Kapitel 4
Faktorisierung von Polynomen

In diesem Kapitel werden wir eine andere Art modularer Methoden kennenlernen, die vor allem für die Faktorisierung von Polynomen nützlich ist, die allerdings auch gelegentlich bei der Berechnung größter gemeinsamer Teiler bessere Ergebnisse liefert als der Ansatz aus dem vorigen Kapitel.

Der dortige Ansatz funktionierte, weil es höchstens endlich viele Stellen schlechter Reduktion gab. Wie wir bald sehen werden, ist das bei der Faktorisierung von Polynomen nicht mehr der Fall: Hier kann es passieren, daß wir *überall* schlechte Reduktion haben, und daß die Faktorisierungen modulo verschiedener Primzahlen zu Faktoren verschiedener Grade führen. Hier ist der chinesische Restesatz offensichtlich keine geeignete Strategie für die modulare Berechnung.

Stattdessen werden wir uns hier auf eine einzige Primzahl p beschränken und dann diese Ergebnisse hochheben zu Faktorisierungen modulo der Potenzen von p, bis wir oberhalb der Schranke für die Beträge der Koeffizienten von Teilern sind. Falls das, was wir dann bekommen, keine Teiler des ursprünglichen Polynoms sind, müssen wir versuchen, diese so lange zu kombinieren, bis wir einen Teiler gefunden haben – im Extremfall das Ausgangspolynom selbst.

Wir wissen aus Kapitel II, §4, daß sich jedes Polynom in endlich vielen Veränderlichen über einem Körper bis auf Reihenfolge und Einheiten eindeutig als Produkt irreduzibler Faktoren schreiben läßt; der auf GAUSS zurückgehende Beweis ist allerdings nicht konstruktiv. Bevor wir uns mit dem Problem der konstruktiven Faktorisierung beschäftigen, sollten wir uns aber zunächst überlegen, ob sich der Aufwand lohnt, ob es uns

also wirklich etwas nützt, die irreduziblen Faktoren eines gegebenen Polynoms zu kennen.

Eine der Grundaufgaben der Computeralgebra und das zentrale Thema dieser Vorlesung ist die Lösung nichtlinearer Gleichungen und Gleichungssysteme. Schon im Falle einer Gleichung in einer Variablen wird dies mit zunehmendem Grad immer schwieriger: Für lineare Gleichungen ist die Lösung fast trivial und für quadratische Gleichungen haben wir die aus der Schule wohlbekannten Formeln. Für kubische und biquadratische Gleichungen gibt es *im Prinzip* immer noch solche Formel, sie sind aber deutlich komplizierter und liefern zumindest *a priori* das Ergebnis oft nicht in seiner einfachstmöglichen Form. Ab Grad fünf zeigt uns ein Satz von NILS ABEL aus der Algebra, daß es zumindest für die allgemeinstmögliche Gleichung diesen Grades keine Formel mehr geben kann, die nur Grundrechenarten und Wurzeln benutzt. Es gibt zwar Formeln, die zumindest für Polynome mit reellen oder komplexen Koeffizienten stattdessen andere Funktionen wie Modulfunktionen und speziell Thetafunktionen verwenden, aber diese Funktionen sind über unendliche Reihen definiert und daher für die exakten algebraischen Rechnungen, um die es uns hier in der Computeralgebra geht, nicht geeignet. Im übrigen sind auch schon die Wurzelausdrücke für die Lösung kubischer und biquadratischer Gleichungen oft numerisch instabil, so daß die direkte numerische Berechnung nach einem numerischen Verfahren wie dem von NEWTON zu erheblich besseren Ergebnissen führt als die numerische Anwendung einer Lösungsformel.

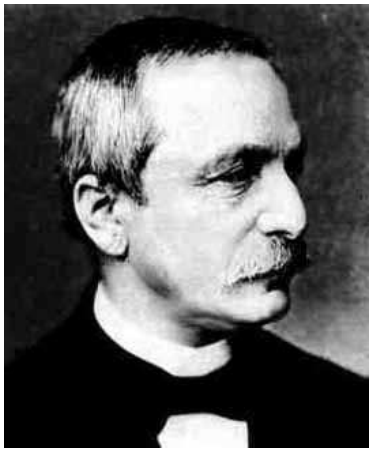
Wir gewinnen daher sehr viel, wenn wir eine Polynomgleichung höheren Grades faktorisieren können in Faktoren der Grade eins und zwei. Wenn wir an exakten Lösungen interessiert sind, gibt uns die reell-algebraische Geometrie Verfahren, mit denen wir die Nullstellen auch Polynome höheren Grades eindeutig charakterisieren können falls die Koeffizienten aus einem Teilkörper von $\mathbb{R}$ oder $\mathbb{C}$ stammen, in dem wir exakt rechnen können; aber auch hier steigt der Aufwand sehr schnell mit dem Grad und es ist daher meist effizienter, die Gleichungen, sofern möglich, über $\mathbb{Q}$ oder einem nicht allzu großen Erweiterungskörper zu zerlegen und dann nach Nullstellen der Faktoren zu suchen.

Im Falle von Gleichungssystemen wächst der Aufwand noch stärker mit

den Graden der Gleichungen; wenn wir diese faktorisieren können und stattdessen mit den Gleichungssystem aus Kombinationen von Faktoren arbeiten, wächst der Aufwand zwar angesichts der Vielzahl von Kombinationen auch deutlich, ist aber doch insgesamt immer noch geringer.

§1: Der Algorithmus von Kronecker

Der erste zumindest im Prinzip konstruktive Beweis für die Faktorisierbarkeit von Polynomen geht zurück auf LEOPOLD KRONECKER. Er führt das Problem der Faktorisierung eines Polynoms über $\mathbb{Z}$ zurück auf das (zumindest für große Zahlen alles andere als einfache) Problem der Faktorisierung ganzer Zahlen. Ausgangspunkt ist die folgende triviale Beobachtung: Angenommen, wir haben in $\mathbb{Z}[X]$ eine Zerlegung $f = gh$. Für jede ganze Zahl a ist dann $f(a) = g(a)h(a)$. Somit ist $g(a)$ für jedes $a \in \mathbb{Z}$ ein Teiler von $f(a)$.



LEOPOLD KRONECKER (1823–1891) ist heute zwar Vielen nur im Zusammenhang mit dem KRONECKER-δ bekannt, er war aber einer der bedeutendsten deutschen Mathematiker seiner Zeit. Seine Arbeiten befaßten sich mit Algebra, Zahlentheorie und Analysis, wobei er insbesondere die Verbindungen zwischen der Analysis und den beiden anderen Gebieten erforschte. Bekannt ist auch seine Ablehnung jeglicher mathematischer Methoden, die, wie die Mengenlehre oder Teile der Analysis, unendliche Konstruktionen verwenden. Er war deshalb mit vielen anderen bedeutenden Mathematikern seiner Zeit verfeindet, z.B. mit CANTOR und mit WEIERSTRASS

Ein Polynom vom Grad d ist eindeutig bestimmt durch seine Werte an d+1 verschiedenen Stellen $a_0, \ldots, a_n$ und kann mit Hilfe wohlbekannter Interpolationsformeln leicht aus den $d + 1$ Paaren $\big(a_i, g(a_i)\big)$ bestimmt werden; die möglichen Werte $g(a_i)$ wiederum sind Teiler der $f(a_i)$.

Daher berechnet KRONECKER auf der Suche nach einem Teiler vom Grad d für $d + 1$ beliebig gewählte ganzzahlige Werte $a_0, \ldots, a_d$ die Funktionswerte $f(a_0), \ldots, f(a_d)$, und konstruiert für jedes $(d + 1)$-tupel $(b_0, \ldots, b_d)$ ganzer Zahlen mit $b_i | f(a_i)$ ein Interpolationspolynom g mit $g(a_i) = b_i$. Falls keines der Polynome Teiler von f ist, hat f keinen Teiler vom Grad d, andernfalls wird einer gefunden.

Über den Grad d eines potentiellen Teilers ist natürlich *a priori* nichts bekannt; wir wissen nur eines: Wenn es einen nichttrivialen Teiler gibt, dann gibt es auch einen, dessen Grad höchstens gleich der Hälfte des Grads von f ist. Im Extremfall müssen wir daher alle diese Grade ausprobieren, bis sich dann möglicherweise herausstellt, daß f irreduzibel ist. Falls dann noch einige der Zahlen $f(a_i)$ viele Teiler haben, läßt sich leicht vorstellen, daß der Aufwand schon für sehr moderate Grade von f astronomisch wird. Zum Glück gibt es deutlich effizientere Alternativen, so daß der Algorithmus von KRONECKER in der Praxis nie eingesetzt wird.

Als Beispiel wollen wir versuchen, das Polynom

$$f = 8X^7 - 16X^6 - 20X^5 + 15X^4 + 13X^3 + 9X^2 + 10X + 2$$

in $\mathbb{Z}[X]$ zu faktorisieren.

Als erstes suchen wir nach Linearfaktoren; diese haben die Form $(bX+c)$. Um sie mit KRONECKERs Methode zu finden, müssen wir die Funktion an zwei Stellen mit möglichst einfachen Funktionswerten betrachten; dazu bieten sich $x_0 = -1$ mit $f(x_0) = -1$ und $x_1 = 0$ mit $f(x_1) = 2$ an. Für einen Teiler $g \in \mathbb{Z}[X]$ von f muß daher $g(x_0) = \pm 1$ und $g(x_1) = \pm 1$ oder ± 2 sein.

Tatsächlich können wir uns auf Polynome mit $g(x_0) = 1$ beschränken, denn g ist genau dann ein Teiler, wenn auch $-g$ einer ist, und wenn das eine Polynom an der Stelle -1 den Wert 1 hat, ist das andere dort gleich -1. Wir müssen also die Interpolationspolynome zu den vier Wertepaaren $\big((-1,1),(0,y_0)\big)$ mit $y_0 \in \{-2,-1,1,2\}$ konstruieren und testen, ob sie f teilen. Der Maple-Befehl zur Konstruktion des Interpolationspolynoms durch die Punkte (x_1,y_1) bis (x_n,y_n) ist `interp([x1, ..., xn], [y1, ..., yn], X);` wir schreiben also

```
> for y0 in [-2, -1, 1, 2] do
> g := interp([-1, 0], [1, y0], X);
> if rem(f, g, X) = 0 then print(g) fi od:
```

1

Die einzige „Lösung“ die wir bekommen, ist das konstante Polynom 1, das natürlich auf keine Faktorisierung führt. Somit gibt es keine linearen Faktoren.

