GEOMETRISCHE KONSTRUKTIONEN UND TRANSZENDENTE ZAHLEN

JENS FRANKE, MATHEMATISCHES INSTITUT, RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

Version 0.2

Die folgenden Ausführungen sollen als Grundlage für ein Seminar über die Beweise der Unlösbarkeit der klassischen geometrischen Konstruktionsprobleme (Verdoppelung des Würfels, Drittelung des Winkels, Quadratur des Kreises) dienen, das im Sommersemester 2016 für Studenten des zweiten Semesters stattfinden soll. Wir folgen im Prinzip der gängigen Vorgehensweise für diese Beweise, die man in vielen Lehrbüchern findet. In der Regel behandelt man aber diese Fragen im Zusammenhang mit einer Vorlesung, die in die Galoissche Theorie der Körpererweiterungen einführt oder darauf aufbaut. Entsprechend hoch sind dann auch Anforderungen, die an die Kenntnisse aus anderen Bereichen der Mathematik, zum Beispiel der aus elementaren komplexen Analysis, gestellt werden.

Um einen guten Anschluß an die Vorlesung „Lineare Algebra I“ des Wintersemesters 2015/16 zu ermöglichen und mit möglichst wenig Material aus der Analysis auszukommen, soll daher der folgende Text als Grundlage des Seminares dienen.

Ich danke Herrn N. Mertens und ganz besonders Frau A. Tarnowsky für Hinweise auf Fehler in der ersten Version.

Inhaltsverzeichnis

1. Einige Resultate der elementaren Zahlentheorie

In den beiden ersten Abschnitten sollen einige einfache zahlentheoretische Fakten über den größten gemeinsamen Teiler, die eindeutige Primfaktorzerlegung ganzer Zahlen sowie die Existenz unendlich vieler Primzahlen gezeigt werden. Dies dürfte zwar bei einem erheblichen Teil der Teilnehmer bekannt sein, ist aber in keiner Modulbeschreibung für eine der Pflichtvorlesungen Programmpunkt und soll daher der Gründlichkeit halber bewiesen werden. Wir benutzen dabei nur das Induktionsprinzip sowie die aus Analysis 1 geläufigen Regeln für die arithmetischen Operationen und Vergleiche reeller Zahlen.

Satz 1 (Eindeutige Division mit Rest)**.** *Seien $A \neq 0$ und n ganze Zahlen, dann ist n eindeutig als $n = qA + r$ mit ganzen Zahlen q und $0 \leq r \leq |A|$ darstellbar.*

Beweis. Wegen $qA+r = (-q)(-A)+r$ darf A durch $-A$ ersetzt und somit $A > 0$ angenommen werden. Angenommen,

$$qA + r = \tilde{q}A + \tilde{r},$$

wobei r und $\tilde{r}$ beide in $[0, A)$ liegen, dann ist $r - \tilde{r} = A(\tilde{q} - q) \in (-A, A)$. Für $\tilde{q} \neq q$ wäre $|A(\tilde{q} - q)| \geq A$, ein Widerspruch. Also gilt $q = \tilde{q}$ und $r = \tilde{r}$, und die Darstellung ist eindeutig.

Zum Beweis der Existenz setzen betrachten wir zunächst $n \geq 0$ und gehen durch Induktion nach n vor. Für $n = 0$ kann $q = r = 0$ genommen werden. Wenn $n - 1 = q'A + r'$ eine Darstellung der gewünschten Art ist, so kann $q = q'$, $r = r' + 1$ für $0 \leq r \leq A - 2$ und $q = q' + 1$, $r = 0$ für $r' = A - 1$ genommen werden. Damit ist die Darstellbarkeit im Fall $n \geq 0$ gezeigt. Für $n < 0$ stellt man $-n = q'A + r'$ dar und nimmt $q = -q'$, $r = 0$ im Falle $r' = 0$ und $q = -q' - 1$, $r' = A - r$ im Fall $r' > 0$. □

Satz 2. *Sei $\Gamma \subseteq \mathbb{Z}$ eine Untergruppe, dann gilt*

$$\Gamma = G\mathbb{Z} = \big\{Gn \;\big|\; n \in \mathbb{Z}\big\}. \tag{1}$$

mit einer eindeutig bestimmten natürlichen Zahl G, und für jede ganze Zahl G ist durch (1) eine Untergruppe von $\mathbb{Z}$ gegeben.

Beweis. Die letzte Behauptung ist einfach. Sei umgekehrt $\Gamma \subseteq \mathbb{Z}$ eine Untergruppe. Für $\Gamma = \{0\}$ gilt $\Gamma = 0 \cdot \mathbb{Z}$, und aus $G \cdot \mathbb{Z} = \{0\}$ folgt $G = 0$ wegen $G \in G \cdot \mathbb{Z}$. Der Fall $\Gamma = \{0\}$ ist damit erledigt, und wir setzen $\Gamma \neq \{0\}$ voraus.

