Algebra Kapitel 14

Solutions of equations by radicals

Merten Lampe

I) Einleitung

In diesem Kapitel werden wir die Galois-Korrespondenz nutzen, um Kriterien anzugeben, wann ein Polynom f durch Radikale lösbar ist:
Die zu f zugehörige Galois-Gruppe muss auflösbar sein.

Dann werden wir ein Polynom fünften Grades konstruieren, dass nicht durch Radikale lösbar ist und damit die mögliche Vermutung, dass nach Polynomen ersten bis vierten Grades auch jene fünften Grades allgemein durch Radikale lösbar sind, widerlegen.

II) Radikale Körpererweiterungen

Definition 1

Ein sukzessive aus verschachtelten n-ten Wurzeln beliebiger Körperelemente zusammengesetzter Ausdruck wird als **Radikal** bezeichnet.

Beispiel 2

Ein Beispiel für ein Radikal wäre dieser Ausdruck:

$$\sqrt[3]{11\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[7]{4}}}.$$

Definition 3

Eine Körpererweiterung $L:K$ heißt **radikal**, falls

$$L = K(\alpha_1, \ldots, \alpha_n)$$

mit $\alpha_k^{N(k)} \in K(\alpha_1, \ldots, \alpha_{k-1})$, $N(k) \in \mathbb{N}$.
Eine radikale Körpererweiterung wird also sukzessive durch Hinzunahme von n-ten Wurzeln bereits erlaubter Terme generiert. Die erweiternden Elemente $\{\alpha_1, \ldots, \alpha_n\}$ heißen **radikale Sequenz** von $L:K$.

Proposition 4

Eine radikale Körpererweiterung kann durch Hinzunahme weiterer Elemente zur Sequenz so dargestellt werden, dass statt der allgemeinen n-ten Wurzeln nur prime Wurzeln auftauchen.

Beweis Betrachte $K(\alpha)$ mit

$$\alpha = \sqrt[N]{\beta} \text{ mit } \beta \in K, N \in \mathbb{N}.$$

Sei $N = p_1 \cdots p_m$ die eindeutige Primfaktorzerlegung von N, dann definiere

$$\gamma_k := \beta^{(p_1 \cdots p_k)^{-1}} = \alpha^{p_{k+1} \cdots p_m}.$$

Es gilt: $K(\gamma_1, \ldots, \gamma_m) = K(\alpha)$, da

i) $\gamma_m = \alpha$

ii) man jedes γ_k wieder durch eine entsprechende Potenz von α ausdrücken kann.

Diese Idee kann für nicht-einfache Körpererweiterungen iterativ angewendet werden, woraus die Behauptung folgt. □

Definition 5

Sei $f \in K[X]$ Polynom über K, die Charakteristik $\text{char}(K)$ des Körpers K sei Null. Sei Σ der Zerfällungskörper von f über K.
f heißt **durch Radikale lösbar**, wenn es einen radikalen Oberkörper $M \supseteq \Sigma$ gibt.

Bemerkung Für durch Radikale lösbare Polynome muss $\Sigma : K$ selbst nicht unbedingt radikal sein, da durch den sukzessiven Aufbau von Wurzeltermen in der Regel weit mehr Terme entstehen, als für die endgültigen Nullstellen nötig sind.
Ein Beispiel dafür wäre ein Zerfällungskörper $\Sigma = K()$, der nicht radikal ist, da er die im radikalen Sinne erzeugenden Elemente ? und ? nicht enthält.

III) Motivation

Elementar für das Vorhaben ist folgender Satz, den wir erst nach Bereitstellung einiger Lemmas beweisen können:

Satz 6

Sei K ein Körper mit $\text{char}(K) = 0$ und seien $M \supseteq L \supseteq K$ zugehörige Körpererweiterungen. Falls $M : K$ eine radikale Erweiterung ist, dann ist $L : K$ auflösbar.

Das erste Ziel dieses Kapitels ist nach obiger Definition äquivalent zu Satz 6:

Korollar 7

Sei f ein Polnom über einem Körper K mit $\text{char}(K) = 0$.
Falls f mit Radikalen auflösbar ist, dann ist die Galois-Gruppe von f über K auflösbar.

