14. Algebraisch abgeschlossene Körper

Ziel:

Konstruktion einer kleinsten algebraisch abgeschlossenen Körpererweiterung $\bar{K}$ des Körpers K und Eindeutigkeit von $\bar{K}$ bis auf K-Isomorphie.

14.1. Definition:

Ein Körper K heißt algebraisch abgeschlossen, wenn gilt:

i. Jedes Polynom $f \in K[X]$ vom Grad $d \geqslant 1$ hat mindestens eine Nullstelle α in K.

   oder äquivalent dazu:

ii. Jedes $f \in K[X]$ vom Grad $d \geqslant 1$ zerfällt in $K[X]$ vollständig in Linearfaktoren.

14.2. Definition:

Die Körpererweiterung $\bar{K}$ des Körpers K heißt algebraischer Abschluss von K, wenn eine der äquivalenten Bedingungen erfüllt ist: [1]

i. $\bar{K}|K$ ist algebraisch und $\bar{K}$ ist algebraisch abgeschlossen

ii. $\bar{K}|K$ ist algebraisch und $\bar{K}$ ist maximal mit dieser Eigenschaft

   (Mit anderen Worten: Ist $K \subset \bar{K} \subset L$, $L|K$ algebraisch, so ist $\bar{K} = L$)

iii. $\bar{K}$ ist algebraisch abgeschlossen und minimale Erweiterung von K mit dieser Eigenschaft

   (Mit anderen Worten: Ist $K \subset L \subset \bar{K}$, L algebraisch abgeschlossen, so ist $L = \bar{K}$)

Beweis.

Übung! □

14.3. Lemma:

R sei ein Ring (kommutativ) und $\mathfrak{a} \subsetneq R$ ein Ideal:

Dann existiert ein maximales Ideal $\mathfrak{m}$ von R mit $\mathfrak{a} \subset \mathfrak{m} \subsetneq R$.

Erinnerung:

Lemma von Zorn:

Ist $(\Sigma, \prec)$ eine nichtleere, induktiv geordnete Menge, so besitzt Σ maximale Elemente.

1. Vergleiche hierzu die Definition einer Basis eines Vektorraums: (maximale linear unabhängige Menge, minimales Erzeugendensystem, oder linear unabhängiges Erzeugendensystem)

induktiv geordnet: Jede vollständig geordnete Teilmenge von Σ besitzt in Σ eine obere Schranke.

Beweis.

Sei $\Sigma := \{\mathfrak{b} \,|\, \mathfrak{b} \text{ ist Ideal von } R \text{ und } \mathfrak{a} \subset \mathfrak{b} \subsetneq R\}$

- geordnet durch Inklusion
- nichtleer, da $\mathfrak{a} \in \Sigma$
- induktiv geordnet:

  Ist $\{\mathfrak{b}_i | i \in I\}$ eine vollständig geordnete Teilmenge von Σ, so ist $\mathfrak{b} := \bigcup\limits_{i \in I} \mathfrak{b}_i$ ein Ideal mit $\mathfrak{b} \supset \mathfrak{a}$ und $\mathfrak{b} \neq R$ (sonst $1 \in \mathfrak{b}_i$ für ein i, also $\mathfrak{b}_i = R$ *Widerspruch*).

Nach dem Lemma von Zorn existiert $\mathfrak{m}$ wie verlangt.

□

14.4. Definition:

Es sei S eine beliebige nichtleere Indexmenge und für jedes $s \in S$ sei X_s eine Unbestimmte.

Setze:

$$K[X_s \mid s \in S]$$

für den Polynomring in S Variablen X_s. Dies ist ein kommutativer, nullteilerfreier Ring.

Beispiel:

$$\begin{array}{lll} S = \{1\} & X_1 = X & , K[X_s \mid s \in S] = K[X] \\ S = \{1, 2, \ldots, n\} & & , K[X_s \mid s \in S] = K[X_1, X_2, \ldots, X_n] \\ S = \mathbb{N} & & , K[X_s \mid s \in S] = K[X_1, X_2, \ldots] \\ S \text{ allgemein} & & , K[X_s \mid s \in S] = \bigcup\limits_{\substack{S' \subset S \\ \text{endlich}}} K[X_s \mid s \in S'] \end{array}$$

14.5. Satz:

Zu jedem Körper K existiert ein algebraischer Abschluss.

