Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 1

Lösungen von polynomialen Gleichungen

Es sei eine polynomiale Gleichung

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0$$

gegeben, wobei die Koeffizienten $a_0, a_1, \ldots, a_n$ reelle (oder komplexe) Zahlen seien und nach Elementen $x \in \mathbb{C}$ gesucht wird, die diese Gleichung erfüllen. Wie kann man solche Lösungen finden? Die Lösbarkeit hängt dabei natürlich wesentlich vom Grad der Gleichung ab, das ist der maximale Index n mit $a_n \neq 0$. Bei $n = 1$ liegt eine lineare Gleichung

$$a_1 x + a_0 = 0$$

vor mit der eindeutigen Lösung $x = -\frac{a_0}{a_1}$. Dies kann man bilden, da nach Voraussetzung $a_1 \neq 0$ ist und da die Koeffizienten aus $\mathbb{C}$ sind, also aus einem Körper, wo man uneingeschränkt durch von 0 verschiedene Zahlen dividieren kann. Bei $n = 2$ liegt eine *quadratische Gleichung* vor, also

$$a_2 x^2 + a_1 x + a_0 = 0$$

mit $a_2 \neq 0$. Hier führt man zunächst eine *Normierung* durch, was man bei jedem Grad machen kann. Das bedeutet, dass man durch den Leitkoeffizienten a_n dividiert, um diesen zu 1 zu normieren. Dabei ändern sich die Lösungen der Gleichung offenbar nicht. Im quadratischen Fall gelangt man so zur äquivalenten Gleichung

$$x^2 + b_1 x + b_0 = 0\,.$$

Diese Gleichung führt man durch *quadratisches Ergänzen* auf eine reine Gleichung zurück. Man macht den Ansatz $y = x + \frac{b_1}{2}$ und schreibt dann die Gleichung als

$$(x + \frac{b_1}{2})^2 + b_0 - (\frac{b_1}{2})^2 = 0$$

bzw. als

$$y^2 + c_0 = 0$$

mit $c_0 = b_0 - (\frac{b_1}{2})^2$. Dieser Koeffizient c_0 gehört wieder zum Körper. Wenn y_1 eine Lösung dieser Gleichung ist, so ist $x_1 = y_1 - \frac{b_1}{2}$ eine Lösung der quadratischen Ausgangsgleichung. Die neu gewonnene äquivalente Gleichung ist eine sogenannte *reine Gleichung*, d.h. eine Gleichung der Form

$$y^n = d\,.$$

Um eine solche reine Gleichung lösen zu können muss man „die“ n-te Wurzel aus d ziehen können. Die Schwierigkeit dieser Aufgabe und die Anzahl der Lösungen hängt von der Arithmetik des Körpers ab und ist nicht trivial. Dennoch ist es eine wesentliche Reduktion, wenn man, wie im quadratischen Fall, die Lösung einer polynomialen Gleichung auf die Lösung einer (oder mehrerer) reinen Gleichungen zurückführen kann.

Kubische Gleichungen

Wir betrachten nun eine normierte kubische Gleichung

$$x^3 + a_2x^2 + a_1x + a_0 = 0\,,$$

wobei die Koeffizienten aus $\mathbb{C}$ seien. Mit einem Ergänzungstrick können wir den quadratischen Koeffizienten a_2 eliminieren. Wir machen den Ansatz $y = x + \frac{a_2}{3}$ und schreiben die Gleichung als

$$(x + \frac{a_2}{3})^3 + (a_1 - 3(\frac{a_2}{3})^2)(x + \frac{a_2}{3}) - (a_1 - 3(\frac{a_2}{3})^2)\frac{a_2}{3} - (\frac{a_2}{3})^3 + a_0 = 0$$

bzw. als

$$y^3 + py + q = 0$$

mit den neuen Koeffizienten

$$p = a_1 - 3(\frac{a_2}{3})^2 \text{ und } q = -(a_1 - 3(\frac{a_2}{3})^2)\frac{a_2}{3} - (\frac{a_2}{3})^3 + a_0\,.$$

Lösungen dieser vereinfachten Gleichung führen direkt zu Lösungen der Ausgangsgleichung.

