Gesamtskript
Kapitel II
zur Vorlesung
Algebra I

Prof.'in Dr. Salma Kuhlmann

Inhaltsverzeichnis für das Gesamtskript Kapitel 2[1]
zur Vorlesung: Algebra I (WiSe2020/2021)

Prof. Dr. Salma Kuhlmann

KAPITEL II: KÖRPERERWEITERUNGEN.

[1]Die Seitenzahlen in Klammern geben die Seitenzahl für die Suche mit Adobe Acrobat Reader an (unter dem Menü ANZEIGE – GEHE ZU – SEITE).

9 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Kapitel 2

KÖRPERERWEITERUNGEN

In diesem Kapitel werden wir besondere Körpererweiterungen kennenlernen. Wir werden algebraische Körpererweiterungen untersuchen, wo wir Nullstellen für Polynome finden. Insbesondere werden wir den Zerfällungskörper und den algebraischen Abschluss konstruieren. Wir werden die Vielfachheit einer Nullstelle, die wir schon in LA II gelernt haben, genauer betrachten, um separable Körpererweiterungen zu untersuchen. Im letztem Kapitel 4 werden wir dann Galois Erweiterungen behandeln, nachdem wir im Kapitel 3 zwischendurch die dafür notwendige Gruppentheorie studieren.
In diesem Skript werden wir im Abschnitt 12 algebraische, insbesondere endliche Körpererweiterungen studieren. Wir fangen an mit Erinnerungen (Definition 9.1, Bemerkung 9.2) aus LA I Skript 4.

Definition 9.1.

1. Die *Charakteristik* eines Körpers F, bezeichnet $\mathrm{Char}(F)$, ist die kleinste $n \in \mathbb{N}$ mit $n \cdot 1 = 0$. Falls ein solches n nicht existiert, dann setzen wir $\mathrm{Char}(F) = 0$.
2. Der *Primkörper* eines Körpers F ist der kleinste Teilkörper von F.

Bemerkung 9.2. Für die Charakteristik gilt: entweder $\mathrm{Char}(F) = p$ für eine Primzahl p, oder $\mathrm{Char}(F) = 0$. Wenn $\mathrm{Char}(F) = p$, dann ist der Primkörper $\mathbb{F}_p$, wenn $\mathrm{Char}(F) = 0$, dann ist der Primkörper $\mathbb{Q}$. ÜA.

§ 12 Algebraische Körpererweiterung

Definition 9.3.
Ein Körper K der ein Teilkörper F enthält heißt *Körpererweiterung* von F, bezeichnet mit K/F. Wir nennen F den *Grundkörper*.

Bemerkung 9.4. Ist K/F eine Körpererweiterung, dann ist K ein F-Vektorraum, wobei die Skalarmultiplikation $F \times K \to K$ die auf K definierte Multiplikation ist. ÜA.

Definition 9.5. Der *Grad (oder deg) einer Körpererweiterung* K/F, bezeichnet mit $[K : F]$, ist die Dimension von K als F-Vektorraum. Die Körpererweiterung heißt *endlich* falls $[K : F]$ endlich ist; sonst heißt die Körpererweiterung *unendlich* und wir schreiben $[K : F] = \infty$.

Beispiel 9.6.

1. Sei $F = \mathbb{F}_p$ und $K = \mathbb{F}_p(x) := \text{Quot}\ (\mathbb{F}_p[x])$. Dann ist $[K : F] = \infty$. ÜA.
2. $[\mathbb{C} : \mathbb{R}] = 2$: Jedes Element aus $\mathbb{C}$ lässt sich als Linearkombination von 1 und i darstellen und, wenn $a + bi = 0$ dann $a^2 + b^2 = (a + bi)(a - bi) = 0$; also $a = b = 0$. Somit bilden $1, i$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.
3. $[\mathbb{R} : \mathbb{Q}] = \infty$. Siehe ÜB.

Satz 9.7.
Seien F ein Körper und $p(x) \in F[x]$ ein irreduzibles Polynom. Dann existiert eine Körpererweiterung von F wo $p(x)$ eine Nullstelle besitzt.

Beweis:
Betrachte den Faktorring $\mathbb{K} := F[x]/ < p(x) >$. Da $p(x)$ irreduzibel ist und $F[x]$ ein Hauptidealring ist, ist das von $p(x)$ erzeugte Ideal ein maximales Ideal (Proposition 5.12 und Proposition 6.3). Daher ist $\mathbb{K}$ ein Körper (Proposition 3.1).

Sei $\varphi : F[x] \to \mathbb{K}$ die kanonische Projektion $a(x) \mapsto \overline{a(x)}$. Die Einschränkung $\varphi|F$ von φ auf F ist ein Körperhomomorphismus und daher ist sie injektiv (s. Korollar 2.7). Es folgt, dass F isomorph ist zu seinem Bild $\varphi(F) \subseteq \mathbb{K}$. Nun können wir F mit dem Teilkörper $\varphi(F)$ von $\mathbb{K}$ identifizieren. Somit ist F ein Teilkörper von $\mathbb{K}$, und die Einschränkung $\varphi|F$ ist nun die Identitätsabbildung Id. [1]

Sei $\varphi(x) = \overline{x}$ das Bild von x in $\mathbb{K}$. Es gilt $p(\overline{x}) = \overline{p(x)}$ (weil φ ein Homomorphismus ist mit $\varphi(a) = a$ für alle $a \in F$). Aber $p(x) \in < p(x) >$, also $0 = \overline{p(x)} = p(\overline{x})$. Dann ist $\overline{x} \in \mathbb{K}$ eine Nullstelle des Polynoms $p(x)$. □

Satz 9.8.
Sei $p(x) \in F[x]$ irreduzibel; $\deg p(x) = n, n \in \mathbb{N}$. Setze $\mathbb{K} := F[x]/ < p(x) >$. Es gilt $[\mathbb{K} : F] = n$.

Beweis:
Setze $\overline{x} := \theta$. Wir behaupten $O := \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ ist eine F-Basis für $\mathbb{K}$.

- Sei $a(x) \in F[x]$. Schreibe $a(x) = q(x)p(x) + r(x)$ mit $r(x) = 0$ oder $\deg r(x) < n$.
  Also $a(x)+ < p(x) >= r(x)+ < p(x) >$,

  $$\begin{array}{lccc} \text{d. h.} & \overline{a(x)} & = & \overline{r(x)} \\ & \shortparallel & & \\ \text{d. h.} & a(\overline{x}) & = & r(\overline{x}) \end{array}$$

  Schreibe $r(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in F$, i.e. $\overline{a(x)} =: r(\theta)$, also $\mathbb{K} \ni \overline{a(x)} \in \text{span}\ O$.

