OSNABRÜCKER SCHRIFTEN ZUR MATHEMATIK

Reihe V Vorlesungsskripten

EHeft 12 Sommersemester 2005

Computer-Algebra

W. Bruns

Fachbereich Mathematik/Informatik
Universität Osnabrück

OSM Osnabrücker Schriften zur Mathematik

September 2005

Herausgeber	Selbstverlag der Universität Osnabrück Fachbereich Mathematik/Informatik 49069 Osnabrück
Geschäftsführer	Prof. Dr. W. Bruns
Berater:	Prof. Dr. P. Brucker (Angew. Mathematik) Prof. Dr. E. Cohors-Fresenborg (Didaktik der Mathematik) Prof. Dr. V. Sperschneider (Informatik) Prof. Dr. R. Vogt (Reine Mathematik)
Druck	Hausdruckerei der Universität Osnabrück

Weitere Reihen der OSM:

Reihe D	Mathematisch-didaktische Manuskripte
Reihe I	Manuskripte der Informatik
Reihe M	Mathematische Manuskripte
Reihe P	Preprints
Reihe U	Materialien zum Mathematikunterricht

Computer-Algebra

Winfried Bruns

Skript zur Vorlesung SS 2005

Inhaltsverzeichnis

Vorwort

Der vorliegende Text ist die Niederschrift einer Vorlesung, die in den Sommersemestern 2003 und 2005 an der Universität Osnabrück gehalten wurde. Die Reihenfolge der beiden großen Teile (Kap. 1 – 6 und 7 – 13) wurde im SS 2005 gegenüber der ursprünglichen Fassung vertauscht. Im SS 2005 hatte die Vorlesung die Form eines *reading course*, und als Leitfaden für solch einen Kurs sollte man diesen Text verstehen.

Er geht davon aus, daß die Hörer neben der Vorlesung „Lineare Algebra“ auch eine „Einführung in die Algebra“ absolviert haben, in der die wichtigsten Sätze und Methoden der elementaren Zahlentheorie, wie die Existenz und Bestimmung des größten gemeinsamen Teilers, der chinesische Restsatz und die Existenz von Primitivwurzeln modulo Primzahlen diskutiert worden sind. Ebenso werden Kenntnisse über Polynome und endliche Körper vorausgesetzt.

Ich danke Marco Scharringhausen, der die Vorlesung des SS 2003 in LaTeX umgesetzt hat, und Christoph Söger für sein genaues Studiums des Manuskripts, das mich vor manchem Fehler bewahrt hat.

Osnabrück, Juli 2005 *Winfried Bruns*

ABSCHNITT 1

Faktorisierung von Polynomen über endlichen Körpern

Wir gehen im folgenden davon aus, daß die grundlegenden Algorithmen für das Rechnen mit Polynomen bekannt sind. Neben Addition und Multiplikation gehört dazu der (erweiterte) euklidische Algorithmus. Er bestimmt den größten gemeinsamen Teiler $\mathrm{ggT}(f, g)$. zweier Polynome f, g im Ring $K[X]$ der Polynome in der Unbestimmten X über einem Körper K. Wir normieren $\mathrm{ggT}(f, g)$ stets, d. h. sein Leitkoeffizient ist 1. In der erweiterten Form bestimmt der euklidische Algorithmus zusätzlich eine Darstellung

$$\mathrm{ggT}(f, g) = af + bg, \qquad a, b \in K[X].$$

Der euklidische Algorithmus „existiert“ in allen euklidischen Ringen, zu denen insbesondere auch der Ring $\mathbb{Z}$ der ganzen Zahlen gehört.

Wir verwenden im folgenden die Kenntnisse, die in jeder einführenden Algebra-Vorlesung vermittelt werden, ohne weitere Referenz. Dazu gehören insbesondere die Sätze über Primfaktorzerlegung in faktoriellen Ringen wie $\mathbb{Z}$ und $K[X]$, sowie die Aussagen über die Konstruktion von endlichen Körpererweiterungen. Siehe zum Beispiel [**Alg**].

Endliche Körper. Wir wiederholen einige aus der Algebra bekannte Aussagen über endliche Körper.

Bemerkung 1.1. (a) Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ ein endlicher Körper.

(b) Wenn K ein endlicher Körper ist, so ist seine Charakteristik eine Primzahl $p > 0$. Insbesondere ist $\mathbb{Z}_p$ in natürlicher Weise ein Teilkörper von K. Da K dann ein Vektorraum über $\mathbb{Z}_p$ ist, ist $\#K$ eine Potenz von p, genauer:

$$\#K = p^e \ , \ e = \dim_{\mathbb{Z}_p} K$$

(c) Sei $\#K = q = p^e$. Dann gilt $x^q - x = 0$ für alle $x \in K$. Dies ist offensichtlich richtig für $x = 0$ und folgt für $x \neq 0$ aus dem kleinen Satz von Fermat, weil $\#K^* = q - 1$. Also besteht K aus den q einfachen Nullstellen von $f = X^q - X$. Als Zerfällungskörper von f ist K bis auf Isomorphie eindeutig bestimmt.

(d) Andererseits existiert auch ein Körper mit $q = p^e$ Elementen für jedes $e \in \mathbb{N}$, $e \geq 1$. Wir wählen K als Zerfällungskörper von $f = X^q - X \in \mathbb{Z}_p[X]$. Die Nullstellen von f bilden einen Teilkörper L von K, daher ist $K = L$. Wegen $f' = -1$ hat f nur einfache Nullstellen. Es folgt $\#K = q$. Der gemäß (c) eindeutig bestimmte Körper mit q Elementen wird mit $\mathbb{F}_q$ bezeichnet.

(e) Beim Beweis von (d) benutzt man, daß $F : K \to K$, $x \mapsto x^p$, ein Automorphismus von K ist, er heißt *Frobenius-Automorphismus*. Also ist auch $F^e = F \circ \cdots \circ F$ ein Automorphismus. Die Menge seiner Fixpunkte ist ein Teilkörper, nämlich K.

(f) Die Einheitengruppe $\mathbb{F}_q^*$ ist zyklisch, denn endliche Untergruppen der Einheitengruppen von Körpern sind immer zyklisch. Sei u ein erzeugendes Element. Dann ist $\mathbb{F}_q$ die kleinste u enthaltende Körpererweiterung von $\mathbb{F}_p$ und das Minimalpolynom μ von u hat den Grad e. Insbesondere existieren stets irreduzible Polynome des Grades e mit Koeffizienten in $\mathbb{Z}_p$.

Teil (f) zeigt, wie man die Arithmetik in $\mathbb{F}_q$, $q = p^e$, effektiv realisieren kann. Die Elemente werden durch Polynome $g \in \mathbb{Z}_p[X]$ mit $\operatorname{grad} g < e$ repräsentiert. Die Summe zweier Polynome hat dann wieder Grad $< e$. Das Produkt wird durch seinen per Division mit Rest ermittelten Rest $r \mod \mu$ repräsentiert. Dazu braucht man die Reste der Potenzen X^k, $e \le k \le 2(e-1)$. Diese kann man dann tabellieren. Sei $g \in \mathbb{Z}_p[X]$ und $\overline{g}$ seine Restklasse in $\mathbb{F}_q$. Wir wenden den erweiterten euklidischen Algorithmus an, um $1/\overline{g}$ zu bestimmen. Er findet eine Darstellung

$$1 = ag + b\mu, \quad a, b \in \mathbb{Z}_p[X].$$

Dann ist der Rest von $a \mod \mu$ ein Repräsentant von $1/\overline{g}$. Man kann den euklidischen Algorithmus so weit vereinfachen, daß nur a bestimmt wird. (Man sollte beachten, daß auch die Division in $\mathbb{Z}_p$ den erweiterten euklidischen Algorithmus in $\mathbb{Z}$ erfordert.)

Das Faktorisierungsverfahren für Polynome $f \in \mathbb{F}_q[X]$, das wir diskutieren wollen, läuft in drei Schritten ab:

(a) Wir bestimmen den quadratfreien Teil von f. Er enthält alle irreduziblen Faktoren von f, deren Vielfachheiten dann leicht zu finden sind.

(b) Man zerlegt ein quadratfreies Polynom g in die *Teile gleichen Grades*

$$g = g_1 \cdots g_d,$$

wobei g_i das Produkt der irreduziblen Faktoren das Grades i ist.

(c) Der letzte Schritt ist die Zerlegung der Teile gleichen Grades.

Wir diskutieren diese Schritte in der gegebenen Reihenfolge.

Bestimmung des quadratfreien Teils. Sei $f \in K[X]$ ein normiertes Polynom über dem Körper K und

$$f = \prod_{i=1}^{n} g_i^{e_i}$$

die Zerlegung von f in ein Produkt von Potenzen paarweise irreduzibler Polynome. Dann gilt

$$f' = \sum_{i=1}^{n} e_i \frac{f}{g_i} g_i'$$

Es ist klar, daß jedes g_i die Ableitung f' mit Vielfachheit $e_i - 1$ teilt. Deshalb betrachten wir

$$h = \frac{f}{\mathrm{ggT}(f, f')}.$$

Im Nenner kommen dann nur die irreduziblen Teiler g_i von f vor, und zwar mindestens mit der Vielfachheit $e_i - 1$, $i = 1, \ldots, n$. Wenn sie alle mit der genau dieser jeweiligen Vielfachheit vorkommen, ist h der quadratfreie Teil von f. Die Summendarstellung zeigt, daß g_i nur dann mit höherer Vielfachheit in f' vorkommen kann, wenn $e_i g_i'$ von g_i geteilt wird. Da grad $g_i' <$ grad g_i, passiert dies genau dann, wenn e_i von der Charakteristik des Körpers geteilt wird. Zumindest gilt:

Satz 1.2. *Sei K ein Körper der Charakteristik 0 und $f \in K[X]$ ein nichtkonstantes normiertes Polynom. Dann ist*

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

der quadratfreie Teil von f.

Natürlich sind wir gerade an Körpern positiver Charakteristik p interessiert, für den dieser Satz keine Lösung des Problems ist. Immerhin finden wir mit h das Produkt aller irreduziblen Faktoren, deren Vielfachheit nicht von p geteilt wird. Dies erlaubt uns, f aufzuspalten in ein Produkt

$$f = f_1 f_2,$$

bei dem f_1 alle irreduziblen Faktoren aufnimmt, die auch in h vorkommen und f_2 dann eine p-te Potenz ist. Da sich p-te Wurzeln über einem endlichen Körper der Charakteristik p leicht ziehen lassen, kann man den Algorithmus vervollständigen. Wir behandeln dies in einer Übungsaufgabe.

Teile gleichen Grades. Der Algorithmus für die Zerlegung in Teile gleichen Grades beruht auf folgendem Satz:

Satz 1.3. *Das Polynom*

$$f = X^{q^e} - X$$

ist Produkt aller normierten irreduziblen Polynome aus $\mathbb{F}_q[X]$, deren Grad ein Teiler von e ist. Alle Faktoren von f sind einfach.

Beweis. Wegen $f' = -1$ ist f quadratfrei, denn jeder Faktor einer Vielfachheit ≥ 2 würde auch f'teilen. Damit ist die letzte Aussage schon bewiesen.

Sei zunächst g ein irreduzibler Teiler von f und vom Grad d. Dann zerfällt g wie sein Vielfaches f über $\mathbb{F}_{q^e}$ in Linearfaktoren. Für eine Nullstelle x_0 von g ist dann $\mathbb{F}_{q^d} = \mathbb{F}_q[x_0]$ in $\mathbb{F}_{q^e}$ enthalten. Da $\mathbb{F}_{q^e}$ also ein Vektorraum über $\mathbb{F}_{q^d}$ ist, muß q^e eine Potenz von q^d sein. Daraus folgt $d \mid e$.

Sei umgekehrt $g \in \mathbb{Z}_p$ ein irreduzibles Polynom, dessen Grad d ein Teiler von e ist. Mit $K = \mathbb{F}_q[X]/(g)$ hat man $\#K = q^d$ und $x^{q^d} = x$ für alle $x \in \mathbb{F}_q$. Da d ein Teiler von e ist, folgt $x^{q^e} = x$ für alle $x \in K$. Speziell gilt dies für eine Nullstelle x_0 von g. Da g deren Minimalpolynom und $f(x_0) = 0$ ist, folgt $g \mid f$. □

Aus diesem Satz ergibt sich sofort ein einfacher Test auf Irreduzibilität:

Korollar 1.4. *Sei $f \in \mathbb{F}_q[X]$ ein nichtkonstantes Polynom. Dann ist f genau dann irreduzibel, wenn $f \mid X^{q^e} - X$, $e = \operatorname{grad} f$, und $\operatorname{ggT}(f, X^{q^t} - X) = 1$ für alle echten Teiler t von e.*

Die Teile gleichen Grades eine quadratfreien Polynoms f über $\mathbb{F}_q$ können wir nun so finden:

Algorithmus 1.5. Teile gleichen Grades

Setze $f_0 = f$. Für $k = 1, \ldots, d = \operatorname{grad} f$ setze:

(1) $g_k = \operatorname{ggT}(f_{k-1}, X^{q^k} - X)$.
(2) $f_k = f_{k-1}/g_k$

Die Teile gleichen Grades sind dann offensichtlich $g_1, \ldots, g_d$.

Hierzu läßt sich allerdings noch einiges bemerken:

Bemerkung 1.6. (a) Die Iteration kann abgebrochen werden, wenn $2(k+1) > \operatorname{grad} f_k$. Dann muß f_k ja irreduzibel sein, denn es hat nur Teile des Grades $\geq k+1$.

(b) Bei der Bestimmung von $\operatorname{ggT}(f_{k-1}, X^{q^k} - X)$ braucht man nicht das Polynom $X^{q^k} - X$ selbst, sondern nur seinen Divisionsrest modulo f_{k-1}. Um ihn zu finden, bestimmt man zunächst den Rest von X^{q^k} modulo f_{k-1} mittels des schnellen Potenzierens modulo f^{k-1} (siehe unten) und subtrahiert dann X. Dies ist natürlich auch beim Irreduzibilitätstest 1.4 zu beachten.

(c) Das Polynom g_k ist das Produkt der irreduziblen normierten Faktoren von f (oder f_{k-1}), die Grad k haben. Jedes dieser Polynome hat Vielfachheit 1 in g_n, auch dann, wenn f selbst nicht quadratfrei ist. Man kann sich deshalb die Bestimmung des quadratfreien Teils sparen, muß dann aber dafür sorgen, daß aus f_{k-1} alle irreduziblen Teiler des Grades k herausgezogen werden. Dies kann man

etwa so machen: Wir setzen $u = f_{k-1}$ und iterieren

$$u = \frac{u}{\mathrm{ggT}(u, g_k)}$$

bis $\mathrm{ggT}(u, g_k) = 1$. Dann setzen wir $f_k = u$.

Schnelle Potenzierung. Sei R ein Ring und $x \in R$. Berechnet werden soll x^n für $n \in \mathbb{N}$. Wenn $n = 2^k$ für ein $k \in \mathbb{N}$, könne wir x^n mit k Quadrierungen bestimmen:

$$X^n = (\cdots((x^2)^2)^2 \cdots)^2$$

Also sind nur k statt der n Multiplikationen bei naivem Vorgehen notwendig. Auch bei beliebigen n hilft diese Idee weiter. Wir betrachten die Dualdarstellung

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0$$

bilden die Potenzen x^{2^i} durch fortgesetztes Quadrieren und multiplizieren diejenigen x^{2^i} mit $a_i \neq 0$ auf.

Zerlegung der Teile gleichen Grades. Es bleibt der letzte Schritt zu diskutieren, die Zerlegung von Polynomen, deren irreduzible Faktoren f_i alle den gleichen Grad d haben. Wir dürfen voraussetzen, daß d bekannt ist. Sei $r = \mathrm{grad}\, f$. Dann ist $n = r/d$ die Anzahl der irreduziblen Faktoren. Im Fall $n = 1$ ist f selbst irreduzibel. Sei also $n > 1$, $f = f_1 \cdots f_n$.

Der Algorithmus von Cantor-Zassenhaus, den wir jetzt diskutieren wollen, beruht auf dem chinesischen Restsatz, den wir hier nur für den Ring $K[X]$, $K = \mathbb{F}_q$ benötigen:

$$K[X]/(f) \cong \Big(K[X]/(f_1)\Big) \times \cdots \times \Big(K[X]/(f_n)\Big)$$

Der Isomorphismus wird gegeben durch die Abbildung

$$g \mod f \longmapsto (g \mod f_1, \ldots, g \mod f_n)$$

Wir schreiben $\pi_i(g)$ für $g \mod f_i$. Jeder der Restklassenringe $K[X]/(f_i)$ ist ein Körper mit q^d Elementen. Wir betrachten zunächst den Fall q ungerade und diskutieren $q = 2^e$ später.

Satz 1.7. *Sei q ungerade. Mit $K \cong \mathbb{F}_{q^d}$ und $r = (q^d - 1)/2$ gilt:*

(a) $x^r \in \{-1, 1\}$ *für alle* $x \in K^*$,

(b) $U := \{x \in K^* \mid x^r = 1\}$ *ist eine Untergruppe von* K^* *der Ordnung* r.

Beweis. (a) Durch Quadrieren erhält man

$$(x^r)^2 = x^{2r} = x^{\#K^*} = 1 \Longrightarrow x^r = \pm 1$$

(b) Betrachte den Endomorphismus $\varphi : K^* \to K^*, x \mapsto x^r$. Es gilt ganz allgemein für jeden Endomorphismus φ einer Gruppe G:

$$(\#\operatorname{Im}\varphi)(\#\operatorname{Ker}\varphi) = \#G.$$

Zu zeigen bleibt daher $\#\operatorname{Im}\varphi = 2$. Offenbar ist $1 \in \operatorname{Im}\varphi$. Aber das Bild enthält auch -1: Wähle zum Beweis einen Erzeuger u von K^*. Dann gilt $u^r \neq 1$, da u die Ordnung $q^d - 1 = 2r$ in K^* hat. Also muß $u^r = -1$ sein. □

Wir wählen nun $g \in K[X]$, $\operatorname{grad} g < d$, und bilden $g^r \mod f$. Dabei können drei verschiedene Fälle auftreten:

(a) $g^r \mod f = (\pi_1(g^r), \ldots, \pi_n(g^r)) = (1, \ldots, 1)$
(b) $g^r \mod f = (\pi_1(g^r), \ldots, \pi_n(g^r)) = (-1, \ldots, -1)$
(c) Es gibt ein i mit $\pi_i(g^r) = 1$ und ein $j \neq i$ mit $\pi_j(g^r) = -1$.

Wir betrachten zuerst den dritten Fall. Es gilt: $f \nmid g^r - 1$, aber $f_i \mid g^r - 1$. Mithin haben wir mit

$$\operatorname{ggT}(f, g^r - 1)$$

einen nichttrivialen Teiler von f gefunden.

Im ersten Fall ist $g^r = 1 \mod f$ und der ggT liefert nur den trivialen Teiler f. Im anderen Ausnahmefall ist $g^r - 1$ teilerfremd zu f.

Natürlich kann man nicht hoffen, bei einmaliger Wahl von g und Bestimmung von $\operatorname{ggT}(f, g^r - 1)$ bereits einen Treffer erzielt zu haben. Man wählt g *zufällig*, und das soll heißen: jedes der q^d Polynome $g \in K[X]$ mit $\operatorname{grad} g < d$ wird mit gleicher Wahrscheinlichkeit $1/q^d$ ausgewählt. Der chinesische Restsatz stellt dann sicher, daß die „Ereignisse“ $g^r \equiv 1 \mod f_i$, $i = 1, \ldots, n$, (total) unabhängig sind. Daher ist die Anzahl der Einträge 1 in $(\pi_1(g^r), \ldots, \pi_n(g^r))$ mit Bernoulli-verteilt mit dem Parameter $1/2$. Jeder der ungünstigen Fälle (a) und (b) tritt mit Wahrscheinlichkeit 2^{-n} auf, der dritte mit Wahrscheinlichkeit $1 - 2^{1-n}$.

Bei k-maliger Iteration bleiben wir daher mit Wahrscheinlichkeit $2^{-k(n-1)}$ erfolglos. Die Wahrscheinlichkeit $2^{-k(n-1)}$ für mindestens $k + 1$ Iterationen geht gegen 0 mit $k \to \infty$.

Diese Überlegungen führen zu folgendem Algorithmus, der f in das Produkt zweier echter Teiler aufspaltet. Auf diese ist dann der Algorithmus wieder anzuwenden, sofern sie nicht schon irreduzibel sind. Die Irreduzibilität kann man nun natürlich schon an dem vorab bekannten Grad der irreduziblen Teiler von f erkennen.

Algorithmus 1.8. Cantor-Zassenhaus

(1) Setze $r = (q^d - 1)/2$.
(2) Wähle zufällig ein $g \in K[X]$ mit $\operatorname{grad}(g) < \operatorname{grad}(f)$.
(3) Ist $\operatorname{ggT}(f, g) \neq 1$, dann ist $\operatorname{ggT}(f, g)$ ein echter Teiler von f. Gib die Teiler $f_1 = \operatorname{ggT}(f, g)$ und $f_2 = f/f_1$ aus und stoppe.

(4) Sei $u = \mathrm{ggT}(f, g^r - 1)$. Ist dann $u \neq f, 1$, so ist u echter Teiler von f. Gib die Teiler $f_1 = u$ und $f_2 = f/u$ aus und stoppe.
(5) Gehe zu (2).

Auch hier kann man das oben beschriebene Verfahren zur schnellen Potenzierung heranziehen.

Der Algorithmus von Cantor-Zassenhaus ist ein *probabilistischer* Algorithmus, dessen Laufzeit nicht nach oben beschränkt ist, sondern nur im Mittel oder durch eine Wahrscheinlichkeitsverteilung angegeben werden kann. Diese haben wir oben schon diskutiert.

Bei den probabilistischen Algorithmen muß man unterscheiden zwischen den Typen *Las Vegas* und *Monte Carlo*. Beim Typ Las Vegas kann man die Ausgabe auf Korrektheit prüfen, wie zum Beispiel beim Cantor-Zassenhaus-Algorithmus. Lediglich die Laufzeit ist dem Zufall unterworfen. Beim Typ Monte Carlo hingegen liefert der Algorithmus nur mit Wahrscheinlichkeit $> 1/2$ die richtige Antwort, so daß bei hinreichend häufiger Wiederholung die Fehlerwahrscheinlichkeit zwar gegen 0 geht, ein Irrtum aber nicht auszuschließen ist.

Man kann den Algorithmus von Cantor-Zassenhaus in einen deterministischen Algorithmus verwandeln, indem man über die bereits verwendeten g Buch führt, um Wiederholungen zu vermeiden. Der Aufwand lohnt sich indes nicht.

Im Fall der Charakteristik 2 ersetzt man $g^r - 1$ durch die Spur von g modulo f_i über $\mathbb{Z}_2$. Für Elemente x aus $\mathbb{F}_{2^m}$ sei

$$\mathrm{Sp}(x) = x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^2 + x = \sum_{i=1}^{m-1} x^{2^i}$$

die Spur von x über $\mathbb{F}_2$.Wir behaupten: $\mathrm{Sp}(x) \in \mathbb{F}_2$, und jeder der Werte 0 und 1 wird mit gleicher Vielfachheit angenommen.Zum Beweis zeigen wir

$$\mathrm{Sp}(x)(\mathrm{Sp}(x) - 1) = 0 \tag{1}$$

Dies folgt mit dem Teleskoptrick:

$$\mathrm{Sp}(x)(\mathrm{Sp}(x) - 1) = (x^{2^{m-1}})^2 + \cdots + x^2 + x - x^{2^{m-1}} - \cdots - x = x^{2^m} - x = 0.$$

Ferner ist $\mathrm{Sp} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ eine $\mathbb{F}_2$-lineare Abbildung! Entweder ist $\mathrm{Sp}(x) = 0$ für alle $x \in \mathbb{F}_{2^m}$, oder es gibt ein x mit $\mathrm{Sp}(x) = 1$, und dann trifft dies auf genau die Hälfte der Elemente zu, denn die Anzahl der Urbilder von 1 stimmt mit der Anzahl der Elemente des Kerns überein. Da $\mathbb{F}_{2^m}$ mehr Elemente hat, als der Grad der Spur (als Polynom) beträgt, kann diese nicht auf $\mathbb{F}_{2^m}$ überall verschwinden.

Zur Anwendung im Cantor-Zassenhaus-Algorithmus wählen wir $m = \mathrm{grad}\, f_i$ und ersetzen $\mathrm{ggT}(f, g^r - 1)$ durch $\mathrm{ggT}(f, \mathrm{Sp}(g))$, wobei die Spur mit dem Exponenten m zu bilden ist, denn wir haben ja die Restklasse von g modulo f_i zu betrachten und $\mathbb{F}_2[X]/(f_i) \cong \mathbb{F}_{2^m}$.

Es sei hinzugefügt, daß die oben definierte Spur mit dem in der Linearen Algebra für Matrizen und lineare Abbildungen definierten Begriff in folgender Weise zusammenhängt: $\mathrm{Sp}(x)$ ist gerade die Spur der durch Multiplikation mit x gegebenen $\mathbb{F}_2$-linearen Abbildung auf $\mathbb{F}_{2^m}$. Wir verzichten darauf, dies hier zu beweisen.

Weiterführende Lektüre: [**MCA**]

ABSCHNITT 2

Resultante und Diskriminante

Resultante und Diskriminante sind wichtige Hilfsmittel für das Rechnen mit Polynomen. In den folgenden Abschnitten diskutieren wir, wie sich die Berechnung des ggT oder die Faktorisierung von Polynomen über $\mathbb{Z}$ auf entsprechende Rechnungen modulo p reduzieren lassen. Dabei muß man zum Beispiel kontrollieren können, daß die Bildung des ggT mit der Restklassenbildung modulo p kommutiert. Dies ist mit Hilfe der Resultante möglich.

Ihren Ursprung hat die Resultante in der Lösung polynomialer Gleichungssysteme. Wir diskutieren dies im einfachsten Fall von zwei Polynomen in zwei Unbestimmten.

Resultante und Sylvester-Matrix. Sei K ein beliebiger Körper. Ob zwei Polynome $f = \sum_{i=1}^{n} f_i X^i$ und $g = \sum_{i=1}^{m} g_i X^i \in K[X]$ positiven Grades einen gemeinsamen Faktor haben, kann man mit euklidischen Algorithmus prüfen, der dann ja sogar den ggT ermittelt. Überraschenderweise kann man dies aber auch durch Auswertung eines Polynoms in den Koeffizienten von f und g erkennen:

Satz 2.1. *Für Polynome $f, g \in K[X]$ mit $n = \operatorname{grad} f > 0$ und $m = \operatorname{grad} g > 0$ sind äquivalent:*

(a) $\operatorname{ggT}(f, g) = 1$.

(b) *Es gibt $a, b \in K[X]$, $\operatorname{grad} a < \operatorname{grad} g$, $\operatorname{grad} b < \operatorname{grad} f$ mit $af + bg = 1$.*

(c) *Die Gleichung $sf + tg = 0$ besitzt keine nichttriviale Lösung mit $s, t \in K[X]$, $\operatorname{grad} s < \operatorname{grad} g$, $\operatorname{grad} t < \operatorname{grad} f$.*

(d) $\det \operatorname{Sylv}(f, g) \neq 0$. *Dabei ist* $\operatorname{Sylv}(f, g)$ *die sogenannte* Sylvester-Matrix. *Sie hat die Form*

$$\operatorname{Sylv}(f,g) = \underbrace{\begin{pmatrix} f_n & & & g_m & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & f_n & \vdots & & g_m \\ \vdots & & \vdots & \vdots & & \vdots \\ f_0 & & \vdots & g_0 & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_0 & & & g_0 \end{pmatrix}}_{m \text{ Spalten}} \underbrace{\qquad\qquad}_{n \text{ Spalten}}$$

(e) *f und g haben keine gemeinsame Nullstelle in $\overline{K}$.*

Beweis. (e) $\Longleftrightarrow$ (b): Aus dem euklidischen Algorithmus ist ersichtlich, daß der größte gemeinsame Teiler von f und g sich bei Übergang zu $\overline{K}$ nicht ändert. Wenn also f und g über K teilerfremd sind, sind sie es auch über $\overline{K}$. Die Umkehrung ist trivial.

(b) $\Rightarrow$ (a): Dies ist klar: jeder gemeinsame Teiler von f und g teilt 1, ist also eine Einheit.

(a) $\Rightarrow$ (b) Nach dem Lemma von Bézout wissen wir, daß es eine Darstellung $1 = af + bg$ gibt. Wir müssen uns aber noch überzeugen, daß die Gradbedingung erfüllbar ist. Dazu teilen wir a durch g mit Rest: $a = qg + r$ mit $\operatorname{grad} r < \operatorname{grad} g$. Dann ist

$$1 = af + bg = rf + (qf + b)g.$$

Wir können nun a durch r ersetzen. Durch Gradbetrachtung folgt $\operatorname{grad}(qf + b) < \operatorname{grad} f$.

(a) $\Longleftrightarrow$ (c): Gilt $sf = -tg$ für s, t wie in (c) gefordert, dann muß g, wenn es teilerfremd zu f ist, ein Teiler von s sein, was bei $\operatorname{grad} s < \operatorname{grad} g$ nicht möglich ist.

Sind umgekehrt f und g nicht teilerfremd, erhalten wir die geforderte Gleichung aus $gf = -fg$, indem wir $s = g/\operatorname{ggT}(f, g)$, $t = f/\operatorname{ggT}(f, g)$ setzen.

(c) $\Longleftrightarrow$ (d): Betrachte die Untervektorräume

$$U = \{h \in K[X] \mid \operatorname{grad} h < m\}, \quad V = \{h \in K[X] \mid \operatorname{grad} h < n\}$$
$$W = \{h \in K[X] \mid \operatorname{grad} h < m + n\}.$$

Die Abbildung

$$\varphi : U \times V \to W, \quad (s, t) \mapsto sf + tg$$

ist K-linear. Offenbar wird φ bezüglich der Basen

$$\{X^{m-1}, \ldots, 1\} \quad , \{X^{n-1}, \ldots, 1\}, \quad \{X^{m+n-1}, \ldots, 1\}$$

gerade durch Sylvester-Matrix dargestellt. Es ist also φ injektiv genau dann, wenn $\det \operatorname{Sylv}(f, g) \neq 0$ ist. Die Bedingung in (c) ist gerade die Injektivität von φ. □

Es ist nützlich und wichtig, Resultanten auch dann zu betrachten, wenn der Koeffizientenbereich kein Körper ist.

Definition. Sei R ein kommutativer Ring, $f, g \in R[X]$. Dann heißt $\operatorname{Sylv}(f, g)$ wie oben definiert die *Sylvester-Matrix* von f und g. Die Determinante der Sylvester-Matrix nennt man *Resultante* $\operatorname{Res}(f, g)$. Speziell heißt $\operatorname{Res}(f, f') = \operatorname{Disk}(f)$ die *Diskriminante* von f.

Es gilt

$$\operatorname{Disk}(f) = 0 \Longleftrightarrow f \text{ hat in } \overline{K} \text{ eine doppelte Nullstelle.}$$

Dies folgt aus Satz 2.1, denn die (mindestens) doppelten Nullstellen von f sind ja die gemeinsamen Nullstellen von f und f'.

Beispiel 2.2. Sei $f = aX^2 + bX + c$ mit $a \neq 0$, also grad $f = 2$. Es gilt dann

$$\mathrm{Disk}(f) = -a(b^2 - 4ac)$$

Dies ist gerade die Diskriminante, wie sie aus der „pq-Formel“ bekannt ist.

Zur Ergänzung setzen wir

$$\begin{aligned} \mathrm{Res}(f, g) &= 1, && \text{falls } f, g \in R \setminus \{0\}, \\ \mathrm{Res}(f, 0) = \mathrm{Res}(0, f) &= 0, && \text{falls } f = 0 \text{ oder grad } f > 0, \\ \mathrm{Res}(f, 0) = \mathrm{Res}(0, f) &= 1, && \text{falls } f \in R \setminus \{0\}. \end{aligned}$$

Wenn $R = K$ ein Körper ist, gilt die Äquivalenz von i),iv),v) von Satz 2.1 dann für alle $f, g \in K[X]$.

Die Resultante ist antisymmetrisch in f und g: Für f, g mit grad f, grad $g > 0$ gilt

$$\mathrm{Res}(g, f) = (-1)^{(\mathrm{grad}\, f)(\mathrm{grad}\, g)} \mathrm{Res}(f, g)$$

Bei den Anwendungen von Satz 2.1, die wir im folgenden diskutieren, ist der Koeffizientenbereich der Polynome kein Körper, sondern einer der euklidischen Ringe $\mathbb{Z}$ oder $K[Y]$, wobei K ein Körper ist. In diesem Fall schwächt sich der Zusammenhang zwischen Teilerfremdheit und Nichtverschwinden der Diskriminante natürlich etwas ab:

Satz 2.3. *Sei R ein faktorieller Integritätsbereich und seien $f, g \in R[X] \setminus \{0\}$. Dann sind äquivalent:*

(a) $\mathrm{Res}(f, g) = 0$,
(b) $\mathrm{ggT}(f, g) \notin R$.

Beweis. Sei u ein Polynom in $R[X]$, $u \neq 0$. Dann können wir u zerlegen in der Form

$$u = p_1 \cdots p_k q_1 \cdots q_l$$

wobei $p_1, \ldots, p_k$ Primelemente in R sind und $q_1, \ldots, q_l$ primitive, irreduzible Polynome. Dabei heißt q *primitiv*, wenn 1 der größte gemeinsame Teiler der Koeffizienten ist. Nach dem Lemma von Gauß sind die Polynome $q_1, \ldots, q_l$ auch irreduzibel über dem Quotientenkörper K von R. Ist umgekehrt $r = a_n X^n + \cdots + a_0$ ein irreduzibles Polynom über K, so ist $s \cdot r$ für den Hauptnenner s der Koeffizienten ein primitives, irreduzibles Polynom über R.

