Ein Henselsches Lemma für multivariate Polynome

Beim bislang betrachteten Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier Polynome in mehreren Veränderlichen hatten wir das Problem zurückgeführt auf die ggT-Berechnung in einer Veränderlichen weniger. Diese Strategie funktioniert für den EZ GCD Algorithmus nicht, da wir für eine Liftung nach dem HENSELschen Lemma den erweiterten EUKLIDischen Algorithmus benötigen, und der steht nur für EUKLIDische Ringe zur Verfügung. Unter den Polynomringen sind nur die in einer Veränderlichen über einem Körper EUKLIDisch; wenn wir den erweiterten EUKLIDischen Algorithmus anwenden wollen, müssen wir also in einem Schritt von n Veränderlichen absteigen zu einer Veränderlichen, und auch da bekommen wir ein Problem, denn wir brauchen ja Polynome mit ganzzahligen Koeffizienten. $\mathbb{Z}[X]$ ist kein EUKLIDischer Ring, und es ist auch leicht, Beispiele zu finden, daß ein ggT nicht linear kombinierbar ist:

Beispielsweise ist der ggT von 2 und X gleich eins, aber es gibt keine Polynome $f, g \in \mathbb{Z}[X]$, für die $2f + Xg = 1$ ist: Jeder Summand in $2f$ hat lauter gerade Koeffizienten, und in Xg kommen nur Monome vor, die X enthalten, so daß $2f + Xg$ für keine Wahl von f und g einen ungeraden konstanten Term enthalten kann. In $\mathbb{Q}[X]$ ist natürlich $2 \cdot \frac{1}{2} + X \cdot 0 = 1$, aber das nützt uns nichts für eine Liftung nach Art von HENSEL, denn für die brauchen wir ganzzahlige Koeffizienten.

Wenn wir allerdings das Problem modulo einer Primzahl p betrachten, haben wir Polynome in einer Veränderlichen über einem Körper, und für die haben wir einen erweiterten EUKLIDischen Algorithmus. Modulo $p = 5$ etwa ist $2 \cdot 3 + X \cdot 0 \equiv 1 \bmod 5$. Auch modulo Fünferpotenzen finden wir entsprechende Linearkombinationen, obwohl $\mathbb{Z}/(p^\ell)$ für $\ell > 1$ kein Körper ist. Hier im Beispiel gibt es für jedes ℓ ganze Zahlen a, für die $2 \cdot a + X \cdot 0 \equiv 1 \bmod 5^\ell$ ist, etwa $a = (5^\ell + 1)/2$.

Das funktioniert nicht nur in diesem einfachen Beispiel; wie die folgende Erweiterung des HENSELschen Lemmas zeigt, können wir jede Linearkombination des ggT modulo einer Primzahl p hochheben zu einer entsprechenden Darstellung modulo jeder beliebigen Potenz von p. Da uns beim HENSELschen Lemma nicht wirklich für eine Darstellung

des ggT interessieren, sondern für die eines beliebigen Polynoms h, ist das Lemma gleich etwas allgemeiner formuliert:

Lemma: f und g seien Polynome aus $\mathbb{Z}[X]$, und p sei eine Primzahl, die weder den führenden Koeffizienten von f noch den von g teilt. Außerdem seien $f \bmod p$ und $g \bmod p$ teilerfremd in $\mathbb{F}_p[X]$. Dann gibt es zu jedem Polynom $h \in \mathbb{Z}[X]$ und jeder natürlichen Zahl ℓ Polynome $f', g' \in \mathbb{Z}[X]$ derart, daß

$$fg' + gf' \equiv h \bmod p^\ell$$

ist. Dabei läßt sich stets erreichen, daß $\deg g' < \deg g$ ist. Unter der Zusatzvoraussetzung $\deg h < \deg f + \deg g$ gilt dann auch noch die Ungleichung $\deg f' < \deg f$.

