§ (Algebraische) Körpererweiterungen

Wir wollen Lösungen von Polynomgleichungen studieren. Sei also $f \in \mathbb{Q}[X]$ und α eine Nullstelle von f in $\mathbb{C}$ (in der Funktionentheorie zeigt man, dann $f \in \mathbb{C}[X]$ in linear faktoren zerfällt)

Definiere $\mathbb{Q}(\alpha) = \bigcap_{\substack{K \subseteq \mathbb{C} \\ \text{Unterkörper} \\ \text{mit } \alpha \in K}} K \subseteq \mathbb{C}$, der kleinste Unterkörper von $\mathbb{C}$ welcher α enthält.

$\mathbb{Q}[X] \to \mathbb{C}$, $X \longmapsto \alpha$ hat dann Bild in $\mathbb{Q}(\alpha)$

Beh: $\mathbb{Q}[X] \to \mathbb{Q}(\alpha)$ ist surjektiv:

sei $R = \mathrm{Im}(\mathbb{Q}[X] \to \mathbb{C})$. Dann ist $\mathbb{Q}[X] \twoheadrightarrow R$ und nach dem Homomorphiesatz $R \cong \mathbb{Q}[X]/(q)$ (da $\mathbb{Q}[X]$ Hauptidealring).

$q \in \mathbb{Q}[X]$ ist prim (da R Integritätsbereich) $\Rightarrow (q)$ max. (da $\mathbb{Q}[X]$ Hauptidealring)

$\Rightarrow R$ Körper, per Konstruktion $\alpha \in R \Rightarrow \mathbb{Q}(\alpha) \subseteq R \subseteq \mathbb{Q}(\alpha)$.

Wir schließen, dass $\mathbb{Q}(\alpha) = \mathbb{Q}[X]/(q)$ für ein $q \in \mathbb{Q}[X]$ prim (was von α abhängt).

Ebenso kann man dann zu f einen kleinsten Unterkörper L von $\mathbb{C}$ konstruieren, sodass alle Nullstellen von f (in $\mathbb{C}$) in L liegen. (Der Zerfällungskörper von f). Im Kontext von allg. Lösungsformeln werden wir solche Zerfällungskörper studieren.

Wir beginnen mit allgemeiner Körpertheorie.

Lemma 3.1 Sei R ein Integritätsbereich, $\mathbb{Z} \xrightarrow{\varphi} R$ die kan. Abbildung. Dann ist $\ker(\varphi) = p\mathbb{Z}$ für p prim oder φ injektiv.

Beweis: angenommen $\ker(\varphi) \neq 0 \rightsquigarrow \ker(\varphi) = m\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \subseteq R$ Integritätsring $\Rightarrow m$ prim.

Wir ~~nennen~~ sagen R hat Charakteristik p, falls $\ker(\varphi) = p\mathbb{Z}$ (p prim, $p \neq 0$)

Bem: $R \subseteq S$ Integritätsringe $\Rightarrow \mathrm{char}(R) = \mathrm{char}(S)$.

Beispiele 3.2 a) $\mathrm{char}(\mathbb{F}_p) = p$

b) $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = 0$

c) $\mathrm{char}(\mathbb{Q}(\mathbb{F}_p[x])) = p$, $\mathbb{F}_p(x) = \mathbb{Q}(\mathbb{F}_p[x])$ ist kein endlicher Ring

Sei K ein Körper. Der Primkörper von K ist $P = \bigcap_{L \subseteq K \text{ Unterkörper}} L$ = kleinster Unterkörper von K.

Lemma 3.3 K Körper, $P \subseteq K$ Primkörper. Dann

a) $\mathrm{char}(K) = p \iff P = \mathbb{F}_p$ (p prim)

b) $\mathrm{char}(K) = 0 \iff P = \mathbb{Q}$.

Beweis: a) $\mathbb{Z} \xrightarrow{\varphi} K$ Hom. $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\cong} \mathrm{Im}(\varphi)$ somit gilt $P \subseteq \mathbb{Z}/p\mathbb{Z}$

$\Rightarrow P = \mathbb{Z}/p\mathbb{Z}$ ($[1] \in P \Rightarrow \mathbb{Z}/p\mathbb{Z} \subseteq P$) , „$\Leftarrow$“ folgt aus der Bem.

b) $\mathbb{Z} \hookrightarrow K$ injektiv. $\Rightarrow$ ~~vgl.~~ induz. Abb. $\mathbb{Z} \hookrightarrow K$, $\mathbb{Z} \to \mathbb{Q}(\mathbb{Z}) = \mathbb{Q} \xrightarrow{i} K$

da $\mathbb{Q}$ Körper $\Rightarrow i$ injektiv

$\Rightarrow P \subseteq \mathbb{Q}$ Unterkörper. $\Rightarrow P = \mathbb{Q}$. , „$\Leftarrow$“ folgt aus der Bem. ∎

Körpererweiterungen

Sind $K \subseteq L$ Körper, so nennen wir L eine Körpererweiterung. Wird schreiben L/K (L heißt über K). Körper E mit $K \subseteq E \subseteq L$ nennen wir Zwischenkörper.

Ist L/K so ist L ein K-VR vermöge $K \times L \to L \times L \xrightarrow{\cdot} L$

Definition 3.4 Der Grad von L/K, geschrieben $[L:K]$ ist definiert als $[L:K] = \dim_K L$. Die Körpererw. L/K ist endlich falls $[L:K] < \infty$ (und unendlich sonst).

Beispiel 3.5 a) $K = L \iff [L:K] = 1$

b) $[\mathbb{R}:\mathbb{Q}] = \infty$, $[\mathbb{C}:\mathbb{R}] = 2$

Lemma 3.6 Seien $K \subseteq E \subseteq L$ Körper. Dann gilt

$$[L:K] = [E:K] \cdot [L:E]$$

Insbesondere ist $[L:K]$ prim $\Rightarrow E = K$ oder $E = L$

Beweis: ist E/K oder L/E unendlich, so auch L/K. es genügt also anzunehmen, dass L/K endlich ist.

es gilt $L \overset{\text{EVR}}{\cong} \bigoplus_{[L:E]} E \overset{K\text{-VR}}{\cong} \bigoplus_{[L:E]} \bigoplus_{[E:K]} K$

Definition 3.7 Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt *algebraisch über K* falls es ein Polynom $0 \neq f \in K[X]$ gibt, sodass α eine Nullstelle von f ist. ist α nicht algebraisch, so heißt α *transzendent* über K

L/K heißt *algebraisch* falls alle $\alpha \in L$ algebraisch über K sind

Bemerkungen: L/K Körpererweiterung

a) $\alpha \in L$, sei $\varphi_\alpha : K[X] \to L$, $X \mapsto \alpha$. eind. Ringhom.
dann ist α algebraisch über $K \iff \ker(\varphi_\alpha) \neq \{0\}$

b) ist $\alpha \in L$ algebraisch / K so ist $\operatorname{Im}(\varphi_\alpha) \subseteq L$ ein Unterring und daher Integritätsbereich. $\Rightarrow K[X]/\ker(\varphi_\alpha) \cong \operatorname{Im}(\varphi_\alpha)$. $K[X]$ HIR $\Rightarrow$ $\ker(\varphi_\alpha) = (q_\alpha)$ mit q_α prim ($\operatorname{Im}(\varphi_\alpha)$ Integritätsbereich) $\Rightarrow (q_\alpha)$ max.
$\Leftrightarrow$ (q_α ist das Minimalpolynom von α) oBdA q_α normiert
(ist q ein normiertes irred. polynom mit Nullstelle $\alpha \Rightarrow q = q_\alpha$)
$\Rightarrow K[X]/(q_\alpha) \subseteq L$ ein Unterkörper ($\cong \operatorname{Im}(\varphi_\alpha)$)
$n = [L:K]$

c) jede endliche Erweiterung L/K ist algebraisch: sei $\alpha \in L$. Betrachte $\{1, \alpha, \alpha^2, \dots, \alpha^n\} \subseteq L$. Diese Menge ist K-linear abhängig, da $\dim_K L = n$
$\Rightarrow \exists\, b_0, \dots, b_n$ sodass $\sum_{i=0}^{n} b_i \alpha^i = 0$. Dann ist α eine Nullstelle von $f = \sum_{i=0}^{n} b_i X^i$ (nicht alle b_i 0)

Proposition 3.8 L/K Körpererweiterung, $\alpha \in L$ algebraisch. $\varphi_\alpha : K[X] \to L$ kan. Hom.
$K \subseteq K(\alpha) = \operatorname{Im}(\varphi_\alpha) \subseteq L$. Dann ist $K(\alpha) \cong K[X]/(q_\alpha)$ ein Körper, q_α Minimalpolynom von α

und $[K(\alpha) : K] = \operatorname{grad}(q_\alpha)$

Beweis: es verbleibt zu zeigen, dass $[K(\alpha):K] = \text{grad}(q_\alpha)$.

dafür behaupten wir, dass $\mathcal{B} = \{\pi(1), \pi(x), \dots, \pi(x^{n-1})\}$ eine K-Basis von $K[x]/(q_\alpha)$ ist, wobei $\pi: K[x] \to K[x]/(q_\alpha)$ die Projektion bezeichnet.

