Kapitel 2
Der Euklidische Algorithmus

Angenommen, wir suchen die gemeinsamen Nullstellen zweier Polynome in derselben Veränderlichen x. Dann können wir natürlich versuchen, zunächst die Nullstellen eines der beiden Polynome zu finden und dann durch Einsetzen zu überprüfen, welche davon auch Nullstellen des zweiten sind. Im Extremfall gibt es keinerlei gemeinsame Nullstellen, und wir müssen trotzdem zunächst alle Nullstellen eines Polynoms von möglicherweise hohem Grad berechnen.

Die bessere Alternative besteht darin, sich zunächst zu überlegen, daß es zu zwei Polynomen über einem Körper (und auch noch unter deutlich schwächeren Voraussetzungen an die Koeffizienten) stets einen größten gemeinsamen Teiler gibt, dessen Nullstellen genau die gemeinsamen Nullstellen der beiden Polynome sind. Wenn sich dieser größte gemeinsame Teiler effizient berechnen läßt, müssen wir nur noch seine Nullstellen bestimmen, was aus Gradgründen meist erheblich einfacher sein dürfte.

Die Existenz des größten gemeinsamen Teilers zweier Polynome beweist der EUKLIDische Algorithmus, der gleichzeitig auch zu dessen Berechnung eingesetzt werden kann. Seine Anwendung auf ein Polynom und dessen Ableitung wird uns auf die sogenannte quadratfreie Zerlegung eines Polynoms führen und damit auf einen ersten Schritt zur Zerlegung eines Polynoms in irreduzible Faktoren.

Wir werden allerdings sehen, daß der EUKLIDische Algorithmus in seiner einfachsten Form zu sehr unübersichtlichen und schwer handhabbaren Zwischenergebnissen führen kann. Durch geeignete Modifikationen läßt sich seine Effizienz ganz deutlich steigern. Diese Modifikationen führen

uns allerdings in andere Zahlbereiche; um hier nicht wieder alles neu beweisen zu müssen, wollen wir uns daher nicht darauf beschränken, den EUKLIDischen Algorithmus für Polynome mit rationalen oder reellen Koeffizienten zu betrachten, sondern gleich am Anfang eine algebraische Struktur definieren, die alles bietet, was für den EUKLIDischen Algorithmus benötigt wird, den EUKLIDischen Ring. Wenn wir dann später größte gemeinsame Teiler anderer Objekte suchen, müssen wir uns nur noch überlegen, ob wir uns in einem EUKLIDischen Ring befinden; falls ja, können wir alle Konstruktionen und Sätze einfach übernehmen.

§ 1: Euklidische Ringe

Wie wir im nächsten Abschnitt sehen werden, beruht der EUKLIDische Algorithmus wesentlich auf der Division mit Rest. Ein EUKLIDischer Ring soll daher definiert werden als eine algebraische Struktur, in der Addition, Subtraktion, Multiplikation und Division mit Rest durchgeführt werden können und den „gewohnten“ Regeln genügen. Konkret heißt das folgendes:

Definition: *a)* Ein Ring ist eine Menge R zusammen mit zwei Rechenoperationen „+“ und „·“ von $R \times R$ nach R, so daß gilt:

1.) R bildet bezüglich „+“ eine abelsche Gruppe, d.h. für die Addition gilt das Kommutativgesetz $f + g = g + f$ sowie das Assoziativgesetz $(f + g) + h = f + (g + h)$ für alle $f, g, h \in \mathbb{R}$, es gibt ein Element $0 \in R$, so daß $0 + f = f + 0 = f$ für alle $f \in R$, und zu jedem $f \in R$ gibt es ein Element $-f \in R$, so daß $f + (-f) = 0$ ist.

2.) Die Verknüpfung „·“: $R \times R \to R$ erfüllt das Assoziativgesetz $f(gh) = (fg)h$, und es gibt ein Element $1 \in R$, so daß $1f = f1 = f$.

3.) „+“ und „·“ erfüllen die Distributivgesetze $f(g + h) = fg + fh$ und $(f + g)h = fh + gh$.

b) Ein Ring heißt *kommutativ*, falls zusätzlich noch das Kommutativgesetz $fg = gf$ der Multiplikation gilt.
c) Ein Ring heißt *nullteilerfrei* wenn gilt: Falls ein Produkt $fg = 0$ verschwindet, muß mindestens einer der beiden Faktoren f, g gleich Null sein. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich*.

Natürlich ist jeder Körper ein Ring; für einen Körper werden schließlich genau dieselben Eigenschaften gefordert und zusätzlich auch noch die Kommutativität der Multiplikation sowie die Existenz multiplikativer Inverser. Ein Körper ist somit insbesondere auch ein Integritätsbereich.

Das bekannteste Beispiel eines Rings, der kein Körper ist, sind die ganzen Zahlen; auch sie bilden einen Integritätsbereich.

Auch die Menge

$$k[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; n \in \mathbb{N}_0, a_i \in k \right\}$$

aller Polynome mit Koeffizienten aus einem Körper k ist ein Integritätsbereich; ersetzt man den Körper k durch einen beliebigen kommutativen Ring R, ist $R[x]$ immerhin noch ein Ring. Man überlegt sich leicht, daß $R[x]$ genau dann ein Integritätsbereich ist, wenn auch R einer ist.

Als Beispiel eines nichtkommutativen Rings können wir die Menge aller $n \times n$-Matrizen über einem Körper betrachten; dieser Ring hat auch Nullteiler, denn beispielsweise ist

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

obwohl keiner der beiden Faktoren die Nullmatrix ist.

Was uns nun noch fehlt, ist eine Division mit Rest. Für Zahlen a, b, q, r aus $\mathbb{N}_0$ ist die Aussage

$$a : b = q \text{ Rest } r$$

äquivalent zu den beiden Bedingungen

$$a = bq + r \quad \text{und} \quad 0 \le r < b\,.$$

Die erste dieser Bedingungen können wir in einem beliebigen Ring hinschreiben, eine Kleinerrelation haben wir dort allerdings nicht. Andererseits brauchen wir aber etwas nach Art der zweiten Bedingung: Falls der Divisionsrest nicht in irgendeiner Weise kleiner als der Divisor sein muß, könnten wir einfach *immer* sagen $a : b = 0$ Rest a, was nicht sonderlich viel nützt.

Wir fordern deshalb die Existenz einer Funktion $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, die im Falle eines von Null verschiedenen Divisionsrests für den Rest einen kleineren Wert annimmt als für den Divisor:

Definition: Ein EUKLIDischer Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, so daß gilt: Ist $f = gh$, so ist $\nu(f) \ge \max\big(\nu(g), \nu(h)\big)$, und zu je zwei Elementen $f, g \in R$ gibt es Elemente $q, r \in R$ mit

$$f = qq + r \quad \text{und} \quad r = 0 \text{ oder } \nu(r) < \nu(g)\,.$$

Wir schreiben auch $f : g = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von f durch g.

