Geometrie WS2018/19

Dozent: Prof. Dr. Arno Fehm

7. Dezember 2018

Inhaltsverzeichnis

Vorwort

Wir freuen uns, dass du unser Skript für die Vorlesung *Geometrie* bei Prof. Dr. Arno Fehm im WS2018/19 gefunden hast. Da du ja offensichtlich seit einem Jahr Mathematik studierst, kannst du dich glücklich schätzen zu dem einen Drittel zu gehören, dass nicht bis zum zweiten Semester abgebrochen hat.

Wenn du schon das Vorwort zu *Lineare Algebra und analytische Geometrie 1+2* gelesen hast, weißt du sicherlich, dass Prof. Fehm ein Freud der Algebra ist.[1] Auf die Frage eines Kommilitonen, wo in seinem Inhaltsverzeichnis (Gruppen, Ringe, Körper) die Geometrie vorkomme, antwortete er:

> *Die Frage ist nicht, wieso wir in dieser Vorlesung Algebra statt Geometrie machen, sondern warum hier seit 20 Jahren Geometrie unterrichtet wird.*

Wie auch im letzten Vorwort können wir dir nur empfehlen die Vorlesung immer zu besuchen, denn dieses Skript ist kein Ersatz dafür. Es soll aber ein Ersatz für deine unleserlichen und (hoffentlich nicht) unvollständigen Mitschriften sein und damit die Prüfungsvorbereitung einfacher machen. Im Gegensatz zu letztem Semester veröffentlicht Prof. Fehm auf seiner Homepage (`http://www.math.tu-dresden.de/~afehm/lehre.html`) kein vollständiges Skript mehr, sondern nur noch eine Zusammenfassung.

Der Quelltext dieses Skriptes ist bei Github (`https://github.com/henrydatei/TUD_MATH_BA`) gehostet; du kannst ihn dir herunterladen, anschauen, verändern, neu kompilieren, ... Auch wenn wir das Skript immer wieder durchlesen und Fehler beheben, können wir leider keine Garantie auf Richtigkeit geben. Wenn du Fehler finden solltest, wären wir froh, wenn du ein neues Issue auf Github erstellst und dort beschreibst, was falsch ist. Damit wird vielen (und besonders nachfolgenden) Studenten geholfen.

Und jetzt viel Spaß bei *Geometrie*!

[1] In Zukunft wird sich Prof. Fehm richtig freuen dürfen, denn im Zuge einer neuen Studienordnung, die am 1.4.2019 in Kraft tritt, kommt so gut wie keine Geometrie im *Bachelor Mathematik* vor.

Kapitel I

Endliche Gruppen

Kapitel II

Kommutative Ringe

1. Erinnerung und Beispiele

▶ **Erinnerung 1.1**
Ein Ring ist eine abelsche Gruppe $(R, +)$ zusammen mit einer Verknüpfung $\cdot : R \times R \to R$ die Assoziativität und Distributivität erfüllt. Eine Teilmenge $\emptyset \neq S \subseteq R$ ist ein Unterring oder Teilring von R, wenn S abgeschlossen unter Addition, Subtraktion und Multiplikation ist. Eine Abbildung $\varphi : R \to R'$ zwischen Ringen ist ein Ringhomomorphismus , wenn $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ und $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ und in diesem Fall ist

$$\ker(\varphi) = \varphi^{-1}(\{0\})$$

der Kern von φ.

▶ **Bemerkung 1.2**
In dieser Vorlesung bedeutet "Ring" immer kommutativer Ring mit Einselement, d.h. $(R, \cdot)$ bildet ein kommutativer Monoid mit Einselement 1_R. Wir fordern dann zusätzlich, dass Unterringe von R das Einselement von R enthalten und dass Ringhomomorphismen $\varphi : R \to R'$ das Einselement von R auf das Einselement von R' abbilden.

■ **Beispiel 1.3**

1. Der Ring $\mathbb{Z}$ der ganzen Zahlen.
2. Der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$.
3. Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
4. Der Nullring $R = \{0\}$

Seien R, S Ringe. (Meisten Beweise sind LAAG1+2 Skript zu entnehmen!)

Satz 1.4
Ein Ringhomomorphismus $\varphi : R \to S$ ist ein Isomorphismus (d.h. bijektiv), wenn es einen Ringhomomorphismus $\psi : S \to R$ mit $\psi \circ \varphi = \mathrm{id}_R$ und $\varphi \circ \psi = \mathrm{id}_S$.

Satz 1.5
Ein Ringhomomorphismus $\varphi : R \to S$ ist genau dann injectiv, wenn $\ker(\varphi) = \{0\}$.

Definition 1.6
Für $x \in R$ heißt invertierbar oder eine Einheit , wenn es $y \in R$ mit $xy = 1$ gibt, und die $R^\times$ der Einheiten bildet eine Gruppe unter Multiplikation.
Für $x \in R$ ist eine Nullteiler , wenn es $0 \neq y \in R$ mit $xy = 0$ gibt, und R ist nullteilerfrei , wenn es keinen Nullteiler $0 \neq x \in R$ gibt.

