Faktorisierung von Polynomen über algebraischen Zahlkörpern

Hauke Rennies

29. Juni 2011

1 Einleitung

Die vorliegende Ausarbeitung ist Teil des Moduls *Computeralgebra und Gröbnerbasen*. Es wird ein Verfahren zur Faktorisierung von Polynomen über algebraischen Zahlkörpern vorgstellt. Es handelt sich um einen Algorithmus von *Trager*.
Grundlegende Vorkenntnisse hierfür sind algebraische Körpererweiterungen von $\mathbb{Q}$ und damit verbunden die Normfunktion in algebraischen Zahlkörpern. Die hier relevanten Ergebnisse aus diesem Bereich werden zunächst kurz wiederholt, jedoch werden Beweise an dieser Stelle weggelassen und können gegebenenfalls in entsprechender Literatur nachgelesen werden.
Im den letzten beiden Abschnitten werden eine Methode für die Faktorisierung von Polynomen mit quadratfreier Norm und schließlich der Algorithmus von Trager vorgestellt. Abgeschlossen wird diese Arbeit mit einem kurzen Beispiel um die Vorgehensweise zu verdeutlichen.
Die wesentliche Idee ist hierbei, zu einem quadratfreien Polynom f über einem algebraischen Zahlkörper die Norm von f über $\mathbb{Q}[x]$ zu faktorisieren um dadurch Faktoren von f selbst zu finden.
Inhaltlich gliedert sich dieses Thema also als Fortsetzung der Theorie über Polynomfaktorisierung in $\mathbb{Q}[x]$ in die Vorlesung ein. Die dort vorgestellten Verfahren[1] finden hier insofern Anwendung, dass sie zur Faktorisierung der Norm des betrachteten Polynoms genutzt werden können. Diese ist ein Teil des Algorithmus

[1] Zum Beispiel Berlekamp-Verfahren, Algorithmus von Cantor-Zassenhaus, Gitterverfahren wie LLL

von Trager.
Die hier vorgestellten Ergebnis beruhen im Wesentlichen auf den Quellen

(GCL) *Algorithms for Computeralgebra*; Geddes, Czapor, Labahn; Kluwer Academic Publishers; Boston; 1992

(CoCuSt) *Some Tapas of Computer Algebra*; Cohen, Cuypers, Sterk; Springer; 1999.

An einigen Stellen werden dabei Argumente ausführlicher als in der angegebenen Literatur oder leicht abgewandelt dargestellt.

2 Grundlagen und Notation

Im Folgenden wird der Körper $\mathbb{Q}$ der rationalen Zahlen als Grundkörper betrachtet. K sei eine Körpererweiterung von $\mathbb{Q}$.

Definition 2.1. *Ein Körper K heißt* ***algebraischer Zahlkörper****, falls $K \supseteq \mathbb{Q}$ eine endliche algebraische Körpererweiterung ist.*
$n := [K : \mathbb{Q}]$ heißt ***Grad*** *der Körpererweiterung.*
$f \in \mathbb{Q}[t] \setminus \{0\}$ heißt ***Minimalpolynom*** *von $\alpha \in K$, falls gilt:*

a) $f(\alpha) = 0$

b) *f ist normiert und irreduzibel über $\mathbb{Q}$*

Das Minimalpolynom wird im Folgenden mit $m_{\alpha,\mathbb{Q}}$ oder falls der Zusammenhang klar ist, einfach mit m bezeichnet.

Da $\mathbb{Q}$ ein Körper der Charakteristik 0 ist, ist jede algebraische Erweiterung von $\mathbb{Q}$ separabel. Daher existiert ein primitives Element $\alpha \in K$ der Körpererweiterung, das heißt, es gilt $K = \mathbb{Q}(\alpha)$. Es ist bekannt, dass dann K ein $\mathbb{Q}$-Vektorraum der Dimension n und $\{1, \alpha, \cdots, \alpha^{n-1}\}$ eine Basis von K über $\mathbb{Q}$ ist. Für jedes $\beta \in K$ existiert also eine Darstellung

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} =: b(\alpha),$$

das heißt eine Darstellung durch ein Polynom $b \in \mathbb{Q}[t]$ vom Grad kleiner oder gleich $n-1$ ausgewertet an der Stelle α.

