§3. Polynomiale Gleichungen

Dieses Kapitel erklärt eine weitere Anwendung der Galoistheorie, die hier in vollem Umfang gebraucht wird.

Problemstellung: Sei $f(x) \in K[x]$ ein Polynom. Gesucht sind Lösungen der Gleichung $f(x)=0$, durch eine allgemeine Formel, die die Lösungen aus den Koeffizienten von f in algebraischen Ausdrücken herleitet. Kann es solch eine allgemeine Formel geben?

Wir gehen Beispiele durch:

$\deg f = 0$: $f(x) = a$ $(a \in K)$, $f(x)=0$ hat für

$a \neq 0$ die Lösungsmenge ?

$a = 0$ die Lösungsmenge ?

$\deg f = 1$: $f(x) = ax+b$, $a \neq 0$, die Lösung von $f(x)=0$ ist durch eine Formel gegeben nämlich?

die die Lösung durch a und b ausdrückt

$\deg f = 2$: $f(x) = \underset{\neq 0}{a}x^2+bx+c$ hat die beiden Lösungen

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a},$$ falls $\sqrt{b^2-4ac}$ in K existiert,

also z.B. in $\mathbb{C}$, aber nicht immer in $\mathbb{R}$

$\rightsquigarrow$ eine Voraussetzung an den Körper K wird gebraucht

$\deg f = 3$: $f(x) = \underset{\neq 0}{a}x^3+bx^2+cx+d$, oder leicht vereinfacht $a=1$

$\rightsquigarrow f(x) = x^3+ax^2+bx+c$ (neue Notation

Substitution: $z := x + \frac{a}{3} \rightsquigarrow z^3+pz+q$

Cardanos Formel (1545) liefert eine Lösung

$z = u+v$ mit $u,v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\Delta}}$ mit $\Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$ falls char $K \neq 2,3$

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

ist eine Lösung, falls diese Ausdrücke in K existieren, z.B. in $\mathbb{C}$

In $\mathbb{C}$ erhält man zwei weitere Lösungen durch Multiplikation von z mit den Einheitswurzeln $\varepsilon = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$ und $\varepsilon^2 = -\frac{1}{2} - \frac{i}{2}\sqrt{3}$

Das wollen wir wirklich nicht nachprüfen, aber es ist jedenfalls eine allgemeine Formel, die die Koeffizienten von f benutzt, die Grundrechenarten und Wurzeln (und in K müssen die Ausdrücke definiert sein).

$\deg f = 4$: wieder gibt es eine Formel, mit $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$ usw, die z.B. in $\mathbb{C}$ funktioniert

$\deg f \geq 5$: es gibt Keine allgemeine Formel dieser Form.

Die Unmöglichkeit einer allgemeinen Formel ist eine Anwendung der Galois-Theorie.

Strategie: Wir modellieren die Situation durch Körpererweiterungen und übersetzen dann in Gruppentheorie.

Die Idee ist analog zum Vorgehen bei konstruierbaren Zahlen (Konstruktionen mit Zirkel und Lineal), aber die Ausführung ist schwieriger. Beim Delischen Problem z.B. haben wir in Algebra nur die Grade der Erweiterungen gebraucht, aber keine Eigenschaften der Galoisgruppen. erinnern Sie sich?

Vom Problem zu Körpererweiterungen: Wir beschränken uns auf Polynome $f(x) \in \mathbb{Q}[x]$ oder zumindest $f(x) \in K[x]$ mit $\mathbb{Q} \subset K$. D.h. char $K = 0$ und $K/\mathbb{Q}$ separabel.

In $\overline{K}$ (alg Abschluß) zerfällt $f(x)$ in ein Produkt von Linearfaktoren. Die Nullstellen $a_1, \ldots, a_n$ von $f(x)$ erzeugen eine Körpererweiterung

$K \subset K(a_1, \ldots, a_n) = L$, L ist der Zerfällungskörper wie war der Zerf. körper definiert?

$\Rightarrow$ L/K ist normal (und separabel)

$\Rightarrow$ L/K ist eine Galoiserweiterung.

Wir suchen nach einer Formel für die Nullstellen von $f(x)$. Die Koeffizienten von f liegen in K. Addieren, Multiplizieren liefert Ergebnisse in K, aber Wurzelziehen (möglich in $\overline{K}$) liefert Elemente in einer Körpererweiterung.

Die gesuchte Formel soll also die Nullstellen $a_1, \ldots, a_n$ (und damit den Körper L) aus K durch Körpererweiterungen herstellen, die schrittweise Wurzeln adjungieren. Also so etwas wie $\mathbb{Q} \subset \underbrace{\mathbb{Q}(\sqrt{b^2-4ac})}_{\substack{\shortparallel \\ \mathbb{Q}(\sqrt{d}) \text{ für } d = b^2-4ac \in \mathbb{Q}}} \ni \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$

Deshalb betrachten wir Körpererweiterungen wie $K(\sqrt[n]{a})$

3.1 Definition: Sei $\mathbb{Q} \subset K$, $n \in \mathbb{N}$, $a \in K$ und $E|K$ eine Körpererweiterung, sodaß $b \in E$ existiert mit $b^n = a$. Dann heißt b ein Radikal von a über K.
Bezeichnung: $b = \sqrt[n]{a}$. ↑ „radix" = Wurzel

(b ist nicht eindeutig, aber es ist eindeutig bis auf Multiplikation mit n-ten Einheitswurzeln was heißt das?)

