Kapitel 5
Polynome in mehreren Veränderlichen

Die wenigsten Probleme lassen sich durch nur eine Größe beschreiben; bei der Lösung algebraischer Gleichungen geht es daher in den meisten Anwendungen um Gleichungen in mehrerern Veränderlichen. Wir wissen bereits aus Kapitel 2, §7, daß auch der Polynomring in mehreren Veränderlichen über $\mathbb{Z}$ oder über einem Körper faktoriell ist, so daß wir auch hier von größten gemeinsamen Teilern und von der Zerlegung in irreduzible Faktoren reden können. In diesem Kapitel wollen wir sehen, daß sich beides auch effektiv berechnen läßt.

§ 1: Berechnung des größten gemeinsamen Teilers

Der Polynomring in mehr als einer Variablen über einem Körper ist nicht mehr EUKLIDisch, so daß uns zur Berechnung des größten gemeinsamen Teilers kein EUKLIDischer Algorithmus zur Verfügung steht. Das ist allerdings keine neue Situation für uns, denn über $\mathbb{Z}$ ist ja schon der Polynomring in einer Veränderlichen nicht EUKLIDsch.

Unsere Strategie zur Berechnung des ggT zweier Polynome aus $\mathbb{Z}[x]$ bestand darin, daß wir jedes Polynom zerlegten in seinen Inhalt und den primitiven Anteil. Die Inhalte sind ganze Zahlen, deren ggT wir mit dem klassischen EUKLIDischen Algorithmus berechnen können. Die primitiven Anteile betrachten wir modulo einer oder mehrerer Primzahlen; für die entstehenden Polynome aus $\mathbb{F}_p[x]$ haben wir wieder einen effizienten EUKLIDischen Algorithmus. Deren Ergebnisse können wir mit dem chinesischen Restesatz zu einem Polynom mit ganzen Koeffizienten zusammenfassen; falls das Produkt der betrachteten Primzahlen

hinreichend groß ist und wir keine „schlechten“ Primzahlen genommen haben, ist das der ggT der primitiven Anteile,

Mit einer ähnlichen Strategie können wir auch die ggT-Berechnung zweier Polynome f, g in $n > 1$ Variablen über einem der Ringe $k = \mathbb{Z}$, $k = \mathbb{F}_p$ oder $k = \mathbb{Q}$ (und weiteren Ringen) zurückführen auf ggT-Berechnungen für Polynome in $n-1$ Variablen über k. Dazu zeichnen wir im Polynomring $R_n = k[x_1, \ldots, x_n]$ eine der Variablen, etwa x_n, aus und betrachten alle Polynome als Polynome in der einen Veränderlichen x_n mit Koeffizienten aus dem Polynomring $R_{n-1} = k[x_1, \ldots, x_{n-1}]$ in $n-1$ Variablen; wir schreiben also $R_n = R_{n-1}[x_n]$. Durch ggT-Berechnungen in R_{n-1} können wir diese Polynome zerlegen in ihre Inhalte und primitiven Anteile; der ggT der Inhalte läßt sich wieder in R_{n-1} berechnen.

Bleibt noch der ggT der primitiven Anteile; diese seien f und g, jeweils aufgefaßt als Polynome in x_n mit Koeffizienten aus R_{n-1}. Um deren ggT zu berechnen, könnten wir den EUKLIDischen Algorithmus über dem Quotientenkörper von R_{n-1} anwenden, allerdings steigen hier die Grade von Zähler und Nenner der Koeffizienten sowie *deren* Koeffizienten im allgemeinen so stark an, daß dies nur bei wenigen Variablen und sehr kleinen Graden praktisch durchführbar ist. Daher müssen wir auch hier wieder nach Alternativen suchen.

