# Jeder endliche Schiefkörper ist ein Körper

Erläuterungen zur Beweisführung von Ernst Witt

Lene Judika Stampa

Allgemeine Informatik
Fachhochschule Wedel

*Seminar 'Elegante Beweise' im WS2016/2017*
Dozent: Prof. Dr. Sebastian Iwanowski

9. März 2017

# Inhaltsverzeichnis

# 1 Einleitung

In der vorliegenden Seminararbeit soll es darum gehen, die Beweisführung von Ernst Witt „Über die Kommutativität endlicher Schiefkörper“ [1] und ihre Besprechung im „Buch der Beweise“ [2] durch Aigner und Ziegler zu erläutern und ggf. zu veranschaulichen. Der Originalbeweis ist äußerst knapp gehalten und seine Besprechung durch die genannten Autoren verwendet teilweise stark verschiedene Begriffe, sodass sich an einigen Stellen eine Verdichtung, eine Veranschaulichung oder manchmal auch nur ein schlichtes Ausformulieren des Nicht-Gesagten anbietet.

Die Argumenationsstruktur des Beweises ist knapp formuliert ein Beweis durch Widerspruch. Sie wird dem folgenden Muster folgen: Wir konstruieren uns einen hypothetischen endlichen Schiefkörper, also eine Menge, auf der alle Gesetzmäßigkeiten eines Körpers bis auf die Kommutativität der Multiplikationsgruppe gegeben sind. Das originale Postulat des Beweises lautet:

> *Eine endliche Additionsgruppe sei gegeben. Außer der Null sollen alle Elemente eine rechts- und linksdistributive Multiplikationsgruppe bilden.* [1]

Anschließend treffen wir Aussagen über das Verhältnis von Mächtigkeiten dieses konstruierten Schiefkörpers und seiner Zentralisatoren.
Im zweiten Schritt erarbeiten wir uns die Struktur eines Kreisteilungspolynoms und können über den Vergleich von Teilbarkeitsbeziehungen zeigen, dass jeder Zentralisator der Schiefkörper selbst sein muss - und damit der Schiefkörper ein Körper sein muss.

Die vorliegende Arbeit versucht dabei möglichst viele Schritte explizit zu machen und unintuitive Sachverhalte ggf. mithilfe von Beispielen zu verdeutlichen.

# 2 Erläuterungen - algebraischer Teil des Beweises

Im ersten Teil des Beweises werden wir einen nicht-kommutativen Schiefkörper $R$ konstruieren und ihn in verschiedene Mengen unterteilen (Zentrum, Zentralisatoren, Konjugationsklassen). Die zulässige Interpretation von $R$ als Vektorraum über seinem eigenen Zentrum ermöglicht uns in Kombination mit den o.g. Konzepten sehr präzise Schlussfolgerungen über gewisse Teilbarkeitsbeziehungen innerhalb der Menge $R$.

## 2.1 Gruppen, Körper, Schiefkörper

Für eine Menge mit einer zweistelligen Verknüpfung $(M, \circ)$ können folgende Strukturgesetze gelten:

1. Innere Verknüpfung: $\forall a, b \epsilon M : a \circ b \epsilon M$
2. Assoziativität: $\forall a, b, c \epsilon M : (a \circ b) \circ c = a \circ (b \circ c)$
3. Neutrales Element: $\exists e \epsilon M \wedge \forall a \epsilon M : e \circ a = a \circ e = a$
4. Inverses Element: $\forall a \epsilon M \wedge \exists a^{-1} \epsilon M : a^{-1} \circ a = a \circ a^{-1} = e$
5. Kommutativität: $\forall a, b \epsilon M : a \circ b = b \circ a$

Für den Beweiszusammenhang wesentlich ist an dieser Stelle die Unterscheidung von **Gruppen** und **abelschen Gruppen**: Eine Gruppe erfüllt die Gesetze 1 bis 4, eine abelsche erfüllt darüber hinaus auch das Gesetz der Kommutativität.

Eine Menge mit zwei zweistelligen Verknüpfungen $(M, \odot, \oplus)$ ist genau dann ein **Körper**, wenn gilt:

1. $(M, \oplus)$ ist abelsche Gruppe.
2. $(M, \odot)$ ohne das neutrale Element bzl. $\oplus$ ist abelsche Gruppe.
3. Rechts- und Linksdistributivität ist gegeben.

Ist die Menge lediglich bzgl. ihrer multiplikativen Verknüpfung nicht kommutativ, so handelt es sich nicht um einen Körper sondern um einen **Schiefkörper**. Im Folgenden arbeiten wir mit dem angenommenen endlichen, nicht-kommutativen Schiefkörper $R$, also einer gegebenen endlichen Menge, die bzgl. ihrer additiven Verknüpfung eine abelsche Gruppe bildet und bzgl. ihrer multiplikativen Verknüpfung nicht kommutativ, also nicht-abelsch ist. Wenn von der Gruppe $R$ gesprochen wird, so ist stets die multiplikative Gruppe gemeint.

