Zusammenfassung zu Algebra B

Sara Adams

25. Juli 2004

Diese Zusammenfassung basiert auf der Vorlesung
Algebra B
gehalten im Sommersemester 2004
von Prof. Dr. Klaus Metsch
an der Justus-Liebig Universität Gießen

Inhaltsverzeichnis

1 Ergänzungen zur Körpertheorie **2**
1.1 Fundamentalsatz der Algebra . . . 2
1.2 Transzendente Zahlen . . . 2
1.3 Einfache transzendente Erweiterungen . . . 3
1.4 Kreisteilungspolynome . . . 3
1.5 Lemma von Zorn . . . 4
1.6 Algebraischer Abschluss eines Körpers . . . 5

2 Einblick in die algebraische Geometrie **5**
2.1 Definitionen und erste Eigenschaften . . . 6
2.2 Basissatz und Nullstellensatz von Hilbert . . . 6
2.3 Ideale und Varietäten . . . 7

1 Ergänzungen zur Körpertheorie

1.1 Fundamentalsatz der Algebra

- Jedes Polynom $f \in \mathbb{R}[x]$ mit ungeradem Grad hat eine Nullstelle in $\mathbb{R}$
- Jedes $c \in \mathbb{C}$ besitzt in $\mathbb{C}$ eine Quadratwurzel.
- Jedes $f \in \mathbb{C}[x]$ mit Grad $f = 2$ zerfällt in $\mathbb{C}[x]$ in Linearfaktoren.
- Jedes nichtkonstante Polynom $f \in \mathbb{R}[x]$ besitzt in $\mathbb{C}$ eine Nullstelle.
- Jedes nichtkonstante $f \in \mathbb{R}[x]$ zerfällt in $\mathbb{C}[x]$ in Linearfaktoren.
- $\mathbb{C}$ ist algebraisch abgeschlossen.
- $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$.
- Die Menge A aller komplexer Zahlen, die algebraisch über $\mathbb{Q}$ sind, ist ein Körper. Er ist der algebraische Abschluss von $\mathbb{Q}$. ($A \neq \mathbb{C}$)

1.2 Transzendente Zahlen

- Die Menge A der über $\mathbb{Q}$ algebraischen Zahlen ist abzählbar.
- (Liouville) Ist $a \in \mathbb{R}$ irrational und algebraisch über $\mathbb{Q}$, so gibt es eine reelle Zahl $c > 0$ mit
$$\left|a - \frac{p}{q}\right| > \frac{c}{q^m} \qquad \forall p \in \mathbb{Z}, q \in \mathbb{N},$$
wobei m der Grad des Minimalpolynoms von a über $\mathbb{Q}$ ist.
- Sei $a \in \mathbb{R}$. Gibt es für jede natürliche Zahl $n \in \mathbb{N}$ eine rationale Zahl $\frac{p}{q}, q > 1$ mit $0 < \left|a - \frac{p}{q}\right| < \frac{1}{q^n}$, so ist a transzendent.

1.3 Einfache transzendente Erweiterungen

Definitionen

- **Körper der rationalen Funktionen** über K $K(x) := \{\frac{f}{g} : f,g \in K[x], g \neq 0\}$
- **Grad** von $u = \frac{f}{g}$: $Grad(u) := \max\{Grad(f), Grad(g)\}$
- t transzendent über K: **Grad** von $\frac{f(t)}{g(t)}$: $Grad(\frac{f(t)}{g(t)}) := Grad(\frac{f}{g})$

Sätze

- $K(x) \to K(t)$, $\frac{f}{g} \mapsto \frac{f(t)}{g(t)}$ Isomorphismus
- $K(t) : K$ einfache transzendente Erweiterung, $n = Grad(u)$ für ein $u \in K(x) \backslash K \Rightarrow$ t algebraisch über $K(u)$, $[K(t) : K(u)] = n$
- $K(t) : K$ einfache transzendente Erweiterung, $u \in K(t) \Rightarrow$ $[K(u) = K(t) \Leftrightarrow u = \frac{at+b}{ct+d}$, $ad \neq bc$, $a,b,c,d \in K]$
- (**Luroth**): $K(t) : K$ einfache transzendente Erweiterung $\Rightarrow$ $K(u)$, $u \in K(t)$ sind alle Zwischenkörper
- $\mathbb{Z}_n = \mathbb{Z} \backslash n\mathbb{Z} = \{0, .., n-1\}$ Ring mit Rechnung modulo n
  - $\mathbb{Z}_n* := \{a \in \mathbb{Z}_n : \exists b \in \mathbb{Z}_n : a \cdot b = 1\}$ **Einheitengruppe** von $\mathbb{Z}_n$

1.4 Kreisteilungspolynome

Im Folgenden bewegen wir uns in einem Körper K mit $Char(K) = 0$, so dass $x^n - 1$ in $K[x]$ in Linearfaktoren zerfällt.