Beweis: Da $f \bmod p$ und $g \bmod p$ teilerfremd sind, liefert uns der EUKLIDische Algorithmus in $\mathbb{F}_p[X]$ Polynome a, b, die wir auch als Polynome in $\mathbb{Z}[X]$ auffassen können, so daß $af + bg \equiv 1 \bmod p$ ist. Damit ist auch $(ah)f + (bh)g \equiv h \bmod p$. Wir dividieren $ah \bmod p$ mit Rest durch $g \bmod p$ und erhalten Polynome $q, r \in \mathbb{F}_p[X]$, für die $ah \bmod p = q(g \bmod p) + r$ ist und $\deg r < \deg g$. Wir fassen q und r wieder auf als Polynome aus $\mathbb{Z}[X]$ (wobei wir natürlich viele Möglichkeiten haben, Repräsentanten zu wählen) und subtrahieren die Gleichung $(qg)f - (qf)g = 0$ von der obigen Darstellung von h. Übrig bleibt $rf + (bh + qf)g \equiv h \bmod p$, und der Grad von r ist kleiner als der von g.

Damit ist auch der Grad von rf kleiner als der von fg, also $\deg f + \deg g$, und wenn zusätzlich $\deg h < \deg f + \deg g$ ist, muß folglich auch der Grad von $(bh + qf)g = h - rf$ kleiner als $\deg f + \deg g$ sein, der Grad von $bh + qf$ also kleiner als $\deg f$. Mit $g_1 = r$ und $f_1 = bh + qf$ haben wir somit Polynome aus $\mathbb{Z}[X]$ gefunden, für die $g_1 f + f_1 g \equiv h \bmod p$ ist und $\deg g_1 < \deg g$. Unter der Zusatzvoraussetzung $\deg h < \deg f + \deg g$ ist auch $\deg f_1 < \deg f$.

Damit ist das Lemma für $\ell = 1$ bewiesen.

Für allgemeines ℓ beweisen wir die Behauptung durch vollständige Induktion. Wir nehmen also an, es gebe Polynome $f_\ell, g_\ell \in \mathbb{Z}[X]$,

für die $g_\ell f + f_\ell g \equiv h \bmod p^\ell$ ist, wobei f_ℓ, g_ℓ auch die jeweiligen Gradbedingungen erfüllen. Wir suchen entsprechende Polynome $f_{\ell+1}, g_{\ell+1}$, für die $g_{\ell+1} f + f_{\ell+1} g \equiv h \bmod p^{\ell+1}$ ist.

Dazu machen wir den Ansatz $f_{\ell+1} = f_\ell + p^\ell f^*$ und $g_{\ell+1} = g_\ell + p^\ell g^*$ mit zunächst noch unbekannten Polynomen $f^*, g^* \in \mathbb{Z}[X]$. Dann ist

$$g_{\ell+1} f + f_{\ell+1} g = g_\ell f + f_\ell g + p^\ell (g^* f + f^* g) \,.$$

Wegen $g_\ell f + f_\ell g \equiv h \bmod p^\ell$ ist die Differenz $h - (g_\ell f + f_\ell g)$ durch p^ℓ teilbar; sie sei etwa $p^\ell \Delta$, wobei $\deg \Delta \leq \deg h$ ist, da $g_\ell f + f_\ell g$ denn gleichen Grad wie h hat.

Wir müssen f^* und g^* so wählen, daß $p^\ell \Delta \equiv p^\ell (g^* f + f^* g) \bmod p^{\ell+1}$ ist; dies ist äquivalent dazu, daß $g^* f + f^* g \equiv \Delta \bmod p$ ist. Wie wir schon beim Fall $\ell = 1$ gesehen haben, können wir diese Gleichung für jede rechte Seite Lösung, und da der Grad von Δ höchstens gleich dem von h ist, erfüllen $f*$ und g^* auch die behaupteten Gradungleichungen. Diese gelten dann auch für $f_{\ell+1} = f_\ell + p^\ell f^*$ und $g_{\ell+1} = g_\ell + p^\ell g^*$, und nach unserer Wahl von f^*, g^* ist auch $g_{\ell+1} f + f_{\ell+1} g \equiv h \bmod p^{\ell+1}$. Somit gilt die Behauptung auch für $\ell + 1$, und das Lemma ist bewiesen. ∎

Damit haben wir zumindest modulo jeder Potenz einer geeigneten Primzahl p auch für $\mathbb{Z}[X]$ das wesentliche Werkzeug zur Anwendung des HENSELschen Lemmas, die lineare Kombinierbarkeit eines gegebenen Polynoms aus zwei modulo p zueinander teilerfremden Polynomen f und g.

Um ein HENSELsches Lemma für Polynome mehrerer Veränderlicher zu bekommen, fehlt uns noch eine Methode, um Faktorisierungen in einer Veränderlichen hochzuheben zu solchen in mehreren.