## 2.2 Zentrum und Zentralisatoren einer Gruppe

Der Zentralisator $C_s$ der Gruppe $R$ zu einem bestimmten Element $s \epsilon R$ sei folgendermaßen definiert:

$$C_s := \{x \epsilon R : xs = sx\} \tag{2.1}$$

$C_s$ ist also eine Untermenge von $R$, welche alle Elemente aus $R$ enthält, die zu $s$ bzgl. der Multiplikation kommutativ sind. Da wir in unserer Annahme $R$ so gewählt haben, dass die Kommutativität der Multiplikationsgruppe *nicht* gegeben ist, wissen wir:

$$\exists s : |C_s| < |R| \tag{2.2}$$

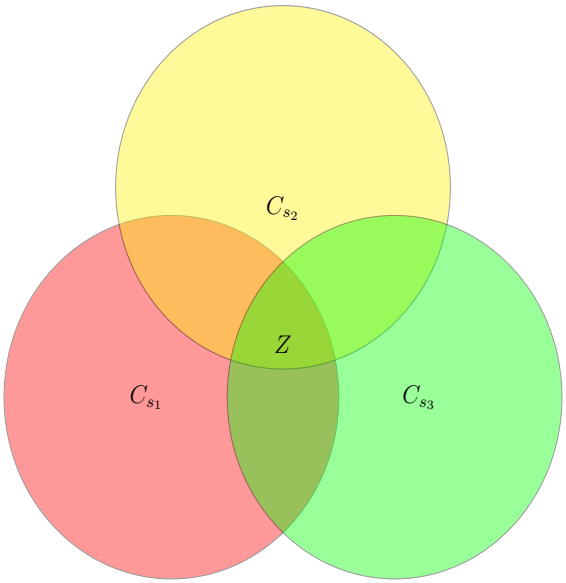
Bildet man nun über alle Zentralisatoren $C_s$ eine Schnittmenge, so erhält man das Zentrum $Z$ der Gruppe R:

$$Z(R) := \bigcap_{s \epsilon R} C_s \tag{2.3}$$

$Z$ ist also die Menge aller zu allen anderen Elementen aus R bzgl. Multiplikation kommutativer Elemente:

$$Z\,(R) := \{z \epsilon R | \forall x \epsilon R : xz = zx\} \tag{2.4}$$

Damit ist $Z(R)$ gemäß unserer Annahmen für $R$ ein Körper.



## 2.3 Der Schiefkörper als Vektorraum über seinem Zentrum – Dimensionen und Mächtigkeiten

Wesentlich im Sinne der späteren Beweisführung ist das Verhältnis von Mächtigkeiten der Menge R und ihrer Zentralisatoren. Zu diesem Zweck betrachten wir sowohl $R$ als auch $C_s$ als Vektorräume über dem Zentrum Z:

$$\begin{aligned} R(Z,+,\cdot) \text{ mit der Skalarmultiplikation } \odot &: Z \times R \to R \\ \text{und der Vektoraddition } \oplus &: R \times R \to R \\ C_s(Z,+,\cdot) \text{ mit der Skalarmultiplikation } \odot &: Z \times C_s \to C_s \\ \text{und der Vektoraddition } \oplus &: C_s \times C_s \to C_s \end{aligned}$$

Die Mächtigkeit des Zentrums $Z(R)$ (2.4) sei $q$:

$$|Z| = q \tag{2.5}$$

Da wir $R$ (mit der Menge $R$ über dem Körper $Z$ (2.4)) als einen Vektorraum betrachten können, können wir von einer Anzahl an Basisvektoren $n \epsilon \mathbb{N}$ ausgehen und somit Rückschlüsse über die Mächtigkeit von R ziehen:

$$|R| = |Z| \odot (v_1) \oplus \ldots \oplus |Z| \odot (v_n) \tag{2.6}$$

$$\Rightarrow |R| = q \odot (v_1) \oplus \ldots \oplus q \odot (v_n) \tag{2.7}$$

$$\Rightarrow |R| = q^n \tag{2.8}$$

Mit derselben Argumentation erhalten wir die Mächtigkeit eines beliebigen Zentralisators von R, indem wir die Anzahl an Basisvektoren mit $n_s$ benennen:

$$|C_s| = q^{n_s} \tag{2.9}$$

Wir wissen außerdem, dass die Anzahl der Basisvektoren mindestens eines Zentralisators $C_s$ kleiner sein muss als die Anzahl der Basisvektoren von $R$ (siehe (2.2), (2.7)), dass es also mindestens ein s gibt, für das gilt:

$$n_s < n \tag{2.10}$$

Denn wäre $n_s$ immer gleich $n$, so wäre jeder Zentralisator gleich der Menge $R$, was bedeutete, dass sich alle Elemente zueinander kommutativ verhielten - und das widerspräche unserer Annahme für $R$.

