IRREDUZIBILITÄTSKRITERIEN NACH SELMER UND PERRON

ANKE DEMMING

Bachelorarbeit

vorgelegt von
Anke Demming

Fakultät für Mathematik
Universität Bielefeld

Oktober 2007

Inhaltsverzeichnis

1. Einführung und Wiederholung

In dieser Arbeit wollen wir uns mit den *Irreduzibilitätskriterien* von *Ernst S. Selmer* und *Oskar Perron* beschäftigen. Dazu sei zunächst an den zentralen Begriff der *Irreduzibilität* erinnert.

Sei R ein Integritätsbereich. Ein Polynom $f(x) \in R[x]$ heißt *irreduzibel*, falls aus jeder Zerlegung $f(x) = g(x) \cdot h(x)$ mit $g(x), h(x) \in R[x]$ stets folgt, dass $g(x)$ oder $h(x)$ eine Einheit ist.

Die Irreduzibilität spielt in vielen Teilgebieten der Mathematik eine zentrale Rolle:

In der Körpertheorie muss man häufig entscheiden, ob ein Polynom irreduzibel ist. Wenn K ein Körper ist, und $f(x) \in K[x]$ ein Polynom, dann möchte man häufig wissen, ob $K[x]/(f(x))$ ein Körper ist. Dies ist jedoch der Fall, wenn $f(x)$ irreduzibel ist.

Beim Studium von *verallgemeinerten Kettenbrüchen* gibt es verschiedene Ersetzungsalgorithmen. Man hat eine Folge mit n Zahlen, etwa:

$$a_1^{(r)} \geq a_2^{(r)} \geq \cdots \geq a_n^{(r)} \geq 0.$$

Diese Zahlen werden durch Divisionen oder Subtraktionen miteinander verrechnet und nach ihrem Betrag neu geordnet. Danach bekommt man die Folge:

$$a_1^{(r+1)} \geq a_2^{(r+1)} \geq \cdots \geq a_n^{(r+1)} \geq 0.$$

Von besonderem Interesse sind nun periodische Entwicklungen, das heißt es gilt:

$$\frac{a_1^{(r+s)}}{a_1^{(r)}} = \frac{a_2^{(r+s)}}{a_2^{(r)}} = \cdots = \frac{a_n^{(r+s)}}{a_n^{(r)}} = \lambda$$

für ein s. Hier wird λ durch eine Gleichung vom Grad n festgelegt. Diese ist irreduzibel genau dann, wenn die n Zahlen linear unabhängig sind (wobei sowohl lineare Unabhängigkeit als auch Irreduzibilität sich hier auf $\mathbb{Q}$ beziehen). Für weitere Informationen siehe [1].

Demnach wünscht man sich Kriterien an die Hand, welche es einem erleichtern zu entscheiden, ob ein Polynom irreduzibel ist.

In einzelnen Spezialfällen ist dies leicht zu sehen:

- Polynome ersten Grades sind offenbar immer irreduzibel.
- Polynome zweiten oder dritten Grades sind genau dann irreduzibel, wenn sie keine Nullstellen im Grundring haben.
- Ein Polynom mit Grad mindestens 3 ist nicht irreduzibel über $\mathbb{R}$.

Wir wollen uns auch noch an zwei häufig zitierte Irreduzibilitätskriterien erinnern:

Das wohl bekannteste Kriterium ist das von *Eisenstein*.

Sei $f \in R[x]$, etwa $f(x) = \sum_{j=0}^{n} a_j x^j$. Außerdem sei $f(x)$ primitiv, das heißt $ggT(a_1, \ldots, a_n) = 1$. Sei $p \in R$ ein Primelement mit

$$\begin{aligned} p &\nmid a_n \\ p &\mid a_i \quad \text{für } 0 \leq i \leq n-1 \\ p^2 &\nmid a_0, \end{aligned}$$

so ist f irreduzibel in $R[x]$.

Ein weiteres Kriterium ist die *Koeffizientenreduktion modulo p.*

Ist $f(x) = \sum_{j=1}^{n} a_j x^j \in \mathbb{Z}[x]$ primitiv, $a_n \not\equiv 0 \ mod\ p$ und $\overline{f(x)} := \sum_{j=1}^{n} \overline{a_j} x^j$, wobei mit $\overline{a_j}$ die Restklasse von a_j modulo p gemeint ist. Ist $\overline{f(x)}$ irreduzibel in $\mathbb{Z}_p[x]$, so ist $f(x)$ irreduzibel in $\mathbb{Z}[x]$.

In dieser Arbeit konzentrieren wir uns auf *normierte Trinome*, also Polynome der Form $f(x) = x^n + ax + b$. Die Koeffizienten dieser Polynome stammen aus dem Integritätsbereich $\mathbb{Z}$, wobei wir uns nur auf den Fall $b = \pm 1$ beschränken. Zu untersuchen ist die Irreduzibilität dieser Polynome über $\mathbb{Q}$.