Auf der Suche nach quadratischen Faktoren brauchen wir einen weiteren Interpolationspunkt; da $f(1) = 21$ nur zwei Primteiler hat, bietet sich $x = 1$ an, wo ein Teiler von f einen der acht Werte $\pm 1, \pm 3, \pm 7$ oder ± 21 annehmen muß. Nun müssen also schon $4 \times 8 = 32$ Interpolationspolynome konstruiert und durchprobiert werden:

```
> for y0 in [-2, -1, 1, 2] do
> for y1 in [-21, -7, -3, -1, 1, 3, 7, 21] do
> g := interp([-1, 0, 1], [1, y0, y1], X);
> if rem(f, g, X) = 0 then print(g) fi od od:
```

$$1$$

Es gibt also auch keine quadratischen Teiler.

Für kubische Faktoren brauchen wir einen weiteren Interpolationspunkt. Wir kennen bereits die beiden Funktionswerte $f(2) = -238$ und $f(-2) = -1254$; Versuche mit anderen betragskleinen x-Werten liefern nicht besseres. Da $238 = 2 \cdot 7 \cdot 17$ nur drei Primteiler hat, $1254 = 2 \cdot 3 \cdot 11 \cdot 19$ aber vier, versuchen wir unser Glück mit dem Punkt $(2, -238)$, wobei wir nun für $g(2)$ schon 16 Werte betrachten müssen, insgesamt also $4 \times 8 \times 16 = 512$ Interpolationspolynome:

```
> for y0 in [-2, -1, 1, 2] do
> for y1 in [-21, -7, -3, -1, 1, 3, 7, 21] do
> for y2 in [-238, -119, -34, -17, -14, -7, -2, -1,
>            1, 2, 7, 14, 17, 34, 119, 238] do
> g := interp([-1, 0, 1, 2], [1, y0, y1, y2], X);
> if rem(f, g, X) = 0 then print(g) fi od od od:
```

$$1$$

$$-2X^3 + 3X^2 + 5X + 1$$

Somit gibt es bis aufs Vorzeichen genau einen kubischen Faktor, und die Zerlegung von f ist

$$\begin{aligned} f &= (-2X^3 + 3X^2 + 5X + 1)(-4X^4 + 2X^3 + 3X^2 + 2) \\ &= (2X^3 - 3X^2 - 5X - 1)(4X^4 - 2X^3 - 3X^2 - 2)\,. \end{aligned}$$

§2: Die quadratfreie Zerlegung eines Polynoms

Wir betrachten ein Polynom f über einem Körper oder einem faktoriellen Ring k. Da der Polynomring $k[X]$ faktoriell ist, zerfällt f dort in ein Produkt aus einer Einheit $u \in k^\times$ und Potenzen irreduzibler Polynome aus $k[X]$:

$$f = u \prod_{i=1}^{N} q_i^{e_i} .$$

Falls alle $e_i = 1$ und kein zwei q_i zueinander assoziiert sind, bezeichnen wir f als quadratfrei. Ziel der quadratfreien Zerlegung ist es, ein beliebiges Polynom f in der Form

$$f = \prod_{j=1}^{M} g_j^j$$

zu schreiben, wobei die g_j paarweise teilerfremde quadratfreie Polynome sind. Vergleichen wir mit der obigen Darstellung und vernachlässigen wir für den Augenblick die Einheit u, so folgt, daß g_j das Produkt aller q_i mit $e_i = j$ ist.

a) Quadratfreie Zerlegung über den reellen Zahlen

Wenn ein Polynom $f \in \mathbb{R}[X]$ eine mehrfache Nullstelle hat, verschwindet dort auch die Ableitung f'. Allgemeiner gilt, daß für ein Polynom $h \in \mathbb{R}[X]$, dessen e-te Potenz f teilt, zumindest h^{e-1} auch die Ableitung f' teilen muß, denn ist $f = h^e g$, so ist

$$f' = eh^{e-1}h'g + h^e g' = h^{e-1}(eh'g + hg') .$$

Falls f *genau* durch h^e teilbar ist, ist auch f' genau durch h^{e-1} teilbar, denn wäre es sogar durch h^e teilbar, so wäre auch $eh^{e-1}h'g$ durch h^e teilbar, so daß h ein Teiler von g wäre.

Damit ist $\mathrm{ggT}(f, f') = \prod_{i=1}^{r} f_i^{e_i - 1}$ und

$$h_1 = \frac{f}{\mathrm{ggT}(f, f')} = \prod_{i=1}^{r} q_i$$

ist das Produkt aller irreduzibler Faktoren von f. Alle irreduziblen Faktoren von f, die dort mindestens in der zweiten Potenz vorkommen, sind auch Teiler von f', also ist

$$g_1 = \frac{h_1}{\mathrm{ggT}(h_1, f')}$$

das Produkt aller irreduzibler Faktoren von f, die dort genau in der ersten Potenz vorkommen.

In $f_1 = f/h_1$ kommen alle irreduziblen Faktoren von f mit einem um eins verminderten Exponenten vor; insbesondere sind also die mit $e_i = 1$ verschwunden. Wenden wir darauf dieselbe Konstruktion an, erhalten wir die Zerlegung $\mathrm{ggT}(f_1, f_1') = \prod_{i=1}^{r} f_i^{\max(e_i-2,0)}$, und

$$h_2 = \frac{f_1}{\mathrm{ggT}(f_1, f_1')} = \prod_{i=1}^{r} q_i$$

ist das Produkt aller irreduzibler Faktoren von f_1, also das Produkt aller Faktoren von f, die mit einem Exponenten von mindestens zwei vorkommen. Damit ist

$$g_2 = \frac{h_2}{\mathrm{ggT}(h_2, f_1')}$$

das Produkt aller Faktoren, die in f mit Multiplizität genau zwei vorkommen.

Nach dem gleichen Schema können wir, falls $f_2(x)$ nicht konstant ist, weitermachen und rekursiv für $i \geq 3$ definieren

$$h_i = \frac{f_{i-1}}{\mathrm{ggT}(f_{i-1}, f_{i-1}')}, \quad g_i(x) = \frac{h_i}{\mathrm{ggT}(h_i, f_{i-1}')} \quad \text{und} \quad f_i(x) = \frac{f_{i-1}}{h_i},$$

bis wir für ein konstantes f_i erhalten. Dann hat jedes Polynom g_i nur einfache Nullstellen, und diese Nullstellen sind genau die i-fachen Nullstellen des Ausgangspolynoms f.

Bis auf eine eventuell notwendige Konstante c ist damit f das Produkt der Polynome g_j^j, und falls wir alle Nullstellen der Polynome g_j bestimmen können, kennen wir alle Nullstellen von f.

Als Beispiel betrachten wir das Polynom

$$f(x) = X^4 - 5X^2 + 6X - 2 \quad \text{mit} \quad f'(X) = 4X^3 - 10X + 6\,.$$

Wir berechnen zunächst den ggT von f und f':

$$(X^4 - 5X^2 + 6X - 2) : (4X^3 - 10X + 6) = \frac{X}{4} \text{ Rest } -\frac{5}{2}X^2 + \frac{9}{2}X - 2$$

$$(4X^3 - 10X + 6) : \left(-\frac{5}{2}X^2 + \frac{9}{2}X - 2\right) = -\frac{8}{5}X - \frac{72}{25} \text{ Rest } -\frac{6}{25}X + \frac{6}{25}$$

$$\left(-\frac{5}{2}X^2 + \frac{9}{2}X - 2\right) : \left(-\frac{6}{25}X + \frac{6}{25}\right) = \frac{125}{12}X - \frac{25}{3}$$

Somit ist der ggT gleich $-\frac{6}{25}(X - 1)$; da es auf Konstanten nicht ankommt, rechnen wir besser mit $(X - 1)$.

Eigentlich sind wir damit schon fertig: Der ggT hat nur die einfache Nullstelle $x = 1$, also hat $f(x)$ an der Stelle eins eine doppelte Nullstelle, und alles andere sind einfache Nullstellen. Da

$$(X^4 - 5X^2 + 6X - 2) : (X - 1)^2 = X^2 + 2X - 2$$

ist, haben wir die quadratfreie Zerlegung

$$f(X) = (X^2 + 2X - 2) \cdot (X - 1)^2\,.$$

Zur Illustration können wir aber auch strikt nach Schema weiterrechnen. Dann brauchen wir als nächstes

$$h_1 = \frac{f}{\text{ggT}(f, f')} = \frac{X^4 - 5X^2 + 6X - 2}{X - 1} = X^3 + X^2 - 4X + 2\,,$$

das Polynom das an jeder Nullstelle von $f(X)$ eine einfache Nullstelle hat. Sodann brauchen wir den ggT von $h_1(X)$ und $f'(X)$; da wir schon wissen, daß f und f' außer der Eins keine gemeinsame Nullstelle haben, muß das $(X - 1)$ sein. Somit ist

$$g_1 = \frac{X^3 + X^2 - 4X + 2}{X - 1} = X^2 + 2X - 2 = (X + 1)^2 - 3$$

das Polynom, das genau bei den einfachen Nullstellen von f verschwindet, also bei $-1 \pm \sqrt{3}$. Als nächstes muß

$$g_1(X) = \frac{f(X)}{h_1(X)} = \frac{X^4 - 5X^2 + 6X - 2}{X^3 + X^2 - 4X + 2} = X - 1$$

untersucht werden; da es nur für $X = 1$ verschwindet, ist die Eins eine doppelte Nullstelle von f. Damit sind alle Nullstellen von $f(X)$ sowie auch deren Vielfachheiten gefunden.

