Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Prof. Marc Nieper-Wißkirchen

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 8 zur Algebra I

Abgabe bis 10. Juni 2013, 17:00 Uhr

Aufgabe 1. *Numerischer Irreduzibilitätstest*

Bestimme numerisch die Nullstellen von $f(X) = X^4 - 12\,X^2 + 1$ bis auf wenige Stellen nach dem Komma, und nutze diese Information um zu zeigen, dass $f(X)$ über den rationalen Zahlen irreduzibel ist.

Lösung. Die Nullstellen von $f(X)$ sind näherungsweise

$$x_1 \approx -3{,}452, \qquad x_2 \approx -0{,}290, \qquad x_3 \approx 0{,}290, \qquad x_4 \approx 3{,}452.$$

Da $f(X)$ normiert ist und ganzzahlige Koeffizienten hat, können wir nun alle Auswahlen der Nullstellen durchgehen und jeweils prüfen, ob die elementarsymmetrischen Funktionen in diesen Nullstellen ganze Zahlen ergeben.

Linearfaktoren: Keine der Nullstellen ist ganzzahlig, also kann kein Linearfaktor abspalten.

Quadratische Faktoren: Für jede zweielementige Auswahl der Nullstellen sind stets nicht beide elementarsymmetrischen Funktionen in den Nullstellen ganzzahlig:

$$\begin{aligned}
e_1(x_1, x_2) &\approx -3{,}7 & e_2(x_1, x_2) &\approx 1{,}0 \\
e_1(x_1, x_3) &\approx -3{,}2 & e_2(x_1, x_3) &\approx -1{,}0 \\
e_1(x_1, x_4) &\approx 0{,}0 & e_2(x_1, x_4) &\approx -11{,}9 \\
e_1(x_2, x_3) &\approx 0{,}0 & e_2(x_2, x_3) &\approx -0{,}1 \\
e_1(x_2, x_4) &\approx 3{,}2 & e_2(x_2, x_4) &\approx -1{,}0 \\
e_1(x_3, x_4) &\approx 3{,}7 & e_2(x_3, x_4) &\approx 1{,}0
\end{aligned}$$

Tatsächlich muss man nicht alle dieser Auswahlen prüfen – es genügen die ersten drei. Denn die letzten drei sind einfach die Komplementärauswahlen zu den ersten drei.

Kubische Faktoren: Kann es nicht geben, da die komplementären Faktoren Linearfaktoren wären.

Aufgabe 2. *Inhalt von Polynomen*

Sei $f(X)$ ein nicht verschwindendes Polynom mit rationalen Koeffizienten. Zeige, dass der Inhalt von f...

a) ...genau dann ganzzahlig ist, wenn alle Koeffizienten von f ganzzahlig sind.

b) ...das Inverse des Leitkoeffizienten von $\widetilde{f}$ ist, wenn f normiert ist.

c) ...das Inverse einer ganzen Zahl ist, wenn f normiert ist. Gilt auch die Umkehrung?

Lösung. Es gilt die Beziehung $\mathrm{Leitkoeff}(\widetilde{f}) = c^{-1} \cdot \mathrm{Leitkoeff}(f)$, wobei $\widetilde{f}$ ein Polynom mit ganzzahligen Koeffizienten ist, das zudem primitiv ist. Diese Beziehung werden wir wiederholt verwenden.

a) „$\Longrightarrow$“: Es gilt $f = c \cdot \widetilde{f}$, also ist f als Produkt von Polynomen aus $\mathbb{Z}[X]$ selbst ein Polynom aus $\mathbb{Z}[X]$.

„$\Longleftarrow$“: Wenn f ganzzahlige Koeffizienten hat, ist c der größte gemeinsame Teiler der Koeffizienten von f (wieso?) und daher ganzzahlig.

b) Wenn f normiert ist, gilt $\text{Leitkoeff}(\widetilde{f}) = c^{-1} \cdot \text{Leitkoeff}(f) = c^{-1} \cdot 1$, also ist c das Inverse der Zahl $\text{Leitkoeff}(\widetilde{f})$.

c) Mit Teilaufgabe b) folgt sofort die Behauptung, denn der Leitkoeffizient von $\widetilde{f}$ ist ganzzahlig. Die Umkehrung gilt überhaupt nicht: Eines von unzähligen Gegenbeispielen ist $f(X) = 2X + 3$, dessen Inhalt 1 ist, das aber nicht normiert ist. Ein anderes Gegenbeispiel ist $f(X) = \frac{1}{3}X$, dessen Inhalt $\frac{1}{3}$ ist.