Hierzu sei noch an ein Korollar aus dem *Lemma von Gauß* erinnert[1].

Ist ein nichtkonstantes Polynom $f(x)$ in $\mathbb{Z}[x]$ irreduzibel, so ist $f(x)$ auch in $\mathbb{Q}[x]$ irreduzibel.

Das heißt jedoch auch, dass ein Polynom $f(x) \in \mathbb{Z}[x]$, welches eine Zerlegung über $\mathbb{Q}$ hat, auch schon über $\mathbb{Z}$ zerlegbar ist. Deshalb gehen wir im Folgenden immer davon aus, dass Zerlegungen der Polynome aus $\mathbb{Z}[x]$ auch ganzzahlige Koeffizienten haben.

In Kapitel 2 zeigen wir die Irreduzibilität der Polynome

$$f_n(x) = x^n - x - 1.$$

Dafür betrachten wir die Verteilung der Nullstellen in der komplexen Ebene. Für die Nullstellen $x_j = r \cdot e^{i\varphi}$ mit $\frac{2\pi}{3} < \varphi < \frac{4\pi}{3}$ gilt $|r| < 1$. Die restlichen Nullstellen sind betragsmäßig größer als eins. Um die Irreduzibilität zu beweisen stellen wir eine Gleichung auf, die die Lage der Nullstellen beschreibt. Außerdem benutzen wir, dass keine der Nullstellen den Betrag eins hat.

Im Kapitel 3 untersuchen wir die Polynome

$$f_n(x) = x^n + ax \pm 1,$$

für $|a| \geq 3$. Auch hier betrachten wir die Verteilung der Nullstellen in der komplexen Ebene. Man kann zeigen, dass Polynome von denen $n-1$ Nullstellen innerhalb des Einheitskreises liegen, irreduzibel sind. Für die Polynome $f_n(x)$ benötigt man zuerst eine Variablentransformation. Hier liegen $n-1$ Nullstellen außerhalb des Einheitskreises. Nach der Transformation kann man den zuvor bewiesenen Satz anwenden und erhält die Irreduzibilität.

[1]Dieses Korollar findet man in [4], Kapitel 11 (3.5)

2. Irreduzibilitätskriterium von Selmer

In diesem Kapitel wollen wir das Irreduzibilitätskriterium von Selmer beweisen, welches im folgenden Satz formuliert wird.

Satz 2.1 (Selmer)**.** *Die Polynome $f_n(x) = x^n - x - 1$ sind irreduzibel über $\mathbb{Q}$ für alle n.*

Bemerkung. Mit kleinen Erweiterungen im Beweis erhält man außerdem noch, dass die Polynome $f_n(x) = x^n + x + 1$ irreduzibel über $\mathbb{Q}$ sind für $n \not\equiv 2 \bmod 3$.

Falls $n \equiv 2 \bmod 3$, so haben die Polynome einen Faktor x^2+x+1. Der zweite Faktor ist dann irreduzibel über $\mathbb{Q}$. Der Beweis läuft in weiten Teilen analog zu dem von Satz 2.1, wird aber in dieser Arbeit nicht behandelt. Dieser Beweis findet sich aber in [1]

Im Weiteren schließen wir die Fälle $n = 1$ und $n = 2$ aus, weil $f_1 = -1$ offensichtlich irreduzibel ist und für $f_2(x) = x^2 - x - 1$ gilt, dass die beiden Nullstellen nicht in $\mathbb{Q}$ liegen, was die Irreduzibilität einschließt.

Sei nun $f(x)$ normiert vom Grad $n \geq 3$, also im Allgemeinen von der Form

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \in \mathbb{Z}[X], \quad a_n \neq 0.$$

Die Nullstellen über $\mathbb{C}$ seien x_j, für $1 \leq j \leq n$.

Definiere:

$$S(f(x)) = \sum_{j=1}^{n} \left(x_j - \frac{1}{x_j} \right) = \sum_{j=1}^{n} x_j - \sum_{j=1}^{n} \frac{1}{x_j}$$

als die Summe der Nullstellen weniger der Summe ihrer Kehrwerte.

Es folgt sofort:

Die Zuordnung

$$S \colon f \mapsto S(f(x))$$

ist additiv bezüglich jeder Faktorisierung von $f(x)$, das heißt ist $f(x) = g(x) \cdot h(x)$, so gilt:

$$S(f(x)) = S(g(x) \cdot h(x)) = S(g(x)) + S(h(x)).$$

Schreibe nun $f(x)$ ein wenig um:

$$\begin{aligned} f(x) &= x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \\ &= \prod_{j=1}^{n} (x - x_j). \\ &= x^n - x^{n-1} \left(\sum_{j=1}^{n} x_j \right) + x^{n-2} \left(\sum_{i>j} x_i \cdot x_j \right) + \cdots + (-1)^n \prod_{j=1}^{n} x_j \end{aligned}$$

also

$$f(x) = \sum_{j=1}^{n} (-1)^j \cdot x^j \cdot \sigma_j(x_1, \ldots, x_n), \tag{1}$$

wobei die σ_j die elementarsymmetrischen Funktionen

$$\sigma_j(x_1, \ldots, x_n) = \sum_{k_1 > \cdots > k_j} x_{k_1} \ldots x_{k_j}$$

sind.