1) $\mathcal{B}$ ist ein EZS: sei $g \in K[x]$. Nach Division mit Rest gilt

$g = q \cdot q_\alpha + r$, $\text{grad}(r) < n$. Das heißt, dass $r \in \text{span}\{x^0, \dots, x^n\}$

und somit $[g] = [r] \in \text{span}\{\pi(x^0), \dots, \pi(x^{n-1})\}$

2) $\mathcal{B}$ ist linear unabhängig: seien $a_i \in K$, $i = 0, \dots, n-1$ und

$$\pi\left(\sum_{i=0}^{n-1} a_i x^i\right) = 0 \quad \to \quad \sum_{i=0}^{n-1} a_i x^i \in \ker(\pi) = (q_\alpha).$$

Da $\text{grad}\left(\sum_{i=0}^{n-1} a_i x^i\right) < \text{grad}(q_\alpha)$ folgt, dass $\sum_{i=0}^{n-1} a_i x^i = 0$ in $K[x]$

d.h. $a_i = 0$ für alle $i = 0, \dots, n-1$. ⊡

Beispiele 3.9 a) $\mathbb{C}/\mathbb{Q}$, $p \in \mathbb{Z}$ prim, $n \geq 2$. $\alpha = \sqrt[n]{p} \in \mathbb{C}$.

dann ist α algebraisch/$\mathbb{Q}$ (Nullstelle von $X^n - p$)

es folgt dass $X^n - p$ das Minimalpolynom q_α ist ($X^n - p$ ist irreduzibel nach Eisenstein)

$\Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}[x]/_{X^n - p}$, $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$, $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$ ist

Bild von $x^0, \dots, x^{n-1}$ unter $\mathbb{Q}[x] \to \mathbb{Q}(\alpha)$, d.h. $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Sei nun L/K Körpererweiterung und $\{\alpha_i\}_{i \in I} \subseteq L$.

Wir schreiben $K(\{\alpha_i\}_{i \in I})$ für den kleinsten Zwischenkörper welcher $\{\alpha_i\}_{i \in I}$ enthält, also $K(\{\alpha_i\}_{i \in I}) = \bigcap_{\substack{K \subseteq E \subseteq L \\ \forall i \in I: \alpha_i \in E}} E$. Ist $|I| = n < \infty$ schreiben wir

$K(\alpha_1, \dots, \alpha_n)$.

Sei $K[x_1, \dots, x_n] \to L$ der Ringhom mit $x_i \mapsto \alpha_i$. Klassischer Notation folgend schreiben wir für das Bild $K[\alpha_1, \dots, \alpha_n]$ (Warnung: dies ist nicht der Polynomring in Variablen $\alpha_1, \dots, \alpha_n$)

Per Konstruktion haben wir

$$K \subseteq K[\alpha_1, \dots, \alpha_n] \subseteq K(\alpha_1, \dots, \alpha_n) \subseteq L$$

und

$$\mathbb{Q}(K[\alpha_1, \dots, \alpha_n]) \xleftarrow{\cong} \text{Unterkörper von } L \text{ welche } \alpha_1, \dots, \alpha_n \text{ enthält.}$$

$$\Rightarrow K(\alpha_1, \dots, \alpha_n) \subseteq \mathbb{Q}(K[\alpha_1, \dots, \alpha_n]) \subseteq K(\alpha_1, \dots, \alpha_n)$$

Definition 3.10 Eine Körpererweiterung L/K heißt **endlich erzeugt** falls es $\alpha_1, \dots, \alpha_n \in L$ gibt sodass $L = K(\alpha_1, \dots, \alpha_n)$.
Ist $L = K(\alpha)$ für $\alpha \in L$ so nennen wir L/K **einfach**.

Lemma 3.11 L/K, $\alpha_1, \dots, \alpha_n \in L$ sodass $L = K(\alpha_1, \dots, \alpha_n)$. Sind alle α_i algebraisch über K so gilt a) $K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$
b) L/K endlich
(algebraisch und endl. erzeugt $\Leftrightarrow$ endlich).

Beweis: Induktion über n. Der Fall $n=1$ ist in Prop 3.8 behandelt
Betrachte nun $K \subseteq K[\alpha_1, \dots, \alpha_{n-1}] \subseteq K[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = K[\alpha_1, \dots, \alpha_{n-1}, \alpha_n]$
Induktion $\quad K(\alpha_1, \dots, \alpha_{n-1}) \subseteq K(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$
$\quad = K(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$.
und alle Inklusionen sind endliche Erweiterungen. □

Lemma 3.12 Seien $K \subseteq E \subseteq L$ Körpererweiterungen. Ist $\alpha \in L$ alg. über E und E/K algebraisch, so ist α alg. über K. Des weiteren ist L/K algebraisch $\Leftrightarrow$ L/E und E/K sind algebraisch.

Beweis: sei $f = X^n + a_{n-1}X^{n-1} + \dots + a_0$ das Minimalpolynom von α, $/E$ d.h. $E[X]/(f) \xrightarrow{\cong} E(\alpha) \subseteq L$. Dann ist $f \in K(a_0, \dots, a_{n-1})[X]$
und nach 3.8 ist $K(a_0, \dots, a_{n-1}) \subseteq K(a_0, \dots, a_{n-1}, \alpha)$ eine endliche Erweiterung
weil da E/K alg. $\Rightarrow a_0, \dots, a_{n-1}$ alg. $/K$ und daher
$K \subseteq K(a_0, \dots, a_{n-1})$ endlich nach 3.11. Daher ist auch $K \subseteq K(a_0, \dots, a_{n-1}, \alpha)$
endlich und somit algebraisch $\Rightarrow \alpha$ algebraisch $/K$.
Es folgt dass L/E und E/K algebr. $\Rightarrow L/K$ algebraisch.
Die Umkehrung ist einfacher, da $K[X] \subseteq E[X]$ und $E \subseteq L$. □

Beispiel 3.13 $L = \{\alpha \in \mathbb{C} \mid \alpha \text{ alg. über } \mathbb{Q}\}$.
Behauptung: $\mathbb{Q} \subseteq L \subsetneq \mathbb{C}$ Unterkörper: sind $a, b \in L \Rightarrow a$ $\mathbb{Q}(a,b)$ endl. über $\mathbb{Q}$
und somit sind alle Elemente von $\mathbb{Q}(a,b)$, wie zB $a+b$, ab, a^{-1} (falls $a \neq 0$)
auch algebraisch über $\mathbb{Q}$.

Per Konstruktion ist daher $L/\mathbb{Q}$ algebraisch, und wir behaupten, dass $[L:\mathbb{Q}] = \infty$. Tatsächlich gilt $X^n - p$ prim in $\mathbb{Z}[X]$

$\Rightarrow \mathbb{Q} \subsetneq \mathbb{Q}(\sqrt[n]{p}) \subseteq L$ und $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$ (Z II)

d.h. $[L:\mathbb{Q}] \geq n \quad \forall n \geq 0$. (es folgt, dass $L/\mathbb{Q}$ nicht endl. erzeugt ist)

L ist also eine unendliche algebraische Erweiterung von $\mathbb{Q}$.

