9.19 Def: Eine Körpererweiterung $L \supset K$ heißt Radikalerweiterung, wenn es eine Kette von Zwischenkörpern $L = Z_m \supset Z_{m-1} \supset \dots \supset Z_0 = K$ gibt, sodass $Z_{i+1} = Z_i[b_i]$, wobei b_i eine Nullstelle eines reinen Polynoms über Z_i ist, also $\exists n_i$ sodass $b_i^{n_i} \in Z_i$; $X^{n_i}_{a=b_i^{n_i}} - a \in Z_i[x]$

Bem Sind $M \supset L$ und $L \supset K$ Radikalerweiterungen, dann ist auch $M \supset K$ Radikalerweiterung
Radikalerweiterungen brauchen nicht galoisch zu sein.
Es gilt jedoch

9.20 Satz Sei K Körper mit $\mathrm{char}(K) = 0$ und $L \supset K$ eine Radikalerweiterung. Dann gibt es eine Körpererweiterung $L' \subset L$ sodass $L' \supset K$ eine galoische Radikal-erweiterung ist.
~~L' entsteht aus L durch Adjunktion einer geeigneten n-ten Einheitswurzel.~~

Beweis: Induktion nach $[L:K]$
Im Fall $[L:K] = 1$ können wir $L' = L = K$ wählen.
Sei nun $[L:K] \geq 2$ und die Beh. für Radikalerweiterung kleinerer Grades schon gezeigt. Dann existiert ein Zwischenkörper $L \supset Z \supset K$, sodass $Z \supset K$ eine Radikalerweiterung ist und ~~$L = Z[b]$~~ $n \in \mathbb{N}$ und $b \in L$ mit $b^n \in Z$ und $L = Z[b]$
Nach Induktionsvoraussetzung existiert eine $Z' \supset Z$ so dass $Z' \supset K$ eine galoische Radikalerweiterung ist.
Als galoiserweiterung ist Z' Zerfällungskörper eines Polynoms $f \in K[x]$.
Wir setzen $G = \mathrm{Aut}(Z'; K)$ und betrachten

$$g = \prod_{\varphi \in G} (x^n - \varphi(b^n))$$

Die Koeffizienten von g sind invariant unter G, liegen also in K. Es sei L' der Zerfällungskörper von g über Z'. Da b eine Nullstelle von g ist können wir $L = Z(b)$ als Zwischenkörper von L' auffassen.

$L' \supset Z'$ L' ist also der Zerfällungskörper
$L \supset Z \supset K$ von $f \cdot g$ über K. Also
$L' \supset K$ ist galoisch. Da $Z' \supset K$ eine Radikalerweiterung reicht es $L' \supset Z$ ist Radikalerw. zu zeigen. Wegen der speziellen Gestalt von g ist jede Nullstelle von g eine n-te Wurzel eines Elements von Z'. Also $L' \supset Z'$ eine Radikalerweiterung. □

Frage: Wo haben wir $\mathrm{char}(K) = 0$ verwendet?
gf ist separabel gilt wg $\mathrm{char}(K) = 0$

5.21 Def Sei K ein Körper und $f \in K[x]$ ein nichtkonstantes Polynom. f heißt durch Radikale lösbar, wenn es eine Radikalerweiterung $L \supset K$ gibt über der f in Linearfaktoren zerfällt.

Bem Ist $\mathrm{char}(K) = 0$, $f \in K[x]$ irreduzibel und a eine Nullstelle von f, die in einer Radikalerweiterung $L \supset K$ liegt. Dann ist f schon durch Radikale lösbar.

Beweis Ist nämlich $L' \supset L \supset K$ eine galoissche Radikalerweiterung, die L umfasst, so sind sämtliche Nullstellen durch die Menge $\{\varphi(a) \mid \varphi \in \mathrm{Aut}(L'; K)\}$ definiert. In der Tat ist M ein Zerfällungskörper von f über L', dann gibt zu jeder Nullstelle β von f in M

einen Automorphismus $\varphi \in Aut(N;K)$ mit $\varphi(\alpha)=\beta$

Zerfällungskörper von f über K: $M \supset L$

Zerfällungskörper von f über K: $Z \supset K$

da wir ein Automorphismus $\varphi \in Aut(Z;K)$, der $\varphi(\alpha)=\beta$ erfüllt zu einem Automorphismus in $Aut(M;K)$ fortsetzen können. Da $M \supset L' \supset K$ galoisch gilt $\varphi(L')=L'$ $\forall \varphi \in Aut(N;K)$.
Es folgt $\varphi(\alpha) \in L'$ und daher $M=L'$ und $\varphi \in Aut(L';K)$ □

3.22 Satz Sei K ein Körper mit $char(K)=0$ und $f \in K[x]$ nicht konstant. Äquivalent sind
1) f ist durch Radikale lösbar
2) Die Galoisgruppe von f über K ist auflösbar.

