§6 Zerfällungskörper und algebraischer Abschluss

1. **Lemma** Sei K ein Körper, sei $f \in K[T]$ mit $\deg(f) = n \geq 1$. Angenommen, $u_1, \dots, u_m \in K$ sind Nullstellen von f, d.h. $f(u_j) = 0$ für $j = 1, \dots, m$. Wenn für alle $i < j$ gilt $u_i \neq u_j$, so gibt es $g \in K[T]$ mit

$$f = (T-u_1)(T-u_2)\cdots(T-u_m)\cdot g$$

Insbesondere ist $m \leq n$.

Beweis: Angenommen, $u \in K$ ist eine Nullstelle von f. Teilen mit Rest wie in §4.11:

$$f = (T-u)\cdot q + r \qquad \deg(r) < \deg(T-u) = 1$$
$$\Rightarrow r \in K \text{ konstant}$$

$$0 = f(u) = (u-u)\cdot q(u) + r$$

Es folgt $f = (T-u)\cdot q$. Ist $v \neq u$ eine weitere Nullstelle von f, so folgt

$$0 = f(v) = \underbrace{(v-u)}_{\neq 0}\cdot q(v) \Rightarrow v \text{ ist Nullstelle von } q = q_1 \neq 0$$

$\Rightarrow q = (T-v)\,q_2$ usw $\Rightarrow$

$$f = (T-u_1)\cdots(T-u_m)\,q_m, \quad q_m \neq 0 \qquad \square$$

$$\deg(f) = m + \deg(q_m)$$

2. <u>Def</u> Ein Polynom f dessen Leitkoeffizient 1 ist, also $f = T^n + a_{n-1}T^{n-1} + \dots + a_0$ heißt <u>normiert</u>.
Ist K ein Körper, so ist jedes $f \in K[T]$, $f \neq 0$ von der Form $f = a \cdot \tilde{f}$, $\tilde{f} \in K[T]$ normiert, $a \in K^*$ und $f, \tilde{f}$ haben die gleichen Nullstellen. (klar).
Ist $f \in K[T]$ normiert und gibt es $u_1, \dots, u_m \in K$ mit $f = (T-u_1)(T-u_2)\cdots(T-u_m)$, so <u>zerfällt f in Linearfaktoren über K</u> ($\rightsquigarrow$ Jordan-Normalform)

3. <u>Def</u> Sei K ein Körper, $f \in K[T]$ normiert.
Eine Körpererweiterung $K \subseteq L$ heißt <u>Zerfällungskörper</u> von f, wenn es $u_1, \dots, u_m \in L$ gibt mit
(i) $f = (T-u_1)\cdots(T-u_m)$
(ii) $L = K(u_1, \dots, u_m)$ (folglich $[L:K] < \infty$)

<u>Bsp</u> $f = T^2+1 \in \mathbb{R}[T]$ $\quad f = (T-i)(T+i)$ $\quad i \in \mathbb{C}$
$\mathbb{C} = \mathbb{R}(i)$ $\rightsquigarrow$ $\mathbb{C}$ ist Zerfällungskörper von T^2+1.

4. <u>Satz</u> Sei K ein Körper und sei $f \in K[T]$ normiert mit $n = \deg(f) \geq 1$. Dann existiert ein Zerfällungskörper $L \supseteq K$ mit $[L:K] \leq n!$

<u>Beweis</u> Induktion nach n

$\boxed{n=1}$ $\rightsquigarrow$ $f = T-u$ $\quad u \in K$ $\rightsquigarrow$ $L = K$ fertig.

Sei jetzt $n \geq 2$, schreibe $f = g \cdot h$ mit $g \in K[T]$ normiert + irreduzibel. Dann ist $K' = K[T]/(g)$ ein Körper nach §4.5.

Via $K \hookrightarrow K[T] \xrightarrow{\pi} K'$ können wir K als Teilkörper von K' auffassen – die Elemente von K' sind von der Form $f + (g)$, $f \in K[T]$.

Setze $u = \pi(T) \in K'$, $u = T + (g) \rightsquigarrow u^k = T^k + (g)$

$$g = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \Rightarrow g(u) = \underbrace{T^n + a_{n-1}T^{n-1} + \ldots + a_0}_{= g} + (g)$$

$= (g) \rightsquigarrow u$ ist Nullstelle von g.

In $K'[T]$ folgt $g = (T-u) \cdot \tilde{g}$. Weiter gilt $\mu_u = g$, da g irreduzibel ist, also gilt für $K' = K(u)$, dass $[K':K] = \deg(g) \leq n$.