b) Ableitungen über einem beliebigen Körper

Auch wenn Ableitungen ursprünglich über Grenzwerte definiert sind, ist doch die Ableitung eines Polynoms rechnerisch gesehen eine rein algebraische Operation, die sich im Prinzip über jedem beliebigen Körper oder sogar Ring k erklären läßt: Wir *definieren* die Ableitung eines Polynoms

$$f = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in k[X]$$

als das Polynom

$$f' = d a_d X^{d-1} + (d-1) a_{d-1} X^{d-2} + \cdots + a_1 \in k[X]\,.$$

Es ist klar, daß die so definierte Abbildung $k[X] \to k[X]$, die jedem Polynom $f \in k[X]$ seine Ableitung f' zuordnet, k-linear ist. Auch die LEIBNIZsche Produktregel $(fg)' = fg' + fg'$ ist erfüllt: Wegen der Linearität der Ableitung und der Linearität beider Seiten der Formel sowohl in f als auch in g genügt es, dies für X-Potenzen nachzurechnen, und für $f = X^n, g = X^m$ ist $(fg)' = (n+m)X^{n+m-1}$ gleich

$$fg' + f'g = X^n m X^{m-1} + n X^{n-1} X^m = (m+n) X^{n+m-1}\,.$$

Damit gelten die üblichen Ableitungsregeln auch für die formale Ableitung von Polynomen aus $k[X]$.

c) Die Charakteristik eines Körpers

Es gibt allerdings einen wesentlichen Unterschied: In der Analysis folgt durch eine einfache Anwendung des Mittelwertsatzes, daß die Ableitung einer differenzierbaren Funktion genau dann identisch verschwindet, wenn die Funktion konstant ist. Bei einer rein algebraischen Behandlung des Themas können wir natürlich nicht auf den Mittelwertsatz der Differentialrechnung zurückgreifen, sondern müssen direkt nachrechnen, wann die Ableitung eines Polynoms gleich dem Nullpolynom ist.

Mit den obigen Bezeichnungen ist dies genau dann der Fall, wenn alle Koeffizienten ia_i der Ableitung verschwinden. Bei den Faktoren dieses Produkts handelt es sich um die Zahl $i \in \mathbb{N}_0$ und das Körperelement a_i.

Falls der Grundkörper k die rationalen Zahlen enthält, können wir auch i als Element von k auffassen und haben somit ein Produkt zweier Körperelemente. Dieses verschwindet genau dann, wenn mindestens einer der beiden Faktoren verschwindet; die Ableitung ist somit genau dann das Nullpolynom, wenn $a_i = 0$ für alle $i \neq 0$, wenn das Polynom also konstant ist.

Auch wenn $\mathbb{N}_0$ keine Teilmenge von k ist, muß k als Körper zumindest die Eins enthalten. Wir können daher rekursiv eine Abbildung φ von $\mathbb{N}_0$ nach k definieren durch die Vorgaben $\varphi(0) = 0$ und $\varphi(n + 1) = \varphi(n) + 1$ für alle $n \in \mathbb{N}_0$. Diese Abbildung läßt sich auf $\mathbb{Z}$ fortsetzen durch die weitere Forderung $\varphi(-n) = -\varphi(n)$.

Da die Addition in $\mathbb{N}$ rekursiv über Summen von Einsen definiert wird, überlegt man sich schnell, daß für zwei ganze Zahlen $a, b \in \mathbb{Z}$ gilt: $\varphi(a + b) = \varphi(a) + \varphi(b)$. Da die Multiplikation in $\mathbb{Z}$ rekursiv definiert ist über die Addition, folgt daraus wiederum, daß auch $\varphi(ab) = \varphi(a)\varphi(b)$ ist; φ ist also mit Addition und Multiplikation verträglich. (In der Algebra sagt man, φ sei ein Ringhomomorphismus.)

Falls $\varphi(n)$ nur für $n = 0$ verschwindet, kann $\mathbb{Z}$ und damit auch $\mathbb{Q}$ als Teilmenge von k aufgefaßt werden; andernfalls gibt es eine kleinste natürliche Zahl p, so daß $\varphi(p) = 0$ ist. Da $\varphi(1) = 1 \neq 0$, ist $p \geq 2$.

Ist a eine weitere ganze Zahl mit $\varphi(a) = 0$, so können wir a mit Rest durch p dividieren: $a = pb + r$ mit $0 \leq r < p$. Dabei ist

$$\varphi(r) = \varphi(a) - \varphi(pb) = \varphi(a) - \varphi(p)\varphi(b) = 0\,,$$

also ist auch $r = 0$, denn p ist die kleinste positive Zahl mit $\varphi(p) = 0$. Somit verschwindet $\varphi(p)$ genau für die Vielfachen von p.

Schreiben wir $p = ab$ als Produkt zweier natürlicher Zahlen a, b, so ist $0 = \varphi(p) = \varphi(a)\varphi(b)$. Da $\varphi(a)$ und $\varphi(b)$ Körperelemente sind, muß daher mindestens eines der beiden verschwinden; da beides natürliche Zahlen und höchstens gleich p sind, geht das nur, wenn eines gleich eins und das andere gleich p ist. Somit ist p eine Primzahl.

Definition: Wir sagen, ein Körper k habe die Charakteristik null, wenn die Abbildung $\varphi\colon \mathbb{Z} \to k$ injektiv ist. Andernfalls sagen wir, die Charakteristik von k sei gleich p, wobei p die kleinste natürliche Zahl ist mit $\varphi(p) = 0$.

Die Charakteristik eines Körpers ist somit entweder null oder eine Primzahl. Wir schreiben char $k = 0$ *bzw.* char $k = p$.

Offensichtlich bilden die rationalen, reellen und auch komplexen Zahlen Körper der Charakteristik null, und char $\mathbb{F}_p = p$.

Gehen wir zurück zur Ableitung eines Polynoms! Das Produkt ia_i ist gleich dem in k berechneten Produkt $\varphi(i)a_i$, verschwindet also genau dann, wenn mindestens einer der beiden Faktoren verschwindet. Für einen Körper der Charakteristik null verschwindet $\varphi(i)$ nur für $i = 0$; hier müssen also alle a_i mit $i \geq 1$ verschwindet, d.h. das Polynom ist konstant.

Für einen Körper der Charakteristik $p > 0$ verschwindet $\varphi(i)$ allerdings auch für alle Vielfachen von p, so daß die entsprechenden Koeffizienten nicht verschwinden müssen. Ein Polynom f über einem Körper der Charakteristik $p > 0$ hat daher genau dann das Nullpolynom als Ableitung, wenn es sich als Polynom in X^p schreiben läßt.

Wir wollen uns überlegen, daß dies genau dann der Fall ist, wenn das Polynom die p-te Potenz eines anderen Polynoms ist, dessen Koeffizienten allerdings möglicherweise in einem größeren Körper liegen. Ausgangspunkt dafür ist das folgende

Lemma: Ist k ein Körper der Charakteristik $p > 0$, so gilt für zwei Polynome $f, g \in k[X]$ und zwei Elemente a, b des Körpers die Gleichung $(af + bg)^p = a^p f^p + b^p g^p$. Insbesondere ist

$$\begin{aligned}&(a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0)^p \\ &= a_d^p X^{dp} + a_{d-1}^p X^{(d-1)p} + \cdots + a_1^p X^p + a_0^p \,.\end{aligned}$$

Beweis: Nach dem binomischen Lehrsatz ist

$$(af + bg)^p = \sum_{i=0}^{p} \binom{p}{i} (af)^i (bg)^{p-i} \quad \text{mit} \quad \binom{p}{i} = \frac{p \cdots (p-i+1)}{i!} \,.$$

Für $i = 0$ und $i = p$ ist $\binom{p}{i} = 1$, für alle anderen i steht p zwar im Zähler, nicht aber im Nenner des obigen Bruchs. Daher ist $\binom{p}{i}$ durch p teilbar, die Multiplikation mit $\binom{p}{i}$ ist also die Nullabbildung. Somit ist

$$(af + bg)^p = (af)^p + (bg)^p = a^p f^p + b^p g^p \ .$$

Durch Anwendung auf die Summanden des Polynoms folgt daraus induktiv auch die zweite Formel. ∎

Wir können dieses Lemma auch speziell auf eine Summe von lauter Einsen anwenden; dann folgt

$$\underbrace{(1 + \cdots + 1)}_{n \text{ mal}}^p = \underbrace{1^p + \cdots + 1^p}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} \ ;$$

solche Summen sind also gleich ihrer p-ten Potenz. Somit gilt

Kleiner Satz von Fermat: Für jedes Element $a \in \mathbb{F}_p$ ist $a^p = a$. ∎

Speziell für den Körper $\mathbb{F}_p$ vereinfacht sich daher das obige Lemma zum folgenden

Korollar: Für ein Polynom mit Koeffizienten aus $\mathbb{F}_p$ ist

$$\begin{aligned}&(a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0)^p \\ &= a_d X^{dp} + a_{d-1} X^{(d-1)p} + \cdots + a_1 X^p + a_0 \ .\end{aligned}$$

Der französische Mathematiker PIERRE DE FERMAT (1601–1665) wurde in Beaumont-de-Lomagne geboren. Bekannt ist er heutzutage vor allem für seine 1994 von ANDREW WILES bewiesene Vermutung, wonach die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine ganzzahlige Lösung mit $xyz \neq 0$ hat. Dieser „große“ Satzes von FERMAT, von dem FERMAT lediglich in einer Randnotitz behauptete, daß er ihn beweisen könne, erklärt den Namen der obigen Aussage. Obwohl FERMAT sich sein Leben lang sehr mit Mathematik beschäftigte und wesentliche Beiträge zur Zahlentheorie, Wahrscheinlichkeitstheorie und Analysis lieferte, war er hauptberuflich Jurist und Chef der Börse von Toulouse.

d) Quadratfreie Zerlegung über beliebigen Körpern

Falls ein Polynom f durch das Quadrat q^2 eines anderen teilbar ist, gibt es ein Polynom $g \in k[X]$ mit $f = q^2 g$, und nach der Produktregel ist $f' = 2qg + q^2 g' = q(2g + qg')$, d.h. q teilt auch f' und damit den ggT von f und f'.