Daraus ergibt sich: $\mathrm{ggT}(f, g) \notin R$ genau dann, wenn f, g als Elemente von $K[X]$ nicht teilerfremd sind. Letzteres ist nach Satz 2.1 äquivalent zu $\mathrm{Res}(f, g) = 0$. Die Resultante ändert sich ja nicht, wenn wir von R zu K übergehen. □

Resultante und Elimination. Die Resultante ist erfunden worden als ein Hilfsmittel zum Lösen polynomialer Gleichungssysteme, also der Bestimmung der gemeinsamen Nullstellenmenge von mehreren Polynomen in mehreren Unbestimmten. Dabei verwenden wir folgende Bezeichnung: Für einen Körper K und Polynome $f_1, \ldots, f_m \in R = K[X_1, \ldots, X_n]$ ist

$$\mathcal{V}(f_1, \ldots, f_m) = \{x \in K^n : f_1(x) = \cdots = f_m(x) = 0\}$$

die gemeinsame Nullstellenmenge oder *Varietät*. Für das von $f_1, \ldots, f_m$ erzeugte Ideal verwenden wir die klassische Schreibweise

$$(f_1, \ldots, f_m) = \left\{ \sum_{i=1}^{m} a_i f_i : a_i \in R \right\}.$$

Wir beschränken uns im folgenden auf den Fall zweier Polynome in zwei Veränderlichen $f, g \in K[X, Y]$. Dann ist $\mathcal{V}(f, g)$ gerade der Durchschnitt der durch die Gleichungen $f(x, y) = 0$ und $g(x, y) = 0$ definierten ebenen Kurven.

Eine sehr vernünftige Strategie zur Bestimmung von $\mathcal{V}(f, g)$ ist folgendes Vorgehen:

(a) Man versucht zunächst, ein $h \in (f, g) \cap K[X]$, $h \neq 0$, zu finden.
(b) Man bestimmt die (endlich vielen) Nullstellen von h, etwa $x_1, \ldots, x_q$.
(c) Man setzt die x_i der Reihe nach für X in f und g ein, so daß man Polynome f_i, g_i in nur noch einer Unbestimmten, nämlich Y, erhält. Deren gemeinsame Nullstellen $y_{i,j}$ ergeben dann mit den x_i die gemeinsamen Nullstellen (x_i, y_{ij}) von f und g, also gerade $\mathcal{V}(f, g)$.

Daß diese Strategie greift, sobald man h gefunden hat, ist klar: Es gibt ja eine Darstellung $h = af + bg$, so daß $h(x, y) = h(x) = 0$, sobald $f(x, y) = g(x, y) = 0$. Es gehen uns also keine gemeinsamen Nullstellen von f und g verloren: Unter den Nullstellen von h kommen die x-Komponenten der gemeinsamen Nullstellen von f und g wirklich alle vor.

Das Ideal $(f, g) \cap K[X]$ heißt *Eliminationsideal* von (f, g) *bezüglich* Y. Da $K[X]$ ein Hauptidealbereich ist, wird es (in unserem Fall) von einem einzigen Polynom erzeugt.

Mit $S = K[X]$ ist $K[X, Y] \cong S[Y]$. Wir können also die Resultante von f und g als Polynome über S bilden. Wir nennen sie die *Y-Resultante* $\mathrm{Res}_Y(f, g)$ von f und g. Entsprechend ist die X-Resultante definiert. Wie der nächste Satz zeigt, ist die Y-Resultante ein Element des Eliminationsideals und damit ein geeignetes Element für die Anwendung der obigen Strategie.

Satz 2.4. *Sei R ein Integritätsbereich und seien $f, g \in R[X]$ Polynome positiven Grad. Dann existieren $a, b \in R[X]$, $a, b \neq 0$ mit* $\operatorname{grad} a < \operatorname{grad} g$, $\operatorname{grad} b < \operatorname{grad} f$ *und*

$$\mathrm{Res}(f, g) = af + bg.$$

Beweis. Im Fall $\operatorname{Res}(f,g)=0$ wählen wir $a=b=0$. Sei nun $\operatorname{Res}(f,g)\neq 0$. Wir gehen zunächst zum Körper K der Brüche von R über. Man betrachte die Abbildung $\varphi : U\times V\to W$, wie sie im Beweis zum Satz 2.1 definiert war. Nach Voraussetzung gilt $\operatorname{ggT}(f,g)=1$ und nach Satz 2.1 ist $1\in W$. Das Gleichungssystem

$$\operatorname{Sylv}(f,g)\begin{pmatrix}a\\ b\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix}$$

hat also eine Lösung. Die Cramersche Regel liefert:

$$a=\frac{\tilde{a}}{\operatorname{Res}(f,g)},\quad b=\frac{\tilde{b}}{\operatorname{Res}(f,g)},\qquad \tilde{a},\tilde{b}\in R[X].$$

Multiplikation mit $\operatorname{Res}(f,g)$ ergibt die gewünschte Darstellung. □

Im allgemeinen erzeugt $\operatorname{Res}_Y(f,g)$ das Eliminationsideal $(f,g)\cap K[X]$ nicht. Inwieweit $\operatorname{Res}_Y(f,g)$ geometrisch davon abweicht, zeigt der folgende Satz.

Satz 2.5. *Sei K ein algebraisch abgeschlossener Körper und seien $f,g\in K[X,Y]$ mit $f=\sum^n f_iY^i$, $g=\sum^m g_iY^i$, $f_i,g_i\in K[X]$, $f_n,g_m\neq 0$, $n,m\geq 1$. Ist $\pi : K^2\to K$, $(a,b)\mapsto a$ die Projektion auf die erste Koordinate, dann gilt:*

$$\mathcal{V}(\operatorname{Res}_Y(f,g))=(\mathcal{V}(f_n)\cap\mathcal{V}(g_m))\cup\pi(\mathcal{V}(f,g)).$$

Beweis. Sei $x_0\in\pi(\mathcal{V}(f,g))$. Dann gilt $h(x_0)=0$ für alle $h\in(f,g)\cap K[X]$, speziell auch $\operatorname{Res}_Y(f,g)(x_0)=0$. Ist stattdessen $x_0\in\mathcal{V}(f_n)\cap\mathcal{V}(g_m)$, dann hat die Sylvester-Matrix nach Einsetzen von x_0 eine Nullzeile in der ersten Zeile und also verschwindet ihre Determinante $\operatorname{Res}_Y(f,g)(x_0)$.

Sei umgekehrt $x_0\in\mathcal{V}(\operatorname{Res}_Y(f,g))$ und $x_0\notin\mathcal{V}(f_n)$. In f,g eingesetzt erhält man Polynome in Y:

$$\tilde{f}=f(x_0,Y),\quad \tilde{g}=g(x_0,Y).$$

Dabei gilt $\operatorname{grad}\tilde{f}=\operatorname{grad}_Y f=n$.

Ist dann $\tilde{g}=0$ wählen wir $y_0\in K$ als Nullstelle von $\tilde{f}$. Dies ist möglich, da K algebraisch abgeschlossen ist, und wir erhalten $(x_0,y_0)\in\mathcal{V}(f,g)$.

Ist $g_m(x_0)\neq 0$, dann gilt $\operatorname{grad}\tilde{g}=\operatorname{grad}_Y g=m$ und Substitution kommutiert mit Bilden der Sylvester-Matrix. (Achtung: Dies gilt nicht immer!) Also ist

$$\operatorname{Sylv}(\tilde{f},\tilde{g})=(\operatorname{Sylv}_Y(f,g))(x_0)$$

und damit

$$\operatorname{Res}(\tilde{f},\tilde{g})=(\operatorname{Res}_Y(f,g))(x_0)=0.$$

Somit haben $\tilde{f}$ und $\tilde{g}$ eine gemeinsame Nullstelle. Wiederum ist $x_0\in\pi(\mathcal{V}(f,g))$.

Als dritten Fall betrachten wir $\tilde{g} \neq 0$, $g_m(x_0) = 0$. sei $k = \operatorname{grad} \tilde{g} < m$. Dann enthält die Sylvester-Matrix von f und g die Sylvester-Matrix von $\tilde{f}$ und $\tilde{g}$ als Submatrix. Es folgt

$$0 = \operatorname{Res}_Y(f,g)(x_0) = f_n(x_0)^{m-k} \cdot \operatorname{Res}(\tilde{f}, \tilde{g}).$$

Man argumentiert nun weiter wie im zweiten Fall. □

Im Sinne unserer obigen Strategie besagt Satz 2.5: Wenn wir für h die Y-Resultante wählen, so besteht die Nullstellenmenge von h zum einen aus den x-Komponenten der gemeinsamen Nullstellen von f und g – an diesen sind wir interessiert – und zusätzlich aus den gemeinsamen Nullstellen der Leitkoeffizienten von f und g, als Polynome in Y betrachtet.

Zumindest in einem Spezialfall können wir eine schärfere Aussage machen:

Satz 2.6. *Bei gleichen Voraussetzungen wie oben sei $f_n \in K$ oder $g_m \in K$, also einer der beiden Leitterme eine Konstante. Ferner sei $h \in K[X]$ ein Erzeuger des Eliminationsideals $(f,g) \cap K[X]$. Dann gilt:*

$$\mathcal{V}(\operatorname{Res}_Y(f,g)) = \pi(\mathcal{V}(f,g)) = \mathcal{V}(h).$$

Beweis. Die erste Gleichung folgt mit Satz 2.5 aus $\mathcal{V}(f_n) \cap \mathcal{V}(g_m) = 0$. Ferner hat man

$$\mathcal{V}(h) \supset \pi(\mathcal{V}(f,g)) = \mathcal{V}(\operatorname{Res}_Y(f,g)) \supset \mathcal{V}(h). \qquad \square$$

Die beiden vorangegangenen Sätze lassen sich auf Polynome in mehr als zwei Veränderlichen verallgemeinern. Wir verweisen dazu auf [**IVA**].

Der Satz von Bézout. Dieser klassische Satz macht eine Aussage über die Anzahl der gemeinsamen Nullstellen zweier Polynome in zwei Veränderlichen. In ihm bezeichnet grad den Totalgrad:

$$\operatorname{grad}\Big(\sum_{i,j=1}^{n} f_{ij} X^i Y^j\Big) = \max\{i + j : f_{ij} \neq 0\}.$$

Satz 2.7 (Bézout)**.** *Sei K ein Körper und seien $f, g \in K[X,Y]$ teilerfremd. Dann gilt:*

$$\#\mathcal{V}(f,g) \leq \operatorname{grad} f \cdot \operatorname{grad} g.$$

Beweis. Wir können annehmen, daß K algebraisch abgeschlossen ist, denn beim Übergang zum algebraischen Abschluß können höchstens Nullstellen dazu kommen und die Teilerfremdheit bleibt erhalten.

Im Beweis verwenden wir lineare Koordinatentransformationen

$$\tilde{X} = aX + bY, \quad \tilde{Y} = cX + dY, \qquad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0.$$

Zunächst zerlegen wir f in die Summe seiner homogenen Bestandteile:

$$f = h_0 + \cdots + h_n, \quad n = \operatorname{grad} f, \quad h_i \text{ homogen vom Grad } i.$$

Nun transformieren wir die Koordinaten so, daß in

$$h_n = a_n \tilde{Y}^n + a_{n-1} \tilde{Y}^{n-1} \tilde{X} \cdots + a_0 \tilde{X}^n, \quad a_i \in K,$$

der Leitkoeffizient nicht verschwindet, also $a_n \neq 0$ gilt. Der $\tilde{Y}$-Leitkoeffizient von f ist dann also eine Konstante in K und hängt nicht von $\tilde{X}$ ab. Wir schreiben nun X für $\tilde{X}$ und Y für $\tilde{Y}$. Es folgt

$$\mathcal{V}(\operatorname{Res}_Y(f, g)) = \pi(\mathcal{V}(f, g)).$$

Aus der Teilerfremdheit ergibt sich $\operatorname{Res}_Y(f, g) \neq 0$ und also $\#\mathcal{V}(\operatorname{Res}_Y(f, g)) < \infty$. Sei $x_0 \in \mathcal{V}(\operatorname{Res}_Y(f, g))$. Dann hat $f(x_0, Y)$ nur endliche viele Nullstellen in K, d. h. $\mathcal{V}(f, g)$ ist endlich.

Weiterhin gilt

$$\operatorname{grad} \operatorname{Res}_Y(f, g) \leq (\operatorname{grad} f)(\operatorname{grad} g),$$

wie man durch Berechnen der Determinante mit dem Laplaceschen Entwicklungssatz leicht bestätigt. Es folgt

$$\#\pi(\mathcal{V}(f, g)) \leq (\operatorname{grad} f)(\operatorname{grad} g).$$

Man wähle nun eine Koordinatentransformation so, daß π injektiv wird (und unsere schon erreichte Voraussetzung über f nicht zerstört wird). Dazu nimmt eine Projektionsrichtung, so daß auf Geraden parallel dazu nicht zwei gemeinsame Nullstellen von f und g gleichzeitig liegen. Dann ändert die Projektion die Anzahl der Nullstellen nicht, d. h. $\#\pi(\mathcal{V}(f, g)) = \#\mathcal{V}(f, g)$. □

Man muß sich natürlich überzeugen, daß die geforderten Koordinatentransformationen auch wirklich existieren. Dabei benutzt man, daß algebraisch abgeschlossenen Körper unendlich viele Elemente haben. Die Einzelheiten überlassen wir einer Übungsaufgabe.

Man kann mit Hilfe der Resultante sogar zeigen, daß in Satz 2.7 Gleichheit gilt, wenn man

(a) voraussetzt, daß K algebraisch abgeschlossen ist,
(b) die Nullstellen mit ihrer Vielfachheit zählt (diese ist dann noch zu definieren) und
(c) auch die Nullstellen „im Unendlichen“ berücksichtigt.

Ferner läßt sich der Satz auf n Polynome in n Veränderlichen erweitern (wobei dann die Teilerfremdheit in richtiger Weise zu fassen ist).

Weiterführende Literatur: [**IVA**]

ABSCHNITT 3

Abschätzungen für Teiler und Resultante

Bei manchen Problemen für Polynome $f_1, \ldots, f_n \in \mathbb{Z}[X]$ ist es notwendig, bei anderen zumindest zweckmäßig, sich eines *modularen Algorithmus* zu bedienen:

(a) Wähle $m \in \mathbb{Z}$ „hinreichend“ groß.
(b) Reduziere die f_i modulo m.
(c) Löse das Problem modulo m.
(d) „Lifte“ die Lösung nach $\mathbb{Z}[X]$.

Das gilt analog für das Rechnen mit Polynomen über $\mathbb{Z}$ in mehreren Unbestimmten, aber auch für Polynome aus $K[X, Y]$, wobei $K[X]$ die Rolle von $\mathbb{Z}$ spielt und $m \in K[X]$ ein Polynom „großen“ Grades ist. Wir konzentrieren uns im folgenden auf $\mathbb{Z}[X]$.

Für m wählt man je nach Aufgabenstellung

(1) eine „große“ Primzahl p,
(2) eine Primzahlpotenz p^e, p „klein“,
(3) ein Produkt $p_1 \cdots p_r$ von „kleinen“ Primzahlen.

Die einfachsten Schritte im obigen Schema sind (b) und (d). Geliftet werden Polynome modulo m mittels des vollständigen Repräsentantensystems:

$$\left\{ a \in \mathbb{Z} \;\middle|\; -\frac{m}{2} < a \leq \frac{m}{2} \right\}.$$

Dadurch erhält man betragsmäßig kleine Zahlen beider Vorzeichen. Der Algorithmus ist erfolgreich, d. h. liefert die wahre Lösung des Problems, wenn $|a| < m/2$ gilt für alle Koeffizienten a der Lösung modulo m.

Wenn es zum Beispiel darum geht, das Polynom f zu faktorisieren, brauchen wir Schranken für die Koeffizienten der potentiellen Teiler von f. Nur dann können wir abschätzen, wie m zu wählen ist, damit der Erfolg sicher ist. Ob es in der Praxis sinnvoll ist, m von vornherein so groß zu wählen, ist eine andere Frage, die wir noch diskutieren werden.

Schranken für Teiler. Für uns von Interesse sind Schranken für Teiler und Resultante. Wir beginnen mit den Teilern. Es ist zweckmäßig, das Problem direkt für Polynome $f \in \mathbb{C}[X]$ anzugehen. Sei $f = \sum_{i=0}^{n} f_i X^i \in \mathbb{C}[X]$, $f_i \in \mathbb{C}$. Wir wollen Aussagen über die „Größe“ von f machen, um diese Erkenntnisse auf Teiler und Resultante anzuwenden. Wir bedienen uns dafür einiger Normen, die wir

durch Anwendung geläufiger Vektornormen auf die Koeffizientenvektoren gewinnen:

$$\|f\|_2 = \left(\sum_{i=1}^{n} |f_i|^2\right)^{\frac{1}{2}},$$
$$\|f\|_1 = \sum_{i=1}^{n} |f_i|,$$
$$\|f\|_\infty = \max\{|f_i| : i = 0, \ldots, n\}.$$

Zwischen den Normen bestehen folgende Abschätzungen, woraus man leicht die Äquivalenz aller drei Normen (bei beschränktem Grad der betrachteten Polynome) folgert:

$$\|f\|_\infty \le \|f\|_1 \le (n+1)\|f\|_\infty,$$
$$\|f\|_\infty \le \|f\|_2 \le (n+1)^{1/2}\|f\|_\infty,$$
$$\|f\|_2 \le \|f\|_1.$$

Ein weiteres Maß für die Größe von Polynomen sind die Abstände der Nullstellen $z_1, \ldots, z_n$ vom Nullpunkt. Da diese nicht vom Leitkoeffizienten abhängen, müssen wir ihn als zusätzlichen Faktor berücksichtigen. Wir setzen

$$M(f) = |f_n| \cdot \prod_{i=1}^{n} \max(1, |z_i|).$$

Dieses Größenmaß erlaubt es uns sofort, ein Polynom f mit seinen Teilern g zu vergleichen. Die Nullstellen von g sind ja auch Nullstellen von f, so daß

$$M(g) \le \left|\frac{g_m}{f_n}\right| M(f). \tag{2}$$

(Dabei sei g_m der Leitkoeffizient von g). Dies würde uns nicht viel nützen, wenn man $M(f)$ nicht zu den oben eingeführten Normen in Verbindung setzen könnte. Daß dies überraschenderweise aber geht, zeigt ein klassischer Satz der Funktionentheorie.

Satz 3.1 (Landausche Ungleichung)**.** *Für alle $f \in \mathbb{C}[X]$ gilt*

$$M(f) \le \|f\|_2.$$

Für den Beweis brauchen wir

Lemma 3.2. *Für $f \in \mathbb{C}[X]$ und $z \in \mathbb{C}$ gilt*

$$\|(X - z)f\|_2 = \|(\overline{z}X - 1)f\|_2.$$

Beweis. Im folgenden sei mit $\|\cdot\|$ stets die 2-Norm bezeichnet. Man rechnet nun nach:

$$\begin{aligned}\|(X-z)f\|^2 &= \sum_{i=0}^{n+1} |f_{i-1} - zf_i|^2 \qquad (f_{-1} = f_{n+1} = 0)\\ &= \sum_{i=0}^{n+1} (f_{i-1} - zf_i)(\overline{f_{i-1}} - \overline{z}\,\overline{f_i})\\ &= \|f\|^2(1+|z|^2) - \sum_{i=0}^{n+1} z\,\overline{f_{i-1}} f_i + \overline{z}\,\overline{f_i} f_{i-1}\\ &= \sum_{i=0}^{n+1} (\overline{z} f_{i-1} - f_i)(z\,\overline{f_{i-1}} - \overline{f_i}) = \|(\overline{z}X - 1)f\|^2. \qquad \square\end{aligned}$$

BEWEIS DER LANDAUSCHEN UNGLEICHUNG. Seien $z_1, \ldots, z_n$ die Nullstellen von f. Wir sortieren sie so, daß $|z_1|, \ldots, |z_k| > 1$, $|z_{k+1}|, \ldots, |z_n| \le 1$. Dann ist offenbar $M(f) = |f_n z_1 \cdots z_k|$. Mit

$$g = f_n \Big(\prod_{i=0}^{k} (\overline{z_i} X - 1) \Big) \Big(\prod_{j=k+1}^{n} (X - z_j) \Big)$$

gilt folgende Abschätzung:

$$M(f)^2 = |f_n \overline{z_1} \cdots \overline{z_k}|^2 = |g_n|^2 \le \|g\|^2 = \left\| \frac{g}{\overline{z_1} X - 1} (X - z_1) \right\| = \cdots = \|f\|^2$$

Dabei schließt man die Lücke, indem man das Lemma noch $k-1$ mal anwendet. $\square$

Als Gegenstück zur Landauschen Ungleichung erhalten wir

Satz 3.3. *Sei $h = h_0 + \cdots + h_m X^m$, $h_m \neq 0$. Dann ist*

$$\|h\|_\infty \le \|h\|_2 \le \|h\|_1 \le 2^m M(h).$$

Beweis. Seien u_i, $i = 1 \ldots m$ die Nullstellen von h, also $h = h_m \prod_i (X - u_i)$. Die Regel von Vieta liefert dann eine Darstellung der h_i als elementarsymmetrische Polynome in den u_i:

$$h_i = (-1)^{m-i} h_m \sum_{\substack{S \subset \{1,\ldots,m\} \\ \#S = m-i}} \prod_{j \in S} u_j.$$

Es folgt

$$|h_i| \le |h_m| \sum_{\substack{S\subset\{1,\dots,m\}\\ \#S=m-i}} \prod_{j\in S} |u_j| \le \binom{m}{i} M(h),$$

$$\|h\|_2 \le \|h\|_1 = \sum_{j=0}^{m} |h_j| \le M(h)\cdot \sum_{i=0}^{m} \binom{m}{i} = 2^m M(h). \qquad \square$$

Damit können wir nun die Teiler von f abschätzen.

Korollar 3.4. *Sei $h = h_0 + \cdots + h_m X^m$, $h_m \neq 0$, ein Teiler von f. Dann gilt*

$$\|h\|_\infty \le \|h\|_2 \le \|h\|_1 \le 2^m M(h) \le 2^m \left|\frac{h_m}{f_n}\right| \|f\|_2.$$

Dies ergibt sich direkt durch Zusammensetzen der Ungleichungen in Satz 3.1, Satz 3.3 und (2).

In Korollar 3.4 stört h_m auf der rechten Seite der Ungleichung. Für Polynome in $\mathbb{Z}[X]$ können wir es leicht beseitigen und noch eine gewisse Verbesserung durch simultane Betrachtung zweier Teiler erhalten.

Satz 3.5 (Faktorschranke von Mignotte)**.** *Für $f, g, h \in \mathbb{Z}[X]$ mit* grad $f = n \ge 1$, grad $g = m$, grad $h = k$ *und $gh \mid f$ gilt:*

$$\|g\|_\infty \|h\|_\infty \le 2^{m+k} \|f\|_2 \le 2^{m+k} (n+1)^{1/2} \|f\|_\infty,$$
$$\|h\|_\infty \le 2^k (n+1)^{1/2} \|f\|_\infty.$$

Beweis. Aus 3.3 und der Landauschen Ungleichung ergibt sich

$$\begin{aligned}\|g\|_1 \|h\|_1 &\le 2^{m+k} M(g) M(h) \le 2^{m+k} M(f)\\ &\le 2^{m+k} \|f\|_2 \le 2^{m+k} (n+1)^{1/2} \|f\|_\infty.\end{aligned}$$

Dabei haben wir benutzt, daß $M(f) = M(g)M(h)M(q)$für $f = ghq$. Ferner ist $M(q) \ge 1$ für $q \in \mathbb{Z}[X]$. Für die letzte Ungleichung verwenden wir nur,$\|f\|_2 \le (n+1)^{1/2}\|f\|_\infty$.

Die zweite Aussage folgt aus der ersten mit $g = 1$. $\square$

Schranken für die Resultante. Wir schätzen nun die Resultante zweier Polynome $f, g \in \mathbb{Z}[X]$ ab. Da diese per Definition eine Determinante ist, brauchen wir eine eine Abschätzung für Determinanten.

Sei $A = (a_{ij})$ eine $n \times n$-Matrix mit Einträgen aus $\mathbb{C}$. Die Entwicklung der Determinante ergibt dann folgende sehr grobe Abschätzung:

$$|\det A| \le n! \, \|A\|_\infty^n.$$

Eine bessere obere Schranke liefert der folgende Satz.

Satz 3.6 (Ungleichung von Hadamard)**.** *Sei $A \in \mathbb{C}^{n\times n}$, und seien $v_1, \ldots, v_n$ die Spalten von A. Dann gilt:*

$$|\det A| \leq \|v_1\|_2 \cdots \|v_n\|_2 \leq n^{n/2}\|A\|_\infty^n$$

Beweis. Ist $\det A \neq 0$, dann bilden die Spalten von A eine Basis des $\mathbb{C}^n$. Diese orthonormalisiere man mit dem Gram-Schmidt-Verfahren. Dabei erhält man

$$AT = B$$

mit einer Matrix B, deren Spalten eine Orthonormalbasis $w_1, \ldots, w_n$ von $\mathbb{C}^n$ bilden. Die Matrix T ist die Transformationsmatrix. Beim Orthonormalisierungsverfahren wählt man induktiv

$$w_k = \frac{v_k - \pi_k(v_k)}{\|v_k - \pi_{k-1}(v_k)\|_2},$$

wobei π_{k-1} die orthonormale Projektion auf den von $v_1, \ldots, v_{k-1}$ erzeugten Unterraum des $\mathbb{C}^n$ bezeichnet ($\pi_1 = 0$). Also ist T eine obere Dreiecksmatrix mit Diagonaleinträgen

$$t_{kk} = \frac{1}{\|v_k - \pi_{k-1}(v_k)\|_2} \geq \frac{1}{\|v_k\|_2}.$$

Da $(\det A)(\det T) = \det B$ und $\det B = 1$, folgt $\det A = (\det T)^{-1}$ und daraus die Behauptung, denn $\det T = \prod_{k=1}^n t_{kk}$.

Bei der zweiten Ungleichung berücksichtigen wir, daß $\|v_k\|_2 \leq n^{1/2}\|v_k\|_\infty$. □

Dieses Ergebnis wird im folgenden zur Abschätzung der Resultante verwandt:

Satz 3.7. *Seien $f, g \in \mathbb{C}[X]$ mit* grad $f = n$, grad $g = m \geq 1$. *Dann gilt:*

$$|\operatorname{Res}(f, g)| \leq \|f\|_2^m \|g\|_2^n \leq (n+1)^{m/2}(m+1)^{n/2}\|f\|_\infty^m \|g\|_\infty^n.$$

Beweis. Die zweite Ungleichung ergibt sich direkt aus Abschätzungen von 2-Norm und ∞-Norm. Die erste Ungleichung folgt aus dem obigen Satz durch Anwendung auf die Sylvestermatrix. □

Im folgenden seien stets zwei primitive Polynome $f, g \in \mathbb{Z}[X]$ gegeben, deren ggT zu bestimmen ist. Man kann dazu natürlich in $\mathbb{Q}[X]$ (mit Nennern) oder in $\mathbb{Z}[X]$ (nach Beseitigen der Nenner) rechnen. Dabei tritt jedoch häufig ein unangenehmer Effekt auf: Die Aufblähung von Zwischenergebnissen, an denen man gar nicht interessiert ist. Deshalb bietet sich ein modularer Ansatz an, der das richtige Endergebnis liefert und bei dem die Größe der Zwischenergebnisse unter Kontrolle bleibt. Sei

$$h = \operatorname{ggT}(f, g).$$

Dann sind f/h und g/h teilerfremde primitive Polynome. Sei weiter $p \in \mathbb{Z}$ eine Primzahl und $\bar{\cdot}$ die Reduktion modulo p. Es gilt dann offensichtlich

$$\overline{h} \mid \mathrm{ggT}(\overline{f}, \overline{g})$$

Aber um $\overline{h} = \mathrm{ggT}(\overline{f}, \overline{g})$ zu bekommen, brauchen wir, daß $\overline{f/h}$ und $\overline{g/h}$ teilerfremd modulo p sind. Das ist genau dann der Fall, wenn $p \nmid \mathrm{Res}(f/h, g/h)$. Obwohl h a priori nicht bekannt ist, läßt sich $\mathrm{Res}(f/h, g/h)$ abschätzen.

Satz 3.8. *Für $f, g \in \mathbb{Z}[X]$ mit* $\operatorname{grad} f = n \geq 1$, $\operatorname{grad} g = m$, $h = \mathrm{ggT}(f, g)$ *und* $\|f\|_\infty, \|g\|_\infty \leq A$ *gilt*

$$|\mathrm{Res}(f/h,\ g/h)| \leq (n+1)^n \cdot A^{2n}$$

Beweis. Wir beweisen eine schwächere Ungleichung. Sei $f^* = f/h$, $g^* = g/h$. Wir wissen schon

$$\|f^*\|_\infty\ ,\ \|g^*\|_\infty \leq 2^{n-k}(n+1)^{1/2} \cdot A$$

mit $k = \min(\operatorname{grad} f^*, \operatorname{grad} g^*)$. Dies ist die Teilerschranke. Daraus folgt direkt

$$|\mathrm{Res}(f^*, g^*)| \leq 4^n (n+1)^n A^{2n} \qquad \square$$

Mit einer etwas aufwendigeren Argumentation (siehe Übungsaufgabe) kann man den Faktor 4^n noch eliminieren.

Die in diesem Abschnitt bewiesenen Schranken erlauben vor allem Abschätzungen über die Laufzeit von Algorithmen. In der Praxis wird man natürlich versuchen, mit kleinen Moduln m auszukommen, da Moduln „mit Erfolgsgarantie“ nach den obigen Ungleichungen oft astronomisch groß sind.

Weiterführende Literatur: [**MCA**].

ABSCHNITT 4

Modulare Algorithmen für den ggT

In diesem Abschnitt seien $f, g \in \mathbb{Z}[X]$ primitiv und h ihr größter gemeinsamer Teiler. Dieser ist in $\mathbb{Z}[X]$ eindeutig bestimmt durch die Forderung, daß sein Leitkoeffizient positiv sei. Außerdem ist er ebenfalls primitiv. Sei $f = f^*h$, $g = g^*h$, und sei p eine Primzahl, welche die Leitkoeffizienten von f und g nicht teilt. Dann erhält die Reduktion modulo p den Grad aller beteiligten Polynome. Es gilt

$$p \nmid \operatorname{Res}(f^*, g^*) \Longrightarrow \operatorname{Res}(\overline{f^*}, \overline{g^*}) \neq 0,$$

und daher sind $\overline{f^*}, \overline{g^*}$ teilerfremd modulo p, wenn p die Resultante von f^* und g^* nicht teilt. Die Reduktion von h hat dann die Form

$$\overline{h} = \overline{h}_k \cdot \operatorname{ggT}(\overline{f}, \overline{g}) \quad \text{mit } h = h_0 + \cdots + h_k X^k,$$

denn über dem Körper $\mathbb{Z}_p$ ist der ggT von $\overline{f}$, $\overline{g}$ per Definition stets normiert. Leider ist h_k nicht bekannt! Man kommt aber auch ohne seine Kenntnis aus: Mit $b = \operatorname{ggT}(f_n, g_m)$ folgt offenbar $h_k \mid b$ und also

$$\overline{\left(\frac{b \cdot h}{h_k}\right)} = \overline{b} \cdot \operatorname{ggT}(\overline{f}, \overline{g}).$$

Wir liften die rechte Seite zu einem Polynom $\tilde{h} \in \mathbb{Z}[X]$. Wenn p groß genug ist, nämlich

$$p > 2 \left\| \frac{b \cdot h}{h_k} \right\|_\infty,$$

erhalten wir

$$\tilde{h} = \frac{b \cdot h}{h_k}.$$

Wir ziehen den größten gemeinsamen Teiler aller Koeffizienten von $\tilde{h}$ heraus, so daß das primitive Polynom h gewonnen wird. Es gilt nach der Schranke von Mignotte:

$$\|h\|_\infty \leq C = \min\bigl(2^n (n+1)^{1/2} \|f\|_\infty,\ 2^m (m+1)^{1/2} \|g\|_\infty\bigr)$$

und

$$\left\| \frac{b \cdot h}{h_k} \right\|_\infty \leq b \cdot C.$$

Es genügt also, $p > 2bC$ zu wählen, damit beim Liften von $\mathbb{Z}_p[X]$ nach $\mathbb{Z}[X]$ wirklich $b \cdot h / h_k$ aus $\tilde{h}$ gewonnen wird. Allerdings ist schwer zu kontrollieren, ob

p ein Teiler von $\mathrm{Res}(f^*, g^*)$ ist. Die Resultante läßt sich bei hinreichend großen Graden nicht mehr ermitteln – ganz abgesehen davon, daß wir f^* und g^* nicht kennen. Wir können das Ergebnis aber kontrollieren. Wenn $\tilde{h}$ sowohl bf als auch bg teilt, ist der primitive Anteil von $\tilde{h}$ der gesuchte größte gemeinsame Teiler. Sollte der Teilbarkeitstest fehlschlagen, wählen wir eine neue Primzahl p. Aus diesen Überlegungen ergibt sich folgender probabilistischer Algorithmus vom Typ Las Vegas: Gegeben seien die primitiven Polynome $f, g \in \mathbb{Z}[X]$ mit Graden n bzw. m und Leitkoeffizienten $f_n,\ g_m$. Wir setzen $b = \mathrm{ggT}(f_n, g_m)$ und wählen C wie oben.