In diesem Fall enthält Γ von 0 verschiedene Elemente. Da $-g \in \Gamma$ aus $g \in \Gamma$ folgt, enthält Γ positive ganze Zahlen. Sei G das kleinste positive Element von Γ. Wir behaupten, daß $\Gamma = G \cdot \mathbb{Z}$ gilt. Sei dazu $\gamma \in \Gamma$. Nach der Division mit Rest gilt

$$\gamma = Gn + r$$

mit ganzen Zahlen n und $0 \leq r < G$. Wegen $G, \gamma \in \Gamma$ und $n \in \mathbb{Z}$ folgt $r = \gamma - Gn \in \Gamma$. Auf Grund der Minimalität von G folgt $r = 0$, also $\gamma = Gn \in G \cdot \mathbb{Z}$. Also gilt $\Gamma \subseteq G \cdot \mathbb{Z}$. Wegen $G \in \Gamma$ gilt andererseits $G \cdot \mathbb{Z} \subseteq \Gamma$. Damit ist die Existenz von G gezeigt. Zum Beweis der Eindeutigkeit von G nehmen wir $\Gamma = G \cdot \mathbb{Z}$ mit $G \geq 0$ an und zeigen, daß G das kleinste positive Element von Γ ist. Wegen $\Gamma \neq \{0\}$ gilt $G \neq 0$, und G ist positiv. Wenn $\gamma \in \Gamma$ positiv

ist, gilt $\gamma = Gn$ mit $n \in \mathbb{Z}$. Wegen der Positivität von γ gilt $n \geq 1$ und $\gamma = nG \geq G$. Alle Behauptungen sind damit gezeigt. □

Wir nennen die im vorigen Satz konstruierte natürliche Zahl G den *nichtnegativen Erzeuger* von Γ.

Satz 3 (Existenz des ggT)**.** *Für zwei beliebige ganze Zahlen a und b existiert eine eindeutig bestimmte natürliche Zahl n mit den folgenden Eigenschaften:*

- *n ist Teiler von a und von b.*
- *Wenn $m \in \mathbb{Z}$ Teiler von a und von b ist, so ist m ein Teiler von n.*

Wir nennen n den größten gemeinsamen Teiler *von a und b und schreiben $n = \mathrm{ggT}(a, b)$.*

Beweis. Zum Beweis der Existenz von n sei

$$\Gamma = a \cdot \mathbb{Z} + b \cdot Z = \left\{ k \cdot a + l \cdot b \;\middle|\; k, l \in \mathbb{Z} \right\},$$

dann ist Γ eine Untergruppe von $\mathbb{Z}$, welche a und b enthält. Sei n der nichtnegative Erzeuger von Γ. Die erste Eigenschaft des ggT folgt daraus, daß a und b als Elemente von $\Gamma = n\mathbb{Z}$ beide Vielfache von n sind. Wenn m ein Teiler von a und von b ist, so folgt aus der Definition von Γ, daß alle Elemente von Γ Vielfache von m sind. Insbesondere gilt dies für $n \in \Gamma$, und n erfüllt auch die zweite Eigenschaft des ggT.

Angenommen, die beiden natürlichen Zahlen n und n' erfüllen beide die obigen Eigenschaften des $\mathrm{ggT}(a, b)$. Dann gilt $n|n'$ und $n'|n$. Wir zeigen, daß daraus $n = n'$ folgt. Wenn $n = 0$ ist, so ist n' als Vielfaches von n ebenfalls 0. Analog dazu verschwindet auch n, wenn $n' = 0$ ist. Seien also n und n' beide positiv. Weil jede dieser beiden Zahlen ein Vielfaches der anderen ist, gilt $n = kn'$ und $n' = ln$ mit ganzen Zahlen k und l. Insbesondere $n = kn' = kln$, und Kürzen mit n liefert $kl = 1$. Es folgt $k = l = \pm 1$, wobei das Vorzeichen positiv ist, weil sonst eine der beiden Zahlen n oder n' negativ wäre. Also $k = l = 1$ und $n = n'$. □

Wir nennen zwei Zahlen a und b teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$ gilt. Man sagt auch, daß a teilerfremd zu b ist. Aus der Beschreibung von $\mathrm{ggT}(a, b)$ als der nichtnegative Erzeuger von $a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$ folgt:

Folgerung 1. *Zwei ganze Zahlen a und b sind genau dann teilerfremd, wenn $a \cdot \mathbb{Z} + b \cdot \mathbb{Z} = \mathbb{Z}$ gilt. Dies ist genau dann der Fall, wenn $1 \in a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$ gilt, maW, wenn 1 eine ganzzahlige Linearkombination von a und b ist.*

Folgerung 2. *Wenn n teilerfremd zu jeder der ganzen Zahlen a und b ist, so ist n auch zu ab teilerfremd.*

Beweis. Aus unserer Voraussetzung folgt, daß 1 eine ganzahlige Linearkombination von n und a sowie von n und b ist, also

$$1 = kn + la = qn + rb$$

mit ganzen Zahlen k, l, q und r. Also ist

$$1 = kn + 1la = kn + (qn + rb)la = (k + qal)n + rl(ab)$$

eine ganzzahlige Linearkombination aus n und ab. □

Folgerung 3. *Wenn n zu der ganzen Zahl a teilerfremd ist, so ist n auch für alle $k \geq 0$ zu a^k teilerfremd.*

Beweis. Der Fall $k = 0$ läuft auf die ziemlich einfache Tatsache $\mathrm{ggT}(n, 1) = 1$ hinaus, und der allgemeine Fall folgt nach der vorigen Folgerung durch Induktion nach k. □

2. Primzahlen

Bekanntlich versteht man unter einer Primzahl eine natürliche Zahl p, welche durch genau zwei natürliche Zahlen teilbar ist. Das ist äquivalent dazu, daß $p > 1$ gilt und 1 und p die einzigen natürlichen Zahlen sind, welche p teilen. Für ganze Zahlen drückt man diesem Umstand auch kurz durch die Formulierung „p ist prim“ aus.