(Fortsetzung der Definition:) Eine Körpererweiterung $L|K$ ist durch Radikale auflösbar :⇔ ∃ Kette $K_0 = K \subset K_1 \subset \dots \subset K_\ell$ (für ein $\ell \in \mathbb{N}$) von Körpererweiterungen mit $L \subset K_\ell$ und für jedes j ist $K_{j+1} = K_j(b_j)$ für ein Radikal $b_j = \sqrt[n_j]{a_j}$, wobei $a_j \in K_j$, $n_j \in \mathbb{N}$.

Ein Polynom $f(x) \in K[x]$ ist durch Radikale auflösbar :⇔ der Zerfällungskörper L von $f(x)$ ist über K durch Radikale auflösbar.

↑ d.h. man beginnt bei $K = K_0$, adjungiert endlich oft Radikale, bis man einen Körper K_ℓ erhält, in dem L enthalten ist.

↑ „enthalten" genügt: wir wollen Elemente von L als Ausdrücke in Wurzeln schreiben, mehr nicht

Was bedeutet das z.B. für Cardanos Formel:

wir beginnen etwa mit $\mathbb{Q} = K_0$

dann adjungieren wir $\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \rightsquigarrow \mathbb{Q}\Big(\overbrace{\sqrt{\underbrace{\left(\tfrac{q}{2}\right)^2 + \left(\tfrac{p}{3}\right)^3}_{\Delta}}}^{\text{ein Radikal}}\Big)$

und dann adjungieren wir $u = \underbrace{\sqrt[3]{-\frac{q}{2} \pm \sqrt{\Delta}}}_{\text{ein Radikal}}$

$\rightsquigarrow (\mathbb{Q}(\sqrt{\Delta}))(u)$

und dann noch v, auch ein Radikal, $\mathbb{Q}(\sqrt{\Delta})(u)(v) = K_\ell$,

Formel ⇒ die Lösungen liegen in K_ℓ

Uns interessiert $L|K$ eine Galois-Erweiterung, also müssen wir herausfinden, was Auflösbarkeit durch Radikale für die Galoisgruppe bedeutet.
Wir gehen in zwei Schritten vor: Erst adjungieren wir $\sqrt[n]{1}$ (also n-te Einheitswurzeln), danach $\sqrt[n]{a}$ unter der Annahme, daß die n-ten Einheitswurzeln bereits adjungiert wurden.

Sei $n \in \mathbb{N}$, K_n der Zerfällungskörper von $x^n - 1$ über K.
$\mathbb{Q} \subset K$, $\overline{\mathbb{Q}} \subset \overline{K} \subset \mathbb{C}$, die n-ten Einheitswurzeln $\sqrt[n]{1}$ sind die komplexen Zahlen $e^{\frac{2\pi j}{n} \cdot i}$ für $j = 1, \dots, n$

zeichnen Sie ein

$\sqrt[4]{1}$ $\sqrt[5]{1}$ $\sqrt[6]{1}$

3.2 Lemma: K_n / K ist eine Galoiserweiterung und es gibt einen injektiven Gruppenhomomorphismus $Gal(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$

$\cup$ Gruppe der multiplikativen Einheiten in $\mathbb{Z}/n\mathbb{Z}$

Das heißt: $Gal(K_n/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, insbesondere also eine abelsche Gruppe.

Beweis: $\operatorname{char} K = 0$, K_n Zerfällungskörper $\Rightarrow$ K_n/K Galoiserweiterung
$K_n = K(e^{2\pi i/n})$ warum? einfache Erweiterung $\Rightarrow$ $\sigma \in Gal(K_n/K)$,
$\sigma : K_n \to K_n$ ist bestimmt durch $e^{2\pi i/n} \mapsto \sigma(e^{2\pi i/n})$
$\uparrow$ Nullstelle desselben Minimalpolynoms
$\sigma^*(x^n - 1) = x^n - 1$ $\Rightarrow$ σ bildet Nullstellen von $x^n - 1$ wieder auf Nullstellen von $x^n - 1$ ab, also $\exists\, l \in \mathbb{Z}/n\mathbb{Z}$: $\sigma : e^{2\pi i/n} \mapsto e^{2\pi l i/n}$
Für ein weiteres $\tau \in Gal(K_n/K)$ analog: $e^{2\pi i/n} \xmapsto{\tau} e^{2\pi i m/n}$ für $m \in \mathbb{Z}/n\mathbb{Z}$
Berechne die Komposition $\tau \circ \sigma$:

$$e^{2\pi i/n} \xmapsto{\sigma} e^{2\pi l i/n} = (e^{2\pi i/n})^l \xmapsto[\text{Gruppen-homom}]{\tau} (\tau(e^{2\pi i/n}))^l = (e^{2\pi i m/n})^l = e^{2\pi i (ml)/n}$$

Das definiert eine Abbildung

$$Gal(K_n/K) \xrightarrow{\chi} \mathbb{Z}/n\mathbb{Z}$$
$$\sigma \longmapsto l$$
$$\tau \longmapsto m$$
$$\tau \circ \sigma \longmapsto ml$$
$$id \longmapsto 1$$
$$\sigma^{-1} \longmapsto l' \text{ mit } l \cdot l' = 1$$

diese Abbildung ist multiplikativ (aber $\mathbb{Z}/n\mathbb{Z}$ ist multiplikativ keine Gruppe, also ist χ ja kein Gruppenhomomorphismus!)

l ist invertierbar in $\mathbb{Z}/n\mathbb{Z}$ warum?
$\Rightarrow l \in (\mathbb{Z}/n\mathbb{Z})^*$, das ist eine Gruppe, also erhalten wir aus χ einen Gruppenhomomorphismus $Gal(K_n/K) \to (\mathbb{Z}/n\mathbb{Z})^*$, injektiv $\square$
warum?