Standardbeispiel sind auch hier wieder die ganzen Zahlen, wo wir als ν einfach die Betragsfunktion nehmen können. Quotient und Divisionsrest sind durch die Forderung $\nu(r) < \nu(y)$ allerdings nicht eindeutig festgelegt, beispielsweise ist im Sinne dieser Definition

$$11 : 3 = 3 \text{ Rest } 2 \quad \text{und} \quad 11 : 3 = 4 \text{ Rest } -1\,.$$

Die Definition des EUKLIDischen Rings verlangt nur, daß es *mindestens* eine Darstellung gibt; Eindeutigkeit ist nicht gefordert.

Das für uns im Augenblick wichtigste Beispiel ist der Polynomring $k[x]$ über einem Körper k; hier zeigt die bekannte Polynomdivision mit Rest, daß die Bedingungen erfüllt sind bezüglich der Abbildung

$$\nu\colon \begin{cases} k[x] \setminus \{0\} \to \mathbb{N}_0 \\ f \mapsto \text{Grad } f \end{cases}.$$

Hier ist es allerdings wichtig, daß k ein Körper ist: Bei der Polynomdivision mit Rest müssen wir schließlich die führenden Koeffizienten durcheinander dividieren, und das wäre etwa im Polynomring $\mathbb{Z}[x]$ nicht möglich.

Dies beweist freilich nicht, daß $\mathbb{Z}[x]$ *kein* EUKLIDischer Ring wäre, denn in der Definition war ja nur gefordert, daß es für *irgendeine* Funktion ν *irgendein* Divisionsverfahren gibt; dessen Nichtexistenz ist sehr schwer zu zeigen – es sei denn, eine der im folgenden hergeleiteten Eigenschaften eines EUKLIDischen Rings ist nicht erfüllt. Bei $\mathbb{Z}[x]$ ist dies, wie wir

bald sehen werden, bei der linearen Kombinierbarkeit des ggT in der Tat der Fall, so daß $\mathbb{Z}[x]$ kein EUKLIDischer Ring sein kann.

Ein weiteres bekanntes Beispiel eines EUKLIDischen Rings ist der Ring der GAUSSschen Zahlen, d.h. die Menge aller komplexer Zahlen mit ganzzahligem Real- und Imaginärteil; hier können wir $\nu(x+iy) = x^2+y^2$ setzen. Da dieser Ring hier keine Rolle spielen wird, sei auf einen Beweis verzichtet.

§ 2: Der größte gemeinsame Teiler

Bevor wir uns mit der Berechnung des größten gemeinsamen Teilers zweier Elemente eines EUKLIDischen Rings beschäftigen, müssen wir zunächst definieren, was das sein soll. Da es bei der Division durch einen Nullteiler keinen eindeutigen Quotienten geben kann, beschränken wir uns auf Integritätsbereiche.

Definition: R sei ein Integritätsbereich.
a) Ein Element $h \in R$ heißt Teiler von $f \in R$, in Zeichen $h|f$, wenn es ein $q \in R$ gibt, so daß $f = qh$ ist.
b) $h \in R$ heißt *größter gemeinsamer Teiler* (kurz ggT) der beiden Elemente f und g aus R, wenn h Teiler von f und von g ist und wenn für jeden anderen gemeinsamen Teiler r von f und g gilt: $r|h$.
c) Zwei Elemente $f, g \in R$ heißen *assoziiert*, wenn f Teiler von g und g Teiler von f ist.
d) Ein Element $u \in R$ heißt *Einheit*, falls es ein $v \in R$ gibt mit $uv = 1$. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$.

In einem Körper ist natürlich jedes von null verschiedene Element Teiler eines jeden anderen Elements und damit auch eine Einheit; in $\mathbb{Z}$ dagegen sind ± 1 die beiden einzigen Einheiten, und zwei ganze Zahlen sind genau dann assoziiert, wenn sie sich höchstens im Vorzeichen unterscheiden.

Man beachte, daß wir beim größten gemeinsamen Teiler die „Größe“ über Teilbarkeit definieren; von daher ist außer 2 auch -2 ein größter gemeinsamer Teiler von 8 und 10. Insbesondere ist „der“ größte gemeinsame Teiler also im allgemeinen nicht eindeutig bestimmt, was uns

bei seiner Berechnung in Polynomringen noch einiges an Problemen schaffen wird.

In einem Polynomring über einem Integritätsbereich ist der Grad des Produkts zweier Polynome gleich der Summe der Grade der Faktoren; da das konstante Polynom eins Grad null hat, muß daher jede Einheit Grad null haben; die Einheiten von $\mathbb{R}[x]$ sind also genau die Einheiten von R. Speziell für Polynomringe über Körpern sind dies genau die von null verschiedenen Konstanten.

Damit wissen wir auch, wann zwei Polynome assoziiert sind:

Lemma: Zwei von null verschiedene Elemente f, g eines Integritätsbereichs sind genau dann assoziiert, wenn es eine Einheit u gibt, so daß $f = ug$ ist.

Beweis: Eine Einheit $u \in R$ hat nach Definition ein Inverses $u^{-1} \in R$, und aus $f = ug$ folgt $g = u^{-1}f$. Somit ist f Teiler von g und g Teiler von f; die beiden Elemente sind also assoziiert.

Sind umgekehrt $f, g \in R \setminus \{0\}$ assoziiert, so gibt es Elemente $u, v \in R$ derart, daß $g = uf$ und $f = vg$ ist. Damit ist $g = uf = uvg$ und $f = vg = vuf$, also $(1 - uv)g = 0$ und $(1 - vu)f = 0$. Da wir in einem Integritätsbereich sind und f, g nicht verschwinden, muß somit $uv = vu = 1$ sein, d.h. u und v sind Einheiten. ∎

Damit sind also zwei Polynome über einem Körper genau dann assoziiert, wenn sie sich nur um eine von null verschiedene multiplikative Konstante unterscheiden. Nur bis auf eine solche Konstante können wir auch den größten gemeinsamen Teiler zweier Polynome bestimmen, denn allgemein gilt:

Lemma: Der größte gemeinsame Teiler zweier Polynome ist bis bis auf Assoziiertheit eindeutig. Sind also h und $\tilde{h}$ zwei größte gemeinsame Teiler der beiden Elemente f und g, so sind h und $\tilde{h}$ assoziiert; ist umgekehrt h ein größter gemeinsamer Teiler von f und g und ist $\tilde{h}$ assoziiert zu h, so ist auch $\tilde{h}$ ein größter gemeinsamer Teiler von f und g.

Beweis: Sind h und $\tilde{h}$ größte gemeinsame Teiler, so sind sie insbesondere gemeinsame Teiler und damit Teiler eines jeden größte gemeinsamen Teilers. Somit müssen h und $\tilde{h}$ einander teilen, sind also assoziiert. Ist h ein größter gemeinsamer Teiler und $\tilde{h}$ assoziiert zu h, so teilt $\tilde{h}$ jedes Vielfache von h, ist also auch ein gemeinsamer Teiler, und da h jeden gemeinsamen Teiler teilt, gilt dasselbe auch für $\tilde{h}$. Somit ist auch $\tilde{h}$ ein größter gemeinsamer Teiler.