Algorithmus 4.1. Modulare Berechnung des ggT, Variante „große Primzahl“

(1) Wähle eine Primzahl $p > 2bC$, die keinen der Leitkoeffizienten $f_n,\ g_m$ teilt.
(2) Reduziere f und g modulo p zu $\overline{f}, \overline{g}$ und bestimme über dem Körper $\mathbb{Z}_p$ ihren ggT.
(3) Lifte $\overline{b} \cdot \mathrm{ggT}(\overline{f}, \overline{g})$ zu $\tilde{h} \in \mathbb{Z}[X]$.
(4) Prüfe, ob $\tilde{h} \mid bf$, $\tilde{h} \mid bg$.
(5) Ja: Der primitive Teil von $\tilde{h}$ ist ggT von $f,\ g$. Stoppe.
Nein: Gehe zu (1).

Das folgende Beispiel deutet an, wie klein die Wahrscheinlichkeit ist, in Schritt (1) eine „schlechte“ Primzahl p zu wählen, d. h. eine solche, die die Resultante teilt.

Beispiel 4.2. Sei $m = n = 100$, $b = 1$, $\|f\|_\infty, \|g\|_\infty \leq 100$. Dann erhält man $C \approx 2.6 \cdot 10^{33}$. Es folgt

$$\left| \mathrm{Res}\left(\frac{f}{\mathrm{ggT}(f,g)}, \frac{g}{\mathrm{ggT}(f,g)} \right) \right| \leq 101^{100} \cdot 100^{200} \approx 2.7 \cdot 10^{600}$$

Die Resultante hat höchstens 18 Primfaktoren $p > C$. Aus dem Primzahlsatz folgt, daß zwischen C und $2C$ etwa

$$\frac{2C}{\ln(2C)} - \frac{C}{\ln(C)} \geq 3 \cdot 10^{31}$$

Primzahlen liegen.

Die Wahrscheinlichkeit, bei zufälliger Wahl einen Teiler der Resultante zu treffen, ist also verschwindend klein. Zudem gibt es Primzahltests, die verläßlich und schnell Primzahlen der erforderlichen Größe liefern. Das Verfahren ist also durchaus praktikabel.

Besser als das bisher geschilderte Verfahren ist jedoch die Verwendung vieler „kleiner“ Primzahlen, d. h. solcher, die nicht länger als ein Computerwort sind.

Die einzelnen Ergebnisse werden dann mit dem chinesischen Restsatz zusammengefügt.

Algorithmus 4.3. Modulare Berechnung des ggT, Variante „viele kleine Primzahlen“

(1) Setze $d = \min(\operatorname{grad} f, \operatorname{grad} g)$.
(2) Setze $q = 1$, $v = 0$.
(3) Wähle eine Primzahl p, die f_n und g_m nicht teilt.
(4) Reduziere f und g modulo p und berechne $u = \overline{b}\ \mathrm{ggT}(\overline{f}, \overline{g})$.
(5) Ist $\operatorname{grad} u > d$, dann gehe zu (3). Ist $\operatorname{grad} u < d$, setze $d = \operatorname{grad} u$ und gehe zu (2).
(6) Im Fall $\operatorname{grad} u = d$ bestimme mit dem chinesischen Restsatz ein Polynom $\tilde{v} \in \mathbb{Z}[X]$ mit

$$\tilde{v} = u \mod p\ ,\ \tilde{v} = v \mod q\ ,\ \|\tilde{v}\|_\infty < \frac{pq}{2}.$$

(7) Gilt $\tilde{v} \mid bf$, $\tilde{v} \mid bg$, dann ist der primitive Teil von $\tilde{v}$ der ggT von f, g. Stoppe.
(8) Sonst setze $v = \tilde{v}$, $q = pq$ und gehe zu (3).

Die Grundidee ist also, durch Akkumulation der Primzahlen p schließlich einen so großen Modul m aufzubauen, daß $\mathrm{ggT}(f, g)$ aus seiner Reduktion modulo m geliftet werden kann.

Die Zahl d ist stets eine obere Schranke für $\operatorname{grad} \mathrm{ggT}(f, g)$. Gilt in (5) die Ungleichung $\operatorname{grad} u > d$, dann ist p eine „schlechte“ Primzahl: $p \mid \mathrm{Res}(f^*, g^*)$.

Andererseits ist aber auch $\operatorname{grad} u$ eine obere Schranke für $\operatorname{grad} \mathrm{ggT}(f, g)$. Wenn also $\operatorname{grad} u < d$, dann sind alle bisherigen Primzahlen Teiler von $\mathrm{Res}(f^*, g^*)$ und müssen daher verworfen werden.

Man kann vor dem Teilbarkeitstest und vor der Bestimmung von $\tilde{v}$ erst einmal testen, ob $v \equiv u \mod p$ ist. In diesen Fall ist $\tilde{v} = v$ und dies ist ein Indikator dafür, daß $\mathrm{ggT}(f, g)$ schon gefunden ist. Die Rechnung modulo p hat dann den bisherigen Kandidaten bestätigt. Ist $v \not\equiv u \mod p$, bestimmt man $\tilde{v}$ und geht direkt zu (8).

Die Beschaffung von Primzahlen ist unproblematisch, da es schnelle und zuverlässige Primzahltests gibt. Für die Variante mit kleinen Primzahlen kann man außerdem vorab Listen mit Primzahlen knapp unterhalb der Wortlänge des Computers anlegen.

Man kann auch den erweiterten euklidischen Algorithmus „modularisieren“. Wenn man für die in ihm auftretenden Größen Schranken ähnlich zur Faktorschranke oder der für die Resultante angeben will, muß man zusätzlich *Subresultanten* betrachten.

Weiterführende Literatur: [**MCA**].

ABSCHNITT 5

Faktorisierung von Polynomen über $\mathbb{Z}$

Polynome über $\mathbb{Z}$ faktorisiert man mit einem modularen Algorithmus, nachdem man sie zunächst quadratfrei und primitiv gemacht hat, d. h. den größten gemeinsamen Teiler der Koeffizienten herausgezogen hat. Sei p eine hinreichend große Primzahl, so daß sich alle Teiler von $f \in \mathbb{Z}[X]$ aus ihren Repräsentanten modulo p liften lassen. Sei

$$f = f_1 \cdots f_s$$

die Zerlegung von f in irreduzible Polynome $f_i \in \mathbb{Z}[X]$. Modulo p haben diese eine Zerlegung in irreduzible und normierte Polynome g_{ij} aus $\mathbb{Z}_p[X]$:

$$\overline{f_i} = \overline{c_i} g_{i,1} \cdots g_{i,r_i} \quad c_i \in \mathbb{Z}_p,\ i = 1, \ldots, r$$

Dabei bezeichnet c_i den Leitkoeffizienten von f_i. Man kann ja keineswegs erwarten, daß $\overline{f_i}$ irreduzibel ist. Wir diskutieren dies noch genauer am Ende dieses Abschnitts.

Das Problem dabei ist nun, daß die g_{ij} bei der Faktorisierung von f gleichsam „auf einem Haufen“ liegen. Man muß auf irgendeine Art und Weise geschickt testen, wie diese sich nach Liftung zu Faktoren von f zusammensetzen. Unvermeidlich ist es, sogenannte „Faktorkombinationen“ zu bilden, diese Produkte mit einem sinnvollen Leitkoeffizienten nach $\mathbb{Z}$ zu liften und dann zu prüfen, ob ein Teiler von f gefunden ist. Ein geeigneter Leitkoeffizient für die potentiellen Teiler von ist der Leitkoeffizient b von f. Wir müssen dann natürlich testen, ob der Kandidat bf teilt und seinen primitiven Teil bilden.

Aus diesen Überlegungen ergibt sich folgender Algorithmus „Variante große Primzahl“ für das Faktorisieren von Polynomen in $\mathbb{Z}[X]$. Sei $f \in \mathbb{Z}[X]$ primitiv, nichtkonstant mit grad $f = n$ und quadratfrei mit Leitkoeffizient $b > 0$. Ferner sei $A = \|f\|_\infty$ und $B = 2^n(n+1)^{1/2}Ab$ (das ist die Faktorschranke für bf). Folgender Algorithmus berechnet dann die Faktorisierung von f mit Hilfe von Faktorkombinationen. Leider kommt man nicht darum herum, alle möglichen Kombinationen auf möglichste effiziente Art und Weise durchzuprobieren. (Es gibt aber auch eine Alternative zur Faktorkombination, die auf dem LLL-Algorithmus beruht; siehe [**MCA**].)

Algorithmus 5.1. Faktorisierung in $\mathbb{Z}[X]$, Variante „große Primzahl“ und Faktorkombination

(1) Wähle eine genügend große Primzahl $p > 2B$, so daß $\mathrm{ggT}(\overline{f}, \overline{f'}) = 1$ gilt.
(2) Zerlege in $\mathbb{Z}_p[X]$: $\overline{f} = \overline{b} \cdot g_1 \cdots g_t$.
(3) Initialisiere $T = \{1, \ldots, t\}$, $f^* = f$, $s = 1$, $c = b$.
(4) Gilt $2s > \#T$, gib f^* als irreduziblen Teiler von f aus und stoppe.
(5) Für alle s-elementigen Teilmengen $S \subset T$ führe man aus:
  (i) Bestimme $g, h \in \mathbb{Z}[X]$ mit $\|g\|_\infty, \|h\|_\infty < p/2$ und

$$\overline{g} = \overline{c} \prod_{i \in S} g_i \ , \ \overline{h} = \overline{c} \prod_{i \in T \setminus S} g_i$$

  (ii) Gilt $cf^* = gh$, dann gib den primitiven Teil von g als irreduziblen Teiler von f aus. Setze ferner $T = T \setminus S$, $f^* =$ primitiver Teil von h, $c =$ Leitkoeffizient von f^* und gehe zu (4).
(6) Setze $s = s + 1$ und gehe zu (4).

Zur Erläuterung: T ist die Menge der Indizes aus $\{1, \ldots, t\}$, für die g_i noch nicht in einem $\mathbb{Z}[X]$-Teiler von f aufgegangen sind. Dabei ist s die Minimalzahl der g_i, die man multiplizieren muß, um nach Liftung bis auf den Leitkoeffizienten einen Teiler von f zu erhalten. Daher müssen die in (5)(ii) gefundenen Teiler von f auch irreduzibel sein: Würden sie zerfallen, so würden zwei echte Teilmengen von S schon zu Teilern von f führen. Das ist aber wegen der Minimalität von s nicht möglich. Genauso sieht man, daß f^* irreduzibel ist, wenn in Schritt (4) der Algorithmus abgebrochen worden ist: Jeder echte irreduzible Teiler von f^* hätte modulo p mindestens s Faktoren. Es gibt aber nur noch weniger als $2s$ Faktoren.

Schließlich muß man sich noch überzeugen, daß in Schritt (5) wirklich alle irreduziblen Teiler von f gefunden wurden, die modulo p in genau s irreduzible Faktoren zerfallen. Wenn $cf^* = gh$ ist, ist der primitive Teil von g sicher ein irreduzibler Teiler von f^* und damit von f. Ist umgekehrt $\tilde{g}$ ein solcher Teiler, so gilt

$$\tilde{g} = \overline{a} \prod_{i \in S} g_i$$

mit einer Teilmenge $S \subset \{1, \ldots, t\}$, $\#S = s$, wobei a der Leitkoeffizient von $\tilde{g}$ ist. Die Teilmenge S wird in Schritt (5) gefunden, weil bei vorangegangenen Verkleinerungen von T kein Element von S entfernt werden konnte: Alle vorher entfernten Elemente g_i gehören zu Teilern von f, die modulo p zu $\tilde{g}$ teilerfremd sind. Da f^* aus f durch Abspalten von zu $\tilde{g}$ teilerfremden Polynomen entstanden ist, muß $\tilde{g}$ auch f^* teilen

$$f^* = \tilde{g}\tilde{h}.$$

Da $f^* = \overline{c} \prod_{i \in T} g_i$, folgt

$$\overline{c}\,\overline{f} = \Big(\overline{c} \prod_{i \in S} g_i\Big)\Big(\overline{c} \prod_{i \in T \setminus S} g_i\Big).$$

Ferner gilt $a \mid c$ und auch der Leitkoeffizient von $\tilde{h}$ teilt c. Da $c\tilde{g} \mid bf$, gilt $\|c\tilde{g}/a\|_\infty < p/2$ und ähnliches gilt für $\tilde{h}$. Folglich ist $c\tilde{g}/a$ Liftung von $\overline{c} \prod_{i \in S} g_i$ und der komplementäre Faktor con cf^* entsteht ebenfalls aus seiner Liftung.

Die Komplexität des obigen Algorithmus ist im schlechtesten Fall exponentiell in grad f. Zerfällt f nämlich modulo p in Linearfaktoren, ist aber über $\mathbb{Z}$ irreduzibel, dann muß man $2^{\operatorname{grad} f - 1}$ Teilmengen von $\{1, \ldots, t\} = \{1, \ldots, n\}$ testen, bis man das erkennt. Folgende Schritte zur Beschleunigung der aufwendigen Teile des Verfahrens sind jedoch möglich und führen i.a. zu einer Verbesserung:

(a) Teste keine Teilmenge von T mehrfach. Dies ist durch eine geschickte Implementierung zu erreichen.

(b) Statt $cf^* = gh$ kann man auch

$$\|g\|_1 \|h\|_1 \le B$$

testen. (Beachte, daß hier die 1-Norm verwendet wird.) Wenn diese Bedingung erfüllt ist, gilt

$$\|gh\|_\infty \le \|gh\|_1 \le \|g\|_1 \|h\|_1\| < \frac{p}{2}$$

und da auch $\|cf^*\|_\infty < p/2$, folgt die Gleichung $cf^* = gh$ aus der entsprechenden Kongruenz modulo p.

Ist umgekehrt $cf^* = gh$, so folgt die Ungleichung aus Satz 3.5. (Achtung: Diese Schlussweise ist nur erlaubt, wenn wirklich $p > 2B$, nicht aber, wenn mit kleineren p gearbeitet wird.)

(c) Prüfe zuerst die Gleichung $c_0 f_0^* = g_0 h_0$ für die konstanten Koeffizienten. Fast alle Faktorkombinationen fallen durch diesen einfachen Test.

(d) Betrachte eine Zerlegung modulo mehrerer kleiner Primzahlen q und ihre Zerlegungstypen. Dadurch kann man die potentiellen Grade der irreduziblen Teiler von f einschränken.

Beispiel 5.2.

$$\begin{aligned} f &= (X^{101} - 1)/(X - 1), \\ g &= 100X^{100} + \cdots + 2X^2 + X + 1, \\ h &= fg. \end{aligned}$$

Beide Polynome sind irreduzibel. Für f ist dies bekannt: $(X^{101} - 1)/(X - 1)$ ist das Kreisteilungspolynome zur Primzahl $p = 101$. Die folgende Tabelle zeigt die Grade der irreduziblen Teiler von h modulo p, aufsteigend geordnet:

p							
7	1	1	2	10	86	100	
11	1	3	6	90	100		
13	1	1	23	35	40	50	50

Zerlegt man modulo 7, dann sind die möglichen Grade irreduzibler Teiler e mit $\operatorname{grad} e \leq (\operatorname{grad} fg)/2$ in $\mathbb{Z}[X]$ gerade

$$1, 2, 3, 4, 10, 11, 12, 13, 14, 86, 87, 88, 89, 90, 96, 97, 98, 99, 100.$$

Nimmt man die Zerlegung modulo 11 hinzu, bleiben nur noch

$$1, 3, 4, 10, 90, 91, 96, 97, 99, 100$$

übrig, und nachdem auch noch die Zerlegung modulo 13 herangezogen worden ist, reduzieren sich die möglichen Grade auf

$$1, 90, 99, 100.$$

Der diskutierte Algorithmus ist durchaus praktikabel, kann aber noch verbessert werden durch Übergang zu einer Variante „Potenz kleiner Primzahl“, die wir im nächsten Abschnitt diskutieren.

Grundsätzlich wäre es auch möglich, eine Variante „viele kleine Primzahlen“ zu realisieren. Dies ist aber wenig sinnvoll, weil der Zerlegungstyp von f modulo p von p abhängt, wie das obige Besispiel schon deutlich gezeigt hat. Man müßte dann etwa Faktoren von f modulo p_1 und Faktoren modulo p_2 mittels des chinesischen Restsatzes kombinieren, was den Aufwand der Faktorkombinationen so in die Höhe treibt, daß diese Variante nicht praktikabel ist.

Der Dichtesatz von Frobenius. Über die Zerlegungstypen und die Häufigkeit, mit der sie unter den Primzahlen auftritt, kann man eine sehr präzise Aussage machen, die wir nun diskutieren wollen. Sei $f \in \mathbb{Z}[X]$ irreduzibel vom Grad n mit Zerfällungskörper $K \supset \mathbb{Q}$. Mit $G = \operatorname{Aut}_{\mathbb{Q}}(K)$ sei dessen Galois-Gruppe bezeichnet. Diese Gruppe permutiert die Nullstellen von f in K und ist dadurch als Untergruppe der symmetrischen Gruppe S_n bis auf die Numerierung der Nullstellen, also bis auf Konjugation eindeutig bestimmt.

Alle $\pi \in S_n$ lassen sich als Produkt elementfremder Zykel darstellen, die bis auf die Reihenfolge eindeutig bestimmt sind:

$$\pi = \sigma_1 \cdots \sigma_t$$

Als *Zerlegungstyp* von π bezeichnet man dann

$$Z = (|\sigma_1|, \ldots, |\sigma_t|), \quad |\sigma_1| \geq \cdots \geq |\sigma_t|.$$

Wir setzen noch

$$\delta_f(Z) = \frac{\Pi(Z)}{|G|}, \quad \Pi(Z) = \#\{\text{Elemente in } G \text{ mit Zerlegungstyp } Z\}.$$

Damit ist $\delta_f(Z)$ ist der relative Anteil der Elemente $\pi \in G$ mit Zerlegungstyp Z.

Für eine Teilmenge $M \subset \mathscr{P}$ der Primzahlen definiert man die *natürliche Dichte* wie folgt:

$$d(M) = \lim_{n\to\infty} \frac{\#\{p \in M \mid p \le n\}}{\#\{p \in \mathscr{P} \mid p \le n\}},$$

vorausgesetzt, der Limes existiert.

Sei f irreduzibel und $M_f(Z)$ die Menge der Primzahlen, für die $f \mod p$ den Zerlegungstyp Z besitzt. Mit diesen Bezeichnungen gilt

Satz 5.3 (Frobenius)**.** *Sei $f \in \mathbb{Z}[X]$ irreduzibel. Für alle Zerlegungstypen Z ist dann*

$$\delta_f(Z) = d(M_f(Z)).$$

Dies zeigt, daß man im allgemeinen nicht einmal damit rechnen kann, überhaupt eine Primzahl p zu finden, für die f modulo p irreduzibel ist. Ist f selbst nicht irreduzibel, so mischen sich zudem die Zerlegungstypen der irreduziblen Komponenten.

In der Verfeinerung von Chebotarev ist der obige Satz eines der wichtigsten Resultate der algebraischen Zahlentheorie. Ausgezeichnete Informationen dazu gibt der folgende Artikel: P. Stevenhagen und H. W. Lenstra jun., *Chebotarev and his density theorem*. Math. Intell. 18, 26-37 (1996).

ABSCHNITT 6

Hensel-Liftung und Faktorisierung

Die Grundidee der Hensel-Liftung besteht darin, $f \in \mathbb{Z}[X]$ modulo einer kleinen Primzahl p zu faktorisieren, diese Zerlegung zu einer Faktorisierung modulo p^k mit hinreichend großem k zu liften und daraus schließlich mittels Faktorkombination die Zerlegung in $\mathbb{Z}[X]$ zu finden.

Die Hensel-Liftung ist eine Variante des Newton-Verfahrens: Aus einer Approximation ersten Grades wird durch Lösung einer linearen Gleichung eine Approximation zweiten Grades gewonnen, in unserem Fall aus der Lösung einer Kongruenz modulo $m = p^l$ eine solche modulo $m^2 = p^{2l}$. Wir diskutieren das Prinzip an einem einfachen Beispiel, dem Wurzelziehen.

Beispiel 6.1. Sei $m \in \mathbb{Z}$, $m > 0$ ungerade (aber nicht notwendig prim), und a teilerfremd zu m. Eine Wurzel x von $a \mod m$ sei bekannt, d. h. es gelte $x^2 \equiv a \mod m$. Wir suchen eine Lösung der Kongruenz $x^{*2} \equiv a \mod m^2$. Dazu machen wir den Ansatz $x^* = x + \tilde{x}m$. Dann ist x^* wirklich eine Liftung von x, denn $x^* \equiv x \mod m$.

Nach Voraussetzung gibt es ein b mit $a - x^2 = bm$, und natürlich ist $\tilde{x}^2 m^2 \equiv 0 \mod m^2$. Einsetzen ergibt

$$\begin{aligned} & x^{*2} \equiv a \ (m^2) \\ \iff \quad & x^2 + 2x\tilde{x}m + \tilde{x}^2 m^2 \equiv a \ (m^2) \\ \iff \quad & 2x\tilde{x}m \equiv bm \ (m^2) \\ \iff \quad & 2x\tilde{x} \equiv b \ (m) \end{aligned}$$

Die letzte Kongruenz ist eindeutig lösbar, denn $2x$ ist nach Voraussetzung teilerfremd zu m.

Zur Illustration wählen wir $m = 9$, $x^2 \equiv 7 \mod 9$, $x = 4$. Gesucht ist x^* mit $(x^*)^2 \equiv 7 \mod 81$ und $x^* \equiv x \mod 9$. Da $7 - 4^2 = (-1) \cdot 9$, ist die Kongruenz $8\tilde{x} \equiv -1 \mod 9$ zu lösen, so daß $\tilde{x} = 1$. Mithin $x^* = 4 + 1 \cdot 9 = 13$. Tatsächlich ist $13^2 = 169 \equiv 7 \mod 81$.

Das Liften der Faktorisierung ist schwieriger, und wir müssen dabei auch noch simultan eine Hilfsgleichung liften. Seien $f, g, h \in R[X]$, $m \in R$ mit

$$f \equiv gh \ (m)$$

In der Situation, in der das Verfahren zur Faktorisierung angewandt werden soll, dürfen wir annehmen, daß

$$sg + th \equiv 1 \ (m)$$

mit $s, t \in R[X]$. Wir wollen beide Kongruenzen simultan liften. Gesucht sind h^*, g^*, s^*, $t^* \in R[X]$ mit $f \equiv g^*h^* \bmod m^2$ und $s^*g^* + t^*h^* \equiv 1 \bmod m^2$. Als Ansatz wählen wir wie oben eine Linearkombination:

$$\begin{aligned} g^* &= g + \tilde{g}m, \qquad & h^* &= h + \tilde{h}m, \\ s^* &= s + \tilde{s}m, \qquad & t^* &= t + \tilde{t}m. \end{aligned}$$

Zunächst ist die Kongruenz

$$f - (g + \tilde{g}m)(h + \tilde{h}m) \equiv 0 \ (m^2)$$

zu lösen. Sei $e = f - gh = um$, $u \in R[X]$. Einsetzen reduziert unser Problem auf die Kongruenz

$$u - (g\tilde{h} + \tilde{g}h) \equiv 0 \ (m).$$

Nun nutzen wir aus, daß $sg + th \equiv 1 \bmod m$. Multiplikation mit u zeigt dann, daß wir

$$\tilde{g} = ut, \quad \tilde{h} = us,$$

also

$$g^* = g + et, \quad h^* = h + es$$

wählen können.

Da wir die Kongruenz $sg + th \equiv 1 \bmod m$ genutzt haben, müssen wir auch sie liften, wenn das Verfahren fortgesetzt werden soll. Dafür ist

$$(s + \tilde{s}m)g^* + (t + \tilde{t})h^* \equiv 1 \ (m^2)$$

zu betrachten. Mit $vm = 1 - (sg + th)$ erhält man als eine mögliche Lösung

$$\tilde{s} = s(v - ust), \quad \tilde{t} = t(v - ust).$$

Natürlich sind $\tilde{g}, \tilde{h}, \tilde{s}, \tilde{t}$ nicht eindeutig bestimmt, und wir werden sehen, daß die bisher getroffene Wahl im allgemeinen verbessert werden kann.

Beispiel 6.2. Sei $R = \mathbb{Z}, m = 5, f = X^4 - 1, g = X^3 + 2X^2 - X - 2, h = X - 2$. Dann ist

$$f \equiv gh \ (5) \qquad \text{und} \qquad (-2)g + (2X^2 - 2X - 1)h \equiv 1 \ (5).$$

Dabei kann man die Darstellung von 1 mit dem erweiterten euklidischen Algorithmus in $\mathbb{Z}_5[X]$ ermitteln. Wir setzen $s = -2, t = 2X^2 - 2X - 1$. Diese Polynome sind eindeutig bestimmt, wenn wir $\operatorname{grad} s < \operatorname{grad} h$, $\operatorname{grad} t < \operatorname{grad} g$ verlangen.

Man erhält

$$\begin{aligned} e &= f - gh = 5X^2 - 505(X^2 - 1), \\ g^* &= g + et = 10X^4 - 9X^3 - 13X^2 + 9X + 3, \\ h^* &= h + es = -10X^2 + X + 8. \end{aligned}$$

In diesem Beispiel zeigt sich ein sehr unerwünschter Effekt: Die Grade von g^* und h^* sind größer als die von g und h. Über einem Ring mit Nullteilern wie $\mathbb{Z}/(25)$ kann man ja $\operatorname{grad} f = \operatorname{grad} g + \operatorname{grad} h$ nicht aus $f = gh$ folgern.

Die Vergrößerung der Grade läßt sich aber mit einer kleinen Modifikation verhindern, wenn, wie im Beispiel, wenigstens eines der Polynome g oder h normiert ist. Wir beachten dabei, daß man durch normierte Polynome über beliebigen Ringen mit Rest dividieren kann:

Satz 6.3. *Seien $f, g \in R[X]$, $g \neq 0$ normiert. Dann existieren eindeutig bestimmte Polynome $q, r \in R[X]$ mit*

$$f = qg + r, \qquad r = 0 \quad \textit{oder} \quad \operatorname{grad} r < \operatorname{grad} g.$$

Gilt dabei $f \equiv 0 \mod m$ für ein $m \in R$, dann ist auch $q \equiv 0 \mod m$, $r \equiv 0 \mod m$,

Dies beweist man mit dem üblichen Divisionsalgorithmus. Die zweite Aussage folgt aus der ersten durch Anwendung auf $R/(m)$, denn wenn $f = 0$ ist, müssen q und r beide 0 sein.

In der oben betrachteten Situation $f = gh$ sei h normiert. Wir schreiben

$$se = qh + r$$

gemäß Satz 6.3. Dann ist $q \equiv 0 \mod m$, $r \equiv 0 \mod m$. Es gilt

$$\begin{aligned} f \equiv g^*h^* &\equiv (g + te)(h + se) \ (m^2) \\ &\equiv (g + te)(h + qh + r) \ (m^2) \\ &\equiv gh + teh + gqh + teqh + gr + ter \ (m^2) \\ &\equiv gh + teh + qgh + gr \ (m^2), \end{aligned}$$

und ebenso

$$\begin{aligned} (g + te + qg)(h + r) &= gh + teh + gr + ter + qgh + qgr \\ &\equiv gh + teh + gr + qgh \ (m^2) \\ &\equiv f \ (m^2) \end{aligned}$$

Beachte daß $teqh, ter, qgr \equiv 0 \mod m^2$; es ist ja

$$e \equiv q \equiv r \equiv 0 \ (m^2).$$

Wir können also die bisherige Wahl von g^* und h^* abändern zu

$$g^* = g + te + qh, \quad h^* = h + r,$$

und erhalten auch damit $g^*h^* \equiv f \mod m^2$. Da $\operatorname{grad} r < \operatorname{grad} h$, ist $\operatorname{grad} h^* = \operatorname{grad} h$, und h^* ist wieder normiert. Ferner können wir (falls nötig) alle Terme von g^* weglassen, die $\equiv 0 \mod m^2$ sind, so daß $\operatorname{grad} g^* = \operatorname{grad}(g \mod m^2)$ angenommen werden darf. Es folgt

$$\operatorname{grad} g^* = \operatorname{grad}(f \mod m^2) - \operatorname{grad} h^* \leq \operatorname{grad} f - \operatorname{grad} h = \operatorname{grad} g.$$

Daher hat g^* allenfalls kleineren Grad als g.

Wir verzichten darauf, die passenden Formeln für s^* und t^* abzuleiten, sondern geben diese einfach an:

Satz 6.4. *Sei R ein Ring und $m \in R$. Gegeben seien Polynome $f, g, h, s, t \in R[X]$ mit*

$$f \equiv gh \ (m), \quad sg + th \equiv 1 \ (m).$$

Es gelte $\operatorname{grad} s < \operatorname{grad} h$, $\operatorname{grad} t < \operatorname{grad} g$. *Ferner sei h normiert. Wir setzen*

$$e \equiv f - gh \ (m^2) \qquad se \equiv qh + r \ (m^2),$$
$$g^* \equiv g + te + gq \ (m^2), \qquad h^* \equiv h + r \ (m^2).$$

Sei

$$b \equiv sg^* + th^* - 1 \ (m^2), \qquad sb \equiv ch^* + d \ (m^2),$$
$$s^* \equiv s - d \ (m^2), \qquad t^* \equiv t - tb - cg^* \ (m^2).$$

mit $d = 0 \mod m^2$ oder $\operatorname{grad} d < \operatorname{grad} h^*$. *Dann gilt*

$$f \equiv g^*h^* \ (m^2), \quad s^*g^* + t^*h^* \equiv 1 \ (m^2).$$

Dabei ist h^* normiert, $\operatorname{grad} h^* = \operatorname{grad} h$, $\operatorname{grad} g^* \leq \operatorname{grad} g$, $\operatorname{grad} s^* < \operatorname{grad} h^*$, $\operatorname{grad} t^* < \operatorname{grad} g^*$.

Es ist nur noch nachzuprüfen, daß $s^*g^* + t^*h^* \equiv 1 \mod m^2$ und die Gradbedingungen für s^* und t^* erfüllt sind. Dies folgt mit ähnlichen Argumenten wie oben.

Satz 6.5. *Unter den Voraussetzungen des vorigen Satzes sei $k \in \mathbb{N}$. Dann existieren $g^*, h^*, s^*, t^* \in R[X]$, die alle Gradbedingungen in Satz 6.4 erfüllen, so daß h^* normiert ist und*

$$f \equiv g^*h^* \ (m^k), \qquad s^*g^* + t^*h^* \equiv 1 \ (m^k)$$

Beweis. Wir iterieren die Bestimmung von g^*, h^*, s^*, t^* gemäß Satz 6.4 und erhalten die Gültigkeit der Kongruenzen modulo $m^2, m^4, m^8, \ldots$ □

Eindeutigkeitssätze. Letzten Endes wollen wir die Zerlegung eines Polynoms $f \in \mathbb{Z}[X]$ aus seiner Zerlegung modulo p^k für hinreichend großes k (und geeignetes p) mittels Faktorkombination konstruieren. Dazu müssen wir uns sicher sein, daß die Zerlegung über $\mathbb{Z}$ sich in der Zerlegung modulo p^k wiederfindet. Nun ist $\mathbb{Z}_{p^k} = \mathbb{Z}/(p^k)$ kein faktorieller Ring, so daß wir nicht ohne weiteres mit den üblichen Sätzen über die Eindeutigkeit der Faktorisierung argumentieren können.

Es gilt aber folgender Eindeutigkeitssatz:

Satz 6.6. *Sei R ein Ring, $m \in R$ ein Nichtnullteiler, $k \in \mathbb{N}$. Seien $g_1, h_1, g_2, h_2 \in R[X]$, so daß folgendes gilt:*

(a) $sg_1 + th_1 \equiv 1 \ (m)$,
(b) *die Leitkoeffizienten von g_1 und h_1 sind Nichtnullteiler modulo m,*
(c) *g_1 und g_2 haben den gleichen Leitkoeffizienten, gleichen Grad und $g_1 \equiv g_2 \mod m$,*
(d) *h_1 und h_2 erfüllen analog die Bedingung in* (c).

Wenn dann $g_1h_1 \equiv g_2h_2 \mod m^k$, so $g_1 \equiv g_2 \mod m^k$, $h_1 \equiv h_2 \mod m^k$.

Beweis. Teilt m^j die Differenzen $g_1 - g_2$ und $h_1 - h_2$ für alle j, so so sind sie beide 0 (weshalb?). Im anderen fall wählen wir den maximalen Exponenten j, für den m^j sowohl $g_1 - g_2$ als auch $h_1 - h_2$ teilt. Nach Voraussetzung ist $m \geq 1$. Zur Ableitung eines Widerspruchs nehmen wir an, daß $j < k$.