In Kapitel II hatten wir, um die Explosion der Koeffizienten beim EUKLIDischen Algorithmus in $\mathbb{Q}[x]$ zu vermeiden, den Umweg über die ganzen Zahlen modulo einer Primzahl p genommen, also zunächst einen ggT in $\mathbb{F}_p[x]$ berechnet. Formal können wir das auch so ausdrücken, daß wir auf die Koeffizienten die Abbildung

$$\varphi_p\colon \begin{cases} \mathbb{Z} \to \mathbb{F}_p \\ a \mapsto a \bmod p \end{cases}$$

angewendet haben. Entsprechend können wir im Polynomring R_{n-1} noch einmal eine Variable auszeichnen, etwa x_{n-1}, und für diese einen festen Wert $c \in k$ einsetzen, d.h. wir wenden auf alle Koeffizienten die

Abbildung

$$\varphi_c: \begin{cases} R_{n-1} \to R_{n-2} \\ a(x_1, \ldots, x_{n-2}, x_{n-1}) \mapsto a(x_1, \ldots, x_{n-2}, c) \end{cases}$$

an. Die entstehenden Polynome $\overline{f}$ und $\overline{g}$ aus $R_{n-2}[x]$ haben wieder insgesamt $n-1$ Variable, wir können ihren ggT also mit dem Algorithmus für Polynome in $n-1$ Variablen berechnen.

Auch hier stellt sich die Frage, was der ggT von $\overline{f}$ und $\overline{g}$ mit dem von f und g zu tun hat. Im folgenden bezeichne $\overline{h}$ für jedes Polynom $h \in R_{n-1}[x_n]$ das Polynom aus $R_{n-2}[x]$, das durch Anwendung von φ_c auf die Koeffizienten von h entsteht.

Ist $h \in R_{n-1}[x]$ ein Teiler von f, etwa $f = qh$, so ist $\overline{f} = \overline{q}\overline{h}$, d.h. auch $\overline{h}$ ist ein Teiler von $\overline{f}$. Dieser Teiler könnte aber einen kleineren Grad haben als h; dies passiert offensichtlich genau dann, wenn der führende Koeffizient von h im Kern von φ_c liegt, durch Einsetzen von $x_{n-1} = c$ also zur Null wird. Da der führende Koeffizient von f das Produkt der führenden Koeffizienten von $\overline{h}$ und $\overline{q}$ ist, gilt dann dasselbe auch für den führenden Koeffizienten von f; wir können dieses Problem also vermeiden, indem wir c so wählen, daß der führende Koeffizient von f durch φ_c nicht auf die Null abgebildet wird. Wenn wir das für f *oder* g sicherstellen, wissen wir daher, daß $\overline{\mathrm{ggT}(f,g)}$ ein Teiler von $\overline{f}$ und $\overline{g}$, also auch von $\mathrm{ggT}(\overline{f},\overline{g})$ ist, und daß beide größte gemeinsame Teiler denselben Grad in x_n haben. Da die führenden Koeffizienten von f und g als Polynome in x_{n-1} geschrieben werden können, gibt es nur endlich viele Werte von c, die wir vermeiden müssen, und diese lassen sich einfach identifizieren.

Auch dann wissen wir allerdings nur, daß $\overline{h} = \overline{\mathrm{ggT}(f,g)}$ ein Teiler von $\mathrm{ggT}(\overline{f},\overline{g})$ ist. $\overline{h}$ ist genau dann ein echter Teiler, wenn $\overline{f}/\overline{h}$ und $\overline{g}/\overline{h}$ einen gemeinsamen Faktor haben, der keine Einheit ist, wenn also die Resultante von $\overline{f}/\overline{h}$ und $\overline{g}/\overline{h}$ bezüglich x_n verschwindet. Bezeichnet h den ggT von f und g, so entsteht diese Resultante aus $\mathrm{Res}_{x_n}(f/h, g/h) \in R_{n-1}$ durch Anwendung von φ_c; da diese Resultante als Polynom in x_{n-1} geschrieben werden kann, gibt es also wieder höchstens endlich viele Werte von c, für die dies der Fall ist. Da wir h nicht kennen, können wir diese Werte allerdings nicht im voraus identifizieren – ganz analog zur Situation bei der modularen Berechnung des ggT in $\mathbb{Z}[x]$.