Überdies in L (als Menge) abzählbar ($\mathbb{Q}$-alg. Elemente in $\mathbb{C}$ haben eine Surjektion von $\mathbb{Q}[X]$). Da $\mathbb{C}$ überabzählbar ist sind die meisten Elemente von $\mathbb{C}$ transzendent über $\mathbb{Q}$, es ist aber garnicht so leicht Elemente von $\mathbb{C} \setminus L$ hinzuschreiben. (Bsp sind oft analytischer Natur, wie $e, \pi, \ldots$)

Algebraische Abschlüsse

Erinnerung: Ist L/K Körpererw. $\alpha \in L$ alg. über K, mit Minimalpolynom f

$\Rightarrow [K(\alpha):K] = \operatorname{grad}(f)$. Wir zeigen umgekehrt, dass zu jedem Polynom $f \in K[X]$ eine endl. Erw. existiert indem f eine Nullstelle hat.

Satz 3.14 (Kronecker) K Körper, $f \in K[X]$ $\operatorname{grad}(f) \geq 1$. Dann existiert ein endlicher Erweiterungskörper L/K indem f eine Nullstelle hat.

Beweis: oBdA können wir annehmen, dass f normiert und irreduzibel ist. Dann ist $(f) \in K[X]$ prim und damit maximal. Setze $L = K[X]/(f)$. Dann hat man eine Abb. $K \to L$ welche L zu einer endl. Erw. vom grad $\operatorname{grad}(f)$ macht. Behauptung: das Bild α von X unter der Abbildung $K[X] \to L = K[X]/(f)$ ist eine Nullstelle von f in L, denn:

$K[X] \to L[X] \xrightarrow{X \mapsto \alpha} L$ ist die kanonische Projektion nach (f), sodass f im Kern liegt. ∎

Bem: Nach Induktion folgt, zu f existiert eine endl. Erweiterung in der f in Linearfaktoren zerfällt.

Definition 3.15 Ein Körper heißt *algebraisch abgeschlossen*, falls jedes nicht-konstante Polynom f vom grad ≥ 1 eine Nullstelle hat (und somit in Linearfaktoren zerfällt)

d.h. $f = c \cdot \prod_{i=1}^{n} (X - \alpha_i)$, $c \in K^\times$, $\alpha_i \in K$.

Bemerkung: • $\mathbb{C}$ ist algebraisch abgeschlossen ("Fundamentalsatz der Algebra" Beweis, siehe Funktionentheorie)

• Ist K algebraisch abgeschlossen so ist K unendlich.
Denn, ist K endlich, so ist $1 + \prod_{\alpha \in K} (X - \alpha) \in K[X]$ ein Polynom P mit $P(\alpha) = 1 \ \forall \alpha \in K$, hat also keine Nullstelle.

Lemma 3.16 Ein Körper K ist genau dann alg. abgeschlossen falls aus L/K algebraisch folgt, dass $K = L$ ist.

Beweis: Sei K alg. abgeschlossen und $\alpha \in L$. Dann ist α eine Nullstelle von $f \in K[X]$. Nach Voraussetzung liegen alle Nullstellen von f in K, also $\alpha \in K$ und daher $L = K$. Umgekehrt, sei $f \in K[X]$ nicht konstant. Dann existiert endl. $\Rightarrow$ alg. Erweiterung L sodass f eine Nullstelle in L hat.
Da $L = K$ hat f eine NS in K ∎

Satz 3.17 Sei K ein Körper. Dann existiert eine alg. Erweiterung L/K mit L algebraisch abgeschlossen.

Beweis: Für den Beweis brauchen wir folgende Konstruktion: sei M eine Menge. Dann existiert ein Ring $K[M]$ mit folgender universeller Eigenschaft (Ringe):
$\mathrm{Hom}_{\mathrm{Ring}}(K[M], L) \xrightarrow{\cong} \mathrm{Hom}_{\mathrm{Ring}}(K, L) \times \prod_{M} L$, induziert von $K \hookrightarrow K[M]$ und $M \hookrightarrow K[M]$ (Mengen)

Für endliches M kann man $K[M]$ induktiv definieren:
$K[m_1, \dots, m_n] = K[m_1, \dots, m_{n-1}][m_n]$
Für unendliches M möchte man sagen $K[M] = \bigcup_{\substack{M' \subseteq M \\ \text{endlich}}} K[M']$
aber diese Vereinigung ergibt natürlich (formal) keinen Sinn. Man kann dies formal definieren als geeigneter Quotient der disjunkten Vereinigung, und im Sinne von Kategorientheorie hat man dann, dass
$K[M] = \operatorname{colim}_{\substack{M' \subseteq M \\ M' \text{ endlich}}} K[M']$

Jede endliche Familie von Elementen

in $K[M]$ ist in $K[M']$ für $M' \subseteq M$ endlich, wir "wissen" also wie man in $K[M]$ addiert und multipliziert.

Nun zum Beweis: Betrachte die Menge $M = \{f \in K[X] \mid \text{grad}(f) \geq 1\}$ und $K[M]$. wir schreiben X_f für das zu $f \in M$ gehörende Element von $K[M]$. Dann ist $f(X_f) \in K[M]$.
Sei $I = (f(X_f) \mid f \in M)$ das von allen $f(X_f)$ aufgespannte Ideal. Wir zeigen: $I \subsetneq K[M]$. falls nicht, so existieren $b_1, \dots, b_n \in K[M]$ und $f_1, \dots, f_n \in M$ mit $1 = \sum_{i=1}^{n} b_i f_i(X_{f_i}) \in K[M]$

Sei K'/K eine endl. erweiterung in der $\prod_{i=1}^{n} f_i$ in Linearfaktoren zerfällt (und damit f_i für jedes $i = 1, \dots, n$) und sei α_i eine Nullstelle von f_i in K'. Betrachte die Abbildung
$K'[M] \to K'$ welche $f \in M$ auf 0 schickt falls $f \notin f_1, \dots, f_n$ und welche f_i auf α_i schickt.
Dann gilt $1 = \sum_{i=1}^{n} b_i \underbrace{f_i(\alpha_i)}_{=0} = 0$ ↯.

Nach Zorn's Lemma existiert ein maximales Ideal $m \subseteq K[M]$ mit $I \subseteq m$ (das Urbild eines max. Ideals in $K[M]/I$)
Betrachte $K_1 = K[M]/m$, ein Körper, $K \to K_1$ macht K_1 zu einem Erweiterungskörper.
Wir zeigen: Ist $f \in K[X]$ mit $\text{grad}(f) \geq 1$, so existiert eine Nullstelle von f in K_1, nämlich das Bild von $X_f \in K[M]$ unter der kan. Projektion $K[M] \xrightarrow{\pi} K_1$ (selbes Argument wie im Beweis von 3.14)
Außerdem gilt, dass $K_1 = K(\{\alpha_f'' \mid f \in M\})$ und α_f ist algebraisch über K ($\pi(X_f)$ Nullstelle von f). somit ist jedes Element von K_1 algebraisch über K.
Wir haben gezeigt: Zu einem Körper K existiert eine algebraische Erweiterung $K \subseteq K_1$ sodass jedes Polynom $f \in K[X]$ mit $\text{grad}(f) \geq 1$ in K_1 eine Nullstelle hat.
Iterieren gibt eine Folge von algebraischen Erweiterungen
$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots$

Wir wollen wieder $L = \bigcup_{n \geq 0} K_i$ definieren (formal als Quotient der disjunkten Vereinigung). Jedes Element von L lebt in einem K_i. Daher folgt aus 3.12, dass L/K algebraisch ist.

Wir zeigen schließlich, dass L algebraisch abgeschlossen ist:

Sei $f \in L[X]$. Schreibe $f = \sum_{i=0}^{n} a_i X^i$. Es folgt, dass $\exists j \geq 1$ sodass $f \in K_j[X]$. Nach Construktion hat f eine Nullstelle in K_{j+1}, daher auch in L ☐

Wir wollen nun zeigen, dass je zwei algebraische Abschlüsse eines Körper (nicht-kanonisch) isomorph sind.

Sei $\sigma: K \to L$ eine Körpererweiterung und K'/K eine weitere.

Eine Fortsetzung σ' von σ entlang $K \subseteq K'$ ist eine Ringabbildung $\sigma': K' \to L$ sodass das Diagram

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & L \\ \downarrow & \nearrow_{\sigma'} & \\ K' & & \end{array}$$

kommutiert.

Sind Bezeichne auch mit $\sigma: K[X] \to L[X]$ den von σ induzierten Homomorphismus, d.h. für $f = \sum_{i \geq 0} a_i X^i$ ist $\sigma(f) = \sum_{i \geq 0} \sigma(a_i) X^i$.

