Die Kronecker-Konstruktion mit LA-Mitteln

Florian Nisbach

Sei k ein Körper und $p \in k[X]$ ein irreduzibles, nicht konstantes Polynom vom Grad $n > 1$. Da p nicht linear ist, hat es also keine Nullstelle $a \in k$, denn sonst könnte man ja $X - a$ als Faktor abspalten. Ziel ist nun, einen größeren Körper $K \supset k$ zu konstruieren, in dem p (aufgefasst als Polynom in $K[X]$) eine Nullstelle hat.

Dazu nehmen wir uns eine Matrix $A \in k^{n\times n}$, die p als charakteristisches Polynom hat. Deren Existenz müssen wir natürlich erst mal nachweisen, aber das ist nicht schwer, denn wir können einfach die *Begleitmatrix* von A nehmen: Sei

$$p = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + X^n$$

(ohne Einschränkung normieren wir p). Dann definiere

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Wir rechnen durch Entwickeln nach der ersten Spalte nach, dass $p(T) = \det(T \cdot I_n - A) = \chi_A(T)$ gilt. Wegen der Irreduzibilität ist p sogar das Minimalpolynom von A.

Nun betrachten wir $k[A] \coloneqq \{\sum_{i=0}^{r} b_i A^i \mid b_i \in k, r \in \mathbb{N}\} \subset k^{n\times n}$. Diese Menge besteht also aus genau denjenigen Matrizen, die man erhält, wenn man A in Polynome aus $k[X]$ einsetzt. Jetzt stellen wir fest, dass die Menge $k[A]$ ein Teilring des Matrizenrings ist, denn sie ist ja unter Addition und Multiplikation abgeschlossen. $I_n \in k[A]$ ist ein Einselement, und der Ring ist sogar kommutativ: Verschiedene Potenzen von A kommutieren ja miteinander.

Sei nun $0 \neq B = \sum_{i=0}^{r} b_i A^i \in k[A]$. Dann gilt $B = q(A)$ mit $q = \sum_{i=0}^{r} b_i^i \in k[X]$. Aus $q(A) \neq 0$ folgt, dass p nicht q teilt, denn p ist ja das MP von A. Aus der Irreduzibilität von p folgt dann sogar $\mathrm{ggT}(p,q) = 1$. Also liefert der Euklidische Algorithmus Polynome $r, s \in k[X]$ mit $rp + sq = 1$. Einsetzen von A liefert

$$r(A) \cdot p(A) + s(A) \cdot q(A) = I_n,$$

wobei wegen $p(A) = 0$ folgt: $s(A) = (q(A))^{-1} = B^{-1}$. Also liegt das Inverse von B auch in $K \coloneqq k[A]$, und somit ist K ein Körper. Dieser enthält k via der Inklusion $\iota\colon k \to K$, $x \mapsto x \cdot I_n$.

Der Witz ist, dass p in K eine Nullstelle besitzt, nämlich A. Das sagt der Satz von Cayley-Hamilton! Insgesamt haben wir also gezeigt:

Proposition: Sei k ein Körper und $p \in k[X]$ ein nichtkonstantes irreduzibles Polynom. Dann gibt es eine Körpererweiterung $k \subset K$, sodass p in K eine Nullstelle besitzt.

Wir können also in $K[X]$ einen linearen Faktor von p abspalten und erhalten ein Polynom $\tilde{p} \in K[X]$ mit $p = (X - A) \cdot \tilde{p}$. Dessen irreduzible Faktoren haben also einen kleineren Grad als n, und durch sukzessives Anwenden der Proposition erhalten wir das folgende

Korollar: Sei k ein Körper und $p \in k[X]$ ein nichtkonstantes irreduzibles Polynom. Dann gibt es eine Körpererweiterung $\mathfrak{Z}(p)$, über der p in Linearfaktoren zerfällt.

Wenn man sich an das obige Verfahren hält, macht man nicht zu viel Arbeit: $k \subset \mathfrak{Z}(p)$ ist eine Erweiterung von minimalem Grad mit der Eigenschaft, dass p zerfällt. Die Eigenschaft »minimale Erweiterung, sodass p zerfällt«, charakterisiert $\mathfrak{Z}(p)$ bis auf Isomorphie eindeutig (das zeigen wir hier nicht!), er heißt *Zerfällungskörper* von p über k.