■ **Beispiel 1.7**

1. $\mathbb{Z}$ ist nullteilerfrei, $\mathbb{Z}^\times = \mu_2 = \{\pm 1\}$.
2. $\mathbb{Z}/n\mathbb{Z}$ ist genau dann nullteilerfrei, wenn n prim ist.

■ **Beispiel 1.8**
Für eine Familie von Ringen $(R_i)_{i\in I}$ wird $\prod_{i\in I} R_i$ durch komponentenweise Addition und Multiplikation zu einem Ring, genannt das direkte Produkt der R_i. Bezeichnet 1_{R_i} das Einselement von R_i, so ist (1_{R_i}) das Einselement von $\prod_{i\in I} R_i$ und

$$(\prod_{i\in I} R_i)^\times = \prod_{i\in I} R_i$$

■ **Beispiel 1.9**
Der Polynomring eine Variablen x über R ist

$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in R, \text{ fast alle } a_i = 0 \right\}$$

mit der Addition und Multiplikation

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) + \left(\sum_{j=0}^{\infty} b_j x^j \right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

Ist $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit $a_n \neq 0$, so ist $\deg(f) = n$ der Grad von f (mit $\deg(0) = -\infty$) und $\mathrm{LC}(f) = a_n$ der Leitkoeffizient von f, f heißt normiert , wenn $\mathrm{LC}(f) = 1$.

Satz 1.10
Seien $f, g \in R[x]$.

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$
3. Ist $f \neq 0$ und $\mathrm{LC}(f)$ kein Nullteiler, so ist $\deg(fg) = \deg(f) + \deg(g)$.

Beweis. Siehe LAAG I.6.4. □

Folgerung 1.11
Ist R nullteilerfrei, so auch $R[x]$ und $(R[x])^\times = R^\times$.

Beweis.

- Ist $fg = 0$, so ist

$$-\infty = \deg(0) = \deg(fg) \overset{1.10}{=} \deg(f) + \deg(g)$$

folglich $f = 0$ oder $g = 0$.

- Ist $fg = 1$, so ist

$$0 = \deg(1) = \deg(fg) \overset{1.10}{=} \deg(f) + \deg(g)$$

folglich $\deg(f) = \deg(g) = 0$, d.h. $f, g \in R$. □

Satz 1.12 (Universelle Eigenschaft des Polynomrings)
Ist $\varphi : R \to S$ ein Ringhomomorphismus und $s \in S$, so gibt es genau einen Ringhomomorphismus $\varphi_s : R[x] \to S$ mit

$$\varphi_s|_R = \varphi \text{ und } \varphi_s(x) = S$$

Beweis. Ist $R[x] \to S$ ein Ringhomomorphismus mit $\varphi_s|_R = \varphi$ und $\varphi_{s(x)} = S$, so ist

$$\varphi_s\left(\sum_{i\geq 0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} \varphi_s(a_i)\varphi_s(x^i) = \sum_{i\geq 0}^{\infty} \varphi(a_i)s^i$$

eindeutig bestimmt. Umgekehrt ist das so definierte φ_s ein Ringhomomorphismus (Übung), der $\varphi_s|_R$ und $\varphi_s(x) = s$ erfüllt. □

▶ **Bemerkung 1.13**
Insbesondere hat man für $a \in R$ den Einsetzungshomomorphismus:

$$\varphi_a : \begin{cases} R[x] & \to R \\ f & \mapsto f(a) \end{cases}$$

gegeben durch $\varphi_a\,|_R = \mathrm{id}_R$ und $\varphi_a(x) = a$. Dies liefert eine Abbildung

$$\begin{cases} R[x] & \to \mathrm{Abb}(R, R) \\ f & \mapsto \tilde{f}, \tilde{f}(a) = \varphi_a(f) \end{cases}$$

Diese Abbildung ist im Allgemeinen nicht injectiv!!! Sei z.B. für $R = \mathbb{Z}/n\mathbb{Z}$ und $f = x^2 + x$ ist $f(0) = \overline{0}$, $f(\overline{1}) = \overline{0}$, aber $\tilde{f} = \tilde{0}$, aber $f \neq 0$.

Satz 1.14 (Polynomdivision)
Sei $0 \neq g \in R[x]$ mit $\mathrm{LC}(g) \in R^\times$. Zu jedem Polynom $f \in R[x]$ gibt es eindeutig bestimmte $q_1 r \in R[x]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.

Beweis. Wie im Falle $R = K$ ein Körper.