## 2.4 Zerlegung von $R^*$ in Konjugationsklassen

Im nächsten Schritt geht es in erster Linie um Teilbarkeitsbeziehungen (um jenen Aspekt also, über den am Ende der Beweis durch Widerspruch durchgeführt werden wird).

Dazu zerlegen wir die Menge $R^*$, also die Menge $R$ ohne ihr additives Null-Element, in Konjugationsklassen. Eine bestimmte Konjugationsklasse zu einem bestimmen Element $s$ aus $R$ beinhaltet dabei alle Elemente, die durch die Konjugationsoperation von s mit allen anderen Elementen aus $R^*$ entstehen (dass es hierbei zu jedem $x \epsilon R$ sein Inverses geben muss, ist Teil unseres Postulats):

$$A_s := \{x^{-1}sx : x \epsilon R^*\} \tag{2.11}$$

### 2.4.1 Beweis: Konjugationsklassen sind Äquivalenzklassen

Wir können an dieser Stelle zeigen, dass diese Konjugationsklassen Äquivalenzklassen sind - dass also zwei angenommene, verschiedene Klassen ein und dieselbe Klasse sein müssen, sobald sie ein gemeinsames Element besitzen. Dieses angenommene, gemeinsame Element sei für die erste Klasse durch $x^{-1}rx$ dargestellt und in der zweiten Klasse durch $y^{-1}sy$. Die verschiedenen Darstellungen desselben Elementes können wir gleichsetzen:

$$\begin{aligned} x^{-1}rx &= y^{-1}sy \\ \Leftrightarrow rx &= xy^{-1}sy \\ \Leftrightarrow r &= xy^{-1}syx^{-1} \end{aligned} \tag{2.12}$$

Wir setzen: $z = yx^{-1}$. Dann gilt: $z^{-1} = xy^{-1}$. Und damit gilt:

$$r = z^{-1}sz \tag{2.13}$$

Damit lässt sich jedes Element aus der ersten Klasse auch als Element der zweiten darstellen und umgekehrt.

Es folgt der Beweis, dass die Vereinigungsmengen der Konjugationsklassen die gesamte Gruppe bilden: Es muss gezeigt werden, dass jedes Element $y$ die Darstellung $x^{-1}rx$

hat für ein $x$ und ein $r$:

$$\begin{aligned} y &= x^{-1}rx \\ \Leftrightarrow xy &= rx \\ \Leftrightarrow xyx^{-1} &= r \end{aligned} \tag{2.14}$$

Wähle also ein beliebiges $x$ und setze $r = xyx^{-1}$. Dann gilt: $y = x^{-1}rx$. Also hat jedes y die gewünschte Darstellung.

### 2.4.2 Konjugationsklassen und Zentralisatoren in $R^*$ - Mächtigkeiten

Zur Veranschaulichung des letzten und des nun folgenden Unterkapitels für den Beweiszusammenhang sei an dieser Stelle bemerkt, dass die Zerlegung eines endlichen Körpers in seine Konjugationsklassen natürlich genau so viele Klassen hervorbringt wie der Körper Elemente hat - jedes Element ist gleichzeitig seine eigene Klasse. Das ist gemäß unseres Postulats für $R^*$ nicht der Fall - somit könnte eine Bildung von Äquivalenzklassen durch Konjugation Aufschluss über das Verhältnis von Mächtigkeiten geben. Wir betrachten also im Folgenden die Abbildung von $R^*$ auf $A_s$

$$f_s : x \mapsto x^{-1}sx \;\; \text{mit } x, s \epsilon R^* \tag{2.15}$$

und fragen: Gegeben sei ein $s \epsilon R^*$ und ein $x \epsilon R^*$. Wieviele andere Elemente aus $R^*$ bilden $s$ auf denselben Wert ab wie das gegebene $x$? Wir setzen $y$ als solch ein anderes Element und formulieren diese Frage als Gleichung:

$$\begin{aligned} x^{-1}sx &= y^{-1}sy \\ \Leftrightarrow (yx^{-1})s &= s(yx^{-1}) \\ \Leftrightarrow (yx^{-1}) &\epsilon C_s^* \end{aligned} \tag{2.16}$$