Ist umgekehrt ein irreduzibles Polynom $q \in k[X]$ Teiler von f, etwa $f = qh$, so ist $f' = q'h + qh'$ genau dann durch q teilbar, wenn $q'h$ durch q teilbar ist. Da q irreduzibel ist, muß dann entweder q' oder h durch q teilbar sein. Wäre q ein Teiler von q', so müßte q' aus Gradgründen das Nullpolynom sein, q selbst also entweder konstant oder – über einem Körper positiver Charakteristik – eine p-te Potenz. Beides ist durch die Definition eines irreduziblen Polynoms ausgeschlossen. Somit muß dann h durch q teilbar sein und $f = qh$ durch q^2. Damit haben wir bewiesen:

Lemma: Ein irreduzibles Polynom q ist genau dann ein mindestens quadratischer Faktor von f, wenn es den ggT von f und f' teilt. ∎

Genauer: Wenn q in der Primfaktorzerlegung von f in der Potenz q^e auftritt, d.h. $f = q^e g$ mit $q \nmid g$, so ist $f' = eq^{e-1} g + q^e g'$.

Über $\mathbb{R}$ würde daraus folgen, daß q^{e-1} die höchste q-Potenz ist, die f' teilt. Da wir aber über einem beliebigen Körper arbeiten, könnte es sein, daß der erste Faktor verschwindet: Dies passiert genau dann, wenn der Exponent e durch die Charakteristik p des Grundkörpers teilbar ist. In diesem Fall ist $f' = q^e g$ mindestens durch q^e teilbar. Da f genau durch q^e teilbar ist, folgt

Lemma: Ist $f = u \prod q_i^{e_i}$ mit $u \in k^\times$ die Zerlegung eines Polynoms $f \in k[X]$ in irreduzible Faktoren, so ist der ggT von f und f' gleich $\prod q_i^{d_i}$ mit $d_i = \begin{cases} e_i - 1 & \text{falls } p \nmid e_i \\ e_i & \text{falls } p \mid e_i \end{cases}$. ∎

Nach dem Lemma ist zumindest klar, daß $h_1 = f / \operatorname{ggT}(f, f')$ ein quadratfreies Polynom ist, nämlich das Produkt aller jener Primfaktoren

von f, deren Exponent nicht durch p teilbar ist. In Charakteristik null ist also $f / \operatorname{ggT}(f, f')$ einfach das Produkt der sämtlichen irreduziblen Faktoren von f. Diejenigen Faktoren, die mindestens quadratisch vorkommen, sind gleichzeitig Teiler des ggT; das Produkt g_1 der Faktoren, die genau in der ersten Potenz vorkommen, ist also $h_1 / \operatorname{ggT}\big(h_1, \operatorname{ggT}(f, f')\big)$.

Falls $\operatorname{ggT}(f, f')$ kleineren Grad als f hat, können wir rekursiv weitermachen und nach derselben Methode das Produkt aller Faktoren bilden, die in $f_1 = \operatorname{ggT}(f, f')$ genau mit Exponent eins vorkommen; in f selbst sind das quadratische Faktoren. Weiter geht es mit $f_2 = \operatorname{ggT}(f_2, f_2')$, dessen Faktoren mit Exponent eins kubisch in f auftreten, *usw.*

Über einem Körper der Charakteristik null liefert diese Vorgehensweise die gesamte quadratfreie Zerlegung; in positiver Charakteristik kann es allerdings vorkommen, daß $\operatorname{ggT}(f, f') = f$ ist. Da $\deg f' < \deg f$, ist dies genau dann der Fall, wenn $f' = 0$ ist. Dies ist in Charakteristik Null genau dann der Fall, wenn f konstant ist; in Charakteristik $p > 0$ verschwindet aber auch die Ableitung eines jeden Polynoms in X^p. Somit ist hier $f' = 0$ genau dann, wenn alle in f vorkommenden X-Potenzen einen durch p teilbaren Exponenten haben. Für $f \in \mathbb{F}_p[X]$ ist dann, wie wir oben gesehen haben,

$$\begin{aligned} f &= a_{dp}X^{dp} + a_{(d-1)p}X^{(d-1)p} + \cdots + a_pX^p + a_0 \\ &= \left(a_{dp}X^p + a_{(d-1)p}X^{(d-1)} + \cdots + a_pX + a_0\right)^p , \end{aligned}$$

f ist dann also die p-te Potenz eines anderen Polynoms, und wir können den Algorithmus auf dieses anwenden. Im Endergebnis müssen dann natürlich alle hier gefundenen Faktoren in die p-te Potenz gehoben werden.

In anderen Körpern der Charakteristik p ist die Situation etwas komplizierter: Dort müssen wir zunächst Elemente b_i finden mit $b_i^p = a_{ip}$; dann ist

$$f = \left(b_dX^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0\right)^p .$$

Solche Elemente müssen nicht existieren, es gibt aber eine große Klasse von Körpern, in denen sie stets existieren:

Definition: Ein Körper k der Charakteristik $p > 0$ heißt vollkommen, wenn die Abbildung $k \to k$; $x \mapsto x^p$ surjektiv ist.

Man kann zeigen, daß jeder endliche Körper vollkommen ist: Im Körper mit p^n Elementen ist $x^{p^n} = x$ für alle $x \in \mathbb{F}_{p^n}$, und damit ist x die p-te Potenz von $y = x^{p^{n-1}}$. Ein Beispiel eines nicht vollkommenen Körpers wäre $\mathbb{F}_p(X)$, wo X offensichtlich nicht als p-te Potenz eines anderen Körperelements geschrieben werden kann.

Über einem vollkommenen Körper der Charakteristik $p > 0$ kann man also jedes Polynom, dessen Ableitung das Nullpolynom ist, als p-te Potenz eines anderen Polynoms schreiben und so, falls man die p-ten Wurzeln auch effektiv berechnen kann, den Algorithmus zur quadratfreien Zerlegung durchführen. Insbesondere gibt es keinerlei Probleme mit den Körpern $\mathbb{F}_p$, denn dort ist jedes Element seine eigene p-te Wurzel.

§3: Der Berlekamp-Algorithmus

Wir gehen aus von einem *quadratfreien* Polynom über dem Körper $\mathbb{F}_p$ mit p Elementen, d.h. $f \in \mathbb{F}_p[X]$ ist ein Produkt von *verschiedenen* irreduziblen Polynomen $f_1, \ldots, f_N$. Durch quadratfreie Zerlegung läßt sich jedes Faktorisierungsproblem in $\mathbb{F}_p[X]$ auf diesen Fall zurückführen.

Um zu sehen, wie wir die f_i bestimmen können, nehmen wir zunächst an, sie seien bereits bekannt. Wir wählen uns dann irgendwelche Zahlen $s_1, \ldots, s_N \in \mathbb{F}_p$ und suchen ein Polynom $g \in \mathbb{F}_p[X]$ mit

$$g \equiv s_i \bmod f_i \quad \text{für alle } i = 1, \ldots, N\,.$$

Falls die s_i paarweise verschieden sind, können wir den Faktor f_i bestimmen als

$$f_i = \mathrm{ggT}(g - s_i, f)\,.$$

Nun können wir freilich nicht immer erreichen, daß die s_i alle paarweise verschieden sind: Wenn N größer als p ist, gibt es dazu einfach nicht genügend Elemente in $\mathbb{F}_p$. In diesem Fall ist $\mathrm{ggT}(g - s_i, f)$ das Produkt aller f_j mit $s_j = s_i$. Sofern nicht alle s_i gleich sind, führt das immerhin

zu einer partiellen Faktorisierung von f, die wir dann mit einem neuen Polynom $\widetilde{g}$ zu neuen Elementen $\widetilde{s}_i$ weiter zerlegen müssen *usw.*

Nach dem chinesischen Restesatz ist klar, daß es zu jeder Wahl von N Elementen $s_1, \ldots, s_N$ ein Polynom g gibt mit $g \equiv s_i \bmod f_i$, denn wegen der Quadratfreiheit von f sind die f_i ja paarweise teilerfremd. Das Problem ist nur, daß wir die f_i erst berechnen wollen und g daher nicht wie im Beweis des chinesischen Restesatzes konstruieren können. Wir müssen g also auch noch anders charakterisieren.

Nach dem kleinen Satz von FERMAT ist jedes s_i gleich seiner p-ten Potenz, also ist

$$g^p \equiv s_i^p = s_i \equiv g \bmod f_i \quad \text{für } i = 1, \ldots, N\,.$$

Da f das Produkt der paarweise teilerfremden f_i ist, gilt daher auch

$$g^p \equiv g \bmod f\,.$$

Falls umgekehrt ein Polynom $g \in \mathbb{F}_p[X]$ diese Kongruenz erfüllt, so ist f ein Teiler von $g^p - g$. Letzteres Polynom können wir weiter zerlegen:

Lemma: *a)* Über einem Körper k der Charakteristik $p > 0$ ist

$$X^p - X = \prod_{j=0}^{p-1}(X - j) \quad \text{und} \quad X^{p-1} - 1 = \prod_{j=1}^{p-1}(X - j)\,.$$

b) Für jedes Polynom $g \in k[X]$ ist

$$g^p - g = \prod_{j=0}^{p-1}(g - j) \quad \text{und} \quad g^{p-1} - 1 = \prod_{j=1}^{p-1}(g - j)\,.$$

Beweis: a) Nach dem kleinen Satz von FERMAT sind alle $i \in \mathbb{F}_p$ Nullstellen des Polynoms $X^p - X$, und da ein von null verschiedenes Polynom vom Grad p nicht mehr als p Nullstellen haben kann, gibt es keine weiteren. Die Gleichheit beider Seiten folgt somit daraus, daß die führenden Koeffizienten beider Polynome eins sind.

b) Im Polynomring $k[X]$ ist, wie wir gerade gesehen haben, $X^p - X$ gleich dem Produkt aller Polynome $(X - j)$. Diese Identität, genau wie

die für $X^{p-1} - 1$, bleibt natürlich erhalten, wenn man auf beiden Seiten für X irgendein Polynom aus $k[X]$ einsetzt.