Definitionen

- **Eulersche φ-Funktion** $\varphi : \mathbb{N} \to \mathbb{N}, n \mapsto |\{t \in \mathbb{N} : 1 \leq t \leq n, (t,n) = 1\}|$
- a **n-te Einheitswurzel** $:\Leftrightarrow a^n - 1 = 0$
- a **n-te primitive Einheitswurzel** $:\Leftrightarrow a^n - 1 = 0, a^j \neq 1 \; \forall j \in \{1, ..., n-1\}$
- $\Phi_n(x)$ **n-tes Kreisteilungspolynom** $:\Leftrightarrow \Phi_n(x) = \prod_{i=1}^{\varphi(n)}(x - a_i)$, $a_i{}^n - 1 = 0 \; \forall i = 1, ..., n$, $a_i{}^j - 1 \neq 0 \, \forall j = 1, ..., n-1$
- $p \in \mathbb{P}$ **Fermat'sche Primzahl** $:\Leftrightarrow \exists m \in \mathbb{N} : p = 2^m + 1$

Sätze

- $p, p_i \in \mathbb{P}, p_i$ pw. verschieden, $m, n, c_i \in \mathbb{N}$
  - $\varphi(p^c) = p^{c-1} \cdot (p-1)$
  - $(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
  - $n = \prod_{i=1}^{s} p_i^{c_i} \Rightarrow \varphi(n) = \prod_{i=1}^{s} p_i^{c_i - 1} \cdot (p_i - 1) = n \cdot \prod_{i=1}^{s}(1 - \frac{1}{p_i})$

- $E_n := \{a \in K : a^n - 1 = 0\}$
  - $|E_n| = n$
  - E_n ist bzgl. Multiplikation zyklische Gruppe.
  - Es existiert eine primitive n-te Einheitswurzel.
- $x^n - 1 = \prod_{d|n} \Phi_d$, $n = \sum_{d|n} \varphi(d)$
- $\Phi_n \in \mathbb{Z}$ normiert und irreduzibel $\forall n \in \mathbb{N}$
- $j + n\mathbb{Z} \in \mathbb{Z}_n^* \Leftrightarrow (j,n) = 1$
- $\mathbb{Z}_n^*$ zyklisch $\Leftrightarrow n \in \{1,2,4\} \vee n = p^c \vee n = 2p^c$, $p \in \mathbb{P} \backslash \{2\}$
- K Körper, $Char(K) = 0, a \in K$ n-te Einheitswurzel
  - Φ_n Minimalpolynom von a über $\mathbb{Q}$
  - $[\mathbb{Q}(a) : \mathbb{Q}] = \varphi(n)$
  - $\mathbb{Q}(a) : \mathbb{Q}$ Galoiserweiterung
  - Galoisgruppe $G(\mathbb{Q}(a) : \mathbb{Q}) \simeq \mathbb{Z}_n^*$
- Wiederholung zu Konstruktion mit Zirkel und Lineal
  - $r \in \mathbb{R}$ aus M konstruierbar $\Leftrightarrow$ P, Q konstruierbar, so dass $|PQ| = r$
  - $\mathbb{Q}(M) = \{a, b : (a,b) \in M\}$
  - $M = \{(0,0),(1,0)\} \Rightarrow \mathbb{Q}(M) = \mathbb{Q}$
  - $r \in \mathbb{R}$ aus M konstruierbar $\Leftrightarrow$ $\exists$ Körperkette $\mathbb{Q}(M) = K_0 \subset K_1 .. \subset K_s$: $r \in K_s, [K_i : K_{i-1}] = 2 \; \forall i = 1, .., s$
  - $M = \{(0,0),(1,0)\}, r \in \mathbb{R}$ aus M konstruierbar $\Rightarrow \exists n \in \mathbb{N}_0 : [\mathbb{Q}(r) : \mathbb{Q}] = 2^n$
- $\{(0,0),(1,0)\} \subset M \subset \mathbb{R}^2, K_0 := \mathbb{Q}(M), r \in \mathbb{R} :$ $K_0(r) : K_0$ Galoiserweiterung, $[K_0(r) : K_0] = 2^s, s \in \mathbb{N}_0 \Rightarrow r$ ist aus M konstruierbar
- $p = 2^m + 1$ Primzahl $\Rightarrow \exists i \in \mathbb{N}_0 : m = 2^i$
- regelmäßiges n-Eck aus $M = \{(0,0),(1,0)\}$ konstruierbar $\Leftrightarrow$ $n = 2^k \cdot \prod_{i=1}^{s} p_i :$ $k \in \mathbb{N}_0$, $p_i \in \mathbb{P}$ pw. verschiedene Fermat'sche Primzahlen