Proposition 2.2. *Es gilt:*

$$S(f(x)) = -a_1 + \frac{a_{n-1}}{a_n}.$$

Beweis. Aus (1) wissen wir bereits:

$$\sigma_1(x_1, \ldots, x_n) = \sum_{j=1}^{n} x_j = -a_1.$$

Damit erhält man bereits die folgende Darstellung für $S(f(x))$,

$$S(f(x)) = -a_1 - \sum_{j=1}^{n} \frac{1}{x_j}.$$

Um den hinteren Teil der Summe umzuschreiben definieren wir die folgende Funktion:

$$g(t) := \prod_{j=1}^{n} (t - \frac{1}{x_j}).$$

Es ist:

$$\begin{aligned}
g(t) &= \prod_{j=1}^{n} \left(t - \frac{1}{x_j} \right) \\
&= \prod_{j=1}^{n} \left(x_j - \frac{1}{t} \right) \cdot \frac{t^n}{x_1 \ldots x_n} \\
&= \prod_{j=1}^{n} \left(\frac{1}{t} - x_j \right) \cdot \frac{(-1)^n \cdot t^n}{x_1 \ldots x_n} \\
&\overset{(1)}{=} f\left(\frac{1}{t} \right) \frac{t^n}{a_n} \\
&= (1 + a_1 \cdot t + \cdots + a_n \cdot t^n) \cdot \frac{1}{a_n} \\
&= t^n + \frac{a_{n-1}}{a_n} \cdot t^{n-1} + \cdots + \frac{a_1}{a_n} \cdot t + \frac{1}{a_n}
\end{aligned}$$

Damit ist

$$\sigma_1\left(\frac{1}{x_1},\ldots,\frac{1}{x_n}\right)=\sum_{j=1}^{n}\frac{1}{x_j}=-\frac{a_{n-1}}{a_n},$$

und wir erhalten

$$S(f(x))=-a_1+\frac{a_{n-1}}{a_n}.$$

□

Wir sehen also, dass für jedes Polynom $f(x)$ mit ganzzahligen Koeffizienten die Summe $S(f(x))$ in $\mathbb{Q}$ ist. Außerdem erhält man, dass $S(f(x))\in\mathbb{Z}$, falls $a_n=\pm 1$.
Damit erhält man für das Polynom $f_n(x)$:

$$S(f_n(x))=0+\frac{-1}{-1}=1 \text{ für } n\geq 3.$$

Sei nun

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x\pm 1.$$

Es sei $f(x)=g(x)\cdot h(x)$ eine Faktorisierung mit

$$g(x)=x^t+b_1x^{t-1}+\cdots+b_t$$
$$h(x)=x^s+c_1x^{s-1}+\cdots+c_s$$

und $t+s=n$.

Weil $g(x),h(x)\in\mathbb{Z}[x]$ folgt $b_t,c_s\in\mathbb{Z}$. Außerdem gilt $a_n=b_t\cdot c_s$, jedoch ist $a_n=\pm 1$. Damit folgt $b_t,c_s=\pm 1$

Für eine mögliche Faktorisierung des Polynoms $f_n(x)=g(x)\cdot h(x)$ gilt nun:

$$1=S(f_n(x))=S(g(x)\cdot h(x))=S(g(x))+S(h(x))$$

mit

$$S(g(x)),S(h(x))\in\mathbb{Z}.$$

Substituiert man nun x_j durch die Darstellung in Polarkoordinaten

$$x_j=r_j\cdot e^{i\varphi_j},$$

so erhält man $x_j^{-1}=r_j^{-1}\cdot e^{-i\varphi_j}$.

Wegen $f_n(x)\in\mathbb{Z}[x]$ gilt, dass für ein $x_j\in\mathbb{C}$, welches Nullstelle von $f_n(x)$ ist auch die komplex konjugierte Zahl $\overline{x_j}$ Nullstelle ist. Schreibe

den Ausdruck aus $S(f(x))$ eines komplexen Nullstellenpaares nun um.

$$\begin{aligned}\left(x_j - \frac{1}{x_j}\right) + \left(\overline{x_j} - \frac{1}{\overline{x_j}}\right) &= r_j \cdot e^{i\varphi_j} - r_j^{-1} \cdot e^{-i\varphi_j} + r_j \cdot e^{-i\varphi_j} - r_j^{-1} \cdot e^{i\varphi_j} \\ &= r_j \cdot e^{i\varphi_j} + r_j \cdot e^{-i\varphi_j} - \left(\frac{1}{r_j} \cdot e^{i\varphi_j} + \frac{1}{r_j} \cdot e^{-i\varphi_j}\right) \\ &= 2 \cdot r_j \cdot \cos(\varphi_j) - 2 \cdot \frac{1}{r_j} \cdot \cos(\varphi_j) \\ &= 2 \cdot \frac{r_j^2 - 1}{r_j} \cdot \cos(\varphi_j)\end{aligned}$$