Es gilt $\operatorname{grad}(\sigma(f)) = \operatorname{grad}(f)$, und ist $\alpha \in K$ eine Nullstelle von f so ist $\sigma(\alpha)$ eine Nullstelle von $\sigma(f)$, denn das Diagram

$$\begin{array}{ccc} K[X] & \xrightarrow{\sigma} & L[X] \\ \downarrow X \mapsto \alpha & & \downarrow X \mapsto \sigma(\alpha) \\ K & \xrightarrow{\sigma} & L \end{array}$$

kommutiert, α NS von $f \iff f \in \ker(X \mapsto \alpha)$, $\sigma(f)$ und $\sigma(\alpha)$ NS von $\sigma(f) \iff \sigma(f) \in \ker(X \mapsto \sigma(\alpha))$

Lemma 3.18 Sei K ein Körper, $K' = K(\alpha)$ eine einfache algebraische Erweiterung von K, $q_\alpha \in K[X]$ das Minimalpolynom von α. Sei $\sigma: K \to L$ eine weitere Körpererweiterung. Dann ist

$$\left\{ \begin{array}{l} \sigma': K' \to L \\ \text{Fortsetzung von } \sigma \end{array} \right\} \xrightarrow{\cong} \{ \beta \in L \mid \beta \text{ Nullstelle von } q_\alpha^\sigma \}$$

$$\sigma' \longmapsto \sigma'(\alpha)$$

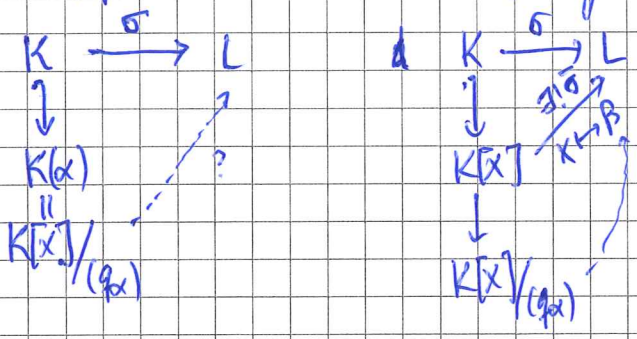
eine Bijektion.

Bemerkung: Insbesondere gilt

$$\left| \left\{ \begin{matrix} \sigma' : K' \to L \\ \text{Fortsetzung} \\ \text{von } \sigma \end{matrix} \right\} \right| = \left| \{ \beta \in L \mid \beta \text{ NS von } \sigma(q_\alpha) \} \right| \leq \operatorname{grad}(q_\alpha)$$

Beweis: die behauptete Abbildung ist wohldefiniert: sei $i : K \hookrightarrow K' = K(\alpha)$.
ist σ' eine Fortsetzung von σ so gilt $\sigma'(\alpha)$ eine Nullstelle von $\sigma'(i(q_\alpha)) = \sigma(q_\alpha)$ da α eine Nullstelle von $i(q_\alpha)$ ist.

wir definieren eine inverse Abbildung wie folgt: sei $\beta \in L$ NS von q_α



wir brauchen:
$\bar{\sigma}(q_\alpha) = 0$
aber $\bar{\sigma}(q_\alpha) = \bar{\sigma}(q_\alpha | \beta) = 0$
nach Voraussetzung.

es existiert also zu $\beta \in L$ NS von q_α genau eine Ringabbildung $K(\alpha) \xrightarrow{\sigma_\beta} L$ sodass $K \to K(\alpha) \xrightarrow{\sigma_\beta} L$ gleich σ ist und $\sigma_\beta(\alpha) = \beta$.

diese Konstruktionen sind per Konstruktion invers zu einander. ∎

Satz 3.19 Sei K'/K eine alg. Körpererw. und L/K mit L alg. abgeschlossen.
Es gelten: a) es existiert eine Fortsetzung $K' \xrightarrow{\sigma'} L$ von $K \xrightarrow{\sigma} L$
b) ist K' algebraisch abgeschlossen und L/K algebraisch so ist σ' ein Isomorphismus.

Korollar 3.20 sei K ein Körper und seien $\bar{K}_1$ und $\bar{K}_2$ alg. Abschlüsse von K.
Dann existiert ein Isomorphismus $\sigma' : \bar{K}_1 \xrightarrow{\cong} \bar{K}_2$ sodass $\sigma'|_K = \mathrm{id}_K$.

Beweis Kor: $L = \bar{K}_2$ und $K' = \bar{K}_1$ in Satz 3.19 ∎

Beweis Satz: betrachte die Menge $S = \{ (E, \sigma_E) \mid K \subseteq E \subseteq K' \text{ Zwischenkörper}, \sigma_E : E \to L \text{ sodass } \sigma_E|_K = \sigma \}$

da $(K, \sigma) \in S$ ist $S \neq \emptyset$.
definiere $(E, \sigma_E) \leq (E', \sigma_{E'}) :\Leftrightarrow E \subseteq E'$ und $\sigma_{E'}|_E = \sigma_E$

für $(E_1, \sigma_{E_1}) \leq (E_2, \sigma_{E_2}) \leq \dots$

existiert eine ~~maximales Element~~ obere Schranke $E = \bigcup_{i \geq 0} E_i \subseteq K'$

und $\sigma_E|_{E_i} = \sigma_{E_i}$.

Zorns Lemma $\Rightarrow$ $\exists$ maximales Element (E, σ_E) in S.

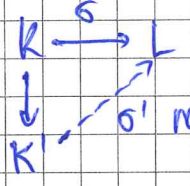
Wir zeigen: $K' = E$ und somit a) des Satzes.

Falls $E \subsetneq K'$ so existiert $\alpha \in K' \setminus E$. da α alg / K ist α auch alg / E und wir bekommen $E \subsetneq E(\alpha) \subseteq K'$.

Nach 3.18 (α ist NS des minimalpolynoms $f_\alpha \in E[X]$)

existiert eine Fortsetzung von σ_E auf $E(\alpha)$ im Widerspruch zur maximalität von E. wir beweisen nun b)

betrachte



$\mathrm{Im}(\sigma') \subseteq L$ Unterkörper, isomorph (vermöge σ') zu K', also algebraisch abgeschl.

$\Rightarrow K \subseteq K' \subseteq L$ L/K ~~endlich~~ algebraisch $\Rightarrow L/K'$ algebraisch.

also $L = K'$ da K' algebraisch abgeschlossen (3.16) ∎

Zerfällungskörper

Definition 3.21 Sei K ein Körper, $\mathcal{F} = \{P_i\}_{i \in I}$ eine Familie von nicht konstanten Polynomen in $K[X]$

L/K heißt Zerfällungskörper von $\mathcal{F}$ über K falls

a) $\forall i \in I$ zerfällt P_i in L in Linearfaktoren

b) L wird von den Nullstellen aller P_i erzeugt.

Ist L/K der Zerfällungskörper einer Familie von Polynomen, so heißt L/K normal.

Bemerkungen: a) sagt, dass alle NS aller P_i's in L liegen und

b) sagt, dass L der kleinste Körper mit dieser Eigenschaft ist.

~~unendliche~~ normale erweiterungen sind algebraisch, sogar endlich falls $\mathcal{F}$ aus endlich vielen P_i's bsth.

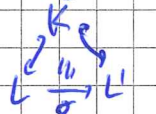
Beispiel: 1) $\mathcal{F} = \{P\}$ und seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von P in einem alg. Abschluss $\bar{K}$ von K, so gilt, dass

$K \subseteq \underbrace{K(\alpha_1, \dots, \alpha_n)}_{=: L_{\mathcal{F}}} \subseteq \bar{K}$ ein Zerfällungskörper von $\mathcal{F}$ ist.

2) ist $\mathcal{F} = \{P_1, \dots, P_n\}$ so sind die Nullstellen aller P_i's genau die Nullstellen von $P_1 \cdot \dots \cdot P_n$. die Zerfällungskörper von $\{P_1, \dots, P_n\}$ und $\{P_1 \cdot \dots \cdot P_n\}$ sind also in $\bar{K}$, also $K(\alpha_j)_{j \in J}$, α_j die NS von $P_1 \cdot \dots \cdot P_n$

3) ist $\mathcal{F}$ beliebig, so ist $L_{\mathcal{F}} = \bigcup_{\substack{\mathcal{F}' \subseteq \mathcal{F} \\ \mathcal{F}' \text{endlich}}} L_{\mathcal{F}'} \subseteq \bar{K}$. ein Zerfällungskörper von $\mathcal{F}$ ($\leftarrow$ wie in 1) oder 2))

Seien L, L' Körpererw. von K. Eine Ringabbildung $\sigma: L \to L'$ heißt K-Homomorphismus, falls $\sigma|_K = \mathrm{id}$, also σ kommutiert.