1.5 Lemma von Zorn

Definitionen

- $\leq$ **Halbordnung auf der Menge** $M :\Leftrightarrow \leq$ reflexive, anti-symmetrische, transitive Relation
- $m, n \in M$ **vergleichbar** $:\Leftrightarrow (m \leq n) \vee (n \leq m)$
- K **Kette von** $M :\Leftrightarrow K \subset M$, $[k, l \in K \Rightarrow k, l$ vergleichbar$]$
- $s \in T \subset M$ **obere Schranke von** $T :\Leftrightarrow t \leq s \; \forall t \in T$
- $t_0 = \in T \subset M$ **maximales Element von** $T :\Leftrightarrow \nexists t \in T : t_0 \leq t, t_0 \neq t$
- M **induktiv geordnet** $:\Leftrightarrow [K$ Kette von $M \Rightarrow K$ besitzt obere Schranke in $M]$

Sätze

- **Lemma von Zorn**: $\leq$ Halbordnung auf $M \neq \emptyset$:
  jede Kette von M besitzt eine obere Schranke $\Rightarrow$ M besitzt ein maximales Element
- **Auswahlaxiom**: I, A Mengen, $\emptyset \neq A_i \subset A \, \forall i \in I \Rightarrow \exists f : I \to A : \; f(i) \in A \, \forall i \in I$
- **Basisergänzungssatz**:
  V Vektorraum, $C \subset V$ lin. unabhängig $\Rightarrow$ $\exists$ Basis B von V mit $C \subset B$
- Jeder Vektorraum besitzt eine Basis.

1.6 Algebraischer Abschluss eines Körpers

Im Folgenden sei K stets ein Körper.

Definitionen

- K **algebraisch abgeschlossen** $:\Leftrightarrow \; [f \in K[x]$ irred. $\Rightarrow \; \mathrm{Grad}(f) = 1]$
- $\overline{K} : K$ Körpererweiterung:
  $\overline{K}$ **algebraischer Abschluss von** $K :\Leftrightarrow \; (\overline{K} : K$ alg.$) \wedge (\overline{K}$ alg. abgeschlossen $)$

Sätze

- K algebraisch abgeschlossen
  $\Leftrightarrow \; [f \in K[x]$ irred. $\Rightarrow \mathrm{Grad}(f) = 1]$
  $\Leftrightarrow \; [a$ algebraisch über $K \Rightarrow \; a \in K]$
  $\Leftrightarrow \; [L : K$ algebraisch $\Rightarrow \; L = K]$
- A Menge von Körpern: $[K_1, K_2 \in A \Rightarrow \; K_1$ Unterkörper von K_2 oder K_2 von K_1
  - T Oberkörper aller $K \in A \Rightarrow \; L := \bigcup_{K \in A} K$ Unterkörper von T
  - $\exists$ Verknüpfungen: L Oberkörper aller $K \in A$
- K Körper $\Rightarrow \; \exists$ alg. Abschluss von K
- $K_1 \simeq K_2$ Körper, $\overline{K_1}$ bzw. $\overline{K_2}$ alg. Abschluss, $\varphi : K_1 \to K_2$ Isomorphismus
  $\Rightarrow \; \exists \, \overline{\varphi} : \overline{K_1} \to \overline{K_2}$ Isomorphismus: $\overline{\varphi}_{|K_1} = \varphi$
- L_1, L_2 alg. Abschluss von $K \Rightarrow \; \exists \varphi : L_1 \to L_2$ Isomorphismus: $\varphi_{|K} =$id
- $\overline{K}$ alg. Abschluss von K, $L : K$ alg. Körpererw. $\Rightarrow \; \exists \, \varphi : L \to \overline{K}$ Körpermonomorphismus: $\varphi_{|K} =$id
- $f_i \in K[x] \, \forall i \in I \Rightarrow \; \exists \, L$ ZFK der $f_i, i \in I$, $L : K$ eindeutig bestimmt

