Algebra II. Galois Theorie.

I. Einleitung.

II. Galois Gruppe einer Körpererweiterung
Grundlegende Eigenschaften und
Beispiele.

III. Auflösbarkeit durch Radikale
und Auflösbare Gruppen.

IV. Galoiskorrespondenz und
Kreisteilungskörper.

I. Einleitung

Das motivierende Problem der Galois Theorie ist folgendes:

finde eine "Formel" für die Lösungen der Gleichung

$$x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

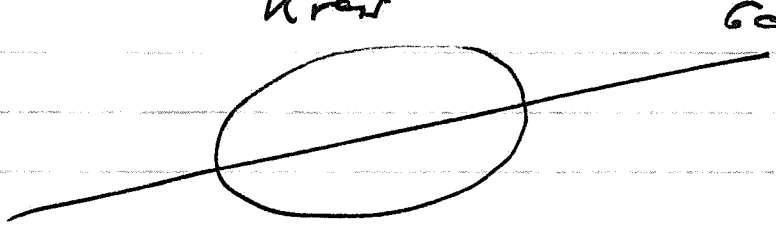
in "Funktion" von den Koeffizienten

$$a_{n-1}, \ldots, a_0.$$

Methoden für die Lösung von linearen und quadratischen Gleichungen waren in Spezialfällen babylonischen Mathematikern bekannt ~ 1700 BC.

Euklid (~ 300 BC) hat die Lösung von quadratischen Gleichungen auf ein geometrisches Problem zurückgeführt

z. B.



Erste systematische Behandlung der Auflösung von linearen und quadratischen Gleichungen geht auf den persischen Gelehrten al-Khwarizmi (780-850) in Bagdad zurück. Sein Buch (813-833) wurde im 12 Jahrhundert ins lateinische übersetzt und war im Mittelalter in den europäischen Universitäten die Standardreferenz. ~~Im Titel seines Buches~~

Er wird als Begründer der Algebra als autonome Disziplin angesehen; der Name kommt übrigens von "al-ǧabr" dass "Vervollständigen" bedeutet und im Titel seines Buches vorkommt.

Wesentliche Fortschritte wurden erst im 16 Jahrhundert erzielt mit der Lösung der Gleichung dritten Grades (Scipione del Ferro 1515) und vierten Grades (Ludovico Ferrari). Diese Methoden wurden im einflussreichen Buch "Ars Magna" in 1545 von Girolamo Cardano (1501-1576) präsentiert.

Hier eine kurze Darstellung der Lösungsmethode, weil sie historisch wichtig ist.

Sei $x^3 + ax^2 + bx + c = 0$

Durch die Substitution

$$z = x - \frac{a}{3}$$

erhält man eine Gleichung der Form:

$$z^3 + pz + q = 0$$

Die Idee ist jetzt $z = y + u$ zu setzen wobei man später u geeignet wählen kann.

Durch Substitution erhalten wir:

$$y^3 + \underbrace{3y^2u + 3yu^2}_{3yu(y+u)} + u^3 + p(y+u) + q = 0$$

Also

$$y^3 + (y+u)(3yu + p) + u^3 + q = 0.$$

Jetzt wählen wir u so dass

$$3yu + p = 0$$

d.h. $$u = -p/3y$$

und erhalten die Gleichung

$$y^3 - \left(\frac{p}{3}\right)^3 \frac{1}{y^3} + q = 0$$

d.h. $$\boxed{y^6 + q y^3 - \left(\frac{p}{3}\right)^3 = 0}$$

auch Resolvente genannt. Der Grund dafür ist, dass hier eine quadratische Gleichung in y^3 ist!

Also folgt:

$$y^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

$$u = -\frac{p}{3y}$$

und schlussendlich erhält man die Cardano. Formel:

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Wir haben hier den modernen algebraischen Formalismus benützt der von Franzos Viete (1540 - 1603) stammt; in "Ars Magna" waren alle diese Operationen in Wörtern beschrieben!

Descarte, Euler u.a. fanden alternative Methoden an für die Lösung von Gleichungen 4ten Grades.