Gerolamo Cardano (1501-1576)

Die vereinfachte Gleichung kann man über die folgende *Formel von Cardano* lösen. Wir brauchen dafür ein Lemma über dritte Einheitswurzeln von $\mathbb{C}$, das sind komplexe Zahlen η mit $\eta^3 = 1$, also die Lösungen der reinen kubischen Gleichung $x^3 = 1$.

Lemma 1.1. *Es gelten folgende Aussagen.*

(1) *Die dritten Einheitswurzeln in* $\mathbb{C}$ *sind* 1, $\epsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ *und* $\eta = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.
(2) *Es ist* $\epsilon^2 = \eta$ *und* $\eta^2 = \epsilon$.
(3) *Es ist* $1 + \epsilon + \epsilon^2 = 0$.
(4) *Es ist* $\epsilon + \epsilon^2 = -1$.

Beweis. Siehe Aufgabe 1.1. □

Satz 1.2. *Es sei*

$$x^3 + px + q = 0$$

mit $p, q \in \mathbb{C}$ *eine kubische Gleichung. Wir setzen* $D = -4p^3 - 27q^2$. *Es seien*

$$u = \sqrt[3]{\frac{1}{2}(-q + \frac{1}{9}\sqrt{-3D})} \text{ und } v = \sqrt[3]{\frac{1}{2}(-q - \frac{1}{9}\sqrt{-3D})}\,,$$

wobei diese dritten Wurzeln so gewählt seien, dass $uv = -\frac{p}{3}$ *ist. Dann sind (mit der dritten Einheitswurzel* $\epsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$*) die Elemente*

$$u + v, \epsilon u + \epsilon^2 v \text{ und } \epsilon^2 u + \epsilon v$$

die Lösungen dieser kubischen Gleichung.

Beweis. Wir zeigen zuerst, dass die dritten Wurzeln u und v so gewählt werden können, dass ihr Produkt gleich $-\frac{1}{3}p$ ist. Für eine irgendwie gewählte Quadratwurzel $\sqrt{-3D}$ und irgendwie gewählte dritte Wurzeln u und v ist

$$\begin{aligned} uv &= \sqrt[3]{\frac{1}{4}(q^2 - \frac{1}{81}(-3D))} \\ &= \sqrt[3]{\frac{1}{4}(q^2 + \frac{1}{27}(-4p^3 - 27q^2))} \\ &= \sqrt[3]{\frac{1}{4} \cdot \frac{-4}{27}p^3} \\ &= \sqrt[3]{-\frac{1}{27}p^3} \\ &= \eta(-\frac{p}{3}), \end{aligned}$$

wobei η eine dritte Einheitswurzel ist. Ersetzt man nun v durch $\eta^2 v$, so ist das Produkt gleich $-\frac{p}{3}$.

Wir berechen nun

$$(x - u - v)(x - \epsilon u - \epsilon^2 v)(x - \epsilon^2 u - \epsilon v)$$

und müssen zeigen, dass dies gleich $x^3 + px + q$ ist. Die angegebenen Elemente sind offenbar die Nullstellen dieses faktorisierten Polynoms. Es ist

$$\begin{aligned} & (x - u - v)(x - \epsilon u - \epsilon^2 v)(x - \epsilon^2 u - \epsilon v) \\ = \; & x^3 - (u + v + \epsilon u + \epsilon^2 v + \epsilon^2 u + \epsilon v)x^2 \\ & +((u + v)(\epsilon u + \epsilon^2 v) + (u + v)(\epsilon^2 u + \epsilon v) + (\epsilon u + \epsilon^2 v)(\epsilon^2 u + \epsilon v))x \\ & -(u + v)(\epsilon u + \epsilon^2 v)(\epsilon^2 u + \epsilon v). \end{aligned}$$

