Wissenswertes zur Kronecker-Konstruktion

Sei K ein Körper und $f \in K[X]$ ein normiertes Polynom vom Grad mindestens 1. Aus diesen Daten können wir einen neuen Ring basteln, den Faktorring

$$K' := K[U]/(f(U)).$$

Wenn wir diese Konstruktion mit dem Ziel ausführen, eine künstliche Nullstelle von f zu bauen (siehe unten), so trägt sie den Namen *Kronecker-Konstruktion.*

Elemente von K'

Die Elemente von K' sind Äquivalenzklassen von Polynomen, wobei zwei Klassen genau dann als gleich angesehen werden, wenn die Differenz ihrer Repräsentanten ein Vielfaches von $f(U)$ ist. In K' rechnet man also *modulo* $f(U)$. Ist g ein Polynom, das bei Division durch $f(U)$ den Rest r lässt, so gilt $[g] = [r]$ in K'. Wir können daher festhalten:

$$K' = \{[r] \,|\, r \in K[U],\ \deg r < \deg f\}.$$

Das Nullelement von K' ist $[0]$, die Äquivalenzklasse des Nullpolynoms. Es gilt $[0] = [f(U)]$. Das Element $\alpha := [U] \in K'$ spielt eine besondere Rolle. Jedes Element von K' ist ein rationaler (und sogar polynomieller) Ausdruck in α, daher können wir auch schreiben:

$$K' = K[\alpha] = K(\alpha).$$

Einbettung von K in K'

Der Ring K' ist nicht im wörtlichen Sinn eine Obermenge von K, da K' ja neu konstruierte Äquivalenzklassen enthält. Vermöge des kanonischen injektiven Ringhomomorphismus

$$K \longrightarrow K',\ z \longmapsto [z]$$

können wir jedoch K als Unterring von K' *ansehen*: Immer, wenn wir in die Verlegenheit kommen, ein Element z von K als Element von K' interpretieren zu müssen (etwa wenn eine Formel nur dann Sinn ergibt, wenn an einer bestimmten Stelle ein Element von K' steht), so lesen wir einfach „$[z]$“ statt dem wörtlichen „z“.

Nutzen von K'

Im Vergleich zum Ausgangskörper K enthält der Ring K' das besondere neue Element $\alpha = [U]$. Dieses erfüllt die Rechenregel

$$f(\alpha) = 0 \in K',$$

denn wenn $f = \sum_{i=0}^{n} a_i X^i$, so gilt

$$f(\alpha) = \sum_{i=0}^{n} a_i [U]^i = \sum_{i=0}^{n} [a_i][U]^i = \Big[\sum_{i=0}^{n} a_i U^i\Big] = [f(U)] = 0.$$

Beim zweiten Gleichheitszeichen haben wir im Sinne des vorherigen Absatzes das Element a_i von K als Element $[a_i]$ von K' aufgefasst.

In K' gibt es also ein Element α, dass die Rechenregel $f(\alpha) = 0$ erfüllt. Das ist der Grund, wieso die Kronecker-Konstruktion wichtig ist: Mit ihrer Hilfe können wir nach Belieben neue Ringe bauen, in denen dann ein vorgegebenes Polynom f eine künstliche Nullstelle α besitzt. Die Kenntnis dieser künstlichen Nullstelle gibt aber keinerlei Information über den Zahlenwert richtiger Nullstellen von f (diese Frage könnte man sich etwa dann stellen, wenn $K = \mathbb{Q}$).

Invertierbarkeit in K'

Sei $[g] \in K'$ ein beliebiges Element. Um zu entscheiden, ob $[g]$ in K' Null, invertierbar oder ein Nullteiler ist, ist es hilfreich, den normierten größten gemeinsamen Teiler d von g und f zu betrachten. Es gibt dann nämlich drei Fälle:

- Fall $d = 1$:

  Dann ist $[g] \in K'$ invertierbar. Aus einer Bézoutdarstellung der Form $d = pg + qf$ können wir das Inverse sofort ablesen: Es ist $[p] \in K'$, denn

  $$1 = [d] = [p]\,[g] + [q]\,[f] = [p]\,[g].$$

- Fall $d = f$:

  Dann ist $[g] \in K'$ Null, da g ein Vielfaches von f ist.

- Fall $0 < \deg d < \deg f$:

  Dann ist $[g] \in K'$ ein Nullteiler, der selbst nicht Null ist. Denn da d gemeinsamer Teiler von f und g ist, gibt es Polynome u und v mit $f = ud$ und $g = vd$; daher gilt in K' die Rechnung

  $$[u]\,[g] = [uvd] = [v]\,[f] = [v] \cdot 0 = 0.$$

  Weder $[u]$ noch $[g]$ sind in K' Null, da u und g keine Vielfachen von f sind.