Von Polynomen in mehreren Veränderlichen kommen wir leicht zu solchen in nur einer Veränderlichen, indem wir allen Variablen mit einer Ausnahme ganzzahlige Werte geben.

Konkret sei $f \in \mathbb{Z}[X_1, \ldots, X_n]$ und $a_2, \ldots, a_n$ seien ganze Zahlen. Dann ist $f(X_1, a_2, \ldots, a_n)$ ein Polynom aus $\mathbb{Z}[X_1]$, und wir nehmen an, daß wir in $\mathbb{Z}[X_1]$ eine Faktorisierung

$$f(X_1, a_2, \ldots, a_n) = g \cdot h \qquad \text{mit} \qquad g, h \in \mathbb{Z}[X_1]$$

kennen. Um in einer Situation wie beim klassischen HENSELschen Lemma zu sein, müssen wir dies irgendwie auffassen als eine Kongruenz im Polynomring $\mathbb{Z}[X_1, \ldots, X_n]$. Dazu erinnern wir uns an einen Begriff aus der Algebra:

Definition: *a)* Eine Teilmenge eines Rings R heißt ein *Ideal* von R, wenn I die Null enthält, zu zwei Elementen $f, g \in I$ auch deren Summe $f + g$ sowie zu einem *beliebigen* $f \in R$ und einem Element $g \in I$ das Produkt $f \cdot g$.
b) Zwei Elemente $f, g \in R$ heißen kongruent modulo dem Ideal I, in Zeichen $f \equiv g \bmod I$, wenn die Differenz $f - g$ in I liegt.

Als Beispiel betrachten wir in $\mathbb{Z}$ zu einem $m \neq 0$ die Menge (m) aller durch m teilbarer Zahlen. Sie ist offensichtlich ein Ideal, denn die Summe zweier durch m teilbarer Zahlen ist wieder durch m teilbar, und das Produkt einer beliebigen ganzen Zahl mit einer durch m teilbaren auch. Zwei ganze Zahlen a, b sind genau dann kongruent im Sinne obiger Definition modulo dem Ideal (m), wenn $a \equiv b \bmod m$ ist.

Im Polynomring $\mathbb{Z}[X_1, \ldots, X_n]$ reichen uns Ideale, die nur aus den Vielfachen eines Elements bestehen nicht.

Definition: R sei ein (kommutativer) Ring und $g_1, \ldots, g_m \in R$. Wir bezeichnen

$$(g_1, \ldots, g_m) = \{f_1 g_1 + \cdots + f_m g_m \mid f_1, \ldots, f_m \in R\}$$

als das von $g_1, \ldots, g_m$ erzeugte Ideal.

Die drei von einem Ideal verlangten Eigenschaften sind offensichtlich erfüllt, denn $0 = 0g_1 + \cdots + 0g_m$ liegt in der Menge, zu zwei gegebenen Elementen ist auch die Summe

$$(f_1 g_1 + \cdots + f_m g_m) + (h_1 g_1 + \cdots + h_m g_m) = (f_1 + h_1) g_1 + \cdots + (f_m + h_m) g_m$$

von der verlangten Form, und für ein beliebiges $f \in R$ gilt dies auch für

$$f(f_1 g_1 + \cdots + f_m g_m) = (f f_1) g_1 + \cdots + (f f_m) g_m \,.$$

Uns interessieren hier vor allem die Ideale der Form

$$I = (X_2 - a_2, \ldots, X_n - a_n) \subset \mathbb{Z}[X_1, \ldots, X_n] \,.$$

Nach Definition bestehen sie allen Polynomen der Form

$$f = (X_2 - a_2)f_2 + \cdots + (X_n - a_n)f_n$$

mit $f_2, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$.

