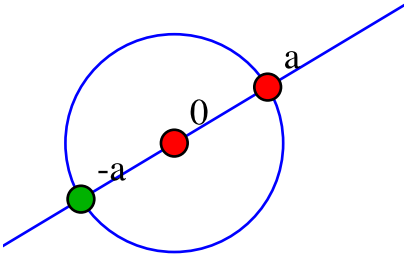
Satz: Ist $\{0,1\} \subseteq S$, so ist $\measuredangle(S)$ ein Teilkörper von $\mathbb{C}$, es gilt also $0,1 \in \measuredangle(S)$ und für $a,b \in (S)$ dass

1. $a+b \in \measuredangle(S)$ und $-a \in \measuredangle(S)$
2. $a \cdot b \in \measuredangle(S)$ und $b^{-1} \in \measuredangle(S)$ falls $b \neq 0$.

Beweis: Zunächst bemerken wir $i \in \measuredangle(S)$ und $a \in \measuredangle(S) \Rightarrow \overline{a} \in \measuredangle(S)$.

- Es ist $a+b$ ist der Schnittpunkt der Parallelen zu $\overline{0b}$ durch a mit der Parallelen zu $\overline{0a}$ durch b. Außerdem ist mit a auch $-a$ in $\measuredangle(S)$.

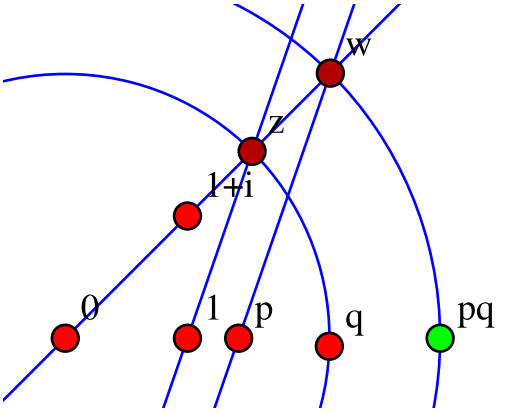




- Wir werden die Behaptungen immer zuerst für reelle Zahlen zeigen:

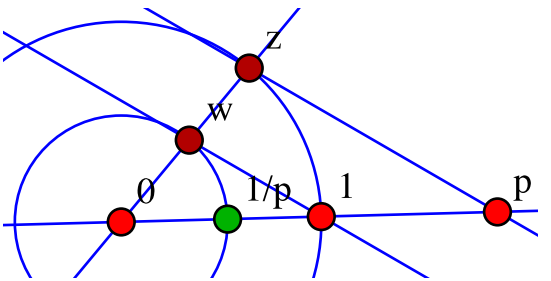
  Es zeigt die nebenstehende Konstruktion, dass falls $p, q \in \measuredangle(S) \cap \mathbb{R}$ wir $pq \in \measuredangle(S) \cap \mathbb{R}$ haben. Schreiben wir $a = (x + iy)$, $b = (z + iw)$, so sind $x, y, z, w \in \measuredangle(S)$ und somit auch

  $$ab = (xz - yw) + i(xw + yz).$$



  Falls $p \in \mathbb{R} \cap \measuredangle(S)$ und $p \neq 0$, so ist nach der nebenstehenden Konstruktion und dem Strahlensatz $\frac{p}{1} = \frac{|z|}{|w|}$, also $p^{-1} = |w| \in \measuredangle(S)$. Damit folgt aus

  $$a^{-1} = \overline{a}(a\overline{a})^{-1}$$



  dass $a^{-1} \in \measuredangle(S)$ für $a \in \measuredangle(S)$.

■

Bemerkung: Offensichtlich hat der Teilkörper $\measuredangle(S)$ außerdem die folgenden Eigenschaften:

$$\begin{aligned}
\mathbb{Q} &\subseteq \measuredangle(S) \text{ (da } \mathbb{Q} \text{ der kleinste Unterkörper von } \mathbb{C} \text{ ist)} \\
\mathbb{Q} + i\mathbb{Q} &\subseteq \measuredangle(S) \text{ (da } i \in \measuredangle(S)) \\
a \in \measuredangle(S) &\Rightarrow \mathrm{Re}(a) \in \measuredangle(S) \text{ und } \mathrm{Im}(a) \in \measuredangle(S) \\
a \in \measuredangle(S) &\Rightarrow \overline{a} = a - 2\,\mathrm{Im}(a) \in \measuredangle(S) \\
\measuredangle(S) &= \measuredangle(S \cup \overline{S})
\end{aligned}$$

Insbesondere folgt aus $\mathbb{Q} + i\mathbb{Q} \subseteq \measuredangle(S)$, dass jeder Punkt aus $\mathbb{C}$ beliebig gut durch konstruierbare Punkte approximiert werden kann.