IV) Beweis von Satz 6

Wiederholung

Sei Γ die Galois-Gruppe eines irreduziblen Polynoms f über einem Körper K mit Charakteristik Null. Für eine Nullstelle $\alpha \in \Sigma$ gilt dann für alle $\gamma \in \Gamma$:

$$f(\gamma(\alpha)) = \gamma(f(\alpha)) = 0.$$

Dies ist klar, da $\Gamma = Aut_K(\Sigma)$ das Polynom mit Koeffizienten aus K nicht verändert. Daher induziert γ eine Permutation der Nullstellenmenge von f in Σ. Da f als Polynom über einem Körper mit Charakteristik Null seperabel ist, haben wir paarweise verschiedene Nullstellen.
Damit ist die Zuordnung von Automorphismus zu Permutation injektiv, dh. zwei verschiedene Elemente in Γ wirken auch unterschiedlich auf die Menge der Nullstellen, weshalb man die Galois-Gruppe immer auch als Permutationsgruppe der Nullstellen betrachten kann.
Dies ist übrigens die Betrachtungsweise, mit der Galois selber seine Theorie aufgestellt hat...

Lemma 8

Falls $L : K$ eine radikale Körpererweiterung ist, dann gilt dies auch für die normale Hülle $M : K$.

Beweis Sei $L = K(\alpha_1, \ldots, \alpha_n)$. Die normale Hülle entsteht jeweils durch Hinzunahme der fehlenden Nullstellen der Minimalpolynome der α_k zu L. Nun ist jede Nullstelle eines solchen Polynoms als körpererweiterndes Element isomorph zu der einen vorgegebenen (Satz(4.4.4)), weshalb man für jede beliebige Nullstelle eines jeden Minimalpolynoms eine radikale Sequenz aufstellen kann. Die Vereinigung dieser Sequenzen liefert die Behauptung. □

Wiederholung 9

Sei K ein Körper mit $\mathrm{char}(K) = 0$ und Σ der Zerfällungkörper von $X^p - 1$ über K, sowie p eine Primzahl. Dann ist die Galois-Gruppe $\Gamma(\Sigma : K)$ von $\Sigma : K$ abelsch.

Wiederholung 10

Sei K ein Köper mit $char(K) = 0$, in dem $X^n - 1$ zerfällt, wobei hier $n \in \mathbb{N}$ beliebig. Weiter sei $\alpha \in K$ und Σ der Zerfällungskörper von $X^n - \alpha$ über K. Dann ist die Galois-Gruppe $\Gamma(\Sigma : K)$ von $\Sigma : K$ abelsch.

Lemma 11

Falls K ein Körper mit Charakteristik Null und $L : K$ eine normale und radikale Erweiterung ist, dann ist $\Gamma(L : K)$ auflösbar.

Beweis Zuerst sei $L = K(\alpha_1, \cdots \alpha_n) =: K$ radikal. Wir nehmen oBdA an, dass wir nur Erweiterungen mit primen Wurzeln haben. Der Rest des Beweises folgt nun per Induktion nach der Anzahl der Erweiterungselemente n:

- $n = 0:$ $\Gamma(K:K) = \{\mathrm{id}\}$
- $n > 0:$ Sei $\alpha_1 \notin K(\alpha_2, \ldots, \alpha_n)$, denn sonst wäre nichts verändert...

Sei $\alpha_1^p \in K$ und f das Minimalpolynom zu α_1 mit $\mathrm{grad}(f) \geq 2$. Da $L:K$ normal ist, zerfällt dieses komplett in L. Da $\mathrm{char}(K) = 0$ gilt, ist f separabel und deshalb hat f keine mehrfachen Nullstellen, insbesondere existiert eine weitere von α_1 unterschiedliche Nullstelle β.
Setze $\varepsilon := \alpha_1/\beta$. Damit ist $\varepsilon \neq 1$ und $\varepsilon^p = 1$, da f von der Form $X^p - k$, $k \in K$ ist.
Damit sind die ε^k gerade die p-ten Einheitswurzeln, denn $\varepsilon^q \neq 1$ für $q < p$ aufgrund der Primheit von p. Die ε^k entstehen durch Körperoperationen aus α_1, β in L, damit zerfällt $X^p - 1$ in L.
Sei $M = K(\varepsilon)$ der Zerfällungskörper von $X^p - 1$. Wir haben folgende Inklusionskette:

$$K \subseteq M \subseteq M(\alpha_1) \subseteq L.$$

Für den Rest des Beweises halten wir uns an folgende Beweisidee:

L		
$\vert$	$\longleftarrow$	$\Gamma(L : M(\alpha_1))$ nach Induktion auflösbar.
$M(\alpha_1)$		
$\vert$	$\longleftarrow$	$\Gamma(M(\alpha_1) : M)$ abelsch nach Wiederholung(10)
M		
$\vert$	$\longleftarrow$	$\Gamma(M : K)$ abelsch nach Wiederholung(9)
K		