- O ist linear unabhängig über F: Seien $b_0, \ldots, b_{n-1} \in F$ mit $\sum b_i\theta^i = 0$.
  Setze $b(x) := \sum b_i x^i$. Es ist: $0 = b(\theta) = \overline{b(x)}$. Also $b(x) \in < p(x) >$ und $\deg b(x) < \deg p(x)$ und damit muss $b(x) = 0$ das Nullpolynom sein, i.e. $b_i = 0$ für alle $i = 0, \ldots, n - 1$. □

Bemerkung 9.9.
$\mathbb{K} = \{a(\theta)\ ;\ a(x) \in F[x], a(x) = 0 \text{ oder } \deg a(x) < n\}$, versehen mit den Verknüpfungen:
$a(\theta) + b(\theta) = (a + b)(\theta)$ für alle $a(x), b(x) \in F[x]$ und $a(\theta)b(\theta) = r(\theta)$; wobei $r(x) \in F[x]$ der Rest ist in E.A.: $a(x)b(x) = q(x)p(x) + r(x)$, $\deg r(x) < n$.

[1] Dies ist subtil: was bedeutet F mit seinem Bild in $\varphi(F) \subseteq \mathbb{K}$ zu identifizieren? Für $a \in F$ können wir einfach jedes Element $\varphi(a)$ als a umbenennen. Dies können wir machen weil $\varphi|F$ injektiv ist: für alle $a, a' \in F$: gilt: $\varphi(a) = \varphi(a')$ genau dann, wenn $a = a'$.

Definition 9.10.

(1) Sei K/F eine Körpererweiterung, und $S \subseteq K$. **Notation:** Setze $F(S)$ = der kleinste Teilkörper von K, der $F \bigcup S$ enthält, d.h. $F(S) := \bigcap\{L \mid L \subseteq K$ Teilkörper $; L \supseteq F \bigcup S\}$. $F(S)$ heißt der *Körper der von S über F erzeugt ist.*

(2) **Notation:** Wenn $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich ist, schreiben wir $L = F(\alpha_1, \ldots, \alpha_n)$. In diesem Fall sagen wir: L ist *endlich erzeugt über F.*

(3) Wenn $S = \{a\}$ heißt $L = F(a)$ eine *einfache Erweiterung* und a heißt ein *primitives Element* für die Körpererweiterung L/F.

Satz 9.11.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, $\alpha \in K$ eine Nullstelle von $p(x)$. Es ist: $F[x]/ < p(x) > \simeq F(\alpha)$.

Beweis: Setze $\mathbb{K} := F[x]/ < p(x) >$. Betrachte die Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{K} & \to & F(\alpha) \subseteq K \\ & a(x)+ < p(x) > & \mapsto & a(\alpha) \end{array}$$

- Das heißt $\varphi|F = Id|F$ (i.e. $\varphi(a) = a$ für alle $a \in F$) und $\varphi(a(\overline{x})) = a(\alpha)$ für alle $a(x) \in F[x]$. Insbesondere ist $\varphi(\overline{x}) = \alpha$.
- φ ist wohldefiniert: $a(x) \equiv b(x) \mod < p(x) > \Leftrightarrow a(x) - b(x) = p(x)q(x)$. Also $a(\alpha) - b(\alpha) = 0$ und damit $a(\alpha) = b(\alpha)$.
- $\varphi \neq 0$, also φ ist ein injektiver Ringhomomorphismus und damit definiert φ einen Isomorphismus $\varphi : F[x]/ < p(x) > \simeq im(\varphi)$. Nun ist $im(\varphi) \subseteq F(\alpha) \subseteq K$ ein Teilkörper von K und enthält $F \bigcup \{\alpha\}$. Somit ist $F(\alpha) \subseteq im(\varphi)$. Also $im(\varphi) = F(\alpha)$. □

Aus Satz 9.11 und Bemerkung 9.9 folgt

Korollar 9.12.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, $\deg p = n$ und $\alpha \in K$ eine Nullstelle von $p(x)$. Es ist $F(\alpha) = \{a(\alpha)\ ;\ a(x) \in F[x]; a(x) = 0$ oder $\deg a(x) < n\}$.

Korollar 9.13.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, und $\alpha, \beta \in K$ Nullstellen von $p(x)$. Es ist $F(\alpha) \simeq F(\beta)$.

Beweis: Aus Satz 9.11 folgt: $F(\alpha) \simeq F[x]/ < p(x) > \simeq F(\beta)$. □

Allgemeiner gilt:

Satz 9.14.
Seien K/F und K'/F' Körpererweiterungen, und $\varphi : F \xrightarrow{\sim} F'$ ein Isomorphismus. Sei $p(x) = \sum a_i x^i \in F[x]$ irreduzibel, und setze $p'(x) := \sum \varphi(a_i)x^i$. Dann ist $p'(x) \in F'[x]$ irreduzibel. Sei $\alpha \in K$ mit $p(\alpha) = 0$ und $\beta \in K'$ mit $p'(\beta) = 0$. Dann läßt sich φ zu einer Isomorphie $\varphi' : F(\alpha) \to F'(\beta)$ fortsetzen (i.e. $\varphi'|F = \varphi$), so dass $\varphi'(\alpha) = \beta$.

Beweis:

Wir betrachten also folgenden Ansatz und Fragestellung:

$$\begin{array}{ccc} F(\alpha) & \overset{?}{\dashrightarrow} & F'(\beta) \\ | & & | \\ F & \xrightarrow[\varphi]{\sim} & F' \end{array}$$

(1) $p'(x)$ ist irreduzibel, weil eine Faktorisierung $p'(x) = a'(x)b'(x)$ mit $\deg a'(x) \geq 1, \deg b'(x) \geq 1, a'(x), b'(x) \in F'[x]$ eine Faktorisierung (durch Anwendung von φ^{-1} auf Koeffizienten) $p(x) = a''(x)b''(x)$ von $p(x)$ in $F[x]$ induziert, mit $\deg(a''(x)) \geq 1, \deg(b''(x)) \geq 1; a''(x), b''(x) \in F[x]$.

(2) $F[x] \simeq F'[x]$ und $< p(x) > \simeq < p'(x) >$ (durch Anwendung von φ auf Koeffizienten). Also $F(\alpha) \simeq F[x]/ < p(x) > \simeq F'[x]/ < p'(x) > \simeq F(\beta)$. □

10 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript führen wir algebraische Erweiterungen ein, und untersuchen wir genau den Zusammenhang zwischen algebraische, endliche, und endlich erzeugte Erweiterungen.

Sei K/F stets eine Körpererweiterung.

Definition 10.1.

(1) $\alpha \in K$ ist *algebraisch über* F (alg/F), wenn es ein Polynom $0 \neq f(x) \in F[x]$ gibt mit $f(\alpha) = 0$.

(2) Wenn α nicht algebraisch über F ist, dann heißt α *transzendent* über F.

(3) Die Körpererweiterung K/F heißt *algebraisch*, falls für alle $\alpha \in K$: α ist algebraisch über F.