■

Für ein Polynom $g \in \mathbb{F}_p[X]$ mit $g^p \equiv g \bmod f$ ist f daher ein Teiler von

$$\prod_{j=0}^{p}(g - j)\,,$$

jeder irreduzible Faktor f_i von f muß daher genau eines der Polynome $g - j$ teilen. Somit gibt es zu jedem Faktor f_i ein Element $s_i \in \mathbb{F}_p$, so daß $g \equiv s_i \bmod p$.

Wenn wir uns auf Polynome g beschränken, deren Grad kleiner ist als der von f, so ist g durch die Zahlen s_i eindeutig bestimmt, denn nach dem chinesischen Restesatz unterscheiden sich zwei Lösungen des Systems

$$g \equiv s_i \bmod f_i \quad \text{für } i = 1, \ldots, N$$

um ein Vielfaches des Produkts der f_i, also ein Vielfaches von f.

Die Menge V aller Polynome g mit kleinerem Grad als f, für die es Elemente $s_1, \ldots, s_N \in \mathbb{F}_p$ gibt, so daß die obigen Kongruenzen erfüllt sind, ist offensichtlich ein $\mathbb{F}_p$-Vektorraum: Für eine Linearkombination zweier Polynome aus V sind solche Kongruenzen erfüllt für die entsprechenden Linearkombinationen der s_i. Die Abbildung

$$\begin{cases} V \to \mathbb{F}_p^N \\ g \mapsto (g \bmod f_1, \ldots, g \bmod f_N) \end{cases}$$

ist nach dem chinesischen Restesatz ein Isomorphismus; somit ist die Dimension von V gleich der Anzahl N irreduzibler Faktoren von f.

Wie die obige Diskussion zeigt, ist V auch der Vektorraum aller Polynome g mit kleinerem Grad als f, für die $g^p \equiv g \bmod f$ ist. In dieser Form läßt sich V berechnen: Ist $\deg f = d$, so können wir jedes $g \in V$ schreiben als

$$g = g_{d-1}X^{d-1} + a_{d-2}X^{d-2} + \cdots + g_1X + g_0$$

und

$$g^p = g_{d-1}X^{(d-1)p} + g_{d-2}X^{(d-2)p} + \cdots + g_1X^p + g_0$$

mit geeigneten Koeffizienten $g_i \in \mathbb{F}_p$.

Modulo f müssen g und g^p übereinstimmen. Um dies in eine Bedingung an die Koeffizienten g_i zu übersetzen, dividieren wir die Potenzen X^{ip} mit Rest durch f:

$$X^{ip} \equiv \sum_{j=0}^{d-1} b_{ij} X^j \bmod f \,.$$

Dann muß gelten

$$\sum_{i=0}^{d-1} g_i X^{ip} \bmod f = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} b_{ij} g_i X^j = \sum_{j=0}^{d-1} g_j X^j \,.$$

Koeffizientenvergleich führt auf das homogene lineare Gleichungssystem

$$\sum_{i=0}^{d-1} b_{ij} g_i = g_j \quad \text{für } j = 0, \ldots, d-1 \,.$$

V ist also auch beschreibbar als der Lösungsraum dieses Gleichungssystems. Dieser läßt sich allein auf Grund der Kenntnis von f explizit berechnen, und seine Dimension ist gleich der Anzahl N der irreduziblen Faktoren von f; insbesondere ist er also genau dann eindimensional, wenn f irreduzibel ist.

Andernfalls wählen wir irgendein Element $g \in V$ und berechnen die Polynome ggT$(g - \lambda, f)$ für alle $\lambda \in \mathbb{F}_p$. Falls wir dabei N mal ein nichtkonstantes Polynom bekommen, haben wir f faktorisiert. Wenn wir weniger Faktoren bekommen, waren für das betrachtete Polynom g einige der Werte s_i gleich; wir bilden eine Liste der gefundenen (und zumindest noch nicht in allen Fällen irreduziblen) Faktoren, wählen ein von v linear unabhängiges neues Polynom $h \in V$ und verfahren damit genauso. Indem wir für jedes nichtkonstante Polynom ggT$(h - \lambda, f)$ den ggT mit den in der Liste stehenden Faktoren bilden, können wir die Listenelemente weiter zerlegen. Bei jeder gefundenen Zerlegung ersetzen wir das zerlegte Element durch seine Faktoren. Sobald die Liste N Faktoren enthält, sind wir fertig.

Falls die sämtlichen ggT($h - \lambda, f$) immer noch nicht ausreichen, um N Faktoren zu produzieren, müssen wir ein neues, von g und h linear unabhängiges Element von V wählen und damit weitermachen *usw.*

Das Verfahren muß spätestens mit dem N-ten Polynom enden, denn dann haben wir eine Basis $g_1, \ldots, g_N$ von V durchprobiert. Hätten wir dann noch nicht alle N Faktoren isoliert, müßte es (mindestens) zwei Faktoren f_i und f_j geben, so daß g mod f_i für alle Polynome g einer Basis von V gleich g mod f_j ist und damit für alle $g \in V$. Das ist aber nicht möglich, denn nach dem chinesischen Restesatz enthält V beispielsweise auch ein Element g mit g mod $f_i = 0$ und g mod $f_j = 1$.

Damit liefert uns dieser Algorithmus von BERLEKAMP zusammen mit der quadratfreien Zerlegung für jedes Polynom über $\mathbb{F}_p$ eine Zerlegung in irreduzible Faktoren. Mit einigen offensichtlichen Modifikationen schafft er dasselbe auch für Polynome über jedem der in dieser Vorlesung nicht behandelten anderen endlichen Körpern, allerdings ist für solche Körper gelegentlich ein alternativer Algorithmus von HARALD NIEDERREITER effizienter.

ELWYN BERLEKAMP wurde 1940 in Dover, Ohio geboren. Er studierte Elektrotechnik am MIT, wo er 1964 mit einer Arbeit aus dem Gebiet der Kodierungstheorie promovierte. Seine anschließenden Arbeiten und auch Positionen sowohl in der Wirtschaft als auch an Universitäten bewegen sich im Grenzgebiet zwischen Mathematik, Elektrotechnik und Informatik; einen gewissen Schwerpunkt bilden Bücher und Zeitschriftenartikel über die Mathematik von Spielen sowie Arbeiten zur Informationstheorie. 2006 emeritierte er als Mathematikprofessor in Berkeley. Seine dortige home page ist `math.berkeley.edu/~berlek/`

Als Beispiel wollen wir $f = X^6 + 2X^5 + 4X^4 + X^3 - X^2 - X - 1$ aus $\mathbb{F}_7[X]$ faktorisieren. Wir setzen ein Polynom vom Grad fünf mit unbestimmten Koeffizienten an:

```
> G := x -> add(g[i]*x^i, i=0..5);
```

$$G := x -> add(g_i x^i, i = 0..5)$$

```
> G(X);
```

$$g_0 + g_1 X + g_2 X^2 + g_3 X^3 + g_4 X^4 + g_5 X^5$$

Die siebte Potenz davon ist

```
> G(X^7);
```

$$g_0 + g_1X^7 + g_2X^{14} + g_3X^{21} + g_4X^{28} + g_5X^{35}$$

Um sie modulo f auszudrücken, müssen wir die Divisionsreste h_i bei der Division von X^{7i} durch f berechnen:

```
> for i to 5 do h[i] := Rem(X^(7*i), f, X) mod 7; od;
```

$$h_1 := 3X^3 + 6X^2 + 6X + 5$$
$$h_2 := 4X^5 + X^4 + 2X^3 + 6X + 6$$
$$h_3 := X^5 + 4X^4 + 6X^3 + 6X^2 + 2X + 5$$
$$h_4 := X^5 + 6X^4 + 5X^3 + X^2 + X + 2$$
$$h_5 := 2X^5 + 4X^4 + 6X^3 + 4X^2 + 2X + 5$$

Damit können wir g^7 mod f explizit hinschreiben:

```
> G7 := sort(collect(expand(
>             g0 + add(g[i]*h[i], i=1..5)), X), X);
```

$$G7 := (4g_2 + g_3 + 2g_5 + g_4)X^5 + (6g_4 + g_2 + 4g_3 + 4g_5)X^4$$
$$+(5g_4 + 6g_5 + 3g_1 + 6g_3 + 2g_2)X^3 + (g_4 + 4g_5 + 6g_1 + 6g_3)X^2$$
$$+(6g_2 + g_4 + 6g_1 + 2g_3 + 2g_5)X + 5g_5 + g0 + 6g_2 + 5g_3 + 2g_4 + 5g_1$$

Das soll gleich g sein, was auf ein lineares Gleichungssystem für die sechs Variablen $g[i]$ führt:

```
> LGS := seq(coeff(G7, X, i) = g[i], i=0..5);
```

$$LGS := \{5g_5 + g0 + 6g_2 + 5g_3 + 2g_4 + 5g_1 = g_0,$$
$$6g_2 + g_4 + 6g_1 + 2g_3 + 2g_5 = g_1,$$
$$g_4 + 4g_5 + 6g_1 + 6g_3 = g_2,$$
$$5g_4 + 6g_5 + 3g_1 + 6g_3 + 2g_2 = g_3,$$
$$6g_4 + g_2 + 4g_3 + 4g_5 = g_4,$$
$$4g_2 + g_3 + 2g_5 + g_4 = g_5\}$$