Satz 3.22 Seien L_1, L_2 Zerfällungskörper einer Familie $\mathcal{F}$ nicht-konst. Polynome in K. Sei $\bar{L}_2$ ein algebraischer Abschluss von L_2 und $\sigma: L_1 \to \bar{L}_2$ ein K-Homomorphismus (ein solches σ existiert nach 3.19). Dann ist $\sigma(L_1) = L_2$ und somit $\sigma: L_1 \to L_2$ ein Isomorphismus.

Beweis wähle wir auch $\bar{L}_1 (= \bar{K})$ so gilt $L_1 = \bigcup_{\substack{\mathcal{F}' \text{endlich} \\ \mathcal{F}' \subseteq \mathcal{F}}} L_1^{\mathcal{F}'} \subseteq \bar{L}_1$

es genügt dann den Satz zu beweisen wenn $\mathcal{F}$ endlich und daher (siehe Beispiel) von der Form $\mathcal{F} = \{P\}$ ist, oBdA P normiert.

Sei $n = \mathrm{grad}(P)$ und $\alpha_1, \dots, \alpha_n$ die NS von P in L_1, $\beta_1, \dots, \beta_n$ die NS von P in L_2.

wir kriegen dann $L_1 = K(\alpha_1, \dots, \alpha_n)$, $L_2 = K(\beta_1, \dots, \beta_n)$.

Sei nun $\sigma: L_1 \to \bar{L}_2$ K-Homomorphismus.

Dann gilt $\sigma(P) = P$ (da σ auf den Koeff. von P, welche aus K kommen die Identität ist). es gilt daher

$$\prod_{i=1}^{n} (X - \sigma(\alpha_i)) = \prod_{i=1}^{n} (X - \beta_i) \in \bar{L}_2[X]$$

Aus der Eindeutigkeit der Primfaktorzerlegung in $\bar{L}_2[X]$ folgt dass $\sigma(\alpha_i) = \beta_{j(i)}$ für ein eindeutig $j \in \{1,\dots,n\}$.
σ schickt daher $\{\alpha_1,\dots,\alpha_n\}$ bijektiv auf $\{\beta_1,\dots,\beta_n\}$ und somit folgt, dass $\sigma(L_1) \subseteq L_2$ ∎

Wir haben folgende Charakterisierung normaler Körpererweiterungen.

Proposition 3.23 Sei L/K algebraisch. Dann sind äquivalent

1) L/K ist normal.
2) ist $f \in K[X]$ irreduzibel und hat eine Nullstelle[a] in L, so zerfällt f in L in Linearfaktoren
3) ist $\sigma: L \to \bar{L}$ ein K-Homomorphismus ($\bar{L}$ alg. Abschluss von L) so ist $\sigma(L) = L$ und $\sigma: L \xrightarrow{\cong} L$

[a] sei $\beta \in \bar{L}$ Nullstelle von f.

Beweis: 3) $\Rightarrow$ 2) nach 3.18 $\exists$ Abbildung $K(\alpha) \xrightarrow{\bar{\sigma}} \bar{L}$ s.d. $\bar{\sigma}(\alpha) = \beta$ fortgesetzt. Wir zeigen, dass $\beta \in L$ gilt.
Nach 3.19 $\exists$ $K(\alpha) \subseteq L \xrightarrow{\bar{\sigma}} \bar{L}$, also existiert eine Erweiterung von σ auf L.
nach 3) gilt $\sigma(L) \subseteq L$ und damit $\beta = \bar{\sigma}(\alpha) \in L$.

2) $\Rightarrow$ 1) sei $\{a_i\}_{i\in I}$ eine Familie von alg. Elementen von L, welche L erzeugen, also sodass $L = K(\{a_i\}_{i\in I})$
ist q_i das Minimalpolynom von a_i so zerfällt q_i in Linearfaktoren in L (da 2) gilt). L ist also der Zerfällungskörper von $\{q_i\}_{i\in I}$
1) $\Rightarrow$ 3) Sei $\sigma: L \to \bar{L}$ K-Homom. und L der Zerfällungskörper von $\mathcal{F} = \{p_i\}_{i\in I}$ in $\bar{L}$
es folgt, dass $\mathrm{Im}(\sigma) \subseteq \bar{L}$ auch ein Zerfällungskörper von $\mathcal{F}$ ist.
es folgt dass $\mathrm{Im}(\sigma) = L$ (3.22) ∎

Beispiele 3.24 a) ist L/K mit $[L:K] = 2$, so ist L/K normal:
Sei $\alpha \in L \setminus K$, q_α sein minimalpolynom. Es ist $K(\alpha) = L$ (aus dim. grüden) und somit $\mathrm{grad}(q_\alpha) = 2$. Da α NS von q_α und $\mathrm{grad}(q_\alpha) = 2$ zerfällt q_α in Linearfaktoren. $\Rightarrow$ L = Zerfällungskörper von $\{q_\alpha\}$.

b) sei $P = X^4 - 4X^2 - 5 \in \mathbb{Q}[X]$

über $\mathbb{C}$ faktorisiert P als $(X^2-5)(X^2-1) = (X-\sqrt{5})(X+\sqrt{5})(X-i)(X+i)$

daher ist $\mathbb{Q}(\sqrt{5}, i)$ ein Zerfällungskörper.

Da $\sqrt{5} \notin \mathbb{Q}$ und $i \notin \mathbb{Q}(\sqrt{5})$ ist X^2-5 das Minimalpolynom von $\sqrt{5}$ über $\mathbb{Q}$ und $X^2+1 \in \mathbb{Q}(\sqrt{5})[X]$ ← von i über $\mathbb{Q}(\sqrt{5})$

$\Rightarrow [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})]$. $\Rightarrow [\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}] = 4$

In dem Diagram

$$\begin{array}{ccc} & & \mathbb{Q}(\sqrt{5}) \\ & \subseteq & \in \\ \mathbb{Q} & & \mathbb{Q}(\sqrt{5}, i) \\ & \in \quad \mathbb{Q}(i) & \subseteq \end{array}$$

sind alle Erw. vom grad 2 und daher normal.

c) betrachte $\sqrt[4]{2} \in \mathbb{R} \setminus \mathbb{Q}$. Wegen $(\sqrt[4]{2})^2 = \sqrt{2}$ haben wir

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ und beide Erweiterungen sind vom grad 2, also normal.

das minimalpolynom von $\sqrt[4]{2}$ ist $X^4-2 \in \mathbb{Q}[X]$

aber X^4-2 zerfällt in $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren:

in $\mathbb{C}$ gilt $X^4-2 = (X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})$

aus Satz 3.23 b) folgt, dass $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht normal ist.

Der Zerfällungskörper von X^4-2 ist $\mathbb{Q}(\sqrt[4]{2}, i)$ und wir haben

$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$.

Ist L/K eine alg. Körpererweiterung so ist ein <u>normaler Abschluss</u> von L/K eine alg. Erweiterung $L \subseteq N$ sodass N/K normal ist und minimal mit dieser Eigenschaft, d.h. falls $L \subseteq N' \subseteq N$ alg. und N'/K normal $\Rightarrow N' = N$.

Lemma 3.25 L/K alg. Körpererweiterung

a) es gibt einen bis auf (nicht-kanonische) Isomorphie eindeutig bestimmten normalen Abschluss N/K.

b) ist L/K endlich, so ist auch N/K endlich.

c) ist M/L alg. und M/K normal, so gibt es $L \subseteq N \subseteq M$ sodass N/K normaler Abschluss ist.