Satz 1. *Sei p eine Primzahl.*

- *Die ganze Zahl a ist genau dann kein Vielfaches von p, wenn sie zu p teilerfremd ist.*
- *Wenn p kein Teiler von a und von b ist, so ist p kein Teiler von ab.*

Beweis. Weil $\mathrm{ggT}(a, p)$ eine natürliche Zahl ist und p teilt, haben wir $\mathrm{ggT}(a, p) = 1$ oder $\mathrm{ggT}(a, p) = p$. Im ersten Fall sind a und p teilerfremd und a kein Vielfaches von p (sonst wäre p der $\mathrm{ggT}(a, p)$), und im zweiten Fall ist a durch p teilbar. Die zweite Behauptung folgt aus der ersten und Folgerung 1.2. □

Satz 2 (Eindeutige Primfaktorzerlegung)**.** *Jede von 0 verschiedne ganze Zahl n hat eine eindeutige Darstellung*

$$n = \pm \prod_{i=1}^{k} p_i^{e_i} \tag{1}$$

mit einer natürlichen Zahl k und Primzahlen $p_1 < \cdots < p_k$ und positiven ganzen Zahlen e_i.

Bemerkung 1. Die Behauptung ist offenbar äquivalent zur eindeutigen Darstellbarkeit von n als

$$n = \pm \prod_{p} p^{\varepsilon_p}, \tag{2}$$

wobei das Produkt über alle Primzahlen genommen wird und nur endlich viele der ganzen Zahlen ε_p von 0 verschieden sind. In der Tat, im Falle von (1) setzt man $\varepsilon_p = 0$, falls p nicht unter den p_i vorkommt, und $\varepsilon_p = e_i$ für $p = p_i$. Im Fall (2) sei $p_1 < \cdots < p_k$ die Auflistung aller Primzahlen p mit $\varepsilon_p \neq 0$, und man setzt $e_i = \varepsilon_{p_i}$.

Die Menge der als (2) darstellbaren Zahlen ist offenbar abgeschlossen unter Multiplikation. Dasselbe gilt dann auch für die durch (1) darstellbaren Zahlen.

Beweis. Offenbar stimmt das Vorzeichen mit dem Vorzeichen von n überein und ist somit eindeutig, und für den Existenzbeweis kann n durch $-n$ ersetzt werden. Sei also ohne Beschränkung der Allgemeinheit n positiv.

Wir gehen durch Induktion vor und setzen voraus, daß die Behauptung für alle positiven ganzen Zahlen $\tilde{n} < n$ bewiesen ist. Im Fall $n = 1$ kann $k = 0$ genommen werden und für primes

n kann $k = 1$, $p_1 = n$ und $e_1 = 1$ genommen werden. Andernfalls gilt $n = ab$ mit positiven ganzen Zahlen a und b. Auf Grund der Induktionsannahme sind a und b beide in der Form (1) darstellbar. Wie zuvor gesehen, gilt dies dann auch für $n = ab$. Zum Beweis der Eindeutigkeit seien

$$n = \prod_{i=1}^{k} p_i^{e_i} = \prod_{i=1}^{\tilde{k}} \tilde{p}_i^{\tilde{e}_i}$$

zwei Darstellungen als (1). Jeder der Faktoren $\tilde{p}_i$ teilt $n = \prod_{i=1}^{k} p_k e^{e_k}$ und muß daher nach dem vorigen Satz unter $p_1, \ldots, p_k$ vorkommen, also

$$\{\tilde{p}_1, \ldots, \tilde{p}_{\tilde{k}}\} \subseteq \{p_1, \ldots, p_k\}$$

und ebenso $\{p_1, \ldots, p_k\} \subseteq \{\tilde{p}_1, \ldots, \tilde{p}_{\tilde{k}}\}$. Es folgt $k = \tilde{k}$ und $p_i = \tilde{p}_i$. Im Fall $k = 0$ ist die Gleichheit der Exponenten trivial. Andernfalls ist nach Induktionsannahme ist die Primfaktorzerlegung von n/p_1 eindeutig. Wegen

$$n/p_1 = p_1^{e_1 - 1} \prod_{i=2}^{k} p_i^{e_i} = p_1^{\tilde{e}_1 - 1} \prod_{i=2}^{k} p_i^{\tilde{e}_i},$$

wobei im Falle $e_1 = 1$ bzw. $\tilde{e}_1 = 1$ jeweils der erste Faktor zu streichen ist, folgt $e_i = \tilde{e}_i$. Damit ist auch die Eindeutigkeit der Primfaktorzerlegung gezeigt. □

Folgerung 1. *Jede ganze Zahl $n > 1$ hat einen Primteiler, maw, es gibt eine Primzahl p, welche n teilt.*