Bemerkung Im Beweis verwenden wir die Charakterisierung von zyklischen Galoiserweiterungen als einfache Radikalerweiterung. Dazu brauchen wir Einheitswurzeln.

Bemerkung Sei $L \supset K$ eine Galoiserweiterung $char(K)=0$, $n \in \mathbb{N}$ und ζ eine primitive n-te Einheitswurzel. Dann sind auch $L_n = L[\zeta] \supset K$, $L_n \supset K_n = K[\zeta]$ und $L_n \supset K$ Galoiserweiterungen, denn $L \supset K$ ist Zerfällungskörper von einem Polynom f daher L_n Zerfällungskörper von $f \cdot (x^n-1)$ über K

Beweis des Satzes
1) ⇒ 2) Sei $L \supset K$ eine Radikalerweiterung über der f zerfällt. Den Zerfällungskörper Z von f können wir dann als Zwischenkörper $L \supset Z \supset K$ auffassen.
Nach Voraussetzung existiert eine Folge von Zwischenkörpern Z_i natürliche Zahlen n_i und $b_i \in Z_{i+1}$ mit $b_i^{n_i} \in Z_i$ und $Z_{i+1} = Z_i[b_i]$

E ---- galoisch ----
$\cap$
$L' \supset L \supset E_m \supset E_{m+1} \supset \dots \supset E_0 = K$,
$L' \supset L' \supset E_m' \supset E_{m-1}' \supset \dots \supset E_0' = K'$
Sei $n = n_0 \cdot \dots \cdot n_{m-1}$ und ζ eine primitive n-te Einheitswurzel im Erweiterungskörper von L. Es sei
$L' = L(\zeta)$, $E_i' = E_i(\zeta)$
Alle Inklusionen sind Galoiserweiterungen.
Da $E_{i+1}' = E_i'(b_i)$ und $b_i^{n_i} \in E_i'$ und E_i' eine n_i-te Primitive Einheitswurzel enthält sind die Gruppen $Aut(E_{i+1}', E_i')$ zyklisch.
Nach Satz 9.16
Nach dem Hauptsatz der Galoistheorie entspricht der Folge E_i' einer Folge von Untergruppen
$\{id\} \subset Aut(L', E_{m-1}') \subset \dots \subset Aut(L', E_0') \subset Aut(L'; K)$
sodass $Aut(L', E_i') / Aut(L'; E_{i+1}') \cong Aut(E_{i+1}', E_i')$
zyklisch ist für $i = 0, \dots, m-1$
und
$Aut(L', K) / Aut(L', E_0') \cong Aut(E_0'; K) = Aut(K'; K) \subset (\mathbb{Z}/n)^\times$
abelsch ist.
Also $Aut(L'; K)$ ist auflösbar
Nach Satz 3.6 ist die Quotientengruppe
$Gal(f) = Aut(E; K) = Aut(L'; K) / Aut(L'; E)$
ebenfalls auflösbar.
2) $\Rightarrow$ 1) Nach Voraussetzung gibt es eine Auflösung
$G_m = \{id\} \subset G_{m-1} \subset \dots \subset G_0 = G$
von der Galoisgruppe $G = Gal(f) = Aut(E; K)$.
mit zyklischen Faktoren.
Sei $n = |G|$ und ζ eine primitive n-te Einheitswurzel in einem Oberkörper von E.