Aufgabe 3. *Kongruenzrechnungen*

a) Sei n eine ganze Zahl und seien a, a', b, b' ganze Zahlen mit $a \equiv a'$ und $b \equiv b'$ modulo n. Rechne explizit nach, dass dann auch $a + b \equiv a' + b'$ modulo n.

b) Sei n eine ganze Zahl und sei a eine zu n teilerfremde ganze Zahl. Zeige, dass für ganze Zahlen b, b' mit $ab \equiv ab'$ modulo n folgt, dass $b \equiv b'$ modulo n.

c) Sei a eine ganze Zahl mit $a \equiv 1$ modulo 5. Für welche Exponenten k ist $a^k \equiv 2$ modulo 5?

d) Finde zwei ganze Zahlen, die modulo 35 invers zu 8 sind.

Lösung.

a) Gelte $a \equiv a'$ und $b \equiv b'$ modulo n, d. h. $a - a'$ und $b - b'$ sind jeweils durch n teilbar. Dann ist auch

$$(a + b) - (a' + b') = (a - a') + (b - b')$$

durch n teilbar, d. h. es gilt $a + b \equiv a' + b'$.

Bemerkung: Etwas abstrakter formuliert hat man in dieser Aufgabe gezeigt, dass die Addition auf dem Restklassenring $\mathbb{Z}/(n)$ wohldefiniert ist.

b) Da a und n zueinander teilerfremd sind, gibt es eine Bézoutdarstellung der Form $1 = pa + qn$ für gewisse ganze Zahlen p und q. Modulo n gilt daher $1 \equiv pa$ (d. h. p ist ein Inverses für a modulo n). Wenn man die gegebene Kongruenz $ab \equiv ab'$ auf beiden Seiten mit p multipliziert, erhält man $pab \equiv pab'$, also $b \equiv b'$.

c) Für keinen einzigen Exponenten ist das erfüllt. Denn wenn $a \equiv 1$ modulo 5, so sind auch a^2, a^3 usw. jeweils kongruent zu 1 modulo 5. Aber 2 ist nicht kongruent zu 1 modulo 5.

Variante: Wenn $a \equiv 1$ modulo 5, gibt es eine ganze Zahl p mit $a - 1 = 5p$. Dann kann man mit dem binomischen Lehrsatz das Produkt $(a - 1)^k$ explizit ausmultiplizieren und sehen, dass es modulo 5 kongruent zu 1 ist.

d) Ein Inverses ist 22, denn $8 \cdot 22 = 176 = 5 \cdot 35 + 1 \equiv 1$ modulo 35. Ein anderes ist -13.

Bemerkung: Allgemein kann man ein Inverses einer ganzen Zahl a modulo n stets so berechnen (vgl. Proposition 3.20): Zunächst bestimmt man eine Bézoutdarstellung $d = p \cdot a + q \cdot n$ des größten gemeinsamen Teilers von a und n, $d \geq 1$. Ist $d \neq 1$, so ist a modulo n nicht invertierbar. Andernfalls folgt $1 \equiv p \cdot a + 0$ modulo n, also ist p ein Inverses zu a modulo n. Eine mögliche Bézoutdarstellung hier ist $1 = (-13) \cdot 8 + 3 \cdot 35$.

Aufgabe 4. *Reduktion modulo einer Primzahl*

Sei $f(X)$ ein normiertes Polynom mit ganzzahligen Koeffizienten. Beweise oder widerlege: Ist $f(X)$ modulo einer Primzahl reduzibel, so ist $f(X)$ auch über den rationalen Zahlen reduzibel.

Lösung. Das stimmt nicht. Etwa ist das Polynom $f(X) = X^2 + 1$ über der Primzahl 2 reduzibel, denn es gilt $f(X) = X^2 + 1 \equiv (X + 1)^2 \mod 2$ – aber bekanntermaßen ist $f(X)$ nicht über den rationalen Zahlen reduzibel.