Beweis: schreibe $L = K(\{a_i\}_{i\in I})$ wir $a_i \in L$ geeignet $(i \in I)$.

sei q_i das Minimalpolynom von a_i über K. sei $\bar{L}$ ein algebraischer Abschluss von L (und somit auch von K).

sei $N = K(\{\text{alle Nullstellen (aller) von } q_i\}_{i\in I}) \subseteq \bar{L}$ in $\bar{L}$

dann ist N ein Zerfällungskörper von $\{q_i\}_{i\in I}$ und somit normal / K.

ist $K \subseteq N' \subseteq N$ mit N' normal, so müssen alle NS von allen q_i's in N' leben (3.23 2): $a_i \in L \subseteq N'$ ist NS von q_i).

daher ist N ein normaler Abschluss von L/K.

wir sehen, dass falls L/K endlich $\Rightarrow$ können I für $\{a_i\}_{i\in I}$ endlich wählen $\Rightarrow N/K$ endl. erzeugt, aber auch algebraisch und daher endlich.

sei nun N' ein weiterer normaler Abschluss von L/K.

wir konstruieren eine Ringabbildung $N \to N'$ kompatibel mit den jeweiligen Inklusionen von L, dh. eine Fortsetzung von $L \to N'$ entlang $L \subseteq N$. Dafür sehen wir, dass N/L und N'/L alg. sind und daher $\bar{N}$ und $\bar{N}'$ auch alg. Abschlüsse von L sind.

betrachten wir dann $L \subseteq N \subseteq \bar{N}$ so gibt es nach
$\cap\!|$
N'
$\cap\!|$
$\bar{N}'$

Satz 3.19 b) einen Isomorphismus $f: \bar{N} \xrightarrow{\sim} \bar{N}'$ sodass $f|_L = id_L$.

wir behaupten, dass $f(N) \subseteq N'$. da N erzeugt ist von Nullstellen von $\{q_i\}_{i\in I}$ und $\forall i \in I$ q_i eine Nullstelle in L hat $(q_i \in K[X])$

folgt, dass es genügt zu sehen, dass falls α_{ij} eine Nullstelle von q_i in $\bar{N}$ ist, so ist $f(a_{ij}) \in N'$. Da N' ein normaler Abschluss von L/K ist, $f(a_{ij}) \in \bar{N'}$ eine Nullstelle von $q_i \cdot (= f(q_i)$ da $f|_L = id_L)$ und q_i eine Nullstelle in $\bar{N'}$ hat, welche in L liegt, folgt, dass alle Nullstellen von q_i in $\bar{N'}$ in N' liegen.
Daher folgt, $f(N) \subseteq N'$. Es gilt also
$K \subseteq L \subseteq f(N) \subseteq N'$ und da $f(N) \overset{f}{\underset{\cong}{\leftarrow}} N$ über L (also $f_L = id_L$)
folgt, dass $f(N)$ eine normal über K ist. Aus der Minimalität der normalen Abschlüsse N' folgt daher $f(N) = N'$ und damit ist $f: N \to N'$ ein Isomorphismus.
Teil c) erscheint auf dem kommenden Übungszettel.

Separable Körpererweiterungen

Sei K ein Körper, $f \in K[x]$ $\text{grad}(f) > 0$. f heißt SEPARABEL über K falls f in einem algebraischen Abschluss $\bar{K}$ keine mehrfachen Nullstellen hat (da je zwei alg. Abschlüsse isomorph sind, ist diese Bedingung unabhängig von der Wahl von $\bar{K}$).

Lemma 3.26 Sei $f \in K[x]$, $\text{grad}(f) > 0$. Es gelten
a) $\alpha \in \bar{K}$ ist mehrfache Nullstelle von $f \iff \alpha$ ist Nullstelle von $\text{ggT}(f, f')$
b) ist f irreduzibel, so hat f eine mehrfache Nullstelle in $\bar{K} \iff f' = 0$.

Beweis: a) Lemma 2.29 sagt α ist mehrfache Nullstelle $\iff \alpha$ ist Nullstelle von f und $f' \iff (x-\alpha)$ teilt f und $f' \iff (x-\alpha) \mid \text{ggT}(f, f')$.
b) nach a) hat f mehrfache Nullstelle $\alpha \iff \alpha$ ist NS von f und f'
da f irreduzibel $\Rightarrow f =$ Minimalpolynom von α. da $\text{grad}(f') < \text{grad}(f)$ und α NS von f' folgt, dass f' im Ideal enthalten ist welches von f aufgespannt wird und daher 0 ist. ∎

Bemerkungen a) ist $\mathrm{char}(K)=0$ und f irreduzibel, so ist $\mathrm{grad}(f)\geq 1$ und daher $f'\neq 0$. Aus 3.26 b) folgt dass irreduzible Polynome über char. 0 Körpern separabel sind.

b) ist $\mathrm{char}(K)=p$, so gilt für $f\in K[X]$: Sei $\Phi: K[X]\to K[X]$, $X\mapsto X^p$

$f'=0 \iff \exists g\in K[X]$ sodass $f=\Phi(g)$, dh. $f(X)=g(X^p)$

denn: sei $f=\sum_{i=0}^{n} a_i X^i$ so ist $f'=\sum_{i=0}^{n} i\cdot a_i X^{i-1}$

und somit $f'=0 \iff i\cdot a_i=0$ in K. $\forall i\geq 1$

$\iff i=0$ falls $a_i\neq 0$ $(\forall i\geq 1)$

da $0=i\in K \iff p\mid i$ sehen wir, dass $a_i\neq 0 \Rightarrow i=pk$

umgekehrt ist für $f=g(X^p)$ offenbar $f'=0$ da $(X^{pk})'=pk\cdot X^{pk-1}=0$.

Für einen Körper K von charakteristik p ist die Abbildung

$\varphi: K\to K$, $a\mapsto a^p$ ein Ringhomomorphismus $(\text{da: } (a+b)^p=a^p+b^p)$

der **FROBENIUS HOMOMORPHISMUS**

Lemma 3.27 Sei K ein Körper mit $\mathrm{char}(K)=p>0$. Dann ist jedes irreduzible Polynom $f\in K[X]$ separabel $\iff$ $\varphi: K\to K$ ist surjektiv (und damit ein Isom.).

Beweis: "$\Rightarrow$" betrachte das Polynom $f=X^p-a\in K[X]$ wobei $a\in K$ beliebig.

sei α eine NS von f in $\bar{K}$. und q_α sein minimalpolynom

nach Voraussetzung ist q_α separabel und $q_\alpha \mid f$ in $K[X]$

In $\bar{K}[X]$ gilt dann $q_\alpha \mid f = (X-\alpha)^p$.

da q_α separabel muss gelten $q_\alpha=(X-\alpha)$ und daher $\alpha\in K$.

aus $\alpha^p=a$ folgt, dass φ surjektiv ist.

"$\Leftarrow$" sei $f\in K[X]$ irreduzibel und α NS von f in $\bar{K}$. wir müssen zeigen dass α keine mehrfache Nullstelle ist. Nach 3.26 b) ist dies der Fall $\iff$ $f'=0$. Nach Bemerkung b) oben ist dies der Fall $\iff$ $\exists g\in K[X]$ sodass $f(X)=g(X^p)=\sum_{i=0}^{n} a_i X^{pi}$. Da Frobenius surjektiv existieren b_i sodass $b_i^p=a_i$. es folgt dass $f=\sum_{i=0}^{n} b_i^p X^{pi}=\left(\sum_{i=0}^{n} b_i X^i\right)^p$ sodass f reduzibel ist. also kann α keine mehrfache NS sein. ∎

Definition 3.28 Sei L/K alg. Erweiterung. $\alpha \in L$ heißt SEPARABEL falls α NS eines separablen Polynoms in $K[X]$ ist.
L/K heißt SEPARABEL falls alle $\alpha \in L$ separabel sind.
Der Körper K heißt PERFEKT falls alle algebraischen Erweiterungen separabel sind.

Bemerkungen a) $\alpha \in L$ ist separabel $\Leftrightarrow$ das Minimalpolynom von α ist separabel
b) Körper von char 0 sind perfekt, ein Körper K von char. p ist perfekt
$\Leftrightarrow$ Frobenius $\varphi: K \to K$ ist ein Isomorphismus;
sei L/K alg. und $\alpha \in L$ mit Minimalpolynom q_α. Dann ist q_α irreduzibel; falls $\mathrm{char}(K)=0$ ist q_α separabel nach Bem. a) S.50 und falls $\mathrm{char}(K)=p>0$ ist q_α separabel nach Lemma 3.27.