■

§3: Berechnung des größten gemeinsamen Teilers

Hier kommen wir endlich zum EUKLIDischen Algorithmus.

Bei EUKLID, in Proposition 2 des siebten Buchs seiner *Elemente*, wird er so beschrieben (nach der Übersetzung von CLEMENS THAER in Oswalds Klassiker der exakten Wissenschaften, Band 235):

> *Zu zwei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß zu finden.*
>
> Die zwei gegebenen Zahlen, die nicht prim gegeneinander sind, seien AB, ΓΔ. Man soll das größte gemeinsame Maß von AB, ΓΔ finden.
>
> A B
>
> Γ Δ
>
> Wenn ΓΔ hier AB mißt – sich selbst mißt es auch – dann ist ΓΔ gemeinsames Maß von ΓΔ, AB. Und es ist klar, daß es auch das größte ist, denn keine Zahl größer ΓΔ kann ΓΔ messen.
>
> Wenn ΓΔ aber AB nicht mißt, und man nimmt bei AB, ΓΔ abwechselnd immer das kleinere vom größeren weg, dann muß (schließlich) eine Zahl übrig bleiben, die die vorangehende mißt. Die Einheit kann nämlich nicht übrig bleiben; sonst müßten AB, ΓΔ gegeneinander prim sein, gegen die Voraussetzung. Also muß eine Zahl übrig bleiben, die die vorangehende mißt. ΓΔ lasse, indem es BE mißt, EA, kleiner als sich selbst übrig; und EA lasse, indem es ΔZ mißt, ZΓ, kleiner als sich selbst übrig; und ΓZ messe AE.
>
> A E B
>
> Γ Z Δ
>
> H
>
> Da Γ*Z* AE mißt und AE ΔZ, muß ΓZ auch ΔZ messen; es mißt aber auch sich selbst, muß also auch das Ganze ΓΔ messen. ΓΔ mißt aber BE; also mißt ΓZ auch BE; es mißt aber auch EA, muß also auch das Ganze BA messen. Und es mißt auch ΓΔ; ΓZ mißt also AB und ΓΔ; also ist ΓZ gemeinsames Maß von AB, ΓΔ. Ich behaupte, daß es auch das größte ist. Wäre nämlich ΓZ nicht das größte gemeinsame Maß von AB, ΓΔ, so müßte irgendeine Zahl größer ΓZ die Zahlen AB und ΓΔ messen. Dies geschehe; die Zahl sei H. Da H dann ΓΔ mäße und ΓΔ BE mißt, mäße H auch BE; es soll aber auch das Ganze BA messen, müßte also auch den Rest AE messen. AE mißt aber ΔZ; also müßte H auch ΔZ messen; es soll aber auch das Ganze ΔΓ messen, müßte also auch den Rest ΓZ messen, als größere Zahl die kleinere; dies ist unmöglich. Also kann keine Zahl größer ΓZ die Zahlen AB und ΓΔ messen; ΓZ ist also das größte gemeinsame Maß von AB, ΓΔ; dies hatte man beweisen sollen.

Es ist nicht ganz sicher, ob EUKLID wirklich gelebt hat; das nebenstehende Bild aus dem 18. Jahrhundert ist mit Sicherheit reine Phantasie. EUKLID ist vor allem bekannt als Autor der *Elemente*, in denen er u.a. die Geometrie seiner Zeit systematisch darstellte und (in gewisser Weise) auf wenige Definitionen sowie die berühmten fünf Postulate zurückführte. Diese Elemente entstanden um 300 v. Chr. und waren zwar nicht der erste, aber doch der erfolgreichste Versuch einer solchen Zusammenfassung. EUKLID arbeitete wohl am Museion in Alexandrien; außer den Elementen schrieb er noch ein Buch über Optik und weitere, teilweise verschollene Bücher.

Was hier als erstes überrascht, ist die Beschränkung auf nicht zueinander teilerfremde Zahlen. Der Grund dafür liegt darin, daß die klassische griechische Philosophie und Mathematik die Eins nicht als Zahl betrachtete: Zahlen begannen erst bei der Zwei, und auch Mengen mußten mindestens zwei Elemente haben. Auch bei den Aristotelischen Syllogismen mußte sich ein Prädikat auf mindestens zweielementige Klassen beziehen: Die oft als klassischer Syllogismus zitierte Schlußweise

> Alle Menschen sind sterblich
> SOKRATES ist ein Mensch
> Also ist SOKRATES sterblich

wäre von ARISTOTELES nicht anerkannt worden, denn es gab schließlich nur einen SOKRATES. Erst bei seinen Nachfolgern, den Peripatetikern, setzte sich langsam auch die Eins als Zahl durch; ihr Zeitgenosse EUKLID macht noch brav eine Fallunterscheidung: In Proposition 1, unmittelbar vor der hier abgedruckten Proposition 2, führt er praktisch dieselbe Konstruktion durch für teilerfremde Zahlen.

Als zweites fällt auf, daß EUKLID seine Konstruktion rein geometrisch durchführt; wenn er von einer Strecke eine andere Strecke abträgt solange es geht, ist das natürlich in unserer heutigen arithmetischen Sprache gerade die Konstruktion des Divisionsrests bei der Division der beiden Streckenlängen durcheinander.

Die wesentliche Operation beim EUKLIDischen Algorithmus ist also die Division mit Rest, und die haben wir (nach Definition) in jedem EUKLIDischen Ring. Tatsächlich funktioniert der so modifizierte EUKLIDische Algorithmus in jedem EUKLIDischen Ring und berechnet dort den größten gemeinsamen Teiler.

In heutiger Sprache ausgedrückt beruht der EUKLIDische Algorithmus auf folgenden beiden Tatsachen:

1. Wenn wir zwei Elemente f, g eines EUKLIDischen Rings mit Rest durcheinander dividieren, so ist $f : g = q$ Rest r äquivalent zu jeder der beiden Gleichungen
$$f = qg + r \quad \text{und} \quad r = f - qg\,.$$
Diese zeigen, daß jeder gemeinsame Teiler von f und g auch ein gemeinsamer Teiler von g und r ist und umgekehrt. Die beiden Paare (f, g) und (g, r) haben also dieselben gemeinsamen Teiler und damit auch denselben größten gemeinsamen Teiler:
$$\text{ggT}(f, g) = \text{ggT}(g, r)\,.$$
2. $\text{ggT}(f, 0) = f$, denn jedes Element eines Integritätsbereichs teilt die Null.