Bemerkung. *In der obigen Situation gilt*

$$\mathbb{Q}[t] / (m(t)) \cong \mathbb{Q}(\alpha).$$

Seien nun $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von $\mathbb{Q}$ in $\mathbb{C}$ mit $\sigma_i|_{\mathbb{Q}} = \mathrm{id}\,|_{\mathbb{Q}}$. Zu $x \in K$ heißen $\sigma_1(x), \ldots, \sigma_n(x)$ die **Konjugierten** von x. Abkürzend wird $\alpha_i := \sigma_i(\alpha)$ für $i = 1, \ldots, n$ gesetzt.
Durch die Konjugierten von α sind alle Nullstellen von dem Minimalpolynom m gegeben. Die Konjugierten von $\beta \in \mathbb{Q}$ sind gegeben durch

$$\beta_i = b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1} = b(\alpha_i).$$

Wie in der Einleitung beschrieben, benötigt man für den hier vorgestellten Algorithmus die in algebraischen Zahlkörpern definierte Norm.

Definition 2.2. *Die Norm eines Elements $\beta \in K$ ist gegeben als*

$$N(\beta) := \prod_{i=1}^{n} \sigma_i(\beta) = \prod_{i=1}^{n} \beta_i \tag{1}$$

oder alternativ über die Resultante

$$N(\beta) = \mathrm{res}_t(b, m) = \prod_{\gamma \text{ Nullstelle von } m} b(\gamma).^{2} \tag{2}$$

Zu beachten ist, dass die Polynome b und m Koeffizienten in $\mathbb{Q}$ haben und damit die Resultante bezüglich t ebenfalls in $\mathbb{Q}$ liegt.

Bemerkung. *Beide Definitionen für die Norm sind äquivalent und es gilt:*

a) $N(\beta) \in \mathbb{Q}$ *für alle* $\beta \in K$

b) $N(\beta) = N(\beta_i)$ *für alle* $i = 1, \ldots, n$ *und alle* $\beta \in K$

c) $N(\beta\gamma) = N(\beta)N(\gamma)$ *für alle* $\beta, \gamma \in K$

Beweis. Die Aussagen a) und c) sind klar bzw. aus der algebraischen Zahlentheorie bekannt, Teil b) folgt sofort aus der Definition der Norm als Produkt der Konjugierten. Die erste Aussage ergibt sich daher mit

$$\begin{aligned} N(\beta) = \mathrm{res}_t(b(x), m(x)) &= \prod_{x:m(x)=0} b(x) \\ &= \prod_{i=1}^{n} b(\alpha_i) = \prod_{i=1}^{n} \beta_i = \prod_{i=1}^{n} \sigma_i(\beta) \end{aligned}$$

[2] Diese Darstellung der Resultante wurde bereits in der Ausarbeitung von Stefan Hellbusch über Swinnerton-Dyer-Polynome hergeleitet.

□

Die Normfunktion kann nun auf den Polynomring $K[x]$ fortgesetzt werden, indem die Norm auf die Koeffizienten der Polynome angewendet wird, d.h. für $f = \sum_{j=0}^{m} a_j x^j \in K[x]$ gilt

$$N(f) := \prod_{i=1}^{n} \sigma_j \left(\sum_{j=1}^{m} a_j x^j \right) = \prod_{i=1}^{n} \sum_{j=1}^{m} \sigma_j(a_j) x^j. \tag{3}$$

Diese Definition führt dazu, dass ein Polynom f seine Norm teilt (für ein i ist σ_i die Identität). Man kann wie oben erläutert die Koeffizienten von f als Polynome vom Grad kleiner oder gleich $n-1$ über $\mathbb{Q}$ auffassen, das heißt es ist möglich, f als Polynom aus $\mathbb{Q}[t,x]$ zu interpretiern. Definiert man nun wie oben die Norm über die Resultante als $N(f) = \mathrm{res}_t(f(t,x),m)$, so erhält man sofort, dass $N(f)$ ein Polynom in $\mathbb{Q}[t]$ ist.[3] Die Norm eines Polynoms $g \in \mathbb{Q}[t]$ ist demnach g^n, da $\sigma_i|_{\mathbb{Q}} = \mathrm{id}\,|_{\mathbb{Q}}$.

