Lineare Algebra II

Inoffizieller Mitschrieb

Stand: 17. April 2018

Vorlesung gehalten von:

Prof. Dr. Amador Martín-Pizarro
Abteilung für Angewandte Mathematik
Albert-Ludwigs-Universität Freiburg

0. Recap

Definition 0.1 – Ring

Ein (kommutativer) Ring (mit Einselement) ist eine Menge zusammen mit zwei binären Operationen $+, \cdot$, derart, dass:

- $(R, +)$ ist eine abelsche Gruppe
- $(R, \cdot)$ ist eine kommutative Halbgruppe
- die Dsitributivgesetze:
  $a(x + y) = ax + ay$
  $(x + y)z = xz + yz)$

Definition 0.2 – Integritätsbereich

Ein Integritätsbereich ist ein Ring ohne Nullteiler. Also $\forall x, y \in R : x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Definition 0.3 – Körper

Ein Körper ist ein Ring der Art, dass

1. $1 \neq 0$
2. $\forall x \in K : x \neq 0 \Rightarrow \exists x^{-1} : xx^{-1} = x^{-1}x = 1$

Bemerkung: Körper sind Integritätsbereiche.

Definition 0.4 – Charakteristik

Sei R ein nicht trivialer Ring ($0 \neq 1$). $\varphi : \mathbb{Z} \to R, z \mapsto \begin{cases} \sum_{i=1}^{n} 1 & n >= 0 \\ -\sum_{i=1}^{n} 1 & \text{ansonsten} \end{cases}$
Dann ist φ ein Ringhomomorphismus.
Für den Kern von φ ($\mathrm{Ker}(\varphi)$) gibt es zwei Möglichkeiten.

1. $\mathrm{Ker}(\varphi) = \{0\}, p = 0$
2. $\mathrm{Ker}(\varphi) \neq \{0\}$. Dann gibt es ein kleinstes echt positives Element $p \in \mathrm{Ker}(\varphi)$.

R hat dann Charakteristik p. Falls R ein Integritaetsbereich ist, dann ist p eine Primzahl. **Beispiele:**
$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \bar{n}\}$ hat Charakteristik n.
Insbesondere enthält jeder Körper mit Charakteristik p eine "Kopie" von $\mathbb{Z}/m\mathbb{Z}$:
k hat Charakteristik p $\Rightarrow \mathbb{Z}/p\mathbb{Z} \overset{injectiv}{\hookrightarrow} K$.
Hier ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper:
$a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \Rightarrow$ es ist a mit p teilerfremd. $1 = a \cdot b + p \cdot m \Rightarrow \bar{1} = \bar{a} \cdot \bar{b}$.

Definition 0.5 – Polynomring

Sei K ein Körper. Der Polynomring $K[T]$ in einer Variable R über K ist die Menge formeller Summen der Form:
$f = \sum_{i=0}^{n} a_i \cdot T^i, n \in \mathbb{N}$
Der Grad von $f \in K[T]$ ist definiert als:

Grad$(f) := max(m|m < n \wedge a_m \neq 0)$
Grad$(0) := -1$ Die Summe und das Produkt von Polynomen sind definiert als:
$\sum_{i=0}^{n} a_i T^i + \sum_{j=0}^{m} b_j T^j := \sum_{k=0}^{max(m,n)} (a_k b_k) T^k$
$\sum_{i=0}^{n} a_i T^i \cdot \sum_{j=0}^{m} b_j T^j := \sum_{k=0}^{m+j} = c_K T^k, c_k = \sum_i +j = k a_i b_j$

Bemerkung: $K[T]$ ist ein Integritätsbereich.

Korollar 0.6

Es seien f, g beide $\neq 0$
$\Rightarrow$ Grad$(f \cdot g) =$ Grad$(f) +$ Grad$(g) \Rightarrow f \cdot g \neq 0$
Grad$(f+g) \leq max($Grad$(f),$ Grad$(g))$

Satz 0.7 – Division mit Rest

Gegeben $f, g \in K[T],$ Grad$(g) > 0$. Dann existieren eindeutige Polynome q, r, so dass $f = g\dot{q} + r$, wobei Grad$(r) <$ Grad(g).

