Das Lemma von Gauß und Quotientenringe

Proseminar Körpertheorie, 02.05.2013

Fabian Cejka

Prof. K. Wingberg, K. Hübner

Zusammenfassung In diesem Teil des Proseminars wird zunächst bewiesen, dass jedes irreduzible Element in $K[X]$ prim ist. Dadurch kann dann gezeigt werden, dass es für jedes Polynom in $K[X]$ eine eindeutige Zerlegung in irreduzible normierte Polynome gibt.
Im Zweiten Abschnitt wird von einem Ring und einem Ideal darin ausgehend der sogenannte Quotientenring modulo diesem Ideal kontruiert. Schließlich wird diese Konstruktion auf $K[X]$ angewandt und dort eine erste Eigenschaft bewiesen.

1 Vorbereitung

K bezeichnet stets einen Körper, nicht näher definierte Ringe sind kommutativ.

Definition 1. *$P \in K[X] - (K^\times \cup \{0\})$ heißt **irreduzibel**, falls aus $P = AB$ mit $Q, R \in K[X]$ stets $A \in K^\times$ oder $B \in K^\times$ folgt.*

Definition 2. *$A \in K[X]$ heißt **Teiler** von $B \in K[X]$, in Zeichen $A \mid B$, wenn es $C \in K[X]$ mit $AC = B$ gibt*

Definition 3. *$P \in K[X] - (K^\times \cup \{0\})$ heißt **prim**, falls aus $P \mid AB$ mit $A, B \in K[X]$ stets $P \mid A$ oder $P \mid B$ folgt.*

Definition 4. *Zwei Polynome $A, B \in K[X]$ heißen **teilerfremd**, falls aus $P \mid A$ und $P \mid B$ für $P \in K[X]$ stets $P \in K^\times$ folgt.*

Satz 5 (Satz von Bézout). *Sind $A, B \in K[X]$ teilerfremd, so existieren $U, V \in K[X]$ mit $AU + BV = 1$ (siehe [AC])*

2 Lemma von Gauß

Satz 6 (Lemma von Gauß). *Für ein irreduzibles $P \in K[X]$ gilt:*

$$P \mid AB \text{ mit } A, B \in K[X] \Longrightarrow (P \mid A \vee P \mid B)$$

Beweis. Gelte $P \mid AB$ und $P \nmid A$ (für $P \mid A$ ist nichts zu zeigen). Um $P \mid B$ zu folgern, zeigt man znächst die Teilerfremdheit von A und P. Betrachte deshalb $Q \in K[X]$ mit $Q \mid P$ bzw. $S \cdot Q = P$ für ein $S \in K[X]$. Wegen der Irreduzibilität

von P folgt, dass in dieser Zerlegung Q oder S eine Einheit ist. Ist nun S eine Einheit, so kann man $Q = S^{-1} \cdot P$ schreiben. Aus $P \nmid A$ folgt jedoch, dass $S^{-1} \cdot P \nmid A$ gilt und somit nur Einheiten gemeinsame Teiler von A und P sind.

Nach dem Satz von Bézout existieren in diesem Fall $U, V \in K[X]$ mit

$$\begin{aligned} AU + PV &= 1 \\ \Longrightarrow ABU + PBV &= B \end{aligned} \tag{1}$$

Aus $P \mid AB$ folgt die Existenz eines $Q \in K[X]$ mit $AB = PQ$. Einsetzen in (1) ergibt:

$$P(QU + BV) = B \Longrightarrow P \mid B$$

□

Satz 7. *$K[X]$ ist **faktoriell**, d.h. jedes $A \in K[X] - \{0\}$ lässt sich (bis auf Reihenfolge) eindeutig in der Form $A = a \cdot \prod_{i=1}^{m} P_i^{n_i}$ schreiben. Dabei ist $a \in K^\times$, $m \geq 0$, $n_i \in \mathbb{N}$ und P_i sind normierte, voneinander verschiedene, irreduzible Polynome aus $K[X]$.*