Als nächstes stellt sich das Problem, was wir aus der Kenntnis von $\mathrm{ggT}(\overline{f},\overline{g})$ für $\mathrm{ggT}(f,g)$ folgern können. Offensichtlich nicht sonderlich viel, denn wenn wir ein Polynom nur an einer Stelle $x_{n-1} = c$ kennen, gibt uns das noch kaum Information. Wenn wir allerdings ein Polynom vom Grad d in x_{n-1} an $d+1$ verschiedenen Punkten kennen, dann kennen wir es vollständig.

Die einfachste Konstruktion des Polynoms aus seinen Funktionswerten an $d+1$ verschiedenen Stellen geht auf JOSEPH-LOUIS COMTE DE LAGRANGE zurück und benutzt dieselbe Strategie, die wir vom chinesischen Restesatz her kennen: Ist R ein Integritätsbereich und suchen wir ein Polynom $h \in R[x]$ vom Grad d, das an den Stellen $c_i \in R$ für $i = 0, \ldots, d$ die Werte $h_i \in R$ annimmt, so konstruieren wir zunächst Polynome α_i mit $\alpha_i(c_i) = 1$ und $\alpha_i(c_j) = 0$ für $j \neq i$. Das Verschwinden an den Stellen c_j können wir erreichen, indem wir die Linearfaktoren $(x - c_j)$ für $j \neq i$ miteinander multiplizieren. Um an der Stelle c_i den Wert eins zu erhalten, müssen wir allerdings noch durch das Produkt der $(c_i - c_j)$ dividieren, und damit kommen wir eventuell aus R hinaus und müssen im Quotientenkörper rechnen. Mit den so definierten Polynomen

$$\alpha_i(x) = \frac{\prod_{j \neq i}(x - c_j)}{\prod_{j \neq i}(c_i - c_j)}$$

ist das Interpolationspolynom dann

$$f(x) = \sum_{i=1}^{d} \alpha_i(x) h_i \,.$$

(Das Interpolationsverfahren von LAGRANGE ist zwar einfach zu verstehen und führt auf eine elegante Formel, es gibt jedoch effizientere Verfahren, die auch hier anwendbar sind, z.B. das von ISAAC NEWTON. Für Einzelheiten sei auf die Numerik-Vorlesung verwiesen.)

Die Nenner in der LAGRANGEschen (oder auch NEWTONschen) Interpolationsformel stören uns nicht besonders, da wir ja spezialisieren, indem

wir für x_{n-1} jeweils Konstanten einsetzen, die c_i liegen also alle im Ring k der Konstanten. Falls es sich dabei um einen Körper handelt, haben wir überhaupt keine Probleme mit den Divisionen; im wohl wichtigsten Fall, daß wir über den ganzen Zahlen arbeiten, erhalten wir zwar Interpolationspolynome mit rationalen Koeffizienten, können diese aber zerlegen in einen konstanten Faktor mal einem ganzzahligen Polynom mit teilerfremden Koeffizienten, das für die Berechnung des ggT zweier primitiver ganzzahliger Polynome an Stelle des Interpolationspolynoms verwendet werden kann.

JOSEPH-LOUIS LAGRANGE (1736–1813) wurde als GIUSEPPE LODOVICO LAGRANGIA in Turin geboren und studierte dort zunächst Latein. Erst eine alte Arbeit von HALLEY über algebraische Methoden in der Optik weckte sein Interesse an der Mathematik, woraus ein ausgedehnter Briefwechsel mit EULER entstand. In einem Brief vom 12. August 1755 berichtete er diesem unter anderem über seine Methode zur Berechnung von Maxima und Minima; 1756 wurde er, auf EULERs Vorschlag, Mitglied der Berliner Akademie; zehn Jahre später zog er nach Berlin und wurde dort EULERs Nachfolger als mathematischer Direktor der dortigen Akademie 1787 wechselte er an die Pariser Académie des Sciences, wo er bis zu seinem Tod blieb und unter anderem an der Einführung des metrischen Systems beteiligt war. Seine Arbeiten umspannen weite Teile der Analysis, Algebra und Geometrie.