Folgerung 2. *Wenn k eine natürliche Zahl und p eine Primzahl ist, so hat jeder Teiler d von p^k die Form $d = \pm p^l$ mit einer natürlichen Zahl $l \leq k$.*

Folgerung 3. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, $\{p_1, \ldots, p_k\}$ wäre die Menge aller Primzahlen. Nach der vorigen Folgerung hat $n = 1 + \prod_{i=1}^{k} p_i$ einen Primteiler, etwa p_j mit $1 \leq j \leq k$. Dann gilt $n = ap_j + 1$ mit der ganzen Zahl $a = \prod_{i \neq j} p_i$, und nach der Eindeutigkeit der Division mit Rest ist n kein Vielfaches von p_j, ein Widerspruch. □

Folgerung 4. *Jede rationale Zahl $n \neq 0$ hat eine eindeutige Darstellung als (1) mit einer natürlichen Zahl k, Primzahlen $p_1 < \cdots < p_k$ und mit von 0 verschiedenen ganzen Zahlen e_k, oder als (2), wobei die Exponenten ε_p ganze Zahlen und nur endlich viele $\varepsilon_p \neq 0$ sind.*

3. Endliche und algebraische Körpererweiterungen

Sei L ein Körper und $K \subseteq L$ eine Teilmenge von L, welche abgeschlossen unter den Körperoperationen auf L ist und mit diesen Operationen ebenfalls zu einem Körper wird. Wir nennen L/K eine *Körpererweiterung* und K einen Unterkörper von L. Durch Einschränkung der Multiplikationsabbildung $L \times L \to L$ auf $K \times L \subseteq L \times L$ wird dann L zu einem K-Vektorraum.

Definition 1. Wir sagen, daß die Körpererweiterung L/K *endlich* ist, wenn L endlichdimensional als K-Vektorraum ist. In diesem Fall wird die Dimension $\dim_K(L)$ von L als K-Vektorraum der *Grad* oder *Ordnung* der Körpererweiterung L/K genannt und mit $[L : K]$ bezeichnet. Unter einer *Basis* einer endlichen Körpererweiterung versteht man eine Basis des K-Vektorraumes L.

Bemerkung 1. Weil ein Körper stets von 0 verschiedene Elemente enthält, ist der Grad einer Körpererweiterung stets positiv. Bekanntlich ist K als Vektorraum über sich selbst eindimensional, also $[K : K] = 1$. Umgekehrt folgt aus $[L : K] = 1$ leicht, daß $L = K$ gilt (Fakt 1 unten). Körpererweiterungen der Grade 2 bzw. 3 nennt man *quadratisch* bzw. *kubisch.* Häufig nennt man auch $[L : K]$ den Grad von L über K und nennt L *endlich über* K, wenn dieser Grad endlich ist.

Satz 1. *Sei L ein Unterkörper von M und K ein Unterkörper von L.*[1] *Dann ist die Körpererweiterung M/K genau dann endlich, wenn die Körpererweiterungen M/L und L/K beide endlich sind. In diesem Fall gilt*

$$[M : K] = [M : L][L : K].$$

Beweis. Sei M/K endlich, also M endlichdimensional als K-Vektorraum. Dann ist L als Unterraum dieses K-Vektorraumes ebenfalls endlichdimensional. Aus den Definitionen folgt weiterhin, daß jede Basis von M als K-Vektorraum eine Erzeugendenmenge von M als L-Vektrraum ist. Also hat M als L-Vektorraum ein endliches Erzeugendensystem und ist daher endlichdimensional. Also sind die Körpererweiterungen M/L und L/K beide endlich.

Wir setzen umgekehrt voraus, daß diese Erweiterungen beide endlich sind. Sei $(\mu_i)_{i=1}^a$ eine Basis von M als L-Vektorraum und $(\lambda_j)_{j=1}^b$ eine Basis von L als K-Vektorraum. Wir behaupten, daß die ab Elemente

$$(+) \qquad \mu_i\lambda_j$$

mit $1 \leq i \leq a$ und $1 \leq j \leq b$ eine Basis von M als K-Vektorraum bilden. Damit sind dann alle Behauptungen des Satzes gezeigt.

Zum Beweis der linearen Unabhängigkeit der Elemente $(+)$ nehmen wir

$$\sum_{i=1}^{a}\sum_{j=1}^{b} k_{i,j}\mu_i\lambda_j = 0$$

mit $k_{i,j} \in K$ an. Dann gilt

$$0 = \sum_{i=1}^{a}\Big(\sum_{j=1}^{b} k_{i,j}\lambda_j\Big)\mu_i = \sum_{i=1}^{a} l_i\mu_i$$

mit $l_i = \sum_{j=1}^{b} k_{i,j}\lambda_j \in L$. Aus der L-linearen Unabhängigkeit der μ_i folgt $l_i = 0$. Aus der K-linearen Unabhängigkeit der λ_j folgt $k_{i,j} = 0$.

[1] In diesem Fall spricht man auch von einem *Turm* $M/L/K$ von Körpererweiterungen oder von einem *Zwischenkörper* L zwischen K und M.