Der quadratische Koeffizient ist (unter Verwendung von Lemma 1.1)

$$u(1+\epsilon+\epsilon^2)+v(1+\epsilon+\epsilon^2) \;=\; 0.$$

Der lineare Koeffizient ist

$$\begin{aligned} & (u+v)(\epsilon u+\epsilon^2 v)+(u+v)(\epsilon^2 u+\epsilon v)+(\epsilon u+\epsilon^2 v)(\epsilon^2 u+\epsilon v) \\ = \;& u^2(\epsilon+\epsilon^2+1)+v^2(\epsilon^2+\epsilon+1)+uv(\epsilon+\epsilon^2+\epsilon^2+\epsilon+\epsilon^2+\epsilon^4) \\ = \;& -\frac{p}{3}(-3) \\ = \;& p. \end{aligned}$$

Der konstante Koeffizient ist

$$\begin{aligned} -(u+v)(\epsilon u+\epsilon^2 v)(\epsilon^2 u+\epsilon v) &= -u^3-u^2v(1+\epsilon+\epsilon^2)-uv^2(1+\epsilon+\epsilon^2)-v^3 \\ &= -u^3-v^3 \\ &= -\frac{1}{2}(-q+\frac{1}{9}\sqrt{-3D})-\frac{1}{2}(-q-\frac{1}{9}\sqrt{-3D}) \\ &= q. \end{aligned}$$

□

Beispiel 1.3. Wir betrachten die kubische Gleichung

$$x^3+2x-1=0$$

und wenden darauf Satz 1.2 an. Es ist demnach $p=2$, $q=-1$, $D=-59$ und somit $u=\sqrt[3]{\frac{1}{2}(1+\frac{1}{9}\sqrt{177})}$ und $v=\sqrt[3]{\frac{1}{2}(1-\frac{1}{9}\sqrt{177})}$. Dabei wählen wir jeweils die reellen dritten Wurzeln, was automatisch die reelle Bedingung $uv=-\frac{2}{3}$ sicherstellt. Somit ist $u+v$ eine reelle Lösung der Gleichung. Man sieht, dass diese Lösung aus Lösungen von rein-quadratischen und rein-kubischen Gleichungen mittels arithmetischer Ausdrücke zusammengesetzt ist, darüber hinaus aber keine einfache Gestalt besitzt. Den numerischen Wert dieser Lösung kann man beliebig genau durch beliebig genaue Berechnungen der Lösungen der reinen Gleichungen ausrechnen, doch könnte man genauso gut direkt (mit dem Halbierungsverfahren oder Ähnlichem) die Nullstelle numerisch berechnen.

Für den Fall eines Polynoms vom Grad 4 gibt es ebenfalls eine Lösungsformel. Eine Hauptmotivation zur Entwicklung der Körper- und Galoistheorie war die Fragestellung, ob es für Polynome vom Grad ≥ 5 ebenfalls Formeln gibt, mit denen man die Nullstellen als arithmetische Ausdrücke in Lösungen zu reinen Gleichungen ausdrücken kann. Eines der Hauptergebnisse, das wir nach einigen Vorbereitungen beweisen werden, ist, dass es eine solche Formel nicht geben kann.

Der Fundamentalsatz der Algebra

Sei ein Polynom $F \in K[X]$, wobei K einen Körper bezeichnet, bzw. die zugehörige Nullstellengleichung $F(x)=0$ gegeben. In K selbst muss F keine Nullstellen besitzen. Ist es überhaupt klar, dass F in irgend einem Körper

Nullstellen besitzt? Oben gehörten alle Koeffizienten von F zum Körper $\mathbb{C}$ der komplexen Zahlen. Dies garantiert, dass es Lösungen zu der polynomialen Gleichung gibt. Diese Eigenschaft der komplexen Zahlen beruht auf dem Fundamentalsatz der Algebra, der in Mathematik I bewiesen wurde und an den wir hier erinnern wollen.

SATZ 1.4. *Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.*

Beweis. Siehe den Beweis zu Satz 30.8 der Vorlesung Mathematik I. □

Bis jetzt kennen wir noch keinen anderen Körper mit dieser Eigenschaft, dennoch halten wir hier schonmal folgende Definition fest.