Damit ergibt sich folgender Algorithmus zur Zurückführung des ggT zweier Polynome in n Veränderlichen auf die Berechnung von ggTs von Polynomen in $n-1$ Veränderlichen:

Wir gehen aus von zwei Polynomen $F, G \in R_n = k[x_1, \ldots, x_n]$, mit $k = \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{F}_p$ (oder sonst einem faktoriellen Ring, über dem wir den ggT zweier Polynome in einer Veränderlichen berechnen können).

1. Schritt (Initialisierung): Schreibe

$$F = \sum_{i=0}^{d} a_i(x_1, \ldots, x_{n-1}) x_n^i \quad \text{und} \quad G = \sum_{j=0}^{e} b_j(x_1, \ldots, x_{n-1}) x_n^j ,$$

wobei die führenden Koeffizienten a_d und b_e nicht identisch verschwinden sollen. Weiter sei $\mathcal{C} = \emptyset$ die Menge aller bislang betrachteten Spezialisieruungen und $\mathcal{M} = \emptyset$ die Teilmenge der nach unserem jeweiligen Erkenntnisstand „guten“ Spezialisierungen.

Als nächstes werden die Inhalte $I(F)$ und $I(G)$ von F und G bezüglich obiger Darstellung berechnet, d.h. $I(F)$ ist der ggT der $a_i(x_1, \ldots, x_{n-1})$ und $I(G)$ der von $b_0(x_1, \ldots, x_{n-1})$ bis $b_e(x_1, \ldots, x_{n-1})$. Beides kann bestimmt werden durch eine Folge von ggT-Berechnungen in $n-1$ Veränderlichen, ebenso auch der ggT I_0 dieser beiden Inhalte. Weiter seien $f = F/I(F)$ und $g = G/I(G)$ die primitiven Anteile von F und G. Der ggT von F und G ist I_0 mal dem in den folgenden Schritten berechneten ggT von f und g.

2. Schritt: Wähle so lange ein neues zufälliges Element $c \in k \setminus \mathcal{C}$ und ersetze $\mathcal{C}$ durch $\mathcal{C} \cup \{c\}$, bis $a_d(x_1, \ldots, x_{n-2}, c)$ und $b_e(x_1, \ldots, x_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. (Meist wird dies bereits beim ersten Versuch der Fall sein.) Berechne dann den ggT h_c von

$$\overline{f} = \sum_{i=0}^{d} a_i(x_1, \ldots, x_{n-2}, c) x_n^i \quad \text{und} \quad \overline{g} = \sum_{j=0}^{e} b_j(x_1, \ldots, x_{n-2}, c) x_n^j .$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis $\mathrm{ggT}(f, g) = 1$. Andernfalls wird $\mathcal{M} = \{c\}$ und $N = \deg_{x_n} h_c$ und m wird eins mehr als das Maximum der Grade der a_i und der b_j in der Variablen x_{n-1}.

3. Schritt: Falls die Elementanzahl $\#\mathcal{M}$ von $\mathcal{M}$ gleich m ist, wird das Interpolationspolynom $h \in k[x_1, \ldots, x_n]$ berechnet, das für jedes $c \in \mathcal{M}$ die Gleichung

$$h(x_1, \ldots, x_{n-1}, c, x_n) = h_c(x_1, \ldots, x_{n-2}, x_n)$$

erfüllt. *Falls* h sowohl f als auch g teilt, ist $h = \mathrm{ggT}(f, g)$ und der Algorithmus endet mit diesem Ergebnis. Andernfalls waren alle bisherigen Spezialisierungen schlecht, und wir müssen von Neuem mit Schritt 2 beginnen.