$(\mathbb{Z}/n\mathbb{Z})^*$ ist eine abelsche Gruppe, deren Elemente repräsentiert sind von j mit $1 \le j \le n$ und $ggT(j,n)=1$ wie folgt das aus dem Euklidischen Algorithmus ?

Die Anzahl dieser Elemente, also $|(\mathbb{Z}/n\mathbb{Z})^*|$ wird mit $\varphi(n)$ bezeichnet. φ ist die Eulersche φ-Funktion.

Beispiele: $\varphi(p) = p-1$ warum?

$\varphi(4) = 2$ Repräsentanten?

$\varphi(9) = 6$ Repräsentanten?

Im nächsten Schritt verlangen wir, daß K die n-ten Einheitswurzeln enthält und adjungieren $\sqrt[n]{a}$ für ein $a \in K$. ¿ Kommt es hier auf eine Wahl an?

<u>3.3 Lemma:</u> Sei $e^{2\pi i/n} \in K$ und $L = K(\sqrt[n]{a})$ für ein $a \in K$. Dann ist L/K eine Galoiserweiterung und $Gal(L/K)$ ist zyklisch, wobei $ord(Gal(L/K))$ ein Teiler von n ist.

Beweis: $char K = 0 \Rightarrow L/K$ separabel

Die n Nullstellen von $x^n - a$ sind $\sqrt[n]{a}, \sqrt[n]{a}\cdot e^{2\pi i/n}, \sqrt[n]{a}\, e^{4\pi i/n}, \dots$ diese liegen alle in $L \Rightarrow L$ ist der Zerfällungskörper von x^n-a, also normal

$\Rightarrow L/K$ ist eine Galoiserweiterung

zz $Gal(L/K)$ ist zyklisch und die Ordnung teilt n

Wir versuchen die Idee des Beweises von 3.2 zu kopieren:

$\sigma \in Gal(L/K)$ bildet Nullstellen von x^n-a in Nullstellen ab, also

τ $\quad \sigma: \sqrt[n]{a} \longmapsto \sqrt[n]{a}\, e^{2\pi i/n \cdot \ell}$ für ein $\ell \in \mathbb{Z}/n\mathbb{Z}$

$\tau: \sqrt[n]{a} \longmapsto \sqrt[n]{a}\, e^{2\pi i/n \cdot m}$ für ein $m \in \mathbb{Z}/n\mathbb{Z}$

$e^{2\pi i/n} \overset{\tau,\sigma}{\longmapsto} e^{2\pi i/n}$, da $\in K$ $\Rightarrow \sigma, \tau$ sind durch das Bild von $\sqrt[n]{a}$ festgelegt

$\Rightarrow$ Injektive Abbildung $Gal(L/K) \to \mathbb{Z}/n\mathbb{Z}$

$\sigma \longmapsto \ell$

$\tau \longmapsto m$

Was passiert bei Verknüpfung?

$\tau \circ \sigma: \sqrt[n]{a} \overset{\sigma}{\longmapsto} \sqrt[n]{a}\cdot e^{2\pi i/n \cdot \ell} \overset{\tau}{\longmapsto} \tau(\sqrt[n]{a})\cdot e^{2\pi i/n \cdot \ell} = \sqrt[n]{a}\cdot e^{2\pi i/n \cdot m}\cdot e^{2\pi i n/\ell} =$

$= e^{2\pi i/n\,(\ell+m)}\cdot \sqrt[n]{a}$

$\rightarrow Gal(L/K) \to \mathbb{Z}/n\mathbb{Z}$

$\sigma \longmapsto \ell$

$\tau \longmapsto m$ $\quad$ additiver Gruppenhomomorphismus warum ist das anders als in 3.2

$\tau\circ\sigma \longmapsto \ell+m$

$\Rightarrow$ Gal$(L|K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$

$\Rightarrow$ $|$Gal$(L|K)|$ teilt $|\mathbb{Z}/n\mathbb{Z}| = n$ $\Rightarrow$ Gal$(L|K)$ ist zyklisch $\square$

nach welchem Satz? nach welchem Satz?

In 3.2 und in 3.3 haben wir jeweils eine abelsche Galoisgruppe gesehen. Was passiert, wenn wir solche Erweiterungen hintereinander ausführen?

Beispiel: $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $L :=$ Zerfällungskörper

$\mathbb{Q} \rightsquigarrow \mathbb{Q}(e^{2\pi i/3}) \rightsquigarrow \mathbb{Q}(e^{2\pi i/3})(\sqrt[3]{2})$

Nullstelle von $x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}_{\text{irreduzibel}}$ warum?