Beweis: Eindeutigkeit: Angenommen $f = g \cdot q + r = g \cdot q' + r', q \neq q' \vee r \neq r'$.
$\Rightarrow g(q-q') = r'-r \Rightarrow$ Grad$(r'-r) = max($Grad$(r'),$ Grad$(r)) <$ Grad$(g) =$ Grad$(g(q-q')) \Rightarrow$ Widerspruch
$\Rightarrow q = q' \Rightarrow r = r'$ Existenz: Induktion auf Grad(f)
Grad$(f) = 0 \Rightarrow f = g \cdot 0 + f$
Grad$(f) = n+1$
Grad$(f) <$ Grad$(g) = m \Rightarrow f = g \cdot 0 + f$
OBdA. $n+1 =$ Grad$(f) \geq$ Grad$(g) = m > 0$
$f = a_{n+1} \cdot T^{n+1} + \hat{f},$ Grad$(\hat{f}) \leq n, a_{n+1} \neq 0$
Sei $f' = f - b_m^{-1} a_{n+1} T^{n+1-m} \cdot g \Rightarrow$ Grad$(f') \leq n$ Ia: $f' = g \cdot q' + r',$ Grad$(r') <$ Grad(g)
$f' = f - b - b^{-1} a_{n+1} Tn + 1 - m \cdot g \Rightarrow f = g(b_n^{-1} a_{n+1} T^{n+1-m} + q') + r' \Rightarrow$ Grad$(r') <$ Grad(g) □

Definition 0.8 – Polynom Teilt

$f, g, q \in K[T]$, Grad$(g) > 0$
g teilt $f = g|_f \Leftrightarrow f = g \cdot q$

Definition 0.9 – Nullstellen von Polynomen

$f \in K[T]$ besizt eine Nullstelle $\lambda \in K$ gdw. $(T - \lambda)|_f \Leftrightarrow f(\lambda) = 0$.
f lässt sich dann schreiben als $f = (T - \lambda)q + r$.

Lemma 0.10

$f \in K[t], f \neq 0,$ Grad$(f) = n \Rightarrow$ f besitzt höchstens n Nullstellen in k.

Beweis:

$n = 0$ $\Rightarrow f = a_0, a_0 \neq 0$

$n > 0$ Falls f keine Nullstellen in K besitzt $\Rightarrow$ ok!
Sonst, sei $\lambda \in K$ eine Nullstelle von f. $f = (T - \lambda) \cdot g,$ Grad$(g) = n - 1 < n$

I.A besitzt g höchstens n - 1 Nullstellen. Jede Nullstelle von f ist entweder λ oder eine Nullstelle von g. $\Rightarrow$ f hat höchstens n Nullstellen.

$\square$

Definition 0.11 – Vielfachheit einer Nulstelle

$f \in K[T], f \neq 0, \lambda \in K$ Nullstelle von f $\Rightarrow f = (T - \lambda)^{K_\lambda} \cdot g, g(\lambda \neq 0$. K_λ ist die Vielfacheit der Nullstelle λ in f.

Definition 0.12

Ein Körper heißt algebraisch abgeschlossen, falls jedes Polynom über K positiven Grades eine Nullstelle besitzt.

Beispiele Ist $\mathbb{R}$ algebraisch abgeschlossen? Nein: $T^2 + 1$.
Bem.: $\mathbb{C}$ ist algebraisch abgeschlossen.
Bemerkung: Jeder algebraisch abgeschlossene Körper muss unendlich sein. Sei $K = \{\lambda_1, \dots \lambda_n\}, f = (T - \lambda), \dots, (T - \lambda_n) + 1$.

Lemma 0.13

K ist genau dann algebraisch abgeschlossen, wenn jedes Polynom positiven Grades in lineare Faktoren zerfällt.
$f = T(\lambda_1) \dots (T - \lambda_n)$.

Beweis:

$\Leftarrow$ trivial

$\Rightarrow$ $\mathrm{Grad}(f) = n > 0 \Rightarrow f = (T - \lambda_1) \cdot g, \mathrm{Grad}(g) \leq n - 1 < n \overset{I.A.}{\Rightarrow} f = c(T - \lambda_1) \dots (T - \lambda_n)$

$\square$