4. Schritt: Falls $\#\mathcal{M} < m$, wählen wir ein zufälliges $c \in k \setminus \mathcal{C}$ solange, bis $a_d(x_1, \ldots, x_{n-2}, c)$ und $b_e(x_1, \ldots, x_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. Wir berechnen wieder den ggT h_c von

$$\overline{f} = \sum_{i=0}^{d} a_i(x_1, \ldots, x_{n-2}, c) x_n^i \quad \text{und} \quad \overline{g} = \sum_{j=0}^{e} b_j(x_1, \ldots, x_{n-2}, c) x_n^j .$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis ggT$(f, g) = 1$.

Falls $\deg_{x_n} h_c > N$ ist, haben wir ein schlechtes c gewählt und gehen zurück zum Anfang des vierten Schritts.

Falls $\deg_{x_n} h_c < N$ ist, waren alle zuvor betrachteten Werte von c schlecht; wir setzen $\mathcal{M} = \{c\}$ und $N = \deg_{x_n} h_c$.

Falls schließlich $\deg_{x_n} h_c = N$ ist, ersetzen wir $\mathcal{M}$ durch $\mathcal{M} \cup \{c\}$, und es geht weiter mit Schritt 3.

Da es nur endlich viele schlechte Werte für c gibt, muß der Algorithmus nach endlich vielen Schritten enden.

Als Beispiel wollen wir den ggT der beiden Polynome

$$f = x^3 + x^2y + x^2z + xyz + y^2z + yz^2$$

und

$$g = x^3 + x^2y + x^2z + xy^2 + xz^2 + y^3 + y^2z + yz^2 + z^3$$

aus $\mathbb{Z}[x, y, z]$ berechnen. Wir fassen Sie zunächst auf als Polynome in z mit Koeffizienten aus $\mathbb{Z}[x, y]$:

$$f = yz^2 + (x^2 + xy + y^2)z + x^3 + x^2y$$

und

$$g = z^3 + (x + y)z^2 + (x^2 + y^2)z + x^3 + x^2y + xy^2 + y^3$$

Der führende Koeffizient von f ist y, der von g ist eins. Wie man leicht sieht, sind beide Polynome bereits primitiv.

Der höchste y-Grad eines Koeffizienten ist drei; wir brauchen daher vier zufällig gewählte Spezialisierungen. Der Einfachheit und vor allem der Übersichtlichkeit halber seien hierfür die (nicht gerade „zufälligen“ Werte $c = 1, 2, 3$ und 4 gewählt.

Für $c = 1$ ist

$$f(x, 1, z) = z^2 + (x^2 + x + 1)z + x^3 + x^2$$

und

$$g(x, 1, z) = z^3 + (x + 1)z^2 + (x^2 + 1)z + x^3 + x^2 + x + 1\,;$$

wir müssen den ggT dieser beiden Polynome berechnen.

Dies leistet der entsprechende Algorithmus für Polynome in zwei Veränderlichen; da die Polynome wieder primitiv sind und der höchste x-Grad eines Koeffizienten gleich drei ist, müssen wir vier Spezialisierungen für x betrachten. Auch diese seien zufällgerweise gerade $1, 2, 3$ und 4. Wir erhalten folgende Ergebnisse:

d	$f(d, 1, z)$	$g(d, 1, z)$	ggT
1	$z^2 + 3z + 2$	$z^3 + 2z^2 + 2z + 4$	$z + 2$
2	$z^2 + 7z + 12$	$z^3 + 3z^2 + 5z + 15$	$z + 3$
3	$z^2 + 13z + 36$	$z^3 + 4z^2 + 10z + 40$	$z + 4$
4	$z^2 + 21z + 80$	$z^3 + 5z^2 + 17z + 85$	$z + 5$