$\Rightarrow [\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q}] = 2 = \deg(x^2+x+1)$

$[L : \mathbb{Q}(e^{2\pi i/3})] = ?$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $\mathbb{Q}(\sqrt[3]{2}) \subset L \supset \mathbb{Q}(e^{2\pi i/3}) \Rightarrow 2 \mid [L:\mathbb{Q}]$

$\text{minpol}_{\sqrt[3]{2}}(x) \mid x^3 - 2$ und $3 \mid [L:\mathbb{Q}]$

$\Rightarrow [L:\mathbb{Q}] \leq 6 \Rightarrow [L:\mathbb{Q}] = 6$, $[L : \mathbb{Q}(e^{2\pi i/3})] = 3$

Gal$(L/\mathbb{Q}) \ni \sigma$: permutiert die Nullstellen von $x^3 - 2$

$\Rightarrow \sigma$ Permutation von drei Elementen

$\rightsquigarrow$ Gal$(L/\mathbb{Q}) \xrightarrow{\text{injektiv}} \Sigma_3$ $\overset{\text{warum?}}{\Rightarrow}$ Gal$(L/\mathbb{Q}) \simeq \Sigma_3$ - nicht abelsch!

$\sigma \longmapsto$ Permutation

Abelsch ist also nicht die gesuchte gruppentheoretische Eigenschaft. Abelsch bei jeder Adjunktion muß aber so etwas wie "stückweise abelsch" bedeuten. Das wird jetzt präzisiert:

<u>3.4 Definition:</u> Sei G eine Gruppe, $n \in \mathbb{N}_0$ und „ist die Eigenschaft "Untergruppe" transitiv?

$G_0 = \{id\} < G_1 < G_2 < \dots < G_n = G$ eine Kette von Untergruppen.

Diese Kette heißt <u>Normalreihe</u> $:\Leftrightarrow \forall j \in \{0, \dots, n-1\}: G_j \trianglelefteq G_{j+1}$

normal

Die Normalreihe heißt <u>abelsch</u> $:\Leftrightarrow$

$\forall j \in \{0, \dots, n-1\}: G_{j+1}/G_j$ ist abelsch

Die Gruppe G heißt <u>auflösbar</u> $:\Leftrightarrow$ G besitzt eine abelsche Normalreihe.

für uns ist dieser Name ein Programm!

Wir wollen die Auflösbarkeit von polynomialen Gleichungen durch Radikale in Verbindung bringen mit der Auflösbarkeit von Gruppen. Insbesondere wollen wir aus der Nicht-Auflösbarkeit bestimmter Gruppen ableiten, daß es für $n \geq 5$ keine allgemeine Formel für die Lösungen von Gleichungen vom Grad 5 gibt.

Beispiele auflösbarer Gruppen:

- abelsche Gruppen sind auflösbar
- Σ_3 ist auflösbar: $H = \langle (123) \rangle$ ist zyklisch
  $|H| = 3 = \frac{6}{2} \Rightarrow H \trianglelefteq G$ Details?
  $|G/H| = 2 \Rightarrow G/H$ abelsch
  $\Rightarrow \{1\} \trianglelefteq H \trianglelefteq G$ ist eine Normalreihe
- Sei p eine Primzahl, $|G| = p^n$ für ein $n \in \mathbb{N}$, d.h. G eine p-Gruppe. Dann ist G auflösbar. Beweis: $\underset{\text{Zentrum}}{Z(G)} \neq \{e\}$ (Algebra, Prop 3.8, eine Folgerung aus der Klassengleichung:
  G operiert auf $X = G$ durch Konjugation $\overset{\text{warum}}{\Rightarrow} |X^G| \equiv |X| \bmod p$
  $\Rightarrow p$ teilt $|X^G|$, $\underset{\neq\{e\}}{X^G \neq \emptyset}$, aber $X^G = Z(G)$ warum?)

  $Z(G)$ abelsch, $G/Z(G)$ ist auch eine p-Gruppe, weiter mit Induktion.
- G nicht abelsch, aber einfach $\Rightarrow$ G nicht auflösbar (solche Gruppen gibt es)
  d.h. nur $\{e\}$ und G sind Normalteiler

Wie testet man (Nicht-) Auflösbarkeit einer gegebenen Gruppe G, ohne alle Untergruppen durchzuprobieren?

<u>3.5 Definition:</u> Sei G eine Gruppe und $a, b \in G$. $[a,b] := aba^{-1}b^{-1} \in G$ heißt der <u>Kommutator</u> von a und b. Die von den Kommutatoren erzeugte Gruppe $D(G) := \langle [a,b] : a, b \in G \rangle := \bigcap\limits_{\substack{H < G \\ H \supset \{[a,b] : a,b \in G\}}} H$ heißt die <u>Kommutatoruntergruppe</u> oder abgeleitete (derivierte) Gruppe von G.

warum ist das eine Untergruppe?

Diese Untergruppen werden wir verwenden, um Normalreihen zu konstruieren, vor allem aber auch, um die Auflösbarkeit bei endlichen Gruppen zu charakterisieren. Damit finden wir dann auch nicht-auflösbare Gruppen.

Rechnungen mit Kommutatoren und mit $D(G)$:

$[a,b]=1_G \Leftrightarrow aba^{-1}b^{-1}=1_G \Leftrightarrow ab=ba \Leftrightarrow$ a und b kommutieren

Also: $D(G)=\{1_G\} \Leftrightarrow G$ abelsch $\Leftrightarrow Z(G)=G$.

