Vortrag 4

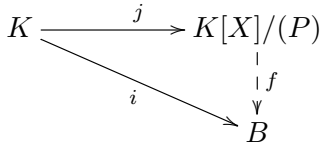
Einstieg in die Theorie der Körper

Mehmet Özüak

16.05.2013

1 Die universelle Abbildungseigenschaft von K[X]

Satz 1.1 (UAE von K[X]) *Sei K ein Körper, $P \in K[X]$ ein Polynom und $j : K \to K[X]/(P)$ der kanonische Ringhomomorphismus. Sei $i : K \to B$ Ringhomomorphismus und $y \in B$, sodass $P(y) = 0$. Dann existiert genau ein Ringhomomorphismus $f : K[X]/(P) \to B$, sodass $f \circ j = i$ und $f(x) = y$. In einem Diagramm dargestellt:*



Beweis: Ist $f(x) = y$, dann gilt $f(Q(x)) = Q(y)$ für alle $Q \in K[X]$, insbesondere für alle Q mit grad $Q <$ grad P. Also kann es höchstens einen Homomorphismus f geben mit $f \circ j = i$. Falls diese Abbildung existiert, gilt

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

Nun bleibt zu prüfen, ob f tatsächlich ein Ringhomomorphismus ist. Seien $Q, R \in K[X]$ Polynome mit grad Q, grad $R <$ grad P. Die Euklidische Division von QR durch P ist gegeben durch $QR = PS + Q * R$. Da $P(y) = 0$ in B ist, gilt

$$f(Q * R) = (Q * R)(y) = (Q * R)(y) + P(y)S(y) = (QR)(y) = Q(y)R(y) = f(Q)f(R),$$

also ist f ein Ringhomomorphismus. □

Definition 1.2 *Sind $i : E \to F$ und $j : E \to F'$ zwei Körpererweiterungen von E, dann ist $f : F' \to F$ ein Körperhomomorphismus von Erweiterungen von F' nach F, wenn gilt $f \circ j = i$.*

2 Der Satz von Kronecker

Satz 2.1 (Satz von Kronecker) *Sei K ein Körper und P ein irreduzibles Polynom mit Koeffizienten in K. Dann existiert eine endliche Körpererweiterung $K \to K_1$ und eine Nullstelle x von P in K_1, sodass gilt:*

(i) $K_1 = K[x]$.

(ii) *Ist $K \to L$ eine Körpererweiterung, M_1 die Menge von Homomorphismen von K_1 zu L und M_2 die Menge von Nullstellen von P in L, dann existiert eine Bijektion $\varphi : M_1 \to M_2$, $f \mapsto f(x)$.*

Beweis:

(i) Setze $K_1 = K[X]/(P)$ und $x := X$, $K \to K_1$ ist endlich beziehungsweise vom Grad grad P.

(ii) 1. Wohldefiniertheit: $P(f(x)) = f(P(x)) = f(0) = 0$.
2. Injektivität: Für $f, f' \in \mathrm{Hom}_K(K, L)$ mit $f(x) = f'(x)$ ist $f = f'$ zu zeigen. Sei $k_1 \in K_1$, dann existiert ein $Q \in K[X]$ mit $k_1 = Q(x)$. Dann gilt

$$f(k_1) = f(Q(x)) = Q(f(x)) = Q(f'(x)) = f'(k_1).$$

3. Surjektivität: Sei $y \in L$ mit $P(y) = 0$. Dann ist $f : K_1 = K[X]/(P) \to L$, $x \mapsto y$, also $P(x) \mapsto P(y) = 0$.

□

3 Zerfällungskörper

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

(i) *P zerfällt über E in Linearfaktoren, das heißt ist grad $P = n$ und ist c höchster Koeffizient, dann gibt es $x_1, \ldots, x_n$ in E, sodass $P = c \cdot \prod_{i=1}^{n}(X - x_i)$.*

(ii) *E wird als Körper von den x_i erzeugt, das heißt $E = K(x_1, \ldots, x_n)$.*

Satz 3.2 *Sei K ein Körper und $P \in K[X]$ ein nicht-konstantes Polynom. Es gilt:*

(i) *Es gibt einen Zerfällungskörper von P.*

(ii) *Jede solcher zwei Erweiterungen sind isomorph, das heißt sind $j : K \to E$ und $j' : K \to E'$ zwei Zerfällungskörper von P, dann existiert ein Körperisomorphismus $f : E \to E'$, sodass $f \circ j = j'$.*