Beispiel 3.29 • Sei $K = \mathbb{F}_p(X) = Q(\mathbb{F}_p[X])$, dann ist $\mathrm{char}(K)=p$ und K nicht perfekt [illegible] X ist nicht im Bild von Frobenius [illegible]
• endliche Körper sind perfekt

Definition 3.30 Sei L/K alg. und sei $\mathrm{Hom}_K(L,\bar{K}) = \{\sigma: L \to \bar{K} \mid \sigma|_K = \text{inclusion}\}$

die Menge der K-Homomorphismen von L in einen alg. Abschluss von K.
Der SEPARABILITÄTSGRAD von L/K ist

$$[L:K]_s := |\mathrm{Hom}_K(L,\bar{K})|$$

Bem: ist $\bar{K}'$ ein weiterer alg. Abschluss von K, so existiert K-Isomorphismus $f: \bar{K} \xrightarrow{\cong} \bar{K}'$. Dieser induziert eine Bijektion $\mathrm{Hom}_K(L,\bar{K}) \cong \mathrm{Hom}_K(L,\bar{K}')$ damit ist obige Definition von $[L:K]_s$ unabhängig von der Wahl von $\bar{K}$.

Bemerkung: ist L/K alg. so sei $\mathrm{Aut}_K(L) = \{\sigma: L \xrightarrow{\cong} L \mid \sigma|_K = \mathrm{id}_K\}$
dies ist eine Gruppe. die Zuordnung

$$\begin{aligned}\mathrm{Aut}_K(L) \times \mathrm{Hom}_K(L,\bar{K}) &\to \mathrm{Hom}_K(L,\bar{K}) \\ (\varphi, f) &\longmapsto f\circ\varphi^{-1}\end{aligned}$$

definiert ein Gruppenwirkung von $\mathrm{Aut}_K(L)$ auf $\mathrm{Hom}_K(L,\bar{K})$.
Übungszettel: ist L/K normal, so ist $\mathrm{Hom}_K(L,\bar{K})$ ein $\mathrm{Aut}_K(L)$-Torsor
und insbesondere gilt: $[L:K]_s = |\mathrm{Aut}_K(L)|$.

Wir zeigen später: ist L/K (zusätzlich) separabel, so gilt $[L:K]_s = [L:K]$ ($= |\mathrm{Aut}_K(L)|$)

Beispiele:
- $\mathbb{C}/\mathbb{R}$ ist normal ($[\mathbb{C}:\mathbb{R}]=2$, + Bsp 3.24) und separabel ($\mathrm{char}\,\mathbb{R}=0$). $\Rightarrow |\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2$ und daher $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \cong \mathbb{Z}/2$ mit $(x \mapsto \bar{x})$ als nicht-trivialem Element.
- genauso: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ normal separabel. $(a+b\sqrt{2} \mapsto a-b\sqrt{2}) \neq \mathrm{id}$ und element von $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$.

Lemma 3.31 Seien L/K einfache alg. Erweiterung, $L = K(\alpha)$, q_α das Minimalpolynom von α. Dann gelten

a) $[L:K]_s = \left|\{\beta \in \bar{K} \text{ Nullstelle von } q_\alpha\}\right|$

b) α ist separabel $\iff [L:K]_s = [L:K]$

c) ist $\mathrm{char}(K) = p > 0$ und α eine Nullstelle von q_α mit Vielfachheit p^r so gilt $[L:K] = p^r \cdot [L:K]_s$

Beweis: a) $[L:K]_s = \left|\mathrm{Hom}_K(L,\bar{K})\right| = \left|\left\{\begin{array}{l}\sigma: L \to \bar{K} \\ \text{Fortsetzung} \\ \text{von } K \to \bar{K}\end{array}\right\}\right| \overset{3.18}{=} \left|\{\beta \in \bar{K} \text{ Nullstelle von } q_\alpha\}\right|$.

b) ist α separabel so ist die Anzahl der NS von q_α in $\bar{K}$ genau $\mathrm{grad}(q_\alpha)$, was nach 3.8 genau $[L:K]$ ist.

c) Auf dem Übungszettel zeigen wir dass die Vielfachheit aller NS eines irred. Polynoms gleich sind. (gleich 1 falls $\mathrm{char}(K)=0$ und von der Form p^r falls $\mathrm{char}(K)=p>0$)

Lemma 3.32 Seien $K \subseteq E \subseteq L$ alg. Erweiterungen. Dann gilt:

$$[L:K]_s = [L:E]_s \cdot [E:K]_s$$

Beweis: Sei $\bar{K}$ ein alg. Abschluss, sodass $K \subseteq E \subseteq L \subseteq \bar{K}$.

Betrachte die Abbildungen

$$\begin{array}{ccc} \mathrm{Hom}_K(L,\bar{K}) & \rightleftarrows & \mathrm{Hom}_K(E,\bar{K}) \times \mathrm{Hom}_E(L,\bar{K}) \\ \downarrow & \longmapsto & (f|_E, (\overline{f|_E})^{-1} \circ f) \\ \bar{g} \circ h & \longleftarrow\!\shortmid & (g,h) \end{array}$$

hierbei ist für $g \in \mathrm{Hom}_K(E,\bar{K})$, $\bar{g}$ eine Fortsetzung auf $\bar{K}$:

$$\begin{array}{ccc} E & \xrightarrow{g} & \bar{K} \\ \downarrow & \nearrow_{\bar{g}} & \\ K & & \end{array}$$

nach 3.19 a) und nach 3.19 b) ist $\bar{g}$ ein Isomorphismus.

Dann gelten: beide Abbildungen sind wohldefiniert: $(\overline{f|_E})^{-1} \circ f)|_E$ ist die kan. Inklusion

des weiteren gilt $\bar{g} \circ h|_E = g$; denn $h|_E$ = kan. Inklusion, also ist

$\bar{g} \circ h|_E = \bar{g}|_E = g$. Damit sieht man sofort, dass obige Abbildungen

invers zueinander sind. ∎

Bemerkung: Sei L/K endlich. Per Induktion über die Kardinalität eines endl. Erzeugendensystems folgt:

- ist $\mathrm{char}(K) = 0$, so gilt $[L:K]_s = [L:K]$
- ist $\mathrm{char}(K) = p > 0$, so gilt $[L:K]_s = p^n \cdot [L:K]_s$ für ein $n \geq 0$.

Insbesondere gilt immer: $[L:K]_s$ teilt $[L:K]$

Proposition 3.33 L/K endlich. Dann sind äquivalent:

a) L/K ist separabel

b) $L = K(a_1, \dots, a_n)$ für a_i separabel in L

c) $[L:K]_s = [L:K]$

Beweis: a) $\Rightarrow$ b) klar, da endlich $\Rightarrow$ endl. erzeugt und alle $a_i \in L$ sind separabel

b) $\Rightarrow$ c) selbes Argument wie in obiger Bemerkung

c) $\Rightarrow$ a) Sei $\alpha \in L$. $K \subseteq K(\alpha) \subseteq L$. aus $[L:K]_s = [L:K]$ und 3.32 folgt,

dass auch $[K(\alpha):K]_s = [K(\alpha):K]$, also α separabel nach 3.31.

Korollar 3.34 Sei L/K algebraisch, $\{a_i\}_{i\in I} \subseteq L$ sodass $L = K(\{a_i\}_{i\in I})$.
Dann sind äquivalent:

a) L/K ist separabel

b) $\forall i \in I$ ist $a_i \in L$ separabel.

Gelten diese, so gilt $[L:K]_s = [L:K]$.

Beweis: a) $\Rightarrow$ b) ist klar nach Definition.

b) $\Rightarrow$ a) sei $c \in L$. Dann $\exists\, I' \subseteq I$ endlich sodass $c \in K(\{a_i\}_{i\in I'})$. $\overset{b)\Rightarrow a)}{3.33}$ gibt dann dass c separabel über K ist.

Ist $[L:K] < \infty$ so gilt $[L:K]_s = [L:K]$ nach 3.33 falls a) oder b) gelten.
Sei also $[L:K] = \infty$. zz: $[L:K]_s = \infty$. Wegen $[L:K] = \infty$ folgt, dass es für $n \geq 1$ einen Zwischenkörper $K \subseteq E_n \subseteq L$ gibt mit $[E_n:K] \geq n$. $(\infty >)$
Dann ist E_n/K endlich und separabel $\Rightarrow [E_n:K]_s \geq n$. mit 3.32 folgt $[L:K] \geq n$ für alle $n \geq 1$. ∎

Korollar 3.35 Seien E/K und L/E alg. Erweiterungen. Dann gilt:

L/K separabel $\Leftrightarrow$ L/E und E/K separabel.