Beweis.

i. Wir konstruieren:

   - zu K eine algebraische Erweiterung K_1, so dass alle nichtkonstanten Polynome $f \in K[X]$ über K_1 eine Nullstelle bekommen.

- zu K_1 eine algebraische Erweiterung K_2, so dass alle nichtkonstanten Polynome $f \in K_1[X]$ über K_2 eine Nullstelle bekommen.
- $\vdots$
- zu K_i eine algebraische Erweiterung K_{i+1}, so dass alle nichtkonstanten Polynome $f \in K_i[X]$ über K_{i+1} eine Nullstelle bekommen.
  $(i \in \mathbb{N})$

Dann ist:

- $K_i|K$ algebraisch $\forall i \in \mathbb{N}$
- $\bar{K} := \bigcup_{i \in \mathbb{N}} K_i$ ist Körpererweiterung von K, algebraisch und jedes $f \in \bar{K}[X]$ mit $\deg f \geqslant 1$ hat in $\bar{K}$ eine Nullstelle.

Also ist dieses $\bar{K}$ der gesuchte algebraische Abschluss von K.

Bleibt also die Konstruktion K_1 zu K zu zeigen.

(Diese muss universell sein, d.h. anwendbar auf jeden Körper K)

ii. Konstruktion dieses $K_1|K$:

Sei $S := \{f \in K[X] \,|\, d(f) \geqslant 1, f \text{ normiert}\}$.

Für jedes $f \in S$ sei X_f eine Unbestimmte. Setze:

$$R := K[X_f \mid f \in S]$$

und $\mathfrak{a} \subset R$ sei das Ideal, das von allen $f(X_f)$ $(f \in S)$ erzeugt wird.

iii. Es ist $\mathfrak{a} \subsetneq R$.

Annahme: $\mathfrak{a} = R$. Dann ist $1 \in \mathfrak{a}$.

$$(\star) \quad 1 = \sum_{1 \leqslant i \leqslant n} g_i \, f_i(X_{f_i})$$

Für jedes $i = 1, 2, \ldots, n$ sei:

$$S_i := \{s \in S \,|\, X_s \, \text{kommt in} \, g_i \, \text{vor}\}, \quad \#S_i < \infty$$

Weiter sei

$$T := \bigcup_{1 \leqslant i \leqslant n} S_i \cup \{f_i \,|\, 1 \leqslant i \leqslant n\}, \quad \#T < \infty$$

und $L|K$ eine $\underset{\text{endliche}}{\text{algebraische}}$ Körpererweiterung, über der jedes der f_i eine Nullstelle α_i besitzt (13.2.).

Setze jetzt für alle $s \in T$ in $(\star)$ Werte für die Variablen X_s ein:

$$\begin{array}{lll} s = f_i\colon & X_{f_i} & \rightsquigarrow \alpha_i \\ s \neq f_i\colon & X_s & \rightsquigarrow 0 \end{array}$$

In L gilt dann:

$$1 = \sum_i g_i(\ldots)\, \underbrace{f_i(\alpha_i)}_{=0} = 0 \quad \textit{Widerspruch!}$$

Also ist $\mathfrak{a} \subsetneq R$.

iv. Sei jetzt $\mathfrak{m}$ ein maximales Ideal oberhalb von $\mathfrak{a}$, d.h. $\mathfrak{a} \subset \mathfrak{m} \subsetneq R$. (14.3.)

Dann ist $K_1 := R/\mathfrak{m}$ ein Körper, der K enthält durch [2]

$$K \hookrightarrow R = K[X_f \mid f \in S] \longrightarrow R/\mathfrak{m} =: K_1$$

Da R über K von den X_f erzeugt wird, wird K_1 über K von

$\underset{\in K_1}{\alpha_f} :=$ Restklasse von X_f modulo $\mathfrak{m}$ erzeugt.

Es gilt: $f(\alpha_f) \equiv f(X_f) \equiv 0 (\text{modulo } \mathfrak{m})$. Damit ist $K_1|K$ algebraisch, und $K_1|K$ hat die benötigte Nullstelleneigenschaft.