Beispiel 10.2.
Betrachte die Erweiterung $F(x)/F$. Hier ist $x \in F(x)$ transzendent über F , weil $f(x) = 0 \Leftrightarrow f = 0$ das Nullpolynom ist. ÜA.

Proposition 10.3.
Sei $\alpha \in K$ alg $/F$. Dann gibt ein eindeutiges normiertes irreduzibles Polynom $m_{\alpha,F}(x) \in F[x]$, so dass:

(i) $m_{\alpha,F}(\alpha) = 0$.

(ii) Ist $f(\alpha) = 0$ für ein $f \in F[x]$, dann teilt $m_{\alpha,F}(x)$ das Polynom $f(x)$ in $F[x]$.

Beweis:

- Setze $m(x) := m_{\alpha,F}(x) :=$ normiertes Polynom vom minimalem deg, so dass $m(\alpha) = 0$. Sei $f(x) \in F[x]$, schreibe $f(x) = q(x)m(x) + r(x), \deg r(x) < \deg m(x)$ oder $r(x) = 0$. Wir sehen $0 = f(\alpha) \Leftrightarrow r(\alpha) = 0$. Die Minimalität vom $\deg m(x)$ impliziert $r(x) = 0$, also $m(x)|f(x)$.
- Ist $m'(x)$ normiert vom minimalem deg mit $m'(\alpha) = 0$, dann gilt wie oben $m'(\alpha)|m(\alpha)$, aber auch $m(\alpha)|m'(\alpha), m(\alpha), m'(\alpha)$ normiert $\Rightarrow m'(x) = m(x)$. □

Definition 10.4.
$m_{\alpha,F}(x)$ heißt das *Minimal-Polynom* von α über F. Wir schreiben $m(x)$, wenn klar.

Bemerkung 10.5.
Im Skript 14. LA II (Definition 14.2) hatten wir das Minimal-Polynom von einem Operator T : Das Min.Pol.(T) in $F[x]$ ist der eindeutige normierte Erzeuger vom Annihilator-Ideal von T

$$\mathcal{A}_T := \{f \in F[x] | f(T) = 0\}.$$

Wir können analog $m_{\alpha,F}(x)$ definieren, ÜA.

Proposition 10.6.
Sei $\alpha \in K$ algebraisch über F. Es ist $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$.

Beweis:
Satz 9.11 impliziert $F(\alpha) \simeq F[x]/ < m_{\alpha,F}(x) >$, aus Satz 9.8 folgt $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$. □

Terminologie:
$\deg \alpha/F := \deg m_{\alpha,F}(x) = \deg F(\alpha)/F$.

Der Beweis dieser Bemerkung ist eine ÜA:

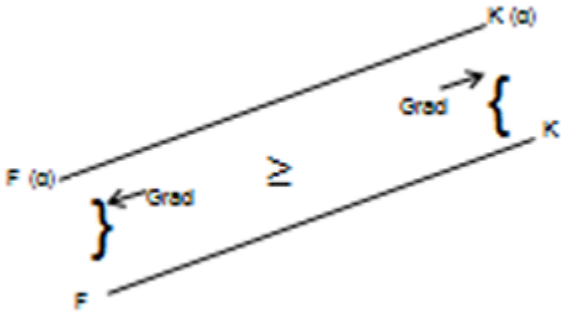
Bemerkung 10.7.
(1) $L \supseteq K \supseteq F, \alpha \in L,$ alg $/F \to \alpha$ alg $/K$ und es gilt

(2) $m_{\alpha,K}(x)$ teilt $m_{\alpha,F}(x)$ in $K[x]$, insbesondere

(3) $\deg m_{\alpha,K}(x) \leq \deg m_{\alpha,F}(x)$. Es gilt ferner

(4) $m_{\alpha,K}(x) = m_{\alpha,F}(x)$ genau dann, wenn $m_{\alpha,F}(x)$ irreduzibel bleibt in $K[x]$.
Wir haben aus (3):

(5) $[K(\alpha) : K] \leq [F(\alpha) : F]$



Wir zeigen nun die Umkehrung von Proposition 10.6.

Proposition 10.8.
Sei $\alpha \in K$, so dass $[F(\alpha) : F] < \infty$. Dann ist α algebraisch über F.

Beweis:
Sei $[F(\alpha) : F] = n$, dann sind $F(\alpha) \ni 1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig über F. Also existieren $b_i \in F$ *nicht alle gleich 0*, so dass $\sum_{i=0}^{n} b_i \alpha^i = 0$. Setze $f(x) := \sum b_i x^i \in F[x]; \not\equiv 0$. Dann gilt $f(\alpha) = 0; \alpha$ alg $/F$. □

Beispiel 10.9.
Die Erweiterung $F(x)/F$ ist endlich erzeugt (eigentlich ist sie eine einfache Erweiterung), aber $[F(x) : F] = \infty$ weil $x \in F(x)$ transzendent ist über F. Wir sehen also: K/F endlich erzeugt $\not\Rightarrow K/F$ endlich.

Korollar 10.10.
K/F ist endlich $\Rightarrow K/F$ algebraisch.

Beweis:
Sei $\alpha \in K$. Es ist $[F(\alpha) : F] \leq [K : F] < \infty$, also ist α algebraisch über F. □

Satz 10.11.
$F \subseteq K \subseteq L$. Es gilt $[L : F] = [L : K][K : F]$. (Also insbesondere ist L/F unendlich genau dann, wenn L/K oder K/F unendlich sind.)

Beweis:
Zunächst nehmen wir an: $[L : K] = m$ mit $\{\alpha_1, \ldots, \alpha_m\}$ Basis für L/K; $[K : F] = n$
mit $\{\beta_1, \ldots, \beta_n\}$ Basis für K/F. Ein Element λ aus L ist also aus der Form $\lambda = \sum_i a_i \alpha_i$
mit $a_i \in K$. $(*)$
Schreibe $a_i = \sum_j b_{ij}\beta_j$ mit $b_{ij} \in F$ $(**)$

$\rightsquigarrow$ Einsetzen von $(**)$ in $(*)$ ergibt $\lambda = \sum_{i,j} b_{ij}\alpha_i\beta_j$. $(***)$

Also ist span $_F\{\alpha_i\beta_j \mid i = 1, \ldots, m, j = 1, \ldots, n\} = L$. Wir zeigen, dass diese Menge auch F-linear unabhängig ist.
Sei also $\sum_{i,j} b_{ij}\alpha_i\beta_j = 0$ für $b_{ij} \in F$. $(\dagger)$
Setze $a_i := \sum_j b_{ij}\beta_j \in K$ und schreibe $(\dagger)$, also $\sum_i a_i\alpha_i = 0$. Nun ist α_i linear unabhängig über $K \Rightarrow a_i = 0$ für alle i, also $\sum_j b_{ij}\beta_j = 0$ für alle i.
Nun ist β_j linear unabhängig über $F \Rightarrow b_{ij} = 0$ für alle j. □

Wir haben gezeigt: $[L : F] = \infty \Rightarrow [L : K] = \infty$ oder $[K : F] = \infty$.
Sei nun $[K : F]$ unendlich, dann ist auch $[L : F]$ unendlich, weil K ein F-Unterraum von L ist.
Sei nun $[L : K] = \infty$, dann ist a fortiori $[L : F] = \infty$ ($\lambda_1, \ldots, \lambda_s$ sind K linear unabhängig $\rightarrow \lambda_1, \ldots, \lambda_s$ sind F-linear unabhängig).