Der Ring K' als Oberkörper

Falls f irreduzibel ist, kann der dritte Fall des vorherigen Abschnitts nicht auftreten. Dann ist also jedes Element von K' entweder Null oder invertierbar, also ist K' in diesem Fall ein Körper.

Falls f reduzibel ist, etwa $f = gh$ mit $\deg g, \deg h \geq 1$, so ist K' kein Körper, da es Nullteiler gibt: Es gilt $[g]\,[h] = [f] = 0$, obwohl $[g] \neq 0$ und $[h] \neq 0$.

Wenn wir also das Problem

> *Konstruiere einen Oberkörper von K, in dem das Polynom f eine Nullstelle hat!*

lösen wollen, können wir *nicht* einfach $K' = K[U]/(f(U))$ betrachten, da dieser Ring vielleicht kein Körper ist. Falls wir aber f in irreduzible Faktoren zerlegen können, etwa $f = g_1 \cdots g_m$, so ist $K[U]/(g_1(U))$ ein Oberkörper von K mit der gewünschten Eigenschaft: In $K[U]/(g_1(U))$ ist das Element $[U]$ eine künstliche Nullstelle von g_1 und damit auch von f.

Das Problem ist nicht eindeutig lösbar, auch nicht bis auf Isomorphie: Die Körper $K[U]/(g_2(U))$, …, $K[X]/(g_m(U))$ enthalten auch jeweils eine künstliche Nullstelle von f, sind aber im Allgemeinen nicht isomorph zu $K[U]/(g_1(U))$.

Der Ring K' als ideeller Oberkörper

Wenn wir keine Zerlegung von f in irreduzible Faktoren bestimmen wollen (oder können), können wir trotzdem $K' = K[U]/(f(U))$ betrachten. Dieser Oberring von K ist zwar im Allgemeinen kein Körper (nur dann, wenn f irreduzibel ist), aber es wäre auch verkehrt, ihn als völlig nutzlosen Ring abzutun.

Addition, Subtraktion und Multiplikation in K' sind unproblematisch, diese Rechenoperationen benötigen nur, dass K' ein Ring ist, und das ist stets der Fall. Nur bei der Division müssen wir aufpassen: Ein Element $[g] \in K'$ kann ja Null, invertierbar oder ein Nullteiler sein. In den ersten beiden Fällen ist alles in Ordnung, diese beiden Fälle erwarten wir ja von einem Körper. Der dritte Fall darf bei einem Körper nicht auftreten. Aber nicht alle Hoffnung ist verloren:

Tritt der dritte Fall ein, so haben wir in $d := \mathrm{ggT}(g, f)$ einen nichttrivialen Faktor von f gefunden. Dann können wir die gesamte Rechnung mit $K[U]/(d(U))$ statt $K[U]/(f(U))$ neustarten (also von Beginn an neu aufrollen). Wenn wir in unserer Rechnung wieder zur Frage kommen, ob $[g]$ invertierbar ist, wird dann die Antwort sein: Nein, $[g]$ ist Null (da g ein Vielfaches von d ist). Beim zweiten Durchgang wird der problematische dritte Fall an dieser Stelle also nicht auftreten.

Sollte an einer späteren Stelle der Rechnung wieder der dritte Fall auftreten, erhalten wir abermals einen nichttrivialen Faktor und können die Rechnung abermals neustarten.

Fazit. Obwohl der Ring $K' = K[U]/(f(U))$ nur dann ein Körper ist, wenn f irreduzibel ist, können wir mit ein wenig Umsicht auch sonst in K' so rechnen, *als ob* er ein Körper wäre: Weil wir wissen, durch welchen besseren Ring wir ihn zu ersetzen haben, wenn wir bei einer Rechnung auf den problematischen dritten Fall stoßen. In diesem Sinn ist K' ein *ideeller Oberkörper* von K. Bei jedem Neustart finden wir einen nichttrivialen Faktor von f.

Beispiel

Sei $K = \mathbb{Q}$ und $f = X^2 - 5\,X + 6$. Eine Nebenrechnung würde zeigen, dass dieses Polynom reduzibel ist, aber auf diese Nebenrechnung haben wir keine Lust; wir versuchen trotzdem, im Ring $K[U]/(f(U))$ zu rechnen.

