§15 Praktische Primzerlegung in $\mathbb{Q}[x]$.

Vorbemerkungen zur Aufgabenstellung in der Vorlesung.

Neuere Verfahren der Computeralgebra zur Primzerlegung von Polynomen mit rationalen Koeffizienten gehen wie folgt vor:

(1) Es genügt Primzerlegungen für Polynome aus $\mathbb{Z}[x]\backslash\mathbb{Z}$ zu bestimmen.

Um dies einzusehen, muss man wissen:

- was Primzerlegung in $\mathbb{Z}[x]$ bedeutet ($\mathbb{Z}[x]$ ist kein Hauptidealring und um so weniger euklidisch),
- Lemma von Gauß, mit dessen Hilfe man u. A. zeigen kann: Ist

$$f = u_1 \cdots u_r \cdot q$$

  die eindeutige normierte Primzerlegung des Polynoms $f \in \mathbb{Z}[x]\backslash\mathbb{Z}$ in $\mathbb{Q}[x]$ mit Primpolynomen $u_1, \ldots, u_r \in \mathbb{Q}[x]$, $HK(u_1) = \cdots = HK(u_r) = 1$ und $q \in \mathbb{Q}\backslash\{0\}$, dann gibt es ganze Zahlen $z_1, \ldots, z_r, z_0$, derart, dass: $z_1u_1, \ldots, z_ru_r$ Primpolynome in $\mathbb{Z}[x]$ sind und

$$f = (z_1u_1) \cdots (z_ru_r) \cdot z_0.$$

(2) Es genügt Primzerlegungen für Polynome aus $\mathbb{Z}[x]\backslash\mathbb{Z}$ zu bestimmen, deren höchster Koeffizient 1 ist. [1]

Dies kann man so einsehen: Sei a der höchste Koeffizient von $f \in \mathbb{Z}[x]\backslash\mathbb{Z}$ und n der Grad von f, dann ist

$$\tilde{f} := a^{n-1} f\left(\frac{x}{a}\right) \in \mathbb{Z}[x]\backslash\mathbb{Z} \text{ und } HK(\tilde{f}) = 1$$

Man muss sich nun allerdings noch klarmachen, wie eine Primzerlegung von $\tilde{f}$ zu einer von f führt. Sei etwa $\tilde{f} = z \cdot v_1 \cdots v_r$ eine Primzerlegung von $\tilde{f}$ mit $z \in \mathbb{Z}$ und Primpolynom $v_1, \ldots, v_r \in \mathbb{Z}[x]$, dann ist

$$f(x) = \frac{1}{a^{n-1}} \tilde{f}(ax) = \frac{z}{a^{n-1}} v_1(ax) \cdots v_r(ax).$$

Mit Hilfe des Lemmas von Gauß erkennt man, dass der Nenner a^{n-1} so auf die Faktoren verteilt werden kann, dass alles ganzzahlig wird.

.....

[1] Dieser Schritt ist nicht zwingend, wird nicht bei allen Verfahren benutzt, vereinfacht das Folgende ein wenig.

(3) Es genügt, Pimzerlegungen für quadratfreie Polynome aus $\mathbb{Z}[x]\backslash\mathbb{Z}$ zu bestimmen.

Dies liegt daran, dass mit Hilfe des euklidischen Algorithmus in $\mathbb{Q}[x]$ zu einem $f \in \mathbb{Z}[x]\backslash\mathbb{Z}$ das Polynom $ggT(f, \frac{df}{dx})$ rasch berechnet werden kann. Es gibt dann eine ebenfalls leicht zu bestimmende Zahl $z \in \mathbb{Z}\backslash\{0\}$ derart, dass

$$g := z \cdot ggT(f, \frac{df}{dx}) \text{ ganzzahlig ist und } f \text{ teilt!}$$

$f_1 := \frac{f}{g}$ ist quadratfrei.
Hat man erst einmal eine Primzerlegung für f_1 gefunden so ergibt sich die von f z. B. durch Probedivisionen von $\frac{f}{f_1}$ durch die Primteiler von f_1, denn andere Primteiler kann f dann nicht mehr haben.
(1), (2) und (3) rechtfertigen die Beschränkung auf **quadratfreie ganzzahlige nicht konstante Polynome mit höchstem Koeffizienten 1.**

Jetzt geht es um die **Beschreibung und Begründung des "modularen" Teils aktueller Faktorisierungsverfahren.**
Im Folgenden ist es zweckmäßig, die symmetrische Division mit Rest zu benutzen. Für $d \geq 2$ sei

$$\sigma_d : \mathbb{Z} \to \mathbb{Z}_{d,0} := (\tfrac{d}{2}, \ldots, \tfrac{d}{2}] \cap \mathbb{Z}$$