Korollar 10.12.
Seien L/K und K/F Körpererweiterungen so dass L/F endlich ist. Es gilt $[K : F] | [L : F]$.

Wir haben bisher gezeigt, dass α algebraisch über F ist $\Leftrightarrow [F(\alpha) : F] < \infty$. Wir sind nun in der Lage dieses für $F(\alpha_1, \ldots, \alpha_n)$ zu verallgmeinern.

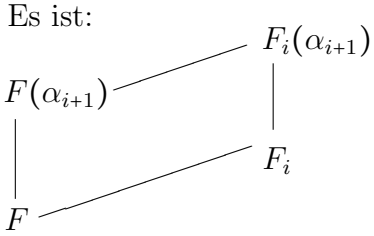
Satz 10.13.
K/F ist endlich $\Leftrightarrow$ K/F ist endlich erzeugt von alg $/F$-Elementen.

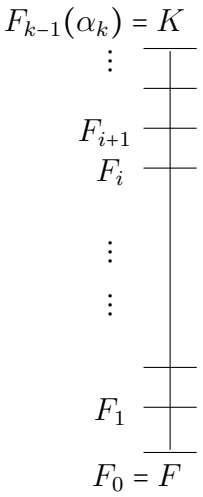
Beweis:

"$\Rightarrow$" Setze $[K : F] = n$. Sei $\{\alpha_1, \ldots, \alpha_n\}$ die F-Basis von K. Jedes α_i ist algebraisch über F. Außerdem ist $K = \text{span}_F\{\alpha_1, \ldots, \alpha_n\} \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq K$
und damit ist $K = F(\alpha_1, \ldots, \alpha_n)$.

"$\Leftarrow$" Wir bemerken vorab dass für $\alpha, \beta \in K$ gilt allgemein: $F(\alpha, \beta) = F(\alpha)(\beta)$ (folgt unmittelbar aus der Definition 9.10, ÜA). Sei $K = F(\alpha_1, \ldots, \alpha_k)$. Sei α_i algebraisch über F und $\deg \alpha_i = n_i$. Setze $F = F_0$ und $F_1 = F_0(\alpha_1)$. $F_{i+1} := F_i(\alpha_{i+1})$, so $K = F_{k-1}(\alpha_k)$.

Es ist:





Also $[F_{i+1} : F_i] \leq n_{i+1}$. Also (Satz 10.11) $[K : F] = [F_k : F_{k-1}] \cdots [F_1 : F_0] \leq n_1 \cdots n_k$ und damit ist K/F endlich. $\square$

11 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst wichtige Begriffe (Zerfällungskörper, normale Erweiterung, Kompositum) einführen und untersuchen. In Abschnitt 13 werden wir die Voraussetzungen erstellen, um dann algebraische Abschlüsse in Skript 12 aufzubauen.

Sei K/F stets eine Körpererweiterung.

Korollar 11.1.
Seien $\alpha, 0 \neq \beta \in K$ algebraisch über F, dann sind $\alpha \pm \beta\,, \alpha\beta\,, \alpha/\beta$ auch algebraisch über F.

Beweis:
Die Erweiterung $F(\alpha,\beta)/F$ ist endlich wegen Satz 10.13. Nun sind $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha,\beta)$. Aus Korollar 10.10 folgt nun unsere Behauptung. □

Korollar 11.2.
Die Menge $\tilde{F} := \{\alpha \in K \mid \alpha \text{ alg } /F\}$ ist ein Teilkörper von K welcher F enthält.

Definition 11.3.
Dieser Teilkörper $\tilde{F}$ heißt der *relative algebraische Abschluss von F in K.*

Beispiel 11.4.
(1) In der Erweiterung $\mathbb{C}/\mathbb{Q}$ ist $\tilde{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ alg } /\mathbb{Q}\}$ der *Körper der algebraischen Zahlen.*

(2) In der Erweiterung $\mathbb{R}/\mathbb{Q}$ ist $\tilde{\mathbb{Q}}^r := \{r \in \mathbb{R} \mid r \text{ alg } /\mathbb{Q}\}$ der *Körper der reellen algebraischen Zahlen.*

Es gilt $\tilde{\mathbb{Q}} \subsetneq \mathbb{C}$ und $\tilde{\mathbb{Q}}^r \subsetneq \mathbb{R}$ (z.B: $\pi, e \in \mathbb{R}\backslash\tilde{\mathbb{Q}}^r$). Eigentlich gilt es ferner: $[\tilde{\mathbb{Q}} : \mathbb{Q}] = [\tilde{\mathbb{Q}}^r : \mathbb{Q}] = \infty$, $|\tilde{\mathbb{Q}}| = |\tilde{\mathbb{Q}}^r| = \aleph_0$ und $|\mathbb{C} \setminus \tilde{\mathbb{Q}}| = |\mathbb{R} \setminus \tilde{\mathbb{Q}}^r| = 2^{\aleph_0}$. Siehe ÜB.

Satz 11.5.

L/K	und	K/F	$\Rightarrow$	L/F
alg		alg		alg

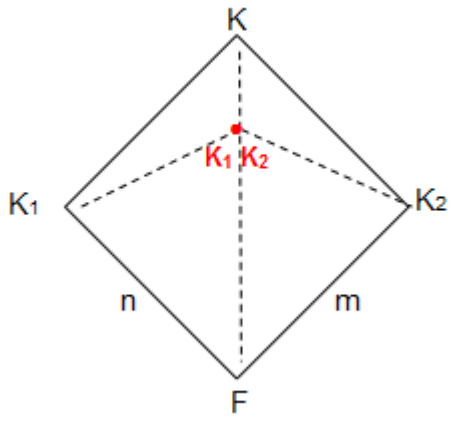
Beweis:
Sei $\alpha \in L$ und $0 \neq k(x) := \sum_{i=0}^{n} a_i x^i \in K[x]$ so dass $k(\alpha) = 0 \qquad (*)$.
Betrachte die folgende Körpererweiterungen:

- $F_1 := F(a_0, \ldots, a_n)\,, F_1 \subseteq K\,, a_i$ alg $/F$, also folgt aus Satz 10.13 dass $[F_1 : F] < \infty$.
- $F_1(\alpha) \subseteq L\,, \alpha$ alg $/F_1$ wegen $(*)$, also folgt aus Satz 10.13 dass $[F_1(\alpha) : F_1] < \infty$.
- Es folgt aus Satz 10.11 dass $[F_1(\alpha) : F] = [F_1(\alpha) : F_1][F_1 : F] < \infty$.