Es gilt

$$g_1 - g_2 = um^j, \quad h_1 - h_2 = vm^j.$$

Wir können annehmen, daß $m \nmid u$. Damit ist

$$\begin{aligned} 0 &\equiv g_1h_1 - g_2h_2 \equiv g_1(h_1 - h_2) + h_2(g_1 - g_2) \\ &\equiv (g_1v + h_2u)m^j \ (m^k). \end{aligned}$$

Da m Nichtnullteiler in R ist, folgt

$$m \mid m^{k-j} \mid g_1v + h_2v$$

Durch Reduktion modulo m erhalten wir

$$0 = \overline{t}(\overline{g_1v} + \overline{h_2u}) = \overline{g_1}(\overline{t}\overline{v} - \overline{su}) + \overline{u}$$

Beachte, daß $g_1 = g_2 \mod m$ und $h_1 = h_2 \mod m$. Es folgt $\overline{g_1} \mid \overline{u}$. Andererseits ist

$$\operatorname{grad}\overline{u} \leq \operatorname{grad} u < \operatorname{grad} g_1 = \operatorname{grad}\overline{g_1},$$

weil $\operatorname{grad}(g_1 - g_2) < \operatorname{grad} g_1$ und der Leitkoeffizient von $g_1 \not\equiv 0 \mod m$ ist. Er ist aber sogar Nichtnullteiler modulo m, und deshalb ist $\operatorname{grad}\overline{u} = \operatorname{grad}\overline{g_1}$ bei $\overline{u} \neq 0$ und $\overline{g_1} \mid \overline{u}$ nicht möglich. □

Die Voraussetzungen dieses Satzes sind sicher erfüllt, wenn wir eine Zerlegung modulo m eines normierten Polynoms f in normierte Faktoren g und h liften. Als Folgerung erhalten wir eine Eindeutigkeitsaussage für die Zerlegung von Polynomen über $\mathbb{Z}_{p^k}$. In ihr nennen wir ein Polynom irreduzibel, wenn es nicht in ein Produkt von Polynomen kleineren Grades zerfällt.

Satz 6.7. *Sei $p \in \mathbb{Z}$ eine Primzahl, $f \in \mathbb{Z}_{p^k}[X]$ ein normiertes Polynom, dessen Reduktion modulo p quadratfrei ist. Dann hat f eine Zerlegung*

$$f = g_1 \cdots g_t$$

in irreduzible normierte Polynome g_i. Die Faktoren g_i sind bis auf die Reihenfolge eindeutig bestimmt. Ihre Reduktionen modulo p sind die irreduziblen Faktoren von f modulo p.

Beweis. Wir werden gleich noch zeigen, daß sich auch Zerlegungen in mehr als zwei Faktoren liften lassen. Also können wir $\overline{f} = f \mod p$ betrachten, dieses Polynom in $\mathbb{Z}_p[X]$ in irreduzible Polynome zerlegen und die Zerlegung zu einer von f liften. Dies beweist die Existenz der behaupteten Zerlegung $f = g_1 \cdots g_t$.

Sei nun $h \in \mathbb{Z}_{p^k}[x]$ in irreduzibles Polynom, das f teilt, und e der komplementäre Faktor. Wäre $h \mod p$ zerlegbar, könnten wir die Zerlegung nach $\mathbb{Z}_{p^k}$ liften, wie gerade gesehen. Also ist $h \mod p$ irreduzibel, und damit gilt $h \mod p = g_i \mod p$ für ein i wegen der Eindeutigkeit der Zerlegung in $\mathbb{Z}_p[X]$. Wir können annehmen, daß $h \mod p = g_1 \mod p$. Es folgt $e \mod p = g_2 \cdots g_t \mod p$.

Nach Voraussetzung ist $f \mod p$ quadratfrei. Deshalb sind $h \mod p = g_1 \mod p$ und $e \mod p = g_2 \cdots g_t \mod p$ teilerfremd: Es ist nicht nur

$$(f \mod p) = (h \mod p)(e \mod p),$$

sondern es gibt auch a, b mit

$$1 = a(h \mod p) + b(e \mod p).$$

Alle Voraussetzungen über die Grade und Leitkoeffizienten in Satz 6.6 sind erfüllt, da die beteiligten Polynome normiert sind. (Um den Satz wörtlich anzuwenden, müssen wir f zunächst nach $\mathbb{Z}$ liften.) Die Eindeutigkeit der Liftung impliziert nun, daß $h = g_1$ und $e = g_2 \cdots g_t$. Damit können wir eine Induktion über t führen. □

Bemerkung 6.8. (a) Satz 6.7 ist falsch ohne die Voraussetzung, daß $f \mod p$ quadratfrei ist. Zum Beispiel gilt $X^2 = (X+2)(X+2)$ in $\mathbb{Z}_4[X]$. Man muß die Behauptung des Satzes dann abschwächen auf die Existenz und Eindeutigkeit der Zerlegung in ein Produkt von Polynomen, die modulo p paarweise teilerfremde Potenzen irreduzibler Polynome sind.

(b) Satz 6.7 gilt ohne wesentliche Änderungen für Primelemente p in Hauptidealringen, speziell natürlich in euklidischen Ringen.

(c) Wir haben der Einfachheit halber nur Aussagen für Restklassenringe modulo m^k, $m \in R$, formuliert. Im Existenzsatz 6.4 kann man das von m erzeugte Ideal durch ein beliebiges Ideal ersetzen. Im Eindeutigkeitssatz 6.6 ist das nicht ohne weiteres möglich.

(d) Wenn man die Hensel-Liftung unendlich oft wiederholt, erhält man Folgen von Elementen, die in der m-adischen Metrik auf R Cauchy-Folgen sind. Damit diese Folgen auch konvergieren, muß man R bezüglich der m-adischen Metrik komplettieren.

Liften des Zerlegungsbaums. Wir haben oben gesehen, wie man eine Zerlegung $f \equiv gh \mod m$ zu einer Zerlegung $f \equiv g^*h^* \mod m^2$ und gleichzeitig eine Darstellung $1 = sg + th \mod m$ zu einer Darstellung $1 = s^*g^* + t^*h^* \mod m^2$ liftet. Es ist noch zu klären, wie man eine Zerlegung in mehrere Faktoren behandelt.

Sei p eine Primzahl, $f \in \mathbb{Z}[X]$ ein quadratfreies, primitives Polynom, dessen Leitkoeffizient b nicht von p geteilt wird und das auch modulo p quadratfrei ist. Dann gilt nach Reduktion modulo p:

$$\overline{f} = \overline{b} g_1 \cdots g_t$$

mit paarweise verschiedenen, normierten und irreduziblen Polynomen $g_i \in \mathbb{Z}_p[X]$. Wir setzen $t_0 = t$, $g_{0i} = g_i$ und definieren rekursiv

$$t_j = \left\lceil \frac{t_{j-1}}{2} \right\rceil, \qquad g_{ij} = g_{j-1,2i-1} \cdot g_{j-1,2i},\ i = 1, \ldots, t_j,$$

wobei $g_{j,2t_j} = 1$, falls $t_{j-1} < 2t_j$. Die Rekursion bricht ab, wenn $t_j = 1$ erreicht ist. Wir haben also die Faktoren von $\overline{f}$ paarweise zusammengefaßt, diese wiederum zu Paaren usw., wobei „fehlende“ Faktoren durch 1 ersetzt worden sind. Auf diese Weise entsteht die Struktur eines Baumes, in dem die g_{ij} die Knoten repräsentieren, und von jedem Knoten (sofern er noch zerlegbar ist) Äste zu den beiden Faktoren führen. An der Wurzel des Baumes steht g_{n1}.

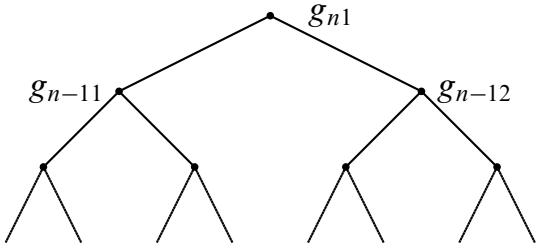

ABBILDUNG 1. Faktorisierungsbaum

Statt die Faktoren paarweise zusammenzufassen, könnte man natürlich einfacher einen Faktor nach dem anderen abspalten, was darauf hinausläuft, daß an

jedem Knoten im Baum einer der beiden Äste nur die Länge 1 hat. Es ist aber besser, die Faktoren so anzuordnen, daß an jedem Knoten die beiden Äste möglichst gleichen Grad haben, damit die Grade so schnell wie möglich „klein“ werden.

Die beiden Faktoren von g_{ij} sind teilerfremd – hier benutzen wir, daß f quadratfrei modulo p ist – so daß wir $s_{j-1,2i-1}$ und $s_{j-1,2i}$ finden mit

$$1 = s_{j-1,2i-1} g_{j-1,2i-1} + s_{j-1,2i} g_{j-1,2i}.$$

Wir liften alle Polynome nach $\mathbb{Z}[X]$ (ohne die Bezeichnungen zu verändern). Dann haben wir ein System

$$\begin{aligned} b g_{n1} &\equiv f \ (p), \\ g_{ij} &\equiv g_{j-1,2i-1} g_{j-1,2i} \ (p), \\ 1 &\equiv s_{j-1,2i-1} g_{j-1,2i-1} + s_{j-1,2i} g_{j-1,2i} \ (p) \end{aligned}$$

von Kongruenzen. Dieses läßt sich rekursiv zu einem System von Kongruenzen modulo $p^2, p^4, \ldots, p^{2^k}, \ldots$ liften, wobei wir an der Wurzel beginnen und die Äste in Richtung der Endknoten durchlaufen.

Es ist nur noch zu klären, wie die Wurzel, nämlich g_{n1} zu liften ist. Es gilt

$$b g_{n1} \equiv f \ (p),$$

also $g_{n1} = af \mod p$ mit $ab \equiv 1 \ (p)$. Nach der Liftung muß gelten

$$b g_{n1}^* \equiv f \ (p^2).$$

Wir haben also das Inverse a von b modulo p zum Inversen a^* von b modulo p^2 zu liften. Die Lösung dieses kleinen Problems überlassen wir einer Übungsaufgabe. (Man könnte natürlich auch den erweiterten euklidischen Algorithmus bemühen. Das ist aber aufwendiger.) Danach wählen wir

$$g_{n1}^* = a^* f.$$

Sodann werden die Daten von p^2 zu p^4 usw. geliftet. Sobald die erreichte Potenz von p hinreichend groß ist, haben wir die gleiche Situation wie bei der Reduktion modulo einer „großen“ Primzahl: Die Produkte bf_j, wobei f_j ein irreduzibler Faktor von f ist, lassen sich aus ihren Repräsentanten modulo p^{2^k} liften. Ferner gilt bei Reduktion modulo p^{2^k}:

$$\overline{f_j} = \overline{b} \prod_{i \in S} \overline{g_i}$$

für eine Teilmenge $S \subset \{1, \ldots, t\}$. Dies folgt aus Satz 6.6.

Zusammenfassend geben wir nun den Algorithmus an:

Algorithmus 6.9. Faktorisierung mittels „Hensel-Liftung“

Sei $f \in \mathbb{Z}[X]$ quadratfrei und primitiv vom Grad $n \geq 1$ mit Leitkoeffizienten b. Sei $A = \|f\|_\infty$, $B = 2^n(n+1)^{1/2} A\, b$.

(1) Wähle eine Primzahl $p \in \mathbb{Z}$ mit $p \nmid b$, $\mathrm{ggT}(\overline{f}, \overline{f'}) = 1$. Sei $l = \lceil \log_p(2B+1) \rceil$. (Das ist die Anzahl der Liftungsschritte.)

(2) Bestimme $a \in \mathbb{Z}$ mit $|a| < p/2$ und $ab = 1 \mod p$. Zerlege f modulo p in normierte und irreduzible $g_i \in \mathbb{Z}_p[X]$:

$$\overline{f} = \overline{b} \cdot g_1 \cdots g_t.$$

Lifte die g_i zu (gleichnamigen) Polynomen $g_i \in \mathbb{Z}[X]$ mit $\|g_i\|_\infty < p/2$ für alle $i = 1, \ldots, t$.

(3) Errichte einen Faktorisierungsbaum modulo p der Tiefe u. Setze

$$t_0 = t, \quad g_{0i} = g_i,\ i = 1, \ldots, t_0,\ t_j = \lceil t_{j-1}/2 \rceil.$$

und

$$\begin{aligned} g_{ji} &\equiv g_{j-1,2i-1} \cdot g_{j-1,2i} \ \ (p) \\ 1 &\equiv s_{j-1,2i-1} g_{j-1,2i-1} + s_{j-1,2i} g_{j-1,2i} \ \ (p) \end{aligned}$$

mit $\operatorname{grad} s_{j-1,2i-1} \operatorname{grad} g_{j-1,2i-1}, \operatorname{grad} g_{j-1,2i} < \operatorname{grad} s_{j-1,2i}$ für alle $j = 0, \ldots, u-1$ und $i = 1, \ldots, t_j$. Außerdem setze

$$g_{u1} = af \ \ (p)$$

Ferner $m = p$.

(4) Hensel-Liftung:

(i) Bestimme a^* mit $a^* b \equiv 1 \ \ (m^2)$.

(ii) Lifte g_{m1} zu $g^*_{m1} \equiv a^* f \ \ (m^2)$.

(iii) Für $j = m-1, \ldots, u$, $i = 1, \ldots, t_j$ lifte alle Polynome in (3) zu $*$-Varianten, so daß alle Kongruenzen auch modulo m^2 erfüllt sind.

(iv) Ersetze m durch m^2 und alle Polynome durch ihre $*$-Varianten.

(v) Wenn $m \geq p^l$, gehe zu (5). Sonst gehe zu (i).

(5) Führe Faktorkombinationen aus und bestimme so die irreduziblen Teiler von f in $\mathbb{Z}[X]$ wie bei der Variante „große Primzahl“.

ABSCHNITT 7

Polynome und monomiale Ordnungen

Im folgenden sei K stets ein Körper. Wie in den vergangenen Abschnitten immer wieder ausgenutzt, ist $K[X]$ ein euklidischer Ring, d. h. man kann für je zwei Polynome $f, g \in K[X]$, $g \neq 0$, eine Division von f durch g mit Rest durchführen. Diese Division mit Rest ist das entscheidende Hilfsmittel für das effektive Rechnen und die Strukturtheorie in den Ringen $K[X]$. Die Division mit Rest zeigt, daß $K[X]$ ein Hauptidealring ist, und sie erlaubt es uns, in Restklassenringen von $K[X]$ zu rechnen:

Satz 7.1. *Sei $I \neq 0$ ein Ideal in $K[X]$. Dann gilt:*

(a) *I ist ein Hauptideal, d. h. es existiert ein $g \in K[X]$ mit $I = \{rg : r \in R\}$. Das Element g ist bis auf eine Einheit eindeutig bestimmt.*

(b) *$K[X]/I$ ist ein K-Vektorraum mit Basis $1, x, \ldots, x^{\operatorname{grad}(g)-1}$. Dabei bezeichnet x die Restklasse von X, d. h. $x = \overline{X}$. Für alle $f \in K[X]$ hat $\overline{f}$ einen eindeutig bestimmten Repräsentanten r mit* $\operatorname{grad}(r) < \operatorname{grad}(g)$. *Man sagt, r sei die* Normalform *von f.*

Polynome in n Veränderlichen. Unser erstes Ziel ist es, diese Division mit Rest auf Polynome in mehreren Veränderlichen auszudehnen und Satz 7.1 entsprechend zu verallgemeinern. Zuerst werden dazu Polynomringe etwas formaler eingeführt.

Sei dazu ab jetzt stets R ein kommutativer Ring mit Eins. Wir betrachten

$$R^{(\mathbb{N}^n)} = \{f : \mathbb{N}^n \to R : f(a) = 0 \text{ für fast alle } a \in \mathbb{N}^n\}.$$

Elemente aus $R^{(\mathbb{N}^n)}$ sind also Abbildungen f von $\mathbb{N}^n$ nach R, so daß $f(a) \neq 0$ für nur endlich viele $a \in \mathbb{N}^n$. Diese Tupel bilden den *Träger* von f:

$$\operatorname{supp}(f) = \{a \in \mathbb{N}^n : f(a) \neq 0\}.$$

Auf $R^{(\mathbb{N}^n)}$ definieren wir eine Addition und eine Multiplikation mittels

$$(f \cdot g)(a) = \sum_{b+c=a} f(b)g(c), \qquad (f + g)(a) = f(a) + g(a).$$

Diese machen $R^{(\mathbb{N}^n)}$ zu einem kommutativen Ring, wie man ohne Mühe nachrechnet. (Da sich jedes $a \in \mathbb{N}^n$ auf nur endlich viele Weisen in eine Summe $b + c$ zerlegen läßt, ist das Produkt auch dann erklärt, wenn wir nicht verlangen würden,

daß $f(a) = 0$ für fast alle a. Ohne diese Einschränkung kämen wir zum Ring der formalen Potenzreihen.) Das Einselement in $R^{(\mathbb{N}^n)}$ ist gegeben durch

$$1(a) = \begin{cases} 1, & a = (0, \ldots, 0), \\ 0, & \text{sonst.} \end{cases}$$

Der Ring $R^{(\mathbb{N}^n)}$ enthält R kanonisch als Unterring: Die Zuordnung $r \mapsto r1 \in R^{(\mathbb{N}^n)}$ ist ein injektiver Ringhomomorphismus. Wir fassen R im folgenden als Unterring von $R^{(\mathbb{N}^n)}$ auf.

Wir betrachten nun spezielle Elemente $X_i \in R^{(\mathbb{N}^n)}$, die sich als die vertrauten Variablen des Polynomrings $R[X_1, \ldots, X_n]$ herausstellen werden. Seien $e_1, \ldots, e_n$ die Einheitsvektoren in $\mathbb{N}^n$. Dann sei

$$X_i(a) = \begin{cases} 1, & a = e_i, \\ 0, & \text{sonst.} \end{cases}$$

Zusätzlich betrachten wir Produkte der Potenzen der X_i:

Definition. Ein *Monom* in $X_1, \ldots, X_n$ ist ein Produkt der Form

$$X^b = X_1^{b_1} \cdots X_n^{b_n}, \quad b \in \mathbb{N}^n.$$

Durch Multiplikation eines Monoms mit einem Element $r \in R$ erhält man einen *Term* rX^a.

Es gilt

$$X^a(b) = \begin{cases} 1, & a = b, \\ 0, & \text{sonst.} \end{cases}$$

für $a, b \in \mathbb{N}^n$.

Satz 7.2. *Jedes $f \in R^{(\mathbb{N}^n)}$ hat eine Darstellung der Form*

$$f = \sum_{a \in \mathbb{N}^n} f_a X^a, \quad f_a \in R,$$

wobei $f_a \neq 0$ nur für endlich viele $a \in \mathbb{N}^n$ gilt. Die auftretenden Koeffizienten f_a sind eindeutig bestimmt: $f_a = f(a)$ für alle $a \in \mathbb{N}^n$.

Beweis. Natürlich ist $f = \sum f(a) X^a$, wie man durch Anwendung der linken und rechten Seite auf $b \in \mathbb{N}^n$ sofort prüft. Dies zeigt die Existenz der Darstellung.

Ist nun $f = \sum f_a X^a$, so gilt $f(a) = f_a$ für alle $a \in \mathbb{N}^n$, was die Eindeutigkeit beweist. □

Die X^a bilden also eine Basis von $R^{(\mathbb{N}^n)}$ als Modul über R. Damit haben wir den Anschluß an die übliche Schreibweise von Polynomen als Linearkombination von Monomen gefunden und kehren daher zur vertrauten Schreibweise $R[X_1, \ldots, X_n]$ statt $R^{(\mathbb{N}^n)}$ zurück. Häufig verwendet man auch andere Namen für die Unbekannten, wie z.B. X, Y, Z im Fall $n = 3$.

Wir können den Polynomring durch seine „universelle Eigenschaft“ charakterisieren:

Satz 7.3. *Seien S ein kommutativer Ring, $\varphi : R \to S$ ein Ringhomomorphismus und $y_1, \ldots, y_n \in S$. Dann existiert genau ein Homomorphismus von Ringen $\psi : R[X_x, \ldots, X_n] \to S$ mit $\psi|_R = \varphi|_R$ und $\psi(X_i) = y_i$. Diesen Homomorphismus nennt man dann* Substitutionshomomorphismus *oder* Einsetzungshomomorphismus.

Beweis. Wir definieren ψ mittels

$$\psi(\sum_{a\in\mathbb{N}^n} f_a X^a) = \sum_{a\in\mathbb{N}^n} \varphi(f_a)x^a.$$

Dabei haben wir die kompakte Schreibweise $x^a = y_1^{a_1} \cdots y_n^{a_n}$ verwendet. Nach Satz 7.2 ist ψ eine wohldefinierte Abbildung.

Außerdem ist ψ auch die einzig mögliche Abbildung, wenn sie ein Ringhomomorphismus sein soll. Dies folgt direkt daraus, daß ein Homomorphismus durch seine Bilder auf Erzeugenden bereits eindeutig bestimmt ist. Die X_i erzeugen aber gerade $R[X_1, \ldots, X_n]$ über R als Ring.

In der Tat ist ψ ein Ringhomomorphismus, denn für polynomiale Ausdrücke in $y_1, \ldots, y_n$ gelten genau die Rechenregeln, mit denen wir die Addition und Multiplikation in $R[X_1, \ldots, X_n]$ definiert haben. □

Der nächste Satz zeigt, daß man Polynomringe in mehreren Variablen durch sukzessives Adjungieren von einzelnen Variablen erhalten kann.

Satz 7.4. *Für alle $m, n \in \mathbb{N}$ existiert genau ein Isomorphismus*

$$(R[X_1, \ldots X_m])[Y_1, \ldots, Y_n] \to R[Z_1, \ldots, Z_{m+n}], \quad X_i \mapsto Z_i,\ Y_i \mapsto Z_{m+i},$$

der die identische Abbildung auf R erweitert.

Beweis. Nach dem Satz über den induzierten Homomorphismus gibt es genau einen Homomorphismus $\psi : R[X_1, \ldots, X_m] \to R[Z_1, \ldots, Z_{m+n}]$, der die natürliche Einbettung $R \mapsto R[Z_1, \ldots, Z_{m+n}]$ so erweitert, daß $\psi(X_i) = Z_i$ für $i = 1, \ldots, m$. Jetzt setzen wir $S = R[X_1, \ldots, X_m]$ und wenden den Satz auf $\psi : S \to R[Z_1, \ldots, Z_{m+n}]$ an. Wir können ψ so zu $\psi' : S[Y_1, \ldots, Y_n] \to R[Z_1, \ldots, Z_{m+n}]$ erweitern, daß $\psi'(Y_i) = Z_{m+i}$.

Umgekehrt kann man die Einbettung $R \mapsto (R[X_1, \ldots X_m])[Y_1, \ldots, Y_n]$ zu einem Homomorphismus $\chi : R[Z_1, \ldots, Z_{m+n}] \to (R[X_1, \ldots X_m])[Y_1, \ldots, Y_n]$ so erweitern, daß $\chi(Z_i) = X_i$ für $i = 1, \ldots, m$ und $\chi(Z_{m+i}) = Y_i$ für $i = 1, \ldots, n$.

Dann sind ψ' und χ zueinander invers, wie man wiederum aus Satz 7.3 schließen kann. □

Als nächstes wird der Begriff des Grades auf mehrere Veränderliche verallgemeinert:

Definition. Sei $X^a = X_1^{a_1} \cdots X_n^{a_n}$ ein Monom und $f = \sum_a f_a X^a$ ein Polynom $\neq 0$. Durch

$$\operatorname{grad} X^a = a_1 + \cdots + a_n, \qquad \operatorname{grad} f = \max\{\operatorname{grad} X^a : f_a \neq 0\}$$

ist der *Grad* (oder *Totalgrad*) von X^a bzw. f definiert. Wir setzen noch $\operatorname{grad} 0 = -\infty$.

Ein Polynom heißt *homogen* von Grad d, wenn $\operatorname{grad} X^a = d$ für alle $a \in \operatorname{supp}(f)$ gilt. Mit

$$f_d = \sum_{\operatorname{grad} X^a = d} f_a X^a$$

bezeichnet man die d-te *homogene Komponente* von f. Es gilt $f = \sum_{d \in \mathbb{N}} f_d$.

Wir können natürlich auch für jedes i den Exponenten a_i von X_i in $X_1^{a_1} \cdots X_n^{a_n}$ betrachten und den i-ten *Partialgrad* eines Polynoms entsprechend definieren.

Aber auch nach der Einführung dieses Grades läßt sich die Division mit Rest nicht auf Polynome in mehreren Veränderlichen übertragen. Das hat mehrere Gründe:

(a) Die homogene Komponente höchsten Grades ist im allgemeinen kein Monom.
(b) Im allgemeinen kann man aus $\operatorname{grad} X^a \leq \operatorname{grad} X^b$ keineswegs auf $X^a | X^b$ schließen.

Die Menge $\mathbb{N}^n$ ist mittels des komponentenweise Vergleichs

$$a \leq b \quad \Longleftrightarrow \quad a_i \leq b_i,\ i = 1, \ldots, n,$$

nur partiell geordnet. Nach Identifikation der $a \in \mathbb{N}^n$ mit den Monomen X^a beschreibt diese partielle Ordnung die Teilbarkeit von Monomen: $X^a \mid X^b \Longleftrightarrow a \leq b$. Dies ist unabhängig vom „umgebenden“ Ring R.

Das Lemma von Dickson. Es besagt, daß jede Teilmenge des $\mathbb{N}^n$ (oder jede Menge von Monomen) bezüglich der eingeführten partiellen Ordnung nur endlich viele minimale Elemente hat. Da wir an ringtheoretischen Anwendungen interessiert sind, formulieren wir es in der Sprache der Monome.

Lemma 7.5 (Dickson)**.** *Sei M eine nicht leere Menge von Monomen in $X_1, \ldots, X_n$. Dann gibt es eine endliche Teilmenge $N \subset M$, so daß für alle $\mu \in M$ ein $\nu \in N$ mit $\nu \mid \mu$ existiert.*

Beweis. Zunächst einmal ist klar, daß die Aussage des Lemmas dazu äquivalent ist, daß M nur endlich viele minimale Elemente bezüglich der Teilbarkeitsrelation hat: Existiert nämlich eine endliche Teilmenge N wie behauptet, so ist jedes minimale Element von M in N enthalten, und umgekehrt können wir N als Menge der minimalen Elemente wählen, wenn diese endlich ist.

Wir beweisen das Lemma durch Induktion nach n. Für $n = 1$ ist es leicht einzusehen: Wir wählen einfach $N = \{X^k\}$, wobei $k = \min\{i : X^i \in M\}$.

Sei $n > 1$. Für $i \in \mathbb{N}$ setzen wir

$$M_i = \{X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} : X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} X_n^i \in M\}.$$

Nach Induktionsvoraussetzung ist die Menge N_i der minimalen Elemente von M_i für alle i endlich.

Wir wenden die Induktionsvoraussetzung nochmals an, und zwar auf die Menge $M' = \bigcup_{i\in\mathbb{N}} N_i$. Da die Menge N' der in M' minimalen Elemente endlich ist, gilt $N' \subset \bigcup_{i=1}^{s} N_i$ für hinreichend großes $s \in \mathbb{N}$. Setze

$$N = \bigcup_{i=1}^{s} \{\mu X_n^i : \mu \in N_i\}$$

Sei nun $\mu = X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} X_n^j \in M$.

Erster Fall, $j \geq s$: Für $\mu' = X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} \in M_j$ existiert ein $\nu' \in N_j$, welches μ' teilt. Außerdem gibt es ein $\nu'' \in N'$, welches das ν' teilt. Es folgt also $\nu'' X_n^k \in N$ für ein $k \leq s$ und $\nu'' X_n^k$ teilt μ'.

Zweiter Fall, $j < s$: Dann existiert ein $\nu' \in N_j$, welches $X_1^{a_1} \cdots X_{n-1}^{a_{n-1}}$ teilt. Es folgt $\nu' X_n^j \in N$ und $\nu' X_n^j \mid \mu$. □

Monomiale Ordnungen. Im Fall $n = 1$ besitzt M genau ein minimales Element. Für $n > 1$ ist dies fast nie richtig. Dieses Problem lösen wir durch Einführung einer *monomialen Ordnung*:

Definition. Sei $\mathscr{M}$ die Menge aller Monome in den Unbestimmten $X_1, \ldots, X_n$. Eine lineare Ordnung $<$ auf $\mathscr{M}$ heißt *monomiale Ordnung* (oder *Termordnung*), wenn gilt:

(a) $1 < \mu$ für alle $\mu \in \mathscr{M} \setminus \{1\}$,
(b) $\mu'\mu < \mu'\nu$ für alle $\mu,\ \mu',\ \nu \in \mathscr{M}$ mit $\mu < \nu$ (Monotonie).

Ist also insbesondere μ ein Teiler von ν, d. h. $\nu = \mu\mu'$ für ein $\mu' \in \mathscr{M}$, dann folgt aus (a) und (b), daß

$$\mu = \mu 1 \leq \mu\mu' = \nu.$$

Wir nennen nun die drei wichtigsten Beispiele von monomialen Ordnungen. In allen drei Fällen kann man leicht überprüfen, daß die Eigenschaften (a) und (b) der Definition erfüllt sind.

Definition.

(a) Lexikographische Ordnung: $X^a <_{\text{lex}} X^b \iff X^a \neq X^b$ und die erste nichtverschwindene Komponente von $b - a$ ist positiv.
(b) Grad-lex-Ordnung: $X^a <_{\text{gradlex}} X^b \iff X^a \neq X^b$ und (i) $\operatorname{grad} X^a < \operatorname{grad} X^b$ oder (ii) $\operatorname{grad} X^a = \operatorname{grad} X^b$ und $X^a <_{\text{lex}} X^b$.

(c) Grad-revers-lex-Ordnung: $X^a <_{\text{revlex}} X^b \iff X^a \neq X^b$ und (i) grad X^a $<$ grad X^b oder (ii) bei grad X^a $=$ grad X^b die letzte Komponente von $b - a$ negativ ist.

Beispiel 7.6. Sei $n = 4$ und $X > Y > Z > W$. Dann gilt

$$X >_{\text{lex}} YW >_{\text{lex}} Z^2,$$
$$YW >_{\text{gradlex}} Z^2 >_{\text{gradlex}} X,$$
$$Z^2 >_{\text{revlex}} YW >_{\text{revlex}} X.$$

Für die drei oben eingeführten monomialen Ordnungen gilt

$$X_1 > \cdots > X_n.$$

Sobald eine solche Ordnung der Veränderlichen definiert ist, kann man diese lexikographisch, grad-lexikographisch oder revers-lexikographisch auf alle Monome fortsetzen. Man sollte sich folgendes Prinzip merken: *In der lexikographischen Ordnung machen große Faktoren ein Monom groß, in der revers-lexikographischen Ordnung machen kleine Faktoren es klein.* Es ist keineswegs so, daß die revers-lexikographische Ordnung einfach durch Umkehrung der lexikographischen entsteht. (Wir vergleichen diese beide Ordnungen in einer Übungsaufgabe.)

Reduktion. Der folgende Satz ist fundamental in theoretischer und algorithmischer Hinsicht. Er ermöglicht Indukionsbeweise „über die Termordnung“ und stellt sicher, daß Algorithmen in endlich vielen Schritten terminieren, wenn sie die jeweils „kritischen“ Polynome durch kleinere Monome ersetzen.

Satz 7.7. *Sei $<$ eine monomiale Ordnung auf $\mathscr{M}$. Dann besitzt jede nichtleere Teilmenge $N \subset \mathscr{M}$ ein genau ein minimales Element. Jede echt absteigende Kette in $\mathscr{M}$ besitzt nur endlich viele Glieder.*

Beweis. Nach Lemma von Dickson ist die Teilmenge N_0 der bezüglich Teilbarkeit minimalen Elemente endlich. Sei $\nu_0 \in N_0$ das bezüglich „ $<$“ minimale Element in N_0. Dies ist auch minimal in N bezüglich $<$: Zu jedem $\nu \in N$ existiert nämlich ein $\nu' \in N_0$ mit $\nu' \mid \nu$. Es folgt $\nu' \leq \nu$. Nach Annahme über ν_0 gilt dann $\nu_0 \leq \nu' \leq \nu$.

Die zweite Aussage folgt unmittelbar aus der ersten: Angenommen, die Kette $\mu_0 > \mu_1 > \cdots$ sei unendlich. Dann hat $\{\mu_n : n \in \mathbb{N}\}$ kein minimales Element. (Es würde für die zweite Aussage genügen, daß jede nichtleere Teilmenge mindestens ein minimales Element besitzt.) □

Wenn es zu jedem $\mu \in \mathscr{M}$ nur endlich viele $\nu \in \mathscr{M}$ mit $\nu < \mu$ gibt, dann ist $\mathscr{M}$ ials geordnete Menge isomorph zu $\mathbb{N}$. Wir können den Isomorphismus einfach durch

$$\varphi(\mu) = \#\{\nu : \nu < \mu\}$$

definieren. Dann ist φ injektiv, weil $\mathscr{M}$ linear geordnet ist und surjektiv, weil $\mathscr{M}$ zusätzlich unendlich ist. Dies gilt für alle grad-monotonen monomialen Ordnungen wie gradlex oder revlex, ist im allgemeinen aber falsch, wie das Beispiel der lexikographischen Ordnung zeigt: $X > Y^k$ für alle k, wenn $X > Y$.

Wir setzen im folgenden voraus, daß der Ring R der Koeffizienten ein Körper K ist.

Definition. Sei $<$ eine Termordnung auf $K[X_1, \ldots, X_n]$ und $f = \sum_a f(a) X^a$ ein Polynom. Dann heißt

$$\mathrm{LM}_<(f) = \max_< \mathrm{supp}(f)$$

das *Initialmonom* von f und f_b für $b = \mathrm{LM}_<(f)$ der *Initialkoeffizient* $\mathrm{LC}_<(f) = f_b$. Wir nennen

$$\mathrm{LT}_<(f) = \mathrm{LC}_<(f)\,\mathrm{LM}_<(f)$$

den *Initialterm* von f. Besteht kein Zweifel über die Termordnung, so wird der Index $<$ weggelassen.