3 Fakorisierung von Polynomen mit quadratfreier Norm

Wie in der Einleitung beschrieben, soll für die Faktorisierung von Polynomen über algebraischen Zahlkörpern ein direkter Zusammenhang zwischen Faktoren der Polynome selbst und Faktoren der Norm hergestellt werden. Ein erstes wichtiges Resultat in diesem Zusammenhang liefert der erste Satz dieser Ausarbeitung.

Satz 3.1. *Sei $f \in K[x]$ irreduzibel. Dann ist $N(f)$ eine Potenz eines in $\mathbb{Q}[x]$ irreduziblen Polynoms.*

Beweis. Angenommen, es existieren teilerfremde Polynome a und b aus $\mathbb{Q}[x]$, so dass $N(f) = ab$. Wie oben erläutert gilt in $K[x]$

$$f | N(f) = ab$$

und da f irreduzibel (d.h. insbesondere prim) damit $f|a$ oder $f|b$. Sei nun ohne Einschränkung f ein Teiler von b. Dann existiert ein Polynom $c \in K[x]$, so dass

[3] Siehe hierzu: Ausarbeitung von Stefan Hellbusch zu Swinnerton-Dyer-Polynomen: Die Resultante liegt immer in dem zu Grunde liegenden Ring, dies ist hier $\mathbb{Q}[t]$.

$b = fc$. Anwenden der Einbettung σ_i auf diese Gleichung ergibt

$$b = \sigma_i(f)\sigma_i(c),$$

da b ein Polynom über $\mathbb{Q}$ ist. Insbesondere ist für alle $i = 1, \ldots, n$ durch $\sigma_i(f)$ ein Teiler von b gegeben. Also gilt auch

$$N(f) = \prod_{i=1}^{n} \sigma_i(f) \mid b \mid N(f).$$

Es folgt $b = N(f)$ und $a = 1$. An dieser Stelle folgt schon, dass b bzw. $N(f)$ irreduzibel oder eine Potenz eines irreduziblen Polynoms ist.[4] □

Folgerung. *Sei $f \in K[x]$, so dass $N(f)$ quadratfrei in $\mathbb{Q}[x]$ ist. Dann ist f genau dann irreduzibel, wenn $N(f)$ irreduzibel ist.*

Beweisidee. Sei $f \in K[x]$ irreduzibel. Dann ist nach Satz 3.1 $N(f) = b^k$ für ein irreduzibles Polynom $b \in \mathbb{Q}[x]$. Da $N(f)$ quadratfrei ist, folgt $k = 1$.
Sei nun $N(f)$ irreduzibel in $\mathbb{Q}[x]$. Angenommen $f = gh$ mit $g, h \in K[x]$. Dann gilt $N(f) = N(gh) = N(g)N(h)$. Da $N(f)$ irreduzibel ist, muss nun o.E. $N(g)$ eine Einheit in $\mathbb{Q}[x]$ sein. Eigenschaften der Normfunktion liefern nun, dass g schon eine Einheit in $K[x]$ ist. □

Diese letzte Aussage lässt sich verallgemeinern und man erhält die folgende Bemerkung.

Bemerkung. *Sei $f \in K[x]$ zerlegt in irreduzible Faktoren $f_1, \ldots, f_k \in K[x]$, d.h.*

$$f = f_1 \cdots f_k.$$

Sei außerdem wieder $N(f)$ quadratfrei. Dann ist

$$N(f) = N(f_1) \cdots N(f_k)$$

eine irreduzible Zerlegung von $N(f)$ in $\mathbb{Q}[x]$.

Für die Faktorisierung eines Polynoms $f \in K[x]$ interessanter ist jedoch die Umkehrung der obigen Bemerkung.