Somit erhalten wir den folgenden Ausdruck

$$\left(x_j - \frac{1}{x_j}\right) + \left(\overline{x_j} - \frac{1}{\overline{x_j}}\right) = 2 \cdot \frac{r_j^2 - 1}{r_j} \cdot \cos(\varphi_j). \tag{2}$$

Falls $x_j \in \mathbb{R}$, dann ist $\cos(\varphi_j) = \pm 1$ und man erhält:

$$x_j - \frac{1}{x_j} = \frac{r_j^2 - 1}{r_j} \cdot \cos(\varphi_j).$$

Proposition 2.3.

(i) *Für die Nullstellen $x_j = r_j \cdot e^{i\varphi_j}$ des Polynoms $f_n(x)$ gilt:*

$$\cos(\varphi_j) = \frac{r_j^{2n} - r_j^2 - 1}{2r_j}$$

(ii) *Es gibt keine Nullstelle $\alpha = r \cdot e^{i\varphi_j}$ des Polynoms $f_n(x)$ mit $r = 1$.*

Beweis.
(i): Betrachte $f_n(x) = x^n - x - 1$ und seien

$$x_j = r_j \cdot e^{i\varphi_j} = r_j(\cos(\varphi_j) + i \cdot \sin(\varphi_j)),$$

$1 \leq j \leq n$, die Nullstellen des Polynoms. Setzt man diese nun in das Polynom ein, so erhält man aus $f_n(x_j) = 0$:

$$\begin{aligned}(r_j \cdot e^{i\varphi_j})^n - r_j \cdot e^{i\varphi_j} - 1 &= 0 \\ r_j^n \cdot e^{i \cdot n \cdot \varphi_j} &= r_j \cdot e^{i\varphi_j} + 1 \\ r_j^n(\cos(n \cdot \varphi_j) + i \cdot \sin(n \cdot \varphi_j)) &= r_j(\cos(\varphi_j) + i \cdot \sin(\varphi_j)) + 1 \\ r_j^n \cdot \cos(n \cdot \varphi_j) + i \cdot r_j^n \cdot \sin(n \cdot \varphi_j) &= r_j \cdot \cos(\varphi_j) + i \cdot r_j \cdot \sin(\varphi_j) + 1\end{aligned}$$

und damit

$$\begin{aligned}r_j^n \cdot \cos(n \cdot \varphi_j) &= r_j \cdot \cos(\varphi_j) + 1 \\ r_j^n \cdot \sin(n \cdot \varphi_j) &= r_j \cdot \sin(\varphi_j)\end{aligned}$$

Nimmt man nun die Summe der Quadrate auf beiden Seiten, so erhält man

$$r_j^{2n} \cdot \cos^2(n \cdot \varphi_j) + r_j^{2n} \cdot \sin^2(n \cdot \varphi_j)$$
$$= r_j^2 \cdot \cos^2(\varphi_j) + 2r_j \cdot \cos(\varphi_j) + 1 + r_j^2 \cdot \sin^2(\varphi_j)$$

Mit $\cos^2 + \sin^2 = 1$ folgt:

$$r_j^{2n} = r_j^2 + 2r_j \cdot \cos(\varphi_j) + 1$$

Also

$$\cos(\varphi_j) = \frac{r_j^{2n} - r_j^2 - 1}{2r_j}.$$

(ii): Wir wissen schon, dass die Nullstellen von $f_n(x)$ folgende Gleichung erfüllen

$$\cos(\varphi_j) = \frac{r_j^{2n} - r_j^2 - 1}{2r_j}$$

Angenommen $r_j = 1$ für ein j. Dann gilt:

$$\cos(\varphi_j) = \frac{1 - 1 - 1}{2} = -\frac{1}{2}$$

Damit erhalten wir

$$\varphi_j = 120^\circ = \frac{2\pi}{3} \text{ oder } \varphi_j = 240^\circ = \frac{4\pi}{3}$$

Damit wäre eine mögliche Nullstelle $\alpha = e^{\frac{2\pi i}{3}}$, die andere $\tilde{\alpha} = e^{\frac{4\pi i}{3}}$. Das sind dritte Einheitswurzeln, wobei die zweite das Quadrat der ersten ist. Betrachte nur die erste, da der Beweis für die zweite völlig analog läuft. Damit gilt:

$$\alpha^n = \begin{cases} \alpha & \text{falls } n \equiv 1 \bmod 3 \\ \alpha^2 & \text{falls } n \equiv 2 \bmod 3 \\ 1 & \text{falls } n \equiv 0 \bmod 3 \end{cases}$$

Betrachten wir nun die 3 Fälle einzeln.