Es verbleibt der Nachweis, daß die Elemente $(+)$ M als K-Vektorraum erzeugen. Sei dazu $m \in M$. Dann kann m in der Basis $(\mu_i)_{i=1}^a$ von M/L als $m = \sum_{i=1}^a l_i\mu_i$ mit $l_i \in L$ dargestellt werden, und jedes l_i kann in der Basis $(\lambda_j)_{j=1}^b$ von L/K als $l_i = \sum_{j=1}^b k_{i,j}\lambda_j$ dargestellt werden. Dann ist

$$m = \sum_{i=1}^{a} l_i\mu_i = \sum_{i=1}^{a}\big(\sum_{j=1}^{b} k_{i,j}\lambda_j\big)\mu_i = \sum_{i=1}^{a}\sum_{j=1}^{b} k_{i,j}\mu_i\lambda_j$$

eine Darstellung von m als K-Linearkombination der Elemente $(+)$. □

Fakt 1. Sei wie zuvor $K \subseteq L \subseteq M$ ein Turm von endlichen Körpererweiterungen. Wenn $[M : L] = 1$ oder $[M : K] = [L : K]$ gilt, so folgt $L = M$.

Beweis. Die Inklusion $L \to M$ ist als Monomorphismus zwischen L-Vektorräumen (erste Voraussetzung) oder K-Vektorräumen (zweite Voraussetzung) derselben Dimension ein Isomorphismus. □

Lemma 1. *Sei M/K eine Körperweiterung und $L \subseteq M$ ein endlichdimensionaler K-Untervektorraum von M mit $1 \in L$ und $L \cdot L \subseteq L$, dann ist L ein Körper.*

Beweis. Alle Körperaxiome mit Ausnahme der Existenz des Inversen zu $l \in L\backslash\{0\}$ sind ziemlich klar. Für die letztere Eigenschaft von Körpern bemerken wir, daß die K-lineare Abbildung

$$L \to L$$
$$x \to l \cdot x$$

ein (auf Grund der Körpereigenschaften von M) injektiver Endomorphismus des endlichdimensionalen K-Vektorraumes L und damit bijektiv ist. Es folgt die Existenz eines $\lambda \in L$ mit $l \cdot \lambda = 1$. □

Satz 2. *Sei M/K eine Körpererweiterung. Die folgenden Bedingungen an $x \in M$ sind äquivalent:*

- **a:** *Es gibt einen über K endlichen Zwischenkörper L zwischen K und M mit $x \in L$.*
- **b:** *Der von $\{x^n \mid n \in \mathbb{N}\}$ aufgespannte K-Untervektorraum $K[x] \subseteq M$ ist endlichdimensional.*
- **c:** *Es gibt ein nichtkonstantes Polynom $P \in K[T]$ mit $P(x) = 0$.*

In diesem Fall ist $K(x) := K[x]$ der kleinste Zwischenkörper zwischen K und M, welcher x enthält, und endlich über K.

Beweis. Es gelte **a**, dann ist der in **b** betrachtete K-Vektorraum in L enthalten und damit endlichdimensional.

Wenn **b** gilt, so gibt es eine kleineste natürliche Zahl n, so daß $\{x^i \mid 0 \leq i \leq n\}$ K-linear abhängig ist. Dann ist auf Grund der Minimalität von n ist[2] x^n eine K-Linearkombination der x^i mit $0 \leq i < n$, und x erfüllt eine algebraische Gleichung n-ten Grades mit Koeffizienten aus K.

[2]Zum Beispiel nach Satz 2.4.1. der Vorlesung „Lineare Algebra I“ aus dem Wintersemester 2015/16.

Es gelte **c**. Dann gilt

$$x^n = \sum_{i=0}^{n-1} a_i x^i \tag{+}$$

mit geeigneten $a_i \in K$. Sei $L \subseteq M$ die K-lineare Hülle der x^i mit $0 \leq i < n$. Wir behaupten, daß L ein Zwischenkörper zwischen K und M ist und L/K endlich ist, womit dann **a** verifiziert ist. Die Endlichdimensionalität von L als K-Vektorraum folgt dabei direkt aus der Konstruktion, und zum Nachweis der Körpereigenschaft genügt die Verifikation der Voraussetzungen von Lemma 1. Direkt aus der Definition folgt $1 \in L$. Zum Nachweis von $L \cdot L \subseteq L$ betrachten wir

$$\tilde{L} = \left\{ \lambda \in M \;\middle|\; \lambda \cdot L \subseteq L \right\}$$

und zeigen

$$L \subseteq \tilde{L}. \tag{@}$$

Offenbar handelt es sich bei $\tilde{L}$ um einen K-Vektorraum. Weil L die lineare Hülle der x^i mit $0 \leq i < n$ ist, genügt zum Beweis von (@) der Nachweis, daß diese x^i zu $\tilde{L}$ gehören. Aus der Definition folgt leicht $\tilde{L} \cdot \tilde{L} \subseteq \tilde{L}$ und $x^0 = 1 \in \tilde{L}$. Also genügt der Nachweis von $x \in \tilde{L}$, also von $x \cdot L \subseteq L$. Weil L die K-lineare Hülle der x^i mit $0 \leq i < n$ ist, genügt der Nachweis von $x \cdot x^i = x^{i+1} \in L$ für alle derartigen i. Für $i < n-1$ ist dies wegen $i+1 < n$ und auf Grund der Definition von L der Fall, für $i = n-1$ wegen (+). □

Definition 2. Ein Element x von M, welches die äquivalenten Bedingungen des Satzes erfüllt, nennt man *algebraisch* über K. Elemente von M, welche nicht algebraisch über K sind, nennt man *transzendent* über K. Im Falle $M = \mathbb{C}$, $K = \mathbb{Q}$ spricht man einfach von algebraischen bzw. transzendenten Zahlen.