Wenn wir an dieser Stelle an jedes Element aus der Menge $C_s^*$ von rechts das Element $x$ konjugieren, so erhalten wir die Menge $C_s^*x = \{zx : z \epsilon C_s^*\}$, welche die gleiche Mächtigkeit wie $C_s^*$ besitzt und für die gilt:

$$y \epsilon C_s^* x \tag{2.17}$$

Die Beantwortung der Frage lautet also: Es bilden immer genau $|C_s^*|$ viele Elemente ein gegebenes $s$ auf denselben Wert ab:

$$|R^*| = |A_s||C_s^*| \tag{2.18}$$

Diesen Sachverhalt werden wir im Abschnitt 2.5 anhand eines Beispiels untersuchen. Bei der Betrachtung von $R$ und $C_s$ als Vektorräume über dem Zentrum $Z$ hatten wir bereits konkrete Mächtigkeiten formuliert (vgl. (2.8)) und (2.9)), sodass wir wissen:

$$|R^*| = q^n - 1 \tag{2.19}$$

$$|C_s^*| = q^{n_s} - 1 \tag{2.20}$$

Die Gleichung (2.18) lässt sich somit konkretisieren:

$$\frac{|R^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s| \tag{2.21}$$

Wir wissen, dass die Mächtigkeit von $A_s$, also die Anzahl der Elemente in einer Äquivalenzklasse immer eine natürliche Zahl ist. Daher wissen wir auch, dass die Mächtigkeit jedes Zentralisators die Mächtigkeit von $R^*$ teilt:

$$(q^{n_s} - 1)|(q^n - 1) \tag{2.22}$$

Im Folgenden fassen wir jene Klassen mit der Mächtigkeit $= 1$ zusammen (jene Klassen

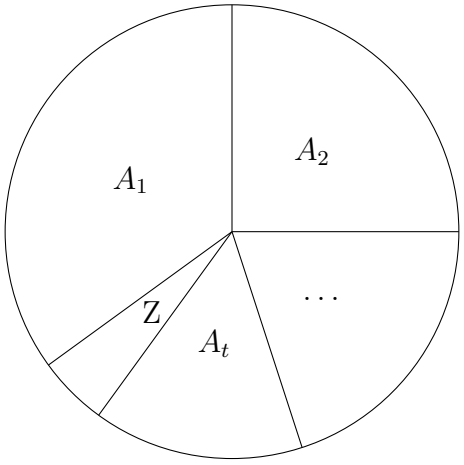



Abbildung 1: $R^*$ unterteilt in $Z$ und $A_{1..t}$

bestehen bekanntlich aus jenen Elementen, die mit allen anderen multiplikativ kommu-

tativ sind) zum Zentrum $Z$. Klassen mit einer Mächtigkeit $> 1$ fassen wir zusammen als insg. $t$ Äquivalenzklassen (vgl. Abbildung 1):

$$|R^*| = |Z^*| + \sum_{k=1}^{t} |A_k| \tag{2.23}$$

Wir können aus (2.23), (2.5), (2.20) und (2.21) folgern:

$$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1} \tag{2.24}$$

$$\text{mit } \frac{q^n - 1}{q^{n_k} - 1} > 1 \tag{2.25}$$

$$\text{und } \frac{q^n - 1}{q^{n_k} - 1} \epsilon N \tag{2.26}$$

Die Gleichung (2.24) wird **Klassenformel** genannt - wir werden im zweiten Teil der Erläuterungen auf diese Gleichung zurückgreifen.
Aus der Teilbarkeitsbeziehung $q^{n_k} - 1 | q^n - 1$ werden wir jetzt die Teilbarkeitsbeziehung $n_k | n$ ableiten. Dazu formulieren wir $n$ als eine zusammengesetzte Zahl aus $n_k$:

$$n = an_k + r \text{ mit } 0 \leq r < n_k \text{ und } a, r \epsilon \mathbb{N} \tag{2.27}$$

$r$ ist hierbei so gewählt, dass das Vielfache von $n_k$ stets durch $a$ angegeben ist. Wir formulieren die Teilbarkeitsbeziehung $q^{n_k} - 1 | q^n - 1$ also folgendermaßen:

$$q^{n_k} - 1 | q^{an_k + r} - 1 \tag{2.28}$$

Die Teilbarkeit ist nach wie vor gegeben, wenn der Teiler ein mal subtrahiert wird:

$$q^{n_k} - 1 | (q^{an_k + r} - 1) - (q^{n_k} - 1) \tag{2.29}$$

Durch Ausklammern ergibt sich:

$$q^{n_k} - 1 | q^{n_k} (q^{(a-1)n_k + r} - 1) \tag{2.30}$$

Da $q^{n_k}$ und $q^{n_k} - 1$ relativ prim sind, dürfen wir folgern:

$$q^{n_k} - 1 | (q^{(a-1)n_k + r} - 1) \tag{2.31}$$

An dieser Stelle wiederholen wir den Vorgang ab (2.28), subtrahieren also einmal den Teiler und klammern aus bis wir nicht weiter reduzieren können und erhalten:

$$q^{n_k} - 1 | (q^r - 1) \tag{2.32}$$

Dies ist gemäß unseren Anforderungen für $r$ (siehe (2.27)) nur für $r = 0$ möglich, sodass wir wissen:

$$n_k | n \quad \text{für jedes } k. \tag{2.33}$$

## 2.5 Exkurs: Kleinste nicht-kommutative Gruppe $S3$

Zur Veranschaulichung des Zusammenhangs der Mächtigkeiten von Zentralisatoren und Äquivalenzklassen einer Menge (siehe (2.18)) wählen wir die kleinste nicht-kommutative Gruppe, die Symmetrische Gruppe $S3$ mit den in Abbildung 2 dargestellten Drehungen und Spiegelungen als Elemente - e ist hierbei das neutrale Element:

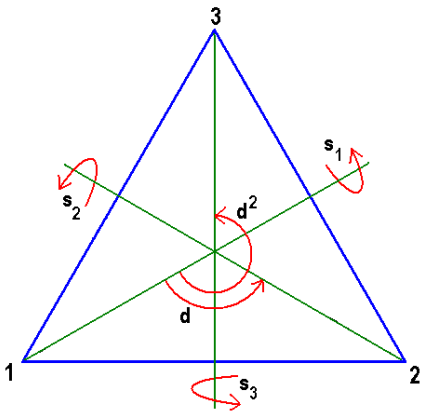
$$S3 = \{e, d, d^2, s_1, s_2, s_3\}$$

Wir bilden die entsprechenden Mengen, also alle Zentralisatoren $C$ und Konjugations-

Abbildung 2: Spiegelungen und Drehungen der Symmetrischen Gruppe $S3$

| * | e | d | d² | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|---|---|---|
| e | e | d | d² | $s_1$ | $s_2$ | $s_3$ |
| d | d | d² | e | $s_3$ | $s_1$ | $s_2$ |
| d² | d² | e | d | $s_2$ | $s_3$ | $s_1$ |
| $s_1$ | $s_1$ | $s_2$ | $s_3$ | e | d | d² |
| $s_2$ | $s_2$ | $s_3$ | $s_1$ | d² | e | d |
| $s_3$ | $s_3$ | $s_1$ | $s_2$ | d | d² | e |

(a) Multiplikationstabelle




(b) Elemente von $S3$

klassen $A$ gemäß der Multiplikationstabelle in Abbildung 2:

$$\begin{aligned} A_d = A_{d^2} &= \{d, d^2\} \\ C_d = Cd^2 &= \{e, d, d^2\} \\ A_{s_1} &= \{s_1, s_2, s_3\} \\ C_{s_1} &= \{e, s_1\} \text{ analog für } s_2, s_3 \\ A_e &= \{e\} \\ C_e &= \{e, d, d^2, s_1, s_2, s_3, \} \end{aligned} \tag{2.34}$$

Es lässt sich nun für jedes gewählte $s$ die Gleichung $|R^*| = |A_s||C_s^*|$ (2.18) exemplarisch nachrechnen: $|A_d| * |C_d| = 2 * 3 = 6 = |S3|$ (ein additives Nullelement ist in dieser Menge nicht enthalten). Die mögliche Aussagekraft von Konjugationsklassen über die algebraische Struktur von nicht-kommutativen Gruppen wird an diesem Beispiel deutlich, da die hier untersuchte Gesetzmäßigkeit (das Verhältnis der Mächtigkeiten) in ihrer Symmetrie anschaulich wird.

# 3 Erläuterungen - Kreisteilungspolynom

Der zweite Teil des Beweises findet sich in der Mathematik der komplexen Zahlen und ihrer grafischen Darstellung in der zweidimensionalen Ebene.

Wir werden zunächst komplexe Zahlen und ihre grafische Darstellung einführen. Danach werden wir mithilfe dieser Darstellung die Lösungen der Gleichung $x^n = 1$ visualisieren und so das Konzept des Kreisteilungspolynoms $\phi_d(x)$ erläutern. Auch hierbei lassen sich präzise Aussagen über Teilbarkeitsbeziehungen formulieren, welche wir abschließend in Bezug zu den Ergebnissen des vorherigen Abschnitts setzen.

## 3.1 Komplexe Zahlen und die komplexe Ebene

Der Zahlenraum der komplexen Zahlen $\mathbb{C}$ stellt eine Erweiterung des Zahlenraumes der reellen Zahlen $\mathbb{R}$ dar. Die komplexe Zahl $i \equiv \sqrt{-1}$ erweitert den Raum der reellen Zahlen um eine Dimension, sodass wir uns den Raum $\mathbb{C}$ als $\mathbb{R}^2$ vorstellen können. Konkret besteht eine komplexe Zahl $z$ aus reellem und komplexen Part:

$$z = a + ib, \tag{3.1}$$

wobei $a, b \in \mathbb{R}$ und, wie eingeführt, $i = \sqrt{-1}$. Bleiben wir bei der Darstellung von $\mathbb{C}$ durch einen $\mathbb{R}^2$, so lässt sich jede Zahl $z$ als Punkt auf einer komplexen Ebene mit Koordinaten $(a, b)$ darstellen. Somit ergibt sich ebenfalls die Möglichkeit, jede Komplexe Zahl $z$ in

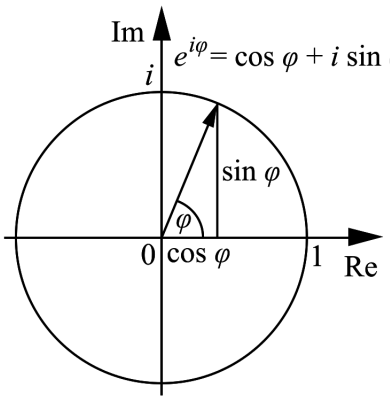



Abbildung 3: Der Einheitskreis in der komplexen Ebene: $\mathbb{C}$ wird dargestellt durch einen $\mathbb{R}^2$.