Fall 1: $\alpha^n = \alpha$ Setzt man dies in das Polynom ein, so erhält man:

$$f_n(\alpha) = \alpha - \alpha - 1 = -1 \neq 0$$

Fall 2: $\alpha^n = \alpha^2$. Dann erfüllt α die Gleichung

$$\alpha^2 - \alpha - 1 = 0$$

Es gilt jedoch auch, dass α dritte Einheitswurzel ist. Damit gilt also auch

$$\alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1) = 0$$

Da $\alpha \neq 1$ gilt folgt sofort, dass

$$\alpha^2 + \alpha + 1 = 0$$

gelten muss. Subtrahiert man nun die beiden oberen Gleichungen, so erhält man: $-2\alpha - 2 = 0$ und damit

$$\alpha = -1.$$

Setzen wir das nun in das Polynom $f_n(x)$ ein.

$$f_n(\alpha) = -1 - (-1) - 1 = -1 \neq 0$$

Fall 3: $\alpha^n = 1$. Setzt man auch dies in das Polynom ein, so erhält man:

$$f_n(\alpha) = 1 - \alpha - 1 = -\alpha \neq 0$$

Insgesamt sehen wir, dass es keine Nullstelle mit $r = 1$ geben kann. □

Lemma 2.4 (Ungleichung vom arithmetischen und geometrischen Mittel)**.** *Für $x_1, \ldots, x_n \in \mathbb{R}_{\geq 0}$ gilt*

$$\sqrt[n]{x_1 \cdot \cdots \cdot x_n} \leq \frac{x_1 + \cdots + x_n}{n}.$$

Beweis. [2]

Wir benutzen hierfür die Bernoulli Ungleichung:

$$(1 + x)^n \geq 1 + n \cdot x$$

und beweisen die Behauptung per Induktion.

Induktionsanfang $n = 2$. Es ist zu zeigen:

$$\sqrt{x_1 \cdot x_2} \leq \frac{x_1 + x_2}{2}$$

quadriert man dies, so erhält man

$$\begin{aligned} & 4 \cdot x_1 \cdot x_2 \leq x_1^2 + 2 \cdot x_1 \cdot x_2 + x_2^2 \\ \Leftrightarrow \quad & 0 \leq x_1^2 - 2 \cdot x_1 \cdot x_2 + x_2^2 \\ \Leftrightarrow \quad & 0 \leq (x_1 - x_2)^2. \end{aligned}$$

Dies ist offensichtlich richtig.

Induktionsschritt $n \to n + 1$. Es sei ohne Einschränkung $x_{n+1} = \max\{x_1, \ldots, x_{n+1}\}$. Es sei

$$\tilde{x} = \frac{x_1 + \cdots + x_n}{n}$$

[2] Die Idee zu diesem Beweis findet sich z.B. auch in [3] Kapitel 12.2

das arithmetische Mittel der ersten n Zahlen. Es gilt: $x_{n+1} - \tilde{x} \geq 0$
Aus der Bernoulli Ungleichung folgt

$$\begin{aligned}\left(\frac{x_1 + \cdots + x_{n+1}}{(n+1)\tilde{x}}\right)^{n+1} &= \left(\frac{\tilde{x}n + x_{n+1}}{(n+1)\tilde{x}}\right)^{n+1} \\ &= \left(\frac{\tilde{x}(n+1) + x_{n+1} - \tilde{x}}{(n+1)\tilde{x}}\right)^{n+1} \\ &= \left(1 + \frac{x_{n+1} - \tilde{x}}{(n+1)\tilde{x}}\right)^{n+1} \\ &\geq 1 + \frac{x_{n+1} - \tilde{x}}{\tilde{x}} \\ &= \frac{x_{n+1}}{\tilde{x}}.\end{aligned}$$

Wir erhalten:

$$\begin{aligned}\left(\frac{x_1 + \cdots + x_{n+1}}{(n+1)}\right)^{n+1} &\geq \tilde{x}^{n+1}\frac{x_{n+1}}{\tilde{x}} \\ &= \tilde{x}^n \cdot x_{n+1} \\ &\overset{\text{(IV)}}{\geq} x_1 \cdot \ldots \cdot x_{n+1}.\end{aligned}$$

□

Nun haben wir alle Hilfsmittel um den Beweis des Satzes von Selmer zu vollenden.