DEFINITION 1.5. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $F \in K[X]$ eine Nullstelle in K besitzt.

Mit diesem Begriff kann man den Fundamentalsatz der Algebra so ausdrücken, dass $\mathbb{C}$ algebraisch abgeschlossen ist.

Wenn man zu einem Polynom F eine Nullstelle a gefunden hat, so kann man nach Lemma Anhang 1.4 $F = (X - a)\tilde{F}$ schreiben. Zu jedem Polynom $F \in \mathbb{C}[X]$ vom Grad n gibt es daher eine Produktdarstellung

$$F = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

mit eindeutig komplexen Zahlen $\alpha_1, \ldots, \alpha_n$. Diese zu finden ist aber schwierig, selbst wenn die Koeffizienten von F harmlos sind (z.B. bei $F \in \mathbb{Q}[X]$), wie schon die Cardanosche Formel für den Grad 3 deutlich macht. Diese „Schwierigkeit“, bei höherem Grad Nullstellen explizit zu finden, ist ein wichtiges Thema dieser Vorlesung.

Der algebraische Zugang

Es ist gut zu wissen, dass es zu einem Polynom $F \in \mathbb{C}[X]$ Nullstellen in $\mathbb{C}$ gibt und dass es daher eine Zerlegung des Polynoms in Linearfaktoren gibt. Allerdings muss man, neben der prinzipiellen Schwierigkeit, diese Nullstellen zu finden, bedenken, dass die komplexen Zahlen $\mathbb{C}$ auf den reellen Zahlen $\mathbb{R}$ beruhen, die selbst wiederum mit topologischen Mitteln (durch die Vervollständigung) aus den rationalen Zahlen $\mathbb{Q}$ konstruiert wurden. Hinter den komplexen Zahlen steckt also ein enormer technischer Apparat, während ein einzelnes Polynom eine völlig andere „Datenstruktur“ aufweist. Ein Polynom

$$F = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{C}[X]$$

ist durch seine endlich vielen Koeffizienten $a_0, a_1, \ldots, a_n \in \mathbb{C}$ festgelegt, und seine Nullstellen sind n Zahlen $\alpha_1, \ldots, \alpha_n$ (die nicht verschieden sein müssen). Um Beziehungen zwischen den Koeffizienten und den Nullstellen ausdrücken zu können, braucht man gar nicht die gesamten komplexen Zahlen. Es genügt,

sich auf diejenigen arithmetischen Ausdrücke zu beschränken, die man ausgehend von den Koeffizienten und den Nullstellen konstruieren kann. Wenn z.B., wie das häufig der Fall sein wird, die Koeffizienten rationale Zahlen sind, so spielt sich alles innerhalb der polynomialen Ausdrücke über $\mathbb{Q}$ in den Nullstellen α_i ab, also Ausdrücken der Form

$$\sum_{\nu=(\nu_1,\dots,\nu_n)} b_\nu \alpha_1^{\nu_1} \cdots \alpha_n^{\nu_n} .$$

Dabei sind die b_ν rationale Zahlen, und sämtliche Exponententupel $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$ sind erlaubt, wobei die Summe aber endlich ist.

Beispiel 1.6. Wir betrachten das Polynom $X^2 + 1$, dessen Koeffizienten zu $\mathbb{Q}$ gehören und das in $\mathbb{Q}$ (und auch in $\mathbb{R}$) keine Nullstelle besitzt. In den komplexen Zahlen besitzt es die beiden Nullstellen i und $-i$, so dass in $\mathbb{C}[X]$ die Faktorzerlegung

$$X^2 + 1 \;=\; (X - i)(X + i)$$

vorliegt. Um dies hinschreiben zu können, braucht man aber nicht die gesamten komplexen Zahlen, sondern lediglich das Element i. Wir betrachten die Menge

$$\mathbb{Q}[i] = \mathbb{Q}1 + \mathbb{Q}i = \{a + bi |\, a, b \in \mathbb{Q}\} ,$$