Polarkoordinaten auszudrücken. Wir schreiben

$$a \equiv r\cos\theta, \tag{3.2}$$

$$b \equiv r\sin\theta, \tag{3.3}$$

und somit

$$z = a + ib = r\,(cos\theta + i\sin\theta) = re^{i\theta}, \tag{3.4}$$

wobei die letzte Gleichheit durch eine Taylor Entwicklung der Exponentialfunktion gezeigt werden kann. Im Folgenden setzen wir, ohne an Allgemeingültigkeit zu verlieren, $r = 1$.[1] Sei nun $\theta \in (0, 2\pi)$, so zeichnet die Gleichung $z = e^{i\theta}$ einen Einheitskreis in der komplexen Ebene, wie in Abbildung 3 zu sehen.

Es gilt folglich, da wir ja $r = 1$ gesetzt hatten, $|z| = 1$. Im nächsten Abschnitt wollen wir die Gleichung $x^n = 1$ anschauen und mit dem hier eingeführten Einheitskreis in Verbindung bringen.

## 3.2 Das $n$-Eck in der komplexen Ebene: Ein Beispiel

Gegeben sei die Gleichung

$$x^n = 1. \tag{3.5}$$

[1] Im Prinzip lassen sich folgende Überlegungen für beliebiges $r$ durchführen. Die zu lösende Gleichung lautete dann $x^n = r$.

Nach dem Fundamentalsatz der Algebra hat Gleichung (3.5) $n$ Lösungen, bzw. Nullstellen, in $\mathbb{C}$. Anders ausgedrückt: Wir können Gleichung (3.5) umformen und in $n$ Linearfaktoren zerlegen:

$$x^n - 1 = 0 \tag{3.6}$$
$$(x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_n) = 0, \tag{3.7}$$

wobei $\lambda_n \in \mathbb{C}$. Nehmen wir zur Veranschaulichung nun das Beispiel

$$x^4 - 1 = 0. \tag{3.8}$$

Wir faktorisieren diese Gleichung als

$$(x - \lambda_1)(x - \lambda_2)(x - \lambda_3)(x - \lambda_4) = 0, \tag{3.9}$$

und identifizieren die Nullstellen $\lambda_n$ wie folgt:

$$(x - 1)(x - (-1))(x - i)(x - (-i)) = 0. \tag{3.10}$$

Die Nullstellen der Gleichung $x^4 - 1 = 0$ sind also

$$\lambda_1 = 1 + 0 \cdot i, \tag{3.11}$$
$$\lambda_2 = -1 + 0 \cdot i, \tag{3.12}$$
$$\lambda_3 = 0 + 1 \cdot i, \tag{3.13}$$
$$\lambda_4 = 0 + (-1) \cdot i. \tag{3.14}$$

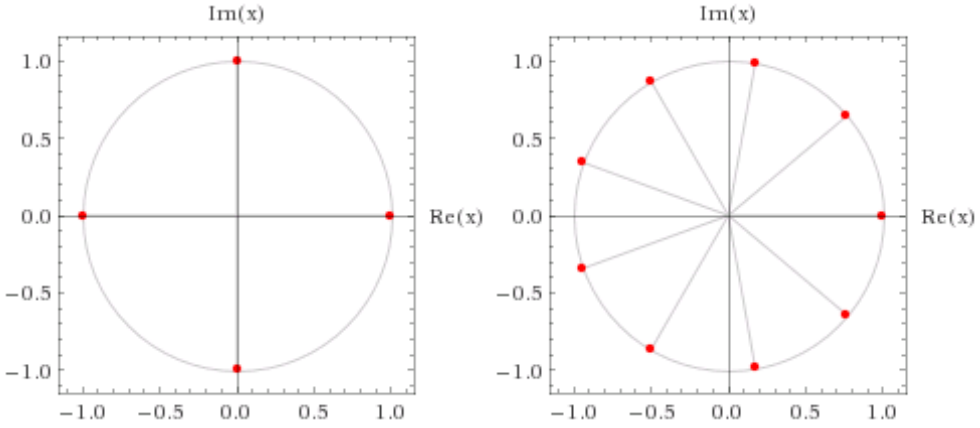
Stellen wir diese vier Zahlen in der komplexen Ebene dar, so erhalten wir Abbildung 4a.