Beweis von Satz 2.1. Angenommen $f_n(x)$ habe eine Faktorisierung in $f_n(x) = g(x) \cdot h(x)$.
Betrachten wir nun zuerst $g(x)$. Seien $x_1, \ldots, x_m$ die Nullstellen von $g(x)$. Nun betrachten wir den Ausdruck (2) und substituieren $\cos(\varphi_j)$

durch den Ausdruck aus Proposition 2.3i)

$$\begin{aligned}
2 \cdot \frac{r_j^2 - 1}{r_j} \cdot \cos(\varphi_j) &= 2 \cdot \frac{r_j^2 - 1}{r_j} \cdot \frac{r_j^{2n} - r_j^2 - 1}{2r_j} \\
&= \frac{(r_j^2 - 1)(r_j^{2n} - r_j^2 - 1)}{r_j^2} \\
&= \frac{r_j^{2n+2} - r_j^4 - r_j^2 - r_j^{2n} + r_j^2 + 1}{r_j^2} \\
&= \frac{1}{r_j^2} - r_j^2 + r_j^{2n} - r_j^{2n-2} \\
&= \frac{1}{r_j^2} - r_j^2 + r_j^{2n-2}(r_j^2 - 1) \\
&\overset{r_j \neq 1}{>} \frac{1}{r_j^2} - r_j^2 + r_j^2 - 1 \\
&= \frac{1}{r_j^2} - 1
\end{aligned}$$

Damit gilt für ein Paar von komplex konjugierten Nullstellen:

$$\left(x_j - \frac{1}{x_j}\right) + \left(\overline{x_j} - \frac{1}{\overline{x_j}}\right) > \frac{1}{r_j^2} - 1$$

Für die reellen Nullstellen gilt entsprechend

$$x_j - \frac{1}{x_j} > \frac{1}{2}\left(\frac{1}{r_j^2} - 1\right).$$

Damit erhält man:

$$S(g(x)) = \sum_{j=1}^{m} \left(x_j - \frac{1}{x_j}\right) > \frac{1}{2} \sum_{j=1}^{m} \left(\frac{1}{r_j^2} - 1\right). \tag{3}$$

Wir wissen bereits $b_t = \prod_{j=1}^{m} x_j = \pm 1$. Dann folgt

$$\prod_{j=1}^{m} r_j = 1,$$

und wir erhalten

$$\prod_{j=1}^{m} \frac{1}{r_j^2} = 1.$$

Wir kennen damit auch das geometrische Mittel der $\frac{1}{r_j^2}$,

$$\sqrt[m]{\prod_{j=1}^{m} \frac{1}{r_j^2}} = 1.$$

Unterscheiden wir nun zwei Fälle:
1. Fall: $m = 1$.

Dann gilt $r_1 = 1$. Das ist ein Widerspruch zu Proposition 2.3(ii).
2. Fall: $m > 1$.
Mit Lemma 2.4 erhält man:

$$\begin{aligned}\frac{1}{m}\sum_{j=1}^{m}\frac{1}{r_j^2} \geq 1 &\Rightarrow \frac{1}{m}\sum_{j=1}^{m}\left(\frac{1}{r_j^2} - 1\right) \geq 0 \\ &\Rightarrow \frac{1}{2}\sum_{j=1}^{m}(\frac{1}{r_j^2} - 1) \geq 0 \\ &\overset{(3)}{\Rightarrow} S(g(x)) > 0\end{aligned}$$

Insgesamt sehen wir also, dass $S(g(x)) > 0$. Analog folgt $S(h(x)) > 0$. Wir wissen jedoch, dass $S(g(x))$ und $S(h(x))$ ganzzahlig sind, das heißt

$$S(g(x)), S(h(x)) \geq 1.$$

Damit folgt

$$S(f_n(x)) = S(g(x)) + S(h(x)) \geq 2$$

Widerspruch zu $S(f_n(x)) = 1$.
$f_n(x)$ ist somit irreduzibel. □

3. Irreduzibilitätskriterium von Perron

Ein allgemeines Polynom sei von der Form

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_n \in \mathbb{Z}[x],$$

wobei hierbei stets $a_n \neq 0$ gilt. Dieses Kapitel beschäftigt sich mit dem Beweis des Irreduzibilitätskriteriums von Perron.

Satz 3.1 (Perron)**.**
Die Polynome $f_n(x) = x^n + ax \pm 1$ sind irreduzibel über $\mathbb{Q}$, für $|a| \geq 3$

Bemerkung.
Für $|a| = 2$ gilt außerdem, dass $f_n(x)$ irreduzibel über $\mathbb{Q}$ ist, oder einen Faktor $x \pm 1$ hat. Im letzteren Fall ist der zweite Faktor irreduzibel über $\mathbb{Q}$. Dies wird hier jedoch nicht bewiesen. Für den Beweis werden jedoch ähnliche Methoden verwendet wie in dem zu Satz 3.1. Weitere Informationen sind in den Quellen [1] und [2] zu finden.

Lemma 3.2.
Ein allgemeines Polynom $f(x)$ habe die Nullstellen $x_j \in \mathbb{C}$,
für $1 \leq j \leq n$. Es sei $|x_j| < 1$ für $1 \leq j \leq n-1$.
Dann ist $f(x)$ irreduzibel über $\mathbb{Q}$.

