Proseminar Körpertheorie

Einstieg in die Theorie der Körper

Kristina Maria Zapp

16.05.2013

Professor Dr. K. Wingberg, K. Hübner

I. Die Universelle Abbildungseigenschaft von $K[X]/(P)$

Theorem 1.1: Sei K ein Körper, P ein Polynom in $K[X]$ und $j: K \to K[X]/(P)$ der kanonische Ringhomomorphismus. Sei $i: K \to B$ ein Ringhomomorphismus und y eine Nullstelle von P in B. Dann existiert genau ein Ringhomomorphismus $f: K[X]/(P) \to B$ der sowohl $f \circ j = i$ als auch $f(\bar{X}) = y$ erfüllt. Hierbei bezeichnet $\bar{X}$ die Äquivalenzklasse von X in $K[X]/(P)$.

Beweis: Zuerst soll die Eindeutigkeit der Abbildung gezeigt werden: Nach Voraussetzung muss die Abbildung $f(\bar{X}) = y$ erfüllen sowie alle $\bar{k} = j(k)$ mit $k \in K$ auf $f(\bar{k}) = i(k)$ abbilden, sodass $f \circ j = i$ gilt. Damit ist der Ringhomomorphismus f, falls dieser existiert, bereits eindeutig festgelegt. Denn alle Äquivalenzklassen aus $K[X]/(P)$ sind multiplikative und additive Verknüpfungen von Äquivalenzklassen der konstanten Polynome und $\bar{X}$. Da K ein Körper ist, ist der Ringhomomorphismus $i: K \to B$ injektiv; deswegen können in diesem Beweis alle $i(k) \in B$ eindeutig mit ihren Urbildern $k \in K$ identifiziert werden. Dies liefert die Abbildungsvorschrift:

$$f: K[X]/(P) \to B, \bar{Q} \mapsto Q(y).$$

Damit ist die Eindeutigkeit des Homomorphismus gezeigt. Für die Existenz ist zu zeigen, dass die oben definierte Abbildung f wohldefiniert und ein Ringhomomorphismus ist.

Die Wohldefiniertheit ergibt sich daraus, dass $\bar{X}$ auf y , also auf eine Nullstelle von P in B abgebildet wird. Falls $Q, R \in K[X]$ mit $\bar{Q} = \bar{R}$ gilt, so ist $Q = R + SP$ für ein $S \in K[X]$. Daraus folgt $f(\bar{Q}) = Q(y) = (R + SP)(y) = R(y) + SP(y) = R(y) + 0 = f(R)$. Somit ist $f(\bar{Q})$ unabhängig von der Wahl einer Äquivalenzklasse.

Damit f ein Ringhomomorphismus ist, müssen die folgenden vier Eigenschaften erfüllt sein (vgl. Definition 1.2.8, Seite 5):

(1) $K[X]/(P)$ und B sind Ringe
(2) $\forall\, a, b \in K[X]/(P)$ gilt: $f(a + b) = f(a) + f(b)$
(3) $\forall\, a, b \in K[X]/(P)$ gilt: $f(ab) = f(a)f(b)$
(4) $f(0_{K[X/(P)]}) = 0_B, f(1_{K[X]/(P)}) = 1_B$

B ist nach Voraussetzung ein Ring. Dass $K[X]/(P)$ ein Ring ist wird in 2.1.1 (Seite 31/32) gezeigt. Aus der Abbildungsvorschrift geht hervor, dass $\bar{0}$ und $\bar{1}$ auf 0 bzw. 1 abgebildet

werden. Denn $f(\bar{0}) = 0(y) + S(y)P(y) = 0$ und $f(\bar{1}) = 1(y) + S(y)P(y) = 1,\ S \in K[X]$ beliebig. Damit gilt (4). Demnach ist noch zu zeigen, dass f die Addition und Multiplikation in $K[X]/(P)$ respektiert. Dies ergibt sich aus den Eigenschaften der Addition und Multiplikation in $K[X]/(P)$ (vgl. Vortrag 3: Das Lemma von Gauß und Quotientenringe). Es gilt:

$$f(\bar{Q} + \bar{R}) = f(\overline{Q+R}) = (Q+R)(y) = Q(y) + R(y) = f(Q) + f(R)$$