Insbesondere folgt nun aus Proposition 10.8 dass $F_1(\alpha)/F$ algebraisch ist, und damit ist α algebraisch über F. □

Definition 11.6.
Seien K/K_1 und K/K_2 Körpererweiterungen. Der Körper $K_1K_2 := K_1(K_2) = K_2(K_1) \subseteq K$ heißt *das Kompositum von K_1 und K_2 in K.*

Lemma 11.7.
Seien K/K_1 und K/K_2 sowie K_1/F und K_2/F Körpererweiterungen, so dass



$\{\alpha_1, \ldots, \alpha_n\}$ eine F-Basis von K_1 und $\{\beta_1, \ldots, \beta_m\}$ eine F-Basis von K_2 . Es gilt:
$\text{span}_F\{\alpha_i\beta_j / i, j\} = K_1K_2$.

Beweis:
Ohne Einschränkung $\alpha_1 = \beta_1 = 1$. Bemerke, dass $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m)$. Nun ist $\text{span}_F\{\alpha_i\beta_j / i, j\} \subseteq K_1K_2$ ein **Teilkörper** von K welcher $F \cup \{\alpha_1, \ldots, \alpha_n\} \cup \{\beta_1, \ldots, \beta_m\}$ enthält (ÜA). Also gilt auch $\text{span}_F\{\alpha_i\beta_j / i, j\} \supseteq K_1K_2$. □

Korollar 11.8.
Seien $K/K_1, K/K_2$; $K_1/F, K_2/F$ die Körpererweiterungen wie in Lemma 11.7, setze $[K_1 : F] := n$, $[K_2 : F] := m$. Es gilt $[K_1K_2 : F] \leq nm$.
Ferner gilt: $[K_1K_2 : F] = mn$, wenn α_i linear unabhängig über K_2 bleiben (oder wenn β_j linear unabhängig über K_1 bleiben.)

Beweis:
Dass $[K_1K_2 : F] \leq nm$, folgt direkt aus dem Lemma 11.7. Wir nehmen an, dass $\alpha_1, \ldots, \alpha_n$ linear unabhängig über K_2 sind und wir zeigen, dass die Familie $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ linear unabhängig über F ist. Seien $(\nu_{ij})_{ij} \subseteq F$ so, dass $\sum_{i,j} \nu_{ij}\alpha_i\beta_j = 0$. Man kann diese Summe umschreiben: $\sum_{i=1}^{n} \alpha_i(\sum_{j=1}^{m} \nu_{ij}\beta_j) = 0$. Für alle $i \in \{1, \ldots, n\}$ ist $\sum_{j=1}^{m} \nu_{ij}\beta_j \in K_2$. Nach Annahme muss dann $\sum_{j=1}^{m} \nu_{ij}\beta_j = 0$ gelten für alle $i \in \{1, \ldots, n\}$. Weil $\beta_1, \ldots, \beta_m$ linear unabhängig über F sind, muss dann $\nu_{ij} = 0$ gelten für alle i, j.
(Analog kann man die zweite Aussage beweisen). □

Korollar 11.9.
Seien $[K_1 : F] = n, [K_2 : F] = m$ und ggT $(n, m) = 1$. Es gilt $[K_1K_2 : F] = mn$.

Beweis:
$$\left.\begin{array}{rcl} n & | & [K_1K_2 : F] \\ m & | & [K_1K_2 : F] \end{array}\right\} \Rightarrow kgV(n, m) \mid [K_1K_2 : F]$$

$kgV(n, m) = \frac{nm}{ggT(n,m)} = mn$. Also $mn \leq [K_1K_2 : F] \leq mn$. □

§ 13 Algebraischer Abschluss

Sei K/F stets eine Körpererweiterung.

Definition 11.10.
Sei $f \in F[x]\,, \deg(f) \geq 1$. Der Körper K ist ein *Zerfällungskörper von* f, wenn folgendes gilt:

1. f zerfällt vollständig in lineare Faktoren in $K[x]$, das heißt ist Produkt von linearen Faktoren in $K[x]$.
2. Für alle Körper L mit $F \subseteq L \subsetneq K$ zerfällt f in $L[x]$ **nicht**.

Allgemeiner können wir diesen Begriff für eine Menge von Polynomen erklären:

Bemerkung 11.11.
Sei $\mathcal{E} \subseteq F[x]$. Der Körper K ist ein *Zerfällungskörper von* $\mathcal{E}$ wenn folgendes gilt:

1. Jedes $f \in \mathcal{E}$ mit $\deg(f) \geq 1$ zerfällt vollständig in lineare Faktoren in $K[x]$
2. K wird von den Nullstellen der Polynome in $\mathcal{E}$ erzeugt, also
   $K = F(\{\alpha \in K \mid \exists f \in \mathcal{E} \text{ mit } f(\alpha) = 0\})$

Bemerkung 11.12.
Sei $f \in F[x]$, $\deg(f) \geq 1$. Dann ist K Zerfällungskörper von f genau dann, wenn K Zerfällungskörper von $\mathcal{E} := \{f\}$ ist.

Definition 11.13.
Die Erweiterung K/F ist *normal*, wenn K ein Zerfällungskörper einer Menge $\mathcal{E} \subseteq F[x]$ ist.

Satz 11.14.
Es gibt einen Zerfällungskörper K/F für $f(x)$ über F.

Beweis:
Per Induktion zeigen wir zunächst, dass es eine Körpererweiterung E/F gibt, in der $f(x)$ vollständig zerfällt.
Setze $n = \deg f(x)$. $n = 1, E = F\checkmark$ Induktionsanfang $n > 1$.
Sei $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ (sonst ist wieder $E = F$).
Sei $\alpha \in E_1/F$ eine Nullstelle von $p(x)$ (s. Satz 9.7), über E_1 haben wir also

$$(*) \qquad f(x) = (x - \alpha) f_1(x)$$

$f_1(x) \in E_1[x]; \deg f_1 \leq n - 1$.