4. Eigenschaften algebraischer Elemente

Wir wollen zeigen, daß in der zuvor betrachteten Situation die über K algebraischen Elemente von M einen Zwischenkörper zwischen K und M bilden. Wir schicken voraus, daß sich unmittelbar aus der Charakterisierung Satz 3.2.c von Algebraizität der folgende Fakt ergibt:

Fakt 1. Sei $K \subseteq L \subseteq M$ ein Turm von Körperweiterungen und $x \in M$ algebraisch über K. Dann ist x auch algebraisch über L.

Satz 1.
- *Es seien $x_1, \ldots, x_n$ endlich viele über K algebraische Elemente von M. Dann gibt es einen über K endlichen Zwischenkörper zwischen K und M, welcher alle x_i enthält.*
- *Die über K algebraischen Elemente von M bilden einen Zwischenkörper zwischen K und M, den* algebraischen Abschluß *von K in M.*

Beweis. Wir beweisen zunächst die erste Aussage durch Induktion nach n. Für $n = 1$ handelt es sich um eine unserer äquivalenten Charakterisierungen von Algebraizität. Sei $n > 1$ und die Behauptung für $n-1$ Elemente bewiesen. Dann gibt es einen Zwischenkörper L_1 zwischen K und M, welcher über K endlich ist und $x_1, \ldots, x_{n-1}$ enthält. Wie vorhin bemerkt, ist x_n algebraisch über L_1. Es gibt also einen über L_1 endlichen Zwischenkörper L zwischen L_1 und

M, welcher x_n enthält. Nach Satz 3.1 ist L endlich über K und wegen $L_1 \subseteq L$ enthält L neben x_n auch $x_1, \ldots, x_{n-1}$.

Für die zweite Aussage sei $\tilde{K}$ die Menge der über K algebraischen Elemente von M. Wir zeigen zunächst, daß $\tilde{K}$ abgeschlossen unter Addition und Multiplikation ist. Seien dazu x_1 und x_2 über K algebraische Elemente von M. Nach dem ersten Teil des Satzes gibt es einen über K endlichen Zwischenkörper L, welcher x_1 und x_2 enthält. Dann gilt auch $x_1 + x_2 \in L$ und $x_1 x_2 \in L$, und nach der Charakterisierung Satz 3.2.a von Algebraizität sind diese Elemente von M algebraisch über K. Da die anderen Körpereigenschaften ziemlich offensichtlich sind, verbleibt nur noch der Nachweis, daß $\tilde{K}$ auch abgeschlossen unter Bildung des Inversen von 0 verschiedener Elemente ist. Sei dazu $x \in M \setminus \{0\}$ algebraisch über K. Dann gibt es einen über K endlichen Zwischenkörper L mit $x \in L$. Dann gilt auch $x^{-1} \in L$, also ist x^{-1} ebenfalls algebraisch über K. □

Definition 1. Eine Körpererweiterung L/K ist *algebraisch*, falls alle Elemente von L algebraisch über K sind.

Insbesondere sind endliche Erweiterungen algebraisch. Der Vollständigkeit halber beweisen wir die folgende Transitivitätseigenschaft von „algebraisch“.

Satz 2. *Sei $M/L/K$ ein Körperturm, wobei die Erweiterung L/K algebraisch ist. Dann ist $m \in M$ genau dann algebraisch über L, wenn m algebraisch über K ist.*

Beweis. Sei m algebraisch über L. Dann erfüllt m eine algebraische Gleichung mit Koeffizienten aus L. Nach Satz 1 gibt es einen über K endlichen Zwischenkörper $K \subseteq \tilde{L} \subseteq L$, der alle Koeffizienten dieser Gleichung enthält. Dann ist m auch algebraisch über $\tilde{L}$, es gibt also eine endliche Erweiterung $\hat{L}/\tilde{L}$ mit $m \in \hat{L}$. Nach Satz 3.1 ist $\hat{L}/K$ endlich, also ist m algebraisch über K. Die entgegengesetzte Implikation ist Fakt 1. □

Wenn M/K eine Körpererweiterung und $x \in M$ algebraisch über K ist, so gibt es nach Satz 3.2 ein kleinstes n, so daß x^n eine K-Linearkombination der x^i mit $0 \leq i < n$ ist, also

$$x^n = \sum_{i=0}^{n-1} p_i x^i$$

mit $p_i \in K$. Aus dem Beweis von Satz 3.2 folgt, daß $(1, x, \ldots, x^{n-1})$ eine Basis von $K(x)/K$ ist. Der Grad dieser Körpererweiterung ist also n. Man nennt x dann *algebraisch vom Grade n über K*, und das Polynom

$$\mathrm{Min}_{x/K}(T) = T^n - \sum_{i=0}^{n-1} p_i T^i$$

wird *Minimalpolynom* von x über K genannt. Der Name ist dadurch motiviert, daß n der kleinste Grad einer algebraischen Gleichung mit Koeffizienten aus K und x als Lösung ist. Würde nämlich x eine algebraische Gleichung vom Grade $m < n$ mit Koeffizienten aus K

lösen, so wäre

$$x^m = \sum_{i=0}^{m-1} q_i x^i$$

mit $q_i \in K$, im Widerspruch zur obigen Minimalität von n. Weiterhin gilt sogar:

Satz 3. *Wenn $P \in K[T]$ ein Polynom mit $P(x) = 0$ ist, so gilt $P = Q\mathrm{Min}_{x/K}$ mit einem Polynom $Q \in K[T]$.*

Beweis. Die Polynomdivision mit Rest ergibt eine Darstellung

$$P = Q\mathrm{Min}_{x/K} + R$$

mit $Q, R \in K[T]$ und $\deg R < n$, und wir haben

$$R(x) = P(x) - Q(x)\mathrm{Min}_{x/K}(x) = 0 - Q(x)0 = 0.$$

Wäre $R \neq 0$, wo wäre dies ein Widerspruch zur Minimalität von n. □

5. Konstruktionen mit dem Lineal

Für den Unmöglichkeitsbeweis der klassischen geometrischen Konstruktionsprobleme ist es grundlegend, die Punkte der Ebene als komplexe Zahlen zu betrachten. Wir geben eine entsprechende Definition von Konstruierbarkeit mit Zirkel und Lineal, wobei wir der Einfachheit halber für die Dauer dieses Seminares einfach von „Konstruierbarkeit“ sprechen wollen. Dabei zeigen wir, daß die aus 0 und 1 konstruierbaren komplexen Zahlen algebraisch sind und einem Zwischenkörper zwischen $\mathbb{Q}$ und $\mathbb{C}$ angehören, welcher Zweierpotenzordnung hat.

Unter einer *Geraden* wollen wir eine Teilmenge von $\mathbb{C}$ verstehen, welche die Form $\mathfrak{g} = x + V$ hat, wobei x eine komplexe Zahl und V ein eindimensionaler $\mathbb{R}$-Untervektorraum von $\mathbb{C}$ ist.

Wir erinnern an die komplexe Konjugation, einen durch $\overline{x+iy} = x - iy$ für $x, y \in \mathbb{R}$ definierten, involutiven (also $\overline{\overline{z}} = z$) Körperautomorphismus von $\mathbb{C}$.

Satz 1. *Für zwei komplexe Zahlen $a \neq b$ gibt es genau eine Gerade $\mathfrak{g}_{a,b}$, welche a und b enthält. Es gilt $z \in \mathfrak{g}_{a,b}$ genau dann, wenn*

$$(b-a)(\overline{z}-\overline{a}) = (\overline{b}-\overline{a})(z-a) \tag{1}$$

gilt.

Beweis. Weil wir $a \neq b$ voraussetzen, gilt $b - a \neq 0$ und $\{b-a\}$ ist eine $\mathbb{R}$-linear unabhängige Teilmenge von $\mathbb{C}$. Also ist

$$V = \mathbb{R} \cdot (b-a) = \big\{\lambda(b-a) \;\big|\; \lambda \in \mathbb{R}\big\}$$

ein eindimensionaler $\mathbb{R}$-Untervektorraum von $\mathbb{C}$ und $\mathfrak{g} = a+V = b+V$ leistet das Gewünschte. Angenommen, $\tilde{\mathfrak{g}} = x + \tilde{V}$ ist eine Gerade, welche a und b enthält. Aus $a \in \tilde{\mathfrak{g}}$ und $b \in \tilde{\mathfrak{g}}$ folgt $a - x \in \tilde{V}$ und $b - x \in \tilde{V}$, also $b - a = (b-x) - (a-x) \in \tilde{V}$ und $V \subseteq \tilde{V}$, wobei auf Grund der Eindimensionalität beider $\mathbb{R}$-Vektorräume Gleichheit eintritt. Wegen $a - x \in \tilde{V}$ gilt

$$\tilde{\mathfrak{g}} = x + \tilde{V} = a + \tilde{V} = a + V = \mathfrak{g},$$

und die Eindeutigkeit von $\mathfrak{g}_{a,b}$ ist bewiesen.

Wegen $a \neq b$ kann jede komplexe Zahl z als $z = a + \lambda(b-a)$ mit einem eindeutigen $\lambda \in \mathbb{C}$ dargestellt werden. Dann ist (1) äquivalent zu $(b-a)(\overline{b}-\overline{a})\overline{\lambda} = (\overline{b}-\overline{a})(b-a)\lambda$, also zu $\lambda = \overline{\lambda}$ oder $\lambda \in \mathbb{R}$ oder $z \in \mathfrak{g}_{a,b}$. □