2 Einblick in die algebraische Geometrie

Im Folgenden sei $K : L$ eine Körpererweiterung mit Char(K)=Char(L)=0, L alg. abgeschlosen.

2.1 Definitionen und erste Eigenschaften

Definitionen

- K **Grundkörper**, L **Koordinatenkörper**
- **algebraisches System über** K: System von Gleichungen $f_i(X_1, .., X_n) = 0, \; f_i \in L[X_1, .., X_n], i = 1, .., m$
- $V \subset L^n$ **affine algebraische** K**-Varietät** $:\Leftrightarrow \; V = \{(x_1, .., x_n) : \; f_i(x_1, .., x_n) = 0 \, \forall i = 1, .., m\}$
- **definierendes Gleichungssystem** zur K-Varietät V: algebraisches System zu V
- $V \cap K^n$ K**-rationale Punkte der Varietät** V
- $f_i, i = 1, .., m$ linear: **lineares System**
- V K**-Hyperfläche von** $L^n :\Leftrightarrow \; V$ kann durch eine Gleichung definiert werden
- V **ebene algebraische Kurve** $:\Leftrightarrow \; V$ K-Hyperfläche von L^2
- f **Minimalpolynom einer Hyperfläche** $V \; :\Leftrightarrow \; f$ definiert V, f quadratfrei, normiert
- K**-Grad** einer Hyperfläche V: Grad des Minimalpolynoms $\in K[X_1, .., X_n]$ von V
- **Grad** einer Hyperfläche V: Grad des Minimalpolynoms $\in L[X_1, .., X_n]$

Sätze

- $V_1, .., V_s$ Varietäten $\Rightarrow \; \bigcup_{i=1}^{s} V_i, \; \bigcap_{i=1}^{s} V_i$ Varietäten
- Seien $H_1 \neq \emptyset \neq H_2$ K-Hyperflächen des L^n, die durch $f_1 \neq 0 \neq f_2$ definiert werden:
  f_1 und f_2 teilerfremd $\Rightarrow \; H_1 \not\subseteq H_2, \; H_2 \not\subseteq H_1$
- $V \subset L^n$ K–Hyperflächen mit def., quadratfreiem Polynom $f \in K[X_1, .., X_n]$:
  $g \in K[X_1, .., X_n], \; g(P) = 0 \, \forall P \in V \Rightarrow f | g$
- $H \subset L^n$ L–Hyperfläche mit Grad d
  - $g \subset L^n$ Gerade $\Rightarrow \; (g \subset H) \; \vee \; (|g \cap H|) \leq d$
  - $\exists g \subset L^n$ Gerade: $|g \cap H| = d$

2.2 Basissatz und Nullstellensatz von Hilbert

Definitionen

- R **noetherscher Ring** $:\Leftrightarrow \; R$ Ring, jedes Ideal von R ist endlich erzeugbar $\Leftrightarrow \; [I \subset R$ Ideal $\Rightarrow \; \exists f_1, .., f_s \in I : \; I =< f_1, .., f_s >$

Sätze

- **Basissatz**: R noethersch $\Rightarrow$ $R[X_1,..,X_n]$ noethersch
- **Hilberts Nullstellensatz**: $L:K$ Körpererweiterung, L alg. abgeschlossen:
  I Ideal von $K[X_1,..,X_n]$, $I \neq K[X_1,..,X_n] \Rightarrow \mathcal{V}(I) = \{P \in L^n : f(P) = 0 \,\forall f \in I\} \neq \emptyset$

2.3 Ideale und Varietäten

Im Folgenden sei $L:K$ stets eine Körpererw., L alg. abg. und I Ideal von $K[X_1,..,X_n]$.