Beweis.
Angenommen $f(x)$ wäre nicht irreduzibel. Dann gäbe es eine Zerlegung von $f(x) = g(x) \cdot h(x)$, mit $g(x)$ und $h(x) \in \mathbb{Z}[x]$ und einer der Faktoren hätte nur Nullstellen deren Betrag kleiner als eins wäre. Dies sei

$$g(x) = x^k + b_1x^{k-1} + ... + b_k,$$

mit den Nullstellen y_j, für $1 \leq j \leq k$. Es gilt jedoch $b_k \in \mathbb{Z}$, also $b_k \geq 1$, aber nach (1)

$$|b_k| = |\prod_{j=1}^{k} y_j| < 1.$$

Widerspruch! □

Es sei nun vorerst

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_n \in \mathbb{C}[X].$$

Wir definieren

$$|a_1| + |a_2| + ... + |a_n| =: A.$$

Lemma 3.3.
Besitzt $f(x)$ eine Nullstelle α die die Ungleichungen

(i) $|\alpha| \geq 1$
(ii) $|a_1 + \alpha| > A + 1 - |a_1| - |\alpha|$

erfüllt so ist auch $|\alpha| > 1$. Dann folgt auch, dass die Beträge der anderen $n-1$ Nullstellen alle kleiner als 1 sind.

Beweis. Definiere die folgenden Polynome:

$$\begin{aligned} f_0(x) &= 1 \\ f_1(x) &= x + a_1 \\ &\vdots \\ f_j(x) &= x^j + a_1 x^{j-1} + \cdots + a_j \\ &\vdots \\ f_n(x) &= x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = f(x) \end{aligned}$$

Für diese Polynome und $1 \leq j \leq n-1$ gilt die folgende Rekursionsformel:

$$x \cdot f_j(x) + a_{j+1} = f_{j+1}.$$

Sei nun α eine Nullstelle von $f(x)$, die die Voraussetzungen des Lemmas erfüllt. Dann gilt $f_n(\alpha) = 0$ und wir definieren

$$\lambda := |f_1(\alpha)| + |f_2(\alpha)| + \cdots + |f_{n-1}(\alpha)|.$$

Man erhält:

$$\begin{aligned} |\alpha| \cdot \lambda &= |\alpha| \cdot (|f_1(\alpha)| + |f_2(\alpha)| + \cdots + |f_{n-1}(\alpha)|) \\ &= |\alpha| \cdot |f_1(\alpha)| + |\alpha| \cdot |f_2(\alpha)| + \cdots + |\alpha| \cdot |f_{n-1}(\alpha)| \\ &= |\alpha \cdot f_1(\alpha)| + |\alpha \cdot f_2(\alpha)| + \cdots + |\alpha \cdot f_{n-1}(\alpha)|. \end{aligned}$$

Wegen der Rekursionsformel gilt dann

$$\begin{aligned} |\alpha| \cdot \lambda &= |-a_2 + f_2(\alpha)| + |-a_3 + f_3(\alpha) + \cdots + |-a_n + f_n(\alpha)| \\ &\leq |a_2| + |f_2(\alpha)| + |a_3| + |f_3(\alpha)| + \cdots + |a_n| + |f_n(\alpha)| \\ &= A - |a_1| + \lambda - |f_1(\alpha)|. \end{aligned}$$

Also

$$\begin{aligned} & |\alpha| \cdot \lambda \leq A - |a_1| + \lambda - |f_1(\alpha)| \\ \Leftrightarrow\ & (|\alpha| - 1) \cdot \lambda \leq A - |a_1| - |f_1(\alpha)| \\ \Leftrightarrow\ & (|\alpha| - 1) \cdot \lambda \leq A - |a_1| - |\alpha + a_1|. \end{aligned} \tag{4}$$

Nach Voraussetzung ist $|\alpha| \geq 1$.
Angenommen es wäre $|\alpha| = 1$, dann liefert die Vorauusetzung (ii)

$$|a_1 + \alpha| > A + 1 - |a_1| - 1 \Leftrightarrow 0 > A - |a_1| - |a_1 + \alpha|.$$

Jedoch folgt aus (4):

$$0 \leq A - |a_1| - |\alpha + a_1|$$

Widerspruch!