Nun $\deg(\tilde{g} \cdot h) = n-1 \rightsquigarrow$ es gibt einen Zerfällungskörper $L \supseteq K'$ für $\tilde{g} \cdot h$ mit

$$L = K'(u_2, \ldots, u_m) = K(u_1, u_2, \ldots, u_m)$$

$u = u_1$

$$[L:K] = \underbrace{[L:K']}_{\leq (n-1)!} \cdot \underbrace{[K':K]}_{\leq n} \leq n! \qquad \square$$

Wir zeigen jetzt, dass ein Zerfällungskörper bis auf Isomorphie eindeutig bestimmt ist.

5. Def Sei $\varphi: K \to K'$ ein Isomorphismus von Körpern.

(a) Für $f \in K[T]$, $f = a_n T^n + \ldots + a_0$ setze
$\varphi(f) = \varphi(a_n)T^n + \ldots + \varphi(a_0) \in K'[T]$. Dann ist
$\varphi: K[T] \to K'[T]$ ein Isomorphismus.

(b) Wenn $L \supseteq K$ und $L' \supseteq K'$ Körpererweiterungen sind
und $\psi: L \to L'$ ein Homomorphismus mit
$\psi|_K = \varphi$

$$\begin{tikzcd} L \arrow[r, "\psi"] & L' \\ K \arrow[u, hook] \arrow[r, "\varphi"] & K' \arrow[u, hook] \end{tikzcd}$$

so heißt ψ <u>Homomorphismus über φ.</u>

6. Lemma Sei $\varphi: K \to K'$ ein Isomorphismus von Körpern, seien $L \supseteq K$ und $L' \supseteq K'$ Körpererweiterungen.
Sei $u \in L$ mit normiertem Minimalpolynom $\mu_u = g$.

(i) Wenn $v \in L'$ eine Nullstelle von $\varphi(g)$ ist, gibt es <u>genau ein</u> Isomorphismus $K(u) \xrightarrow{\psi} K'(v)$ über φ mit $\psi(u) = v$.

(ii) Wenn $\varphi(g)$ keine Nullstelle in L' hat, gibt es <u>kein</u> Homomorphismus $\psi: K(u) \to L'$ über φ.

<u>Beweis.</u> Da g irreduzibel ist und $\varphi: K[T] \to K'[T]$ ein Isomorphismus ist, ist $\varphi(g)$ irreduzibel. Betrachte

$$\begin{tikzcd} K(u) \arrow[r, "\cong"] & K[T]/(g) \arrow[r, "\cong"] & K'[T]/(\varphi(g)) \arrow[r, "\cong"] & K'(v) \\ K \arrow[u, hook] \arrow[r, equal] & K \arrow[u, hook] \arrow[r, "\varphi"] & K' \arrow[u, hook] \arrow[r, equal] & K' \arrow[u, hook] \end{tikzcd}$$

Es folgt die Existenz von $\psi : K(u) \xrightarrow{\cong} K(v)$ mit $\psi(u) = v$. Jedes Element $z \in K(u)$ ist von der Form $z = a_\ell u^\ell + \ldots + a_0$ mit $a_j \in K$, also ist $\psi(z)$ festgelegt durch $\psi(u)$. □ #

(ii) Ist $\psi : K(u) \to L'$ ein Homomorphismus über φ, so folgt für $\psi(u) = v$, dass $\varphi(g)(v) = \psi(g(u)) = 0$ □

7. <u>Theorem</u> Sei $\varphi : K \to K'$ ein Isomorphismus von Körpern, sei $f \in K[T]$ normiert, seien $L \supseteq K$ sowie $L' \supseteq K'$ Zerfällungskörper von f bzw. $\varphi(f)$. Sei $H = \{ \psi : L \to L' \mid \psi \text{ Isomorphismus über } \varphi \}$. Dann gilt

$$1 \leq \# H \leq [L : K]$$

(d.h. es gibt solche Isomorphismen über φ, aber höchstens $[L:K]$ viele).

<u>Bew.</u> Induktion nach $n = \deg(f)$.

$\boxed{n=1}$ $f = T - u$ $\quad \varphi(f) = T - \varphi(u)$ $\quad u \in K$, $\varphi(u) \in K'$

$\leadsto L = K \quad L' = K' \Rightarrow \psi = \varphi$ fertig.