Zur Lösung eines Gleichungssystems über einem Körper $\mathbb{F}_p$ können wir den Befehl `msolve` verwenden; sein erstes Argument ist eine Menge von Gleichungen, das zweite, das auch fehlen kann, eine Menge von Variablen, und das dritte die Primzahl p. Da wir hier nach *allen* Variablen auflösen wollen, können wir auf das zweite Argument verzichten:

```
> msolve(LGS, 7);
```

$$g_0 = \_Z1, g_5 = \_Z2, g_4 = 3\_Z2, g_3 = 5\_Z2, g_1 = 6\_Z2, g_2 = 3\_Z2$$

Das bedeutet folgendes: Die Lösungen hängen ab von zwei Parametern; für diese führt Maple die Bezeichnungen `_Z1` und `_Z2` ein, wobei der Buchstabe „Z“ für ganze Zahl stehen soll. Insbesondere ist also der Lösungsraum zweidimensional, das Polynom f hat also zwei irreduzible Faktoren. Wir können uns eine Basis des Lösungsraums verschaffen, indem wir für das erste Basispolynom $\_Z1 = 1$ und $\_Z2 = 0$ setzen und für das zweite $\_Z1 = 0$ und $\_Z2 = 1$. Mit dem Befehl

```
> assign(%);
```

können wir aus den obigen Gleichungen Zuweisungen machen und dann substituieren:

```
> G_1 := subs(_Z1 = 1, _Z2 = 0, G(X)) mod 7;
```

$$G\_1 := 1$$

Das bringt offensichtlich nichts. Beim zweiten Versuch

```
> G_2 := subs(_Z1 = 0, _Z2 = 1, G(X)) mod 7;
```

$$G\_2 := X^5 + 3X^4 + 5X^3 + 3X^2 + 6X$$

haben wir mehr Glück und müssen nun für alle $i \in \mathbb{F}_7$ die größten gemeinsamen Teiler von $G\_2 - i$ und f berechnen:

```
> for i from 0 to 6 do Gcd(G_2-i, f) mod 7; od;
```

$$X^3 + 5X + 2$$
$$1$$
$$X^3 + 2X^2 + 6X + 3$$
$$1$$
$$1$$
$$1$$
$$1$$

Somit ist $f = (X^3 + 5X + 2)(X^3 + 2X^2 + 6X + 3)$ die Zerlegung von f in irreduzible Faktoren. Zur Vorsicht können wir das noch von Maple verifizieren lassen:

```
> expand((X^3+2*X^2+6*X+3)*(X^3+5*X+2)) mod 7;
```

$$X^6 + 2X^5 + 4X^4 + X^3 + 6X^2 + 6X + 6$$

Da $6 = -1$ in $\mathbb{F}_7$, ist das in der Tat unser Ausgangspolynom f.

§4: Faktorisierung über den ganzen Zahlen und über endlichen Körpern

Wie bei der Berechnung des ggT zweier Polynome wollen wir auch bei der Faktorisierung den Umweg über endliche Körper benutzen, um das Problem für Polynome über $\mathbb{Z}$ zu lösen. Allerdings kann es hier häufiger passieren, daß sich Ergebnisse über $\mathbb{F}_p$ deutlich unterscheiden von denen über Z:

Zunächst einmal muß ein quadratfreies Polynom aus $\mathbb{Z}[X]$ modulo p nicht quadratfrei bleiben: $f = (X + 10)(X - 20)$ etwa ist modulo zwei oder fünf gleich X^2 und modulo drei $(X + 1)^2$. Dieses Problem tritt allerdings nur bei endlich vielen Primzahlen auf und kann vermieden werden: Ist $f \in \mathbb{Z}[X]$ quadratfrei, seine Reduktion $f^{(p)} \in \mathbb{F}_p[X]$ aber nicht, so haben $f^{(p)}$ und seine Ableitung einen gemeinsamen Faktor, ihre Resultante verschwindet also. Da diese Resultante die Reduktion modulo p der Resultante von f und f' ist, bedeutet dies einfach, daß p ein Teiler der über $\mathbb{Z}$ berechneten Resultante ist, und das läßt sich leicht nachprüfen. Dazu müssen wir zwar eine Resultante berechnen, was wir im vorigen Kapitel aus Effizienzgründen vermieden hatten, aber wie wir bald sehen werden, ist das Problem der Faktorisierung deutlich komplexer als der EUKLIDische Algorithmus, so daß hier der Aufwand für die Resultantenberechnung nicht weiter ins Gewicht fällt.

Tatsächlich betrachtet man in der Algebra meist nicht die Resultante von f und f', sondern die sogenannte *Diskriminante*

$$D(f) = \frac{(-1)^{\frac{1}{2}d(d-1)}}{a_n} \operatorname{Res}_X(f, f') \quad \text{mit} \quad d = \deg f\,,$$

deren algebraische Eigenschaften etwas besser sind. Für praktische Rechnungen ist der Unterschied hier aber unbedeutend, denn wie man der SYLVESTER-Matrix von f und f' leicht ansieht, ist die Resultante eines nichtkonstanten Polynoms durch eine höhere Potenz des führenden Koeffizienten a_n teilbar als nur die erste; die Primteiler von Resultante und Diskriminante sind also dieselben.

Vermeidet man diese, bleibt f auch modulo p quadratfrei, jedoch können sich die Zerlegungen in irreduzible Faktoren in $\mathbb{Z}[X]$ und $\mathbb{F}_p[X]$ deutlich unterscheiden:

Betrachten wir dazu als erstes Beispiel das Polynom $X^2 + 1$ aus $\mathbb{Z}[X]$. Es ist irreduzibel, da eine Zerlegung die Form $(X - a)(X + a)$ haben müßte mit $a \in \mathbb{Z}$, und in $\mathbb{Z}$ gibt es kein Element a mit $a^2 = -1$.

Auch über dem Körper $\mathbb{F}_p$ muß eine eventuelle Faktorisierung die Form $(X - a)(X + a)$ haben mit $a^2 = -1$; wir müssen uns also überlegen, wann das der Fall ist. Die elementare Zahlentheorie sagt uns:

Lemma: Genau dann gibt es im endlichen Körper $\mathbb{F}_p$ ein Element a mit $a^2 = -1$, wenn $p = 2$ oder $p \equiv 1 \bmod 4$ ist.

Beweis: Für $p = 2$ ist natürlich $1^2 = 1 = -1$ die Lösung. Für ungerade $p \equiv 1 \bmod 4$ schreiben wir $p = 4k + 1$. Nach dem kleinen Satz von FERMAT und der dritten binomischen Formel ist für alle $x \in \mathbb{F}_p^\times$

$$x^{p-1} - 1 = x^{4k} - 1 = (x^{2k} + 1)(x^{2k} - 1) = 0\,,$$

das Polynom $X^{p-1} - 1$ hat somit $p - 1 = 4k$ Nullstellen und zerfällt daher über $\mathbb{F}_p$ in Linearfaktoren. Damit gilt dasselbe für die beiden Faktoren $X^{2k} \pm 1$; insbesondere gibt es also ein $x \in \mathbb{F}_p$ mit $x^{2k} + 1 = 0$. Für $a = x^k$ ist dann $a^2 = x^{2k} = -1$.

Ist $p \equiv 3 \bmod 4$ und $a^2 = -1$ für ein $a \in \mathbb{F}_p$, so ist $a^4 = 1$. Außerdem ist nach dem kleinen Satz von FERMAT $a^{p-1} = 1$. Wegen $p \equiv 3 \bmod 4$ ist ggT$(4, p-1) = 2$, die Zwei ist also als Linearkombination von 4 und $p - 1$ darstellbar. Damit ist auch $a^2 = 1$, im Widerspruch zu Annahme

$a^2 = -1$. Somit gibt es für $p \equiv 3 \bmod 4$ keine Elemente mit Quadrat -1 in $\mathbb{F}_p$.

■

Damit ist $X^2 + 1$ genau dann irreduzibel über $\mathbb{F}_p$, wenn $p \equiv 3 \bmod 4$; in allen anderen Fällen zerfällt das Polynom in zwei Linearfaktoren. Nach einem berühmten Satz von DIRICHLET über Primzahlen in arithmetischen Progressionen bleibt $X^2 + 1$ damit nur modulo der Hälfte aller Primzahlen irreduzibel; insbesondere gibt es also unendlich viele Primzahlen, modulo derer das Problem schlechte Reduktion hat.

Noch schlimmer ist es bei $X^4 + 1$: Auch dieses Polynom ist irreduzibel über $\mathbb{Z}$: Da seine Nullstellen $\frac{1}{2}\sqrt{2}(\pm 1 \pm i)$ nicht in $\mathbb{Z}$ liegen, gibt es keinen linearen Faktor, und wäre

$$\begin{aligned} X^4 + 1 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd \end{aligned}$$

eine Zerlegung in quadratische Faktoren, so zeigen die Koeffizienten von X^3 und der konstante Term, daß $c = -a$ und $b = d = \pm 1$ sein müßte. Die Produkte

$$(X^2 + aX + 1)(X^2 - aX + 1) = X^4 + (2 - a^2)X^2 + 1$$

und

$$(X^2 + aX - 1)(X^2 - aX - 1) = X^4 - (2 + a^2)X^2 + 1$$

zeigen aber, daß beides nur für $a^2 = \pm 2$ zu einer Faktorisierung führen könnte, was in $\mathbb{Z}$ nicht erfüllbar ist.

In den Körpern $\mathbb{F}_p$ dagegen kann es sehr wohl Elemente geben, deren Quadrat ± 2 ist, und dann zeigen die obigen Formeln, daß $X^4 + 1$ dort in ein Produkt zweier quadratischer Polynome zerlegt werden kann. Auch wenn es ein Element $a \in \mathbb{F}_p$ gibt mit $a^2 = -1$, können wir $X^4 + 1$ als Produkt schreiben, nämlich genau wie oben im Falle $X^2 + 1$ als

$$X^4 + 1 = (X^2 + a)(X^2 - a)\,.$$

Somit ist $X^4 + 1$ über dem Körper $\mathbb{F}_p$ zumindest dann reduzibel, wenn dort wenigstens eines der drei Elemente -1 und ± 2 ein Quadrat ist. Um

zu sehen, daß $X^4 + 1$ über jedem dieser Körper zerfällt, müssen wir uns also überlegen, daß in keinem der Körper $\mathbb{F}_p$ alle drei Elemente *keine* Quadrate sind. Da $-2 = -1 \cdot 2$ ist, folgt dies aus

Lemma: Sind im Körper $\mathbb{F}_p$ die beiden Elemente a, b nicht als Quadrate darstellbar, so ist ab ein Quadrat.