$D(G)$ enthält nach Definition auch Produkte von Kommutatoren und Inverse von Kommutatoren:

$1_G=[1_G,1_G]$ ist ein Kommutator

$[a,b]\cdot[b,a] \overset{?}{=} \Rightarrow [a,b]=[b,a]^{-1}$, das Inverse ist also selbst ein Kommutator

$g[a,b]g^{-1} \overset{?}{=} [gag^{-1}, gbg^{-1}]$, Konjugierte von Kommutatoren sind Kommutatoren

$\Rightarrow D(G)$ ist eine normale Untergruppe von G: $D(G)\trianglelefteq G$

$\Rightarrow G/D(G)$ ist eine Gruppe mit induzierter Multiplikation,

für $\bar a,\bar b \in G/D(G)$ ist $[\bar a,\bar b]=\overline{[a,b]}$ warum?

$\Rightarrow [\bar a,\bar b]=1_{G/D(G)} \Rightarrow G/D(G)$ ist eine abelsche Gruppe

$\rightsquigarrow$ Also kann man versuchen, eine Normalreihe von oben nach unten aufzubauen:

$G \trianglerighteq D(G) \trianglerighteq D(D(G)) \trianglerighteq \dots$ Die Quotienten sind jeweils abelsch.

Falls $G \supsetneq D(G) \supsetneq D(D(G)) \supsetneq \dots$ (lauter echte Inklusionen) folgt für G endlich: $\exists n: D^n(G)=\{id\}$ und eine abelsche Normalreihe ist gefunden.

$$D^n(G) = \underbrace{D(\dots D(G)\dots)}_{n \text{ mal}}$$

Der Versuch scheitert, wenn $\exists e: D^e(G)=D^{e+1}(G)$. Das ist Pech, aber wir zeigen: Wenn wir scheitern, scheitern alle anderen auch.

3.6 Proposition: Eine endliche Gruppe G ist auflösbar genau dann, wenn es ein $n \in \mathbb{N}$ gibt mit $D^n(G) = \{1\}$.

Beweis: "$\Leftarrow$" ?

"$\Rightarrow$" Sei G auflösbar und $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ eine abelsche Normalreihe.

Wir zeigen mit Induktion nach i:

$$D^i(G) \subseteq G_{n-i} \quad \forall i$$

Daraus folgt dann $D^n(G) \subseteq G_0 = \{1\}$.

Induktionsanfang: $i=0$? ($D^0(G)$ ist nach Definition G selbst)

$i=1$: wir wollen $D^1(G) = D(G) \subseteq G_{n-1}$

$G_n / \underline{G_{n-1}}$ ist abelsch, also $\bar{a}\bar{b} = \bar{b}\bar{a}$ in G_n/G_{n-1} $\forall a,b \in G$

$\Rightarrow$ $\overline{[a,b]} = [\bar{a},\bar{b}] = \bar{1}$, also $[a,b] \in G_{n-1}$ $\forall a,b \in G$

$\Rightarrow$ $D(G) \subseteq G_{n-1}$

Induktionsschritt: Sei $D^i(G) \subseteq G_{n-i}$. Zu zeigen: $D^{i+1}(G) \subseteq G_{n-1-i}$.

$D^{i+1}(G)$ ist erzeugt von $\underset{\{[x,y]\,:\, x,y \in D^i(G)\}}{\underset{\shortparallel}{[D^i(G), D^i(G)]}} \subseteq [G_{n-i}, G_{n-i}] \underset{\substack{\uparrow \\ \text{warum?}}}{\subseteq} G_{n-i-1}$ D

Diese Charakterisierung können wir anwenden.

3.7 Proposition: Sei $n \geq 5$, Σ_n die symmetrische Gruppe und A_n die Untergruppe der geraden Permutationen. Dann ist $D(\Sigma_n) = D(A_n) = A_n$.

$\uparrow$ Bedeutung? Also sind Σ_n und A_n nicht auflösbar.

(A_n ist für $n \geq 5$ sogar einfach.)

Beweis: Aus linearer Algebra kennen wir das Vorzeichen von Permutationen

$$\mathrm{sgn}: \Sigma_n \mapsto \{\pm 1\}$$
$$\sigma \longmapsto (-1)^k, \quad k = \#\{\text{Fehlstände in } \sigma\} = |\{i<j : \sigma(i) > \sigma(j)\}|$$

und $A_n = \ker(\mathrm{sgn}) = \{\text{gerade Permutationen}\}$

A_n hat Index 2 in Σ_n $\Rightarrow$ $A_n \triangleleft \Sigma_n$ ist ein Normalteiler.

Σ_n ist erzeugt von Transpositionen $(a\,b)$, A_n ist erzeugt von Elementen der Form ~~(ab)o(cd)~~ $(a\,b) \circ (c\,d)$. Wir zeigen, daß diese Elemente Produkte von Kommutatoren sind. Dann folgt $A_n \subset D(A_n)$, also $A_n = D(A_n)$.

Bei $(ab)\circ(cd)$ sind Fälle zu unterscheiden:

$\{a,b\}=\{c,d\} \Rightarrow (ab)\circ(cd)=id$, Kommutator ✓

$\{a,b\}\cap\{c,d\}=\{a\}=\{c\} \Rightarrow (ab)\circ(cd)=(adb)$

$\{a,b\}\cap\{c,d\}=\emptyset \Rightarrow (ab)\circ(cd)=(acb)\circ(acd)$

} Produkte von 3-Zyklen

Deshalb zeigen wir: 3-Zyklen sind in A_n Kommutatoren. liegen 3-Zyklen überhaupt in A_n?

Dazu brauchen wir $n\geq 5$.

Sei (abc) ein 3-Zykel und d,e so daß $|\{a,b,c,d,e\}|=5$

Dann ist $(abc)=(abd)\circ(ace)\circ\underbrace{(abd)^{-1}}_{(adb)}\circ\underbrace{(ace)^{-1}}_{(aec)}$ ein Kommutator in A_n.