Für jedes solche Polynom ist offensichtlich $f(X_1, a_2, \ldots, a_n)$ das Nullpolynom, und umgekehrt liegt auch jedes Polynom f, für das $f(X_1, a_2, \ldots, a_n)$ das Nullpolynom ist, in I: Üblicherweise schreiben wir Polynome zwar als Linearkombinationen von Monomen der Form $X_1^{e_1} \cdots X_n^{e_n}$, aber wir könnten sie genauso gut schreiben als Linearkombinationen von Produkten der Form

$$X_1^{e_1} \cdot (X_2 - a_2)^{e_2} \cdots (X_n - a_n)^{e_n} .$$

Bei dieser Darstellung ist klar, daß ein Polynom genau dann das Nullpolynom ist, wenn es keine Terme der Form X_1^e enthält, sondern nur solche, die durch mindestens ein $X_j - a_j$ mit $j \geq 2$ teilbar sind. Dies kann man auch so ausdrücken, daß I der Kern der Abbildung

$$\begin{cases} \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1] \\ \qquad\qquad\qquad f \mapsto f(X_1, a_2 \ldots, a_n) \end{cases}$$

ist.

Für uns ist wichtig, daß für jedes Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$ gilt

$$f \equiv f(X_1, a_2, \ldots, a_n)] \bmod I .$$

Wenn wir eine Faktorisierung von $f(X_1, a_2, \ldots, a_n)$ haben, können wir das also auch so ausdrücken, daß wir modulo I eine Faktorisierung haben, und wir können versuchen, diese schrittweise anzuheben zu einer Faktorisierung modulo einer geeigneten Potenz von I. Dazu müssen wir als erstes definieren, was eine Potenz eines Ideals sein soll:

Definition: Für ein Ideal I eines Rings R und eine natürliche Zahl k ist I^k das Ideal, das alle R-Linearkombinationen von Produkten aus k Elementen von I enthält.

Für das Ideal (m) im Ring der ganzen Zahlen ist somit $(m)^k$ einfach das Ideal (m^k).

Für das uns hier interessierende Ideal $I = (X_2 - a_2, \ldots, X_n - a_n)$ ist die Situation etwas komplizierte: I^k wird erzeugt von den Polynomen

$$(X_2 - a_2)^{e_2} \cdots (X_n - a_n)^{e_n} \qquad \text{mit} \qquad e_2 + \cdots + e_n = k\,.$$

Insbesondere sind dies alles Polynome vom Grad k in $X_2, \ldots, X_n$; wenn wir also von einer Faktorisierung modulo I übergehen zu einer modulo I^2, müssen wir nur Polynome hinzufügen, die linear in $X_2, \ldots, X_n$ sind, beim Übergang zu I^3 kommen noch quadratische dazu, und so weiter.

Da wir so etwas wie den erweiterten EUKLIDischen Algorithmus, wie wir gerade gesehen haben, nicht in $\mathbb{Z}[X]$, sondern nur in $\mathbb{Z}[X]$ modulo einer geeigneten Primzahlpotenz haben, können wir alle Konstruktionen nur modulo einer Primzahlpotenz durchführen, d.h wir rechnen nicht nur modulo der Ideale I^k, sondern modulo der etwas größeren Ideale (p^ℓ, I^k), die zusätzlich noch p^ℓ als Erzeugendes enthalten, so daß alle Koeffizienten nur modulo p^ℓ betrachtet werden.

Lemma: $f \in \mathbb{Z}[X_1, \ldots, X_n]$ sei ein Polynom in n Veränderlichen, $a_2, \ldots, a_n$ seien ganze Zahlen, p^ℓ eine Primzahlpotenz, und g, h seien zwei modulo p teilerfremde Polynome aus $\mathbb{Z}[X_1]$, deren führende Koeffizienten nichts durch p teilbar sind. Außerdem sei

$$f(X_1, a_2, \ldots, a_n) \equiv g(X_1) \cdot h(X_1) \bmod p^\ell\,.$$

Dann gibt es zu jedem $k \in \mathbb{N}$ Polynome $g_k, h_k \in \mathbb{Z}[X_1, \ldots, X_n]$ mit der Eigenschaft, daß

$$f(X_1, \ldots, X_n) \equiv g_k(X_1, \ldots, X_n) \cdot h_k(X_1, \ldots, X_n) \bmod (p^\ell, I^k)\,.$$

Außerdem ist

$$g_\ell(X_1, a_2, \ldots, a_n) = g(X_1) \qquad \text{und} \qquad h_\ell(X_1, a_2, \ldots, a_n) = h(X_1)\,.$$

Beweis durch vollständige Induktion nach k: Für $k = 1$ setzen wir einfach $g_1 = g$ und $h_1 = h$; da $\mathbb{Z}[X_1]$ ein Teilring von $\mathbb{Z}[X_1, \ldots, X_n]$ ist, liegen sie auch in diesem Polynomring, und die Voraussetzung ist äquivalent zu $f \equiv gh \bmod (p^\ell, I)$.