Aus diesen beiden Beobachtungen folgt nun leicht

Satz: In einem EUKLIDischen Ring gibt es zu je zwei Elementen $f, g \in R$ stets einen größten gemeinsamen Teiler. Dieser kann nach folgendem Algorithmus berechnet werden:
Schritt 0: Setze $r_0 = f$ und $r_1 = g$
Schritt i, $i \geq 1$: Falls $r_i = 0$ ist, endet der Algorithmus mit dem Ergebnis $\text{ggT}(f, g) = r_{i-1}$; andernfalls wird r_{i-1} mit Rest durch r_i dividiert, wobei r_{i+1} der Divisionsrest sei.
Der Algorithmus endet nach endlich vielen Schritten und liefert den größten gemeinsamen Teiler.

Beweis: Wir überlegen uns als erstes, daß im i-ten Schritt für $i \geq 1$ stets $\text{ggT}(f, g) = \text{ggT}(r_{i-1}, r_i)$ ist. Für $i = 1$ gilt dies nach der Konstruktion im nullten Schritt. Falls es im i-ten Schritt für ein $i \geq 1$ gilt und der Algorithmus nicht mit dem i-ten Schritt abbricht, wird dort r_{i+1} als Rest bei der Division von r_{i-1} durch r_i berechnet; wie wir oben gesehen haben, ist somit $\text{ggT}(r_i, r_{i+1}) = \text{ggT}(r_{i-1}, r_i)$, und das ist nach Induktionsvoraussetzung gleich dem ggT von f und g.

Falls der Algorithmus im i-ten Schritt abbricht, ist dort $r_i = 0$. Außerdem ist dort wie in jedem anderen Schritt auch $\text{ggT}(f, g) = \text{ggT}(r_{i-1}, r_i)$. Somit ist r_{i-1} der ggT von f und g.

Schließlich muß noch gezeigt werden, daß der Algorithmus nach endlich vielen Schritten abbricht. Dazu dient die Funktion ν: Nach Definition eines EUKLIDischen Rings ist im i-ten Schritt entweder $\nu(r_i) < \nu(r_{i-1})$ oder $r_i = 0$. Da ν nur natürliche Zahlen und die Null als Werte annimmt und es keine unendliche absteigende Folge solcher Zahlen gibt,

muß nach endlich vielen Schritten $r_i = 0$ sein, womit der Algorithmus abbricht.

■

Als erstes Beispiel wollen wir den EUKLIDischen Algorithmus anwenden auf zwei ganze Zahlen: Um den ggT von 200 und 148 zu Berechnen, müssen wir als erstes 200 durch 148 dividieren:

$$200 : 148 = 1 \text{ Rest } 52$$

Als nächstes wird 148 durch 52 dividiert:

$$148 : 52 = 2 \text{ Rest } 44$$

Weiter geht es mit der Division von 52 durch 44:

$$52 : 44 = 1 \text{ Rest } 8$$

Im nächsten Schritt dividieren wir

$$44 : 8 = 5 \text{ Rest } 4$$

und kommen schließlich mit

$$8 : 4 = 2 \text{ Rest } 0$$

zu einer Division,die aufgeht. Somit haben 200 und 148 den größten gemeinsamen Teiler vier.

Als zweites Beispiel wollen wir den größten gemeinsamen Teiler der beiden Polynome

$$f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$$

und

$$g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$$

aus $\mathbb{Q}[x]$ berechnen. Da Polynomdivision aufwendiger ist als die obigen Rechnungen, wollen wir die Rechenarbeit von Maple erledigen lassen. Wir brauchen dazu im wesentlichen nur den Befehl `rem(f, g, x)`, der den Rest bei der Division von f durch g berechnet, wobei f und g als Polynome in x aufgefaßt werden. Falls uns auch der Quotient interessiert, können wir den durch `quo(f, g, x)` berechnen lassen. Alternativ können wir aber auch dem Befehl `rem` noch ein viertes Argument geben: `rem(f, g, x, 'q')` führt auf dasselbe Ergebnis wie `rem(f, g, x)`,

weist aber zusätzlich noch der Variablen q den Wert des Quotienten zu. Das q muß dabei in Hochkommata stehen, weil auf der linken Seite einer Zuweisung eine Variable stehen muß. Falls der Quotient etwa das Polynom $x^2 + x + 1$ wäre und die Variable q aus einer vorigen Rechnung den Wert $x - 3$ hätte, würde `rem(f, g, x, q)` versuchen, die Zuweisung

$$x - 3 := x^2 + x + 1$$

auszuführen, was natürlich Unsinn ist und auf eine Fehlermeldung führt. Die Hochkommata in `'q'` sorgen dafür, daß unabhängig von einem etwaigen vorigen Wert von q in jedem Fall nur der Variablenname q verwendet wird, so daß die sinnvolle Anweisung $q := x^2+x+1$ ausgeführt wird.

```
> f := x^8 + x^6 - 3*x^4 - 3*x^3 + 8*x^2 + 2*x - 5;
```

$$f := x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$$

```
> g := 3*x^6 + 5*x^4 - 4*x^2 - 9*x + 21;
```

$$g := 3x^6 + 5x^4 - 4x^2 - 9x + 21$$

```
> r2 := rem(f, g, x, 'q'); q;
```

$$r2 := -\frac{5}{9}x^4 + \frac{1}{9}x^2 - \frac{1}{3}$$

$$\frac{x^2}{3} - \frac{2}{9}$$

```
> r3 := rem(g, r2, x);
```

$$r3 := -\frac{117}{25}x^2 - 9x + \frac{441}{25}$$

```
> r4 := rem(r2, r3, x);
```

$$r4 = \frac{233150}{6591}x - \frac{102500}{2197}$$

```
> r5 := rem(r3, r4, x);
```

$$r5 := \frac{1288744821}{543589225}$$

```
> r6 := rem(r4, r5, x);
```

$$r6 := 0$$

Der ggT von f und g ist somit $r_5 = \frac{1288744821}{543589225}$. Da der ggT nur bis auf eine multiplikative Konstante bestimmt ist, können wir freilich genauso gut sagen, der ggT von f und g sei eins. In der Tat liefert uns Maple auch diese Antwort, wenn wir direkt nach dem ggT von f und g fragen:

```
> gcd(f, g);
```

$$1$$

Die Frage ist nun: Müssen wir wirklich mit so riesigen Brüchen wie r_5 rechnen, um auf diese einfache Antwort zu kommen?