Induktionsannahme für f_1 und E_1 ergibt eine E/E_1 und f_1 zerfällt vollständig in $E[x]$. Nun ist auch $\alpha \in E$. Also zerfällt f wie in $(*)$ vollständig über E.
Setze nun $K := \bigcap\{L/F \subseteq L \subseteq E; f \text{ zerfällt vollständig in } L[x]\}$ □

Proposition 11.15.
Sei $\deg f = n \geq 1$, und K/F ein Zerfällungskörper von f über F. Es gilt $[K : F] \leq n!$

Beweis:
Sei $\alpha_1 \in F_1/F$, α_1 ist Nullstelle von f. Dann ist $[F_1 : F] \leq n$ und $f(x) = (x - \alpha_1)f_1(x)$, $f_1(x) \in F[x]$, $\deg f_1 \leq n-1$. Wiederholung des Vorgangs ergibt: Sei $\alpha_2 \in F_2/F_1, \alpha_2$ ist Nullstelle von f_1. Dann ist $[F_2 : F_1] \leq n-1$, und damit $[F_2 : F] \leq n(n-1)$ (wegen Satz 10.11).
Wir verfahren so weiter (ÜA). □

12 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Abschnitt 13 beenden; unser Endresultat ist Korollar 12.6 wo wir die Existenz und Eindeutigkeit für algebraische Abschluss etablieren.

In Satz 11.14 haben wir die Existenz vom Zerfällungskörper gezeigt, nun zeigen wir die Eindeutigkeit:

Satz 12.1.
Seien F und F' Körper und $\varphi : F \xrightarrow{\sim} F'$ eine Isomorphie, $f(x) \in F[x]$ mit $\deg f \geq 1$ und $\varphi(f) := f'(x) \in F'[x]$ das Bild von f (nach Anwendung von φ auf die f-Koeffiziente). Seien E Zerfällungskörper für f über F und E' ist Zerfällungskörper für f' über F'.
Dann läßt sich φ fortsetzen:

$$\begin{array}{ccc} E & \overset{\sigma}{\xrightarrow{\sim}} & E' \\ | & & | \\ F & \underset{\varphi}{\xrightarrow{\sim}} & F' \end{array}$$

Beweis:
Sei $\deg f := n$. Beweis per Induktion nach n. Es ist klar dass wenn f über F als Produkt von linearen Faktoren zerfällt, dann zerfällt ebenfalls f' über F' als Produkt von linearen Faktoren (ÜA). In diesem Fall $E = F$ und $E' = F'$ und wir setzen $\sigma = \varphi$.

Sei also $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ und $p' = \varphi(p)$ der entsprechende irreduzibler Faktor von $f'(x)$ in $F'[x]$ (s. Satz 9.14). Sei $\alpha \in E$ eine Nullstelle für $p(x)$ und $\beta \in E'$ eine Nullstelle für $p'(x)$. Setze $F_1 := F(\alpha)$ und $F_1' := F'(\beta)$.

Aus Satz 9.14. folgt, dass ein σ_1 existiert, so dass

$$\begin{array}{ccc} F_1 & \underset{\sigma_1}{\xrightarrow{\sim}} & F_1' \\ | & & | \\ F & \underset{\varphi}{\xrightarrow{\sim}} & F' \end{array}$$

Nun haben wir also den folgenden Ansatz:

$$\sigma_1 : F_1 \xrightarrow{\sim} F_1'$$

und $f(x) = (x-\alpha)f_1(x)$ über F_1, mit $\deg f_1 \leq n-1$. Bemerke dass E ein Zerfällungskörper von f_1 über F_1 ist: $E \supseteq F_1$ und E enthält alle Nullstellen von f_1; und für L mit $E \supsetneq L \supseteq F_1$, ist es unmöglich, dass L alle Nullstellen von f_1 enthält (sonst enthält L auch α und alle Nullstellen von f_1, also alle Nullstellen von f - Widerspricht Minimalität von E als ein Zerfällungskörper von f über F). Analog ist $f'(x) = (x-\beta)f_1'(x)$ über F_1', $\deg f_1' \leq n-1$ und E' ist ein Zerfällungskörper von f_1' über F_1'. Also haben wir nun den Ansatz f_1, F_1, σ_1 mit $\deg f_1 \leq n-1$ für die Induktion.

Die Induktionsannahme liefert ein σ, so dass

$$\begin{array}{ccc} E & \xrightarrow[\sigma]{\sim} & E' \\ | & & | \\ F_1 & \xrightarrow[\sigma_1]{\sim} & F_1' \end{array}$$

Also

$$\begin{array}{ccc} E & \xrightarrow[\sigma]{\sim} & E' \\ | & & | \\ F_1 & \xrightarrow[\sigma_1]{\sim} & F_1' \\ | & & | \\ F & \xrightarrow[\varphi]{\sim} & F' \end{array}$$

□

Korollar 12.2.
Ein Zerfällungskörper von $f \in F[x]$ über F ist bis Isomorphie auf F eindeutig.

Beweis:
Seien K und K' Zerfällungskörper von f über F. Wegen Satz 12.1 gilt:

mit $\sigma|F = Id$

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\sim} & K' \\ | & & | \\ F & \xrightarrow{Id} & F \end{array}$$

□

Definition 12.3.

(a) $\tilde{F}/F$ ist ein *algebraischer Abschluss* von F, falls
   (a) $\tilde{F}/F$ algebraisch ist;
   (b) jedes $f(x) \in F[x]$ mit $\deg f \geq 1$ zerfällt vollständig als Produkt von linearen Faktoren über $\tilde{F}$.

(b) K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[x]$ mit $\deg f \geq 1$ eine Nullstelle in K hat.

Bemerkung 12.4.
K ist algebraisch abgeschlossen $\Leftrightarrow$ jedes $f \in K[x]$ mit $\deg f \geq 1$ zerfällt vollständig in linearen Faktoren über $K \Leftrightarrow K = \tilde{K}$.

Proposition 12.5.
Sei $\tilde{F}$ ein algebraischer Abschluss von F. Dann ist $\tilde{F}$ algebraisch abgeschlossen.

Beweis:
Sei $f(x) \in \tilde{F}(x)$ $\deg f \geq 1$, α ist Nullstelle von $f(x)$ (in irgend einer Körpererweiterung $K/\tilde{F}$, s. Satz 9.7). Dann ist $\tilde{F}(\alpha)/\tilde{F}$ algebraisch und $\tilde{F}/F$ algebraisch. Also ist auch $\tilde{F}(\alpha)/F$ algebraisch (s. Satz 11.5) und damit ist auch α/F algebraisch.
Sei $m_{\alpha,F}$ das Minimalpolynom von α/F, dann zerfällt $m_{\alpha,F}$ in $\tilde{F}[x]$ und hat $(x-\alpha)$ als linearen Faktor. Es folgt $\alpha \in \tilde{F}$. □

Sei F ein beliebiger Körper. Wir zeigen nun:
Hauptsatz
Es gibt eine algebraische abgeschlossene Körpererweiterung von F.