Wir erkennen, dass die Nullstellen der Gleichung (3.8) ein Viereck in der komplexen Ebene bezeichnen. Man erkennt leicht, dass alle Nullstellen der Gleichung $x^n - 1 = 0$ auf dem Einheitskreis in der komplexen Ebene liegen müssen.[2] Die Nullstellen $\lambda_n$ bezeichnen daher ein $n$-Eck im $\mathbb{R}^2$.

Zuletzt betrachten wir Folgendes: Die Nullstelle $\lambda_1 = 1 + 0 \cdot i$ löst alle Gleichungen $x^n - 1 = 0$ für $n \in \mathbb{N}^*$. Da diese Nullstelle bereits die Gleichung $x^1 - 1 = 0$ löst, sagt man, dass sie Nullstelle erster Ordnung ist. In anderen Worten: Eine beliebige Nullstelle $\lambda_n$ der Gleichung $x^n - 1 = 0$, die bereits die Gleichung $(\lambda_n)^d - 1 = 0$ mit $d < n$ löst, hat Ordnung $d$. Im obigen Beispiel $x^4 - 1 = 0$ hat also $\lambda_1$ die Ordnung 1, $\lambda_2$ die Ordnung 2, $\lambda_3$ die

[2] Dies folgt aus der Bedingung $r = 1$, die wir vorausgesetzt hatten, um uns eben auf den Einheitskreis zu beschränken.

Abbildung 4: Darstellungen des Einheitskreises in der komplexen Ebene als n-Eck




(a) Die Nullstellen $\lambda_1, \ldots, \lambda_4$ von (3.8) als Punkte im Einheitskreis der komplexen Ebene.

(b) Nullstellen der Gleichung $x^9 - 1 = 0$.

Ordnung 4 und $\lambda_4$ ebenfalls die Ordnung 4, da z.B. bereits gilt $(\lambda_3)^4 - 1 = (i)^4 - 1 = 0$.

Grafisch gesprochen: Die Nullstellen der Gleichung $x^2 - 1 = 0$ bilden in der Komplexen Ebene ein 'Zweieck', also eine Strecke; betrachten wir nun die Gleichung $x^4 - 1 = 0$ so kommen zwei Punkte in der komplexen Ebene hinzu. Zwar formen alle vier Punkte nun zusammen ein Viereck, aber nur die beiden neuen Punkte sind vierter Ordnung, da die beiden Punkte $x = 1, -1$ bereits das 'Zweieck' formten, also Gleichungen niedrigerer Ordnung lösten.[3]

## 3.3 Kreisteilungspolynom

Nun führen wir das Konzept des Kreisteilungspolynoms ein. Multiplizieren wir alle Nullstellen einer Gleichung $x^n - 1 = 0$ gleicher Ordnung miteinander, so erhalten wir ein Polynom, welches Kreisteilungspolynom genannt wird. Aus unserem Beispiel $x^4 - 1 = 0$ ergeben sich

$$\phi_1 = x - 1, \tag{3.15}$$

$$\phi_2 = x + 1, \tag{3.16}$$

$$\phi_4 = x^2 + 1. \tag{3.17}$$

Generell gilt:

$$\phi_d = \prod_{\lambda_d} (x - \lambda) \tag{3.18}$$

[3]Sie sind erster und zweiter Ordnung.

Unser Beispiel $x^4 - 1 = 0$ können wir auch schreiben als

$$x^4 - 1 = \phi_1 \cdot \phi_2 \cdot \phi_4 = 0. \tag{3.19}$$

Wir können also ein beliebiges $n$-Eck in der komplexen Ebene als Produkt der Kreisteilungspolynome definieren:

$$x^n - 1 = \prod_{d|n} \phi_d(x) \tag{3.20}$$

Dies ist ein Beispiel des Satzes von Lagrange, dass die Ordnung jedes Elements einer Gruppe die Ordnung der Gruppe teilt, und stellt die zentrale Eigenschaft von Kreisteilungspolynomen dar. Nun manipulieren wir (3.20) und ziehen das Polynom $\phi_n(x)$ aus dem Produkt:

$$x^n - 1 = \phi_n(x) \prod_{d|n, d\neq n} \phi_d(x) \tag{3.21}$$

Im nächsten Schritt ziehen wir alle Polynome der Ordnung $n_k$ oder kleiner, also den Ausdruck $(x^{n_k} - 1)$ aus dem Produkt:

$$x^n - 1 = (x^{n_k} - 1)\phi_n(x) \prod_{d|n, d\neq n, d\nmid n_k} \phi_d(x) \tag{3.22}$$

Umgeformt ergibt sich:

$$\frac{x^n - 1}{x^{n_k} - 1} = \phi_n(x) \prod_{d|n, d\neq n, d\nmid n_k} \phi_d(x) \tag{3.23}$$