□

14.6. Situation:

K Körper, $\bar{K}$ ein algebraischer Abschluss, $L|K$ eine einfache algebraische Erweiterung von K, $L = K(\alpha)$, $m(X) = m_{K,f}(X)$. Betrachte K-Einbettungen von L in $\bar{K}$, d.h. Ringhomomorphismen:

$$\begin{tikzcd} \sigma\colon L \arrow[rr] & & \bar{K} \\ & K \arrow[ul, hook] \arrow[ur, hook] \arrow[u, phantom, "\bigcirc"] & \end{tikzcd} \qquad \text{mit } \sigma|_K = \mathrm{id}_K$$

Es ist

$$K[X]/(m) \overset{X \longmapsto \alpha}{\xrightarrow{\cong}} L \qquad \text{(Isomorphiesatz)}$$

Da $\bar{K}$ algebraisch abgeschlossen ist, $\exists$ Nullstelle β von m in $\bar{K}$. Der Ringhomomorphismus

$$\begin{tikzcd} \tilde{\sigma}\colon K[X] \arrow[r, "X \longmapsto \beta"] \arrow[d] & \bar{K} & \\ K[X]/(m) \arrow[ur, hook] \arrow[rr, "\cong", "X \longmapsto \alpha"'] & & K(\alpha) = L \arrow[ul, "\sigma"'] \end{tikzcd}$$

hat Kern (m) und faktorisiert also über $L = K(\alpha)$, d.h. $\exists! \sigma$ wie oben. D.h. σ ist eine K-Einbettung von L in $\bar{K}$, die durch die Wahl der Nullstelle $\beta \in \bar{K}$ von m wohlbestimmt ist.

2. Die Hintereinanderausführung von Ringhomomorphismen ist wieder ein Ringhomomorphismus. Ein Homomorphismus von einem Körper in einen Ring ist injektiv $\rightsquigarrow$ „Einbettung“.

Damit ist bewiesen:

14.7. Proposition:

Sei $L|K$ einfach, $L = K(\alpha)$, $m = m_{K,\alpha}$ das Minimalpoynom. $\bar{K}|K$ ein algebraischer Abschluss. Dann $\exists K$-Einbettungen σ: $L \hookrightarrow \bar{K}$. Sie entsprechen eineindeutig den Nullstellen β von m in $\bar{K}$.

□

14.8. Satz:

K Körper, $\bar{K}|K$ algebraischer Abschluss, $L|K$ algebraische Erweiterung. Dann

i. $\exists K$-Einbettung $\sigma: L \longrightarrow \bar{K}$;

ii. ist auch L algebraisch abgeschlossen, so ist jedes σ wie in (i) ein K-Isomorphismus.

Beweis.

i. ist gezeigt, falls $L = K(\alpha)$ ist. Daraus erhält man (i) auch für L von der Form

   $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, schließlich für L von der Form $L = K(\alpha_1, \alpha_2, \ldots, \alpha_i \,|\, i \in \mathbb{N})$

   Allgemeiner Fall:

   Anwendung des Lemmas von Zorn. Setze:

$$S := \left\{ (M, \tau) \,\middle|\, \begin{array}{c} M \text{ ist Zwischenerweiterung von } L|K \\ K \subset M \subset L \\ \text{und } \tau: M \longrightarrow \bar{K} \text{ ist eine } K\text{-Einbettung} \end{array} \right\}$$

   S ist

   - geordnet bzgl. „$\prec$“,

$$(M, \tau) \prec (M', \tau') :\Leftrightarrow M \subset M', \tau'|_M = \tau$$

   - nichtleer (alle endlich erzeugten $M|K$ gehören zusammen mit ihren $\tau's$ zu S)

   - S ist induktiv geordnet[3] (!)

   Deshalb $\exists$ maximales Element (M, τ) in S, und es muss $M = L$ sein.

ii. Sei L algebraisch abgeschlossen, $\sigma: L \longrightarrow K$ eine K-Einbettung.

   Zu zeigen ist: σ ist surjektiv.