[4] Angenommen, b erfülle in $N(f) = ab$ diese Eigenschaft nicht, so kann das obige Verfahren erneut auf eine Zerlegung von b in teilerfremde Faktoren angewendet werden.

Satz 3.2. *Sei $f \in K[x]$ mit $N(f)$ quadratfrei. Seien $p_1, \ldots, p_k$ die sämtlichen paarweise verschiedenen irreduziblen Faktoren von $N(f)$ aus $\mathbb{Q}[x]$. Dann ist*

$$f = \prod_{i=1}^{k} \mathrm{ggT}_{K[x]}(f, p_i) \tag{4}$$

eine vollständige Faktorisierung von f in irreduzible Faktoren über $K[x]$.

Beweis. Seien $f_1, \ldots, f_k$ die irreduziblen Faktoren von f. Dann sind die irreduziblen Faktoren von $N(f)$ gerade $N(f_1), \ldots, N(f_k)$, das heißt, es gilt $N(f_j) = p_i$ für passende i, j. Die Voraussetzung, dass $N(f)$ quadratfrei ist, führt dazu, dass für $j \neq l$ auch $N(f_j) \neq N(f_l)$ ist.
Es ist nun zu zeigen, dass

$$f_j = \mathrm{ggT}_{K[x]}(f, p_i).$$

Nach Wahl von f_j ist f_j ein Teiler von f und per Definition der Norm gilt $f_j | N(f_j) = p_i$.
Angenommen, es existiert ein größerer gemeinsamer Teiler g von f und p_i. Dann enthält g zusätzlich zu f_j einen Faktor f_l für ein $l \in \{1, \ldots, k\} \setminus \{j\}$. Insbesondere ist f_l ein Teiler von f und p_i
Die Multiplikativität der Norm führt dazu, dass

$$N(f_l) | N(p_i).$$

Außerdem ist $N(p_i) = p_i^n$, da $p_i \in \mathbb{Q}[x]$ (folgt aus der Definition der Norm über die Konjugierten). $N(f_l)$ ist irreduzibel, da f_l irreduzibel und $N(f)$ quadratfrei ist. Daher gilt schon

$$N(f_l) = p_i.$$

Hier folgt $f_l = f_j$, was ein Widerspruch zu $l \neq j$ ist.
Es folgt die Behauptung. □

Als Zwischenergebnis kann also festgehalten werden, dass eine Faktorisierung von f auf natürliche Weise eine Faktorisierung von $N(f)$ liefert. Andererseits kann man nach Satz 3.2 eine Faktorisierung des Polynoms f gewinnen, wenn eine *quadratfreie* Faktorisierung der zugehörigen Norm $N(f)$ vorliegt.

4 Faktorisierung von Polynomen mit nicht quadratfreier Norm

Die Idee für diesen Abschnitt ist es, durch Variablentransformation ein Polynom $f \in K[x]$ so anzupassen, dass die sich ergebende Norm quadratfrei wird. Dann können auf dieses Polynom die Resultate aus dem vorherigen Abschnitt angewendet werden.

Bemerkung. *Sei $f \in K[x]$. Setze $g(x) := f(x + s\alpha)$, wobei $s \in \mathbb{Q}$ und α das primitive Element der Körpererweiterung ist. Ist*

$$g = g_1 \cdots g_k$$

eine Faktorisierung von g und $f_i := g_i(x - s\alpha)$ für $i = 1, \ldots, k$, dann gilt

$$f = f_1 \cdots f_k.$$

Beweis. Es gilt zunächst $g(x - s\alpha) = f((x - s\alpha) + s\alpha) = f(x)$ und damit

$$\prod_{i=1}^{n} f_i(x) = \prod_{i=1}^{n} g_i(x - s\alpha) = g(x - s\alpha) = f(x).$$

Damit ist die Behauptung bereits gezeigt. □

Der folgende Satz begründet, dass die oben angegebene Transformation die richtige ist.