Auch ohne Interpolationsformel sehen wir, daß

$$h_1(x, z) = x + 1 + z$$

das Interpolationspolynom ist. Division zeigt, daß

$$\frac{f(x, 1, z)}{h_1(x, z)} = x^2 + z \quad \text{und} \quad \frac{g(x, 1, z)}{h_1(x, z)} = x^2 + z^2 + 1$$

beides Polynome sind; somit ist

$$\text{ggT}\big(f(x, 1, z), g(x, 1, z)\big) = x + 1 + z\,.$$

Als nächstes setzen wir $c = 2$ für y ein; wir erhalten

$$f(x, 2, z) = 2z^2 + (x^2 + 2x + 4)z + x^3 + 2x^2$$

und

$$g(x, 2, z) = z^3 + (x + 2)z^2 + (x^2 + 4)z + x^3 + 2x^2 + 4x + 8$$

und spezialisieren darin wieder x zu $1, 2, 3, 4$:

d	$f(d, 2, z)$	$g(d, 2, z)$	ggT
1	$2z^2 + 7z + 3$	$z^3 + 3z^2 + 5z + 15$	$z + 3$
2	$2z^2 + 12z + 16$	$z^3 + 4z^2 + 8z + 32$	$z + 4$
3	$2z^2 + 19z + 45$	$z^3 + 5z^2 + 13z + 65$	$z + 5$
4	$2z^2 + 28z + 96$	$z^3 + 6z^2 + 20z + 120$	$z + 6$

Hier ist unser ggT-Kandidat somit $h_2(x,z) = x+2+z$, und wieder zeigt Division, daß dies tatsächlich ein Teiler beider Polynome und somit deren ggT ist.

Für $c = 3$ ist

$$f(x,3,z) = 3z^2 + (x^2+3x+9)z + x^3 + 3x^2$$

und

$$g(x,3,z) = z^3 + 4z^2 + 10z + 40\,.$$

Die Spezialisierungen in x und ihre größten gemeinsamen Teiler sind

d	$f(d,3,z)$	$g(d,3,z)$	ggT
1	$3z^2+13z+4$	$z^3+4z^2+10z+40$	$z+4$
2	$3z^2+19z+20$	$z^3+5z^2+13z+65$	$z+5$
3	$3z^2+27z+54$	$z^3+6z^2+18z+108$	$z+6$
4	$3z^2+37z+112$	$z^3+7z^2+25z+175$	$z+7$

Hier ist entsprechend $h_3(x,z) = x+3+z$.

Für $c = 4$ schließlich erhalten wir

$$f(x,4,z) = 4z^2 + (x^2+4x+16)z + x^3 + 4x^2$$

und

$$g(x,4,z) = z^3 + (x+4)z^2 + (x^2+16)z + x^3 + 4x^2 + 16x + 64\,.$$

Die Spezialisierungen in x und ihre größten gemeinsamen Teiler sind

d	$f(d,4,z)$	$g(d,4,z)$	ggT
1	$4z^2+21z+5$	$z^3+5z^2+17z+85$	$z+5$
2	$4z^2+28z+24$	$z^3+6z^2+20z+120$	$z+6$
3	$4z^2+37z+63$	$z^3+7z^2+25z+175$	$z+7$
4	$4z^2+48z+128$	$z^3+8z^2+32z+256$	$z+8$

Dies führt auf $h_4(x,z) = x+4+z$.

Auch das Polynom $h(x,y,z)$ mit $h(x,c,z) = h_c(x,z)$ für $c = 1,2,3,4$ läßt sich ohne Interpolationsformel leicht erraten: Offensichtlich ist

$$h(x,y,z) = x+y+z\,.$$

Division zeigt, daß

$$\frac{f}{h} = x^2 + yz \quad \text{und} \quad \frac{g}{h} = x^2 + y^2 + z^2$$

ist; somit ist

$$\mathrm{ggT}(f,g) = h = x+y+z\,.$$

Dieses Ergebnis hätten wir natürlich schon sehr viel früher erraten können, und in der Tat wird der Algorithmus oft so implementiert, daß man bereits nach eigentlich zu wenigen Spezialisierungen interpoliert und nachprüft, ob man einen gemeinsamen Teiler gefunden hat; wenn ja, ist dies der ggT. Falls nein, läßt sich aber noch nicht schließen, daß alle bisherigen Spezialisierungen schlecht waren; vielleicht waren auch nur die Grade einiger Koeffizienten zu klein, was sich nur durch weitere Spezialisierungen und Interpolationen feststellen läßt.