Nach Wiederholung(10) ist $M(\alpha_1)$ der Zerfällungskörper von $X^p - \alpha_1^p$, also ist $M(\alpha_1) : M$ normal und $\Gamma(M(\alpha_1) : M)$ abelsch. Nach Wiederholung(9) ist $\Gamma(M : K)$ abelsch.
Da mit $L : K$ auch $L : M$ endlich, separabel und normal ist (???), gilt der Hauptsatz und wir wissen:

$$\Gamma(M(\alpha_1) : M) \simeq \Gamma(L : M)/\Gamma(L : M(\alpha_1)).$$

Wegen $L = M(\alpha_1)(\alpha_2, \ldots, \alpha_n)$ ist $L : M(\alpha_1)$ radikal und normal (???) und von niedrigerem Grade, deshalb ist es nach Induktionsvoraussetzung auflösbar. Wieder liefert der Hauptsatz:

$$\Gamma(M : K) \simeq \Gamma(L : K)/\Gamma(L : M).$$

Damit ist $\Gamma(L : K)$ auflösbar, da es auch $\Gamma(L : M)$ und $\Gamma(M : K)$ sind. □

Satz 6

Sei K ein Körper mit $char(K) = 0$ und seien $M \supseteq L \supseteq K$ zugehörige Körpererweiterungen. Falls $M : K$ eine radikale Erweiterung ist, dann ist $L : K$ auflösbar.

Beweis Sei $K_0 = K^{*\dagger} = \{x \in L \mid \forall \gamma \in \Gamma(L : K) : \ \gamma(x) = x\} \supseteq K$ der Fixkörper der ganzen Gruppe $\Gamma(L : K)$, dann gilt allgemein:

$$K \subseteq K_0 \subseteq L.$$

Sei $N \supseteq M$ die normale Hülle von $M : K_0$. Wir haben folgende Inklusionskette:

$$K \subseteq K_0 \subseteq L \subseteq M \subseteq N.$$

Da mit $M : K$ auch $M : K_0$ radikal ist (K_0 ist Oberkörper, zur Not nehmen wir die gleiche radikale Sequenz), ist es nach Lemma(8) auch die normale Hülle $N : K_0$. Wegen obigem Lemma ist $\Gamma(N : K_0)$ deshalb auflösbar.
Da "$*\dagger$" ein Hüllenoperator ist, gilt:

$$K^{*\dagger *\dagger} = K_0^{*\dagger} = K_0.$$

Damit kann man Satz(4.10.14) auf $L : K_0$ anwenden; dieser besagt, dass $L : K_0$ wegen $K_0^{*\dagger} = K_0$ normal und separabel (und natürlich endlich) ist.
Der Hauptsatz (Teil 5) gilt für $N : K_0$, da nach $L : K_0$ auch die Radikal- M und die Normalerweiterung N separabel sind und damit $N : K_0$ normal, endlich, separabel ist. Er liefert:

$$\Gamma(L : K_0) \simeq \Gamma(N : K_0)/\ \Gamma(N : L).$$

Nach dem Abschnitt über auflösbare Gruppen ist $\Gamma(N : K_0)/\ \Gamma(N : L)$ auflösbar, da $\Gamma(N : K_0)$ auflösbar ist; damit ist es aber auch $\Gamma(L : K_0)$.
Nun ist zwar meist $K_0 \neq K$, aber es gilt:

$$\Gamma(L : K) = K_0^* = K^{*\dagger *} = K^* = \Gamma(L : K_0)$$

und damit ist auch $\Gamma(L : K)$ auflösbar. □

V) Ein unauflösbares Polynom vom Grade 5

Definition 12

Sei $f \in K[X]$ ein Polynom mit Zerfällungskörper Σ über K. Dann wird die Galois-Gruppe $\Gamma(\Sigma : K)$ auch **die Galois-Gruppe von** f genannt.

Lemma 13

Sei f ein irreduzibles Polynom mit Primzahlgrad über $\mathbb{Q}$. Falls f genau 2 imaginäre Nullstellen in $\mathbb{C}$ hat, dann ist die Galois-Gruppe von f über K die symmetrische Gruppe S_p.