Ein wesentlicher Schritt wurde von Joseph Louis Lagrange (1736-1813) gemacht. Er bemerkte folgendes:

Falls z_1, z_2, z_3 Lösungen sind von

$$z^3 + pz + q = 0$$

und $\omega = e^{2\pi i/3}$ eine primitive dritte Wurzel von 1 dann sind die 6 Lösungen der Resolventen

$$y^6 + qy^3 - \left(\frac{p}{3}\right)^3 = 0$$

gegeben durch

$$y_\sigma := \frac{1}{3}\left(z_{\sigma(1)} + \omega z_{\sigma(2)} + \omega^2 z_{\sigma(3)}\right)$$

Wobei σ die Menge der Permutationen von

3 Elementen durchläuft von denen es 6 gibt.
Seine fundamentale Einsicht war, dass

$$\left(z_{\sigma(1)} + \omega z_{\sigma(2)} + \omega^2 z_{\sigma(3)} \right)^3$$

nur 2 Werte annimmt.
Der Punkt hier ist, dass die klassische Lösungsmethode von Cardano in Verbindung mit ~~der~~ einer Permutationsgruppe gebracht wird.
Der nächste Schritt bezüglich Paolo Ruffini, Arzt und Professor für Mathematik in Modena. Sein Programm war zu zeigen dass die Gleichung 5. Grades im allgemeinen keine Lösung besitzt. Er untersuchte rationale Funktionen

$$f(z_1, \ldots, z_5)$$

wobei $\beta_1, \ldots, \beta_5$ Wurzeln der Gleichung

$$z^5 + \cdots + a_0 = 0$$

bezeichnen; er realisiert, dass die Menge der Permutationen $\sigma \in S_5$ die solch einen Ausdruck invariant lassen eine Untergruppe von S_5 bilden. In einer 1799 begonnenen Arbeit betrachtet er alle Untergruppen von S_5 und gibt einen (unvollständigen) Beweis, dass die allgemeine Gleichung 5. Grades keine "Lösung" besitzt. Es ist dann Niels Henrik Abels (1802-1829) der 1824 einen vollständigen Beweis publizierte.

Thm. (Abels-Ruffini)

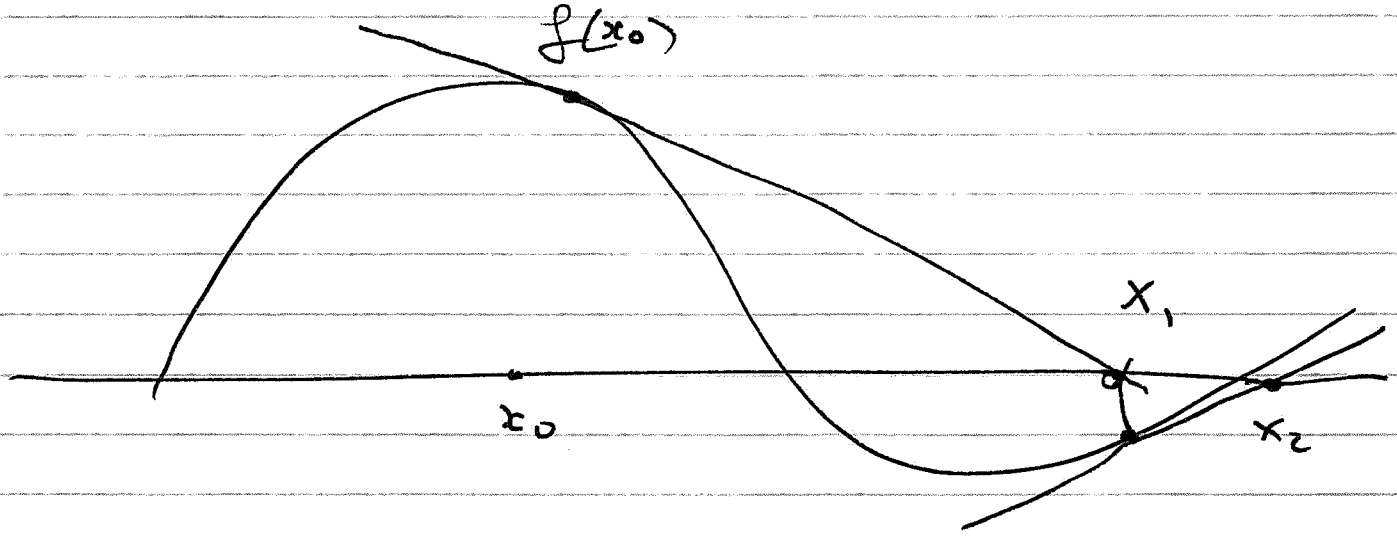
Die allgemeine Gleichung 5. Grades

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

ist mittels Radikalen nicht auflösbar.