Definitionen

- $\mathcal{I}(V)$ **Verschwindungsideal** von $V \subset L^n :\Leftrightarrow \mathcal{I}(V) = \{f \in K[X_1,..,X_n : f(P) = 0 \,\forall P \in V\}$
- $\mathcal{V}(I)$ **Nullstellenmenge** von $I :\Leftrightarrow \mathcal{V}(I)$ **Varietät** zu $I :\Leftrightarrow \mathcal{V}(I) = \{P \in L^n : f(P) = 0 \,\forall f \in I\}$
- $\mathrm{Rad}I$ **Radikal** von $I :\Leftrightarrow \mathrm{Rad}I = \{f \in K[X_1,..,X_n] : \exists s \in \mathbb{N} : f^s \in I\}$
- P **Primideal** $:\Leftrightarrow [fg \in P \Rightarrow f \in P \vee g \in P]$
- Varietät V **zerlegbar** $:\Leftrightarrow \exists V_1, V_2$ Varietäten: $V_1 \neq V \neq V_2$, $V_1 \cup V_2 = V$

Sätze

- I Ideal von $K[X_1,..,X_n] \Rightarrow \mathcal{V}(I)$ K-Varietät von L^n
- $V \subset L^n \Rightarrow \mathcal{I}(V)$ Ideal von $K[X_1,..,X_n]$
- $\mathrm{Rad}I$ Ideal von $K[X_1,..,X_n]$
- $I \subset \mathrm{Rad}I = \mathrm{Rad}(\mathrm{Rad}I)$
- $\mathcal{V}(I) = \mathcal{V}(\mathrm{Rad}I)$
- Seien $V, V_1, V_2, V_s, s \in S$ K-Varietäten. Es gilt:
  - $\mathcal{I}(\emptyset) = K[X_1,..,X_n]$, $\mathcal{I}(L^n) = \{0\}$
  - $V \subset L^n \Rightarrow \mathcal{I}(V) = \mathrm{Rad}\big(\mathcal{I}(V)\big)$
  - $\mathcal{V}\big(\mathcal{I}(V)\big) = V$
  - $V_1 \subset V_2 \Leftrightarrow \mathcal{I}(V_1) \supset \mathcal{I}(V_2)$
  - $\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$, $V_1 \cup V_2 = \mathcal{V}\big(\mathcal{I}(V_1) \cap \mathcal{I}(V_2)\big)$
  - $V_1 \cup V_2 = \mathcal{V}\big(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2)\big)$
  - $V_s \subset L^n \,\forall s \in S \Rightarrow \bigcup_{s\in S} V_s = \mathcal{V}\big(\mathcal{I}(V_1) \cap \mathcal{I}(V_2)\big)$
  - $V_1 \supseteq V_2 \supseteq .. \Rightarrow \exists s \in \mathbb{N} : V_i = V_s \,\forall i \geq s$
- $\mathcal{I}\big(\mathcal{V}(I)\big) = \mathrm{Rad}I$

- I_1, I_2 Ideale: $\mathcal{V}(I_1) = \mathcal{V}(I_2) \Leftrightarrow \mathrm{Rad}I_1 = \mathrm{Rad}I_2$
- $f : \{V \subset L^n : V \text{ K-Varietät}\} \to \{I \subset K[X_1,..,X_n] : I \text{ Ideal, } \mathrm{Rad}I = I\}, V \mapsto \mathcal{I}(V)$ Bijektion
- Seien V_1, V_2 K-Varietäten. Es gilt:

$$\mathcal{I}(V_1 \cap V_2) = \mathrm{Rad}\big(\mathcal{I}(V_1) + \mathcal{I}(V_2)\big)$$

$$\mathcal{I}(V_1 \cup V_2) = \mathrm{Rad}\big(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2)\big) = \mathrm{Rad}\big(\mathcal{I}(V_1) \cap \mathcal{I}(V_2)\big)$$

- I maximales Ideal $\Rightarrow I = \mathrm{Rad}I$
- Seien $a_1,..,a_n \in K$. Es gilt:
  $J := (X_1 - a_1,..,X_n - a_n)$ max. Ideal von $K[X_1,..,X_n]$, $\mathcal{V}(J) = (a_1,..,a_n)$ (ein Punkt)
- Sei V Varietät. Es gilt: V zerlegbar $\Leftrightarrow \mathcal{I}(V)$ kein Primideal