§ 2: Faktorisierung von Polynomen mehrerer Veränderlicher

Auch bei der Faktorisierung von Polynomen in mehrerer Veränderlichen können wir uns anlehnen an die Vorgehensweise, den wir (aus Kapitel 3) für Polynome einer Veränderlichen über $\mathbb{Z}$ kennen.

Wir gehen wieder aus vom Polynomring $R_n = k[x_1,\ldots,x_n]$ in n Veränderlichen über $k = \mathbb{Z}$ oder einem der Körper $k = \mathbb{Q}$ oer $k = \mathbb{F}_p$, oder einem anderen Ring oder Körper, für den wir Polynome aus $k[x]$ faktorisieren können. Wir fassen unsere Polynome auf als Polynome in der einen Variablen x_n über dem Ring R_{n-1}. Indem wir jeder der Variablen $x_1,\ldots,x_{n-1}$ einen Wert $c_i \in k$ geben, erhalten wir ein Polynom aus $k[x_n]$, das wir mit den Methoden aus Kapitel 3 faktorisieren können. Um diese Faktorisierung hochzuheben zu einer Faktorisierung in $R_n = R_{n-1}[x_n]$ brauchen wir eine Art HENSELsches Lemma, allerdings wird dieses hier etwas komplizierter als in Kapitel 3, da wir nicht einfach modulo einer Primzahl oder einem irreduziblen Polynom rechnen. In unserer Situation sind einige Begriffe aus der absgtrakten Algebra nützlich:

Definition: *a)* Eine Teilmenge I eines kommutativen Rings R heißt Ideal, in Zeichen $I \lhd R$, wenn erstens die Summe zweier Elemente aus I wieder in I liegt und wenn zweitens für jedes Element $f \in R$ und jedes $g \in I$ das Produkt fg in I liegt.
b) Für $g_1, \ldots, g_r \in R$ bezeichnen wir mit $(g_1, \ldots, g_r)$ das kleinste Ideal von R, das die Elemente g_i enthält, d.h.

$$(g_1, \ldots, g_r) = \left\{ f_1 g_1 + \cdots + f_r g_r \;\middle|\; f_i \in R \right\} .$$

Im Falle eines einzigen Elements g bezeichnen wir (g) als das von g erzeugte Hauptideal. *c)* Sind I, J zwei Ideale von R, so bezeichnen wir mit IJ das kleinste Ideal von R, das alle Elemente der Form fg mit $f \in I$ und $g \in J$ enthält. Die Potenzen I^n eines Ideals I werden durch fortgesetzte Produktbildung definiert.
d) Zwei Elemente $f, g \in R$ heißen kongruent modulo dem Ideal $I \lhd R$, in Zeichen $f \equiv g \bmod I$, wenn ihre Differenz in I liegt.

Beispielsweise ist in $\mathbb{Z}$ jedes Ideal I ein Hauptideal: Falls I nur aus der Null besteht, ist das klar; andernfalls sei z das betragskleinste von Null verschiedene Element. Dann muß jedes andere Element $w \in I$ durch z teilbar sein, denn andernfalls hätte der Rest bei der Division durch z kleineren Betrag als z und wäre als Linearkombination $r = w - qz$ Element von I. Somit ist $I = (z)$.