Um lästige Fallunterscheidungen zu vermeiden, ordnen wir dem Nullpolynom das Initialmonom $X^{-\infty}$ zu, wobei $X^{-\infty} < X^a$ für alle $a \in \mathbb{N}^n$ gelten soll. Wir betrachten $X^{-\infty}$ ebensowenig als Element des Polynomringes, wie ∞ als reelle Zahl angesehen wird.

Beispiel 7.8. Sei $n = 4$, $X > Y > Z > W$ und $f = X + YW + Z^2$. Dann ist

$$\mathrm{LM}_{\mathrm{lex}}(f) = X, \quad \mathrm{LM}_{\mathrm{gradlex}}(f) = YW, \quad \mathrm{LM}_{\mathrm{revlex}}(f) = Z^2.$$

Für das Rechnen mit Initialmonomen gelten folgende Regeln:

Satz 7.9. *Sei $<$ eine monomiale Ordnung auf $K[X_1, \ldots, X_n]$. Dann gilt:*

(a) $\mathrm{LM}(fg) = \mathrm{LM}(f)\,\mathrm{LM}(g)$

(b) $\mathrm{LM}(f + g) \leq \max(\mathrm{LM}(f), \mathrm{LM}(g))$

für alle $f, g \in K[X_1, \ldots, X_n]$.

In (b) *gilt Gleichheit, wenn* $\mathrm{LM}(f) \neq \mathrm{LM}(g)$.

Beweis. Die erste Gleichung folgt aus der Monotonie der monomialen Ordnung bezüglich der Multiplikation und der Tatsache, daß jedes $X^a \in \mathrm{supp}(fg)$ von der Form $X^b X^c$ mit $X^b \in \mathrm{supp}(f)$, $X^c \in \mathrm{supp}(g)$ ist, wenn $f, g \neq 0$. Im Fall $f = 0$ oder $g = 0$ ist $\mathrm{LM}(f) = X^{-\infty} = \mathrm{LM}(fg)$. Die Ungleichung ergibt sich aus

$$\mathrm{supp}(f + g) \subset \mathrm{supp}(f) \cup \mathrm{supp}(g).$$

Wenn $\mathrm{LM}(f) > \mathrm{LM}(g)$, dann ist $\mathrm{LM}(f) \in \mathrm{supp}(f + g)$, und wir erhalten $\mathrm{LM}(f + g) = \mathrm{LM}(f)$. Dies beweist die letzte Aussage. □

Wir können nun denn grundlegenden Satz über die Division mit Rest formulieren. Wir lassen dabei gleich mehrere Teiler zu.

Satz 7.10. *Seien* $f, g_1, \ldots, g_m \in K[X_1, \ldots, X_n]$, $g_1, \ldots g_m \neq 0$. *Dann existieren Polynome* $q_1, \ldots, q_m, r \in K[X_1, \ldots, X_n]$ *mit folgenden Eigenschaften:*

(a) $f = q_1 g_1 + \cdots + q_m g_m + r$,
(b) $\mathrm{LM}(q_i g_i) \leq \mathrm{LM}(f)$ *für* $i = 1, \ldots, m$,
(c) $\mathrm{LM}(g_i)$, $i = 1, \ldots, m$, *teilt keines der Monome* $X^a \in \mathrm{supp}(r)$.

Beweis. Sei

$$G = \{X^a \in \mathrm{supp}(f) : X^a \text{ wird von einem der Monome } \mathrm{LM}(g_i) \text{ geteilt}\}.$$

Im Fall $G = \emptyset$ können wir $q_1 = \cdots = q_m = 0$ und $r = f$ wählen. Im Fall $G \neq \emptyset$ sei $X^b = \max(G)$ und X^b werde von $\mathrm{LM}(g_i)$ geteilt. Wir schreiben $f = \sum_a f_a X^a$ und setzen

$$\tilde{f} = f - \frac{f_b}{\mathrm{LC}(g_i)} \cdot \frac{X^b}{\mathrm{LM}(g_i)} \cdot g_i.$$

Dann gilt $X^b \notin \mathrm{supp}(\tilde{f})$, denn für

$$\tilde{g} = \frac{f_b}{\mathrm{LC}(g_i)} \cdot \frac{X^b}{\mathrm{LM}(g_i)} \cdot g_i$$

ist $\mathrm{LT}(\tilde{g}) = f_b X^b$, so daß die X^b-Terme sich gerade wegheben. Außerdem ist

$$X^a \notin G \quad \text{für } a \in \mathrm{supp}(\tilde{f}),\ X^a > X^b,$$

Wir können also auf $\tilde{f}$ Induktion über die monomiale Ordnung anwenden und erhalten eine Darstellung, welche den Bedingungen des Satzes genügt:

$$\tilde{f} = \tilde{q}_1 g_1 + \cdots + \tilde{q}_m g_m + \tilde{r}.$$

Wir setzen $q_j = \tilde{q}_j$ für $i \neq j$, $r = \tilde{r}$ und

$$q_i = \tilde{q}_i + \frac{f_b}{\mathrm{LC}(g_i)} \cdot \frac{X^b}{\mathrm{LM}(g_i)}.$$

Dann gelten (a) und (c) offensichtlich, und auch (b) ist erfüllt, denn

$$\mathrm{LM}(q_i g_i) \leq \max\big(\mathrm{LM}(\tilde{q}_i g_i)\, \mathrm{LM}(\tilde{g})\big) \leq \mathrm{LM}(f). \qquad \square$$

Definition. Man nennt r eine *Reduktion* von f modulo $g_1, \ldots, g_m$. Falls kein Monom X^a mit $a \in \mathrm{supp}(f)$ von einem der $\mathrm{LM}(g_i)$ geteilt wird, nennt man f *reduziert* modulo $g_1, \ldots, g_m$.

Ohne weitere Bedingungen ist r aber keineswegs eindeutig bestimmt. „Algorithmisch“ läßt sich Eindeutigkeit erreichen, wenn man verlangt, daß für i im Beweis des Satzes der kleinstmögliche Wert gewählt wird. Andere Bedingungen, die r eindeutig bestimmen, werden wir noch kennenlernen.

Beispiel 7.11. Sei $n = 2$ und $<$ die lexikographische Ordnung mit $X > Y$. Es sei

$$f = X^2Y + XY^2 + Y^2,\ g_1 = XY - 1,\ g_2 = Y^2 - 1$$

Man erhält dann zwei verschiedene Reduktionen von f:

$$f = (X + Y)g_1 + g_2 + (X + Y + 1) = Xg_1 + (X + 1)g_2 + 2X + 1.$$

Weiterführende Literatur: [**Sing**], [**IVA**], [**CCA**].

ABSCHNITT 8

Ideale und ihre Gröbner-Basen

Gröbner-Basen. Zur Erinnerung: Eine Teilmenge eines Ringes R heißt ein Ideal, wenn $I \neq \emptyset$ und mit $x, y \in I$, $r \in R$ auch $x + y$, $rx \in I$ gilt. Ideale sind genau die Kerne von Ringhomomorphismen, und dies erklärt ihre Bedeutung. In diesem Abschnitt geht es uns darum, den Zusammenhang zwischen der Idealtheorie und den im letzten Abschnitt entwickelten Begriffen herzustellen.

Definition. Sei I ein Ideal in $K[X_1, \ldots, X_n]$ und $<$ eine monomiale Ordnung. Man nennt eine Teilmenge $G \subset I$ eine *Gröbner-Basis* von I bezüglich $<$, wenn es zu jedem $f \in I$, $f \neq 0$ ein $g \in G$ mit

$$\mathrm{LM}(g) \mid \mathrm{LM}(f)$$

gibt.

Im folgenden sei stets eine monomiale Ordnung auf $K[X_1, \ldots, X_n]$ gegeben.

Natürlich ist I eine triviale Gröbner-Basis von sich selbst. Es gibt aber auch stets endliche Gröbner-Basen.

Satz 8.1. *Mit den Bezeichnungen der Definition gilt: Jede Gröbner-Basis G von I enthält eine endliche Gröbner-Basis G'.*

Beweis. Im Fall $I = 0$ ist $G = \emptyset$ eine Gröbner-Basis. Sei nun $I \neq 0$. Wir bilden

$$\mathscr{M} = \{\mathrm{LM}(f) : f \in I,\ f \neq 0\}.$$

Nach dem Lemma von Dickson ist die Teilmenge $\mathscr{M}_0$ der bezüglich Teilbarkeit minimalen Elemente in $\mathscr{M}$ endlich. Wir setzen

$$G' = \{g_{\mu'} : \mu' \in \mathscr{M}_0\},$$

wobei $g_{\mu'} \in G \subset I$ so gewählt ist, daß $\mathrm{LM}(g_{\mu'}) \mid \mu'$ und damit $\mathrm{LM}(g_{\mu'}) = \mu'$. □

Dieser Satz zeigt, daß es genügt, endliche Gröbner-Basen zu betrachten.

Satz 8.2. *Sei $I \subset K[X_1, \ldots, X_n]$ ein Ideal und $G := \{g_1, \ldots, g_m\}$ eine endliche Teilmenge von I. Dann sind äquivalent:*

(a) *G ist eine Gröbner-Basis von I.*

(b) *Jedes $f \in I$ reduziert sich modulo G zu 0, und dabei spielt die Anordnung von G keine Rolle.*

Beweis. (a) $\Rightarrow$ (b): Sei $f \in I$, $f \neq 0$. Es existiert ein $g_j \in G$, so daß $\mathrm{LM}(g_j) \mid \mathrm{LM}(f)$. Setze $f' := f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_j)} g_j$. Dann ist $\mathrm{LM}(f') < \mathrm{LM}(f)$ und $f' \in I$. Induktiv (über $\mathrm{LM}(f)$) folgt die Existenz von $q'_1, \ldots, q'_m$ mit

$$f' = q'_1 g_1 + \cdots + q'_m g_m, \quad \mathrm{LM}(q'_i g_i) \leq \mathrm{LM}(f') < \mathrm{LM}(f),\ i = 1, \ldots, m.$$

Wir setzen

$$q_i = \begin{cases} q'_j + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_j)}, & i = j, \\ q'_i, & \text{sonst.} \end{cases}$$

(b) $\Rightarrow$ (a): Nach Voraussetzung besitzt f eine Darstellung

$$f = q_1 g_1 + \ldots q_m g_m, \quad \mathrm{LM}(q_i g_i) \leq \mathrm{LM}(f),\ i = 1, \ldots, m.$$

Dabei muß $\mathrm{LM}(q_i g_i) = \mathrm{LM}(f)$ gelten für mindestens ein i. Es folgt $\mathrm{LM}(g_i) \mid \mathrm{LM}(f)$. □

Korollar 8.3. *Jede Gröbner-Basis eines Ideals $I \subset K[X_1, \ldots, X_n]$ ist ein Erzeugendensystem von I. Insbesondere ist I endlich erzeugt.*

Wir nennen dabei eine Teilmenge E des Ideals I im Ring R ein *Erzeugendensystem*, wenn sich jedes Element von I als Linearkombination von Elementen aus E mit Koeffizienten aus R schreiben läßt. Sei $(x_k)_{k \in M}$ eine Familie von Elementen von R. Dann bezeichnet

$$(x_k : k \in M)$$

traditionell (auch) das von den x_k erzeugte Ideal, also das kleinste Ideal, das alle x_k enthält. Wir erhalten es auch als Menge aller Linearkombinationen

$$r_1 x_{k_1} + \cdots + r_m x_{k_m}$$

der x_k mit Koeffizienten aus R. Im Fall einer endlichen Familie schreiben wir $(f_1, \ldots, f_m)$, um das von $f_1, \ldots, f_m$ erzeugte Ideal zu benennen. (Es sollte stets klar sein, ob wir das von den f_i gebildete m-Tupel oder das von ihnen erzeugte Ideal meinen.)

Ringe, in denen jedes Ideal endlich erzeugt ist, heißen *noethersch*. Korollar 8.3 besagt, daß $K[X_1, \ldots, X_n]$ ein noetherscher Ring ist, Das ist ein Spezialfall des *Hilbertschen Basissatzes*, der allgemeiner besagt, daß mit R auch $R[X]$ noethersch ist. Mit Induktion folgt dann, daß auch $R[X_1, \ldots, X_n]$ für alle n noethersch ist. Man kann den Hilbertschen Basissatz, der älter ist als das Lemma von Dickson, ähnlich wie dieses beweisen.

Allerdings ist nicht jedes Erzeugendensystem auch eine Gröbner-Basis des erzeugten Ideals.

Beispiel 8.4.

$$R = K[X, Y], \quad g_1 = XY + 1,\ g_2 = Y^2 - 1, \quad I = (g_1, g_2).$$

Dann ist $g_3 = X + Y = Yg_1 - Xg_2 \in I$, aber weder $\mathrm{LM}(g_1) = XY$ noch $\mathrm{LM}(g_2) = Y^2$ teilt $\mathrm{LM}(g_3)$ (unabhängig von der monomialen Ordnung).

Abgesehen von ihrer grundlegenden Bedeutung für das Rechnen mit Polynomen in $K[X_1, \ldots, X_n]$ sind Gröbner-Basen auch ein wichtiges Hilfsmittel für strukturelle Überlegungen, weil sie uns erlauben, das Ideal I mit dem *Initialideal*

$$\mathrm{LM}(I) = (\mathrm{LM}(f) : f \in I)$$

zu vergleichen.

Monomiale Ideale. Wir nennen ein Ideal *monomial*, falls es von Monomen erzeugt wird. Monomiale Ideale haben eine sehr viel einfachere Struktur als „allgemeine" Ideale. Dies zeigt sich schon in folgendem

Satz 8.5. *Sei $I \subset K[X_1, \ldots, X_n]$ ein Ideal.*

(a) *Genau dann ist I monomial, wenn mit jedem $f \in I$, $f = \sum f_b X^b$ auch alle Monome X^b für $b \in \mathrm{supp}(f)$ in I liegen.*

(b) *Ein monomiales Ideal besitzt ein eindeutig bestimmtes minimales Erzeugendensystem aus Monomen. Dieses besteht aus den bezüglich Teilbarkeit minimalen Elementen in der Menge der Monome in I.*

Beweis. (a) Sei I ein monomiales Ideal, etwa erzeugt von $X^{a_1}, \ldots, X^{a_m}$. (Wir wissen bereits, daß jedes Ideal in $K[X_1, \ldots, X_n]$ endlich erzeugt ist, und in diesem Fall enthält jedes Erzeugendensystem ein endliches.) Sei $f \in I$. Dann gilt

$$f = \sum_{i=1}^{m} q_i X^{a_i}$$

mit $q_1, \ldots, q_m \in K[X_1, \ldots, X_n]$. Für $b \in \mathrm{supp}(f)$ gilt also $b \in \bigcup_i \mathrm{supp}(q_i X^{a_i})$, und jedes Monom X^c mit $c \in \mathrm{supp}(q_i X^{a_i})$ ist durch X^{a_i} teilbar. Folglich existiert ein i mit $X^{a_i} \mid X^b$, so daß $X^b \in I$.

Die Umkehrung ist trivial, denn jedes Polynom liegt ja in dem von „seinen" Monomen erzeugten Ideal.

(b) Sei $\mathscr{M}$ die Menge der Monome in I, $\mathscr{M}_0$ die Menge der hinsichtlich Teilbarkeit minimalen Elemente in $\mathscr{M}$ und $\mathscr{N}$ ein monomiales Erzeugendensystem von I. Dann ist jedes $X^b \in \mathscr{N}$ Vielfaches eines $X^a \in \mathscr{M}_0$, so daß jedes $X^b \in \mathscr{N}$ in dem von $\mathscr{M}_0$ erzeugten Ideal enthalten ist: $\mathscr{M}_0$ erzeugt I.

Es muß nun aber auch $\mathscr{M}_0 \subset \mathscr{N}$ gelten, denn $\mathscr{M}_0 \subset I$, und gemäß dem Beweis von (a) ist jedes Element $X^a \in \mathscr{M}_0$ Vielfaches eines Elements $X^b \in \mathscr{N}$. Das kann aber nur für $X^a = X^b$ gelten, da X^a (per Definition von $\mathscr{M}_0$) von keinem Monom in I außer sich selbst geteilt wird.

Insgesamt folgt: $\mathscr{M}_0$ ist das einzige minimale monomiale Erzeugendensystem von I. □

Das Liften von Syzygien. Um Gröbnerbasen für das praktische Rechnen nutzbar zu machen, brauchen wir einen Algorithmus, der es uns erlaubt, aus einem gegebenen Erzeugendensystem eine Gröbner-Basis zu berechnen. Einen solchen wollen wir im folgenden entwickeln.

Sei wieder allgemein $I = (g_1, \ldots, g_m)$ ein Ideal und $f = q_1 g_1 + \cdots + q_m g_m$ mit

$$X^b = \max\{\mathrm{LM}(q_i g_i) : i = 1, \ldots, m\} = \mathrm{LM}(q_k g_k).$$

Ist $X^b = \mathrm{LM}(f)$, dann folgt sofort $\mathrm{LM}(f) = \mathrm{LM}(q_k g_k)$ und die Darstellung von f zwingt uns nicht, $g_1, \ldots, g_m$ durch ein weiteres Polynom zu ergänzen, um einer Gröbner-Basis näher zu kommen: f läßt sich modulo $g_1, \ldots, g_m$ reduzieren.

Wenn wir mit den Bezeichnungen des Beispiels 8.4

$$f = XY + Y^2$$

wählen, dann gilt

$$f = XY + Y^2 = Yg_1 - Xg_2 + (Y - 1)g_3.$$

Wir haben eine Darstellung von f als Linearkombination von g_1, g_2, g_3 mit den Koeffizienten $q_1 = Y$, $q_2 = -X$, $q_3 = Y - 1$. Es gilt aber

$$\max\{\mathrm{LM}(q_1 g_1), \mathrm{LM}(q_2 g_2), \mathrm{LM}(q_3 g_3)\} = XY^2 > \mathrm{LM}(f) = XY,$$

wenn wir etwa die lexikographische Ordnung mit $X > Y$ betrachten. Wir können nun aber keinesfalls schließen, daß g_1, g_2, g_3 keine Gröbner-Basis ist.

Dieser Schluß ist deshalb unzulässig, weil die q_i nicht eindeutig bestimmt sind und sich Leitterme der Produkte $q_i g_i$ wegheben können (und im Beispiel auch tun). Die Nichteindeutigkeit der Koeffizienten von Linearkombinationen wird durch Syzygien erfaßt:

Definition. Seien $g_1, \ldots, g_m \in R$. Ein m-Tupel $(s_1, \ldots, s_m) \in R^m$ heißt *Syzygie* von $g_1, \ldots, g_m$, wenn

$$s_1 g_1 + \cdots + s_m g_m = 0$$

ist.

Mit den Bezeichnungen des Beispiels 8.4 ist $s = (Y, -X, -1)$ eine Syzygie von g_1, g_2, g_3, denn

$$Yg_1 - Xg_2 + (-1)g_3 = 0.$$

Im Fall $X^b > \mathrm{LM}(f)$ können wir also versuchen, die q_i durch hinsichtlich der monomialen Ordnung kleinere Faktoren zu ersetzen, bis wir nach einer Kette solcher Ersetzungen in der Situation $X^b = \mathrm{LM}(f)$ angekommen sind - oder steckenbleiben! Bei einer solchen Ersetzung müssen wir von

$$f = q_1 g_1 + \cdots + q_m g_m$$

übergehen zu

$$f = (q_1 - s_1)g_1 + \cdots + (q_m - s_m)g_m,$$

wobei sie s_i eine Syzygie der g_i bilden.

Um die folgenden Überlegungen technisch besser beschreibbar zu machen, erweitern wir die Begriffe Initialmonom und Initialterm auf Elemente von R^m.

Definition. Das *Initialmonom* von $s = (s_1, \ldots, s_m) \in R^m$ *bezüglich der Gewichte* $X^{a_1}, \ldots, X^{a_m}$ sei

$$\mathrm{LM}(s) = \max\{X^{a_i}\,\mathrm{LM}(s_i) : i = 1, \ldots, m\}$$

und der *Initialterm* $\mathrm{LT}(s) \in R^m$ sei das Element mit den Komponenten

$$\mathrm{LT}(s)_i = \begin{cases} \mathrm{LT}(s_i), & X^{a_i}\,\mathrm{LM}(s_i) = \mathrm{LM}(s), \\ 0, & \text{sonst.} \end{cases}$$

Ferner sagen wir, daß s *multihomogen* (bezüglich der Gewichte $X^{a_1}, \ldots, X^{a_m}$) sei, wenn $s = \mathrm{LT}(s)$ gilt.

Die multihomogenen Elemente s sind durch folgende Eigenschaften gekennzeichnet: Sie haben in jeder Komponente s_i einen Term $r_i X^{b_i}$, und überdies gilt $X^{a_i} X^{b_i} = X^{a_j} X^{b_j}$ für alle i, j mit $r_i, r_j \neq 0$. Dies zeigt, daß die Eigenschaft multihomogen zu sein, von der monomialen Ordnung unabhängig ist.

Wir setzen im folgenden stillschweigend voraus, daß stets mit den Gewichten $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m)$ gearbeitet wird. In unserem obigen Beispiel ist $\mathrm{LM}(s) = XY^2$ und $\mathrm{LT}(s) = (X, -Y, 0)$.

Wir kehren nun zu der Situation

$$f = q_1 g_1 + \cdots + q_m g_m, \quad \mathrm{LM}(f) < X^b = \mathrm{LM}(q),$$

zurück. Dabei haben wir $q = (q_1, \ldots, q_m)$ gesetzt. Diese Gleichung kann nur bestehen, wenn sich in der Linearkombination auf der rechten Seite die Terme mit Monom X^b wegheben. Dies ist genau dann der Fall, wenn für $t = \mathrm{LT}(q)$ gilt:

$$t_1\,\mathrm{LT}(g_1) + \cdots + t_m\,\mathrm{LT}(g_m) = 0,$$

mit anderen Worten, wenn t eine Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ ist. (Dies ist im Beispiel erfüllt.) Da $t = \mathrm{LT}(t)$, ist t multihomogen.

Genau dann erreichen wir durch Übergang von $f = q_1 g_1 + \cdots + q_m g_m$ zu $f = (q_1 - s_1)g_1 + \cdots + (q_m - s_m)g_m$, daß $\mathrm{LM}(q - s) < \mathrm{LM}(q)$, wenn

$$\mathrm{LT}(s) = \mathrm{LT}(q).$$

Dies bedeutet: Wir benötigen eine Syzygie s von $g_1, \ldots, g_m$, für die $\mathrm{LT}(s)$ genau die Syzygie t von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ ist.

Definition. Wir sagen, daß die Syzygie s von $g_1, \ldots, g_m$ die multihomogene Syzygie t von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ *liftet*, wenn $\mathrm{LT}(s) = t$.

Wenn wir also $t = \mathrm{LT}(q)$ zu einer Syzygie s von $g_1, \ldots, g_m$ liften können, haben wir unser Ziel erreicht, das Initialmonom von q durch das kleinere Initialmonom von $q - s$ zu ersetzen.

Läßt sich jede multihomogene Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ liften, so können wir den Prozeß iterieren, bis wir schließlich eine Linearkombination $f = \tilde{q}_1 g_1 + \cdots + \tilde{q}_m g_m$ mit $\mathrm{LM}(\tilde{q}) = \mathrm{LM}(f)$ erreicht haben. Dann aber gilt $\mathrm{LM}(g_i) \mid \mathrm{LM}(f)$ für mindestens ein i, und $g_1, \ldots, g_m$ hat sich als Gröbner-Basis des von $g_1, \ldots, g_m$ erzeugten Ideals herausgestellt.

Dies zeigt die Implikation (b) $\Rightarrow$ (a) in

Satz 8.6. *Sei $I = (g_1, \ldots, g_m)$. Dann sind äquivalent:*

(a) *$g_1, \ldots, g_m$ ist eine Gröbner-Basis von I.*
(b) *Jede multihomogene Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ läßt sich liften.*

Beweis. Nur noch (a) $\Rightarrow$ (b) ist zu zeigen. Sei $t \in R^m$ eine multihomogene Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$. Dann betrachten wir

$$f = t_1 g_1 + \cdots + t_m g_m \in I.$$

Es gilt $\mathrm{LM}(f) < \mathrm{LM}(t)$, da t eine Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ ist.

Nach Satz 8.2 reduziert sich f zu 0 modulo $g_1, \ldots, g_m$. Es gibt also eine Darstellung

$$f = s_1 g_1 + \ldots s_m g_m \quad \text{mit } \mathrm{LM}(s) \leq \mathrm{LM}(f).$$

Offensichtlich ist $t - s$ eine Syzygie von $g_1, \ldots, g_m$. Da aber $\mathrm{LM}(s) \leq \mathrm{LM}(f) < \mathrm{LM}(t)$, folgt $t = \mathrm{LT}(t - s)$. □

Im Beweis haben wir gerade folgendes Argument benutzt, das wir gesondert festhalten:

Satz 8.7. *Sei $t = (t_1, \ldots, t_m)$ eine multihomogene Syzygie von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$. Wenn sich $t_1 g_1 + \cdots + t_m g_m$ modulo $g_1, \ldots, g_m$ zu 0 reduziert, läßt sich t liften zu einer Syzygie von $g_1, \ldots, g_m$.*

Das Buchberger-Kriterium. Entscheidend für die Wirksamkeit der vorangegangenen Sätze ist, daß wir nur endlich viele Syzygien zu testen brauchen. Sei e_i der i–te Einheitsvektor des R^m. (Wir erlauben uns von Vektoren zu sprechen, obwohl R^m kein Vektorraum über R ist.) Dann ist durch

$$\varkappa_{ij} := \frac{\mathrm{LT}(g_j)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))} e_i - \frac{\mathrm{LT}(g_i)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))} e_j$$

eine multihomogene Syzygie der Initialterme von $g_1, \ldots, g_m$ gegeben. Sie ist liftbar genau dann, wenn das sogenannte *S-Polynom*

$$S_{ij} = \frac{\mathrm{LT}(g_j)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))} g_i - \frac{\mathrm{LT}(g_i)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))} g_j$$

sich modulo $g_1, \ldots, g_m$ zu 0 reduziert.

Satz 8.8 (Buchberger-Kriterium)**.** *Sei $g_1, \ldots, g_m \in R$ ein Erzeugendensystem des Ideals $I \subset K[X_1, \ldots, X_n]$. Dann sind äquivalent:*

(a) *$g_1, \ldots, g_m$ ist eine Gröbner-Basis von I.*
(b) *Alle $\varkappa_{ij}$ mit $i < j$ lassen sich zu Syzygien von $g_1, \ldots, g_m$ liften.*
(c) *Alle S_{ij} reduzieren sich modulo $g_1, \ldots, g_m$ zu 0.*

Beweis. Wir haben schon gesehen, daß (a) $\Rightarrow$ (c) und (c) $\Rightarrow$ (b). Es bleibt (b) $\Rightarrow$ (a) zu zeigen.

Um uns im folgenden nicht mit den Leitkoeffizienten beschäftigen zu müssen, nehmen wir an, daß alle g_i den Leitkoeffizienten 1 haben. Dies hat offensichtlich auf keine der drei Aussagen (a) – (c) wesentlichen Einfluß.

Wir haben gesehen, daß es genügt, multihomogene Syzygien $(t_1, \ldots, t_m)$ von $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$ zu liften. Sei $j = \min\{i : t_i \neq 0\}$ und $k = \min\{i > j : t_i \neq 0\}$. Beachte, daß mindestens zwei Komponenten $t_i \neq 0$ sind! Wäre es nur eine einzige, dann müßte $t_i \,\mathrm{LT}(g_i) = 0$ sein, obwohl $t_i, \mathrm{LT}(g_i) \neq 0$.

Wir dürfen annehmen, daß t_j ein Monom ist. Andernfalls teilen wir zunächst durch den Koeffizienten des Terms t_j und multiplizieren die erreichte Liftung wieder mit ihm.

Wir betrachten zunächst den Fall, daß $t_i = 0$ für alle $i \neq j, k$. Dann ist $t_i \,\mathrm{LT}(g_i) = -t_j \,\mathrm{LT}(g_j)$. Nach Kürzen von $\mathrm{ggT}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$ ergibt sich

$$t_i u = -t_j v, \quad u = \frac{\mathrm{LT}(g_j)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}, \quad v = \frac{\mathrm{LT}(g_i)}{\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}. \quad (3)$$

Wegen der Teilerfremdheit der Monome u und v folgt $t_i = wv$, $t_j = -wu$ für einen Monom w. Also ist

$$t = w\varkappa_{jk}.$$

Nach Voraussetzung ist $\varkappa_{jk}$ liftbar und damit auch $w\varkappa_{jk}$ – die Multiplikation wit dem Monom w überführt die Liftung von $\varkappa_{jk}$ in die von $w\varkappa_{jk}$.

Sei nun $t_i \neq 0$ für ein $i \neq j, k$. Jedes Produkt $t_i \,\mathrm{LT}(g_i) \neq 0$ ist von der Form $r_i X^b$ mit dem Monom $\mathrm{LM}(t)$ und $r_i \in K$, $r_i \neq 0$. Es gilt $\sum r_i = 0$ und $r_j = 1$ nach unserer Annahme über die g_i und t.

Wir können nun durch Subtraktion eines Vielfachen von $\varkappa_{jk}$ der Form $w\varkappa_{jk}$ mit einem Monom w zu einer multihomogenen Syzygie $t' = t - w\varkappa_{jk}$ gleichen Initialmonoms kommen, so daß $t'_i = 0$ für $i = 1, \ldots, j$. Dann können wir absteigende Induktion über j anwenden und t' nach Induktionsvoraussetzung zu s' liften. Da wir, wie schon gesehen, auch $w\varkappa_{jk}$ zu einer Syzygie s'' liften können, erhalten wir mit $s' + s''$ eine Liftung von t. (Dabei ist wesentlich, daß $\mathrm{LM}(s') = \mathrm{LM}(s'') = \mathrm{LM}(s)$.)

Man findet nun $w\varkappa_{jk}$ wie folgt. Es gilt

$$t_i \operatorname{LM}(g_i) = -(r_j + \cdots + r_m)X^b = X^b = \frac{1}{\operatorname{LC}(t_j)} t_j \operatorname{LM}(g_j),$$

so daß wir nach Teilen durch $\operatorname{ggT}(\operatorname{LM}(g_i), \operatorname{LM}(g_j))$ wieder bei einer Gleichung der Form (3) ankommen. Wie dort folgt $t_i = wu$ mit u wie oben, und $t - w\varkappa_{jk}$ hat die gewünschte Form. □

Beispiel 8.9. Sei wie schon so oft $R = K[X, Y]$, $g_1 = XY + 1$, $g_2 = Y^2 - 1$ und $<$ die lexikographische Ordnung mit $X > Y$. Dann ist

$$S_{12} = Yg_1 - Xg_2 = X + Y$$

und also $g_1,\ g_2$ keine Gröbner-Basis, denn keines der Leitmonome $\operatorname{LM}(g_1), \operatorname{LM}(g_2)$ teilt X. Nun setzen wir $g_3 = X + Y$ und testen, ob $g_1,\ g_2,\ g_3$ eine Gröbner-Basis bilden. Es gilt

$$\begin{aligned} S_{12} &= g_3, \\ S_{13} &= g_1 - Yg_3 = Y^2 - 1 = -g_2, \\ S_{23} &= Xg_2 - Y^2 g_3 = -X + Y^3 = -g_3 + Y^3 - Y = -g_3 + Yg_2. \end{aligned}$$

Alle drei S-Polynome lassen sich also modulo g_1, g_2, g_3 zu 0 reduzieren. Somit bilden g_1, g_2, g_3 eine Gröbner-Basis. Es stellt sich sogar heraus, daß g_1 überflüssig ist, denn $\operatorname{LM}(g_3)$ teilt $\operatorname{LM}(g_1)$.

Der Buchberger-Algorithmus. Die konsequente Fortsetzung der Überlegung dieses Beispiels führt auf den *Buchberger-Algorithmus*. Sei $I = (g_1, \ldots, g_m) \subset K[X_1, \ldots, X_n]$ das von $g_1, \ldots, g_m$ erzeugte Ideal. Der folgende Algorithmus findet dann eine Gröbner-Basis von I.

Algorithmus 8.10. Buchberger-Algorithmus

(1) Setze $G = \{g_1, \ldots, g_m\}$.
(2) Setze $G' = \emptyset$.
(3) Für alle $i, j = 1, \ldots, m, i < j$: Reduziere S_{ij} modulo $G \cup G'$ zu r; ist $r \neq 0$, dann ersetze G' durch $G' \cup \{r\}$.
(4) Ist $G' = \emptyset$, dann ist G eine Gröbner-Basis. Stoppe.
(5) Sonst setze $G = G \cup G'$, $m = \#G$, numeriere die Elemente von G als $g_1, \ldots, g_m$ und gehe zu (2).

Das ist der Buchberger-Algorithmus in seiner rohesten Form. In vielen Fällen hat er eine hohe Laufzeit. Daher ist eine effiziente Implementierung absolut notwendig. Mögliche Verbesserungen des Algorithmus sind unter anderem:

(a) Die naheliegende Unterscheidung von „alten“ und „neuen“ Polynomen in G, d. h. bereits reduzierte S-Polynome müssen nicht noch einmal reduziert werden.
(b) Ist $\mathrm{ggT}(\mathrm{LM}(g_i), \mathrm{LM}(g_j)) = 1$, dann reduziert sich S_{ij} schon modulo g_i, g_j zu 0 und man kann sich diese Reduktion sparen (vgl. Übungsaufgabe).
(c) Man betrachte zuerst diejenigen S-Polynome, die in ihrer Reduktion mit hoher Wahrscheinlichkeit ein „kleines“ neues initiales Monom liefern. Ist die monomiale Ordnung grad-monoton, dann sollte man die S-Monome nach ihrem Grad ordnen und mit dem kleinsten beginnen. Bei der *normal selection strategy* ordnet man die S-Polynome nach $\mathrm{kgV}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$, beginnend mit dem kleinsten.