Beweis. Sei A irreduzibel und a höchster Koeffizient von A. Setze $P := a^{-1} \cdot A \in K[X]$ und erhalte $A = a \cdot P$. Weil P irreduzibel und normiert ist und es genau ein multiplikativ Inverses zu a in K gibt, ist die Zerlegung von geforderter Art. Sei A reduzibel. Folglich existieren nicht-konstante Polynome $A_1, A_2 \in K[X]$ mit $A_1 \cdot A_2 = A$. Weil $K[X]$ ein Integritätsring ist, gilt $\deg A = \deg A_1 + \deg A_2$, was zusammen mit der Nicht-Konstanz von A_1 und A_2

$$1 \leq \deg A_1, \deg A_2 < \deg A \in \mathbb{N} \tag{2}$$

impliziert. Diese Zerlegung führt man für A_1 und A_2 falls möglich fort. Aufgrund von (2) bricht das Verfahren nach endlich vielen Schritten ab und man erhält eine Zerlegung in irreduzible Polynome. Sind $a_1, \ldots, a_r$ die höchsten Koeffizienten der $r \in \mathbb{N}$ irreduziblen Polynome, so multipliziert man diese Zerlegung mit $a_1^{-1} \cdot \ldots \cdot a_r^{-1}$ und hat dann eine Zerlegung der geforderten Art.

Um nun die Eindeutigkeit zu zeigen, betrachte man zu einer Zerlegung $A = aP_1 \cdot \ldots \cdot P_r$, eine weitere Zerlegung $A = a'Q_1 \cdot \ldots \cdot Q_s$, wobei $r, s \in \mathbb{N}, P_i, Q_j \in K[X]$ normiert und irreduzibel. Ohne Einschränkung kann $r \leq s$ angenommen werden. Weil das Produkt normierter Polynome wieder normiert ist, gilt $a = a'$. Aus $P_1 \mid A = a'Q_1 \cdot \ldots \cdot Q_s$ folgt mit dem Lemma von Gauß $P_1 \mid Q_j$ für ein $j \in \{1, \ldots, s\}$, und durch Umnummerierung $P_1 \mid Q_1$ bzw. $RP_1 = Q_1$ für ein $R \in K[X]$. Aus der Normiertheit und der Irreduzibilität von Q_1 folgt hieraus $R = 1$ und $P_1 = Q_1$. Somit gilt:

$$A/(aP_1) = P_2 \cdot \ldots \cdot P_r = Q_2 \cdot \ldots \cdot Q_s$$

Auf gleiche Weise wird gezeigt, dass nach entsprechenden Umnummerierungen $P_i = Q_i$, für $i \in \{2, \ldots r\}$ ist und schließlich

$$A/(aP_1 \cdot \ldots \cdot P_r) = 1 = Q_{r+1} \cdot \ldots \cdot Q_s$$

folgt. Da Q_j keine Einheiten sind, folgt $r = s$ und insgesamt die Eindeutigkeit der Zerlegung.

□

Beispiel 8. Ein Beispiel für einen Ring, der nicht faktoriell ist, ist $A := \mathbb{Z} + \sqrt{-5} \cdot \mathbb{Z} \subset \mathbb{C}$ mit den irreduziblen und paarweise nichtassoziierten Elementen $2, 3, \left(1 + \sqrt{-5}\right), \left(1 - \sqrt{-5}\right) \in A$. Für $6 \in A$ gilt jedoch

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$$

Es heißen $a, b \in A$ assoziiert, wenn es $c \in A^\times$ mit $b = c \cdot a$ gibt (siehe [SB]). Eine Primfaktorzerlegung in einem faktoriellen Ringen ist bis auf Assoziiertheit (und Reihenfolge) eindeutig. Beispielsweise ist $6 = (-2) \cdot (-3)$ eine weitere Zerlegung von $6 \in A$, doch -2 bzw. -3 und 2 bzw. 3 sind assoziiert. Die Zerlegungen in $K[X]$ in obigem Satz sind eindeutig, da nur Zerlegungen in normierte Polynome betrachtet werden.