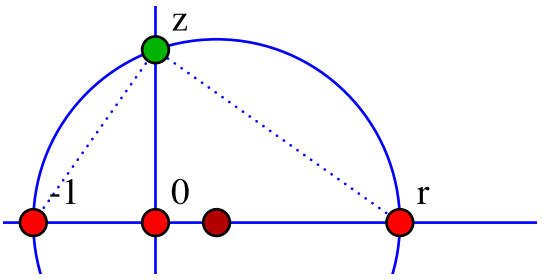
Eine der wichtigsten Eigenschaften des Teilkörpes $\measuredangle(S)$ ist die folgende.

Satz: Der Teilkörper $\measuredangle(S)$ von $\mathbb{C}$ ist **quadratisch abgeschlossen**, d.h. aus $a \in \measuredangle(S)$ und $b^2 = a$ folgt $b \in \measuredangle(S)$.

Beweis: Es sei $a = re^{i\varphi}$ mit $\varphi \in [0, 2\pi)$. Dann gilt $b = \sqrt{r}e^{i\varphi/2}$ oder $b = \sqrt{r}e^{i(\varphi/2+\pi)}$, in jedem Fall liegt b auf der Winkelhalbierenden des Winkels φ. Da sich letztere konstruieren lässt genügt es also zu zeigen dass $\sqrt{r} \in \measuredangle(S)$ für $r \in \mathbb{R} \cap \measuredangle(S)$ mit $r > 0$.

In nebenstehender Konstruktion gilt $|z|^2 = |-1| \cdot r$ nach dem Satz des Thales, also

$$|z| = \sqrt{r} \in \measuredangle(S).$$



■

Der Begriff des **Teilkörpers** wird der zentrale Begriff in der Analyse der oben genannten klassischen Probleme sein. Er ist darüber hinaus eines der wichtigsten Objekte in der Algebra. Deshalb erhält er einen weiteren Namen.

Definition: Sei E ein Körper und $k \subseteq E$ ein Unterkörper. Dann heißt E ein **Erweiterungskörper** von k. Ist $A \subseteq E$ beliebig, dann setze

$$k(A) := \bigcap \{F \subseteq E \mid F \text{ ist Teilkörper mit } k \subseteq F \text{ und } A \subseteq F\}.$$

Falls $A = \{a_1, ..., a_n\}$ endlich ist, so schreiben wir $k(A)$ auch als $k(a_1, ..., a_n)$.

Wir werden gleich sehen, dass $k(A)$ ebenfalls ein Erweiterungskörper von k ist. Die Analyse der Beziehung von E zu $k(A)$ und der von $k(A)$ zu k wird im Folgenden zentral sein.

Satz: $k(A)$ ist ein Teilkörper von E, der k und A enthält. Ferner gilt für jeden Teilkörper F, der k und A enthält dass $k(A) \subseteq F$.

Beweis: Es ist nur zu zeigen, dass $k(A)$ ein Teilkörper von E ist. Es gilt z.B.:

$$\begin{aligned} a, b \in k(A) &\Rightarrow a, b \in F \text{ für alle Teilkörper } F \text{ mit } k \subseteq F \text{ und } A \subseteq F \\ &\Rightarrow a + b \in F \text{ für alle Teilkörper } F \text{ mit } k \subseteq F \text{ und } A \subseteq F \\ &\Rightarrow a + b \in k(A). \end{aligned}$$

Die anderen Bedingungen folgen analog. ■

Beispiel:

1. Ist $E = \mathbb{C}$, $k = \mathbb{Q}$ und $A = \{i\}$, so ist
$$\mathbb{Q}(i) = \mathbb{Q} + i\mathbb{Q}.$$
2. Ist $E = \mathbb{C}$, $k = \mathbb{Q}$ und $A = \{\sqrt{2}\}$, so ist
$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \sqrt{2} \cdot \mathbb{Q}.$$

In beiden Fällen liegt dies daran, dass $i^2 = -1$ und $\sqrt{2}^2 = 2$ wieder in $\mathbb{Q}$ sind. Dieses Phänomen machen wir wiederum zur Definition.

Definition: Sei E ein Erweiterungskörper von k. Dann sagen wir E entsteht durch **Adjunktion einer Quadratwurzel** aus k, wenn es ein $w \in E$ gibt so dass $w^2 \in k$ und $E = k(w)$.
Wir sagen E entsteht durch **sukzessive Adjunktion von Quadratwurzeln**, wenn es eine endliche Kette $k = F_0 \subset F_1 \subset ... \subset F_m = E$ gibt, so dass jedes F_{i+1} aus F_i durch Adjunktion einer Quadratwurzel entsteht.