also einen zweidimensionalen $\mathbb{Q}$-Vektorraum mit den Basiselementen 1 und i, wobei zusätzlich noch eine Multiplikation durch die Bedingung $i^2 = -1$ festgelegt wird. Dies ist die gleiche Konstruktion, mit der man aus $\mathbb{R}$ die komplexen Zahlen gewinnt, nur dass man hier von den rationalen Zahlen ausgeht. Es lässt sich leicht zeigen, dass das konstruierte Objekt $\mathbb{Q}[i]$ ein Körper ist. Für ein von 0 verschiedenes Element $a + bi$ ist

$$\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

das inverse Element, und dies gehört offenbar wieder zu $\mathbb{Q}[i]$. Die Zerlegung $X^2 + 1 = (X - i)(X + i)$ gilt ebenfalls in $\mathbb{Q}[i][X]$, und durch die Zuordnung $a+bi \mapsto a-bi$ gibt es auch eine Konjugation, die völlig analoge Eigenschaften hat wie die komplexe Konjugation in $\mathbb{C}$.

Beispiel 1.7. Wir betrachten das Polynom $X^2 - 3$, dessen Koeffizienten zu $\mathbb{Q}$ gehören. In den reellen Zahlen $\mathbb{R}$ besitzt dieses Polynom die Nullstelle[1] $\sqrt{3}$, die irrational ist. Über $\mathbb{R}$ hat man die Zerlegung $X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3})$. Um dies auszudrücken, braucht man aber nicht die gesamten reellen Zahlen, sondern lediglich $\sqrt{3}$, das man einfach als ein Symbol auffassen kann mit der Eigenschaft, dass sein Quadrat gleich 3 sein soll. Eine „Verortung“ innerhalb der reellen Zahlen ist dazu nicht nötig. Präziser formuliert betrachtet man

$$L = \mathbb{Q}1 + \mathbb{Q}u = \{a + bu |\, a, b \in \mathbb{Q}\} ,$$

[1] Die Existenz der Nullstelle beruht auf dem Zwischenwertsatz, wobei sich die Existenz von $\sqrt{3}$ auch direkt aus der Vollständigkeit von $\mathbb{R}$ ergibt.

also einen zweidimensionalen $\mathbb{Q}$-Vektorraum mit den Basiselementen 1 und u, wobei eine Multiplikation durch die Bedingung $u^2 = 3$ (und distributive Fortsetzung) festgelegt wird. Das Element u ist hier lediglich ein Symbol, für das man häufig wegen der intendierten Eigenschaft auch $\sqrt{3}$ schreibt (man schreibt auch $L = \mathbb{Q}[\sqrt{3}]$). In L gilt die Zerlegung $X^2 - 3 = (X - u)(X + u)$, und wegen

$$(a + bu)(\frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}u) \; = \; \frac{a^2 - 3b^2}{a^2 - 3b^2} \; = \; 1$$

handelt es sich um einen Körper. Dazu muss man sich klar machen, dass bei $a + bu \neq 0$ mit rationalen Zahlen $a, b \in \mathbb{Q}$, die nicht beide 0 sind, auch $a^2 - 3b^2 \neq 0$ ist, was äquivalent zur Irrationalität von $\sqrt{3}$ ist. Es sind also wesentliche Eigenschaften des Polynoms $X^2 - 3$, die über $\mathbb{R}$ sichtbar werden, bereits über L sichtbar. Es gibt aber auch Unterschiede, bspw. sind bei dieser algebraischen Konstruktion von L die beiden Elemente u und $-u$ vollkommen gleichberechtigt, während innerhalb der reellen Zahlen die eine Quadratwurzel positiv und die andere negativ ist. Diese Gleichberechtigung zeigt sich auch darin, dass durch

$$L \longrightarrow L,\, a + bu \longmapsto a - bu,$$

eine „Konjugation“ definiert wird, die es innerhalb der reellen Zahlen nicht gibt.

Abbildungsverzeichnis