Wir haben noch zu beweisen, daß der Algorithmus nach endlich vielen Schritten stoppt. Sei $r \neq 0$, d. h. $\mathrm{LM}(r)$ wird von keinem der $\mathrm{LM}(g_i)$ geteilt. In Idealschreibweise bedeutet dies:

$$\mathrm{LM}(r) \notin \big(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m)\big).$$

Daraus folgt mit Satz 8.5, daß

$$\big(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m)\big) \subsetneq \big(\mathrm{LM}(r), \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m)\big).$$

Das Ideal der bereits gefundenen Initialterme wird also bei einem solchen Schritt echt vergrößert. Da $K[X_1, \ldots, X_n]$ noethersch ist, muß dieser Prozeß nach endlich vielen Schritten stoppen:

Satz 8.11. *Sei R ein Ring. Dann sind äquivalent:*

(a) *R ist noethersch.*
(b) *Jede aufsteigende Kette von Idealen wird stationär.*
(c) *Jede Menge von Idealen hat ein bezüglich Inklusion maximales Element.*

Beweis. (a) $\Rightarrow$ (b): Sei $I_1 \subset I_2 \subset \cdots$ eine aufsteigende Kette von Idealen. Dann ist $I = \bigcup_{i=1}^{\infty} I_i$ ein Ideal. (Achtung: Im allgemeinen ist die Vereinigung von Idealen keineswegs ein Ideal.) Nach Voraussetzung ist I endlich erzeugt, etwa von $f_1, \ldots, f_m$. Dann existiert ein p mit $f_j \in I_p$ für alle j, und es muß $I = I_p = I_q$ für alle $q \geq p$ gelten.

(b) $\Rightarrow$ (c): Wenn es eine Menge $\mathscr{M}$ von Idealen ohne maximales Element gibt, dann können wir eine echt aufsteigende Kette $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ bauen, indem wir $I_1 \in \mathscr{M}$ beliebig wählen. Da I_1 nicht maximal in $\mathscr{M}$ ist, existiert ein $I_2 \in \mathscr{M}$ mit $I_1 \subsetneq I_2$ usw.

(c) $\Rightarrow$ (a): Wir nehmen an, es gäbe ein nicht endlich erzeugtes Ideal I in R. Dann können wir die Menge $\mathscr{M}$ aller Ideale $(f_1, \ldots, f_n) \subset I$ mit $n \in \mathbb{N}$ betrachten. Hätte sie ein maximales Element J, so würde dieses alle Elemente von I enthalten und somit I gleich dem endlich erzeugten Ideal J sein. □

Bemerkung 8.12. Wir haben oben den Begriff Syzygie benutzt. Dahinter steht die Betrachtung der surjektiven R-linearen Abbildung

$$\varphi : R^m \to I, \qquad e_i \mapsto g_i.$$

Die Syzygien sind gerade die Elemente von $\operatorname{Ker}\varphi$. Analog betrachten wir die ebenfalls surjektive R-lineare Abbildung

$$\psi : R^m \to I, \qquad e_i \mapsto \operatorname{LT}(g_i).$$

Da die Elemente $\operatorname{LT}(g_i)$ Terme sind, kann man leicht sehen, daß die Syzygien $\varkappa_{ij}$ den R-Modul $\operatorname{Ker}\psi$ erzeugen.

Die Reduktion der S-Polynome läuft daraus hinaus, die Syzygien $\varkappa_{jk} \in \operatorname{Ker}\psi$ zu Elementen s_{jk} von $\operatorname{Ker}\varphi$ zu liften. Es läßt sich dann ohne große Mühe zeigen (im wesentlichen nach dem Schema des Satzes 7.10), daß die gelifteten Syzygien $\operatorname{Ker}\varphi$ erzeugen.

Dies ist ein wesentlicher Gesichtspunkt, weil er zeigt, wie man den „Syzygienmodul“ $\operatorname{Ker}\varphi$ von I effektiv berechnet. Bei einer konsequenten Fortsetzung des Buchberger-Algorithmus von Idealen auf Untermoduln von R^m kann man dann freie Auflösungen von endlich erzeugten R-Moduln bestimmen.

Weiterführende Literatur: [**Sing**], [**IVA**], [**CCA**].

ABSCHNITT 9

Erste Anwendungen auf Ring- und Idealtheorie

Standard-Basis des Restklassenrings und Ideal-Mitgliedschaft. Wenn man eine Gröbner-Basis von I kennt, dann kann man in R/I „effizient“ rechnen. Mit dem folgenden Satz haben wir auch den letzten Teil von Satz 7.1 verallgemeinert.

Satz 9.1. *Sei I ein Ideal in $R = K[X_1, \ldots, X_n]$ mit Gröbner-Basis G (bezüglich einer monomialen Ordnung). Ferner sei $\pi : R \to R/I$ die kanonische Projektion.*

(a) *Jede Restklasse $\pi(x)$, $x \in R$, hat genau einen bezüglich G reduzierten Repräsentanten, nämlich die Reduktion von x modulo G.*

(b) *Die Teilmenge*

$$B = \{\pi(\mu) : \mu \text{ Monom }, \mu \notin \mathrm{LM}(I)\}$$

ist eine Basis des K-Vektorraums R/I.

Beweis. (a) Sei $G = \{g_1, \ldots, g_m\}$. Dann reduziert sich x wie folgt:

$$x = q_1 g_1 + \cdots + q_m g_m + r.$$

Es folgt

$$\pi(x) = \pi(r).$$

Also besitzt $\pi(x)$ den reduzierten Repräsentanten r. Dieser ist eindeutig: Sei r' mit $r - r' \neq 0$ ein weiterer solcher Repräsentant. Es gilt $\mathrm{LM}(r - r') \in \mathrm{supp}(r) \cup \mathrm{supp}(r')$ und $r - r' \in I$. Aber kein Element aus $\mathrm{supp}(r) \cup \mathrm{supp}(r')$ wird von einem der Monome $\mathrm{LM}(g_i)$ geteilt. Das ist ein Widerspruch dazu, daß G eine Gröbner-Basis ist.

(b) Die bezüglich G reduzierten Polynome sind genau diejenigen, die Linearkombination der Monome aus B sind. Daher ist (b) eine Umformulierung von (a). □

Die im Satz beschriebene Basis von R/I heißt *Standard-Basis* bezüglich der gegebenen monomialen Ordnung.

Mit diesem Satz ist auch das Problem der „Ideal-Mitgliedschaft“ gelöst. Bei ihm geht es darum, zu gegebenen Elementen $g, f_1, \ldots, f_m \in R$ zu entscheiden, ob g im Ideal $(f_1, \ldots, f_m)$ liegt. Dazu bestimmt man eine Gröbner-Basis G von I und reduziert g modulo G. Es gilt $g \in (f_1, \ldots, f_m)$ genau dann, wenn g sich zu 0 reduziert.

In Anwendungen tritt das Problem der Ideal-Mitgliedschaft in folgender Form auf: Für Elemente $x_1, \ldots, x_n$ einer K-Algebra S und die Polynome $g, f_1, \ldots, f_m \in R = K[X_1, \ldots, X_n]$ gelte

$$f_i(x_1, \ldots, x_n) = 0, \quad \imath = 1, \ldots, m.$$

Kann man folgern, daß für ein $g \in R$ auch $g(x_1, \ldots, x_n) = 0$ gilt?

Definition. Sei K ein Körper und $g, f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Die Gleichung $g(x) = 0$, $g \in K[X_1, \ldots, X_n]$, ist *algebraische Konsequenz* von $f_1(x) = \cdots = f_m(x) = 0$, wenn für jede K-Algebra S und alle $x = (x_1, \ldots, x_n) \in S^n$ gilt:

$$f_1(x) = \cdots = f_m(x) = 0 \quad \Longrightarrow \quad g(x) = 0.$$

Klar ist:

$$g \in (f_1, \ldots, f_m),\ f_1(x) = \cdots = f_m(x) = 0 \Longrightarrow g(x) = 0.$$

Die Umkehrung gilt, da man von $x_1, \ldots, x_n$ verlangt, daß sie in einer beliebigen K-Algebra S liegen dürfen. Man wähle speziell $S = R/I$ und $x_i = \overline{X_i}$, also als Restklasse von X_i. Dann ist $g(x) = 0$ äquivalent zu $\overline{g} = 0$, mit anderen Worten: äquivalent zu $g \in I$.

Beispiel 9.2. Wir betrachten den Satz vom Schnittpunkt der Seitenhalbierenden eines Dreiecks: *Der Schnittpunkt zweier Seitenhalbierender eines Dreiecks liegt auch auf der dritten; also schneiden sich alle Seitenhalbierenden in einem Punkt.*

Wir wählen Koordinaten, in denen das Dreieck folgende Lage hat:

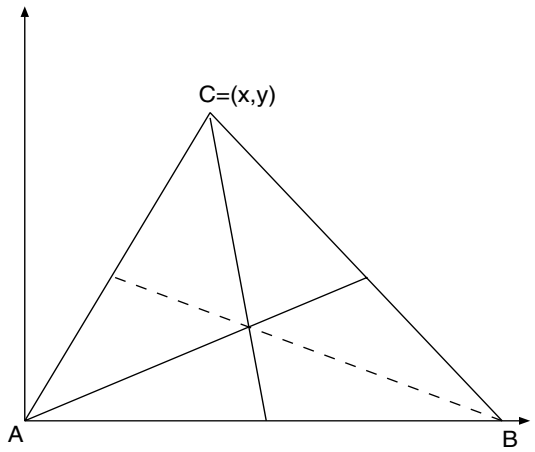

ABBILDUNG 1. Satz vom Schnittpunkt der Seitenhalbierenden

Sei $C = (x, y)$ und (u, v) der Schnittpunkt der Seitenhalbierenden s_a und s_c (in der Notation der Elementargeometrie). Dann gelten die Gleichungen:

$$\frac{uy}{2} = \frac{v(x+c)}{2}, \qquad v\left(x - \frac{c}{2}\right) = y\left(u - \frac{c}{2}\right)$$

oder äquivalent:

$$uy - v(x + c) = 0, \qquad 2vx - vc = 2uy - cy.$$

Daß der Schnittpunkt auch auf s_b liegt, ist äquivalent zu

$$vx - 2vc - uy + cy = 0$$

und diese Gleichung ist über $\mathbb{Q}$ algebraische Konsequenz der ersten beiden.

Etwas Vorsicht ist hierbei jedoch angebracht: Die Unbestimmten u, v nehmen Werte in $\mathbb{R}$ an und nicht in einer beliebigen $\mathbb{R}$-Algebra. Die Gültigkeit des Satzes ist daher nicht a priori äquivalent dazu, daß die dritte Gleichung algebraische Konsequenz der ersten beiden ist. Im allgemeinen ist der „automatische Beweis" geometrischer Aussagen nicht so einfach, wie es dieses Beispiel suggeriert, da man versteckte Nebenbedingungen oft übersieht. Wir werden dies noch an einigen Beispielen studieren.

Elimination von Variablen. Eines der wichtigsten Probleme, das sich mit Hilfe von Gröbner-Basen lösen läßt, ist die *Elimination von Variablen*, die grundlegende Technik zum Lösen von algebraischen Gleichungssystemen. Es sei ein Gleichungssystem

$$\begin{aligned} f_1(x_1, \ldots, x_n, y_y, \ldots, y_m) &= 0 \\ \vdots \qquad\qquad & \vdots \\ f_p(x_1, \ldots, x_n, y_y, \ldots, y_m) &= 0 \end{aligned}$$

gegeben, aus dem wir $y_1, \ldots, y_m$ eliminieren wollen: Wir wollen alle Gleichungen $g(x_1, \ldots, x_n) = 0$ finden, die aus obigen Gleichungen resultieren. Aus idealtheoretischer Sicht können wir das Problem so formulieren:

> *Gegeben sei ein Ideal $I \subset K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Bestimme das Eliminationsideal $I \cap K[X_1, \ldots, X_n]$.*

Definition. Eine monomiale Ordnung $<$ auf $R = K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ heißt *Eliminationsordnung* für $X_1, \ldots, X_n$, wenn für jedes Polynom $f \in R$ gilt:

$$\mathrm{LM}_<(f) \in K[X_1, \ldots, X_n] \Longrightarrow f \in K[X_1, \ldots, X_n].$$

Mit anderen Worten: Kommt eine der Unbestimmten $Y_1, \ldots, Y_m$ nicht im Leitterm von f vor, dann soll sie überhaupt nicht in f vorkommen. Beispielsweise ist die lex-Ordnung mit $Y_1 > \cdots > Y_m > X_1 > \cdots > X_n$ eine Eliminationsordnung, denn jedes Monom, in dem eines der Y_i vorkommt, ist größer als jedes Monom aus $K[X_1, \ldots, X_n]$.

Satz 9.3. *Sei $I \subset R$ ein Ideal, $<$ eine Eliminationsordnung für $X_1, \ldots, X_n$ und G eine Gröbner-Basis von I bezüglich $<$. Dann ist $G \cap K[X_1, \ldots, X_n]$ eine Gröbner-Basis von $I \cap K[X_1, \ldots, X_n]$.*

Beweis. Sei $f \in I \cap K[X_1, \ldots, X_n]$. Dann existiert ein $g \in G$, so daß $\mathrm{LM}(g) \mid \mathrm{LM}(f)$. Wegen $\mathrm{LM}(f) \in K[X_1, \ldots, X_n]$ gilt auch $\mathrm{LM}(g) \in K[X_1, \ldots, X_n]$ und nach Definition der Eliminationsordnung folgt $g \in I \cap K[X_1, \ldots, X_n]$. □

Beispiel 9.4. Wie läßt sich der Flächeninhalt F eines ebenen Dreiecks durch die Seitenlängen a, b, c ausdrücken? Wir wählen folgende Lage des Dreiecks: Nach

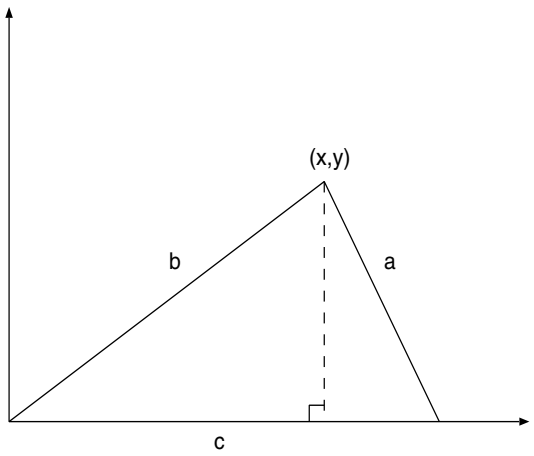

ABBILDUNG 2. Flächeninhalt eines Dreiecks

dem Satz von Pythagoras gilt:

$$b^2 = x^2 + y^2, \qquad a^2 = (c - x)^2 + y^2.$$

Ferner gilt

$$F = \frac{1}{2} cy.$$

Wir suchen eine Gleichung, in der nur F, a, b, c vorkommen, müssen also x und y eliminieren. Zu betrachten ist das von

$$\begin{aligned} &x^2 + y^2 - b^2, \\ &x^2 - 2cx - y^2 - a^2, \\ &cy - 2F \end{aligned}$$

erzeugte Ideal I in $K[a, b, c, F, x, y]$. Wir wollen $I \cap K[F, a, b, c]$ bestimmen. Eine Rechnung von Hand ist schon sehr aufwendig. Man erkennt das an der Komplexität der Lösung

$$F^2 = \frac{1}{16}(a + b + c)(a + b - c)(a - b + c)(-a + b + c),$$

der berühmten *Formel von Heron*.

Eine Aufgabe, die mittels Elimination gelöst werden kann, ist die Bestimmung des Kerns eines Ringhomomorphismus.

Satz 9.5. *Seien* $R = K[X_1, \ldots, X_n]$ *und* $S = K[Y_1, \ldots, Y_m]$ *Polynomringe und* $f_1, \ldots, f_n \in S$. *Wir betrachten den Homomorphismus*

$$\varphi : R \to S, \quad \varphi(X_i) = f_i,\ i = 1, \ldots, n.$$

Sei $I = (X_1 - f_1, \ldots, X_n - f_n)$ *das von den* $X_i - f_i$ *erzeugte Ideal in*

$$T = K[X_1, \ldots, X_n, Y_1, \ldots, Y_m].$$

Dann gilt $\operatorname{Ker}\varphi = I \cap R$.

Beweis. Wir Setzen φ fort zu einem Homomorphismus $\psi : T \to S$ vermöge $\psi(Y_i) = Y_i$, $i = 1, \ldots, m$. Dann ist offenbar $\operatorname{Ker}\varphi = \operatorname{Ker}\psi \cap R$. Zu zeigen ist also $I = \operatorname{Ker}\psi$.

Für alle $i = 1, \ldots, n$ gilt

$$\psi(X_i - f_i) = \psi(X_i) - \psi(f_i) = f_i - f_i = 0,$$

denn auf $S \subset T$ wirkt ψ wie die Identität und es ist $f_i \in S$.

Wir betrachten nun die lex-Ordnung

$$X_1 > \cdots > X_n > Y_1 > \cdots > Y_m.$$

Sei $f \neq 0$, $f \in \operatorname{Ker}\psi$. Dann ist $f \notin S$ (wegen $\psi|_S = \mathrm{id}$) und also auch $\mathrm{LM}(f) \notin S$. Folglich kommt eine der Unbestimmten X_i in f vor, und $\mathrm{LM}(f)$ wird von $X_i = \mathrm{LM}(X_i - f_i)$ geteilt. Die $X_i - f_i$ bilden also eine Gröbner-Basis von $\operatorname{Ker}\psi$ und es folgt die Behauptung. □

Man kann diesen Satz auch ohne Gröbner-Basen beweisen. Dazu betrachten wir die Kopie $T' = K[X_1', \ldots, X_n', Y_1', \ldots, Y_m']$ von T und den Isomorphismus $\chi : T' \to T$, der durch $\chi(X_i') = X_i - f_i$ und $\chi(Y_j') = Y_j$ gegeben ist. Dann ist der Kern von $\varphi \circ \chi$ offensichtlich von $T_1', \ldots, T_n'$ erzeugt und deshalb $\operatorname{Ker}\varphi$ von $\chi(X_i') = X_i - f_i$, $i = 1, \ldots, n$.

Allgemeiner als Satz 9.5 gilt sogar

Satz 9.6. *Sei* $R = K[X_1, \ldots, X_n]$, $S = K[Y_1, \ldots, Y_m]$ *und* $J \subset S$ *ein Ideal. Seien* $f_1, \ldots, f_n \in S$ *und* I *das von* $X_1 - f_1, \ldots, X_n - f_n$ *und* J *erzeugte Ideal in* $T = K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. *Dann ist* $I \cap R$ *der Kern des Homomorphismus*

$$\varphi : R \to S/J, \quad \varphi(X_i) = \overline{f_i}.$$

Beweis. Wir betrachten die Komposition

$$R \to T \xrightarrow{\psi} S \xrightarrow{\pi} S/J$$

mit $\psi(X_i) = f_i$, $\psi(Y_i) = Y_i$. Dann ist $\operatorname{Ker}\pi \circ \psi = \psi^{-1}(\operatorname{Ker}\pi) = \psi^{-1}(J)$.

Um $\psi^{-1}(J)$ zu bestimmen, genügt es, ein Ideal J' in T zu finden mit $\psi(J') = J$; dann nämlich ist $\psi^{-1}(J) = J' + \operatorname{Ker}\psi$. Wenn wir S auf natürliche Weise als Unterring von T betrachten, können wir J' als das von J in T erzeugte Ideal wählen.

Den Kern von ψ liefert der vorangegangene Satz: $\mathrm{Ker}(\pi \circ \psi)$ wird erzeugt von J und den $X_i - f_i$. □

Beispiel 9.7. Sei $L \supset K$ eine endliche Körpererweiterung der Form

$$L = K[X]/(f), \quad f \text{ irreduzibel.}$$

Für ein $y \in L$ ist dann dessen Minimalpolynom gesucht. Mit anderen Worten: Gesucht ist ein Erzeuger des Kerns des Homomorphismus

$$\varphi : K[Y] \to L, \quad \varphi(Y) = y.$$

Also haben wir y in der Form $g(x)$, $x = \overline{X}$, zu schreiben, dann das Ideal $(f, Y-g)$ zu betrachten und aus ihm X zu eliminieren.

Idealtheoretische Operationen. Liegen zwei Ideale $I, J \subset K[X_1, \ldots, X_n]$ vor, dann ist man oft interessiert an Verknüpfungen dieser Ideale wie Summe, Produkt oder Durchschnitt. Für die ersten beiden Konstruktionen kann man sehr einfach Erzeugendensysteme angeben: Ist I von f_i, $i = 1, \ldots, p$, und J von g_j, $j = 1, \ldots, q$ erzeugt, dann ist

$$I + J = \{a + b : a \in I,\, b \in J\}$$

erzeugt von $f_i + g_j$, $i = 1, \ldots, p$, $j = 1, \ldots, q$. Das Produkt

$$I \cdot J = \{a_1 b_1 + \cdots + a_m b_m : m \in \mathbb{N},\, a_i \in I,\, b_i \in J\}$$

ist von allen Produkten $f_i g_j$, $i = 1, \ldots, p$, $j = 1, \ldots, q$ erzeugt.

Schwieriger ist das Problem des Idealdurchschnitts. Auch $I \cap J$ ist ein Ideal, aber wie man ein Erzeugendensystem oder gar eine Gröbner-Basis findet, ist alles andere als offensichtlich. Der folgende Satz löst das Problem:

Satz 9.8. *Seien I, J Ideale in $R = K[X_1, \ldots, X_n]$ und S der erweiterte Polynomring $S = R[T]$. Dann gilt:*

$$I \cap J = \big(TIS + (1-T)JS\big) \cap R.$$

Beweis. Sei $f \in I \cap J$. Dann ist sicherlich $f = Tf + (1-T)f \in TIS + (1-T)JS$.

Sei nun $g \in R$ von der Form

$$g = Tg_1 r + (1-T)g_2 s, \quad g_1 \in I,\, g_2 \in J,\, r, s \in S.$$

Substitution von 0 für T ergibt dann $g \in JS$, und Substitution von 1 ergibt IS. Also ist $g \in (IS \cap R) \cap (JS \cap R) = I \cap J$. □

Weiterführende Literatur: [**Sing**], [**IVA**], [**CCA**].

ABSCHNITT 10

Ideale und Varietäten

In der Geometrie interessiert man sich oft für Nullstellenmengen von Polynomen über den Körpern $\mathbb{R}$ oder $\mathbb{C}$ und viele „interessante“ Teilmengen kann man durch solche algebraischen Gleichungssysteme beschreiben.

Definition. Eine Teilmenge $A \subset K^n$ heißt *affine Varietät*, wenn sie von folgender Form ist:

$$A = \{x \in K^n : f_1(x) = \cdots = f_m(x) = 0\}$$

für Polynome $f_i \in K[X_1, \ldots, X_n]$. Man schreibt dann $A = \mathscr{V}(f_1, \ldots, f_m)$.

Klassische Beispiele sind die *Kegelschnitte*

$$C = \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\}$$

für ein Polynom f des Grades 2. Zu ihnen gehören Parabeln, Ellipsen und Hyperbeln.

Wir wollen in diesem Abschnitt den Zusammenhang zwischen den Idealen in $K[X_1, \ldots, X_n]$ und den Teilmengen $A \subset K^n$, die als affine Varietät dargestellt werden können, studieren.

$\mathscr{V}(I)$ *und* $\mathscr{I}(A)$. Wir können zuerst einmal $f_1, \ldots, f_m$ durch das von ihnen erzeugte Ideal ersetzen:

Satz 10.1. *Ist $I = (f_1, \ldots, f_m) \subset K[X_1, \ldots, X_n]$, so gilt*

$$\mathscr{V}(f_1, \ldots, f_m) = \{x \in K^n : f(x) = 0 \textit{ für alle } f \in I\}.$$

Beweis. Klar, da jedes $f \in I$ Linearkombination der $f_1, \ldots, f_m$ ist (mit Koeffizienten aus $K[X_1, \ldots, X_n]$). □

Statt $\mathscr{V}(f_1, \ldots, f_m)$ können wir also

$$\mathscr{V}(I)$$

schreiben. Umgekehrt können wir auch jeder Teilmenge von K^n ein Ideal im Polynomring $K[X_1, \ldots, X_n]$ zuordnen:

Definition. Für $A \subset K^n$ sei $\mathscr{I}(A)$ die Menge der auf ganz A verschwindenden Polynome,

$$\mathscr{I}(A) := \{f \in K[X_1, \ldots, X_n] : f(x) = 0 \text{ für alle } x \in A\}.$$

Offensichtlich ist $\mathscr{I}(A)$ ein Ideal. Es ist der Kern des Homomorphismus

$$\varphi : K[X_1, \ldots, X_n] \to \mathrm{Abb}(A, K), \quad f \mapsto f|_A.$$

Wir haben nun zwei Zuordnungen definiert, die Ideale in $K[X_1, \ldots, X_n]$ und und Teilmengen von K^n in Beziehung setzen, nämlich

$$I \to \mathscr{V}(I), \qquad A \to \mathscr{I}(A).$$

Inwieweit sind diese beiden Zuordnungen zueinander invers? Zum Beispiel hat man im allgemeinen nur $A \subset \mathscr{V}(\mathscr{I}(A))$. Eine notwendige Bedingung für Gleichheit ist offenbar, daß A bereits eine affine Varietät ist. Das ist auch schon hinreichend:

Satz 10.2. *Sei $A \subset K^n$ eine affine Varietät. Dann ist $A = \mathscr{V}(\mathscr{I}(A))$.*

Beweis. Sei $A = \mathscr{V}(f_1, \ldots, f_m)$. Dann sind $f_1, \ldots, f_m \in \mathscr{I}(A)$. Es folgt $\mathscr{V}(\mathscr{I}(A)) \subset A$. Umgekehrt sei $x \in A$. Dann ist $f(x) = 0$ für alle $f \in \mathscr{I}(A)$ und also $x \in \mathscr{V}(\mathscr{I}(A))$. □

Recht nützlich (und offensichtlich richtig) sind die folgenden Monotonieeigenschaften von $\mathscr{V}$ und $\mathscr{I}$ bezüglich der Inklusion:

$$A \subset B \Longrightarrow \mathscr{I}(A) \supset \mathscr{I}(B), \qquad I \subset J \Longrightarrow \mathscr{V}(I) \supset \mathscr{V}(J).$$

Der mit Satz 10.2 errungene kleine Erfolg sollte uns aber nicht täuschen. Die ungleich schwerere Frage ist die Bestimmung von $\mathscr{I}(\mathscr{V}(I))$, mit anderen Worten die Beantwortung der folgenden Frage: Gegeben seien Polynome $g, f_1, \ldots, , f_m \in K[X_1, \ldots, X_n]$. Wann gilt $g(x) = 0$ für alle $x \in \mathscr{V}(f_1, \ldots, f_m)$?

Gilt in Umkehrung zu $A = \mathscr{V}(\mathscr{I}(A))$ auch $I = \mathscr{I}(\mathscr{V}(I))$ für ein Ideal I? Welche Voraussetzungen muß I erfüllen? Im allgemeinen gilt Gleichheit nämlich nicht, wie man sich schnell klarmacht:

$$n = 1,\ I = (X^2) \Longrightarrow \mathscr{V}(I) = \{0\},\ \mathscr{I}(\mathscr{V}(I)) = (X) \supsetneq (X^2).$$

Ein extremeres Beispiel:

$$n = 2,\ K = \mathbb{R},\ I = (1 + X^2 + Y^2) \Longrightarrow \mathscr{V}(I) = \emptyset,\ \mathscr{I}(\mathscr{V}(I)) = \mathbb{R}[X, Y].$$

Da zweite Beispiel beruht natürlich auf der Tatsache, daß der zugrundeliegende Körper nicht algebraisch abgeschlossen ist. Darauf kommen wir noch zurück.

Radikalideale. Das im ersten Beispiel beobachtete Phänomen ist dagegen leicht zu erklären.

Definition. Sei $I \subset R$ ein Ideal. Dann nennt man die Menge

$$\sqrt{I} := \{f \in R : f^k \in I \text{ für ein } k \in \mathbb{N}\}$$

das *Radikal* von I. Gilt $I = \sqrt{I}$, dann heißt I ein *Radikalideal*.

Offenbar ist $\sqrt{I}$ eine Obermenge von I, und ist R kommutativ, dann ist $\sqrt{I}$ ebenfalls ein Ideal:

Satz 10.3. *Ist R ein kommutativer Ring, so ist $\sqrt{I}$ ein Ideal.*

Beweis. Wenn $f^p \in I$, dann auch $(rf)^p = r^p f^p \in I$ für alle $r \in R$. Wenn außerdem $g^q \in I$, so ist

$$(f+g)^{p+q} = \sum_{k=0}^{p+q} \binom{p+q}{k} f^k g^{p+q-k} \in I,$$

denn $k \geq p$ oder $p+q-k \geq k$. □

Satz 10.4. *Für alle $A \subset K^n$ ist $\mathscr{I}(A)$ ein Radikalideal.*

Beweis. Da wir in einem Körper rechnen, gilt

$$g^k(x) = 0 \Longrightarrow g(x) = 0 \quad \text{für } g \in K[X_1, \ldots, X_n].$$

Das liefert die Behauptung. □

Damit ist klar: $\sqrt{I} \subset \mathscr{I}(\mathscr{V}(I))$ und wir können $I = \mathscr{I}(\mathscr{V}(I))$ nur erwarten, wenn $I = \sqrt{I}$ gilt.

Wir diskutieren erst einmal den Fall $n = 1$, also Nullstellen von Polynomen in einer Veränderlichen. Dann ist jedes Ideal Hauptideal. Sei $I = (f)$, wobei f die Faktorisierung

$$f = g_1^{e_1} \ldots g_m^{e_m}, \quad e_1, \ldots, e_m > 0,$$

mit irreduziblen und paarweise teilerfremden g_i hat. Dann wird $\sqrt{I}$ vom Produkt der g_i erzeugt:

$$\sqrt{I} = (g_1 \ldots g_m).$$

Denn ist $h \in \sqrt{I}$, dann teilt jedes der g_i auch h und wegen $\mathrm{ggT}_{i \neq j}(g_i, g_j) = 1$ wird h auch von ihrem Produkt geteilt. Daraus folgt $h \in (g_1 \ldots g_m)$. Die umgekehrte Inklusion ist klar.

Diese Bemerkung zeigt insbesondere, daß $\sqrt{I} = I$ gilt, falls I von einem quadratfreien Polynom erzeugt wird.

Ist der Körper K nicht algebraisch abgeschlossen, dann existiert ein irreduzibles Polynom $f \in K[X]$ ohne Nullstelle, und für dieses gilt

$$\mathscr{I}(\mathscr{V}(f)) = \mathscr{I}(\emptyset) = K[X].$$

Der Hilbertsche Nullstellensatz. Ist K hingegen algebraisch abgeschlossen, stehen Ideale und Varietäten in der bestmöglichen Beziehung:

Satz 10.5 (Hilbertscher Nullstellensatz)**.** *Sei K ein algebraisch abgeschlossener Körper und I ein Ideal in $K[X_1, \ldots, X_n]$. dann gilt*

$$\mathscr{I}(\mathscr{V}(I)) = \sqrt{I}.$$

Wir beweisen hier nur den Fall $n = 1$. Für den allgemeinen Fall siehe etwa [**IVA**] oder [**CCA**].

Sei also $(f) = I$ und $f \notin K$. Die irreduziblen Faktoren g_i von f in obiger Zerlegung sind von der Form $g_i = X - x_i$, wobei $x_1, \ldots, g_m$ die paarweise verschiedenen Nullstellen von f sind. Genau dann verschwindet $h \in K[X]$ in $x_1, \ldots, x_m$, wenn h ein Vielfaches von $(X-x_1)\cdots(X-x_m)$ ist, also zu $\sqrt{I}$ gehört. Daraus folgt die Behauptung. Ist $f = 0$, so ist $\mathscr{V}(I) = K$ und $\mathscr{I}(\mathscr{V}(I)) = 0 = \sqrt{(0)}$. Ist allgemeiner f eine Konstante $\neq 0$, dann ist $\mathscr{V}(I) = \emptyset$ und $\mathscr{I}(\mathscr{V}(I)) = K[X] = \sqrt{I}$.

Man kann den Hilbertschen Nullstellensatz auch in einer *schwachen* Form formulieren, aus der sich die obige *starke* Form dann herleiten läßt, wie dies auch in der Literatur oft getan wird. Wir leiten allerdings die schwache aus der starken Form her.