Gleichung (3.22) stellt eine Faktorisierung von $x^n - 1 = 0$ dar. Deshalb gilt:

$$\phi_n(x) | x^n - 1 \tag{3.24}$$

Gleichung (3.23) stellt eine Faktorisierung von $(x^n - 1)/(x^{n_k} - 1)$ dar. Dementsprechend gilt gleicherweise:

$$\phi_n(x) | \frac{x^n - 1}{x^{n_k} - 1} \tag{3.25}$$

Mithilfe der **Klassenformel** (2.24) können wir eine weitere Teilbarkeitsbeziehung behaupten. Wir formen um:

$$(q^n - 1) - \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1} = q - 1$$

Da $\phi_n(q)$ bekanntlich die linke Seite der hier umgestellten Klassenformel teilt (sowohl den ersten Summanden, vgl. (3.24)) als auch den zweiten Summanden, vgl. (3.25) und

(2.33)), muss $\phi_n(q)$ zwangsläufig auch die rechte Seite der Klassenformel teilen:

$$\phi_n(q) \mid (q^n - 1) \quad \wedge \quad \phi_n(q) \mid \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}$$
$$\Rightarrow \ \phi_n(q) \mid (q - 1) \tag{3.26}$$

Ernst Witt formuliert diese für den Beweis wesentliche Schlussfolgerung folgendermaßen:

> $q - 1$ *muss hierbei durch* $|\phi_n(q)|$ *teilbar sein, denn alle anderen Glieder sind es.*

$\phi_n(q)$ muss also $\phi_1(q)$ teilen (3.26) und zwar für alle n. Dies ist ein Widerspruch - bis auf einen Fall: für $n = 1$ stimmt die Schlussfolgerung.

Dass es sich um einen Widerspruch handelt, wissen wir durch die Konstruktion der Kreisteilungspolynome, siehe (3.18) und (3.20). Klar ist, dass $\phi_2(q) > \phi_1(q)$. Auch wissen wir, dass der Grad von $\phi_{n>2}$ immer grösser ist als der Grad von $\phi_1$.[4] Daraus folgt, dass $\phi_n$ nur dann $\phi_1$ teilen kann, wenn $n = 1$. Das wiederum bedeutet, *"dass das abelsche Zentrum mit der ganzen Multiplikationsgruppe zusammenfällt"* [1].

Wir haben also nicht nur einen Widerspruch, sondern aus dem Widerspruch lässt sich die falsche Annahme inklusive ihrer Korrektur direkt ablesen, was wir im nächsten und finalen Abschnitt unternehmen und so den Beweis noch einmal Revue passieren lassen.

[4] Aigner zeigt, dass die Koeffizienten $c_i$ der Polynome $\phi_n$ ganze Zahlen sind mit $c_i = -1, 1$. Daraus folgt, dass $\phi_{1,2}$ die einzigen Kreisteilungspolynome vom Grad 1 sein müssen. Dementsprechend haben alle $\phi_{n>2}$ einen Grad $> 1$. Siehe [2], S.38

# 4 Zusammenfassende Beweisführung

Wir haben zu Beginn den endlichen, nicht-kommutativen Schiefkörper $R$ behauptet und sein Verhältnis zu seinen (in der Folge ebenfalls behaupteten) Zentralisatoren untersucht. Durch die Betrachtung dieses Schiefkörpers und seiner Zentralisatoren als Vektorräume über dem Zentrum des Schiefkörpers konnten wir (unter Zuhilfenahme der Konjugationsklassen) schlussfolgern, dass die Dimensionalität eines jeden Zentralisators die Dimensionalität von $R$ teilt - jeweils ohne das additive Nullelement und jeweils als Vektorraum über $Z$, vgl. hierzu (2.22).
Statt von der Dimensionalität von $R$ kann man auch von der *"Ordnung der Multplikationsgruppe"*[5] sprechen, wodurch der Zusammenhang zum zweiten Teil des Beweises auch begrifflich deutlicher wird. Der Ausdruck $\phi_n(q)|q-1$ (siehe (3.26)) ist nur für den Fall richtig, dass $n = 1$ ist. Das wiederum bedeutet, dass die Dimensionalität des betrachteten Vektorraums 1 beträgt, der Vektorraum also gleich seinem Körper $Z$ sein muss - und wenn dass Zentrum eines Schiefkörpers der Schiefkörper selbst ist, ist für jedes Element dieses Schiefkörpers multiplikative Kommutativität gegeben - und damit ist der Schiefkörper kein Schiefkörper mehr, sondern ein Körper.

[5] siehe Originalbeweis durch Ernst Witt [1]

# Literatur

[1] E. Witt, "Über die Kommutativität endlicher Schiefkörper" *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 8, no. 1, pp. 413–413, 1931.

[2] M. Aigner, K. Hofmann, and G. Ziegler, *Das BUCH der Beweise*. Springer Berlin Heidelberg, 2013.