Die Ideale haben ihren Namen von ERNST EDUARD KUMMER (1810–1893), der sie als *ideale Zahlen* betrachtete: KUMMER glaubte zunächst, er habe einen Beweis der FERMAT-Vermutung gefunden, allerdings war er davon ausgegangen, daß der Ring $\mathbb{Z}[\zeta_p]$, wobei p eine primitive p-te Einheitswurzel bezeichnet, faktoriell ist. Dies ist zwar für unendlich viele Primzahlen p der Fall, aber eben nicht für alle. KUMMER konnte aber zeigen, daß es auf dem Niveau der Ideale eine eindeutige Primzerlegung gibt – nur reichte das leider nicht aus, um seinen Beweis auch für die Primzahlen zu retten für die $\mathbb{Z}[\zeta_p]$ nicht faktoriell ist.

Uns interessiert vor allem das Ideal

$$I = (x_1 - c_1, \ldots, x_m - c_m) \lhd R_m ;$$

wir wollen uns überlegen, daß für zwei Elemente $f, g \in R_m$ gilt:

$$f(c_1, \ldots, c_m) = g(c_1, \ldots, c_m) \Longleftrightarrow f \equiv g \bmod I .$$

Es ist klar, daß zwei Polynome, deren Differenz in I liegt, an der Stelle $(c_1, \ldots, c_m)$ denselben Wert annehmen müssen; zu zeigen ist die Umkehrung.

Für $m = 1$ ist sie wohlbekannt: Dann ist $f - g$ ein Polynom in einer Veränderlichen, und das verschwindet genau dann an der Stelle $x_1 = c_1$, wenn es durch $(x_1 - c_1)$ teilbar ist.

Für $m > 1$ schreiben wir

$$f - g = \sum_{j=0}^{r} a_j(x_1, \ldots, x_{m-1})(x_m - c_m)^j .$$

Einsetzen von $x_i = c_i$ für alle i sorgt dafür, daß rechts alle Summanden mit $j > 0$ verschwinden; wenn $f - g$ insgesamt bei diesen Werten verschwinden soll, muß also $a_0(c_1, \ldots, c_{m-1}) = 0$ sein. Nach Induktionsannahme läßt sich dieses Polynom als Summe von Vielfachen der $(x_i - c_i)$ für $i < m$ schreiben, und da die Summanden mit $j > 0$ Vielfache von $(x_m - c_m)$ sind, zeigt dies die Behauptung.

Wenn wir bei einem Polynom $f \in R_n$ für die Variablen $x_1, \ldots, x_{n-1}$ Zahlen $c_i \in k$ einsetzen, erhalten wir ein Polynom aus $k[x_n]$, das wir mit den Methoden aus Kapitel 3 faktorisieren können. Für eine Faktorisierung

$$f(c_1, \ldots, c_{n-1}, x_n) = g(x_n)h(x_n)$$

können wir auch sagen, daß $f \equiv gh \bmod I$ ist mit

$$I = (x_1 - c_1, \ldots, x_{n-1} - c_{n-1}) \lhd R_n .$$

Die Polynomversion des HENSELschen Lemmas gibt uns für jedes $k \in \mathbb{N}$ Polynome $g_k, h_k \in R_n$, für die $f \equiv g_k h_k \bmod I^k$ ist. Da I^k erzeugt wird von Polynomen k-ten Grades, gibt uns das für Exponenten von k, die über dem Gesamtgrad von f liegen, Kandidaten für eine Faktorisierung in R_n. In Analogie zum klassischen HENSELschen Lemma gilt:

Lemma: Zu $f \in R_n = k[x_1, \ldots, x_n]$ gebe es zwei teilerfremde Polynome $g, h \in k[x_n]$ derart, daß für gewisse Elemente $c_i \in k$ gilt

$$f(c_1, \ldots, c_{n-1}, x_n) = g(x_n) \cdot h(x_n) .$$

Dann gibt es auch zu jedem $\ell \in \mathbb{N}$ Polynome $g_\ell, h_\ell \in R_n$, so daß

$$g_\ell \equiv g \bmod I^\ell, \quad h_\ell \equiv h \bmod U^\ell \quad \text{und} \quad f \equiv g_\ell \cdot h_\ell \bmod I^\ell$$