Nach dem Hauptsatz der Galoistheorie entspricht
dies einer Folge von Zwischenkörpern

$$L = L_m \supset L_{m-1} \supset \dots \supset L_0 = K \quad \text{(Alles Galoiserweiterungen)}$$
$$\cap \qquad\qquad\qquad\qquad\qquad\qquad \cap$$
$$L' = L_m' \supset L_{m-1}' \supset \dots \supset L_0' = K', \quad \text{mit } L_i' = L_i[\vartheta].$$

Alle Inklusionen Galoiserw. z.B.

$$\begin{array}{ccc} L_i & \supset & L_{i-1} \\ \cap & & \cap \\ L_i[\vartheta] & \supset & L_{i-1}[\vartheta] \end{array}$$

Es gibt daher einen Epimorphismus

$$\mathrm{Aut}(L_i[\vartheta], L_{i-1}) \to \mathrm{Aut}(L_i, L_{i-1}),$$
$$\varphi \mapsto \varphi|_{L_i}$$

und daher wegen $\mathrm{Aut}(L_i[\vartheta], L_{i-1}[\vartheta]) \subset \mathrm{Aut}(L_i[\vartheta]; L_{i-1})$
ein Gruppenhomomorphismus.

$$\mathrm{Aut}(L_i[\vartheta], L_{i-1}[\vartheta]) \to \mathrm{Aut}(L_i, L_{i-1})$$

Dieser ist injektiv, denn ist φ ein Element des Kerns,
dann ist φ die Identität auf $L_{i-1}[\vartheta] \cup L_i$
also auf $L_i[\vartheta]$
Als Untergruppe der zyklischen Gruppe
$\mathrm{Aut}(L_i; L_{i-1})$ ist $\mathrm{Aut}(L_i[\vartheta], L_{i-1}[\vartheta])$,
ebenfalls zyklisch von einer Ordnung n_i, die n_i teilt
$L_{i-1}[\vartheta]$ enthält eine n_i-te primitive Einheitswurzel.
Nach der Charakterisierung von zyklischen Galoiserweiterungen
existiert ein $b_i \in L_i[\vartheta]$ mit $b_i^{n_i} \in L_{i-1}[\vartheta]$ und
$L_{i-1}[\vartheta][b_i] = L_i[\vartheta]$
$L' = L[\vartheta] \supset K$ ist also eine Radikalerweiterung über der
f zerfällt. □

Lsg 2 Grad $\mathrm{char}(K) = 0$
Dann lässt sich jedes Polynom vom Grad ≤ 4 durch
Radikale lösen.

Rem: Die Galoisgruppe ist eine Untergruppe von S_n, $n \leq 4$

$$S_4 \supset \underset{\mathbb{Z}/2}{A_4} \supset V_4 = \{(12)(34), (13)(24), (14)(23)\} \underset{\mathbb{Z}_2 \times \mathbb{Z}_2}{\supset} id$$
$$\cup$$
$$S_3 \supset A_3 \underset{\mathbb{Z}_2}{\supset} \{id\}$$
$$\cup$$
$$S_2 \supset \{id\}$$

Jede Untergruppe (und Quotientengruppe) von S_4 ist auflösbar nach Satz 3.6 □

Beispiel Das Polynom

$$f = x^5 - 4x + 2 \in \mathbb{Q}[x]$$

hat die Galoisgruppe S_5. Da S_5 nicht auflösbar ist, ist f nicht durch Radikale lösbar.

9.24 Satz A_n und S_n sind für $n \geq 5$ nicht auflösbar.

Beweis $[S_n, S_n] = A_n$ hat wir schon gesehen:

$[(12),(23)] = (12)(23)(12)(23) = (123)(123) = (132)$

ein 3-Zykel und A_n wird erzeugt von allen 3-Zykeln.

Wir zeigen $[A_n, A_n] = A_n$ für $n \geq 5$.

$[(123),(124)] \cdot [(123),(125)]$

$= (123)(124)(132)(142) \cdot [(123)(125)]$

$= (12)(34)(12)(35) = (354)$ ein 3 Zykel.

Da $[A_n, A_n] \subset A_n$ ein Normalteiler ist enthält $[A_n, A_n]$ alle 3 Zykel und daher alle ungeraden Zykeln

$(123)(345) = (12345)$ und wegen

$(123)(234) = (12)(34)$ alle geraden Produkte von disjunkten 2-Zykeln

Also $[A_n, A_n] = A_n$ □

9.25 Beispiel. Das Polynom

$$f = x^5 - 4x + 2$$

hat die Galoisgruppe S_5. ist also nicht auflösbar durch Radikale.