Sei $Q * R = QR - PS$ mit $S \in K[X]$ der Rest von QR bei Polynomdivision durch P. Für die Multiplikation gilt dann:

$$f(\bar{Q}\bar{R}) = f(\overline{QR}) = (QR)(y) = (Q * R)(y) + P(y)S(y) = Q(y)R(y) = f(Q)f(R).$$

Somit ist f ein Ringhomomorphismus.

II. Der Satz von Kronecker

Definition 2.1: Seien $i: E \to F$ und $j: E \to F'$ zwei Körpererweiterungen. Dann nennt man einen Körperhomomorphismus $f: F' \to F$, der $f \circ j = i$ erfüllt, Erweiterungshomomorphismus von F' nach F. Ein bijektiver Erweiterungshomomorphismus wird als Erweiterungs-isomorphismus bezeichnet.

Theorem 2.2 (Satz von Kronecker): Sei K ein Körper und P ein irreduzibles Polynom aus $K[X]$, dann existiert eine endliche Körpererweiterung $K \to K_1$ und eine Nullstelle von P in K_1 derart, dass

(1) $K_1 = K[x]$
(2) Für alle Körpererweiterungen $K \to L$ kann die Menge A der Erweiterungs-homomorphismen von K_1 nach L bijektiv auf die Menge B der Nullstellen von P in L abgebildet werden. Die Abbildung $i: A \to B, f \mapsto f(x)$ definiert eine Bijektion.

Beweis: Zu (1): Man setze $K_1 = K[X]/(P)$ und $x = \bar{X}$. Da P irreduzibel ist, ist $K[X]/(P)$ ein Körper. P hat nach Konstruktion die Nullstelle $\bar{X}$ in $K_1 = K[X]/(P)$. Eine Basis von $K[X]/(P)$ ist durch $\{1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{\deg P - 1}\}$ gegeben, die Körpererweiterung $K \to K_1$ ist also endlich. Aus der angegebenen Basis wird ebenso $K_1 = K[\bar{X}] = K[X]/(P)$ deutlich. Denn sei

$\bar{Q} \in K[X]/(P)$ und Q ein Repräsentant aus $\bar{Q}$ so ist $\bar{Q} = Q(\bar{X}) = Q(x) \in K_1$. Sei umgekehrt $Q(x) \in K_1$ so ist $Q(x) = Q(\bar{X}) = \bar{Q} \in K[X]/(P)$.

Zu (2): Zuerst ist zu zeigen, dass die definierte Abbildung i wohldefiniert ist, das heißt dass für alle $f \in A$ ein eindeutiges $b \in B$ existiert mit $i(f) = b$. Es ist $P(f(x)) = f(P(x)) = f(0) = 0$, da f ein Körperhomomorphismus ist. Daraus folgt $i(f) \in B$. Wie im Beweis zur universellen Abbildungseigenschaft gezeigt wurde, ist die Wohldefiniertheit für ein beliebiges $f \in A$ nur gegeben, wenn f die Äquivalenzklasse von X auf eine Nullstelle abbildet. In dem Beweis wurde gezeigt, dass zu jeder Nullstelle genau ein solcher Erweiterungshomomorphismus existiert, der $\bar{X}$ auf die betreffende Nullstelle abbildet. Durch die Existenz des Erweiterungshomomorphismus ist die Surjektivität von i gezeigt und durch die Eindeutigkeit die Injektivität von i. Also ist i bijektiv.

III. Zerfällungskörper

Idee: Sei K ein Körper. Für ein nicht konstantes Polynom P aus $K[X]$ soll der minimale Körper konstruiert werden, der alle Nullstellen von P enthält.