Dabei ist $\sigma_d(z)$ der eindeutig bestimmte Rest in $\mathbb{Z}_{d,0}$ bei Division mit d. Genau wie $\mathbb{Z}_d$ wird auch $\mathbb{Z}_{d,0}$ zu einem Ring gemacht und natürlich gilt $\mathbb{Z}_d \cong \mathbb{Z}_{d,0}$. Die Multiplikation in $\mathbb{Z}_{d,0}$ bezeichnen wir wie in $\mathbb{Z}_d$ mit $\odot$.
Auf Polynome in $\mathbb{Z}[x]$ wenden wir σ_d wie folgt an:

$$\sigma_d(a_n x^n + \cdots + a_1 x + a_0) = \sigma(a_n)x^n + \cdots + \sigma(a_1)x + \sigma(a_0)$$

Dadurch entsteht ein Ringmorphismus (den wir auch mit σ_d bezeichnen)

$$\sigma_d : \mathbb{Z}[x] \to \mathbb{Z}_{d,0}[x]\,,$$

der eine Fortsetzung von σ_d auf $\mathbb{Z}[x]$ ist. Bei der gewählten Schreibweise ist $\mathbb{Z}_{d,0}[x]$ Teilmenge von $\mathbb{Z}[x]$ und offensichtlich gilt $\sigma_d[x] = x$. Auch die Multiplikation in $\mathbb{Z}_{d,0}[x]$ werde mit $\odot$ bezeichnet.

(4) Jede nicht triviale Produktzerlegung eines ganzzahligen Polynoms mit höchstem Koeffizienten 1 bleibt modular erhalten.

Genauer: Sei $f \in \mathbb{Z}[x]\backslash\mathbb{Z}$ mit höchstem Koeffizienten 1 und gelte $f = u_1 \cdots u_r$ mit $u_1, \ldots, u_r \in \mathbb{Z}[x]\backslash\mathbb{Z}$. Zwangsläufig ist dann $HK(u_1) = \cdots = HK(u_r) = \pm 1$.
Modulo $d, d \geq 2$, erhält man dann eine Zerlegung

$$\sigma_d(f) = \sigma_d(u_1) \odot \cdots \odot \sigma_d(u_r)$$

mit den Eigenschaften:

$$\deg \sigma_d(f) = \deg f,\ \deg \sigma_d(u_1) = \deg u_1,\ \ldots, deg\sigma_d(u_r) = \deg u_r$$

und $HK(\sigma_d(u_i)) = \pm 1$ für $1 \leq i \leq r$.
Eine Primzerlegung von f erscheint demnach zumindest als echte Zerlegung von $\sigma_d(f)$ in $\mathbb{Z}_{d,0}[x]$ für **alle** $d \geq 2$. **Unter den echten Zerlegungen von $\boldsymbol{\sigma_d(f)}$ in ein Produkt muss also stets eine Zerlegung sein, die von einer Zerlegung von $\boldsymbol{f}$ herkommt. Andererseits brauchen nicht alle Zerlegungen von $\boldsymbol{\sigma_d(f)}$ in $\boldsymbol{\mathbb{Z}_{d,0}[x]}$ von einer Zerlegung von $\boldsymbol{f}$ herzustammen.** Ein krasses Beispiel in diesem Zusammenhang sind die **Swinnerton-Dyer-Polynome** (siehe [GaGe] p.415). Diese sind unzerlegbar und ihre Grade sind nicht beschränkt. Sie zerfallen aber in höchstens quadratische Faktoren in $\mathbb{Z}_p[x]$ für jede Primzahl p !
Wenn $d = p$ eine Primzahl ist, dann existiert für $\sigma_d(f)$ in $\mathbb{Z}_{p,0}[x]$ eine eindeutige Primzerlegung, ebenso wie für **die $\boldsymbol{\sigma_p(u_i)}$, die leider modulo $\boldsymbol{p}$ zerlegbar werden können.** Am übersichtlichsten wird dies, wenn $\sigma_p(f)$ ebenfalls quadratfrei ist in $\mathbb{Z}_{p,0}[x]$ (siehe **(5)**). Dann ist $\sigma_p(f)$ ein Produkt paarweise verschiedener Primteiler von $\sigma_p(f)$. Wenn man die Primzerlegung eines quadratfreien $\sigma_p(f)$ in $\mathbb{Z}_{p,0}[x]$ kennt (siehe **(6)**) , gibt es also eine eindeutige bestimmte Partition der Menge der Primteiler von $\sigma_p(f)$, die der Primzerlegung von f entspricht. Die große Frage allerdings bleibt: Welches ist die richtige Partition? Und: Wie findet man die entsprechenden Teiler von f ? Dazu mehr in **(6)**, **(7)** und **(8)**.

(5) Suche nach Primzahlen p mit quadratfreiem $\sigma_p(f)$

Zu gegebenen $f \in \mathbb{Z}[x] \backslash \mathbb{Z}$ mit höchstem Koeffizienten 1 gibt es stets nur endlich viele Primzahlen p, derart, dass $\sigma_p(f)$ nicht quadratfrei ist in $\mathbb{Z}_p[x]$. Dies kann man z. B. mit Hilfe der sogenannten Resultante von f und f' beweisen.

(6) Berechnung einer Primzerlegung von $\sigma_p(f)$ in $\mathbb{Z}_p[x]$, p prim.