Beweis: f ist irreduzibel nach Eisenstein.
Also $5 \mid |Gal(f)|$. Nach den Sylowsätzen
gibt es eine Untergruppe der Ordnung 5 in der
Galoisgruppe. Nach durchnummerieren der Wurzeln
können wir bei geeigneter Nummerierung $Gal(f) \subset S_5$ also
enthält $Gal(f) \ni (12345)$
Da $f' = 5x^4 - 4$ zwei reelle Nullstellen hat $\pm \sqrt[4]{\frac{4}{5}}$
hat f höchstens zwei Extrema und daher höchstens
3 Nullstellen.
$f(-1) = 5 > 0$, $f(1) = -1 < 0$
$\Rightarrow$ f hat genau 3 reelle Nullstellen und ein Paar
konjugiert komplexer Nullstellen, komplexe Konjugation
vertauscht diese. Also $Gal(f)$ enthält auch eine
Transposition.
Bei geeigneter Nummerierung etwa $(12), (12345) \in Gal(f)$
da in einer der 4 Potenzen des 5 Zyklus 1 auf 2
abbildet.
Konjugation von (12) mit (12345) gibt $(23) \in Gal(f)$,
$(34), (45)$. Also
$\langle (12), (23), (34), (45) \rangle \leq Gal(f)$
$\| S_5$ □

§ 10 Das Zornsche Lemma und Anwendungen in der Algebra

10.1 Definition Eine partielle Ordnung $\leq$ auf einer
Menge M ist eine Relation, die
1) reflexiv $x \leq x$
2) antisymmetrisch $x \leq y, y \leq x \Rightarrow x = y$
3) transitiv $x \leq y, y \leq z \Rightarrow x \leq z$ erfüllt.

Man schreibt $x<y$ für $x\leq y$ und $x\neq y$

Eine Kette K ist eine Teilmenge von M in der je zwei Elemente vergleichbar sind, $x,y\in K \Rightarrow x\leq y$ oder $y\leq x$

Eine obere Schranke einer Kette K ist ein Element $z\in M$, sodass $x\leq z$ $\forall x\in K$ gilt.

Eine obere Grenze von K ist eine kleinste obere Schranke von K, d.h. obere Schranke z_0 für $z_0\leq z$ für alle oberen Schranken z von K.

Ein maximales Element von M ist ein Element z für das es kein $x\in M$ gibt $z<x$

10.2 Zornsches Lemma

Sei M eine nicht leere partiell geordnete Menge, in der jede Kette eine obere Schranke besitzt. Dann hat M ein maximales Element.

Eine typische Anwendung

10.3 Satz Sei R kommutativer Ring mit 1, $I\subsetneq R$. Dann existiert ein maximales Ideal $\mathfrak{M}\subsetneq R$ mit $I\subset\mathfrak{M}$

Beweis: Betrachte $M=\{J \mid I\subset J\subsetneq R$ ein Ideal$\}\neq\emptyset$, da $I\in M$. Sei $K\subset M$ eine Kette. Dann ist

$$\bigcup_{J\in K} J \text{ eine obere Schranke.}$$

In der Tat $\bigcup_{J\in K} J$ ist ein Ideal, $a_1,a_2\in\bigcup_{J\in K} J$

$\exists J_1,J_2$ mit $a_1\in J_1$, $a_2\in J_2$. Bei geeigneter Nummerierung $J_1\subset J_2 \Rightarrow a_1+a_2\in J_2\subset\bigcup_{J\in K} J$.

$\bigcup_{J\in K} J\subsetneq R$, da $1\notin J$ $\forall J\in K$

Nach dem Zornschen Lemma existiert ein maximales Element

$\mathfrak{M} \in M$. Wir zeigen m ist ein maximales Ideal.
Angenommen $a \in R \setminus m$. $\Rightarrow (a) + m \supsetneq m \Rightarrow (a) + m = R$
Also $\exists b \in R$ sodass $ab \equiv 1 \bmod \mathfrak{M}$. Also $\bar{a} \in R/m$ ist eine Einheit $\Rightarrow R/m$ ist ein Körper $\Rightarrow m$ ist max. Ideal □

Wir werden das Zornsche Lemma aus dem Auswahlaxiom herleiten.