Definition 3.1: Sei K ein Körper und P ein nicht-konstantes Polynom aus $K[X]$. Ein Zerfällungskörper von P ist eine Körpererweiterung $j: K \to E$ sodass,

(1) P in E vollständig in Linearfaktoren zerfällt, das heißt $P = c\prod_{i=1}^{d}(X - x_i)$, wobei c der höchste Koeffizient von P ist, d der Grad von P und für alle x_i gilt: $x_i \in E$.
(2) E ist der Körper, der durch K und die Elemente $x_1, \dots, x_d$ erzeugt wird: $E = K(x_1, \dots, x_d)$. Das heißt E entsteht durch Adjunktion aller Nullstellen von P zu K.

Theorem 3.2: Sei K ein Körper und P ein nicht konstantes Polynom aus $K[X]$. Dann gilt:

(1) Es existiert ein Zerfällungskörper von P.
(2) Zwei beliebige Zerfällungskörper sind isomorph. Genauer: Seien $j: K \to E$ und $j': K \to E'$ Zerfällungskörper von P. Dann existiert ein Körperisomorphismus $f: E \to E'$, sodass $f \circ j = j'$.

Beweis: (1) und (2) werden per vollständiger Induktion nach dem Grad von P gezeigt. Für $\deg P = 1$ zerfällt P bereits über K selbst, demnach ist $E = K$ ein Zerfällungskörper von P. (1) gelte nun für alle $P \in K[X]$ mit $\deg P = n$. Sei nun $\deg P = n + 1$. Für P mit $\deg P \geq 1$

gilt, dass P irreduzibel ist oder einen irreduziblen Faktor enthält, denn $K[X]$ ist faktoriell. Sei nun $Q \in K[X]$ ein irreduzibler Faktor von P. Nach dem Satz von Kronecker existiert dann eine Körpererweiterung $j: K \to K_1,\ K_1 = K[x_1]$ für ein $x_1 \in K_1$ mit $Q(x_1) = 0$. Da Q ein Faktor von P ist, ist in K_1 auch $P(x_1) = 0$. Somit ergibt sich in K_1: $P = (X - x_1)P_1$. P_1 ist nun ein Polynom mit Koeffizienten in $K[x_1] = K_1$, das heißt $P_1 \in K_1[X]$. Außerdem folgt $\deg P_1 = n$. Nach Induktionsvoraussetzung gibt es dann eine Körpererweiterung $i: K_1 \to E$, sodass P_1 in E vollständig in Linearfaktoren zerfällt. Seien $x_2, .., x_{n+1}$ die Nullstellen von P_1 in E. Dann gilt:

$$E = K_1(x_2, \dots, x_{n+1}) = K(x_1)(x_2, \dots, x_{n+1}) = K(x_1, \dots, x_{n+1}),$$

denn $K_1 = K[x_1]$ ist nach dem Satz von Kronecker ein Körper. Somit ist $K \to K_1 \to E$ eine zusammengesetzte Körpererweiterung, in der P komplett in Linearfaktoren zerfällt und E ist ein Zerfällungskörper von P.

Zu (2): Sei E' ein weiterer Zerfällungskörper von P. Für $\deg P = 1$ folgt nach (a) und der Minimalitätseigenschaft des Zerfällungskörpers $E' = K = E$ und damit natürlich auch, dass E' und E isomorph sind. Die geforderten Eigenschaften werden dann durch $f: E \to E'$ mit $f = id$ erfüllt. Gelte nun, dass alle Zerfällungkörper für Polynome mit Grad n isomorph sind. Sei $\deg P = n + 1$. Da E' alle Nullstellen von P umfasst, hat auch der irreduzible Faktor Q eine Nullstelle x_1' in E'. Sei $K_1' = K(x_1') \subseteq E'$. Dann ist $j': K \to K_1'$ eine Körpererweiterung und Q hat in K_1' eine Nullstelle. Dann existiert nach dem Satz von Kronecker ein Körperhomomorphismus $f_1: K_1 \to K_1',\ x_1 \mapsto x_1'$ und $f_1 \circ j = j'$. f_1 ist ein Körperhomomorphismus und deshalb injektiv. f_1 ist außerdem surjektiv, denn alle Elemente aus K_1' sind Verknüpfungen von x_1' und Elementen aus K und haben somit ein Urbild. Durch die zusammengesetzte Körpererweiterung $K_1 \to K_1' \to E'$ ist E' ein Zerfällungskörper von P_1. Da $\deg P_1 = n$ ist, lässt sich die Induktionsvoraussetzung anwenden. E und E' sind demnach isomorph, das heißt f_1 lässt sich zu einem Isomorphismus $f: E \to E'$ fortsetzen, der die gewünschten Eigenschaften erfüllt.