Damit erhalten wir $|\alpha| > 1$ und Division durch $|\alpha| - 1$ liefert

$$\lambda \leq \frac{A - |a_1| - |\alpha + a_1|}{|\alpha| - 1} < 1.$$

Dies gilt, weil aus Voraussetzung (ii) folgt, dass

$$|\alpha| - 1 > A - |a_1| - |\alpha + a_1|.$$

Führt man nun eine Polynomdivision durch und setzt die Polynome f_j ein, so erhält man:

$$\frac{f(x)}{x-\alpha} = x^{n-1} + f_1(\alpha)x^{n-2} + \cdots + f_{n-1}(\alpha).$$

Angenommen dies hätte noch eine Nullstelle β für die gilt $|\beta| \geq 1$. Dann erhält man:

$$\begin{aligned} &\beta^{n-1} + f_1(\alpha) \cdot \beta^{n-2} + \cdots + f_{n-1}(\alpha) = 0 \\ &\Leftrightarrow \beta^{n-1} = -(f_1(\alpha) \cdot \beta^{n-2} + \cdots + f_{n-1}(\alpha)) \\ &\Rightarrow |\beta|^{n-1} = |f_1(\alpha) \cdot \beta^{n-2} + \cdots + f_{n-1}(\alpha)|. \end{aligned}$$

Nun ist,

$$\begin{aligned} |f_1(\alpha) \cdot \beta^{n-2} + \cdots + f_{n-1}(\alpha)| &\leq |f_1(\alpha)| \cdot |\beta|^{n-2} + \cdots + |f_{n-1}(\alpha)| \\ &\overset{|\beta|\geq 1}{\leq} \lambda \cdot |\beta|^{n-2}. \end{aligned}$$

Damit ist

$$|\beta| \leq \lambda.$$

Mit $|\beta| \geq 1$ folgt $\lambda \geq 1$. Widerspruch! □

Sei nun wieder $f(x) \in \mathbb{Z}[x]$. Wir wollen nun das obige Irreduzibilitätskriterium von Perron beweisen. Dazu zunächst der folgende Satz.

Satz 3.4 (Perron)**.**
Wenn die Koeffizienten von $f(x)$ der Ungleichung

$$|a_1| > 1 + |a_2| + |a_3| + ... + |a_n|$$

genügen, so ist $f(x)$ irreduzibel über $\mathbb{Q}$.

Beweis.
Es gilt $0 \neq a_n \in \mathbb{Z}$, also $|a_n| \geq 1$. Nach (1) gilt jedoch auch, dass

$$|a_n| = |\prod_{j=1}^{n} x_j|,$$

wobei x_j die Nullstellen von $f(x)$ sind. Dann gibt es eine Nullstelle α, für die gilt:

$$|\alpha| \geq 1$$

Außerdem gilt nach Voraussetzung die Ungleichung

$$\begin{aligned} &|a_1| > 1 + |a_2| + \cdots + |a_n| \\ \Leftrightarrow\ &|a_1| - |\alpha| > A + 1 - |a_1| - |\alpha|. \end{aligned}$$

Es gilt immer:

$$|a_1| - |\alpha| \leq |a_1 + \alpha|$$

und wir erhalten

$$|a_1 + \alpha| > A + 1 - |a_1| - |\alpha|.$$

Somit sind die Voraussetzungen für das Lemma erfüllt und $n-1$ Nullstellen von $f(x)$ sind betragsmäßig kleiner als 1.
Mit Lemma 3.2 folgt dann, dass $f(x)$ irreduzibel ist. □

Nun erhalten wir Satz 3.1 als Korollar aus Satz 3.4 wie folgt:

Beweis von Satz 3.1.
Betrachten wir nun $f_n(x) = x^n + ax \pm 1$ und substituieren $x = \frac{1}{z}$.
Dann erhalten wir

$$f_n\left(\frac{1}{z}\right) = \left(\frac{1}{z}\right)^n + a \cdot \left(\frac{1}{z}\right) \pm 1.$$

Durch Multiplikation mit z^n erhalten wir dann:

$$\hat{f}_n(z) = 1 + a \cdot z^{n-1} \pm z^n$$

Nun sind die folgenden Polynome auf Irreduzibilität zu untersuchen:

$$\tilde{f_n}(x) = z^n + a \cdot z^{n-1} + 1$$
$$\overline{f_n}(x) = z^n - a \cdot z^{n-1} - 1$$

Untersuchen wir diese Polynome für $|a| \geq 3$ auf Irreduzibilität indem wir die Voraussetzungen von Satz 3.4 prüfen.

$$|a| = |a_1| \geq 3 > 2 = 1 + |\pm 1| = 1 + |a_2| + \cdots + |a_n|$$

Die Voraussetzungen sind somit erfüllt und $f_n(x)$ ist irreduzibel. □

Literatur

[1] Ernst S. Selmer, *On the irreduzibility of certain trinomials*, Math. Scand. 4 (1956), 287 - 302
[2] Oskar Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, Journal für reine und angewandte Mathematik 132 (1907), 288 - 307
[3] Harro Heuser, *Lehrbuch der Analysis Teil 1*, B.G. Teubner Verlag, Stuttgart 1994[11]
[4] Michael Artin, *Algebra*, Birkhäuser Verlag, Basel 1993

Eigenständigkeitserklärung

Hiermit versichere ich, Anke Demming, dass ich die vorliegende Bachelorarbeit ohne die Hilfe Anderer verfasst habe. Außerdem habe ich keine Quellen verwendet, die nicht im Literaturverzeichnis angegeben sind.