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 $O := \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ 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 $a(x)+ < p(x) >= r(x)+ < p(x) >$,

  d. h. $\overline{a(x)} = \overline{r(x)}$

  $\quad\ \ \|$

  d. h. $a(\overline{x}) = r(\overline{x})$

  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 $b_0, \dots, b_{n-1} \in F$ 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 $i = 0, \dots, n - 1$. □

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 $F(\alpha) \simeq F[x]/ < p(x) > \simeq F'[x]/ < p'(x) > \simeq F(\beta)$. □