Eine "Lösung mittels Radikalen" ist eine Formel die endlich viele arithmetische Operationen und Wurzelzeichen involviert.

Man weiss seit Newton, dass sich reelle Wurzeln von Polynomen approximieren lassen:



rekursiv: $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$

und $\lim_{n \to \infty} x_n$ ist eine Wurzel.

Der Satz von Abel-Ruffini ist unser erstes grosse Ziel. Wir werden diesen Satz als Korollar eines systematischen Aufbaus der Galoistheorie ~~erhalten~~ sowie der folgenden Tatsache von Algebra I:

Thm Die alternierende Gruppe A_5 ist einfach und nicht abelsch.

Wir werden jedem Polynome

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$$

wobei k ein Körper "mit guten Eigenschaften" bezeichnet eine Untergruppe

$$Gal(f) < S_n$$

zuordnen und zeigen:

Thm. (Galois) f ist genau dann mittels Radikalen auflösbar falls $Gal(f)$ eine auflösbare Gruppe ist.

II. Galoisgruppe einer Körpererweiterung.

Grundlegende Eigenschaften und Beispiele.

Sei E ein Körper. Die Menge $Aut(E)$ aller Körperautomorphismen ist eine Gruppe wobei das Produkt die Verkettung von Abbildungen ist. Sei $k \subset E$ ein Unterkörper, d.h. E ist eine Körpererweiterung von k. Dann ist

$$Gal(E/k) := \{\sigma \in Aut(E) : \sigma(x) = x \quad \forall x \in k\}$$

eine Untergruppe von $Aut(E)$.

Definition II-1 $Gal(E/k)$ ist die Galois-Gruppe der Erweiterung E/k.

Aus Algebra I wissen wir, dass E ein k-Vektorraum ist.

Übung II.2. Jedes $\sigma \in Gal(E/k)$ ist ein k-Vektorraum isomorphismus.

Übung II.3 Sei $k = \mathbb{R}$, $E = \mathbb{C}$, dann ist $Gal(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \sigma\}$ Wobei σ komplexe Konjugation bezeichnet.

Sei nun $f \in k[X]$ ein Polynom mit Koeffizienten in k und $E \supset k$ eine Körpererweiterung so dass f in $E[X]$ in lineare Faktoren zerfällt. Sei $R(f) \subset E$ die Menge der Wurzeln von f.

Lemma II.4 (Siehe Prop. 3.1) Jedes $\sigma \in Gal(E/k)$ induziert eine Permutation von $R(f)$.

Beweis: Sei $f(x) = a_n x^n + \dots + a_0 \in k[x]$

$\alpha \in R(f)$ und $\sigma \in Gal(E|k)$.

Dann folgt

$$0 = \sigma(f(\alpha)) = \sigma(a_n \alpha^n + \dots + a_0)$$

$$= a_n \sigma(\alpha)^n + \dots + a_0$$

$$= f(\sigma(\alpha))$$ woraus $\sigma(\alpha) \in R(f)$ folgt.

Also gilt $\sigma(R(f)) \subset R(f)$ und da

σ injektiv und $R(f)$ endlich ist, folgt

$$\sigma(R(f)) = R(f). \qquad \square$$

Sei $f \in k[x]$.

Def II.5: Die Galois Gruppe von f ist die Galois Gruppe $Gal(E|k)$ eines Zerfällungskörpers E von f.

Übung II.6 Zeige, dass wenn E und E' Zerfällungskörper von f sind, dann sind die Gruppen $Gal(E|k)$ und $Gal(E'|k)$ isomorph.

Sei X eine Menge; wir bezeichnen mit S_X die Gruppe der Bijektionen von X und falls $X = \{1, 2, \dots, n\}$, $n \in \mathbb{N}$ setzen wir $S_X = S_n$.

Lemma II.7 (Lemma 3.2 + Thm 3.3)

Sei $E|k$ ein Zerfällungskörper eines Polynoms $f \in k[X]$. Dann ist die Restriktionsabbildung

$$\begin{aligned} Gal(E|k) &\longrightarrow S_{R(f)} \\ \sigma &\longmapsto \sigma|_{R(f)} \end{aligned}$$

ein injektiver Gruppenhomomorphismus.