Satz 4.1. *Sei $f \in K[x]$ quadratfrei. Dann ist $N(f(x - s\alpha))$ für alle bis auf endlich viele $s \in \mathbb{Q}$ quadratfrei.*

Beweis. Sei $\sigma_i(f) = \prod_{j=1}^{r} (x - \beta_{i,j})$ in Linearfaktoren zerlegt mit $\beta_{i,j} \in \mathbb{C}$. Es gilt $\beta_{i,j} \neq \beta_{i,k}$ für $j \neq k$, da f und damit auch $\sigma_i(f)$ quadratfrei ist. Es gilt

$$\sigma_i(f(x - s\alpha)) = \sigma_i(f)(x - s\alpha_i),$$

denn: Ist $f(x) = \sum_{j=1}^{r} \tau_j x^j$ mit $\tau_j \in K$, so ist $\sigma_i(f(x)) = \sum_{j=1}^{r} \sigma_i(\tau_j) x^j$. Damit

ergibt sich

$$\begin{aligned}\sigma_i(f(x-s\alpha)) &= \sigma_i(\sum_{j=1}^{r}\tau_j(x-s\alpha)^j)\\ &= \sum_{j=1}^{r}\sigma_i(\tau_j)(x-s\sigma_i(\alpha))^j\\ &= \sigma_i(f)(x-s\alpha_i).\end{aligned}$$

Es folgt

$$\sigma_i(f(x-s\alpha)) = \sigma_i(f)(x-s\alpha_i) = \prod_{j=1}^{r}(x-s\alpha_i-\beta_{i,j}).$$

Bildet man nun das Produkt über $i = 1, \ldots, n$, so erhält man

$$N(f(x-s\alpha)) = \prod_{i=1}^{n}\sigma_i(f(x-s\alpha)) = \prod_{i=1}^{n}\prod_{j=1}^{r}(x-s\alpha_i-\beta_{i,j}).$$

Die Nullstellen von $N(f(x-s\alpha))$ sind damit gerade $(s\alpha_i+\beta_{i,j})$. Es gelten nun die Äquivalenzbeziehungen

$$\begin{aligned}N(f(x-s\alpha))\ &ist\ nicht\ quadratfrei \Leftrightarrow\\ N(f(x-s\alpha))\ &hat\ mehrfache\ Nullstellen \Leftrightarrow\\ (s\alpha_i+\beta_{i,j}) = (s\alpha_u+\beta_{u,v})\ &mit\ passenden\ Indizes\ i \neq u, j, v \Leftrightarrow\\ s &= \frac{\beta_{u,v}-\beta_{i,j}}{\alpha_i-\alpha_u}\end{aligned}$$

Für α und β kommen jeweils nur endlich viele komplexe Zahlen in Frage, da es sich um Nullstellen des Minimalpolynoms bzw. von $\sigma_i(f)$ handelt. Damit ist die Behauptung gezeigt. □

Mit diesen Ergebnissen als Grundlage lässt sich nun ein Algorithmus formulieren, der ein gegebenes quadratfreies Polynom $f \in K[x]$ vollständig faktorisiert.

Algorithmus. *Das Polynom f wird hier wieder als Polynom in zwei Variablen über $\mathbb{Q}$ betrachtet.*

Input $f \in \mathbb{Q}[t,x]$, *primitives Element α der Körpererweiterung, Minimalpolynom* $m_{\alpha,\mathbb{Q}}$

1. Schritt *Bestimme $s \in \mathbb{Q}$, so dass $f(x - s\alpha)$ quadratfreie Norm hat:*

$s := 0$
$f_s := f(t, x)$
$N(f_s) := \mathrm{res}_t(f_s, m)$
while $\deg(\mathrm{ggT}_{\mathbb{Q}[x]}(N(f_s), N(f_s)')) \neq 0$ ***do***
$s := s + 1$
$f_s := f_s(t, x - \alpha)$
$N(f_s) := \mathrm{res}_t(f_s, m)$
end while

2. Schritt *Faktorisiere $N(f_s)$*

$B := factors(N(f_s))$
if $\mathrm{length}(B) = 1$, ***return*** f_s
else
for $p_i \in B$ ***do***
$p_i := \mathrm{ggT}_{K[x]}(p_i, f)$
$p_i := p_i(\alpha, x + s\alpha)$
return B
end if

Beachte, dass der erste Schritt auf Grund von Satz 4.1 terminiert. $\mathrm{length}(B) = 1$ bedeutet, dass $N(f_s)$ schon irreduzibel ist. Damit ist auch f_s irreduzibel und die Faktorisierung ist trivial. Es gibt auch alternative Formulierungen, bei denen die letzten Schritte zusammengefasst werden, das heißt man bestimmt dann

$$p_i := \mathrm{ggT}_{K[x]}(p_i(x + s\alpha), f)$$

als irreduzible Faktoren von f.
Das Vorgehen soll nun noch an Hand eines Beispiels verdeutlicht werden.