Bemerkung: Die Umkehrung stimmt aber schon, siehe Proposition 3.23 im Skript.

Aufgabe 5. *Irreduzibilitätstest nach Leopold Kronecker*

a) Seien $b_0, \ldots, b_m$ von Null verschiedene ganze Zahlen. Zeige, dass es nur endlich viele Polynome $g(X)$ vom Grad $\leq m$ mit ganzzahligen Koeffizienten gibt, sodass für alle $i = 0, \ldots, m$ die ganze Zahl $g(i)$ ein Teiler von b_i ist.

b) Sei $f(X)$ ein primitives Polynom vom Grad n mit ganzzahligen Koeffizienten und $f(i) \neq 0$ für alle $0 \leq i \leq \frac{n}{2}$. Zeige, dass es nur endlich viele Polynome $g(X), h(X)$ mit ganzzahligen Koeffizienten und $f = g \cdot h$ gibt.

c) Verwende Teilaufgabe b), um ein Verfahren anzugeben, das von einem primitiven Polynom $f(X)$ mit ganzzahligen Koeffizienten feststellt, ob es über den rationalen Zahlen reduzibel oder irreduzibel ist.

Lösung.

a) Jede der Zahlen b_i besitzt nur endlich viele Teiler, da sie nicht null ist. Daher gibt es nur endlich viele Tupel $(g_0, \ldots, g_m)$ mit $g_i \mid b_i$ für alle $i = 0, \ldots, m$. Wegen des Satzes über die Eindeutigkeit der Polynominterpolation gibt es für jedes dieser Tupel nur genau ein Polynom $g(X)$ vom Grad $\leq m$ mit $g(i) = g_i$ für alle $i = 0, \ldots, m$.

b) Gelte $f(X) = g(X) \cdot h(X)$. Nach Aufgabe 4e) von Blatt 4 sind dann für jedes i mit $0 \leq i \leq \frac{n}{2}$ die Zahlen $g(i)$ und $h(i)$ jeweils Teiler von $b_i := f(i)$. Mindestens einer der beiden Faktoren hat Grad $\leq \frac{n}{2}$; daher folgt mit Teilaufgabe a), dass es nur endlich viele Möglichkeiten für ihn gibt. Der andere Faktor ist aus dem ersten sowieso eindeutig bestimmt. Das zeigt zusammengenommen die Behauptung.

c) Von einem gegebenen primitiven Polynom $f(X)$ vom Grad n mit ganzzahligen Koeffizienten können wir zunächst prüfen, ob eine der Zahlen $f(i)$ für $0 \leq i \leq \frac{n}{2}$ null ist. Wenn ja, ist $f(X)$ sicherlich reduzibel. Wenn nein, können wir die endlich vielen Teiler der Zahlen $f(i)$ bestimmen, durch Polynominterpolation jeweils ein Polynom $g(X)$ konstruieren und prüfen, ob die Polynomdivision von $f(X)$ durch $g(X)$ glatt in einem ganzzahligen Polynom aufgeht. Wenn ja, ist $f(X)$ reduzibel, da wir einen abspaltenden Faktor gefunden haben. Wenn die Division so nie aufgeht, ist $f(X)$ über den ganzen Zahlen und wegen seiner Primitivität auch über den rationalen Zahlen irreduzibel.

Bemerkung: Das hier vorgestellte Verfahren ist in der Praxis relativ untauglich. Besser ist es, spezialisierte Algorithmen zu verwenden; einen davon (bei weitem nicht der beste) haben wir in der Vorlesung kennengelernt (Auswahlen von Nullstellen betrachten). All diese besseren Verfahren verwenden aber die reellen oder komplexen Zahlen. Der Vorteil des Verfahrens dieser Aufgabe ist, dass es ausschließlich mit der Betrachtung rationaler Zahlen auskommt. Das ist von einem theoretischen Standpunkt aus wünschenswert: Denn in der Formulierung der Frage nach der Irreduzibilität eines primitiven Polynoms mit ganzzahligen Koeffizienten treten die reellen oder komplexen Zahlen ja gar nicht auf.