3 Quotientenringe

Satz 9. *Auf dem Ring R mit einem Ideal $I \neq R$ definiert*

$$r_1 \sim r_2 :\Longleftrightarrow r_1 - r_2 \in I \quad , r_1, r_2 \in R$$

eine Äquivalenzrelation.

Die Menge der Äquivalenzklassen R/I bildet zusammen mit den Verknüpfungen

$$\begin{aligned} + &: R/I \times R/I \longrightarrow R/I, \quad [a] + [b] = [a + b] \\ \cdot &: R/I \times R/I \longrightarrow R/I, \quad [a] \cdot [b] = [a \cdot b] \end{aligned}$$

einen Ring,den ***Quotientenring*** *R* ***modulo*** *I.*

Beweis. Zuerst wird nachgewiesen, dass es sich bei "$\sim$" um eine Äquivalenzrelation handelt. Für $a \in R$ gilt $a \sim a$ wegen $a - a = 0 \in I$. Weil I eine additive Untergruppe ist, folgt aus $a \sim b$ bzw. $a - b \in I$ für $a, b \in R$, dass $-(a - b) \in I$ bzw. $b \sim a$. Ist schließlich $a \sim b$ und $b \sim c$ für $a, b, c \in R$, so gilt zunächst $a - b \in I$, $b - c \in I$ und aus der Untergruppeneigenschaft von I folgt

$$a - c = (a - b) + (b - c) \in I$$

also $a \sim c$.

Nun wird die Wohldefiniertheit der Verknüpfungen gezeigt. Eine Verknüpfung ist insbesondere eine Abbildung. Eine Abbildung heißt (vereinfacht formuliert) wohldefiniert, wenn jedem Element aus dem Definitionsbereich genau ein Element in der Zielmenge zugeordnet wird. In den betrachteten Verknüpfungen ist diese Eigenschaft nicht unmittelbar einzusehen, denn das zugeordnete Element

in der Zielmenge scheint vom Repräsentanten der verknüpften Äquivalenzklassen abzuhängen.

Gelte $[a] = [a'], [b] = [b'], a, b, a', b' \in R$. Aus [LA1] folgt:

$$a \sim a', b \sim b' \Longleftrightarrow a' = a + x, b' = b + y, \quad x, y \in I$$

Dadurch ist

$$\begin{aligned} a' + b' &= a + b + (x + y), \\ a'b' &= ab + (ay + bx + xy) \end{aligned}$$

also $[a + b] = [a' + b'], [ab] = [a'b']$

Schließlich ist $(R/I, +, \cdot)$ ein Ring, da die Verknüpfungen so definiert sind, dass sich die Ringeigenschaften von R auf R/I übertragen, z.B.:

$$\begin{aligned} (K+) &\quad [a] + [b] = [a + b] = [b + a] = [b] + [a] \\ (I+) &\quad \text{Das additiv Inverse zu } [a] \text{ ist } [-a] \\ (N\cdot) &\quad [1] \text{ ist das neutrale Element der Multiplikation} \end{aligned}$$

□

Korollar 10. *Für $x \in R$ gilt: $x \in [0] \Longleftrightarrow x - 0 = x \in I$*

In folgendem Satz wird die kanonische Projektion auf den Quotientenring definiert. Dabei wird auch die übliche Notation für Elemente aus dem Quotientenring eingeführt.

Satz 11. *Die Abbildung $\Pi : R \longrightarrow R/I, a \longmapsto \overline{a} := [a]$ definiert einen surjektiven Ringhomomorphismus mit* $\ker \Pi = I$

Beweis. Π ist ein Ringhomomorphismus:

$$\begin{aligned} \Pi(a + b) &= \overline{a + b} = \overline{a} + \overline{b} = \Pi(a) + \Pi(b) \\ \Pi(a \cdot b) &= \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \Pi(a) \cdot \Pi(b) \\ \Pi(0) &= \overline{0} \\ \Pi(1) &= \overline{1} \end{aligned} \tag{3}$$

Dabei gilt (3) wegen $I \neq R$. Die Surjektivität ist damit begründet, dass R/I aus den Äquivalenzklassen von Elementen aus R besteht. Aufgrund der Reflexivität von "$\sim$" sind diese Elemente jeweils in ihrer eigenen Äquivalenzklasse enthalten. $\ker \Pi = I$ folgt aus obigem Korollar.