Da der größte gemeinsame Teiler ohnehin nur bis auf eine multiplikative Konstante bestimmt ist, bestünde ein einfacher Ausweg darin, vor jeder Polynomdivision den Dividenden mit einer geeigneten Konstanten zu multiplizieren um so sicherzustellen, daß beim Dividieren keine Nenner auftreten. Bei der Division eines Polynoms vom Grad n durch ein Polynom vom Grad $m \le n$ wird bis zu $n - m + 1$ mal durch den führenden Koeffizienten a des Divisors dividiert; wir müssen als den Dividenden vorher mit a^{n-m+1} multiplizieren. Im obigen Beispiel führt das auf folgende Rechnung:

```
> r2 := rem(3^3*f, g, x);
```

$$r2 := -15x^4 + 3x^2 - 9$$

```
> r3 := rem((-15)^3*g, r2, x);
```

$$r3 := 15795x^2 + 30375x - 59535$$

```
> r4 := rem(15795^3*r2, r3, x);
```

$$r4 := 1254542875143750x - 1654608338437500$$

```
> r5 := rem(1254542875143750^2*r3, r4, x);
```

$$r5 := 1259333879550074310093114199218750 0$$

Verglichen mit der Größe der Ausgangsdaten und des Ergebnisses entstehen auch hier wieder riesige Zahlen. Das ist leider kein Einzelfall: Auch wenn es sich hier um ein (von DONALD E. KNUTH für sein Buch *The Art of Computer Programming*, Abschnitt 4.6.1) konstruiertes besonders extremes Beispiel handelt, zeigt die Erfahrung, daß wir es beim EUKLIDischen Algorithmus für Polynome über den rationalen Zahlen

oft mit einer Explosion der Koeffizienten zu tun haben, die in keiner Weise der Komplexität des Ergebnisses entspricht. Wenn wir den Algorithmus ernsthaft auf größere Polynome anwenden wollen, sollten wir nach Wegen suchen, um dieses Problem zu umschiffen.

Solche Wege gibt es in der Tat; für ihr Verständnis ist allerdings einiges mehr an Theorie erforderlich als für den hier behandelten einfachen EUKLIDischen Algorithmus.

§4: Der erweiterte Euklidische Algorithmus

Zur Bestimmung des ggT zweier Elemente eins EUKLIDischen Rings R berechnen wir eine Reihe von Elementen r_i, wobei r_0 und r_1 die Ausgangsdaten sind und alle weiteren r_i durch Division mit Rest ermittelt werden:

$$r_{i-1} : r_i = q_i \text{ Rest } r_{i+1}$$

Damit ist $r_{i+1} = r_{i-1} - q_i r_i$ als Linearkombination seiner beiden Vorgänger r_i und r_{i-1} mit Koeffizienten aus R darstellbar, die wiederum R-Linearkombinationen ihrer Vorgänger sind, *usw.* Wenn wir alle diese Darstellungen ineinander einsetzen, erhalten wir r_i schließlich als Linearkombination der Ausgangselemente. Dies gilt insbesondere für das letzte nichtverschwindende r_i, den ggT. Der ggT zweier Elemente f, g eines EUKLIDischen Rings ist somit darstellbar als R-Linearkombination von f und g.

Algorithmisch sieht dies folgendermaßen aus:

Schritt 0: Setze $r_0 = f$, $r_1 = g$, $\alpha_0 = \beta_1 = 1$ und $\alpha_1 = \beta_0 = 0$. Mit $i = 1$ ist dann

$$r_{i-1} = \alpha_{i-1} a + \beta_{i-1} b \quad \text{und} \quad r_i = \alpha_i a + \beta_i b\,.$$

Diese Relationen werden in jedem der folgenden Schritte erhalten:

Schritt i, $i \ge 1$**:** Falls $r_i = 0$ ist, endet der Algorithmus mit

$$\text{ggT}(f, g) = r_{i-1} = \alpha_{i-1} f + \beta_{i-1} g\,.$$

Andernfalls dividiere man r_{i-1} mit Rest durch r_i mit dem Ergebnis

$$r_{i-1} = q_i r_i + r_{i+1}\,.$$

Dann ist

$$r_{i+1} = -q_i r_i + r_{i-1} = -q_i(\alpha_i f + \beta_i g) + (\alpha_{i-1} f + \beta_{i-1} g)$$
$$= (\alpha_{i-1} - q_i \alpha_i) f + (\beta_{i-1} - q_i \beta_i) g\,;$$

man setze also

$$\alpha_{i+1} = \alpha_{i-1} - q_i \alpha_i \quad \text{und} \quad \beta_{i+1} = \beta_{i-1} - q_i \beta_i\,.$$

Da die Schritte hier einfach Erweiterungen der entsprechenden Schritte des klassischen EUKLIDischen Algorithmus sind, ist klar, daß auch dieser Algorithmus nach endlich vielen Schritten abbricht und als Ergebnis den ggT liefert. Da die beiden Relationen aus Schritt 0 in allen weiteren Schritten erhalten bleiben, ist auch klar, daß dieser ggT am Ende als Linearkombination dargestellt ist.

Obwohl es keinerlei Anhaltspunkt dafür gibt, daß diese Erweiterung EUKLID bekannt gewesen sein könnte, bezeichnet man sie als den *erweiterten* EUKLIDischen Algorithmus, Vor allem in der französischen Literatur wird die Darstellung des ggT als Linearkombination auch als Identität von BÉZOUT bezeichnet, da dieser sie 1766 in einem Lehrbuch beschrieb und als erster auch auf Polynome anwandte. Für Zahlen ist die Erweiterung jedoch bereits 1624 zu finden in der zweiten Auflage des Buchs *Problèmes plaisants et délectables qui se fonts par les nombres* von BACHET DE MÉZIRIAC. (Eine vereinfachte Ausgabe dieses Buchs von 1874 wurde 1993 bei Blanchard neu aufgelegt; sie ist auch online verfügbar unter `cnum.cnam.fr/DET/8PY45.html`.)

CLAUDE GASPAR BACHET SIEUR DE MÉZIRIAC (1581-1638) verbrachte den größten Teil seines Lebens in seinem Geburtsort Bourg-en-Bresse. Er studierte zwar bei den Jesuiten in Lyon und Milano und trat 1601 in den Orden ein, trat aber bereits 1602 wegen Krankheit wieder aus und kehrte nach Bourg zurück. Sein Buch erschien erstmals 1612, Am bekanntesten ist BACHET für seine lateinische Übersetzung der *Arithmetika* von DIOPHANTOS. In einem Exemplar davon schrieb FERMAT seine Vermutung an den Rand. Auch Gedichte von BACHET sind erhalten. 1635 wurde er Mitglied der französischen Akademie der Wissenschaften.

ETIENNE BÉZOUT (1730-1783) wurde in Nemours in der Ile-de-France geboren, wo seine Vorfahren Magistrate waren. Er ging stattdessen an die Akademie der Wissenschaften; seine Hauptbeschäftigung war die Zusammenstellung von Lehrbüchern für die Militärausbildung. Im 1766 erschienenen dritten Band (von vier) seines *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine* ist die Identität von BÉZOUT dargestellt. Seine Bücher waren so erfolgreich, daß sie ins Englische übersetzt und z.B. in Harvard als Lehrbücher benutzt wurden. Heute ist er vor allem bekannt durch seinen Beweis, daß sich zwei Kurven der Grade n und m in höchstens nm Punkten schneiden können.

Als Beispiel wollen wir den ggT von 200 und 148 als Linearkombination darstellen. Der Rechengang ist natürlich genau derselbe wie in §3, nur daß wir jetzt noch in jedem Schritt den Divisionsrest als ganzzahlige Linearkombination von 200 und 148 darstellen.