Beweis:
Setze $F = K_0$. Wir definieren per Induktion nach $n \in \mathbb{N}_0$ eine ansteigende Folge

$$K_0 \subseteq \cdots \subseteq K_j \subseteq K_{j+1} \subseteq \cdots$$

von der Körpererweiterung, so dass jedes Polynom $f \in K_{j-1}[x]$ mit $\deg f \geq 1$ eine Nullstelle in K_j hat. Dann setzen wir $K := \bigcup K_j$. Dann ist K/F eine Körpererweiterung,und wenn $f(x) \in K[x]$ $(\deg f \geq 1)$, dann existiert ein j mit $f(x) \in K_j[x]$ und f hat eine Nullstelle in $K_{j+1} \subseteq K$. Also ist K algebraisch abgeschlossen.

Und nun zur Induktion:
Für $f(x) \in F[x](\deg f \geq 1)$ sei x_f eine neue Variable. Betrachte $F[\cdots, x_f, \cdots]$ (Polynomring in der Variablen x_f ; siehe ÜB) und das Ideal $I :=< \{f(x_f); f \in F[x]\} >$.

Behauptung:
I ist echt. Sonst ist

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})(*)$$

mit $g_i \in F[\cdots, x_f, \cdots]$. Schreibe $x_i := x_{f_i}$ für $i = 1, \ldots, n$ und seien $x_{n+1}, \ldots, x_m$ alle anderen Variablen, die unter den g_i's noch vorkommen. Also ist

$$1 = g_1(x_1, \ldots, x_m) f_1(x_1) + \cdots + g_n(x_1, \ldots, x_m) f_n(x_n)(*)$$

eine polynomiale Gleichung.
Sei F'/F eine Körpererweiterung mit $\alpha_i \in F'$, Nullstelle für $f_i(x)$. Durch Einsetzen von α_i für x_i mit $i = 1, \ldots, n$ und 0 für x_j mit $j = n-1, \ldots, m$ in $(*)$ muss es immer noch eine Gleichung ergeben, die nun im Körper F' gelten muss, das heißt $1 = 0$ in F' - Widerspruch.

I ist echt. Per ZL, sei $\mathcal{M}$ maximal. $\mathcal{M} \lhd F[\cdots, x_f, \cdots]$ und $I \subseteq \mathcal{M}$. Setze $K_1 := F[\cdots, x_f, \cdots]/\mathcal{M}$. K_1/K_0 und $f \in K_0[x]$ hat eine Nullstelle in K_1, weil $f(\overline{x_f}) = \overline{f(x_f)} = 0$ (da $f(x_f) \in I$).
Wiederhole mit K_j/K_{j-1} und setze $K = \bigcup K_j$ wie schon erwähnt. □

Korollar 12.6.
Existenz:: Sei K algebraisch abgeschlossen und $F \subseteq K$. Dann ist der relative algebraische Abschluss von F in K ein algebraischer Abschluss von F.
Eindeutigkeit: (siehe ÜB)
Ein algebraischer Abschluss von F ist bis auf Isomorphie eindeutig.

Beweis:
Per Definition ist $\tilde{F}/F$ algebraisch. Sei $f(x) \in F[x]$ $(\deg f \geq 1)$, da K algebraisch abgeschlossen ist, $K[x] \ni f(x)$ zerfällt vollständig in lineare Faktoren $(x-\alpha)$ in $K[x]$. Aber α ist algebraisch über F und $\alpha \in K$, also $\alpha \in \tilde{F}$. Also zerfällt $f(x)$ in $\tilde{F}[x]$. □

13 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Kapitel 2 beenden. Im Abschnitt 14 werden wir LA II Skript 4 ergänzen, indem wir die Vielfachheit der Nullstellen in einem Grundkörper F ($Char(F) = 0$ oder $Char(F) = p$) untersuchen.

§14: Separable und inseparable Körpererweiterung

Definition 13.1.
Sei $f(x) \in F[x]$, mit $f(x) = a_n x^n + \cdots + a_0$, $\deg f \geq 1$, und sei K/F ein Zerfällungskörper für f. Dann ist

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

in $K[x]$; mit $n_i \geq 1$, $\alpha_i \neq \alpha_j$ für $i \neq j$.

- n_i ist die *Vielfachheit* der Nullstelle α_i.
- α_i ist eine *mehrfache* Nullstelle, wenn $n_i > 1$, sonst ist
- α_i eine *einfache* Nullstelle.

Definition 13.2. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$.
(1) f ist *separabel*, wenn es nur einfache Nullstellen hat.
(2) f nicht separabel heißt *inseparabel*.

Definition 13.3. Sei $f(x) = a_n x^n + \cdots + a_0 \in F[x]$, die *Ableitung* Df von f ist
$Df(x) = D(a_n x^n + \cdots + a_0) = n a_n x^{n-1} + \cdots + a_1 \in F[x]$.
$D : F[x] \to F[x]$ ist *Ableitungsoperator* und erfüllt die Produktregel

$$Dfg = gDf + fDg.$$

Bemerkung 13.4.
Sei $f(x) \in F[x]$ mit $\deg f = n \geq 1$.

1. $Df = 0$ oder $\deg Df < \deg f$ gilt immer.
2. Sei Char $F = 0$, dann ist $Df \neq 0$, weil zum Beispiel $na_n \neq 0$, für den Hauptkoeffizient $a_n \neq 0$ von f.
3. Sei p eine Primzahl und Char $F = p$. Betrachte $f(x) = x^p \in F[x]$. Dann ist $\deg f(x) > 1$, jedoch ist $Df(x) = px^{p-1} = 0$.

Proposition 13.5.
Sei $f(x) \in F[x]$ mit $\deg f \geq 1$. Eine Nullstelle α für $f(x)$ ist eine mehrfache Nullstelle genau dann, wenn α auch eine Nullstelle für $Df(x)$ ist. Das heißt,

$$\{x; x \text{ ist eine mehrfache Nullstelle von } f\} = \{x; x \text{ ist eine gemeinsame Nullstelle von } f \text{ und } Df\}.$$

Beweis:

"⇒" Sei α eine mehrfache Nullstelle. Schreibe $f(x) = (x-\alpha)^n g(x)$ mit $n \geq 2$.
Berechne $Df(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n Dg(x)$; $n-1 \geq 1 \Rightarrow \alpha$ ist Nullstelle von $Df(x)$.

"⇐" Sei α eine gemeinsame Nullstelle von $f(x)$ und $Df(x)$.
Schreibe $f(x) = (x-\alpha)h(x)$. $(*)$
Also ist $Df(x) = h(x) + (x-\alpha)Dh(x)$. Beim Einsetzen von α für x, ergibt das $h(\alpha) = 0$.
Zurück in $(*)$ ergibt es $f(x) = (x-\alpha)^2 h_1(x)$. □

Bemerkung 13.6. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$; α eine Nullstelle, und $m_{\alpha,F} \in F[x]$ das minimal Polynom. Dann ist α auch Nullstelle von $Df(x) \Leftrightarrow m_{\alpha,F} \,/\, Df(x)$.

Lemma 13.7.
Die gemeinsamen Nullstellen von f und Df sind die Nullstellen von ggT (f, Df).