Beweis: Für $p = 2$ ist jedes Element ein Quadrat und nicht zu beweisen.

Ansonsten betrachten wir die Abbildung $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, die jedes von Null verschiedene Element von $\mathbb{F}_p$ auf sein Quadrat abbildet. Für zwei Elemente $x, y \in \mathbb{F}_p^\times$ ist offensichtlich $\varphi(x) = \varphi(y)$ genau dann, wenn $x = \pm y$ ist. Daher besteht das Bild von φ aus $\frac{1}{2}(p-1)$ Elementen, und genau die Hälfte der Elemente von $\mathbb{F}_p^\times$ sind Quadrate. Ist a keines, so ist auch ax^2 für kein $x \in \mathbb{F}_p^\times$ ein Quadrat, denn wäre $ax^2 = y^2$, sonst wäre auch $a = y^2x^{-2} = (y/x)^2$ ein Quadrat.

Da es $\frac{1}{2}(p-1)$ Quadrate und genauso viele Nichtquadrate gibt, läßt sich somit jedes Nichtquadrat b als $b = ax^2$ schreiben mit einem geeigneten Element $x \in \mathbb{F}_p$. Damit ist $ab = a \cdot ax^2 = (ax)^2$ ein Quadrat. ∎

Die Situation ist also deutlich schlechter als im Fall des EUKLIDischen Algorithmus, wo wir sicher sein konnten, daß es höchstens endlich viele Primzahlen gibt, modulo derer das Problem schlechte Reduktion hat: Das Problem der Faktorisierung des Polynoms $X^4 + 1$ hat, wie wir gerade gesehen haben, modulo *jeder* Primzahl schlechte Reduktion, und auch bei $X^2 + 1$ gibt es unendlich viele solche Primzahlen.

Aus diesem Grund empfiehlt sich für die Faktorisierung definitiv kein Ansatz mit dem chinesischen Restesatz: Wenn wir die Faktorisierung modulo verschiedener Primzahlen durchführen, können wir praktisch sicher sein, daß es darunter auch schlechte gibt, und meist werden auch die Ergebnisse modulo verschiedener Primzahlen entweder nicht zusammenpassen, oder aber wir haben mehrere Faktoren gleichen Grades, von denen wir nicht wissen, welche wir via chinesischen Restesatz miteinander kombinieren sollen. Es hat daher keinen Zweck, zufällig Primzahlen

zu wählen und dann eine Rückfallstrategie für schlechte Primzahlen zu entwickeln.

Der Weg über endliche Körper verfolgt daher im Falle der Faktorisierung eine andere Strategie als beim EUKLIDischen Algorithmus: Wir beschränken uns auf eine einzige Primzahl – unabhängig davon, ob diese nun gut oder schlecht dafür geeignet ist.

Wir kennen bereits aus dem vorigen Kapitel Schranken für die Koeffizienten der Faktoren eines Polynoms; wir könnten also eine Primzahl wählen, die größer ist als das Doppelte dieser Schranke und modulo dieser rechnen.

Der Nachteil dabei ist, daß das Rechnen modulo einer Primzahl p umso teurer wird, je größer die Primzahl ist: Die Kosten für Multiplikationen wachsen quadratisch mit der Stellenzahl von p, die Kosten für Divisionen modulo p nach dem erweiterten EUKLIDischen Algorithmus können sogar bis zu kubisch ansteigen.

Die Alternative bietet ein für völlig andere Zwecke bewiesenes Resultat des deutschen Zahlentheoretikers HENSEL, das es erlaubt eine Faktorisierung modulo p fortzusetzen zu einer Faktorisierung modulo jeder beliebiger p-Potenz und, was HENSEL wirklich interessierte, zu den sogenannten p-adischen Zahlen, mit denen wir uns in Rahmen dieser Vorlesung allerdings nicht beschäftigen werden.

§5: Das Henselsche Lemma

Lemma: f, g, h seien Polynome aus $\mathbb{Z}[X]$ derart, daß $f \equiv gh \bmod p$; dabei seien $g \bmod p$ und $h \bmod p$ teilerfremd über $\mathbb{F}_p[X]$. Dann gibt es für jede natürliche Zahl n Polynome g_n, h_n derart, daß

$$g_n \equiv g \bmod p, \quad h_n \equiv h \bmod p \quad \text{und} \quad f \equiv g_n h_n \bmod p^n .$$

Beweis durch vollständige Induktion: Der Fall $n = 1$ ist die Voraussetzung des Lemmas. Ist das Lemma für ein n bewiesen, machen wir den Ansatz

$$g_{n+1} = g_n + p^n g^* \quad \text{und} \quad h_{n+1} = h_n + p^n h^* .$$

Nach Induktionsvoraussetzung ist $f \equiv g_n h_n \bmod p^n$, die Differenz $f - g_n h_n$ ist also durch p^n teilbar und es gibt ein Polynom $f^* \in \mathbb{Z}[X]$, so daß $f = g_n h_n + p^n f^*$ ist. Wir möchten, daß

$$f \equiv (g_n + p^n g^*)(h_n + p^n h^*) = g_n h_n + p^n (g_n h^* + h_n g^*) + p^{2n} \bmod p^{n+1}$$

wird. Da $2n \geq n+1$ ist, können wir den letzten Summanden vergessen; zu lösen ist also die Kongruenz

$$f \equiv g_n h_n + p^n f^* = g_n h_n + p^n (g_n h^* + h_n g^*) \bmod p^{n+1}$$

oder

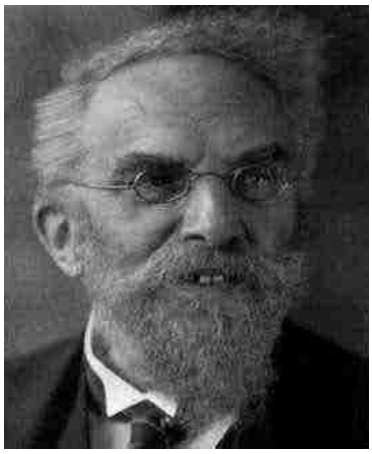
$$p^n f^* \equiv p^n (g_n h^* + h_n g^*) \bmod p^{n-1} .$$

Division durch p^n macht daraus

$$f^* \equiv g_n h^* + h_n g^* \bmod p \quad \text{oder} \quad f^* \equiv g h^* + h g^* \bmod p ,$$

denn $g_n \equiv g \bmod p$ und $h_n \equiv h \bmod p$. Die letztere Kongruenz können wir als Gleichung in $\mathbb{F}_p[X]$ auffassen und dort lösen, indem wir den erweiterten EUKLIDischen Algorithmus auf die Polynome $g \bmod p$ und $h \bmod p$ aus $\mathbb{F}_p[X]$ anwenden: Da diese nach Voraussetzung teilerfremd sind, können wir ihren ggT Eins und damit auch jedes andere Polynom über $\mathbb{F}_p$ als Linearkombination der beiden darstellen. Da der Grad von f die Summe der Grade von g und h ist und f^* höchstens denselben Grad wie f hat, können wir dann auch eine Darstellung $f^* = g h^* + h g^*$ in $\mathbb{F}_p[X]$ finden mit $\deg g^* \leq \deg g$ und $\deg h^* \leq \deg h$. Ersetzen wir g^* und h^* durch irgendwelche Repräsentantanten gleichen Grades aus $\mathbb{Z}[X]$, erfüllen $g_{n+1} = g_n + p^n g^*$ und $h_{n+1} = h_n + p^n h^*$ die Kongruenz $f \equiv g_n h_n$ modulo p^{n+1}.

■



KURT HENSEL wurde 1861 im damaligen Königsberg geboren; als er neun Jahre alt war, zog die Familie nach Berlin. Er studierte dort und in Bonn; 1884 promovierte er in Berlin bei KRONECKER, 1886 folgte die Habilitation. Er blieb bis 1901 als Privatdozent in Berlin; 1901 bekam er einen Lehrstuhl in Marburg, den er bis zu seiner Emeritierung 1930 innehatte. Er starb 1941 in Marburg. Seine Arbeiten drehen sich hauptsächlich um die Zahlentheorie und die eng damit verwandte Arithmetik von Funktionenkörpern. Bekannt wurde er vor allem durch die Einführung der p-adischen Zahlen. Er ist Autor dreier Lehrbücher.

§6: Der Algorithmus von Zassenhaus

Die Werkzeuge aus den vorigen Paragraphen erlauben uns, gemeinsam eingesetzt, nun die Faktorisierung von Polynomen f aus $\mathbb{Z}[X]$ oder $\mathbb{Q}[X]$. Das einzige, was wir noch nicht explizit formuliert haben, ist eine Schranke für die Koeffizienten eines Faktors. Aus Kapitel III, §4, wissen wir, daß für einen Teiler $g \in \mathbb{C}[z]$ eines Polynoms $f \in \mathbb{C}[z]$ gilt:

$$H(g) \leq \binom{e}{[e/2]} \left|\frac{b_e}{a_d}\right| \|f\|_2 \ ,$$

wobei e den Grad von g bezeichnet und a_d, b_e die führenden Koeffizienten von f und g. Für $g, f \in \mathbb{Z}[X]$ muß b_e ein Teiler von a_d sein, der Quotient b_e/a_d hat also höchstens den Betrag eins. Der Grad e eines Teilers kann höchstens gleich dem Grad d von f sein, also ist für jeden Teiler $g \in \mathbb{Z}[X]$ von $f \in \mathbb{Z}[X]$

$$H(g) \leq \binom{d}{[d/2]} \|f\|_2 \ .$$

Nach ZASSENHAUS gehen wir zur Faktorisierung eines Polynoms f aus $\mathbb{Z}[X]$ oder $\mathbb{Q}[X]$ nun folgendermaßen vor:

Erster Schritt: Berechne die quadratfreie Zerlegung von f und ersetze die quadratfreien Faktoren durch ihre primitiven Anteile g_i. Dann gibt es eine Konstante c, so daß $f = c\prod_{i=1}^{r} g_i^{\,i}$ ist. Falls f in $\mathbb{Z}[X]$ liegt, ist c eine ganze Zahl. Für eine Faktorisierung in $\mathbb{Z}[X]$ muß auch c in seine Primfaktoren zerlegt werden; für eine Faktorisierung in $\mathbb{Q}[X]$ kann c als Einheit aus $\mathbb{Q}^\times$ stehen bleiben. Die folgenden Schritte werden einzeln auf jedes der g_i angewandt, danach werden die Ergebnisse zusammengesetzt zur Faktorisierung von f. Für das Folgende sei g eines der g_i.