$\boxed{n \geq 2}$ Schreibe $f = g \cdot h$ $\quad g \in K[T]$ normiert und irreduzibel. Da f in $L[T]$ in Linearfaktoren zerfällt, zerfällt auch g

in $L[T]$ in Linearfaktoren. Sei $u \in L$ eine Nullstelle von g. Sei $v \in L'$ eine Nullstelle von $\varphi(g)$ ($\varphi(g)$ zerfällt in $L'[T]$ in Linearfaktoren).
Nach Lemma §6.6. gibt es genau einen Isomorphismus
$\rho: K(u) \longrightarrow K'(v)$ über φ mit $\rho(u) = v$.
Setze $M = K(u) \subseteq L$ sowie $M' = K(v) \subseteq L'$

$\rightsquigarrow g = (T-u)\tilde{g}$ für $\tilde{g} \in M[T]$

$\rightsquigarrow f = (T-u)\cdot\tilde{g}\cdot h$ $\quad \tilde{g}\cdot h \in M[T]$. Nach Induktionsannahme gibt es Isomorphismus

$\psi: L \xrightarrow{\psi} L'$ über ρ, also über φ.

$$\begin{tikzcd}
L \arrow[r, "\psi"] & L' \\
M \arrow[u, hook] \arrow[r, "\rho"] & M' \arrow[u, hook] \\
K \arrow[u, hook] \arrow[r, "\varphi"] & K \arrow[u, hook]
\end{tikzcd}$$

Für ψ über ρ gibt es höchstens $[L:M]$ Möglichkeiten,
ist ψ über φ, so gibt es höchstens $\deg(g)$ viele Möglichkeiten für $\psi(u) = v$, zu jeder davon höchstens $[M:K]$ Möglichkeiten über $K(u) \xrightarrow{\rho} K(v)$

$\rightsquigarrow$ höchstens $[L:M]\cdot[M:K] = [L:K]$ Möglichkeiten. $\square$

8. <u>Korollar</u> Sei $f \in K[T]$ normiert, sei $L \supseteq K$ ein Zerfällungskörper. Sei

$$\mathrm{Aut}(L|K) = \{ \varphi : L \to L \mid \varphi \text{ Isomorphismus über } \mathrm{id}_K \}$$

$$\begin{tikzcd} L \arrow[r, "\varphi"] & L \\ K \arrow[u, hook] \arrow[r, equal] & K \arrow[u, hook] \end{tikzcd}$$

Dann ist $\mathrm{Aut}(L|K)$ eine Gruppe (bezüglich Komposition von Isomorphismen) und

$$\# \mathrm{Aut}(L|K) \leq n! \qquad \text{wobei } n = [L:K]$$

<u>Bem</u> Über Eigenschaften der Gruppe $\mathrm{Aut}(L|K)$ kann man Aussagen über die Lösbarkeit der Gleichung $f(u)=0$ machen. Das ist (unter anderem) Inhalt der <u>Galois-Theorie</u>. Auflösbarkeit von $\mathrm{Aut}(L|K)$ entspricht (grob gesagt) der Auflösbarkeit der Gleichung $f(u)=0$ durch Wurzeln (vgl. Mitternachtsformel für $\deg(f)=2$). Die nicht-Auflösbarkeit von $\mathrm{Sym}(n)$ für $n \geq 5$ entspricht der nicht-Existenz von allgemeinen Lösungsformeln für Gleichungen von Grad $n \geq 5$.

9. <u>Def</u> Ein Körper K heißt <u>algebraisch abgeschlossen</u>, wenn es eine der folgenden äquivalenten Bedingungen erfüllt

(i) jedes normierte Polynom $f \in K[T]$ mit $\deg(f) = n \geq 1$ zerfällt in Linearfaktoren, $f = (T-u_1)\cdots(T-u_n)$, $u_j \in K$

(ii) jedes Polynom $f \in K[T]$ mit $\deg(f) = n \geq 1$ hat mindestens eine Nullstelle $u \in K$.

⌈ (i) ⇒ (ii) nach §6.2 und (ii) ⇒ (i) nach §6.1 mit Induktion nach n. ⌋

<u>Bsp</u> Der Körper $\mathbb{C}$ ist abgeschlossen nach LA §5.27

10. <u>Satz</u> Sei $K \subseteq L$ eine Körpererweiterung. Wenn L algebraisch abgeschlossen ist, dann ist $\mathrm{acl}_L(K) \subseteq L$ algebraisch abgeschlossen.

<u>Beweis</u> Sei $K' = \mathrm{acl}_L(K)$, sei $f \in K'[T]$ normiert, $\deg(f) \geq 1$. Sei $u \in L$ eine Nullstelle von f. Dann gilt

$$u \in \mathrm{acl}_L(K') \underset{\S 5.21}{=} \mathrm{acl}_L(K) = K' \qquad \square$$

11. <u>Theorem</u> Sei K ein Körper. Dann existiert eine Körpererweiterung $L \supseteq K$ mit (i) L ist algebraisch über K und (ii) L ist algebraisch abgeschlossen.