Damit ist $A_n=D(A_n)$ gezeigt.

Noch zu zeigen: $D(A_n)=D(\Sigma_n)$.

$A_n\subset\Sigma_n \Rightarrow D(A_n)\subset D(\Sigma_n)$. Umgekehrt: $sgn(ghg^{-1}h^{-1})=$

$=sgn(g)\cdot sgn(h)\cdot \underbrace{sgn(g^{-1})}_{sgn(g)}\cdot \underbrace{sgn(h^{-1})}_{sgn(h)} \Rightarrow ghg^{-1}h^{-1}$ ist gerade

warum

$\Rightarrow D(\Sigma_n)\subset A_n$. □

__3.8 Theorem__ (Abel, Galois): Sei L/K eine endliche Körpererweiterung und $char(K)=0$. Dann sind äquivalent:

(a) L/K ist durch Radikale auflösbar.

(b) Es existiert eine endliche Galoiserweiterung M/K mit $M\supset L$, so daß $Gal(M/K)$ auflösbar ist.

Wenn $f(x)\in K[x]$ und L der Zerfällungskörper von $f(x)$ ist, bedeutet das: Die Nullstellen können durch einen Ausdruck in Elementen von K und Wurzeln ausgedrückt werden genau dann, wenn die Galoisgruppe $Gal(L/K)$ auflösbar ist.

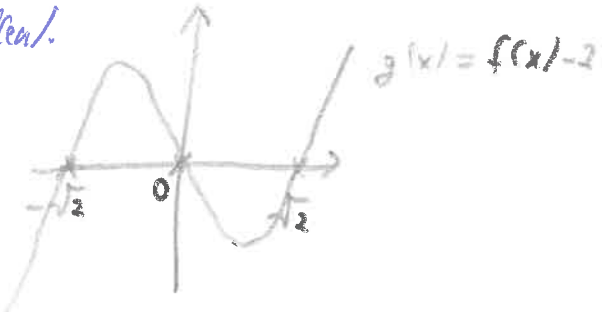
Da wir eigentlich die Unmöglichkeit einer allgemeinen Formel zeigen wollen, beweisen wir (a) ⇒ (b). Für die Gegenrichtung kann man z.B. eine Umkehrung von Lemma 3.3 zeigen. Einen Beweis von (b) ⇒ (a) finden Sie im Buch von Jantzen und Schwermer in VI, §4 und §5. Der Beweis ist nicht schwieriger als der von (a) ⇒ (b), aber noch technischer.

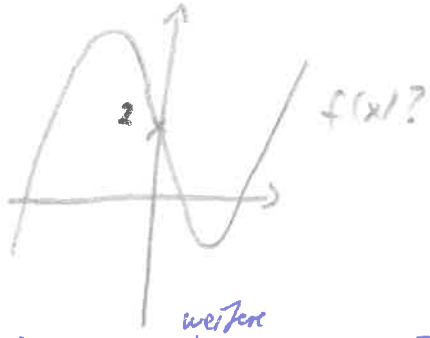
Vor dem Beweis die Anwendung. Gegeben sei $f(x) \in K[x]$ mit Zerfällungskörper L. M kennen wir nicht.
L ist als Zerfällungskörper normal und wegen $\mathrm{char}(K)=0$ auch separabel
$\Rightarrow L/K$ ist Galoiserweiterung, M/K auch (nach Voraussetzung) bzw Theorem
warum? $\Rightarrow \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K) \,/\, \mathrm{Gal}(M/L)$
$\mathrm{Gal}(M/K)$ ist auflösbar $\overset{(*)}{\underset{\text{noch zz}}{\Rightarrow}}$ $\mathrm{Gal}(L/K)$ ist auflösbar

Aus dem Theorem folgt also: Wenn die Gleichung $f(x)=0$ eine nicht-auflösbare Galoisgruppe hat, kann sie nicht durch Radikale auflösbar sein.

Wir müssen noch (*) nachprüfen. Allgemeiner:
G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler, $\bar{G} := G/N$ die Restklassengruppe
Dann gilt: G auflösbar $\Rightarrow \bar{G}$ auflösbar
Denn: $[\bar{g},\bar{h}] = \overline{[g,h]} \Rightarrow D^n(\bar{G}) = \{\bar{e}\}$ falls $D^n(G)=\{e\}$ Details?

Jetzt betrachten wir ein nicht auflösbares Polynom in $\mathbb{Q}[x]$.
Sei $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. $f(x)$ ist irreduzibel warum?
$g(x) := f(x) - 2 = x^5 - 4x = x(x^4-4) = x(x^2-2)(x^2+2)$ hat zumindest (sogar: genau) die drei Nullstellen 0, $\sqrt{2}$ und $-\sqrt{2}$ in $\mathbb{R}$ (und natürlich zwei weitere komplexe Nullstellen).





Hat $f(x)$ auch genau drei reelle Nullstellen (und zwei weitere komplexe)?
Wo liegen die lokalen Extrema? $f'(x) = 5x^4 - 4$, Nullstellen:
$5x^4 - 4 = 0 \Leftrightarrow x = \pm \sqrt[4]{\frac{4}{5}}$, abschätzen: $\underbrace{f(-\sqrt[4]{\tfrac{4}{5}})}_{\approx 5} > 0$, $\underbrace{f(\sqrt[4]{\tfrac{4}{5}})}_{\approx -1} < 0$
$\Rightarrow f$ hat auch drei reelle Nullstellen
(und zwei komplexe, die nicht reell sind)

Wir zeigen: f hat Galoisgruppe Σ_5, ist also nicht auflösbar.