Im nullten Schritt haben wir 200 und 148 als die trivialen Linearkombinationen

$$200 = 1 \cdot 200 + 0 \cdot 148 \quad \text{und} \quad 148 = 0 \cdot 200 + 1 \cdot 148\,.$$

Im ersten Schritt dividieren wir, da 148 nicht verschwindet, 200 mit Rest durch 148:

$$200 = 1 \cdot 148 + 52 \Longrightarrow 52 = 1 \cdot 200 - 1 \cdot 148$$

Da auch $52 \neq 0$ ist, dividieren wir im zweiten Schritt 148 durch 52 mit Ergebnis $148 = 2 \cdot 52 + 44$, d.h.

$$44 = 148 - 2 \cdot (1 \cdot 200 - 1 \cdot 148) = 3 \cdot 148 - 2 \cdot 200$$

Auch $44 \neq 0$, wir dividieren also weiter: $52 = 1 \cdot 44 + 8$ und

$$8 = 52 - 44 = (1 \cdot 200 - 1 \cdot 148) - (3 \cdot 148 - 2 \cdot 200)$$
$$= 3 \cdot 200 - 4 \cdot 148\,.$$

Im nächsten Schritt erhalten wir $44 = 5 \cdot 8 + 4$ und

$$4 = 44 - 5 \cdot 8 = (3 \cdot 148 - 2 \cdot 200) - 5 \cdot (3 \cdot 200 - 4 \cdot 148)$$
$$= 23 \cdot 148 - 17 \cdot 200\,.$$

Bei der Division von acht durch vier schließlich erhalten wir Divisionsrest Null; damit ist vier der ggT von 148 und 200 und kann in der angegebenen Weise linear kombiniert werden. Diese Darstellung ist freilich nicht eindeutig: Beispielsweise können wir beliebige Vielfache der trivialen Darstellung $200 \cdot 148 - 148 \cdot 200 = 0$ der Null addieren. Tatsächlich können wir diese auch noch durch den ggT kürzen zu $50 \cdot 148 - 36 \cdot 200 = 0$; wir haben also für jede ganze Zahl k eine Darstellung $1 = (23 + 50k) \cdot 148 - (17 + 36k) \cdot 200$.

Wir können den erweiterten EUKLIDischen Algorithmus natürlich auch auf die beiden Polynome f und g aus dem vorigen Paragraphen anwenden, allerdings ist das Ergebnis alles andere als schön: $1 = \alpha f + \beta g$, wobei α ein Polynom vom Grad fünf und β eines vom Grad sieben ist. Der Hauptnenner der Koeffizienten ist in beiden Fällen 130 354. Wir können den Algorithmus allerdings verwenden, um ein negatives Resultat zu beweisen:

Lemma: Der Ring $\mathbb{Z}[x]$ aller Polynome mit ganzzahligen Koeffizienten ist nicht EUKLIDisch.

Beweis: Wir wissen zwar noch nicht, daß zwei beliebige Elemente von $\mathbb{Z}[x]$ auch in $\mathbb{Z}[x]$ einen größten gemeinsamen Teiler haben, es ist aber klar, daß der größte gemeinsame Teiler der beiden Polynome x und 2 existiert und eins ist: Die einzigen Teiler von 2 sind ± 1 und ± 2, und ± 2 sind keine Teiler von x. Wäre $\mathbb{Z}[x]$ ein EUKLIDischer Ring, gäbe es also Polynome $\alpha, \beta \in \mathbb{Z}[x]$, so daß $\alpha x + 2\beta = 1$ wäre. Der konstante Koeffizient von $\alpha x + 2\beta$ ist aber das Doppelte des konstanten Koeffizienten von β, also eine gerade Zahl. Somit kann es keine solche Darstellung geben. ∎

(In $\mathbb{Q}[x]$ gibt es selbstverständlich so eine Darstellung: $1 = 0 \cdot x + \frac{1}{2} \cdot 2$. Auch ist dort 2 ein Teiler von x.)

§5: Die endlichen Primkörper

Die Explosion der Koeffizienten bei der Rechnung in §3 hängt natürlich damit zusammen, daß wir mit rationalen Zahlen gerechnet haben. Über

einem endlichen Körper gibt es nur endlich viele Möglichkeiten für jeden Koeffizienten, er kann also nicht unbegrenzt wachsen.

In der Computeralgebra führt man deshalb Probleme mit ganzzahligen Koeffizienten gerne zurück auf solche über endlichen Körpern, und auch das gängigste Verfahren zur effizienten Berechnung des größten gemeinsamen Teilers zweier Polynome verwendet diese Strategie.

Für eine zusammengesetzte Zahl $n = pq$ mit $p, q > 1$ bilden die Zahlen modulo n offensichtlich keinen Körper, denn $p \bmod n$ und $q \bmod n$ sind beide von Null verschieden, aber ihr Produkt $pq \bmod n = n \bmod n = 0$ verschwindet. Daher müssen wir uns auf Primzahlen beschränken, und hier gilt

Satz: Für jede Primzahl p ist die Menge $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ mit den Operationen

$$a \oplus b = (a + b) \bmod p \quad \text{und} \quad a \otimes b = (a \cdot b) \bmod p$$

ein Körper. Alle vier Grundrechenarten in $\mathbb{F}_p$ können algorithmisch ausgeführt werden.

Beweis: Es ist klar, daß alle die Addition betreffenden Körperaxiome sowie die Distributivgesetze erfüllt sind und daß sich Addition, Subtraktion und Multiplikation problemlos durchführen lassen. Auch mit Assoziativ- und Kommutativgesetz der Multiplikation gibt es keinerlei Probleme, und natürlich ist $1 \in \mathbb{F}_p$ Neutralelement bezüglich der Multiplikation. Bis hierher ist es auch völlig egal, ob p eine Primzahl ist oder nicht.

Zu zeigen bleibt die Existenz von multiplikativen Inversen.

Seien also $b \in \mathbb{F}_p \setminus \{0\}$. Dann ist $1 \le b \le p - 1$, d.h. b ist teilerfremd zu p, da die Primzahl p keine echten Teiler hat. Der größte gemeinsame Teiler von b und p ist also die Eins, und mit Hilfe des erweiterten EUKLIDischen Algorithmus können wir sie darstellen als ganzzahlige Linearkombination von b und p:

$$1 = \alpha b + \beta p \quad \text{mit} \quad \alpha, \beta \in \mathbb{Z}.$$

Somit ist $\alpha b \equiv 1 \bmod p$, d.h. $\alpha \bmod p$ ist ein multiplikatives Inverses von a und läßt sich mit Hilfe des erweiterten EUKLIDischen Algorithmus

auch effektiv berechnen. Damit können alle Quotienten algorithmisch berechnet werden, denn $a/b = a \cdot b^{-1}$.