IV. Der Algebraische Abschluss (Skizze)

Definition 4.1: Ein Körper K heißt algebraisch abgeschlossen, wenn jedes nicht konstante Polynom $P \in K[X]$ eine Nullstelle in K hat.

Bemerkung 4.2: Diese Definition ist äquivalent zu den Aussagen, dass

(1) jedes nicht konstante $P \in K[X]$ in K vollständig in Linearfaktoren zerfällt.

(2) K nur triviale algebraische Körpererweiterungen zulässt. Das heißt, dass für alle algebraischen Körpererweiterungen $j: K \to E$ gilt, dass j ein Isomorphismus ist.

Beweis: Zu (1): Wenn K algebraisch abgeschlossen ist, also jedes nicht konstante Polynom P eine Nullstelle $k_p \in K$ hat, dann existiert für jedes Polynom $P \in K[X]$ eine Darstellung $P = (X - k_p)Q$ für ein $Q \in K[X], \deg Q < \deg P$. Dieses Verfahren kann induktiv fortgesetzt werden, sodass P als das Produkt von Linearfaktoren mit Koeffizienten in K und einem konstanten Polynom dargestellt werden kann. Das bedeutet, dass jedes nicht konstante P in $K[X]$ vollständig in Linearfaktoren zerfällt. Zerfällt umgekehrt jedes nicht konstante Polynom $P \in K[X]$ in K vollständig in Linearfaktoren, so hat jedes nicht konstante Polynom in K bereits eine Nullstelle, sodass K algebraisch abgeschlossen ist.

Zu (2): Sei K ein algebraisch abgeschlossener Körper, $j: K \to E$ eine algebraische Körpererweiterung und x ein Element aus E mit dem dazugehörigen Minimalpolynom P. Wie bereits gezeigt zerfällt P in K vollständig in Linearfaktoren sobald K algebraisch abgeschlossen ist, das heißt $P = c\prod_{i=1}^{d}(X - x_i)$, wobei alle x_i Elemente aus K sind. Nach Voraussetzung gilt $P(x) = 0$, also ist $x = j(x_i)$ für ein $i \in \{1,..d\}$. Damit ist $j: K \to E$ surjektiv und da Körperhomomorphismen immer injektiv sind, ist $j: K \to E$ ein Isomorphismus. Sei nun K ein Körper, der nur triviale algebraische Körpererweiterungen zulässt und P ein nicht konstantes Polynom in $K[X]$ mit dem irreduziblen Faktor Q. Nach dem Satz von Kronecker existiert eine algebraische Körpererweiterung $f: K \to K_1$ mit $[K_1: K] = \deg Q$. Da aber alle algebraischen Körpererweiterungen über K trivial sind, gilt $\deg Q = 1$ für alle irreduziblen nicht konstanten Polynome in $K[X]$. Damit haben alle nicht konstanten Polynome aus $K[X]$ bereits in K eine Nullstelle. K ist daher algebraisch abgeschlossen.

Definition 4.3: Sei K ein Körper. Eine algebraische Körpererweiterung $j: K \to \Omega$ heißt algebraischer Abschluss von K, falls Ω algebraisch abgeschlossen ist.

Quelle:

Chambert-Loir, Antoine: A Field Guide to Algebra, Springer 2000
(insbesondere 2.1.3-2.3.3, Seite 33 ff.)