Satz 10.6. *Sei K algebraisch abgeschlossen und $I \subset K[X_1, \ldots, X_n]$ ein echtes Ideal, d. h. $I \neq K[X_1, \ldots, X_n]$. Dann ist $\mathscr{V}(I) \neq \emptyset$.*

Beweis. Gilt $I \neq K[X_1, \ldots, X_n]$, dann ist auch $\sqrt{I} \neq K[X_1, \ldots, X_n]$. Nach dem Nullstellensatz ist $\mathscr{V}(I) = \mathscr{V}(\sqrt{I}) \neq \emptyset$. □

Eine algebraisch gefärbte Version des Nullstellensatzes ist

Satz 10.7. *Sei K ein algebraisch abgeschlossener Körper. Die maximalen Ideale von $K[X_1, \ldots, X_n]$ sind dann genau die Ideale der Form*

$$(X_1 - x_1, \ldots, X_m - x_n) \quad \textit{mit } x_1, \ldots, x_n \in K.$$

Beweis. Ein Ideal der obigen Form ist stets maximal. Zum Beweis betrachte man den Substitutionshomomorphismus

$$\varphi : K[X_1, \ldots, X_n] \to K, \quad X_i \mapsto x_i.$$

Nach Satz 9.5 ist $\operatorname{Ker}\varphi = (X_1 - x_1, \ldots, X_m - x_m)$ und wegen

$$K[X_1, \ldots, X_n]/\ker\varphi \cong K$$

ist $(X_1 - x_1, \ldots, X_m - x_m)$ maximal.

Sei umgekehrt $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ maximal. Da $\mathfrak{m}$ keine Einheit enthält, tut es auch $\sqrt{\mathfrak{m}}$ nicht, und aus der Maximalität von $\mathfrak{m}$ folgt $\mathfrak{m} = \sqrt{\mathfrak{m}}$. Wegen $\mathfrak{m} \neq K[X_1, \ldots, X_n]$ gilt $\mathscr{V}(\mathfrak{m}) \neq \emptyset$, denn nur auf der leeren Menge verschwinden alle Polynome (gemäß der schwachen Form des Nullstellensatzes). Es existiert also ein $x \in K^n$ mit $x \in \mathscr{V}(\mathfrak{m})$. Der Übergang zu den Verschwindungsidealen gibt

$$\mathfrak{m} = \sqrt{\mathfrak{m}} \subset \mathscr{V}(\{x\}) \subset (X_1 - x_1, \ldots, X_n - x_n).$$

Aus der Maximalität von $(X_1 - x_1, \ldots, X_n - x_n)$, bewiesen im ersten Teil, folgt die Gleichheit. □

Wir ziehen noch ein Korollar aus dem Hilbertschen Nullstellensatz, der den Zusammenhang von Idealen und affinen Varietäten deutlich macht; es ist nur eine Umformulierung des Nullstellensatzes:

Korollar 10.8. *Ist K algebraisch abgeschlossen, dann ist vermöge*

$$I \longmapsto \mathscr{V}(I), \qquad A \longmapsto \mathscr{I}(A)$$

eine bijektive Zuordnung zwischen den Radikalidealen von R und den affinen Varietäten von K^n gegeben.

In Analogie zur algebraischen Konsequenz könne wir nun den Begriff der *geometrischen Konsequenz* einführen und analysieren:

Definition. Sei K ein Körper und $g, f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Dann nennt man $g(x) = 0$ *geometrische Konsequenz* von $f_1(x) = \cdots = f_m(x) = 0$, wenn für alle $x \in K^n$ die Implikation

$$f_1(x) = \ldots f_m(x) = 0 \Longrightarrow g(x) = 0$$

gilt.

Der Begriff der geometrischen Konsequenz ist schwächer als der Begriff der algebraischen Konsequenz, weil man bei ersterer nur Elemente des Körpers einsetzen darf. Deutlicher wird dies im Teil (a) des folgenden Satzes, der unsere obigen Überlegungen zusammmenfaßt:

Satz 10.9. *Sei $x \in K^n$.*

(a) *Ist $g \in \sqrt{(f_1, \ldots, f_m)}$, dann ist $g(x) = 0$ geometrische Konsequenz von $f_1(x) = \cdots = f_m(x) = 0$.*

(b) *Ist K algebraisch abgeschlossen, dann gilt in (a) auch die Umkehrung.*

Insbesondere gilt für alle $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ die Gleichheit

$$\sqrt{(f_1, \ldots, f_m)} = \mathscr{I}(\mathscr{V}(f_1, \ldots, f_m))$$

genau dann, wenn K algebraisch abgeschlossen ist.

Die Bestimmung von $\sqrt{I}$. Die vorangegangenen Betrachtungen, insbesondere der Hilbertsche Nullstellensatz, werfen die Frage auf, wie man $\sqrt{I}$ berechnet. Dieses Problem ist schwierig, aber lösbar; es existiert ein aufwendiger Algorithmus. Wir behandeln den allgemeinen Fall nicht. (Siehe aber Abschnitt 13 für den Fall, in dem $\mathscr{V}(I)$ eine endliche Menge ist.)

Einfacher ist die Frage zu beantworten, ob ein gegebenes $g \in K[X_1, \ldots, X_n]$ in $\sqrt{I}$ liegt, denn es gilt

Satz 10.10. *Seien $g, f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Dann gilt*

$$g \in \sqrt{(f_1, \ldots, f_m)} \Longleftrightarrow (f_1, \ldots, f_m, 1 - gT) = K[X_1, \ldots, X_n, T].$$

Offenbar ist die rechte Bedingung genau dann erfüllt, wenn $\{1\}$ eine Gröbner-Basis von $J = (f_1, \ldots, f_m, 1 - gT)$. (Jede Gröbner-Basis des Polynomrings (als Ideal über sich selbst) enthält zumindest eine Einheit $c \in K^*$.)

Beweis. $\Rightarrow$: Sei $S = K[X_1, \ldots, X_m, T]/J$. Dann ist $\overline{g}$ nilpotent in S, d. h. es existiert ein $k \geq 1$ mit $\overline{g}^k = 0$. Wegen $\overline{1} = \overline{g}\overline{T}$ gilt $\overline{1}^k = \overline{1} = 0$ und also ist S der Nullring.

$\Leftarrow$: Sei

$$1 = r_1 f_1 + \ldots r_m f_m + s(1 - gT), \quad r_i, s \in K[X_1, \ldots, X_m, T].$$

Die Substitution $T \mapsto 1/g$ ergibt

$$1 = r_1(g^{-1}) f_1 + \cdots + r_m(g^{-1}) f_m$$

Man beachte $f_i \in K[X_1, \ldots, X_n]$, also kommt T in keinem f_i vor. In den Nennern der $r_i(g^{-1})$ kommen nur Potenzen von g vor, Multiplikation mit g^k für hinreichend großes $k \in \mathbb{N}$ ergibt dann

$$g^k = r_1' f_1 + \ldots r_m' f_m \quad , \; r_i' = g^k r_i(g^{-1}). \qquad \square$$

Auch wenn wir nicht allgemein erklärt haben, wie man das Radikal eines Ideals berechnet, so wollen wir doch den Fall eines Hauptideal betrachten, das vom Polynom f erzeugt wird. Im Fall $n = 1$ haben wir dieses Problem schon im Zusammenhang mit der Faktorisierung diskutiert.

Die Faktorisierung von f sei

$$f = g_1^{e_1} \ldots g_m^{e_m}$$

mit paarweise teilerfremden, irreduziblen $g_i \in K[X_1, \ldots, X_n]$ und $e_i \in \mathbb{N}$. Wir kennen schon eine Darstellung des Radikals des von f erzeugten Hauptideals:

$$\sqrt{(f)} = (g_1 \cdots g_m).$$

Aber wir kennen die g_i im allgemeinen nicht.

Analog zur Differentiation über $\mathbb{R}$ kann man nun auch im Ring $K[X_1, \ldots, X_n]$ partielle Ableitungen definieren. Man tut dies zunächst für die Monome mittels

$$\frac{\partial}{\partial X_i}(X_1^{a_1} \ldots X_m^{a_m}) = a_i X_1^{a_1} \cdots X_i^{a_i - 1} \cdots X_m^{a_m}$$

und setzt dann K-linear auf ganz $K[X_1, \ldots, X_n]$ fort. Wie man leicht nachrechnet, gilt dann auch die Produktregel:

$$\frac{\partial}{\partial X_i}(fg) = f \frac{\partial}{\partial X_i} g + g \frac{\partial}{\partial X_i} f, \qquad \frac{\partial}{\partial X_i} f^m = m f^{m-1} \frac{\partial}{\partial X_i} f.$$

In Verallgemeinerung von Satz 1.2 erhält man

Satz 10.11. *Sei K ein Körper der Charakteristik 0 und $f \in K[X_1, \ldots, X_n]$ ein nichtkonstantes Polynom mit der Zerlegung $f = g_1^{e_1} \ldots g_m^{e_m}$. Dann ist*

$$\frac{f}{\mathrm{ggT}\,(f, \frac{\partial}{\partial X_1} f, \ldots, \frac{\partial}{\partial X_m} f)}.$$

der quadratfreie Teil von f.

Beweis. Sei $f = g_1^{e_1} \ldots g_m^{e_m}$ wie oben und $h = f/g_j^{e_j}$. Dann gilt

$$\frac{\partial}{\partial X_i} f = \frac{\partial}{\partial X_i} h g_j^{e_j} = e_j h g_j^{e_j - 1} \frac{\partial}{\partial X_i} g_j + g_j^{e_j} \frac{\partial}{\partial X_i} h.$$

Es folgt

$$g_j^{e_j - 1} \mid \mathrm{ggT}(f, \frac{\partial}{\partial X_1} f, \ldots, \frac{\partial}{\partial X_m} f),$$

und es bleibt zu zeigen, daß $g_j^{e_j}$ kein Teiler des ggT ist.

Dies ist genau dann der Fall, wenn es ein j gibt, so daß $g_j^{e_j}$ kein Teiler von $h g_j^{e_j - 1} \frac{\partial}{\partial X_i} g_j$ ist. Wegen der Teilerfremdheit der g_k ist g_j zu h teilerfremd. Aus Gradgründen gilt

$$g_j \nmid \frac{\partial}{\partial X_i} g_j,$$

außer wenn die partielle Ableitung 0 ist. Falls aber X_i in g_j vorkommt (was für ein i und j der Fall sein muß, denn f ist nicht konstant), dann ist $\frac{\partial}{\partial X_i} g_j \neq 0$ und also $g_j^{e_j}$ kein Teiler von $h g_j^{e_j - 1} \frac{\partial}{\partial X_i} g_j$. □

In Charakteristik $p \neq 0$ versagt die Formel, wenn ein e_j durch p teilbar ist. Dann kommt g_j nämlich im Quotienten nicht mehr vor. Allerdings läßt sich dieser ungünstige Umstand leicht erkennen. Sei

$$g = \frac{f}{\mathrm{ggT}\,(f, \frac{\partial}{\partial X_1} f, \ldots, \frac{\partial}{\partial X_m} f)}.$$

Genau dann geht *kein* irreduzibler Teiler von f verloren (im obigem Sinne, d. h. $p^{e_j} \mid \mathrm{ggT}(\ldots)$), wenn $f \in \sqrt{(g)}$, und das läßt sich mit Satz 10.10 prüfen.

Es gibt aber noch einen weiteren Grund für das Versagen der Formel in Charakteristik p. Es kann vorkommen, daß alle partiellen Ableitungen eines irreduziblen Polynoms verschwinden. Mit einer Primzahl p sei $k = \mathbb{Z}_p$ und $K = k(Y)$ der Körper der rationalen Funktionen in Y über k. Dann ist $X^p - Y$ ein irreduzibles Polynom mit verschwindender Ableitung. (Beachte: Das Element Y gehört zum Körper K.)

Ist aber der Körper K perfekt, also jedes Element von K eine $p$te Potenz, dann ist jedes Polynom, dessen partielle Ableitungen alle verschwinden, eine $p$te Potenz. (Vgl. Übungsaufgabe.)

Zur Bestimmung von $\mathrm{ggT}(f,g)$ steht bei Polynomen mehrerer Variablen der euklidische Algorithmus nicht mehr zur Verfügung. Man kann aber leicht das $\mathrm{kgV}(f,g)$ ausrechnen und dann $\mathrm{ggT}(f,g) = fg/\mathrm{kgV}(f,g)$. (Vgl. Übungsaufgabe.)

Weiterführende Literatur: [**IVA**], [**CCA**].

ABSCHNITT 11

Varietäten und ihre irreduziblen Komponenten

Wir untersuchen zuerst, wie sich affine Varietäten unter Vereinigungen und Durchschnitten verhalten.

Satz 11.1.

(a) *Seien $A_1, \ldots, A_m$ affine Varietäten in K^n. Dann ist auch*

$$A_1 \cup \cdots \cup A_m = \mathscr{V}\big(\mathscr{I}(A_1) \cap \cdots \cap \mathscr{I}(A_m)\big)$$

eine affine Varietät.

(b) *Sind A_i, $i \in I$ affine Varietäten, dann auch*

$$\bigcap_{i \in I} A_i = \mathscr{V}\left(\sum_{i \in I} \mathscr{I}(A_i)\right).$$

Beweis. (a) Die Inklusion „$\subset$“ folgt aus der Tatsache, daß alle $f \in \mathscr{I}(A_1) \cap \cdots \cap \mathscr{I}(A_m)$ auf $A_1 \cup \cdots \cup A_m$ verschwinden. Zum Beweis der umgekehrten Inklusion wählen wir ein $x \in \mathscr{V}\big(\mathscr{I}(A_1) \cap \cdots \cap \mathscr{I}(A_m)\big)$. Falls $x \notin A_1 \cup \cdots \cup A_m$ ist, dann existiert zu jedem $j \in \{1, \ldots, m\}$ ein $f_j \in \mathscr{I}(A_j)$ mit $f_j(x) \neq 0$, denn $A_j = \mathscr{V}(\mathscr{I}(A_j))$. Das Produkt $g = f_1 \cdots f_m$ liegt in $\mathscr{I}(A_1) \cap \cdots \cap \mathscr{I}(A_m)$, aber $g(x) \neq 0$. Widerspruch!

(b) Es gilt $x \in \bigcap_{j \in J} A_j$ genau dann, wenn $f(x) = 0$ für alle $f \in \bigcup_{j \in J} \mathscr{I}(A_j)$ ist. Das Ideal $\sum_{j \in J} \mathscr{I}(A_j)$ ist das von $\bigcup_{j \in J} \mathscr{I}(A_j)$ erzeugte Ideal. □

Die Menge der affinen Varietäten ist also abgeschlossen gegen endliche Vereinigungen und beliebige Durchschnitte. Damit erfüllen die Menge der affinen Varietäten die Eigenschaften des Systems der abgeschlossenen Mengen einer Topologie, denn auch $\emptyset = \mathscr{V}(K[X_1, \ldots, X_n])$ und $K^n = \mathscr{V}(0)$ sind Varietäten. Die Topologie, deren abgeschlossene Mengen die affinen Varietäten sind, nennt dann man die *Zariski-Topologie* auf K^n.

Die Allgemeinheit in Teil (b) des vorigen Satzes ist aber nur ein formaler Aspekt: Es existieren $j_1, \ldots, j_m \in J$ mit $\bigcap_{j \in J} A_j = A_{j_1} \cap \cdots \cap A_{j_m}$. Dies liegt einfach daran, daß das Ideal $J = \sum_{j \in J} \mathscr{I}(A_j)$ endlich erzeugt ist: es existieren $j_1, \ldots, j_m$ mit $J = \mathscr{I}(A_{j_1} + \cdots + \mathscr{I}(A_{j_m})$, und damit ist $\bigcap_{j \in J} A_j = A_{j_1} \cap \cdots \cap A_{j_m}$. Dies macht deutlich, daß sich die Zariski-Topologie ganz erheblich von der gewohnten Topologie auf $\mathbb{R}^n$ oder $\mathbb{C}^n$ unterscheidet.

In jeder Topologie gilt, daß Urbilder abgeschlossener Mengen abgeschlossen sind. Dies ist natürlich auch in der Zariski-Topologie richtig:

Satz 11.2. *Die Abbildung $f : K^n \to K^m$ sei komponentenweise durch Polynome $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ gegeben. Für jede affine Varietät $W \subset K^m$ ist dann $V = f^{-1}(W)$ eine affine Varietät in K^n.*

Beweis. Mittels der Substitution von f_i für Y_i,

$$g \mapsto g(f_1, \ldots, f_m),$$

induziert f einen Homomorphismus $\varphi : K[Y_1, \ldots, Y_m] \to K[X_1, \ldots, X_n]$. Dann ist $g(f(x)) = (\varphi(g))(x)$ für alle $x \in K^m$. Damit folgt: $x \in V \iff f(x) \in W \iff p(f(x)) = 0$ für alle $p \in \mathscr{I}(W) \iff x \in \mathscr{V}(\varphi(\mathscr{I}(W))$. Also ist V eine affine Varietät. □

Sei $f \in K[X_1, \ldots, X_n]$ ein nichtkonstantes Polynom mit der Zerlegung $f = f_1 \ldots f_m$ in irreduzible Polynome. Wir wollen $A = \mathscr{V}(f)$ betrachten, dazu können wir annehmen, daß f quadratfrei ist. Offenbar muß in jedem Punkt von $\mathscr{V}(f)$ mindestens ein f_i verschwinden und umgekehrt reicht $f_i(x) = 0$ für ein $i \in \{1, \ldots, m\}$, damit auch $f(x) = 0$ ist. Es folgt:

$$\mathscr{V}(f) = \mathscr{V}(f_1) \cup \cdots \cup \mathscr{V}(f_m).$$

Sei etwa $n = 2$, $K = \mathbb{R}$ und

$$f = (X - Y)(X + Y)(X + 1)(Y - 1).$$

Es ergibt sich das folgende Bild:

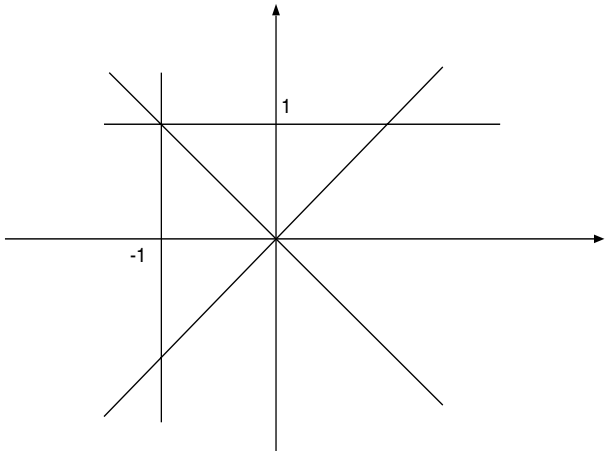

ABBILDUNG 1. $A = V\big((X - Y)(X + Y)(X + 1)(Y - 1)\big)$

Wir werden sehen, daß sich jede affine Varietät so in Komponenten zerlegen kann, wie man jedes quadratfreie Polynom in irreduzible Faktoren zerlegt.

Definition. Eine affine Varietät A heißt *irreduzibel*, wenn sie nicht Vereinigung echter Untervarietäten ist, d. h.

$$A = A_1 \cup A_2 \quad \Longrightarrow \quad A_1 = A \text{ oder } A_2 = A.$$

Die irreduziblen Varietäten lassen sich durch eine algebraische Eigenschaft der zugehörigen Ideale charakterisieren:

Satz 11.3. *Eine affine Varietät A ist genau dann irreduzibel, wenn $\mathscr{I}(A)$ ein Primideal ist.*

Beweis. Sei A reduzibel, also $A = A_1 \cup A_2$, $A_1, A_2 \subsetneq A$. Es folgt $\mathscr{I}(A_1)$, $\mathscr{I}(A_2) \supsetneq \mathscr{I}(A)$. Für $f_i \in \mathscr{I}(A_i) \setminus \mathscr{I}(A)$ gilt $f_1 f_2 \in \mathscr{I}(A)$, und also ist $\mathscr{I}(A)$ kein Primideal.

Sei umgekehrt $\mathscr{I}(A)$ nicht prim, d. h. es existieren $f_1, f_2 \notin \mathscr{I}(A)$ mit $f_1 f_2 \in \mathscr{I}(A)$. Wir wählen dann dann

$$A_1 = A \cap \mathscr{V}(f_1), \quad A_2 = A \cap \mathscr{V}(f_2).$$

Dann sind A_1 und A_2 echte Untervarietäten, die zusammen A ausfüllen. □

Bemerkung 11.4. K^n ist irreduzibel genau dann, wenn K unendlich ist. Denn ist K endlich, so auch K^n und die Reduzibilität von K^n ergibt sich aus der Tatsache, daß jedes $\{x\}$ eine affine Varietät ist. Die Umkehrung beweist man induktiv über n. Daß K selbst irreduzibel ist, folgt aus der Endlichkeit der Nullstellenmenge eines Polynoms. Die affinen Varietäten in K sind gerade die endlichen Mengen.

Satz 11.5. *Sei $A \subset K^n$ eine affine Varietät. Dann besitzt A eine Zerlegung in irreduzible Varietäten:*

$$A = A_1 \cup \cdots \cup A_m$$

mit $A_i \not\subset A_j$ für $i \neq j$. In ihr sind die A_i bis auf die Reihenfolge eindeutig bestimmt.

Beweis. Wir beweisen zunächst die Existenz der Zerlegung von A in irreduzible Untervarietäten. Sei $\mathscr{N}$ die Menge aller Varietäten ohne eine solche endliche Zerlegung. Wir nehmen an, daß $\mathscr{N} \neq \emptyset$. In der Menge

$$\{\mathscr{I}(A) : A \in \mathscr{N}\}$$

gibt es dann ein maximales Element, weil $K[X_1, \ldots, X_n]$ noethersch ist. Sei $\mathscr{I}(A_0)$ ein solches maximales Element. Dann ist $A_0 = \mathscr{V}(\mathscr{I}(A_0))$ minimal in $\mathscr{N}$. Da A_0 nicht irreduzibel ist, muß A_0 eine Zerlegung haben in echte Untervarietäten:

$$A_0 = A_1 \cup A_2, \quad A_1,\ A_2 \subsetneq A_0.$$

Die Varietäten $A_1,\ A_2$ liegen also nicht in $\mathscr{N}$, haben also eine Zerlegung in irreduzible Untervarietäten. Das gilt dann aber auch für A_0 , im Widerspruch dazu, daß $A_0 \in \mathscr{N}$.

Wenn wir überhaupt einmal eine Zerlegung $A = A_1 \cup \cdots \cup A_m$ haben, können wir durch Weglassen überflüssiger A_i erreichen, daß $A_i \not\subset A_j$ für $i \neq j$.

Nun zur Eindeutigkeit: Sei $B_1 \cup \cdots \cup B_p$ eine weitere minimale Zerlegung in irreduzible Varietäten. Dann gilt offenbar

$$A_1 = A_1 \cap A = (A_1 \cap B_1) \cup \cdots \cup (A_1 \cap B_m).$$

Da A_1 irreduzibel ist, muß $A_1 = A_1 \cap B_j$ für ein $j \in \{1, \ldots, p\}$ gelten. Mithin gilt $A_1 \subset B_j$. Analog folgert man, daß $B_j \subset A_i$ für ein i. Es folgt $A_1 \subset A_i$, was aber nur bei $i = 1$ möglich ist. Mithin $A_1 = B_j$, und man schließt dann induktiv weiter. □

Definition. Die Varietäten $A_1, \ldots, A_m$ des Satzes heißen *irreduzible Komponenten* von A.

Wir wollen eine algebraische Konsequenz aus Satz 11.5 ziehen: Sei $I = \mathscr{I}(A)$ und $A = A_1 \cup \cdots \cup A_m$ wie im Satz. Aus der Definition von $\mathscr{I}$ folgt dann sofort, daß $\mathscr{I}(A) = \mathscr{I}(A_1) \cap \cdots \cap \mathscr{I}(A_m)$ ist. Da die Ideale $\mathscr{I}(A)$ gemäß Satz 11.3 prim sind, gewinnen wir eine Darstellung des Radikalideals $\mathscr{I}(A)$ als Durchschnitt endlich vieler Primideale. Ist K algebraisch abgeschlossen und daher $I = \mathscr{I}(\mathscr{V}(I))$ für jedes Radikalideal $I \subset K[X_1, \ldots, X_n]$, können wir jedes Radikalideal in $K[X_1, \ldots, X_n]$ als Durchschnitt endlich vieler Primideale schreiben. Das gilt allerdings viel allgemeiner in allen noetherschen Ringen, und so formulieren wir auch

Satz 11.6. *Sei R ein noetherscher Ring und $I \subset R$ ein Radikalideal. Dann existieren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, $m \in \mathbb{N}$, mit $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$.*

Dieser Satz erinnert uns mit Recht an die Zerlegung quadratfreier Polynome oder ganzer Zahlen in ein Produkt paarweise teilerfremder Primelemente. Er ist ja eine sehr weitgehende Verallgemeinerung. Wenn man noch weiter gehen will und die Zerlegung beliebiger Polynome oder ganzen Zahlen verallgemeinern will, muß man *Primärideale* einführen, die den Potenzen von Primelementen entsprechen. (Achtung: Potenzen von Primidealen sind nicht notwendig primär.) Man kommt dann zur *Lasker-Noether-Zerlegung* von Idealen, für die wir auf die Literatur verweisen.

Wir illustrieren das Zerfallen einer Varietät am Satz des Ptolemäus. In der klassischen Sprache der Elementargeometrie lautet er: *In einem Sehnenviereck ist das von den Diagonalen gebildete Rechteck gleich der Summe der Rechtecke aus den Paaren gegenüberliegender Seiten.* Zum algorithmischen Beweis dieses Theorems kodiere man zuerst die Voraussetzungen in polynomialer Form, wobei man annehmen kann, daß der Nullpunkt Mittelpunkt des Kreises ist. Dann haben wir

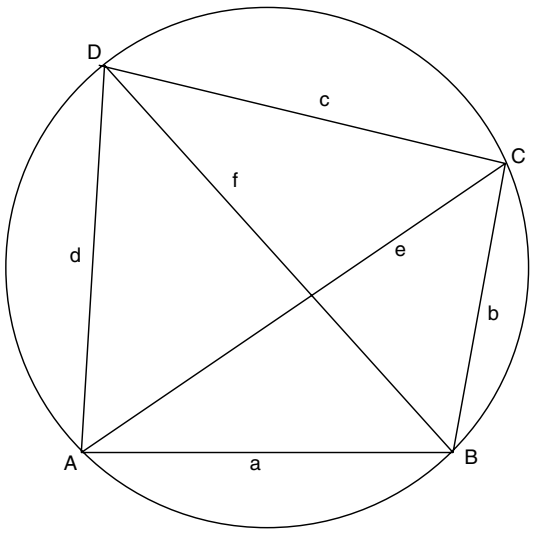

ABBILDUNG 2. Satz des Ptolemäus

zunächste drei Gleichungen, die beschreiben, daß die Punkte A, B, C, D auf einem Kreis liegen:

$$\|A\| = \|B\| = \|C\| = \|D\|$$

also

$$\begin{aligned}(x_A^2 + y_A^2) - (x_B^2 + y_B^2) &= 0,\\ (x_B^2 + y_B^2) - (x_C^2 + y_C^2) &= 0,\\ (x_C^2 + y_C^2) - (x_D^2 + y_D^2) &= 0.\end{aligned} \tag{4}$$

Wir bringen a, b, c, d, e, f folgendermaßen ins Spiel:

$$\begin{aligned}(x_A - x_B)^2 + (y_A - y_B)^2 - a^2 = 0, \quad (x_B - x_C)^2 + (y_B - y_C)^2 - b^2 = 0\\ (x_C - x_D)^2 + (y_C - y_D)^2 - c^2 = 0, \quad (x_D - x_A)^2 + (y_D - y_A)^2 - d^2 = 0\\ (x_A - x_C)^2 + (y_A - y_C)^2 - e^2 = 0. \quad (x_B - x_D)^2 + (y_B - y_D)^2 - f^2 = 0.\end{aligned}$$

Diese neun Gleichungen beschreiben eine affine Varietät $V \subset \mathbb{C}^{14}$. (Es ist zweckmäßig, $\mathbb{R}$ zu $\mathbb{C}$ zu erweitern, damit wir den Hilbertschen Nullstellensatz zur Verfügung haben.) Sei I das von den entsprechenden Polynomen in $\mathbb{C}[x_A, , \ldots, y_D, a, \ldots, f]$ erzeugte Ideal. Die zu beweisende Hypothese lautet

$$h(A, B, C, D) = ef - (ac + bd) = 0.$$

für Punkte A, B, C, D, die wie im Diagramm angeordnet sind.

Im bestmöglichen Fall ist das Polynom $h \in I$, d. h. $h(A, B, C, D) = 0$ ist algebraische Konsequenz der Gleichungen, die V definieren. Das kann aber unmöglich gelten, denn a, b, c, d, e, f gehen in die I erzeugenden Polynome nur über ihre Quadrate ein.

Vielleicht haben wir ja zuviel verlangt – es würde uns reichen, daß $h \in \sqrt{I}$. `Singular` sagt „nein“. Allerdings sollte uns diese negative Antwort nicht enttäuschen, denn wir haben bisher (mindestens) zwei Aspekte nicht berücksichtigt.

(i) Wie schon bemerkt, gehen die Unbestimmten a, b, c, d, e, f nur über ihre Quadrate in die V definierenden Gleichungen ein. Das bedeutet für ein Polynom $F(a, \ldots, f) \in \sqrt{I}$, daß auch $F(\pm a, .., \pm f) \in \sqrt{I}$ gilt. Aus $h \in \sqrt{I}$ würde folgen, daß auch $ef + (ac + bd) \in \sqrt{I}$, und damit $2ef \in I$, was nun aber wirklich nicht sein kann.

(ii) Daß die Ecken auf dem Viereck in der Reihenfolge angeordnet sind, wie es der Satz des Ptolemäus verlangt, kommt in den Gleichungen nicht zum Ausdruck. Um zu erfassen, was dies bedeutet, lassen wir etwa den Punkt C in Richtung B wandern und sogar durch B hindurch. Wenn dann der Satz des Ptolemäus immer noch richtig ist, ergibt sich $ac = ef + bd$, und das paßt nur dann „stetig“ zu $ef = ac + bd$, wenn wir b negativ messen, nachdem C durch B hindurch gelaufen ist.

Beide Überlegungen bringen uns zu folgendem Schluß: Man muß also außer $h = h_1$ alle Polynome betrachten, die sich aus h durch Vorzeichenwechsel der Variablen ergeben. Bis auf einen Faktor -1 sind dies genau die folgenden vier Polynome:

$$\begin{aligned} h_1 = h &= ef - ac - bd \\ h_2 &= ef + ac - bd \\ h_3 &= ef - ac + bd \\ h_4 &= ef + ac + bd \end{aligned}$$

Eine überprüfung ergibt, daß sogar $h_1 h_2 h_3 h_4 \in I$ gilt. Mindestens eine der Gleichungen muß also in jedem Punkt von V erfüllt sein. Durchläuft man das Viereck in der „richtigen“ Reihenfolge A, B, C, D, dann müssen alle Längen positiv sein und außerdem $ef > ac$ und $ef > bd$ gelten. Letzteres folgt mit der Dreiecksungleichung. Unter diesen Voraussetzungen gilt $h_1 \cdots h_4 = 0$ nur, wenn $h = h_1 = 0$, was zu zeigen war.

Mit $V_i = V \cap \mathcal{V}(h_i)$ gilt $V_i \not\subset V_j$, $i \neq j$, und

$$V = V_1 \cup \cdots \cup V_4.$$

Auf V_i gilt $h_i(x) = 0$. Nicht klar ist allerdings, ob $V_1, \ldots, V_4$ die irreduziblen Komponenten von V sind. Es gibt zwar Algorithmen, mit denen es prinzipiell möglich ist, diese Frage zu entscheiden, aber das Ideal I ist für sie noch zu komplex. Immerhin können wir eine etwas einfachere Aufgabe lösen. Wir projizieren die Elemente $(x_A, \ldots, y_D, a, \ldots, f) \in V$ auf die letzten 6 Komponenten $(a, \ldots, f)$. Die kleinste das Bild von V enthaltende affine Untervarietät von $\mathbb{C}^6$

wird dann durch

$$J = I \cap \mathbb{C}[a, b, c, d, e, f]$$

definiert. (Wir werden dies im nächsten Abschnitt beweisen.) Wenn wir J etwa mit `Singular` bestimmen, erleben wir eine kleine Überraschung: J wird von 4 irreduziblen homogenen Polynomen des Grades 6 erzeugt. Da $h_1h_2h_3h_4 \in I$, folgt natürlich, daß $h_1h_2h_3h_4 \in J$.

Wenn wir die Funktion `primdecGTZ` der `Singular`-Bibliothek `primdec.lib` anwenden, zeigt sich im Nu, daß J Durchschnitt von 4 Primidealen $\mathfrak{p}_i$ ist. Jedes wird von einem Polynom vom Grad 2 und einem des Grades 3 erzeugt. Wir können sie so numerieren, daß $h_i \in \mathfrak{p}_i$. Dann ist der zweite Erzeuger von $\mathfrak{p}_1$ etwa durch

$$(ab + cd)e - (ad + bc)f$$

gegeben, und wir haben ein zweite einfache Gleichung entdeckt, die von den Seiten und Diagonalen eines Sehnenvierecks erfüllt wird.

Daß J Durchschnitt von 4 Primidealen ist, ist immerhin ein Indiz dafür, daß dies auch für I gilt. Dann würde folgen, daß $V_1, \ldots, V_4$ die irreduziblen Komponenten von V sind.

Es gibt an diesem Beispiel noch einen interessanten Aspekt zu beobachten: Nur in $V_1, \ldots, V_3$ liegen reelle Punkte, für die A, B, C, D paarweise everschieden sind! Dies erkennen wir daran, daß für die Abstände $a = \|A - B\|$ usw. genau eine der drei Gleichungen $h_1 = 0$, $h_2 = 0$ oder $h_3 = 0$ erfüllt sein muß, wie man durch Ausprobieren aller relativen Lagen der Punkte auf dem Kreis ausprobieren kann. (Es gibt nur 3 wesentlich verschiedene Anordnungen der Punkte A, B, C, D auf dem Kreis gibt, wenn wir die Durchlaufrichtungen nicht unterscheiden.)