■

Im folgenden werden wir auf die Symbole $\oplus$ und $\odot$ verzichten und Addition sowie Multiplikation auch in $\mathbb{F}_p$ einfach mit dem gewöhnlichen Plus- und Malzeichen schreiben.

Da $\mathbb{F}_p$ ein Körper ist, bilden die Polynome über $\mathbb{F}_p$ einen EUKLIDischen Ring, wir können also mit dem EUKLIDischen Algorithmus größte gemeinsame Teiler berechnen. Das Problem explodierender Koeffizienten, mit dem wir in §3 zu kämpfen hatten, existiert hier nicht, denn jedes Divisionsergebnis ist einfach wieder ein Element von $\mathbb{F}_p$, also eine ganze Zahl zwischen 0 und $p-1$.

Zur Illustration betrachten wir die beiden Polynome aus §3 über dem Körper mit elf Elementen. Der Operator `mod` sorgt dafür, daß Maple etwas modulo dem zweiten Argument des Operators betrachtet; wir erhalten also

```
> f mod 11;
```

$$x^8 + x^6 + 8x^4 + 8x^3 + 8x^2 + 2x + 6$$

```
> g mod 11;
```

$$3x^6 + 5x^4 + 7x^2 + 2x + 10$$

Bei der Berechnung von Quotienten und Divisionsresten dürfen wir allerdings nicht einfach `rem(f, g, x) mod 11` schreiben, denn dann würde ja erst modulo 11 reduziert, wenn der Rest bereits über $\mathbb{Q}$ berechnet wurde. Um dies zu vermeiden, bietet Maple die Operatoren `rem` und `quo` auch in einer trägen Form `Rem` *bzw.* `Quo` an: Diese Operatoren führen zu keiner Polynomdividision, sondern bleiben einfach unausgewertet stehen:

```
> Rem(f, g, x);
```

$$\mathrm{Rem}(x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21, x)$$

Wendet man darauf nun allerdings den Operator `mod p` an, so sorgt dieser dafür, daß die Polynomdivision modulo p durchgeführt und der Divisionsrest aus $\mathbb{F}_p[x]$ zurückgegeben wird:


```
> r2 := Rem(f, g, x) mod 11;
```

$$r2 := 8x^4 + 5x^2 + 7$$

```
> r3 := sort(Rem(g, r2, x) mod 11, x);
```

$$r3 := 5x^2 + 2x + 4$$

```
> r4 := sort(Rem(r2, r3, x) mod 11, x);
```

$$r4 := 10x + 10$$

```
> r5 := Rem(r3, r4, x) mod 11;
```

$$r5 := 7$$

```
> r6 := Rem(r4, r5, x) mod 11;
```

$$r6 := 0$$

Der ggT von f mod 11 und g mod 11 ist somit gleich der Konstanten sieben und damit ist auch die Eins ein ggT, denn der ggT im Polynomring über einem Körper ist nur bis auf eine multiplikative Konstante bestimmt.

Folgt damit, daß auch die Ausgangspolynome f und g aus $\mathbb{Z}[x]$ teilerfremd sind? Mit unseren derzeitigen Kenntnissen können wir das nicht sagen, denn bislang wissen war ja noch nicht einmal, ob es in $\mathbb{Z}[x]$ größte gemeinsame Teiler gibt. Um zu sehen, daß es durchaus Unterschiede zwischen ganzzahligen Polynomen und solchen über endlichen Körpern gibt, wollen wir die Rechnung auch modulo sieben durchführen:

```
> f mod 7;
```

$$x^8 + x^6 + 4x^4 + 4x^3 + x^2 + 2x + 2$$

```
> g mod 7;
```

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

```
> r2 := Rem(f, g, x) mod 7;
```

$$r2 := x^4 + 4x^2 + 2$$

```
> r3 := sort(Rem(g, r2, x) mod 7, x);
```

$$r3 := 4x^2 + 5x$$

```
> r4 := sort(Rem(r2, r3, x) mod 7, x);
```

$$r4 := 3x + 2$$

```
> r5 := Rem(r3, r4, x) mod 7;
```

$$r5 := 0$$

Hier ist der ggT also das lineare Polynom $3x + 2$ oder, wenn wir durch drei dividieren, $x + 3$.

§6: Faktorielle Ringe

Wenn wir größte gemeinsame Teiler für Polynome mit rationalen Koeffizienten in Verbindung bringen wollen mit solchen für Polynome über endlichen Körpern, kommen eigentlich nur Polynome mit ganzzahligen Koeffizienten als Bindeglied in Frage: Durch Multiplikation mit dem Hauptnenner können wir die Koeffizienten eines rationalen Polynoms ganzzahlig machen, und das entstehende Polynom können wir dann modulo einer Primzahl p betrachten.

Das so erhaltene Polynom muß nicht unbedingt viel mit dem Ausgangspolynom zu tun haben: Falls wir modulo einer Primzahl rechnen, die den führenden Koeffizienten teilt, unterscheiden sich selbst die Grade, und wenn wir eine Primzahl nehmen, die *alle* Koeffizienten teilt, erhalten wir einfach das Nullpolynom.

Wir müssen uns daher genau überlegen, womit wir erweitern und modulo welcher Primzahlen wir reduzieren, und vor allem müssen wir auch etwas mehr wissen über den Polynomring $\mathbb{Z}[x]$: Bislang wissen wir schließlich nur, daß er *kein* EUKLIDischer Ring ist,

Definition: *a)* Ein Element f eines Integritätsbereichs R heißt *irreduzibel*, falls gilt: f ist keine Einheit, und ist $f = gh$ das Produkt zweier Elemente aus R, so muß g oder h eine Einheit sein.
b) Ein Integritätsbereich R heißt *faktoriell* oder *ZPE*-Ring, wenn gilt: Jedes Element $f \in R$ läßt sich bis auf Reihenfolge und Assoziiertheit eindeutig schreiben als Produkt $f = u\prod_{i=1}^{n} p_i^{e_i}$ mit einer Einheit $u \in R^\times$, irreduziblen Elementen $p_i \in R$ und natürlichen Zahlen e_i.
(*ZPE* steht für **Z**erlegung in **P**rimfaktoren **E**indeutig.)

Lemma: In einem faktoriellen Ring R gibt es zu je zwei Elementen $f, g \in R$ einen größten gemeinsamen Teiler.

Beweis: Sind $f = u\prod_{i=1}^{n} p_i^{e_i}$ und $g = v\prod_{j=1}^{m} q_j^{d_j}$ mit $u, v \in R^\times$ und p_i, q_j irreduzibel die Zerlegungen von f und g in Primfaktoren, so können wir, indem wir nötigenfalls Exponenten null einführen, o.B.d.A. annehmen, daß $n = m$ ist und $p_i = q_i$ für alle i. Dann ist offenbar $\prod_{i=1}^{n} p_i^{\min(e_i,d_i)}$ ein ggT von f und g, denn $h = \prod_{i=1}^{r} p_i^{a_i}$ ist genau dann Teiler von f, wenn $a_i \le e_i$ für alle i, und Teiler von g, wenn $a_i \le d_i$. ∎

Wie wir bald sehen werden, bedeutet dies keineswegs, daß jeder faktorielle Ring EUKLIDisch wäre. Umgekehrt gilt allerdings

Satz: Jeder EUKLIDische Ring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $f \neq 0$ aus R bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich f überhaupt so darstellen läßt.