- **Eindeutigkeit:** Sei $f = q_1 g + r_1 = q_2 g + r_2$ und $\deg(r_1) < \deg(g) \Rightarrow r_1 - r_2 = (q_2 - q_1)g$. Da $\mathrm{LC}(g) \in R^\times$ ist $\mathrm{LC}(g)$ kein Nullteiler $\overset{1.10}{\Rightarrow} \deg(r_1 - r_2) < \deg(g) = \deg(q_2 - q_1) + \deg(g)$

$\Rightarrow \deg(q_2 - q_1) < 0 \Rightarrow q_1 = q_2$ und $r_1 = r_2$

- **Existenz:** Sei $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$ und $g = \sum_{j=0}^{m} b_j x^j$ mit $b_m \neq 0$. Nach Vorraussetzung ist $b_m \in R^\times$ es existiert also $b_m^{-1} \in R$.
  Induktion nach $\deg(f) = n$:
  - $n < m$**:** $q = 0$, $r = f$
  - $n \geq m$**:** $f_i = f - a_n b_m^{-1} x^{n-m} \cdot g \Rightarrow \deg(f_1) < \deg(f)$ mit Induktionshypothese folgt $f_1 = q_1 \cdot g + r_1$ mit $\deg(r) < m \Rightarrow f = (q_1 + a_n b_m^{-1} x^{n-m})g + r$ □

Folgerung 1.15
Ist $f \in R[x]$ und $a \in R$, $f(a) = 0$, so ist

$$f(x) = (x - a) \cdot q(x) \text{ mit } q \in R[x].$$

Beweis. Sei $f = q(x - a) + r$, $\deg(r) < \deg(x - a)$, d.h. $\deg(1) \leq 0 \Rightarrow 0 = f(a) = q(a - a) + r(a) \Rightarrow r(a) = 0$.□

Folgerung 1.16
Ist R nullteilerfrei, so hat $0 = f \in R[x]$ höchstens $\deg(f)$ viele Nullstellen in R.

Definition 1.17 (Polynomring in kommutieren Variablen)
Für eine Menge I definieren wir den Monoid

$$\mathbb{N}_0^{(I)} := \left\{ (\mu_i)_{i\in I} \in \prod_{i\in I} \mathbb{N}_0 \colon \mu_i = 0 \text{ für fast alle } i \right\}$$

mit Addition

$$(\mu_i)_{i\in I} + (\nu_i)_{i\in I} := (\mu_i + \nu_i)_{i\in I},$$

sowie den Ring

$$R[x_i \colon i \in I] = \{(\mu)_{\mu\in\mathbb{N}_0} \colon a_\mu \in R, \text{ fast alle gleich } 0\}$$

mit Addition

$$(a_\mu)_{\mu\in\mathbb{N}_0}^{(I)} + (b_\mu)_{\mu\in\mathbb{N}_0}^{(I)} := (a_\mu + b_\mu)_{\mu\in\mathbb{N}_0}^{(I)}$$

und Multiplikation

$$(a_\lambda)_{\lambda\in\mathbb{N}_0^{(I)}} \cdot (b_\nu)_{\nu\in\mathbb{N}_0^{(I)}} = \left(\sum_{\lambda+\nu=\mu} a_\lambda b_\mu \right)_{\mu\in\mathbb{N}_0}^{(I)},$$

gennant Polynomring in kommutierenden Variablen $x_i, i \in I$. Wir identifizieren den Ring R mit den Unterring

$$\{(r\delta_{\mu,\underline{0}})_{\mu\in\mathbb{N}_0}^{(I)} \colon r \in R\}.$$

Wir schreiben $x_i := (\delta_{\mu\nu})_{\mu\in\mathbb{N}_0}^{(I)}$, $\mu := (\delta_{ij})_{i\in I}$ und $x^\mu := \prod_{i\in I} x_i^{\mu_i}$. Damit ist dann

$$(a_\mu)_{\mu\in\mathbb{N}_0}^{(I)} = \sum_{\mu\in\mathbb{N}_0}^{(I)} a_\mu x^\mu.$$

Weiter schreiben wir

$$R[x_1, \ldots, x_n] := R[x_i \colon i \in \{i, \ldots, n\}].$$

■ **Beispiel 1.18**
Sei $R = \mathbb{Z}$ und $I = \{1, 2\}$, dann

$$\left(x_1x_2 + x_2^2\right)^2 = a_{(2,1)}x_1^2x_2^2 + a_{(1,3)}x_1x_2^2 + a_{(0,4)}x_2^4$$

mit $a_{(2,1)} = 1$, $a_{(1,3)} = 2$ und $a_{(0,4)} = 1$

▶ **Bemerkung 1.19**
Satz 1.10 und Satz 1.12 kann man allgemein für $R[x_i \colon i \in I]$ anstatt $R[x]$ formulieren. Für Satz 1.14

- Folgerung 1.16 gibt es keine Verallgeminerung. So hat z.B. $f = x_1 - x_2$ unendlich viele Nullstellen, da $f(a, a) = 0$ für alle $a \in \mathbb{Z}$.

Kapitel III

Körpererweiterungen

Anhang

Anhang A: Listen

A.1. Liste der Theoreme

A.2. Liste der benannten Sätze, Lemmata und Folgerungen