3.9 Proposition: Sei $f(x) \in \mathbb{Q}[x]$ irreduzibel vom Grad 5, so daß $f(x)$ in $\mathbb{C}$ genau drei reelle Nullstellen hat. Dann ist die Galoisgruppe von f, das heißt die Galoisgruppe des Zerfällungskörpers von f nicht auflösbar.
Genauer: $Gal(f) \simeq \Sigma_5$.
Daraus folgt: f ist nicht durch Radikale auflösbar.

Im Beweis müssen wir die Galoisgruppe von f als Σ_5 entlarven. Dafür dient das folgende Lemma:
3.10 Lemma: Sei p eine Primzahl und G eine Untergruppe von Σ_p mit den beiden Eigenschaften: $p \mid ord(G)$ und

$\exists\, \tau$ Transposition in Σ_p mit $\tau \in G$.

Dann ist $G = \Sigma_p$.
Beweis: $p \mid ord(G) \Rightarrow \exists\, g \in G$ mit $ord(g) = p$. welche Sätze aus Algebra kann man hier verwenden?
Behauptung: g ist ein p-Zykel.
Beweis der Behauptung: Sei $X = \{1, \dots, p\}$. Σ_p operiert auf X durch Permutationen, $G < \Sigma_p$ also auch, und damit auch g als eine Permutation. Wir müssen zeigen, daß g auf X genau eine Bahn hat. (Warum ist das so??)
Angenommen $X = X_1 \dot\cup X_2$ (zwei nicht leere Mengen), so daß g die Menge X_1 in sich abbildet und die Menge X_2 in sich. Folglich: $\underbrace{g \text{ permutiert } X_1 \text{ und separat } X_2.}$
$X_1 \subsetneq X \Rightarrow |X_1| < p$, ebenso $|X_2| < p$.
d.h. $g = (g_1, g_2) \in \Sigma_{X_1} \times \Sigma_{X_2} \subset \Sigma_X = \Sigma_p$
$g_1 g_2 = g_2 g_1$
$ord(g_1) \mid ord(\Sigma_{X_1}) = |X_1|!$
$ord(g_2) \mid ord(\Sigma_{X_2}) = |X_2|!$
Aber $p \mid ord(g) = kgV(ord(g_1), ord(g_2)) \mid |X_1|! \cdot |X_2|!$ ↯ Details?
$\Rightarrow$ Behauptung
Es folgt: $X = \{1, g(1), g^2(1), \dots, g^{p-1}(1)\}$ und g ist ein p-Zyklus,
oBdA $g = (1\,2 \dots p) = (2\,3 \dots p\,1)$
Außerdem liegt in G die Transposition τ, oBdA $\tau = (1\,a)$ für ein $a \in \{2, \dots, p\}$

$g^{a-1} = (1\,a \ldots)$, das erzeugt $\langle g \rangle$, da p Primzahl ist.
Deshalb können wir g durch g^{a-1} ersetzen und erhalten (mit neuer Notation)

$g = (1\,2 \ldots p)$ und $\tau = (1\,2)$

$g: 1 \mapsto 2,\ g^2: 1 \mapsto 3, \ldots, g^{a-1}: 1 \mapsto a$

$\tau, g \in G \Rightarrow$ die folgenden Elemente liegen auch in G:

$g \circ \tau \circ g^{-1} = g \circ (1\,2) \circ g^{-1} = (2\,3)$

$g \circ (2\,3) \circ g^{-1} = (3\,4)$

usw $\Rightarrow \forall i: (i\ i{+}1) \in G$ Details nachrechnen!

Außerdem: $(1\,2) \circ (2\,3) \circ (1\,2) = (1\,3) \in G$

~~th~~ $(1\,3) \circ (3\,4) \circ (1\,3) = (1\,4) \in G$

$(i\,j) = (1\,i) \circ (1\,j) \circ (1\,i) \in G$

Also liegen alle Transpositionen in $G \xRightarrow{\text{Lin Algebra}} G = \Sigma_p$

(oder: $(x_1 x_2 \ldots x_m) = (x_1 x_m) \circ (x_1 x_{m-1}) \circ \ldots \circ (x_1 x_2) \in G$) $\square$

Zurück zur eigentlichen Aufgabe:

Beweis von Proposition 3.9: ~~z~~z $Gal(f) \simeq \Sigma_5$

f irreduzibel vom Grad 5, L Zerfällungskörper

$L/\mathbb{Q}$ separabel $\xRightarrow{\text{warum}}$ f hat 5 einfache Nullstellen $x_1, x_2, x_3 \in \mathbb{R} \setminus \mathbb{Q}$, $x_4, x_5 \in \mathbb{C} \setminus \mathbb{R}$

Wir betrachten die einfache Erweiterung $\mathbb{Q}(x_1) \subset L$, $\mathbb{Q}(x_1) \subset \mathbb{R}$

$m_{x_1}(x) = f(x)$, Grad $5 \Rightarrow [\mathbb{Q}(x_1):\mathbb{Q}] = 5$ und $5 \mid [L:\mathbb{Q}]$