Beweis:

"⇐" α ist Nullstelle von ggT $(f, Df) \to \alpha$ ist Nullstelle von f und Df. Ist klar, ÜA.

"⇒" Sei α eine Nullstelle von f und Df. Da $m_{\alpha,F} \,/\, f$ und $m_{\alpha,F} \,/\, Df$, $m_{\alpha,F} /$ ggT (f, Df) auch.
Da α Nullstelle von $m_{\alpha,F}$ ist, folgt nun α ist Nullstelle von ggT (f, Df). □

Korollar 13.8.
Sei $f \in F[x]$ mit $\deg f \geq 1$ ein normiertes Polynom. Dann ist f separabel genau dann, wenn ggT $(f, Df) = 1$.

Beweis:

"⇐" Folgt aus Proposition 13.5 und Lemma 13.7.

"⇒" f separabel $\Rightarrow$ f hat keine gemeinsame Nullstelle mit Df (s. Proposition 13.5)
$\Rightarrow$ ggT $(f, Df) = 1$ (ÜA). □

Korollar 13.9.
Sei $f(x)$ mit $\deg f \geq 1$ ein irreduzibles Polynom. Es gilt: f ist inseparabel genau dann, wenn $Df = 0$.

Beweis:
α ist eine mehrfache Nullstelle von $f \Leftrightarrow m_{\alpha,F}$ ist gT von f und Df (s. Bemerkung 13.6). Nun f irreduzibel $\Rightarrow \deg m_{\alpha,F} = \deg f$. Also $m_{\alpha,F} \,/\, Df \Leftrightarrow Df = 0$ (s. Bemerkung 13.4 (1)). □

Beispiel 13.10.

(1) Sei $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
Berechne $Df(x) = p^n x^{p^n-1} - 1 = -1$.
Df hat gar keine Nullstelle, also ist f separabel.

(2) Sei F so dass Char $F = 0$ oder Char $F := p \nmid n$. Sei $f(x) = x^n - 1$, berechne $Df(x) = nx^{n-1}$.
Dann ist $Df \neq 0$ und hat 0 als einzige Nullstelle, 0 ist aber keine Nullstelle von f, also ist f separabel und die Gleichung $x^n - 1 = 0$ hat n paarweise verschiedene Nullstellen. Diese Nullstellen heißen die $n$te *Einheitswurzel*.

(3) Sei nun F so dass Char $F = p | n$. Für $f(x) = x^n - 1$, $Df(x) = nx^{n-1} = 0 \Rightarrow f$ ist inseparabel.

Korollar 13.11.
Sei Char $F = 0$, und $f \in F[x]$ mit $\deg f \geq 1$.

1. Wenn f irreduzibel, dann ist f separable.
2. Allgemeiner gilt: $f(x)$ ist separabel genau dann, wenn die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

Beweis:

1. $f \neq 0 \Rightarrow Df \neq 0$ (weil Char $F = 0$).
2. "$\Leftarrow$" Wegen Eindeutigkeit des minimal Polynoms, können verschiedene irreduzible, normierte Polynome in $F[x]$ keine gemeinsame Nullstelle in K haben (ÜA). In der Primfaktorisierung
   $$f = c\prod_{i=1}^{k} p_i(x) \qquad p_i \neq p_j$$
   haben außerdem keiner der Faktoren eine mehrfache Nullstelle (folgt aus 1.). Also hat f keine mehrfache Nullstelle, f ist separabel.

"$\Rightarrow$": Analog (ÜA). □

Beispiel 13.12.
$f = x^2 - t \in \mathbb{F}_2(t)[x]$. f ist irreduzibel, weil $\sqrt{t} \notin \mathbb{F}_2(t)$ (ÜA).
$Df = 0$, also ist f irreduzibel, aber inseparabel.

Bemerkung 13.13.
Sei Char $F = p > 0$; $g \in F[x]$, $\deg g \geq 1$. Setze $f(x) := g(x^p)$, schreibe

$$f(x) = \gamma_m(x^p)^m + \cdots + \gamma_1 x^p + \gamma_0 \qquad (*) .$$

Dann ist $Df(x) = 0$ und f ist inseparabel.
Umgekehrt: $f(x) \in F[x](\deg f \geq 1)$ mit $Df = 0$ muss die Gestalt $(*)$ haben, i.e. $f(x) = g(x^p)$ mit $g(x) \in F[x]$. (ÜA).

Proposition 13.14. Sei Char $F = p > 0$.

Es gelten $(a+b)^p = a^p + b^p$ für alle $a, b \in F$

$(ab)^p = a^p b^p$

und $\varphi : F \to F$, $a \mapsto a^p$

ist ein injektiver Körper-Homomorphismus (Frobenius).

Beweis: (ÜB).

Korollar 13.15.
$\mathbb{F}$ ist endlich $\Rightarrow \varphi : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$
ist auch surjektiv, also ein Automorphismus. Das heißt $\mathbb{F} = \mathbb{F}^p := \{a^p; a \in \mathbb{F}\}$.

Beweis:
$\mathbb{F}$ ist endlich, also endlich dimensional über den Primkörper $\mathbb{F}_p$ und kann also nicht isomorph sein zu einem echten Unterraum (vgl. LA I Skript 13). □

Korollar 13.11. gilt also auch für endliche Körper.

Proposition 13.16. Sei $\mathbb{F}$ ein endlicher Körper.

1. Jedes irreduzible Polynom $f \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel.
2. Ein Polynom $f(x) \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel $\Leftrightarrow$ die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

Beweis:
(1) Sei Char $\mathbb{F} := p > 0$, $f \in \mathbb{F}[x](\deg f \geq 1)$, f irreduzibel.

- f inseparabel $\Leftrightarrow Df = 0 \Leftrightarrow f(x) = g(x^p)$. Berechne:

$$\begin{aligned} f(x) = g(x^p) &= a_m(x^p)^m &+\cdots+ &\quad a_1x^p + a_0 \\ &= b_m^p(x^m)^p &+\cdots+ &\quad b_1^p x^p + b_0^p \\ &= (b_m x^m)^p &+\cdots+ &\quad (b_1 x)^p + b_0^p \\ &= (b_m x^m &+\cdots+ &\quad b_1 x + b_0)^p \end{aligned}$$

Widerspruch.
(2) Analog zum Beweis vom Korollar 13.11. (ÜA). □

Bemerkung 13.17.
Im Beweis von Proposition 13.16 haben wir die wichtige Eingenschaft $\mathbb{F}^p = \mathbb{F}$ benutzt (s.Korollar 13.15).

Definition 13.18.
Ein Körper F heißt *perfekt*, falls Char $F = 0$ oder Char $F = p > 0$ und $F = F^p$.

Bemerkung 13.19.
Proposition 13.16. gilt allgemeiner für F perfekt (anstatt $\mathbb{F}$ endlich).

Beweis: (ÜB).