   Sei $\beta \in \bar{K}$, $f = m_{K,\beta} \in K[X]$, β_i $(i = 1, \ldots, n)$ die Nullstellen von f in $\bar{K}$, $\beta = \beta_1$. Weil auch L algebraisch abgeschlossen ist, zerfällt f in $L[X]$ in Linearfaktoren,

3. Man beachte, dass die (M_i, τ_i) eine aufsteigende Kette von Körpern bilden. Wobei für zwei solcher, (M_i, τ_i), (M_j, τ_j) gilt: $(M_i, \tau_i) \prec (M_j, \tau_j)$ oder $(M_i, \tau_i) \succ (M_j, \tau_j)$. $\rightsquigarrow \bigcup_{i \in I} (M_i, \tau_i)$ ist auch Körper und ist eine obere Schranke für die (M_i, τ_i). Also ist „$\prec$“ induktiv geordnet.

$f(X) = \prod_{1 \leqslant i \leqslant n} (X - \alpha_i)$.

Setze:

$$\begin{array}{rcl} L' & := & K(\alpha_1, \alpha_2, ..., \alpha_n) \subset L \\ K' & := & K(\beta_1, \beta_2, ..., \beta_n) \subset \bar{K} \end{array}$$

$$\begin{tikzcd} L \arrow[r, "\sigma"] \arrow[d, no head] & \bar{K} \arrow[d, no head] \\ L' \arrow[r] \arrow[dr, no head] & K' \arrow[d, no head] \\ & K \end{tikzcd}$$

Es gilt: $\sigma(L') \subset K'$ und es muss $\sigma(L') = K'$ gelten.

(!)

(!!)

Insbesondere ist $\beta \in \sigma(L)$, d.h. σ surjektiv.

□

Beispiel:

$K = \mathbb{Q}$, $\quad f(X) = X^3 - 2$, $\qquad N = N_{\mathbb{Q},f}$, $\qquad Z = Z_{\mathbb{Q},f}$.

$[Z : \mathbb{Q}] = 6$ und es existieren genau 6 verschiedene $\mathbb{Q}$-Einbettungen

$\sigma : Z \longrightarrow \bar{\mathbb{Q}} = \{z \in \mathbb{C} | z \text{ ist algebraisch über } \mathbb{Q}\}$

$Z = \mathbb{Q}(\eta, i) = \mathbb{Q}(\eta, \sqrt{-1})$; $\qquad\qquad N = \mathbb{Q}(\eta)$

$\eta^3 = 2, \sqrt{-1}^2 = -1$

14.10. Satz/ Definition:

Es sei $\bar{K}$ „der“ algebraische Abschluss von K, und L sei eine Zwischenerweiterung $K \subset L \subset \bar{K}$. Dann sind äquivalent:

i. Jede K-Einbettung von L nach $\bar{K}$ ist ein Automorphismus.

   (d.h. $\forall \sigma : L \longrightarrow \bar{K}$ ist $\sigma(L) = L$)

ii. L ist Zerfällungskörper einer Menge S von Polynomen aus $K[X]$.

iii. Jedes irreduzible $f \in K[X]$, das in L eine Nullstelle besitzt, zerfällt vollständig über L.

Sind (i),(ii),(iii) für $L|K$ erfüllt, so heißt $L|K$ normal.

Gegenbeispiel:

$K = \mathbb{Q}$, $L = Z_{\mathbb{Q},f}$, $\quad f = X^3 - 2$,

$L = \mathbb{Q}(\eta)$ mit $\eta^3 = 2$.

(i) verletzt (aus mengentheoretischen Gründen)

(iii) verletzt, da $f(X) = m_\eta(X)$. In $\bar{\mathbb{Q}}[X]$ ist $f(X) = (X - \eta) \underbrace{(X - \rho\,\eta)(X - \rho^2\eta)}_{= X^2 + \eta X + \eta^2 \text{ irreduzibel über } L}$,

$\rho = e^{2\frac{\pi i}{3}}$

$\rightsquigarrow f(X) = (X - \eta)(X^2 + \eta X + \eta^2)$ Primzerlegung in $L[X]$.

Beweis.