$f(x) \in \mathbb{Q}[x] \Rightarrow f(x)$ fest unter komplexer Konjugation, also permutiert diese die Nullstellen von f warum? $x_1, x_2, x_3 \in \mathbb{R}$ bleiben fest, $x_4 \neq \overline{x_4} \Rightarrow x_5 = \overline{x_4}$

$\Rightarrow$ die Einschränkung der komplexen Konjugation ist ein $\mathbb{Q}$-Automorphismus von L, d.h. $\exists \tau \in Gal(L/\mathbb{Q})$, $\tau(x_4) = x_5$, $\tau(x_5) = x_4$, $\tau(x_1) = x_1$, $\tau(x_2) = x_2$, $\tau(x_3) = x_3$

Elemente in $Gal(L/\mathbb{Q})$ permutieren die Nullstellen von f und sind durch diese Permutation festgelegt, d.h. $Gal(L/\mathbb{Q}) \subset \Sigma_5$

$\tau \mapsto (4\,5)$, Transposition

und $5 \mid ord(Gal(L/\mathbb{Q}))$

$\xRightarrow{3.10}$ $Gal(L/\mathbb{Q}) = \Sigma_5$. $\square$

Der letzte Teil unserer Aufgabe ist der Beweis des Theorems.

Beweis von 3.8; (a) $\Rightarrow$ (b): Wir zeigen zuerst:

Behauptung: $\exists\, M' \supset L \supset K$, sodaß M'/K eine Galoiserweiterung ist und M' ist durch Radikale auflösbar

Nach Voraussetzung $\exists\, M \supset L \supset K$, wobei M durch iterierte Adjunktion von Radikalen ~~existiert~~ entsteht. Wegen char $K = 0$ ist M separabel, aber es ist vielleicht nicht normal. Wir können es natürlich zu einem Zerfällungskörper vergrößern, aber der ist dann vielleicht nicht auflösbar.

Induktion nach $[M:K]$. $[M:K] = 1$: nichts zu zeigen.

Sei $[M:K] > 1$. M ist durch iterierte Adjunktion von Radikalen entstanden, das heißt $\exists\, a_1, \ldots, a_l$: $M = K(a_1, \ldots, a_l) \supset K$, $a_1, \ldots, a_l$ die benötigten Radikale, in minimaler Anzahl gewählt $\Rightarrow M \supsetneq K(a_1, \ldots, a_{l-1}) = M_0$, $M = M_0(a_l)$

$[M_0:K] < [M:K] \Rightarrow$ Zu $M_0/K\ \exists\, M_0' \supset M_0$, M_0' normal und durch Radikale auflösbar.

$$\begin{array}{ccccc} ?\,M'\,? & \supset & M_0' & & \\ \cup & & \cup & & \\ M & \supset & M_0 & \supset & K \end{array}$$

a_l Radikal, d.h. $\exists\, m: a_l^m \in M_0$, m minimal, Abkürzung: $a := a_l$

Sei $f(x) := \prod_{\varphi \in Gal(M_0'/K)} (x^m - \varphi(a^m))$

Alle Nullstellen von f sind Radikale warum?

$\Rightarrow$ Der Zerfällungskörper von f ist eine Radikalerweiterung.

$f \in K[x]$, denn:

Für $\varphi \in Gal(M_0'/K)$ ist $\varphi^*(x^m - \overset{Gal(M_0'/K) \ni}{\psi}(a^m)) = x^m - \underbrace{(\varphi^*\psi)}_{\in Gal(M_0'/K)}(a^m)$, d.h. φ^* permutiert die Faktoren $\Rightarrow \varphi^* f(x) = f(x) \Rightarrow f(x) \in K[x]$

M_0' ist nach Induktionsannahme Zerfällungskörper eines Polynoms $g(x) \in K[x]$, dessen Nullstellen Radikale sind

Sei M' der Zerfällungskörper von $f \cdot g \in K[x]$, also $M' \supset M \supset L$ und alle Nullstellen sind Radikale.

Damit ist die Behauptung bewiesen. Und M' ist gewählt.

Zu zeigen ist: $Gal(M'/K)$ ist auflösbar.

Aus der Definition von M' erhalten wir eine Kette

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = M' \quad \text{mit } K_{j+1} = K_j(u_{j+1}),\ u_{j+1}^{m_{j+1}} \in K_j$$

Sei $m := \text{kgV}(m_1, \ldots, m_r)$ und ξ eine primitive m-te Einheitswurzel, z.B. $\xi := e^{2\pi i/m}$. Die Erweiterung $K_0 \subset K_0(\xi)$ ist nach 3.2 eine Galois-Erweiterung mit abelscher Galoisgruppe.

Sei $M'' := M'(\xi)$ $\rightsquigarrow$ erweiterte Kette: $K = K_0 \subset K_0(\xi) \subset K_1(\xi) \subset \ldots \subset K_r(\xi) = M''$

ξ überall enthalten $\Rightarrow$ an jeder Stelle sind auch die m_i-ten Einheitswurzeln enthalten $\Rightarrow$ 3.3 ist an jeder Stelle anwendbar.

Nach Konstruktion sind alle $K_j(\xi)$ normal und separabel

Hauptsatz der Galoistheorie $\rightsquigarrow$ normale Untergruppen von $\text{Gal}(M''/K)$ und die Quotienten $\text{Gal}(K_{j+1}(\xi)/K_j(\xi))$ sind nach 3.2 und 3.3 abelsch.

Folglich ist $\text{Gal}(M''/K)$ auflösbar. $\square$