10.4 Auswahlaxiom Sei $(M_i)_{i \in I}$ eine Familie von nicht leeren Mengen, $M = \bigcup_{i \in I} M_i$. Dann gibt es eine Abbildung $f: I \to M$ mit $f(i) \in M_i \; \forall i \in I$. (eine Auswahlfunktion). Mit anderen Worten

$$\prod_{i \in I} M_i \neq \emptyset$$

Angenommen es gibt kein maximales Element in M. Dann sind die Mengen $M_x = \{y \in M \mid x < y\}$ alle nicht leer.
Das Auswahlaxiom liefert eine Abbildung $f: M \to M$ mit $x < f(x) \; \forall x \in M$

10.5 Def Eine partiell geordnete Menge M heißt strikt induktiv geordnet, wenn jede Kette in M eine obere Grenze hat.
Bem: Strikt induktiv geordnete Mengen sind nicht leer. Die obere Grenze z der leeren Menge $\emptyset \subset M$ ist dann das kleinste Element von M.

10.6 Satz Sei M eine strikt induktiv geordnete Menge und $f: M \to M$ eine Abbildung mit $x \leq f(x) \; \forall x \in M$
Dann hat f einen Fixpunkt.
Den Beweis führen wir in mehreren Schritten und führen einige nur im Beweis verwendete Begriffe ein.
Bew: Eine Teilmenge $N \subset M$ heißt zulässig, wenn mit jeder Kette K in N die obere Grenze von K in M

ebenfalls in N liegt und außerdem $f(N) \subset N$.
Da Durchschnitte von zulässigen Mengen zulässig sind, können wir M durch diesen Durchschnitt ersetzen und im Folgenden Annehmen, dass M die einzige zulässige Teilmenge von M ist.
Unsere Strategie ist zu zeigen, dass dann M selbst eine Kette ist.
Ein Punkt $x \in M$ heißt Trennpunkt, wenn $\forall y \in M$ mit $y < x$, $f(y) \leq x$ gilt.

HS 1 Sei $x \in M$ ein Trennpunkt $\forall y \in M$ gilt dann $y < x$ oder $f(x) \leq y$.
Insbesondere sind Trennpunkte mit allen Elementen von M vergleichbar

Beweis: Sei $P = \{y \in M \mid y \leq x \text{ oder } f(x) \leq y\}$
Es reicht zu zeigen, dass P zulässig ist
Sei $K \subset P$ eine Kette und z die obere Grenze von K in M.
Ist x eine obere Schranke von K in M dann ist $z \leq x$ also $z \in P$.
Ist x keine obere Schranke, dann gibt es ein $y \in K$ sodass $y \leq x$ nicht gilt, also $f(x) \leq y$ gilt.
~~Da x ein Trennpunkt ist gilt dann $x < y \leq f(y)$ also~~
Also $f(x) \leq y \leq z$ und daher $z \in P$ ebenfalls.
Bleibt noch $f(P) \subset P$ zu zeigen.
Sei $y \in P$. Bei $y < x \Rightarrow f(y) \leq x$ also $f(y \in P)$
Bei $y = x$ $f(y) = f(x) \geq f(x)$ also $f(y) \in P$
Schließlich bei $x < y \Rightarrow f(x) \leq y \leq f(y)$, $f(y) \in P$
Also $P = M$ und x ist mit allen Elementen vergleichbar
da $x \leq f(x) \leq y$ oder $y \leq x$ erfüllt ist $\square$

HS2 Jedes Element von M ist ein Trennpunkt.

Bew: Es reicht zu zeigen, dass die Menge Q der Trennpunkte von M zulässig ist.

Sei K eine Kette in Q und z die obere Grenze von K in M.

Wir müssen zeigen, dass z ein Trennpunkt ist.

Sei $y \in M$ mit $y < z$ vorgegeben.

Da y keine obere Schranke von K ist gibt es ein $x \in K$, so dass $x \leq y$ nicht gilt. Da x ein Trennpunkt ist, gilt dann $y < x$ und daher $f(y) \leq x \leq z$ z ist also ein Trennpunkt.

Es bleibt $f(Q) \subset Q$ zu zeigen.

Sei $x \in Q$ vorgegeben. Wir müssen zeigen, dass $F(x)$ ebenfalls ein Trennpunkt ist. Sei $y < F(x)$ vorgegeben. Dann gilt $y \leq x$ nach HS 1 also $f(y) \leq x \leq F(x)$

Bei $y = x$ folgt $f(y) = F(x) \leq f(x)$. Also $F(x) \in Q$ □

Nach HS 1 & HS 2 ist M eine Kette. Sei z die obere Grenze von M. Dann gilt:

$z \leq f(z) \leq z$ also z ist ein Fixpunkt von f.

Damit ist Satz 10.6 bewiesen