Für den Kenner der Begriffe sei folgendes hinzugefügt: Es gilt $\dim V = 5$ und folglich ist I ist ein vollständiger Durchschnitt. Da $\mathbb{C}[X_A, \ldots, f]/I$ Multiplizität 512 hat und diese mit der geometrischen Multiplizität von V übereinstimmt, ist $I = \mathscr{I}(V)$.

Weiterführende Literatur: [**IVA**], [**CCA**].

ABSCHNITT 12

Parametrisierung und Elimination

Eine Aufgabe, die sich mit unseren Methoden vollständig lösen läßt, ist die Bestimmung einer impliziten Beschreibung von Teilmengen des K^n, die durch eine Parametrisierung mit rationalen Funktionen gegeben sind. Allgemeiner werden wir die Bilder von affinen Varietäten unter rationalen Abbildungen betrachten.

Rationale Funktionen sind von der Form

$$f = \frac{p}{q} \in K(T_1, \ldots, T_m), \quad p, q \in K[T_1, \ldots, T_m].$$

Durch die runden Klammern wird der Quotientenkörper des Polynomrings bezeichnet. Wir können nach Kürzen gemeinsamer Faktoren p und q als teilerfremd annehmen. Die Funktion p/q mit Werten in K ist nur auf $K^m \setminus \mathcal{V}(g)$ sinnvoll definiert.

Beispiel 12.1. $K = \mathbb{R}, m = 1,$

$$x = f_1(t) = \frac{1 - t^2}{1 + t^2}, \quad y = f_2(t) = \frac{2t}{1 + t^2}.$$

Der Nenner hat keine Nullstelle (beachte, daß dies in $K = \mathbb{C}$ nicht mehr gilt). Welche Gleichung erfüllen $f_1(t)$, $f_2(t)$ für alle $t \in \mathbb{R}$? Anders gesagt: Wie lautet die implizite Darstellung der Kurve, die der Punkt $(f_1(t), f_2(t)) \in \mathbb{R}^2$ beschreibt, wenn t durch $\mathbb{R}$ (bzw. durch $\mathbb{C} \setminus \{\pm i\}$) läuft? Wir haben t aus den parametrischen Gleichungen zu eliminieren.

Nach Multiplikation mit $1 + t^2$ gilt

$$(1 + t^2)x - (1 - t^2) = 0, \quad (1 + t^2)y - 2t = 0.$$

Indem man t aus f_1 und f_2 eliminiert, erhält man

$$x^2 + y^2 - 1 = 0, \quad t = \frac{y}{x + 1}$$

Die obigen Darstellungen parametrisieren also einen Kreis in der Ebene. Allerdings wird der Punkt $(0, 1)$ für keinen endlichen Wert t getroffen (siehe Abb. 1). (Wir haben bei der Rechnung etwas Glück gehabt; siehe Satz 12.3.)

Am obigen Beispiel zeigt sich ein unangenehmer Effekt: wir können nicht erwarten, daß das Bild einer rationalen Abbildung abgeschlossen ist – das ändert sich auch bei polynomialen Abbildungen nicht. Man ist also interessiert an der *kleinsten* affinen Varietät, welche die parametrisierte Menge umfaßt.

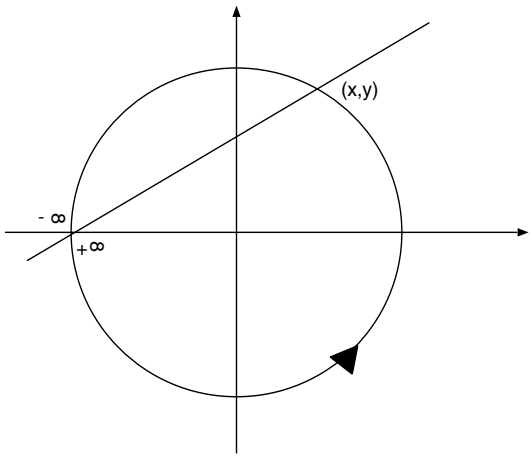

ABBILDUNG 1. Rationale Parametrisierung des Einheitskreises

Parametrisierungen sind natürlich nur spezielle Abbildungen. Im folgenden Satz betrachten wir Abbildungen, die durch Polynome gegeben sind, und die Bildmengen affiner Varietäten unter ihnen.

Satz 12.2. *Sei K ein Körper und seien $f_1, \ldots, f_n \in K[T_1, \ldots, T_m]$ Polynome, welche die Abbildung*

$$\tau : K^m \to K^n, \quad t \mapsto (f_1(t), \ldots, f_n(t)),$$

definieren.

Sei V eine affine Varietät in K^m. Mit A sei die kleinste $\tau(V)$ umfassende affine Varietät bezeichnet, d. h. die abgeschlossene Hülle von $\tau(V)$ in der Zariski-Topologie von K^n. Dann gilt

$$\mathscr{I}(A) = K[X_1, \ldots, X_n] \cap \big(\mathscr{I}(V), X_1 - f_1, \ldots, X_n - f_n\big).$$

Insbesondere gilt: Wenn V irreduzibel ist, so ist auch A irreduzibel.

Beweis. Sei $I = \mathscr{I}(\tau(V)) \subset K[X_1, \ldots, X_n]$. Dann ist $A = \mathscr{V}(I)$ und $I = \mathscr{I}(A)$. Also gilt $g \in \mathscr{I}(A)$ genau dann, wenn $g(\tau(t)) = 0$ für alle $t \in V$.

Es gilt

$$g(\tau(t)) = g(f_1(t), \ldots, f_n(t)).$$

Dies zeigt: $g \circ \tau$ ist nichts anderes als das Polynom in $T_1, \ldots, T_m$, das aus g entsteht, wenn wir $f_1, \ldots, f_n$ der Reihe nach für $X_1, \ldots, X_n$ substituieren. Sei $\varphi : K[X_1, \ldots, X_n] \to K[T_1, \ldots, T_m]$ der durch diese Substitution definierte Homomorphismus. Dann ist $g \circ \tau$ die durch $\varphi(g)$ definierte polynomiale Funktion auf K^n, und

$$g \in \mathscr{I}(A) \iff g(\tau(t)) = 0 \text{ für alle } t \in V \iff \varphi(g) \in \mathscr{I}(V),$$

mit anderen Worten: $\mathscr{I}(A)$ ist der Kern des induzierten Homomorphismus $\overline{\varphi} : K[X_1, \ldots, X_n] \to K[T_1, \ldots, T_m]/\mathscr{I}(V)$.

Den Kern von $\overline{\varphi}$ haben wir aber schon in Satz 9.6 ausgerechnet: $\operatorname{Ker}\overline{\varphi} = K[X_1, \ldots, X_n] \cap \big(\mathscr{I}(V), X_1 - f_1, \ldots, X_n - f_n\big)$, wie behauptet.

Wenn $\mathscr{I}(V)$ ein Primideal ist, ist $\mathscr{I}(A)$ der Kern eines Homomorphismus von $K[X_1, \ldots, X_n]$ in den Integritätsbereich $K[T_1, \ldots, T_m]/\mathscr{I}(V)$ und damit selbst ein Primideal. Wir können natürlich auch geometrisch argumentieren: Wenn A nichttrivial in der Form $A = A_1 \cup A_2$ dargestellt werden kann, so ist $V = (V \cap \tau^{-1}(A_1) \cup (V \cap \tau^{-1}(A_2)$ eine nichttriviale Zerlegung von V. □

Hervorheben wollen wir noch den Speziallfall, in dem $m \geq n$ ist, $X_1 = T_1, \ldots, X_n = T_n$ und $f_i = T_i$ für $i = 1, \ldots, n$. In diesem Fall ist τ die natürliche Projektion auf die ersten n Komponenten und $\mathscr{I}(A)$ entsteht aus $\mathscr{I}(V)$ durch Elimination von $T_{n+1}, \ldots, T_m$.

Ein weiterer Spezialfall ist $V = K^m$. Wenn K unendlich ist, ist $\mathscr{I}(V) = 0$ und $\mathscr{I}(A) = \mathscr{I}(\tau(K^n)) = K[X_1, \ldots, X_n] \cap (X_1 - f_1, \ldots, X_n - f_n)$. Diesen Fall haben wir in Satz 9.5 behandelt. In ihm ist A immer irreduzibel.

Es ist wichtig, den vorangegangenen Satz auf rationale Abbildungen zu verallgemeinern – dies zeigt schon das Beispiel des Einheitskreises, den wir nicht polynomial parametrisieren können.

Definition. Eine *rationale Abbildung* auf K^m ist von der Form

$$\tau : t \mapsto \left(\frac{f_1(t)}{g_1(t)}, \ldots, \frac{f_n(t)}{g_n(t)}\right), \quad f_i,\ g_i \in K[T_1, \ldots, T_m], g_i \neq 0.$$

Sie ist definiert auf $K^n \setminus \bigcup \mathscr{V}(g_i)$. (Durch Übergang zum Hauptnenner kann man $g = g_1 = \cdots = g_m$ annehmen.)

Satz 12.3. *Sei K ein Körper und $f_1, \ldots, f_n, g \in K[T_1, \ldots, T_m]$, $g \neq 0$. Sei $\tau : K^m \setminus \mathscr{V}(g) \to K^n$ gegeben durch $\tau(t) = (f_1(t)/g(t), \ldots, f_n(t)/g(t))$. Sei $V \subset K^m$ eine affine Varietät und A die kleinste $\tau(V \setminus \mathscr{V}(g))$ umfassende affine Varietät. Dann gilt*

$$\mathscr{I}(A) = K[X_1, \ldots, X_n] \cap (1 - Yg, \mathscr{I}(V), X_1 - Yf_1, \ldots, X_n - Yf_n)$$

wobei das Ideal auf der rechten Seite in $K[X_1, \ldots, X_n, T_1, \ldots, T_m, Y]$ zu bilden ist.

Beweis. Die Funktionen, die wir für $X_1, \ldots, X_n$ substituieren, gehören zwar nicht zu $R = K[T_1, \ldots, T_m]$, aber zu

$$S = R\left[\frac{1}{g}\right] = \{p/g^k : p \in R,\ k \in \mathbb{N}\}.$$

Wir haben also den Ringhomomorphismus $\varphi : K[X_1, \ldots, X_n] \to S$ zu betrachten, bei dem $\varphi(X_i) = f_i/g$ ist. Genau dann verschwindet $h \in K[X_1, \ldots, X_n]$ auf $\tau(V \setminus \mathscr{V}(g))$, wenn $\varphi(h)$ als rationale Funktion auf $V \setminus \mathscr{V}(g)$ verschwindet.

Wir behaupten, daß $p \in S$ genau dann auf $V \setminus \mathscr{V}(g)$ verschwindet, wenn $p = q/g^k$ mit einem $q \in \mathscr{I}(V)$ und $k \in \mathbb{N}$ ist. Ist $q \in \mathscr{I}(V)$, dann verschwindet q/g^k natürlich auf $V \setminus \mathscr{V}(g)$.

Umgekehrt können wir jedes $p \in S$ in der Form $p = q/g^k = qg/g^{k+1}$, $q \in K[T_1, \ldots, T_m]$, für hinreichend großes k schreiben. Wenn dann $p(t) = 0$ für alle $t \in V \setminus \mathscr{V}(g)$, gilt $g(t)q(t) = 0$ für alle $t \in V$, und damit $qg \in \mathscr{I}(V)$). Wir ersetzen nun einfach q durch qg.

Also haben wir das Urbild von $\mathscr{I}(V)S$ unter φ zu bestimmen. Um unsere vorhandenen Sätze anwenden zu können, schreiben wir S als Restklassenring von $K[T_1, \ldots, T_m, Y]$ vermöge der Substitution

$$T_i \mapsto T_i, \qquad Y \mapsto 1/g.$$

Dann gilt $S \cong K[T_1, \ldots, T_m, Y]/(1 - YT)$ (siehe Übungsaufgabe). Insgesamt erhalten wir

$$S/\mathscr{I}(V)S \cong K[T_1, \ldots, T_m, Y]/(1 - Yg, \mathscr{I}(V)).$$

Wie wir in Satz 9.6 gesehen haben, ist unser gesuchtes Ideal gegeben durch

$$K[X_1, \ldots, X_n] \cap (1 - YT, \mathscr{I}(V), X_1 - Yf_1, \ldots, X_n - Yf_n). \qquad \square$$

Wir haben schon am Beispiel einer Übungsaufgabe und am Kreis in der Ebene gesehen, daß selbst im Fall $K = \mathbb{C}$ und $V = K^n$ nicht zu erwarten ist, daß $A = \tau(K^m \setminus W)$ gilt. Wir verzichten an dieser Stelle darauf, die Differenz $A \setminus \tau(K^m \setminus W)$ genauer zu untersuchen.

Wir haben die Bestimmung der Gleichungen für A auf ein Eliminationsproblem zurückgeführt, und Elimination ist ein gefundenes Fressen für Gröbner-Basen, wenn man einmal davon absieht, daß die konkrete Rechnung am Aufwand scheitern kann.

Das umgekehrte Problem, nämlich zu einer implizit gegebenen Varietät eine rationale Parametrisierung zu finden, ist im allgemeinen nicht lösbar, weil nur wenige Varietäten eine solche Parametrisierung besitzen. Eine weitere Untersuchung würde uns in tiefere Gebilde der algebraischen Geometrie führen, die wir im Rahmen dieser Vorlesung nicht erreichen könne.

Weiterführende Literatur: [**IVA**], [**CCA**].

ABSCHNITT 13

Polynomiale Gleichungssysteme mit endlich vielen Lösungen

In diesem Abschnitt beschäftigen wir uns mit speziellen affinen Varietäten, nämlich solchen, die nur endlich viele Punkte enthalten. Speziell wollen wir bestimmen, wie viele Lösungen ein Gleichungssystem der Form

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= 0 \\ &\vdots \qquad\qquad \text{mit } \ f_1,\ldots,f_m \in K[X_1,\ldots,X_n] \\ f_m(x_1,\ldots,x_n) &= 0 \end{aligned}$$

hat, vorausgesetzt die Zahl der Lösungen ist endlich.

Es ist klar, daß wir die Endlichkeit der Lösungsmenge mit algebraischen Mitteln nur entscheiden können, wenn der Körper K abgeschlossen ist oder wir allgemeiner die Lösungen in $\overline{K}^n$ zählen, wobei $\overline{K}$ der algebraische Abschluß von K ist. Dies sieht man an einem so einfachen Beispiel wie der Gleichung $x^2+y^2+1=0$ die über $\mathbb{R}$ keine Lösungen besitzt, aber über $\mathbb{C}$ unendlich viele. Durch einen Index an $\mathscr{V}$ zeigen wir, wo die Nullstellen gesucht werden.

Zuerst wollen wir ein Kriterium angeben, um zu entscheiden, ob ein Gleichungssystem wie oben überhaupt nur endlich viele Lösungen hat.

Satz 13.1. *Sei I ein Ideal in $R = K[X_1,\ldots,X_n]$. Mit $\overline{R}$ sei der Polynomring $\overline{K}[X_1,\ldots,X_n]$ über dem algebraischen Abschluß $\overline{K}$ von K bezeichnet. Ferner sei $<$ eine monomiale Ordnung auf R und $\overline{R}$. Dann sind äquivalent:*

(a) $\mathscr{V}_{\overline{K}}(I)$ *ist endlich.*
(b) $I\overline{R}$ *ist nur in endlich vielen maximalen Idealen von $\overline{R}$ enthalten.*
(c) *Für alle $i = 1,\ldots,n$ ist $K[X_i] \cap I \neq \{0\}$.*
(d) R/I *ist ein endlichdimensionaler K-Vektorraum.*
(e) $\mathscr{M}_n \setminus \mathrm{LM}(I)$ *ist endlich, wobei $\mathscr{M}_n$ die Menge aller Monome in den X_i bezeichnet.*
(f) *Für alle $i = 1,\ldots,n$ existiert ein $e_i \in \mathbb{N}$ mit $X_i^{e_i} \in \mathrm{LM}(I)$, d. h. $X_i \in \sqrt{\mathrm{LM}(I)}$.*

Beweis. Wir wollen uns zunächst überlegen, daß man in den Aussagen (c) – (f) überall K durch $\overline{K}$, R durch $\overline{R}$ und I durch $I\overline{R}$ ersetzen darf.

Für (d), (e) und (f) ist dies sofort klar, denn der Buchberger-Algorithmus berechnet aus einem Erzeugendensystem von I, das ja auch ein Erzeugendensystem von $\overline{I}$ ist, eine Gröbner-Basis, die in R liegt. Mit anderen Worten, die Menge der

Monome $\mathrm{LM}(f)$, $f \in I$, vergrößert sich nicht, wenn man zu $\mathrm{LM}(f)$, $f \in I\overline{R}$ übergeht.

Aussage (c) ist unabhängig von der monomialen Ordnung. Wir können also eine passende Eliminationsordnung wählen und das gleiche Argument wie soeben verwenden. Nun ist klar, daß wir für den Rest des Beweises annehmen dürfen, K sei algebraisch abgeschlossen.

(a) $\Longleftrightarrow$ (b): Nach dem Hilbertschen Nullstellensatz entsprechen die Punkte $x \in K^n$ bijektiv den maximalen Idealen $\mathfrak{m}_x \subset R$. Dabei gilt $m_x \supset I \Longleftrightarrow x \in \mathscr{V}_K(I)$.

(d) $\Longleftrightarrow$ (e) $\Longleftrightarrow$ (f): Die Restklassen von Monomen aus $\mathscr{M}_n \setminus \mathrm{LM}(I)$ bilden eine Basis von R/I (Satz 9.1). Daraus folgt die erste Äquivalenz. Die zweite ist offensichtlich.

(a) $\Rightarrow$ (c): Man projiziere $\mathscr{V}_K(I)$ auf die $i$te Koordinatenachse. Das ergibt nach Voraussetzung eine endliche Menge $y_1, \ldots, y_q$. Dann können wir

$$g_i = (X_i - y_1) \cdots (X_i - y_q)$$

wählen. Dieses Polynom verschwindet auf ganz $\mathscr{V}_K(I)$. Wegen $\mathscr{I}(\mathscr{V}_K(I)) = \sqrt{I}$ folgt $g^m \in I$ für m hinreichend groß.

(c) $\Rightarrow$ (a): Sei $g_i \in K[X_i] \cap I$, $g_i \neq 0$.Mit $A_i = \mathscr{V}(g_i)$ folgt dann

$$\mathscr{V}_K(I) \subset A_1 \times \cdots \times A_n.$$

Also ist A endlich, denn die A_i sind endlich.

(c) $\Rightarrow$ (f): Aus $g_i \in K[X_i] \cap I$ folgt $\mathrm{LM}(g_i) = X_i^{e_i} \in \mathrm{LM}(I)$.

(d) $\Rightarrow$ (c): Wähle eine Eliminationsordnung für X_i. Wegen (d) $\Rightarrow$ (f) folgt dann $X_i^{e_i} \in \mathrm{LM}(I)$. Ein Polynom g mit $\mathrm{LM}(g) = X_i^{e_i}$ gehört zu $K[X_i]$. □

Definition. Ein Ideal $I \subset K[X_1, \ldots, X_n]$, das eine der obigen Eigenschaften erfüllt, heißt *nulldimensional*. Dieser Begriff beruht darauf, daß R/I (die von uns nicht eingeführte) Krull-Dimension 0 hat.

Als nächstes wollen wir auch die genaue Anzahl der Lösungen eine polynomialen Gleichungssystems bestimmen.

Satz 13.2. *Mit den Bezeichnungen wie oben sei $I \subset K[X_1, \ldots, X_n]$ ein nulldimensionales Ideal. Setze $\overline{I} = I\overline{R}$. Dann gilt:*

$$\dim_K R/I \geq \dim_K R/\sqrt{I} \geq \dim_{\overline{K}} \overline{R}/\sqrt{\overline{I}} = \#\mathscr{V}_{\overline{K}}(I)$$

Beweis. Offenbar gilt

$$R/\sqrt{I} \cong (R/I)/(\sqrt{I}/I)$$

also folgt $\dim_K R/\sqrt{I} = \dim_K R/I - \dim_K \sqrt{I}/I$. Daraus folgt die erste Ungleichung.

Betrachte nun $\sqrt{I}$ und seine Erweiterung in $\overline{R}$. Die Ideale $\sqrt{I}$ und $\sqrt{I} \cdot \overline{R}$ enthalten die gleichen Monome, weil im Buchberger-Algorithmus nur Koeffizienten aus K auftauchen, wenn man mit einem Erzeugendensystem von $\sqrt{I}$ startet. Mit Satz 9.1 ergibt sich

$$\dim_K R/\sqrt{I} = \dim_{\overline{K}} \overline{R}/\sqrt{I} \cdot \overline{R}.$$

(Das kann man auch mit strukturellen Argumenten begründen.) Da $\sqrt{I\,\overline{R}} \subset \sqrt{I\,\overline{R}}$, ergibt sich nun die zweite Ungleichung wie die erste.

Aus der Voraussetzung der Nulldimensionalität von I folgt die Endlichkeit von $\mathscr{V}_{\overline{K}}(I)$:

$$\mathscr{V}_{\overline{K}}(I) = \{y_1, \ldots, y_m\}.$$

Betrachte nun den Substitutionshomomorphismus

$$\varphi : \overline{K}[X_1, \ldots, X_n] \to \overline{K} \times \cdots \times \overline{K}, \quad f \mapsto (f(y_1), \ldots, f(y_m)).$$

Aus dem Hilbertschen Nullstellensatz folgt $\operatorname{Ker} \varphi = \mathscr{I}(\mathscr{V}_{\overline{K}}(I)) = \sqrt{I \cdot \overline{R}}$. Die Abbildung φ ist aber auch surjektiv, man konstruiert zum Beispiel nach der Lagrangeschen Methode Polynome $e_i \in \overline{K}[X_1, \ldots, X_n]$ mit $e_{\mathscr{I}}(y_j) = \delta_{ij}$. Insgesamt folgt

$$\overline{R}/\sqrt{I \cdot \overline{R}} \cong \overline{K} \times \cdots \times \overline{K}. \qquad \square$$

Sei nun K algebraisch abgeschlossen. Wir haben im vorangegangenen Beweis bewußt vermieden, K^m für $K \times \cdots \times K$ zu schreiben, denn wir wollen $K \times \cdots \times K$ nicht nur als K-Vektorraum, sondern auch als Ring mit komponentenweiser Addition und Multiplikation verstehen. Sei

$$S = K \times \cdots \times K.$$

Ist $e_i = (0, \ldots, 1, 0 \ldots, 0)$ wie stets der i-te „Einheitsvektor“ mit der 1 an der i-ten Stelle, dann bilden die e_i offenbar ein System orthogonaler Idempotenter (also $e_i e_j = 0$ für $i \neq j$ und $e_i^2 = e_i$). Leicht einzusehen ist ebenfalls, daß S genau 2^m Ideale I hat, nämlich gerade die Ideale der Form

$$I = (e_{i_1}, \ldots, e_{i_p}), \quad i_1 < \cdots < i_p,\ 0 \leq p \leq n.$$

Denn mit $(a_1, \ldots, a_n) \in I$, $a_i \neq 0$, ist auch

$$(0, \ldots, a_i^{-1}, \ldots, 0) e_i (a_1, \ldots, a_n) = e_i \in I,$$

und es gilt $Se_i = Ke_i$.

Ferner sind alle Ideale Radikalideale, denn

$$(a_1, \ldots, a_n)^k = (a_1^k, \ldots, a_n^k)$$

und $(a_1^k, \ldots, a_n^k) \in (e_{i_1}, \ldots, e_{i_p})$ genau dann, wenn $a_j^k = 0$ für alle $j \notin \{i_1, \ldots, i_p\}$. Im Körper K gilt $a_j^k = 0$ genau dann der Fall, wenn schon $a_j = 0$ ist. In

äquivalenter Formulierung heißt das: Jedes Ideal J mit

$$\sqrt{I} \subset J \subset R$$

ist selbst ein Radikalideal (zur Erinnerung: $R/\sqrt{I} \cong S$).

Wir fassen dies so zusammen:

Satz 13.3. *Sei K algebraisch abgeschlossen und $I \subset K[X_1, \ldots, X_n]$ nulldimensional. Dann gilt: Jedes $\sqrt{I}$ umfassende Ideal in $R = K[X_1, \ldots, X_n]$ ist ein Radikalideal.*

Beweis. Sei $S = R/\sqrt{I} \cong K \times \cdots \times K$ wie oben und $J \supset \sqrt{I}$ ein weiteres Ideal in R. Es gilt

$$R/J \cong (R/\sqrt{I})/(J/\sqrt{I}) = S/(J/\sqrt{I})$$

und ein Restklassenring von S hat keine nilpotenten Elemente, wie wir schon gesehen haben. □

Daß K algebraisch abgeschlossen ist, ist für den Satz zwar unwesentlich, aber es können in der Zerlegung von $R/\sqrt{I}$ sonst auch andere Körper als K auftreten. Einzig wesentlich ist, daß I ein Ideal in einem Ring R ist, das Durchschnitt endlich vieler maximaler Ideale $\mathfrak{m}_1, \ldots, \mathfrak{m}_q$ ist. Dann zeigt der Chinesische Restsatz, daß $R/I = R/\mathfrak{m}_1 \times \cdots \times R/\mathfrak{m}_q$ ein direktes Produkt von Körpern ist und wir können so argumentieren wie oben.

Satz 13.4. *Sei K ein perfekter Körper und $I \subset K[X_1, \ldots, X_n]$ ein nulldimensionales Ideal mit $I \cap K[X_i] = (g_i)$ für $i = 1, \ldots, n$. Sei h_i der quadratfreie Teil von g_i. Die Erweiterungen von I und $H = (h_1, \ldots, h_n)$ in $\overline{K}[X_1, \ldots, X_n]$ seien mit $\overline{I}$ und $\overline{H}$ bezeichnet. Dann gilt:*

$$I + H = \sqrt{I}, \quad \overline{I} + \overline{H} = \sqrt{\overline{I}}.$$

Beweis. Es ist klar, daß $H \subset \sqrt{I}$ ist, weil h_i^k für genügend großes k Vielfaches von g_i ist. Also gilt

$$I + H \subset \sqrt{I}, \quad \overline{I} + \overline{H} \subset \sqrt{\overline{I}}$$

(siehe Übungsaufgabe). Es genügt zu zeigen, daß $\overline{I} + \overline{H}$ und $I + H$ Radikalideale sind. Wegen

$$I + H = (\overline{I} + \overline{H}) \cap K[X_1, \ldots, X_n]$$

reicht es sogar zu zeigen, daß nur $\overline{I} + \overline{H}$ ein Radikalideal ist. Wir schreiben im folgenden einfacher $\overline{K} = K$, denn weil K perfekt ist, sind $h_1, \ldots, h_n$ auch in $\overline{K}[X_1, \ldots, X_n]$ quadratfrei. Dafür genügt ja, daß $\mathrm{ggT}(f, f') = 1$ in $K[X_1, \ldots, X_n]$, un dies gilt für quadratfreie Polynome über perfekten Körpern.

Aus Satz 13.1 folgt, daß H ein nulldimensionales Ideal ist. Sei $A = \mathscr{V}(H)$. Es genügt dann zu zeigen, daß $H = \sqrt{H}$ ist. Dann ist nämlich H ein nulldimensionales Radikalideal und $I + H$ ein H umfassendes Ideal, also ebenfalls ein Radikalideal gemäß Satz 13.3. Wir setzen $A_i = \mathscr{V}(g_i) = \mathscr{V}(h_i) \subset K$. Dann gilt

$$A = \mathscr{V}(H) = A_1 \times \cdots \times A_n.$$

Mit $d_i = \operatorname{grad} h_i$ folgt

$$\#A = \prod_{i=1}^{n} \#A_i = d_1 \cdots d_n.$$

Nun gilt $\dim K[X_1, \ldots, X_n]/H = d_1 \cdots d_n$, was unmittelbar aus Satz 9.1 folgt, denn $\mathrm{LM}(H) = (X_1^{d_1}, \ldots, X_n^{d_n})$. Andererseits ist auch $\dim K[X_1, \ldots, X_n]/\sqrt{H} = d_1 \cdots d_n$ und damit

$$\dim_K \sqrt{H}/H = \dim K[X_1, \ldots, X_n]/\sqrt{H} - \dim_K K[X_1, \ldots, X_n]/H = 0.$$

Das geht nur bei $H = \sqrt{H}$. □

Damit haben wir einen Algorithmus gefunden, mit dem wir die Radikale nulldimensionaler Ideale bestimmen können. Außerdem können wir die Anzahl der Nullstellen eines nulldimensionalen Ideals ausrechnen:

Korollar 13.5. *Mit den Bezeichnungen des Satzes gilt*

$$\dim K[X_1, \ldots, X_n]/(I + H) = \#\mathscr{V}_{\overline{K}}(I)$$

Beweis.

$$\begin{aligned} \#\mathscr{V}_{\overline{K}}(I) &= \dim_{\overline{K}} \overline{K}[X_1, \ldots, X_n]/\sqrt{\overline{I}} \\ &= \dim_{\overline{K}} \overline{K}[X_1, \ldots, X_n]/(\overline{I} + \overline{H}) \\ &= \dim_K K[X_1, \ldots, X_n]/(I + H) \end{aligned}$$ □

Nun sind wir bereit, ein Verfahren zur Bestimmung von $\#\mathscr{V}_{\overline{K}}(I)$ anzugeben: Sei weiterhin $I \subset K[X_1, \ldots, X_n]$ mit einem perfekten Körper K. Solche Körper sind z.B. die endlichen Körper oder die Körper mit Charakteristik 0.

(a) Bestimme für alle $i = 1, \ldots, n$ durch Elimination ein $g_i \in K[X_i]$ mit $(g_i) = K[X_i] \cap I$.
(b) Bestimme h_i, den quadratfreien Teil von g_i, zum Besipiel mit Hilfe der partiellen Ableitungen.
(c) Bestimme die Dimension von $K[X_1, \ldots, X_n]/(I + (h_1, \ldots, h_n))$, zum Bweispiel durch Abzählen von $\mathscr{M}_n \setminus \mathrm{LM}(I + (h_1, \ldots, h_n))$. Berechne dazu eine Gröbner-Basis von $I + (h_1, \ldots, h_n)$.

Wir können Gröbner-Basis-Methoden nicht nur verwenden, um zu testen, ob ein Ideal nulldimensional ist und dann die Anzahl der Nullstellen der I erzeugenden Polynome zu bestimmen. Wir können sie auch anwenden, um die Nullstellen effektiv auszurechnen. Hierfür bieten sich zwei Ansätze an:

(a) Bestimme $g_1, \ldots, g_n$ wie oben und berechne $A_i = \mathscr{V}_K(g_i)$, $i = 1, \ldots, n$. Dann bestimmen wir einfach durch Einsetzen in die Erzeuger von I, welche $x \in A = A_1 \times \cdots \times A_n$ auch in $\mathscr{V}_K(I)$ liegen. Beachte, daß A endlich ist. Natürlich bleibt das Problem, die Nullstellen von g_i zu bestimmen, wofür die numerische Mathematik viele Näherungsverfahren anbietet. Der Vorteil der vorangegangenen Elimination liegt darin, daß das Problem der Bestimmung der Nullstellen eines System von Polynomen mehrerer Veränderlicher auf die Bestimmung von Nullstellen von univariaten Polynomen zurückgeführt ist.

(b) Man wähle als monomiale Ordnung die lexikographische Ordnung mit $X_1 > \cdots > X_n$ und ermittle eine Gröbner-Basis G von I. Dann ist $G \cap K[X_{i+1}, \ldots, X_n]$ eine Gröbner-Basis von $I \cap K[X_{i+1}, \ldots, X_n]$, so daß wir die Gröbner-Basis in „Dreiecksform“ bekommen:

$$f_1 \in K[X_n], \quad \left.\begin{matrix} f_2 \\ \vdots \\ f_{i_{n-1}} \end{matrix}\right\} \in K[X_{n-1}, X_n], \quad \left.\begin{matrix} f_{i_{n-1}+1} \\ \vdots \\ f_{i_{n-2}} \end{matrix}\right\} \in K[X_{n-2}, X_{n-1}, X_n]$$

usw. Dabei gilt stets $i_j + 1 \leq i_{j-1}$. Nun kann man die Nullstellen von f_1 bestimmen, diese in $f_2, \ldots, f_{i_{n-1}}$ einsetzen. Dann verbleibt in diesen Polynomen nur die Unbekannte X_{n-1}. So fährt man fort, bis alle Elemente der Gröbner-Basis ausgewertet sind.

Weiterführende Literatur: [**IVA**], [**CCA**].

Literaturverzeichnis

[Alg] W. Bruns: Einführung in die Algebra. OSM, Reihe V, EHeft 8, `http://www.math.uos.de/staff/phpages/brunsw/algebra.pdf`

[MCA] J. von zur Gathen, J. Gerhard: Modern computer algebra. Cambridge University Press 1999, 2. Aufl. 2003

[Sing] G.-M. Greuel, G. Pfister: A Singular introduction to commutative algebra. Springer 2002

[IVA] D. Cox, J. Little, D. O'Shea: Ideals, varieties and algorithms. New York: Springer, 1998

[UAG] D. Cox, J. Little, D. O'Shea: Using algebraic geometry. New York: Springer, 1998

[CCA] M. Kreuzer, L. Robbiano: Computational commutative algebra I. Berlin: Springer, 2000