Beweis: (i) und (ii) werden per Induktion nach grad P gezeigt. Ist grad $P = 1$, genügt es $E = K$ zu setzen. Sei $Q \in K[X]$ ein irreduzibler Faktor von P. Nach dem Satz von Kronecker existiert eine Erweiterung $K \to K_1$ und $x_1 \in K$, sodass $Q(x_1) = 0$ und $K_1 = K[x_1]$. Sein nun P_1 der Quotient aus P und $(X - x_1)$ im Ring $K_1[X]$, also $P_1 = P/(X - x_1) \in K_1[X]$. Nach Induktionsvoraussetzung hat P_1 einen Zerfällungskörper $K_1 \to E$. Die zusammengesetzte Erweiterung $K \to E$ ist eine Körpererweiterung, in der

P in Linearfaktoren zerfällt. Sei grad $P = d$ und $x_2, \ldots, x_d$ Nullstellen von P_1 in E, dann gilt

$$E = K_1(x_2, \ldots, x_d) = K[x_1](x_2, \ldots, x_d) = K(x_1, \ldots, x_d),$$

sodass E von den x_i über K erzeugt wird. Nun ist E nach Definition ein Zerfällungskörper von P über K und (i) ist gezeigt.

Sei nun $K \to E'$ ein weiterer Zerfällungskörper und definieren wir uns einen Isomorphismus $E \to E'$. Dann hat der irreduzible Faktor Q eine Nullstelle x_1' in E'. Nach dem Satz von Kronecker existiert ein Erweiterungshomomorphismus $f_1 : K_1 \to K_1'$, wobei $K_1 = K[x_1']$ ein Unterkörper von E' ist, erzeugt von x_1'. f_1 ist surjektiv und somit ein Isomorphismus, der P_1 auf $P_1' = P_1/(X - x_1)$ abbildet. Die Komposition $K_1 \to K_1' \to E'$ ist somit ein Zerfällungskörper vom Polynom $P/(X - x_1)$. Nach Induktionsvoraussetzung sind die beiden Erweiterungen $K_1 \to E$ und $K_1 \to E'$ isomorph und es gibt einen Isomorphismus $f : E \to E'$. □

4 Algebraischer Abschluss

Definition 4.1 *Man sagt, dass ein Körper K algebraisch abgeschlossen ist, falls jedes nicht-konstante Polynom in $K[X]$ eine Nullstelle in K besitzt.*

Bemerkung 4.2 *Diese Definition ist äquivalent zu:*

(i) *Jedes nicht-konstante Polynom $P \in K[X]$ zerfällt in Linearfaktoren.*

(ii) *Es existieren nur triviale algebraische Erweiterungen von K.*

Beweis:

(i) Beweis durch Induktion nach grad P:
IA: grad $P = 1 \Rightarrow P(X) = X - a$ mit $a \in K$. Somit ist a Nullstelle von P in K.
IV: Jedes Polynom $P \in K[X]$ (K algebraisch abgeschlossen) mit grad $P = n$ zerfällt in Linearfaktoren.
IS: Sei grad $P = n+1$. P besitzt eine Nullstelle a in K. Also existiert $Q \in K[X]$ mit grad $Q = n$, sodass $P(X) = (X - a) \cdot Q(X)$. Nach IV zerfällt Q in Linearfaktoren. Also zerfällt auch P in Linearfaktoren.

(ii) „⇒“:
Sei $x \in E$ Nullstelle von P und $P \in K[X]$ das Minimalpolynom von x. Dann existieren $x_1, \ldots, x_n$ ($n =$ grad P), sodass

$$P(X) = (X - a_1) \cdots (X - a_n), \quad a_i \in K \text{ mit } i = 1, \ldots, n$$

und somit

$$0 = P(x) = (x - a_1) \cdots (x - a_n).$$

Da Körper nullteilerfrei sind, ist einer der Faktoren $(x - a_i) = 0 \Leftrightarrow x = a_i \in K$ $\Rightarrow E = K$.

„$\Leftarrow$“:
Sei P ein irreduzibles Polynom mit grad $P > 0$ in K. Sei $L = K[X]/(P)$ algebraische Erweiterung von K. Nach Voraussetzung gilt $L = K$ und somit $1 = [L : K] = \text{grad}$ $P \Rightarrow P(X) = X - a$, $a \in K \Rightarrow P$ hat eine Nullstelle in K.

□

Definition 4.3 (Algebraischer Abschluss) *Ein algebraischer Abschluss einer Körpers K ist eine algebraische Erweiterung $j : K \to \Omega$, wobei Ω ein algebraisch abgeschlossener Körper ist.*

Literatur

[1] A. Chambert-Loir, *A Field Guide to Algebra*, Springer Verlag, 1. Auflage (Oktober 2004)

[2] F. Modler und M. Kreh, *Tutorium Algebra*, Springer Spektrum Verlag, 1. Auflage (Juli 2012)