Etwa können wir uns die Frage stellen, ob $\alpha - 1$ invertierbar ist. Dazu müssen wir den normierten größten gemeinsamen Teiler von $g := U - 1$ und $f(U)$ bestimmen: Dieser ist $d = 1$, und eine Bézoutdarstellung ist durch

$$d = 1 = -\tfrac{1}{2}(U^2 - 5\,U + 4) \cdot g + \tfrac{1}{2} \cdot f(U)$$

gegeben. Also ist $[-\frac{1}{2}(U^2 - 5\,U + 4)] = -\frac{1}{2}(\alpha^2 - 5\alpha + 4)$ ein Inverses von $\alpha - 1$.

Auch können wir uns die Frage stellen, ob $\alpha - 2$ invertierbar ist. Der normierte größte gemeinsame Teiler von $\tilde{g} := U - 2$ und $f(U)$ ist $\tilde{d} = U - 2$. Also tritt der dritte Fall ein: Wir haben den nichttrivialen Faktor $X - 2$ von $f(X)$ gefunden und Rollen unsere Rechnung neu auf, mit $K[U]/(\tilde{d}(U))$ statt $K[U]/(f(U))$.

Nun können wir die Frage nach der Invertierbarkeit von $\alpha - 2$ erneut stellen; jetzt ist der normierte größte gemeinsame Teiler von $U - 2$ und $\tilde{d}$ zu berechnen. Dieser ist $\tilde{d}$ und daher ist $\alpha - 2$ im verbesserten Ring $K[U]/(\tilde{d}(U))$ Null.

Konzept des Zerfällungskörpers

Ein Zerfällungskörper eines Polynoms über einem Körper K ist ein Oberkörper von K, in dem das Polynom vollständig in Linearfaktoren $(X - x_1) \cdots (X - x_n)$ zerfällt und in dem jedes Element ein polynomieller Ausdruck in den Nullstellen x_i ist.

Ein Zerfällungskörper eines Polynoms ist also minimal unter allen Oberkörpern von K, in denen das Polynom in Linearfaktoren zerfällt.

Beispiel. Der Körper $\mathbb{Q}$ ist kein Zerfällungskörper für das Polynom $X^2 + 1 \in \mathbb{Q}[X]$, da dieses über $\mathbb{Q}$ noch nicht in Linearfaktoren zerfällt. Der Rechenbereich $\mathbb{C}$ ist auch kein Zerfällungskörper, da sich nicht jedes Element von $\mathbb{C}$ als polynomiellen Ausdruck mit rationalen Koeffizienten in den beiden Nullstellen $\pm\mathrm{i}$ schreiben lässt; $\mathbb{C}$ ist viel zu groß. Ein Zerfällungskörper ist $\mathbb{Q}[\mathrm{i}]$.

Konstruktion von Zerfällungskörpern

Manchmal zerfällt in $K' = K[U]/(f(U))$ das Polynom f schon in Linearfaktoren: Zwar haben wir nur *eine* Nullstelle künstlich hinzugefügt, es kann aber sein, dass sich die weiteren Nullstellen von f über diese eine ausdrücken lassen. In diesem Fall ist K' ein (vielleicht nur ideeller) Zerfällungskörper für f.

Beispiel. Im Ring $K[U]/(f(U))$ aus dem vorherigen Zahlenbeispiel besitzt f neben der künstlichen Nullstelle $\alpha = [U]$ noch die Nullstelle $5 - \alpha$, denn es gilt

$$\begin{aligned}(X - \alpha) \cdot (X - (5 - \alpha)) &= X^2 - (\alpha + 5 - \alpha)\, X + \alpha \cdot (5 - \alpha) \\ &= X^2 - 5\, X + (5\alpha - \alpha^2) \\ &= X^2 - 5\, X + 6 = f.\end{aligned}$$

Es kommt aber auch vor, dass f über K' noch nicht in Linearfaktoren zerfällt. Wenn wir dann einen nichttrivialen Faktor $h \in K'[X]$ von f finden (zum Beispiel das Ergebnis der Polynomdivision von f durch $X - \alpha$), können wir die Kronecker-Konstruktion einfach wiederholen und $K'[V]/(h(V))$ betrachten. In diesem Ring wird h eine künstliche Nullstelle $\beta := [V]$ besitzen und daher reduzibel sein, sodass wir einer Zerlegung von f in Linearfaktoren ein Stück näher gekommen sind.

Bemerkung zu Blatt 11, Aufgabe 5

Bei Aufgabe 5 von Blatt 11 ist zu zeigen, dass ein *tatsächlicher* Zerfällungskörper existiert, nicht nur ein ideeller. Dazu kann man die Kronecker-Konstruktion verwenden, muss aber darauf aufpassen, nur modulo irreduzibler Polynome zu rechnen. Damit das gelingt, ist die Voraussetzung, dass der Grundkörper K endlich ist, wesentlich.