„(i) $\Rightarrow$ (ii)"

Wir geben eine passende Menge $S \subset K[X]$ an:

$$S := \{ f \in K[X] \mid \exists \alpha \in L \text{ mit } f(X) = m_\alpha(X) \}$$

Ist $f \in S$, $f = m_\alpha$ mit $\alpha \in L$ und $\beta \in \bar{K}$ eine Nullstelle von f, so $\exists K$-$\underset{(14.7.)}{\text{Einbettung}}$ $\sigma_0\colon \begin{array}{ccc} K(\alpha) & \longrightarrow & \bar{K} \\ \alpha & \longmapsto & \beta \end{array}$. Setze σ_0 zu einer K-Einbettung σ von L nach $\bar{K}$ fort (14.8.)

$$\begin{tikzcd}
L \arrow[rr, dashed, "\sigma"] \arrow[d, dash] & & \bar{K} \arrow[d, dash] \\
K(\alpha) \arrow[rr, "\sigma_0", "\alpha \longmapsto \beta"'] \arrow[dr, dash] & & K(\beta) \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

Nach (i) ist $\sigma(L) = L$ $\rightsquigarrow$ Jede Nullstelle β' von f in $\bar{K}$ liegt in L
$\rightsquigarrow$ f in $L[X]$ zerfällt vollständig
$\rightsquigarrow$ In L zerfallen alle $f \in S$ vollständig, und L ist minimal mit dieser Eigenschaft
$\rightsquigarrow$ $L = Z_{K,S}$

Genau dasselbe Argument zeigt auch „(i) $\Rightarrow$ (iii)"

„(ii) $\Rightarrow$ (i)"

Sei σ eine K-Einbettung von L nach $\bar{K}$, $L = Z_{K,S}$.

$$S = \{ f_i \in K[X] \mid i \in I \}, \quad L = Z_{K,S} = K(\alpha_{ij} \mid \alpha_{ij} = \text{Nullstelle von } f_i)$$

Da α_{ij} Nullstelle von f_i ist, ist $\sigma(\alpha_{ij})$ auch Nullstelle von f_i, also $L = K(\alpha_{ij})$

$\rightsquigarrow \sigma(L) = K(\sigma(\alpha_{ij})) = K(\alpha_{ij}) = L$, d.h. (i).

Wieder dasselbe Argument zeigt auch „(iii) $\Rightarrow$ (i)"

$\square$

14.11. Proposition:

$L|K$ algebraische Erweiterung, σ: $L \longrightarrow L$ eine K-Einbettung. Dann ist σ auch surjektiv, d.h. ein Automorphismus.

Beweis.

$\alpha \in L,\ f(X) = m_{K,\alpha}(X),\ \ L' := K(\beta \,|\, \beta \in L \,\text{Nullstelle von}\, f)$

Dann ist $[L' : K] < \infty$ und $\sigma(L') \subset L'$, also ist $\sigma|_{L'}$ surjektiv, insbesondere $\alpha \in \sigma(L)$ und σ ist surjektiv.

$\square$

14.12. Beispiele:

i. Ist $[L : K] = 2$, so ist $L|K$ normal.

ii. $\mathbb{Q}(\eta)|\mathbb{Q}$, $\quad \eta^3 = 2$ ist nicht normal.

iii. Die Erweiterungen $\mathbb{Q}(\alpha)|\mathbb{Q}$, $\mathbb{Q}(\beta)|\mathbb{Q}$ mit $\alpha :=$ primitive 9. Einheitswurzel, $\beta := \alpha + \bar{\alpha}$ (Beispiel (13.4.(ii))) sind normal.

iv. Die Erweiterung $N|\mathbb{F}_2$ von 13.4.(iii) $N = N_{\mathbb{F}_2, f}$, $\ f(X) = X^5 + X^2 + 1$ ist normal.

14.13. Proposition:

Es sei K ein Körper mit algebraischem Abschluss $\bar{K}$.

i. Sind K', L Teilerweiterungen von $\bar{K}|K$ und ist $L|K$ normal, so ist auch $LK'|K'$ normal.

$$\begin{tikzcd} & \bar{K} \arrow[d, no head] & \\ & LK' \arrow[dl, no head] \arrow[dr, no head, dashed] & \\ L \arrow[dr, no head, dashed] & & K' \arrow[dl, no head] \\ & K & \end{tikzcd}$$

