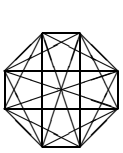
TU CLAUSTHAL
INSTITUT FÜR MATHEMATIK
Prof. Dr. W. Klotz



Lineare Algebra II
SS 2000
Übungsblatt 6

Faktorisierung von Polynomen

Analog zur Primteilerzerlegung von ganzen Zahlen will man oft Polynome in irreduzible Polynome zerlegen. Während bei den Zahlen aber offensichtlich nur endlich viele mögliche Zahlen als Faktoren in Frage kommen, ist dies bei Polynomen nicht offensichtlich. In dieser Übung werden wir Methoden kennenlernen, Polynome zu faktorisieren, bzw. zu erkennen, dass sie unzerlegbar sind.

1. Ein Polynom, das über $\mathbb{Z}$ irreduzibel ist, kann natürlich über $\mathbb{C}$ reduzibel sein, z.B. $f(x) = x^2 + 1$. Analog ist $x^2 - 2$ über $\mathbb{Q}$ irreduzibel, aber über $\mathbb{Q}(\sqrt{2})$ oder über $\mathbb{R}$ reduzibel.

2. Der Fundamentalsatz der Algebra besagt, dass jedes Polynome $f \in \mathbb{C}[x]$ über $\mathbb{C}$ in lineare Faktoren zerfällt, bzw. dass das Polynom n komplexe Nullstellen hat, wobei $\deg f = n$ ist. Über $\mathbb{R}$ zerfallen Polynome in lineare oder quadratische Faktoren. Da ein Beweis dieser Tatsachen naturgemäß Eigenschaften der reellen Zahlen ausnützt (z.B. Zwischenwertsatz), wird der Beweis meist im Rahmen der Analysisvorlesungen gegeben. Es sind auch zahlreiche elegante Beweise bekannt, die Kenntnisse über Funktionentheorie voraussetzen.

3. Besonders wichtig ist die Faktorisierung über $\mathbb{Q}$.
   Satz (Gaußsches Lemma):
   Ist ein Polynom f mit ganzzahligen Koeffizienten über $\mathbb{Z}$ irreduzibel, so ist es auch über $\mathbb{Q}$ irreduzibel. Andersherum induziert eine Faktorisierung über $\mathbb{Q}$ auch eine solche über $\mathbb{Z}$.

   Es reicht daher, nach Faktoren mit ganzzahligen Koeffizienten zu suchen.

4. **Satz (Eisensteinsches Irreduzibilitätskriterium):**
   Sei $f \in \mathbb{Z}[x]$ ein Polynom mit $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Weiter sei p eine Primzahl. Wenn die folgenden Bedingungen erfüllt sind

   $$\begin{aligned} &i) && a_n \not\equiv 0 \bmod p \\ &ii) && a_i \equiv 0 \bmod p \text{ für } i = 0, \cdots, n-1 \\ &iii) && a_0 \not\equiv 0 \bmod p^2, \end{aligned}$$

   dann ist f irreduzibel über $\mathbb{Q}$. Dies ist ein hinreichendes, aber kein notwendiges Kriterium.

5. Beispiele: Warum sind folgende Polynome über $\mathbb{Q}$ irreduzibel?
   $f(x) = x^5 + 3x^2 + 3$,
   $f(x) = x^2 + x + 1$,
   $f(x) = x^5 + 3x^2 + 1$.

6. Wir wollen einen Algorithmus skizzieren, mit dem man Polynome faktorisieren kann. Er zeigt, dass doch nur endlich viele Faktoren in Frage kommen. Der Algorithmus wurde bereits von Kronecker (1823-1891) beschrieben.

a) Zunächst eine Bemerkung über Polynominterpolation. Wenn man die Werte eines Polynoms an $n+1$ Stellen (x_i, y_i) vorgibt, so gibt es genau ein Polynom f vom Grad kleiner oder gleich n, das diese Werte annimmt. Man kann dies Polynom sogar explizit angeben (Lagrange-Polynom, Lagrange (1736-1813)):

$$f(x) = \sum_{i=0}^{n} y_i \frac{(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}.$$

b) Wenn das Polynom g ein Teiler vom Polynom f ist, also $f = gh$ gilt, so gilt auch an jeder einzelnen Stelle $g(x_i) \mid f(x_i)$.

Wenn f überhaupt einen Teiler hat, dann auch einen mit Grad kleiner oder gleich $\frac{n}{2}$. Wenn man nun an $r = [\frac{n}{2}] + 1$ vielen Stellen $x_0, \cdots, x_r$ die Funktionswerte von f auswertet, so erhält man alle (endlich vielen) in Frage kommenden Werte von $g(x_i)$ als Teiler von $f(x_i)$. Da zu jeder Wahl $(g(x_0), \cdots, g(x_r))$ genau ein Interpolationspolynom gehört, kann man auf diese Weise alle (endlich vielen) in Frage kommenden Faktoren g von f aufzählen und testen.

c) Beispiel: Sei $f(x) = x^4 + x + 1$. f hat keinen linearen Faktor, da f keine ganzzahlige Nullstelle hat. Sei $f = gh$ und deg $g = 2$. die Stellen $x_0 = -1, x_1 = 0, x_1 = 1$ erscheinen besonders geeignet, da hier $f(x_i)$ aus wenigen Faktoren besteht. $f(-1) = 1, f(0) = 1, f(1) = 3$. Daher ist $g(-1) = \pm 1, g(0) = \pm 1, g(1) = \pm 1, \pm 3$. Es kommen also nur 16 verschiedene Polynome g als Teiler von f in Frage.

In einer solchen Situation reicht oft auch ein Ansatz mit unbestimmten Koeffizienten:

$$f(x) = x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

7. Eine andere Eigenschaft von Faktoren:
Die Koeffizienten von einem Faktor g können mittels der Koeffizienten von f beschränkt werden: Das Polynom f habe den Grad n, das Polynom g den Grad m. Sei $H(f)$ der betragsmäßig größte Koeffizient von f, und $H(g)$ der von g. Dann gilt $H(g) \leq 2^m \sqrt{n+1} H(f)$.

8. In der Praxis wird man ein Polynom nicht über $\mathbb{Z}$, sondern über geeigneten endlichen Körpern $\mathbb{Z}_p$ faktorisieren. Wenn das Polynom sich über einem $\mathbb{Z}_p$ als irreduzibel erweist, ist es auch über $\mathbb{Z}$ irreduzibel. Andererseits kann das Wissen über die Faktoren in $\mathbb{Z}_p$ modulo mehrerer Primzahlen zusammengesetzt werden.