Zweiter Schritt: Wir setzen $L = \binom{\deg g}{[\frac{1}{2}\deg g]} \|g\|_2$ und $M = 2L + 1$. Dann wählen wir eine Primzahl p, die weder den führenden Koeffizienten noch die Diskriminante von g teilt. Damit ist auch g mod p quadratfrei.

Dritter Schritt: Wir faktorisieren g mod p nach BERLEKAMP in $\mathbb{F}_p[X]$.

Vierter Schritt: Die Faktorisierung wird nach dem HENSELschen Lemma hochgehoben zu einer Faktorisierung modulo p^n für eine natürliche Zahl n mit $p^n \geq M$.

Fünfter Schritt: Setze $m = 1$ und teste für jeden der gefundenen Faktoren, ob er ein Teiler von g ist. Falls ja, kommt er in die Liste $\mathcal{L}_1$ der Faktoren von g, andernfalls in eine Liste $\mathcal{L}_2$.

Sechster Schritt: Falls die Liste $\mathcal{L}_2$ keine Einträge hat, endet der Algorithmus und g ist das Produkt der Faktoren aus $\mathcal{L}_1$. Andernfalls setzen wir $m = m + 1$ und testen für jedes Produkt aus m verschiedenen Polynomen aus $\mathcal{L}_2$, ob ihr Produkt modulo p^n (mit Koeffizienten vom Betrag höchstens L) ein Teiler von g ist. Falls ja, entfernen wir die m Faktoren aus $\mathcal{L}_2$ und fügen ihr Produkt in die Liste $\mathcal{L}_1$ ein. Wiederhole diesen Schritt.

Auch wenn der sechste Schritt wie eine Endlosschleife aussieht, endet der Algorithmus natürlich nach endlich vielen Schritten, denn $\mathcal{L}_2$ ist eine endliche Liste und spätestens das Produkt aller Elemente aus $\mathcal{L}_2$ muß Teiler von g sein, da sein Produkt mit dem Produkt aller Elemente von $\mathcal{L}_1$ gleich g ist. Tatsächlich kann man schon abbrechen, wenn die betrachteten Faktoren einen größeren Grad haben als $\frac{1}{2} \deg g$, denn falls f reduzibel ist, gibt es einen Faktor, der höchstens diesen Grad hat.

HANS JULIUS ZASSENHAUS wurde 1912 in Koblenz geboren, ging aber in Hamburg zur Schule und zur Universität. Er promovierte 1934 über Permutationsgruppen; seine Habilitation 1940 handelte von LIE-Ringen in positiver Charakteristik. Da er nicht der NSdAP beitreten wollte, arbeitete er während des Krieges als Meteorologe bei der Marine; nach dem Krieg war er von 1949 bis 1959 Professor in Montréal, dann fünf Jahre lang in Notre Dame und schließlich bis zu seiner Emeritierung an der Ohio State University in Columbus. Dort starb er 1991. Bekannt ist er vor allem für seine Arbeiten zur Gruppentheorie und zur algorithmischen Zahlentheorie.

§7: Swinnerton-Dyer Polynome

Der potentiell problematischste Schritt des obigen Algorithmus ist der sechste: Vor allem, wenn wir auch Produkte von mehr als zwei Faktoren betrachten müssen, kann dieser sehr teuer werden. Ein Beispiel dafür bieten die sogenannten SWINNERTON-DYER-Polynome: Zu n paarweise

verschiedenen Primzahlen $p_1, \ldots, p_n$ gibt es genau ein Polynom f vom Grad 2^n mit führendem Koeffizienten eins, dessen Nullstellen genau die 2^n Zahlen

$$\pm\sqrt{p_1} \pm \sqrt{p_2} \pm \cdots \pm \sqrt{p_n}$$

sind. Dieses Polynom hat folgende Eigenschaften:

1. Es hat ganzzahlige Koeffizienten.
2. Es ist irreduzibel über $\mathbb{Z}$.
3. Modulo jeder Primzahl p zerfällt es in Faktoren vom Grad höchstens zwei.

Beweisen läßt sich das am besten mit Methoden der abstrakten Algebra, wie sie in jeder Vorlesung *Algebra I* präsentiert werden. Da hier keine Algebra I vorausgesetzt wird, sei nur kurz die Idee angedeutet: Um den kleinsten Teilkörper von $\mathbb{C}$ zu konstruieren, in dem alle Nullstellen von f liegen, können wir folgendermaßen vorgehen: Wir konstruieren als erstes einen Körper K_1, der $\sqrt{p_1}$ enthält. Das ist einfach: Der Vektorraum $K_1 = \mathbb{Q} \oplus \mathbb{Q}\sqrt{p_1}$ ist offensichtlich so ein Körper. Als nächstes konstruieren wir einen Körper K_2, der sowohl K_1 als auch $\sqrt{p_2}$ enthält. Dazu können wir genauso vorgehen: Wir betrachten einfach den zweidimensionalen K_1-Vektorraum $K_2 = K_1 \oplus K_1\sqrt{p_2}$. Als Vektorraum über $\mathbb{Q}$ ist K_2 natürlich vierdimensional. Weiter geht es mit $K_3 = K_2 \oplus K_2\sqrt{p_3}$ *usw.* bis $K_n = K_{n-1} \oplus K_{n-1}\sqrt{p_n}$. Als $\mathbb{Q}$-Vektorraum hat dieser Körper die Dimension 2^n.

Offensichtlich ist K_n der kleinste Erweiterungskörper von $\mathbb{Q}$, der alle Quadratwurzeln der p_i enthält. Er enthält natürlich auch alle der oben postulierten Nullstellen, und umgekehrt muß ein Körper, der diese enthält, auch alle $\sqrt{p_i}$ enthalten, denn $2\sqrt{p_i}$ läßt sich als Summe zweier solcher Nullstellen schreiben. K_n ist also auch der kleinste Körper, der alle diese Nullstellen enthält, der sogenannte *Zerfällungskörper* des Polynoms.

In der Algebra ordnet man einem solchen Zerfällungskörper die Gruppe seiner Automorphismen zu, die sogenannte GALOIS-Gruppe. Ihre Ordnung ist die Vektorraumdimension des Körpers, hier also 2^n. Da sie offensichtlich die Abbildungen $\sqrt{p_i} \mapsto -\sqrt{p_i}$ enthält, ist sie die von diesen Automorphismen erzeugte elementarabelsche Gruppe. Sie läßt

die Nullstellenmenge von f als ganzes betrachtet fest, also nach dem Wurzelsatz von VIÈTE auch die Koeffizienten. Somit hat f rationale Koeffizienten, und da alle Nullstellen ganz sind (im Sinne der algebraischen Zahlentheorie), liegen diese Koeffizienten sogar in $\mathbb{Z}$. Außerdem operiert die GALOIS-Gruppe transitiv auf der Nullstellenmenge von f; also ist f irreduzibel in $\mathbb{Q}[X]$ und damit auch $\mathbb{Z}[X]$.

Betrachten wir f modulo einer Primzahl p, so können wir die analoge Konstruktion durchführen ausgehend vom Körper $\mathbb{F}_p$ anstelle von $\mathbb{Q}$. Während wir aber im Falle der rationalen Zahlen sicher sein konnten, daß $\sqrt{p_i}$ nicht bereits im Körper K_{i-1} liegt, ist dies hier nicht mehr der Fall: Für ungerades p gibt es $\frac{1}{2}(p+1)$ Quadrate in $\mathbb{F}_p$; dazu könnte auch p_i gehören. Falls nicht, ist $K = \mathbb{F}_p \oplus \mathbb{F}_p\sqrt{p_i}$ ein Körper mit p^2 Elementen. Wie man in der Algebra lernt, gibt es aber bis auf Isomorphie nur einen solchen Körper; K enthält daher die Quadratwurzeln *aller* Elemente von $\mathbb{F}_p$ und somit *alle* Nullstellen von f mod p. Spätestens über K zerfällt f mod p also in Linearfaktoren, und da alle Koeffizienten in $\mathbb{F}_p$ liegen, lassen sich je zwei Linearfaktoren, die nicht in $\mathbb{F}_p[X]$ liegen, zu einem quadratischen Faktor aus $\mathbb{F}_p[X]$ zusammenfassen. Somit hat f mod p höchstens quadratische Faktoren.

(Für eine ausführlichere und etwas elementarere Darstellung siehe etwa §6.3.2 in MICHAEL KAPLAN: Computeralgebra, *Springer,* 2005.)

Falls wir f nach dem oben angegebenen Algorithmus faktorisieren, erhalten wir daher modulo *jeder* Primzahl p mindestens 2^{n-1} Faktoren. Diese lassen sich über das HENSELsche Lemma liften zu Faktoren über $\mathbb{Z}$, und wir müssen alle Kombinationen aus mindestens 2^{n-2} Faktoren ausprobieren bis wir erkennen, daß f irreduzibel ist, also mindestens $2^{2^{n-2}}$ Möglichkeiten. Für $n = 10$ etwa ist f ein Polynom vom Grad 1024, dessen Manipulation durchaus im Rahmen der Möglichkeiten eines heutigen Computeralgebrasystems liegt. Das Ausprobieren von $2^{256} \approx 10^{77}$ Möglichkeiten überfordert aber selbst heutige Supercomputer oder parallel arbeitende Cluster aus Millionen von Computern ganz gewaltig: Der heutige Sicherheitsstandard der Kryptographie geht davon aus, daß niemand in der Lage ist, 2^{128} (oder sogar nur 2^{100}) Rechenoperationen in realistischer Zeit (d.h. wenigen Jahren) auszuführen.