Dazu benutzen wir die Funktion $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$ des EUKLIDischen Rings R und beweisen induktiv, daß für $N \in \mathbb{N}_0$ alle $f \neq 0$ mit $\nu(f) \le N$ in der gewünschten Weise darstellbar sind.

Ist $\nu(f) = 0$, so ist f eine Einheit: Bei der Division $1 : f = g$ Rest r ist nämlich entweder $r = 0$ oder aber $\nu(r) < \nu(f) = 0$. Letzteres ist nicht möglich, also ist $gf = 1$ und f eine Einheit. Diese kann als sich selbst mal dem leeren Produkt von Potenzen irreduzibler Elemente geschrieben werden.

Für $N > 1$ unterscheiden wir zwei Fälle: Ist f irreduzibel, so ist $f = f$ eine Darstellung der gewünschten Form, und wir sind fertig.

Andernfalls läßt sich $f = gh$ als Produkt zweier Elemente schreiben, die beide keine Einheiten sind. Nach Definition eines EUKLIDischen Rings sind dann $\nu(g), \nu(h) \le \nu(f)$. Wir wollen uns überlegen, daß sie tatsächlich sogar echt kleiner sind.

Dazu dividieren wir g mit Rest durch f; das Ergebnis sei q Rest r, d.h. $g = qf + r$ mit $r = 0$ oder $\nu(r) < \nu(f)$. Wäre $r = 0$, wäre g ein Vielfaches

von f, es gäbe also ein $u \in R$ mit $g = uf = u(gh) = (uh)g$. Damit wäre $uh = 1$, also h eine Einheit, im Widerspruch zur Annahme. Somit ist $\nu(r) < \nu(f)$. Außerdem ist g ein Teiler von $r = g - qf = g(1 - qh)$, also muß gelten $\nu(g) \leq \nu(r) < \nu(f)$.

Genauso folgt die strikte Ungleichung $\nu(h) < \nu(f)$.

Nach Induktionsvoraussetzung lassen sich daher g und h als Produkte von Einheiten und Potenzen irreduzibler Elemente schreiben, und damit läßt sich auch $f = gh$ so darstellen.

Als nächstes müssen wir uns überlegen, daß diese Darstellung bis auf Reihenfolge und Einheiten eindeutig ist. Das wesentliche Hilfsmittel hierzu ist die folgende Zwischenbehauptung:

Falls ein irreduzibles Element p ein Produkt fg teilt, teilt es mindestens einen der beiden Faktoren.

Zum *Beweis* betrachten wir den ggT von f und p. Dieser ist insbesondere ein Teiler von p, also bis auf Assoziiertheit entweder p oder 1. Im ersten Fall ist p Teiler von f, und wir sind fertig; andernfalls können wir

$$1 = \alpha p + \beta f$$

als Linearkombination von p und f schreiben. Multiplikation mit g macht daraus $g = \alpha pf + \beta fg$, und hier sind beide Summanden auf der rechten Seite durch p teilbar: Bei αpf ist das klar, und bei βfg folgt es daraus, daß nach Voraussetzung p ein Teiler von fg ist. Also ist p Teiler von g, und die Zwischenbehauptung ist bewiesen.

Induktiv folgt sofort:

Falls ein irreduzibles Element $p \in R$ ein Produkt $\prod_{i=1}^{n} f_i$ teilt, teilt es mindestens einen der Faktoren.

Um den Beweis des Satzes zu beenden, zeigen wir induktiv, daß für jedes $N \in \mathbb{N}_0$ alle Elemente mit $\nu(f) \leq N$ eine bis auf Reihenfolge und Einheiten *eindeutige* Primfaktorzerlegung haben.

Für $N = 0$ haben wir oben gesehen, daß f eine Einheit sein muß, und hier ist die Zerlegung $f = f$ eindeutig.

Für $N \geq 1$ betrachten wir ein Element

$$f = u \prod_{i=1}^{n} p_i^{e_i} = v \prod_{j=1}^{m} q_j^{d_j}$$

mit zwei Zerlegungen, wobei wir annehmen können, daß alle $e_i, f_j \geq 1$ sind. Dann ist p_1 trivialerweise Teiler des ersten Produkts, also auch des zweiten. Wegen der Zwischenbehauptung teilt p_1 daher mindestens eines der Elemente q_j, d.h. $p_1 = wq_j$ ist bis auf eine Einheit w gleich q_j. Da p_i keine Einheit ist, ist $\nu(f/p_i) < \nu(f)$; nach Induktionsannahme hat also $f/p_i = x/(wq_j)$ eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x diese Eigenschaft.

■

Als nächstes wollen wir Produktzerlegungen in $\mathbb{Q}[x]$ vergleichen mit solchen in $\mathbb{Z}[x]$. Das entsprechende Argument von GAUSS wird uns auch nützlich sein für den Beweis der Faktorialität von Polynomringen in mehreren Veränderlichen; wir fassen es daher gleich etwas allgemeiner.

Dazu brauchen wir als erstes für einen beliebigen Integritätsbereich eine Entsprechung für die rationalen Zahlen, den sogennanten Quotientenkörper, der genauso konstruiert wird wie die rationalen Zahlen aus den ganzen:

Wir betrachten für einen Integritätsbereich R auf der Menge aller Paare (f, g) mit $f, g \in R$ und $g \neq 0$ die Äquivalenzrelation

$$(f, g) \sim (r, s) \iff fs = gr\,;$$

die Äquivalenzklasse von (f, g) bezeichnen wir als den *Bruch* $\frac{f}{g}$.

Verknüpfungen zwischen diesen Brüchen werden nach den üblichen Regeln der Bruchrechnung definiert:

$$\frac{f}{g} + \frac{r}{s} = \frac{fs + rg}{gs} \quad \text{und} \quad \frac{f}{g} \cdot \frac{r}{s} = \frac{fr}{gs}\,.$$

Dies ist wohldefiniert, denn sind $(f, g) \sim (\tilde{f}, \tilde{g})$ und $(r, s) \sim (\tilde{r}, \tilde{s})$, so ist

$$\frac{\tilde{f}}{\tilde{g}} + \frac{\tilde{r}}{\tilde{s}} = \frac{\tilde{f}\tilde{s} + \tilde{r}\tilde{g}}{\tilde{g}\tilde{s}} \quad \text{und} \quad \frac{\tilde{f}}{\tilde{g}} \cdot \frac{\tilde{r}}{\tilde{s}} = \frac{\tilde{f}\tilde{r}}{\tilde{g}\tilde{s}}\,.$$