Für den Induktionsschritt nehmen wir an, daß wir Polynome g_k, h_k aus $\mathbb{Z}[X_1, \ldots, X_n]$ kennen, für die

$$f \equiv g_k h_k \bmod (p^\ell, I^k)$$

ist. Dann liegt $f - g_k h_k$ in (p^ℓ, I^k). Da uns dieses Polynom nur modulo I^{k+1} interessiert, setzen wir $\Delta = (f - g_k h_k) \bmod I^{k+1}$.

$f - g_k h_k$ ist als Element von I^k eine Linearkombination von Polynomen $(X_2 - a_2)^{d_2} \ldots (X_n - a_n)^{d_n}$ mit $d_2 + \cdots + d_n = k$. Die Koeffizienten sind dabei Elemente des Polynomrings $\mathbb{Z}[X_1, \ldots, X_n]$.

Jedes Polynom in $X_1, X_2, \ldots, X_n$ läßt sich auch schreiben als Polynom in $X_1, X_2 - a_2, \ldots, X_n - a_n$; tun wir dies, können wir jeden Summanden $q(X_2 - a_2)^{d_2} \ldots (X_n - a_n)^{d_n}$ mit $q \in \mathbb{Z}[X_1, \ldots, X_n]$ auch schreiben als Summe von Termen

$$c(X_2 - a_2)^{e_1} \cdots (X_n - a_n)^{e_n} \qquad \text{mit} \qquad c \in \mathbb{Z}[X_1]\,,$$

wobei jetzt die Summe der e_i größer oder gleich k sein kann.

Falls die Summe größer als k ist, liegt der Summand in I^{k+1}, fällt also weg, wenn wir $\Delta = (f - g_k h_k) \bmod I^{k+1}$ bilden. Daher ist Δ eine Linearkombination der Form

$$\Delta = \sum_{i=1}^{r} c_i M_i \qquad \text{mit} \qquad c_i \in \mathbb{Z}[X_1]\,,$$

wobei jedes M_i ein Produkt der Form $(X_2 - a_2)^{e_2} \cdots (X_n - a_n)^{e_n}$ mit $e_2 + \cdots + e_n = k$ ist.

Wegen der Voraussetzungen an $g \bmod p$ und $f \bmod p$ können wir das vorige Lemma anwenden und finden für jeden Koeffizienten c_i Polynome $g_i', h_i' \in \mathbb{Z}[X_1]$, für die gilt

$$g_i' h + h_i' g \equiv c_i \bmod p^\ell$$

mit $\deg g_i' < \deg g$ und $\deg h_i' < \deg h$. Setzen wir

$$g_{k+1} = g_k + \sum_{i=1}^{r} g_i' M_i \qquad \text{und} \qquad h_{k+1} = h_k + \sum_{i=1}^{r} h_i' M_i\,,$$

ändert sich daher nichts an den Graden.

Beim Ausmultiplizieren der beiden Summe können wir alle Summanden aus I^{k+1} weglassen. Nach Induktionsannahme ist $g_k \equiv g \bmod I$ und $h_k \equiv h \bmod I$; da die M_i in I^k liegen, ist also $g_k M_i \equiv g M_i \bmod I^{k+1}$ und $h_k M_i \equiv h M_i \bmod I^{k+1}$ für alle i. Somit ist

$$\begin{aligned} g_{k+1}h_{k+1} &\equiv g_k h_k + g_k \sum_{i=1}^{r} h_i' M_i + h_k \sum_{i=1}^{r} g_i' M_i \bmod (p^\ell, I^{k+1}) \\ &\equiv g_k h_k + g \sum_{i=1}^{r} h_i' M_i + h \sum_{i=1}^{r} g_i' M_i \bmod (p^\ell, I^{k+1}) \\ &\equiv g_k h_k + \sum_{i=1}^{r} (h_i' g + g_i' h) M_i \bmod (p^\ell, I^{k+1}) \\ &\equiv g_k h_k + \sum_{i=1}^{r} c_i M_i = g_k h_k + \Delta \equiv f \bmod (p^\ell, I^{k+1}) \,. \end{aligned}$$

Damit ist das Lemma bewiesen. ∎