Beweis Nach dem Fundamentalsatz der Algebra gilt $\mathbb{C} \supseteq \Sigma$, wobei Σ wieder den Zerfällungskörper von f darstellt. Sei Γ die Galois-Gruppe von f über $\mathbb{Q}$, also $\Gamma = \Gamma(\Sigma : \mathbb{Q})$, betrachtet als Permutationsgruppe der Nullstellen von f. Wegen Charakteristik Null sind die Nullstellen unterschiedlich (f war dann ja nach Satz(4.7.15) wegen seiner Irreduzibilität separabel), weshalb Γ eine Untergruppe von S_p ist, da ja p Elemente vertauscht werden.
Da das Minimalpolynom Grad p hat, so auch mindestens eine Nullstelle davon, weshalb $[\Sigma : \mathbb{Q}]$ nach dem Turmgesetz auf jeden Fall durch p teilbar ist.
Es gilt: $[\Sigma : \mathbb{Q}] = |\Gamma|$, deshalb teilt p damit auch die Ordnung der Galois-Gruppe Γ. Damit hat Γ ein Element der Ordnung p (siehe auch Wiederholungszettel des vorherigen Vortrages), die einzigen Elemente in S_p mit dieser Ordnung sind von der Bauart: $(12 \dots p)$.
Betrachte die komplexe Konjugation auf Σ, diese ist ein $\mathbb{Q}$-Automorphismus. Er läßt die $p-2$ rellen Nullstellen unberührt und weißt einer komplexen Nullstelle ihr konjugiertes zu. Dieses Phänomen dürfte allgemein bekannt sein.
Damit enthält Γ aber auch eine Transition (ab), oBdA sei dies (12). (Ansonsten potenziere $(12 \dots p)$ solange, bis a vorne steht und benenne um.)

Die Kombination der beiden Elemente erzeugt aber schon die ganze Gruppe S_p, deshalb ist $\Gamma = S_p$. □

Korollar 14

Das Polynom $f(X) = X^5 - 6X + 3 \in \mathbb{Q}[X]$ ist nicht durch Radikale lösbar.

Beweis Zu zeigen ist, dass die Galois-Gruppe von f nicht auflösbar ist. Da wir wissen, dass die S_5 nicht auflösbar ist, brauchen wir nach vorherigem Satz nur noch zu zeigen, dass

i) f irreduzibel und grad(f) prim ist.

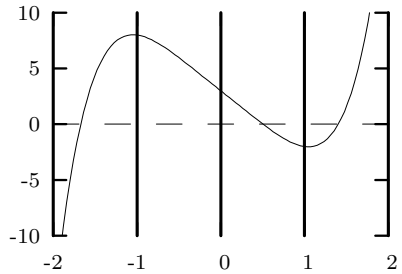
ii) f zwei komplexe Nullstellen hat.

Zur Irreduzibilität betrachten wir Eisensteins Kriterium mit $p = 3$. Die 3 teilt sowohl -6 als auch 3 und nicht den Leitkoeffizienten 1.
Ferner teilt 3^2 nicht den konstanten Term 3. Damit ist f irreduzibel über $\mathbb{Q}$ und hat die Funktionswerte:

x	-2	-1	0	1	2
$f(x)$	-17	8	3	-2	23.

Damit hat f mindestens wegen Stetigkeit mindestens 3 reelle Nullstellen; je mindestens eine in den Invervallen $(-2,-1)$, $(0,1)$ und $(1,2)$. Nach dem Satz von Rolle werden die Nullstellen von f durch die von Df getrennt.
Wegen

$$Df = (X^2 + \sqrt{5/6})(X^2 - \sqrt{5/6})$$



hat Df keine Nullstellen mit f gemein, weshalb keine der obigen drei reellen Nullstellen doppelt vorkommt. Damit hat f genau ein konjugiertes Paar komplexe Nullstellen. □

VI) Ausblick

Wir haben nun ein spezielles Polynom 5ten Grades vorgestellt, dass nicht durch Radikale lösbar ist. Allgemein kann man zeigen, dass ähnliche Resultate für die überwältigende Masse an Gleichungen 5ten und höheren Grades zutreffen: fast immer ist die zugehörige Galois-Gruppe die maximal mögliche S_n, die für $n > 4$ nicht mehr auflösbar ist. Es gilt sogar, dass der Qoutient von nicht auflösbaren Polynomen und allen Polynomen eines Grades M mit wachsendem M gegen 1 strebt.
Mit diesem Kapitel haben wir gleichzeitig auch die Idee widerlegt, dass es vielleicht für Polynome vom Grade M zwar keine allgemeine, aber vielleicht je nach „Muster“ des Polynoms unterschiedliche Löser durch Radikale gibt.
Eine möglicher Ausweg ist die Verallgemeinerung des Begriffes Radikal. Beispielsweise kann man Gleichungen 5ten Grades wieder allgemein faktorisieren, wenn man Radikal und Ultra-Radikale zuläßt, letztere entstehen aus der einzigen reellen Nullstelle von $X^5 + X - a$, a irgendeine reelle Zahl.

Literatur

[Stuart] Ian Stuart: Galois theory, Verlag Chapman & Hall/CRC