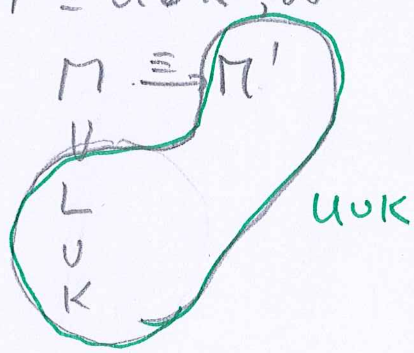
<u>Beweis</u> Mengentheoretische Vorüberlegungen. Es gilt

$\# K[T] \leq \#(K \times \mathbb{N})$. Jedes Polynom in $K[T]$ hat nur endlich viele Nullstellen. Ist also $M \supseteq K$

algebraisch, so folgt $\# M \leq \#(K \times \mathbb{N})$, denn jedes Polynom $f \in K[T]$ hat höchstens endlich viele Nullstellen. Es folgt: es gibt eine Menge U mit folgenden Eigenschaften:

(i) Ist $L \supseteq K$ algebraisch, so gibt es einen zu L isomorphen Körper L', dessen Elemente Elemente der Menge $K \cup U$ sind

(ii) Sind $M \supseteq L \supseteq K$ beides algebraische Körpererweiterungen (dann ist auch $M \supseteq K$ algebraisch nach § 5.21!) und ist L Teilmenge von $U \cup K$, so gibt es einen Körper $M' \subseteq U \cup K$, der über L isomorph zu M ist



Sei $P = \{ M \supseteq K \mid M$ alg. Körpererweiterung, die Elemente von M sind Elemente von $U \cup K \}$

Definiere $M_1 \leq M_2 \iff M_1 \subseteq M_2$ ist Körpererweiterung. Damit ist $(P, \leq)$ partiell geordnet.

Ist $\mathcal{G} \subseteq P$ eine Kette, setze $\tilde{L} = \bigcup \mathcal{G}$.

Beh: $\tilde{L} \in P$. Seien $a, b \in \tilde{L}$ ⇝ es gibt $L_1, L_2 \in \mathcal{G}$

$a \in L_1$, $b \in L_2$ OE $L_1 \leq L_2$ ⇝

$a, b, a \pm b, a \cdot b, a/b \in L_2 \Rightarrow \tilde{L}$ Körper

weiter ist $a \in L_2$ algebraisch über K ⇝ $\tilde{L}$ algebraisch über K ⇝ $\tilde{L} \in P$

Nach Zorns Lemma gibt es in P maximale Elemente. Sei $L \in P$ maximal. Beh: Dann ist L algebraisch abgeschlossen.

Denn: $f \in L[T]$ nicht konstant ⇝ $M \supseteq L$, f hat Nullstelle $u \in M$ (z.B. algebraisch, M ein Zerfällungskörper von f über L) OE $M \in P$

(→ mengentheoretische Vorbemerkung geht jetzt ein!)

$\Rightarrow M = L \Rightarrow u \in L$.

Also ist L algebraisch abgeschlossen. $\square$

Man nennt $L \supseteq K$ einen (den) <u>algebraischen Abschluss</u> von K.

12. __Theorem__ (__Eindeutigkeit des algebraischen Abschlusses__)

Sei K ein Körper, seien $L \supseteq K$ und $L' \supseteq K$ algebraische Körpererweiterungen. Wenn L und L' algebraisch abgeschlossen sind, gibt es einen Isomorphismus

$$\begin{tikzcd} L \arrow[r, "\varphi"] & L' \\ K \arrow[u, hook] \arrow[r, equal] & K \arrow[u, hook] \end{tikzcd}$$

über id_K.

__Bew:__ Sei $P = \left\{ M \xrightarrow[\cong]{\varphi} M' \;\middle|\; \begin{array}{l} M \subseteq L \text{ Teilkörper} \\ M' \subseteq L' \text{ Teilkörper} \\ \varphi \text{ über } id_K \text{ Isomorphismus} \end{array} \right\}$

$\Rightarrow$ $K \xrightarrow{id} K \in P$

Definiere $(M \xrightarrow{\varphi} M') \leq (N \xrightarrow{\varrho} N')$

$\Leftrightarrow$ $$\begin{tikzcd} N \arrow[r, "\varrho"] & N' \\ M \arrow[u, hook] \arrow[r, "\varphi"] & M' \arrow[u, hook] \end{tikzcd}$$ kommutiert

$\Rightarrow$ jede Kette in P hat obere Schranke (ähnlich wie oben)

$\Rightarrow$ P enthält maximales Element.

Sei $(M \xrightarrow[\cong]{\varphi} M') \in P$ maximal. Ist $u \in L$

so erhalten wir mit §6.5 $(M(u) \xrightarrow{\cong} M'(v)) \in P$

$\Rightarrow u \in M$, $u' \in M'$ $\Rightarrow$ $M = L$ und $M' = L'$ $\square$