Hiermit haben wir jetzt alle Begriffe zusammen, die wir benötigen um das Konstruierbarkeitsproblem durch die Beziehung der Körper $\mathbb{Q}(S)$ und $\measuredangle(S)$ zu beschreiben. Beachte zunächst, dass $\mathbb{Q}(S) \subseteq \measuredangle(S)$ und dass $\measuredangle(S) = \measuredangle(S \cup \overline{S})$, wobei $\overline{S} := \{\overline{z} \mid z \in S\}$ (komplexe Konjugation von S). Wir benötigen zunächst noch einen Hilfssatz (Beweis in dem Übungen).

Lemma: Ist $k \subseteq \mathbb{C}$ ein Teilkörper mit $k = \overline{k}$, so gilt

1. Sind $\gamma, \eta \in \mathrm{Ge}(k)$ und $\gamma \neq \eta$, so ist $\gamma \cap \eta \in k$.

2. Ist $\gamma \in \mathrm{Ge}(k)$, $\kappa \in \mathrm{Kr}(S)$ und $z \in \gamma \cap \kappa$, so gibt es ein $w \in \mathbb{C}$ mit $w^2 \in k$ und $z \in k(w)$.

3. Sind $\kappa, \lambda \in \mathrm{Kr}(S)$, $\kappa \neq \lambda$ und $z \in \kappa \cap \lambda$, so gibt es ein $w \in \mathbb{C}$ mit $w^2 \in k$ und $z \in k(w)$.

Satz: Sei $S \subseteq \mathbb{C}$ mit $0, 1 \in S$. Setze $F := \mathbb{Q}(S \cup \overline{S})$. Dann sind äquivalent:

1. Es ist z aus S konstruierbar, also $z \in \measuredangle(S)$.
2. Es gibt einen Teilkörper E von $\mathbb{C}$, der z und F enthält und der aus F durch sukzessive Adjunktion von Quadratwurzeln entsteht.

Beweis: 2.⇒1.: Es gibt eine Kette

$$F = F_0 \subset F_1 \subset ... \subset F_m = E \quad \text{mit} \quad F_{i+1} = F_i(w_{i+1}) \text{ für } w_{i+1}^2 \in F_i$$

so dass $z \in E$. Da $\measuredangle(S)$ quadratisch abgeschlossen ist und $F_0 \subseteq \measuredangle(S)$ gilt $w_1 \in \measuredangle(S)$, und damit $F_1 = F_0(w_1) \subseteq \measuredangle(S)$. Mit dem gleichen Argument sieht man $w_2 \in \measuredangle(S)$ und $F_2 \subseteq \measuredangle(S)$ und iterativ dann $a \in E \subseteq \measuredangle(S)$.

1.⇒2.: Wir betrachten zunächst einen der elementaren Konstruktionsschritte. Ist $z \in \gamma \cap \eta$ mit $\gamma, \eta \in \mathrm{Ge}(S)$, so ist $z \in F_1 := F$.
Ist $z \in \gamma \cap \kappa$ oder $z \in \kappa \cap \lambda$, so ist (nach dem vorigen Lemma) $z \in F(w)$ für ein $w \in \mathbb{C}$, da $F = \overline{F}$ nach Voraussetzung. Insbesondere ist dann auch $z \in F_1 := (F(w))(\overline{w})$ und $F_1 = \overline{F_1}$.
Eine Induktion nach der Anzahl der Konstruktionsschritte zeigt dann die Behauptung. ■

Satz: Sei $S \subseteq \mathbb{C}$ mit $0, 1 \in S$. Setze $F := \mathbb{Q}(S \cup \overline{S})$. Dann sind äquivalent:

1. Es ist z aus S konstruierbar, also $z \in \measuredangle(S)$.

2. Es gibt einen Teilkörper E von $\mathbb{C}$, der z und F enthält und der aus F durch sukzessive Adjunktion von Quadratwurzeln entsteht.

Mit diesem Satz haben wir das Konstruierbarkeitsproblem vollständig in in rein algebraisches Problem übersetzt. Wir werden nun einen ersten Versuch unternehmen, das algebraische Problem zu lösen, indem wir einer Körpererweiterung eine (sehr grobe aber fundamentale) **Invariante** zuordnen.

Lemma/Definition: Ist E ein Erweiterungskörper von k, so ist E (mit der Einschränkung der Körperoperationen) ein Vektorraum über k. Wir bezeichnen mit

$$[E : k]$$

die Dimension dieses Vektorraums und nennen diese auch den **Grad** von E über k.

Beweis: Die Körperaxiome implizieren die Vektorraumaxiome. ■

Beispiele:

- $\mathbb{R}$ ist Teilkörper von $\mathbb{C}$ und es gilt $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = 2$.
- Da $\mathbb{R}$ überabzählbar ist kann $[\mathbb{R} : \mathbb{Q}]$ nicht abzählbar sein.