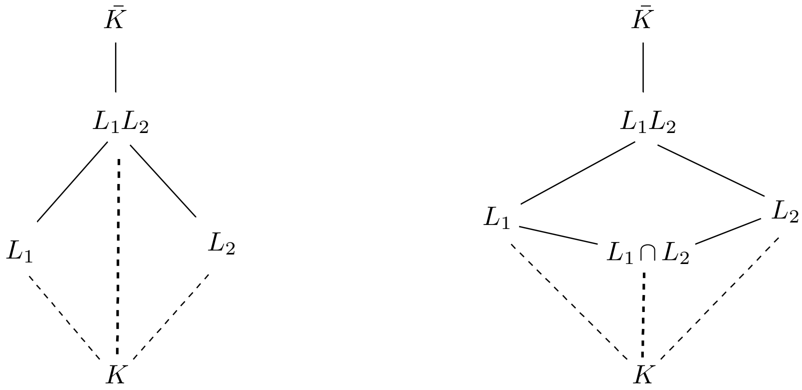
- - - - - - - - - - $:=$ normal

ii. $K \subset K' \subset L \subset \bar{K}$,

$L|K$ normal $\Rightarrow L|K'$ normal

(Spezialfall von (i))

iii. $K \subset L_i \subset \bar{K}$ $(i=1,2)$. $L_i|K$ normal $\Rightarrow \begin{cases} L_1L_2|K \text{ normal} \\ L_1 \cap L_2|K \text{ normal} \end{cases}$



- - - - - - - : = normal

Beweis.

i. $L|K$ normal, $L = Z_{K,S}$, $\quad S \subset K[X]$, $S = \{f_i \mid i \in I\}$,

$\{\alpha_{ij}\}$ Nullstellenmenge von f_i in L bzw. $\bar{K}$

$\rightsquigarrow L = K(\alpha_{ij})$, $LK' = K'(\alpha_{ij}) = Z_{K',S}$ normal über K'.

ii. ✓

iii. Sei $\sigma\colon L_1L_2 \longrightarrow \bar{K}$ eine K-Einbettung.

Dann ist $\left.\begin{array}{l}\sigma(L_1) = L_1 \\ \sigma(L_2) = L_2\end{array}\right\}$, da $L_i|K$ normal. $(i=1,2)$

Deshalb $\sigma(L_1L_2) = \sigma(L_1)\,\sigma(L_2) = L_1L_2 \rightsquigarrow L_1L_2|K$ normal.

Ist σ_0: $L_1 \cap L_2 \longrightarrow \bar{K}$ eine K-Einbettung, σ: $L_1L_2 \longrightarrow \bar{K}$ eine Fortsetzung (!), dann ist $\sigma_0(L_1 \cap L_2) = \sigma(L_1 \cap L_2) = \sigma(L_1) \cap \sigma(L_2) = L_1 \cap L_2 \rightsquigarrow L_1 \cap L_2|K$ normal.

□

14.14. Warnung:

Im allgemeinen gilt **nicht:** $\left.\begin{array}{c} M|L \\ L|K \end{array}\right\}$normal $\Rightarrow$ $M|K$ normal.

Gegenbeispiel:

$K = \mathbb{Q}, L = \begin{array}{l} \mathbb{Q}(\sqrt{2}) \\ \mathbb{Q}(\alpha) \text{ mit } \alpha^2 = 2 \end{array}$, $M = \begin{array}{l} L\mathbb{Q}(\sqrt{\sqrt{2}}) \\ = L(\eta),\ \eta^2 = \alpha \Leftrightarrow \eta^4 = 2 \end{array}$

$M \ = \mathbb{Q}(\eta)$
$2|$
L
$2|$
$\mathbb{Q}$

$f = m_{\mathbb{Q},\eta} = X^4 - 2$. Die drei weiteren Nullstellen von $m_{\mathbb{Q},\eta}$ sind $-\eta, \pm i\eta$,

also ist $Z_{\mathbb{Q},f} = \mathbb{Q}(\eta, i) \underset{\text{Grad } 4}{\supsetneq \mathbb{Q}(\eta)} = M$

M besitzt eine $\mathbb{Q}$-Einbettung $\sigma: M \longrightarrow \mathbb{C}$ mit Bild in $\mathbb{R}$, nämlich

$\eta \longmapsto$ die $\begin{matrix}\text{positive}\\ \text{negative}\end{matrix}$ [4] 4. Wurzel von 2 in $\mathbb{R}$.

Deshalb enthält M keine primitive 4. Einheitswurzel, also ist $\mathbb{Q}(\eta, i) \neq \mathbb{Q}(\eta)$.

4. Die Wahl der positiven oder der negativen 4. Wurzel ist vollkommen willkürlich.