Beispiel. *Gesucht ist die Faktorisierung von $f(x) = x^2 - 2$ über $\mathbb{Q}(\alpha)[x]$ für $\alpha = \sqrt{2}$. Es ist offensichtlich, dass $n = 2$. Anwendung des ersten Schrittes liefert:*

$$\begin{array}{lcl} f_0 = x^2 - 2 & \Rightarrow & N(f_0) = (x^2 - 2)^2 \\ f_1 = (x - \sqrt{2})^2 - 2 = x^2 - 2\sqrt{2}x & \Rightarrow & N(f_1) = x^4 - 8x^2 = x^2(x^2 - 8) \\ f_2 = (x - 2\sqrt{2})^2 - 2 = x^2 - 4\sqrt{2}x + 6 & \Rightarrow & N(f_2) = x^4 - 20x^2 + 36 \end{array}$$

$N(f_2)$ ist quadratfrei[5]. Die Faktorisierung von $N(f_2)$ über $\mathbb{Q}[x]$ ist

$$N(f_2) = (x^2 - 2)(x^2 - 18) =: p_1(x)p_2(x).$$

[5]Berechne dazu zum Beispiel $ggT(N(f_2), N(f_2)') = 1$ über den euklidischen Algorithmus

Um daraus ein Faktorisierung von f zu erhalten, bestimme

$$\mathrm{ggT}_{\mathbb{Q}(\sqrt{2})[x]}(f, p_1(x+2\sqrt{2})) = \mathrm{ggT}_{\mathbb{Q}(\sqrt{2})[x]}(f, x^2+4\sqrt{2}x+6) = x+\sqrt{(2)}$$

sowie

$$\mathrm{ggT}_{\mathbb{Q}(\sqrt{2})[x]}(f, p_2(x+2\sqrt{2})) = \mathrm{ggT}_{\mathbb{Q}(\sqrt{2})[x]}(f, x^2+4\sqrt{2}x-10) = x-\sqrt{(2)}.$$

Die Faktorisierung[6] *von f ist also gegeben durch*

$$x^2-2 = (x+\sqrt{2})(x-\sqrt{2}).$$

5 Kurzer Ausblick

Eine auf den ersten Blick nicht offensichtliche Anwendung der erzielten Resultate ist die symbolische Integration in Computeralgebrasystemen. Allerdings soll dieser Bereich an dieser Stelle unberücksichtigt bleiben.[7]
Weiterhin kann diese Arbeit fortgesetzt werden, indem man die Effizienz von Tragers Algorithmus untersucht. Es ist zwar klar, dass das Verfahren nach endlich vielen Schritten ein Ergebnis liefert, allerdings ist es zunächst unklar, ob bzw. für welche Polynome der gesuchte Werte s "schnell" gefunden wird. Hier lohnt sich ein Blick in

> *Computer Algebra Handbook, Foundations, Applications, Systems*; Grabmeier, Kaltofen, Weispfenning; Springer; 2003.

Abschließend ist zu erwähnen, dass *Maple* für die Faktorisierung von Polynomen über algebraischen Zahlkörpern den Algorithmus von Trager als Grundlage benutzt.[8]

[6] Die letzten beiden Berechnungen aus dem Algorithmus wurden in der Berechnung eines ggT zusammengefasst.
[7] Siehe hierzu zum Beispiel (GCL), Kapitel 11 und 12
[8] Siehe hierzu Kapitel 7.2 *von Introduction to Maple, 3rd Edition*; Heck; Springer; New York; 2003