Satz: E : Erweiterungskörper von k mit $1 + 1 \neq 0$. Dann sind äquivalent:

1. $[E : k] = 2$
2. E entsteht aus k durch Adjunktion einer Quadratwurzel, die nicht schon in k liegt.

Beweis: 1.⇒2.: Sei $\alpha \in E \backslash k$. Dann ist $\{1, \alpha\}$ eine k-Basis von E. Insbesondere existieren $p, q \in k$ so dass

$$\alpha^2 + p\alpha + q = 0$$

Mit $w := \alpha + \frac{p}{2}$ ist $w^2 \in k$, und $E = K(\alpha) = K(w)$ zeigt die Behauptung. 2.⇒1.: Ist $E = k(w)$ mit $w^2 \in k$, so ist $F := \{x + wy \mid x, y \in k\}$ ein Teilkörper (vgl. Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$) von E, der k und w enthält. Also gilt $F = E$ und offensichtlich ist $\dim_k(F) = 2$. ■

Um die Invariante des Körpergrads jetzt mit der vorigen iterativen Konstruktion von Zwischenkörpern

$$F = F_0 \subset F_1 \subset ... \subset F_m = E$$

in Verbindung zu bringen müssen wir wissen, dass sich der Grad mit Zwischenkörpern verträgt.

Satz (Gradformel): Sei F ein Teilkörper von E und k ein Teilkörper von F. Dann ist k ein Teilkörper von E und es gilt

$$[E : k] = [E : F] \cdot [F : k].$$

Falls $[F : k]$ und $[E : F]$ endlich sind.

Beweis: Es ist $E \cong F^n$ als F-Vektorraum und $F \cong k^m$ als k-Vektorraum. Also gilt

$$E \cong F^n \cong (k^m)^n$$

als k-Vektorraum. Also gilt $\dim_k(E) = nm$. ■

Korollar: Entsteht E aus k durch sukzessive Adjunktion von Quadratwurzeln, so gilt

$$[E : k] \text{ ist eine Potenz von 2.}$$

Korollar: Ist $k = \overline{k} \subseteq \mathbb{C}$ Teilkörper und $z \in \mathbb{C}$ aus k konstruierbar, so gilt

$$[k(z) : k] \text{ ist eine Potenz von 2.}$$

Leider ist die Umkehrung dieses Korollars im Allgemeinen nicht richtig, man kann hieraus also nur ein Kriterium für die **nicht-Konstruierbarkeit** ableiten. Darüber hinaus liefert es auch nur dann ein Kriterium, wenn man $[\mathbb{Q}(S \cup \overline{S}) : \mathbb{Q}]$ **auf irgendeine andere Weise berechnen** kann. Wir werden beide Sachverhalte **im Laufe der Vorlesung** erörtern.

Abschließend sei noch erwähnt, dass die **Auflösbarkeit** von Polynomgleichungen auch durch eine Körpererweiterung entschieden werden kann. Die Invariante (die **Auflösbarkeit der assoziierten Galois-Gruppe**) ist hier jedoch deutlich komplizierter.

Wir fassen die zuvor genanten Probleme noch einmal in der neuen Sprache zusammen:

- Delisches Problem: Ist $\sqrt[3]{2}$...
- Winkeldrittelung: Für welche φ ist $e^{i\frac{\varphi}{3}}$...
- Quadratur des Kreises: Ist $\frac{1}{\sqrt{\pi}}$ (äquivalenter Weise π)...
- Regelmässige n-Ecke: Ist $e^{\frac{2\pi i}{n}}$...

...in einem Teilkörper von $\mathbb{C}$ enthalten, der aus $\mathbb{Q}$ durch sukzessive Adjunktion von Einheitswurzeln entsteht?

Bemerkung: Man kann z.B. mit reletiv elementaren Mitteln zeigen, dass $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Daraus folgt dann insbesondere auch, dass π nicht in einem Teilkörper von $\mathbb{C}$ enthalten ist, der aus $\mathbb{Q}$ durch sukzessive Adjunktion von Einheitswurzeln entsteht, da in diesem Fall $[\mathbb{Q}(\pi) : \mathbb{Q}] < \infty$ gelten würde. Es ist also **die Quadratur des Kreises unmöglich**.

Nachlesen kann man dies hier alles unter [LL07, Kapitel 1].

Literatur

[LL07] Lorenz, F. and Lemmermeyer, F. **Algebra 1. Körper und Galoistheorie. (4. Auflage)** (Heidelberg: Elsevier/Spektrum Akademischer Verlag, 2007)