Beweis: "$\Rightarrow$" aus L/K sep. folgt sofort, dass E/K separabel.
um zu sehen, dass L/E separabel ist, sei $c \in L$. Dann ist q_c separabel als Element von $K[X]$ und daher auch als Element von $E[X]$ $(K \subseteq E)$.
"$\Leftarrow$" sei $\alpha \in L$ und q_α sein Minimalpolynom über E. sei E'/K eine endl. Erweiterung sodass alle Koeff. von q_α in E' sind $(K \subseteq E' \subseteq E)$ (z.B. die um den Koeff. erzeugte Erweiterung). es ist dann $E'(\alpha)/E'$ separabel und einfach.
(Minimalpolynom von α über E' ist immernoch q_α, also separabel).
Da $E' \subseteq E$ und E/K separabel $\Rightarrow E'/K$ separabel. außerdem $E'(\alpha)/K$ endlich.

$$[E'(\alpha):K]_s = [E'(\alpha):E']_s \cdot [E':K]_s$$
$$= [E'(\alpha):E'] \cdot [E':K] = [E(\alpha):K]$$

3.33 c) $\Rightarrow$ a) sagt, dass $E'(\alpha)/K$ separabel, also α separabel, also L/K separabel. ∎

Anwendungen

Proposition 3.36 Sei K ein Körper, $H \leq K^\times$ eine endliche UG. Dann ist H zyklisch.

Beweis: Sei $a \in H$ ein Element maximaler Ordnung, sagen wir $m = \text{ord}(a)$. Sei $H_m = \{h \in H \mid |h| \text{ teilt } m\}$. Betrachte $f = X^m - 1 \in K[X]$. Dann hat f höchstens m NS und $f(h) = 0 \ \forall h \in H_m$. $\Rightarrow |H_m| \leq m$. Da $a \in H_m$ gilt aber: $m = |\langle a \rangle| \leq |H_m| \leq m$, daher gilt $\langle a \rangle = H_m$.

angenommen $b \in H \setminus H_m$, sei $n = \text{ord}(b)$. Dann gilt $n \nmid m$.

Nach LA $\exists$ element $c \in H$ mit $\text{ord}(c) = \text{kgV}(n,m) > m$ ↯. Daher gilt $H = H_m$. ∎

Satz 3.37 (Satz vom primitiven Element) Sei L/K eine endliche, separable Körpererweiterung. Dann ist L/K einfach, d.h. $\exists \alpha \in L$ mit $L = K(\alpha)$.

(α heißt primitives Element zu L/K.) Bsp: $\mathbb{Q}/\mathbb{Q}$ algebraisch, endlich.

Beweis: Fallunterscheidung: ist $|K| < \infty$, so auch $|L|$ (denn L ist endl. dim K-VR). Daher ist nach 3.36 die Gruppe $L^\times$ zyklisch. Sei $a \in L^\times$ ein Erzeuger. Dann gilt offenbar $L = K(\alpha)$.

Sei also $|K| = \infty$, und nehmen wir an, dass $L = K(\alpha, \beta)$ gilt.

Sei $n = [L:K]_s$ und seien $f_1, \dots, f_n \in \text{Hom}_K(L, \bar{K})$ die paarweise versch. Elemente.

Betrachte $F = \prod_{\substack{i \neq j \\ i,j \in \{1,\dots,n\}}} (f_i(\alpha) - f_j(\alpha)) + (f_i(\beta) - f_j(\beta)) \cdot X \in \bar{K}[X]$.

da $f_i \neq f_j$ für $i \neq j$ und L von α, β erzeugt wird sehen wir, dass $F \neq 0$. Da F hat also nur endl. viele Nullstellen. Da $|K| = \infty$ folgt, es existiert $c \in K$ sodass $F(c) \neq 0$. Es folgt, dass für $i \neq j$ gilt

$$f_i(\alpha + c\beta) \neq f_j(\alpha + c\beta) \in \bar{K}.$$

ist g das minimalpolynom von $\alpha + c\beta \Rightarrow \text{grad}(g) \geq n$ denn die $f_i(\alpha + c\beta)$ bilden NS von g in $\bar{K}$ ($f_i|_K$ = kan. inklusion).

wir bekommen: $[L:K]_s = n \leq \text{grad}(g) = [K(\alpha + c\beta) : K] \leq [L:K]$

nach 3.33 gilt aber auch gleichheit $\Rightarrow [L : K(\alpha + \beta c)] = 1$ und somit $K(\alpha + \beta c) = L$. Im allgemeinen ist $K L = K(\alpha_1, \dots, \alpha_n)$ und die Behauptung folgt induktiv. ∎

Endliche Körper Ist K ein endlicher Körper, so ist sein Primkörper isom. zu $\mathbb{F}_p$ für $p>0$ prim, also $\mathrm{char}(K)=p$. es gilt also, dass $|K|=p^n$ für ein $n\geq 1$. Wir zeigen nun, dass es bis auf Isomorphie genau einen Körper mit p^n- vielen Elementen gibt (und beschreiben diesen).

Satz 3.38 Sei p prim und $n\geq 1$. Für $q=p^n$ existiert bis ein Körper $\mathbb{F}_q$ mit $|\mathbb{F}_q|=q$. $\mathbb{F}_q$ ist ein Zerfällungskörper von $X^q-X\in\mathbb{F}_p[X]$. Jeder endl. Körper F mit $|F|=q$ ist isomorph zu $\mathbb{F}_q$.

Beweis: Sei $\overline{\mathbb{F}}_p$ ein alg. Abschluss von $\mathbb{F}_p$. Betrachte die Menge aller NS von X^q-X in $\overline{\mathbb{F}}_p$. Da $0\neq -1=(X^q-X)'$ folgt, dass X^q-X separabel ist. sind α,β verschiedene Nullstellen so folgt aus $(\alpha+\beta)^q=\alpha^q+\beta^q=\alpha+\beta$ und $(\alpha\beta)^q=\alpha^q\beta^q=\alpha\beta$ dass $\alpha+\beta$ und $\alpha\cdot\beta$ auch Nullstellen sind. ist $0\neq\alpha$ so ist $\alpha^{-1}=\alpha^{q-2}$ wieder Nullstelle von X^q-X. Die Menge aller NS von X^q-X in $\overline{\mathbb{F}}_p$ bildet daher einen Unterkörper $\mathbb{F}_q\subseteq\overline{\mathbb{F}}_p$ mit q Elementen. $\mathbb{F}_q$ ist daher ein Zerfällungskörper von X^q-X über $\mathbb{F}_p$.

Ist K Körper mit $|K|=q$, so gilt $|K^\times|=q-1$. Ist $\alpha\in K^\times$, so ist daher $\alpha^{q-1}=1$ und somit $\alpha^q=\alpha$. Es folgt, dass K ein Zerfällungskörper von X^q-X über dem Primkörper von K ist. Da der Primkörper $\cong\mathbb{F}_p$ ist, folgt dass $K\cong\mathbb{F}_q$ nach 3.22 ☐

Ist K ein Körper mit $|K|=q=p^n$ so gilt: bis auf Isomorphie ist $\mathbb{F}_p\subseteq K$ und nach 3.19 gibt es einen $\mathbb{F}_p$-Homom $K\to\overline{\mathbb{F}}_p$, also $\mathbb{F}_p\subseteq K\subseteq\overline{\mathbb{F}}_p$, d.h. K kann als UK von $\overline{\mathbb{F}}_p$ aufgefasst werden.

Korollar 3.39 Sei $\mathbb{F}_p\subseteq\mathbb{F}_q\subseteq\overline{\mathbb{F}}_p$ mit $q=p^n$. Ist $q'=p^{n'}$ so gilt

$$\mathbb{F}_q\subseteq\mathbb{F}_{q'}\iff n\mid n'.$$

Die Erweiterungen $\mathbb{F}_q\subseteq\mathbb{F}_{q'}$ sind bis auf Isomorphie genau die endlichen Erweiterungen von $\mathbb{F}_q$.

Beweis: ÜA.