Dazu kann man z.B. das in §14 behandelte **Berlekamp'sche Verfahren** benutzen. Andere (z.B. auch probabilistische) Verfahren und Vergleiche sind recht gründlich in dem Buch [GaGe][(2)] Ch. 14 beschrieben.

(7) Wie findet man einen Faktor von f, wenn man die Primzerlegung von $\sigma_p(f)$ kennt ?

Kennt man die Primzerlegung, so kennt man alle Teiler von $\sigma_p(f)$. Ist v ein Teiler von $\sigma_p(f)$ in $\mathbb{Z}_{p,0}[x]$, dann können alle Polynome aus

$$v + p\mathbb{Z}[x]$$

vom Grad $< \deg f$ **vielleicht** ein Teiler von f sein und man müsste alle "ausprobieren".

.....

[(2)] Siehe Literaturangaben am Ende dieses Textes.

Auswege:

(A) $\boldsymbol{p}$ so **groß** wählen, dass die Koeffizienten möglicher Teiler von f betragsmäßig kleiner $\frac{p}{2}$ sind (siehe **(8)**) . Dann kommt nur noch v selbst in Frage und eine einfache Division mit Rest führt zur Entscheidung. Nachteil: man muss Faktoren in $\mathbb{Z}_{p,0}[x]$ mit großem p bestimmen, was aufwendig sein kann.

(B) Hensel-Lift: Zu einem Teiler v von $\sigma_p(f)$ in $\mathbb{Z}_{p,0}[x]$ berechnet man nacheinander mit einem **Hensel'schen Lemma** (siehe z.B. [GaGe] Ch. 15) zuerst einen Teiler v_1 von $\sigma_{p^2}(f)$ mit $\sigma_p(v_1) = v$, dann einen Teiler v_2 von $\sigma_{p^4}(f)$ mit $\sigma_{p^2}(v_2) = v_1$, ... , einen Teiler v_k von $\sigma_{p^{2^k}}(f)$ mit $\sigma_{p^{2^k}}(v_k) = v_{k-1}$ solange, bis $p^{2^k} > 2 \cdot M$ **mit einer reellen Zahl $\boldsymbol{M}$, die größer ist als das Maximum der Koeffizientenbeträge potentieller Teiler von $\boldsymbol{f}$** (siehe **(8)**). Die Polynome $v_1, \ldots, v_k$ sind beim Hensel-Lifting jeweils eindeutig bestimmt. v_k kommt als Teiler von f in Frage. Division mit Rest führt zur Entscheidung. Da jeder echte Teiler von f zu einem echten Teiler von $\sigma_p(f)$ führt und da der "Lifting"-Prozess in jeder Stufe eindeutig ist, muss man auf alle Teiler von f stoßen, wenn man für v alle Teiler von $\sigma_p(f)$ zulässt. Man braucht dabei nicht alle Teiler zu testen, wie man sich leicht überlegt.
Trotzdem liegt hier ein Schwachpunkt des Verfahrens, wenn es um die Faktorzerlegung von Polynomen hohen Grades geht, die zudem viele Primteiler besitzen: eine Menge von m Primteilern modulo p hat 2^m Teilmengen. Es gibt allerdings eine **Alternative zum Hensel-Lift** mit asymptotisch 'polynomialer' Komplexität: das sogenannte **$\boldsymbol{L^3}$-Verfahren**, so benannt nach den drei AutorInnen Lenstra, Lenstra und Lovacz, siehe [GaGe] Ch. 16. Bei diesem Verfahren genügt es, einzelne Primfaktoren von $\sigma_p(f)$ zu liften nach $\mathbb{Z}_{p^{2^k},0}[x]$. Danach wird mit Hilfe von Zahlengittern entschieden ob 'darüber' ein echter Primfaktor von f liegt oder nicht.

(C) Der **chinesische Restsatz** ist bei der Aufgabe 'Zerlegung eines Polynoms in Primfaktoren' weniger geeignet, da man dann ja für mehrere Primzahlen $p_1, \ldots, p_n$ jeweils eine Primzerlegung in $\mathbb{Z}_{p_i}[x],\ 1 \leq i \leq n$ berechnen müsste (was man aber parallel erledigen könnte) und dann noch für eine große Anzahl von Teilerkombinationen entscheiden müsste, ob sie von einem Teiler von f stammen.

(8) Eine reelle Zahl (Schranke) $\boldsymbol{M}$, die größer ist als das Maximum der Koeffizientenbeträge potentieller Teiler von $\boldsymbol{f}$ lässt sich formelmäßig aus den Koeffizienten des zu zerlegenden Polynoms f berechnen. Am bekanntesten ist eine Schranke von Mignotte, siehe ebenfalls in [GaGe] Ch. 6, p. 164.

Ausblick und allgemeinere Aufgabenstellung in der Vorlesung.

[GaGe] J. von zurGathen, J. Gerhard:
Modern Computeralgebra, Cambridge University Press, 2. Auflage 2003
(1. Auflage von 1999 in meinem Handapparat und in der HA und Lehrbuchsammlung)