□

Beispiel 12. Sei $P \in K[X] - (K^\times \cup \{0\})$. Betrachte $K[X]/(P)$. Sei $A \in K[X] - \{0\}$ und $A = PQ + R$ die euklidische Division A durch P, also eindeutige $Q, R \in K[X], \deg R < \deg P$. Dann ist $\overline{A} = \overline{R}$. Somit besteht ein Element in $K[X]/(P)$ aus all jenen Polynomen aus $K[X]$, die bei euklidischer Division durch P denselben Rest haben.

Beispiel 13. Sei $p \in \mathbb{Z} - \{\pm 1\}$. Betrachte $\mathbb{Z}/(p)$. Sei $m \in \mathbb{Z} - \{0\}$ und $m = sp+r$ die euklidische Division m durch p, also eindeutige $s, p \in \mathbb{Z}, |r| < |p|$. Dann ist $\overline{m} = \overline{r}$ und ein Element aus $\mathbb{Z}/(p)$ besteht aus all jenen ganzen Zahlen, die bei euklidischer Division durch p denselben Rest haben.

Satz 14. *Sei $P \in K[X] - (K^\times \cup \{0\})$. Es ist äquivalent:*

(i) $K[X]/(P)$ *ist ein Körper.*
(ii) $K[X]/(P)$ *ist ein Integritätsring.*
(iii) P *ist irreduzibel in* $K[X]$

Beweis. Bedingung (i) impliziert (ii) (siehe dazu [LA1]).

Um (iii) indirekt aus (ii) herzuleiten, sei P reduzibel, also $\deg P \geq 2$ und $P = QR$ eine Zerlegung von P in $K[X]$ mit $Q, R \in K[X] - (K^\times \cup \{0\})$. Dass P, Q nicht konstant sind, führt unter Berücksichtigung dessen, dass $K[X]$ ein Integritätsring ist, zu

$$1 \leq \deg R, \deg Q < \deg P$$

Bei der euklidischen Division durch P lassen R und Q somit von 0 verschiedenene Reste. Es gilt also $\overline{Q}, \overline{R} \neq \overline{P} = \overline{0}$, doch $\overline{P} = \overline{QR} = \overline{Q} \cdot \overline{R} = \overline{0}$. Damit sind Q, R Nullteiler in $K[X]/(P)$.

Um (i) aus (iii) zu folgern, genügt es $(K[X]/(P))^\times = K[X]/(P) - \{0\}$ zu zeigen, da $K[X]/(P)$ bereits ein Ring ist. Sei P irreduzibel in $K[X]$, $\overline{A} \in K[X]/(P) - \{0\}$ und $A \in \overline{A}$ mit $degA < degP$ (Dass dieses Polynom existiert, wird in Beispiel 12 gezeigt). A und P sind teilerfremd in $K[X]$, weshalb wegen des Satzes von Bézouts $U, V \in K[X]$ existieren mit

$$UA + VP = 1$$

Weil $VP \in \overline{0}$ folgt

$$\overline{U} \cdot \overline{A} = 1$$

also die Existenz eines multiplikativ Inversen zu einem beliebigen Element aus $K[X]/(P) - \{0\}$ bzw. $(K[X]/(P))^\times = K[X]/(P) - \{0\}$

□

Literatur

[AC] Chambert-Loir, A.: A field guide to algebra. Springer, 1999
[LA1] Wingberg, K.: Lineare Algebra (Vorlesung), WS 2012
[SB] Bosch, S.: Algebra. Springer, 2009