In den folgenden Beweisen wird es oft zweckmäßig sein, die Invarianz der betrachteten Operationen unter Ähnlichkeitsabbildungen der Art

$$T_{\tau,\lambda}(z) = \tau + \lambda z$$

mit $\tau \in \mathbb{C}$, $\lambda \in \mathbb{C}^*$ zu benutzen, um die Rechnungen zu vereinfachen. Da $T_{\tau,\lambda}$ und $T_{-\lambda^{-1}\tau,\lambda^{-1}}$ zueinander invers sind, handelt es sich um bijektive Abbildungen von $\mathbb{C}$ auf sich selbst. Aus unserer Definition von „Gerade“ folgt ziemlich leicht, daß das Bild einer Geraden unter $T_{\tau,\lambda}$ wieder eine Gerade ist, also

$$T_{\tau,\lambda}(\mathfrak{g}_{a,b}) = \mathfrak{g}_{T_{\tau,\lambda}(a),T_{\tau,\lambda}(b)}. \tag{2}$$

Geometrisch gesehen kann man sich die Abbildungen $T_{\tau,\lambda}$ als eine Verknüpfung einer Verschiebung um τ mit einer Drehstreckung vorstellen.

Wir betrachten erneut die durch die komplexe Konjugation definierte Selbstabbildung von $\mathbb{C}$. Geometrisch gesehen handelt es sich um die Spiegelung an der reellen Achse. Anwendung dieser Operation auf eine Gerade ergibt wieder eine Gerade:

$$\overline{\mathfrak{g}_{a,b}} = \mathfrak{g}_{\overline{a},\overline{b}} \tag{3}$$

Wir sind vor allem an Unterkörpern $K \subseteq \mathbb{C}$ interessiert, welche unter dieser Operation abgeschlossen sind. Aus $z \in K$ soll also $\overline{z} \in K$ folgen.

Satz 2. *Seien $a \neq b$ und $c \neq d$ komplexe Zahlen.*

- *Wenn die Geraden $\mathfrak{g}_{a,b}$ und $\mathfrak{g}_{c,d}$ verschieden sind, so hat $\mathfrak{g}_{a,b} \cap \mathfrak{g}_{c,d}$ höchstens ein Element.*
- *Wenn zusätzlich $K \subseteq \mathbb{C}$ ein unter komplexer Konjugation abgeschlossener Unterkörper ist, welcher a, b, c und d enthält, so gilt auch $\mathfrak{g}_{a,b} \cap \mathfrak{g}_{c,d} \subseteq K$.*

Beweis. Sei $\lambda = b-a$, dann bildet $T_{\lambda,a}$ 0 auf a und 1 auf b ab. Für den ersten Punkt dürfen wir daher und wegen (2) $a = 0$, $b = 1$ voraussetzen. Dasselbe gilt auch für den zweiten Punkt, denn $T_{\lambda,a}$ ist unter den dortigen Voraussetzungen eine bijektive Abbildung von K auf sich selbst.

Sei also $a = 0$, $b = 1$. Dann gilt $\mathfrak{g}_{a,b} = \mathbb{R}$, und aus der Verschiedenheit der beiden Geraden folgt, daß eine der beiden Zahlen c und d einen von 0 verschiedenen Imaginärteil hat. Wegen $\mathfrak{g}_{c,d} = \mathfrak{g}_{d,c}$ dürfen wir $\Im(c) \neq 0$ annehmen.

Wir haben $\mathfrak{g}_{c,d} = \left\{c + (d-c)\vartheta \;\middle|\; \vartheta \in \mathbb{R}\right\}$. Für $\Im d = \Im c$ haben alle diese Zahlen Imaginärteil $\Im c \neq 0$, so daß $\mathfrak{g}_{a,b} \cap \mathfrak{b}_{c,d}$ leer ist. Andernfalls erhält man genau für $\vartheta = \frac{\Im c}{\Im c - \Im d}$ eine reelle Zahl. In der Situation des zweiten Punktes gilt $i\Im c = \frac{c-\overline{c}}{2} \in K$, analog $\Im d \in K$, also enthält K auch ϑ und den Schnittpunkt $c + (d-c)\vartheta$ der beiden Geraden. □

6. Konstruktionen mit Zirkel und Lineal

Wir erinnern an die Beziehung

$$|z|^2 = z \cdot \overline{z}$$

zwischen komplexer Konjation und komplexem Absolutbetrag und bezeichnen mit

$$K_{a,b} = \big\{ z \in \mathbb{C} \;\big|\; |z-a| = |b-a| \big\} = \big\{ z \in \mathbb{C} \;\big|\; (z-a)(\overline{z}-\overline{a}) = (b-a)(\overline{b}-\overline{a}) \big\}$$

den Kreis durch b mit Mittelpunkt a, also den geometrischen Ort aller z, welche von a denselben Abstand haben wie b. Im Unterschied zu $\mathfrak{g}_{a,b} = \mathfrak{g}_{b,a}$ gilt also $K_{a,b} \neq K_{b,a}$.

Wegen

$$|T_{\lambda,\tau}(z) - T_{\lambda,\tau}(\zeta)| = |\lambda(z-\zeta)| = |\lambda| \cdot |z-\zeta|$$

gilt

$$T_{\lambda,\tau}\big(K_{a,b}\big) = K_{T_{\lambda,\tau}(a),T_{\lambda,\tau}(b)} \tag{1}$$

und aus $|z| = |\overline{z}|$ folgt

$$\overline{K_{a,b}} = K_{\overline{a},\overline{b}} \tag{2}$$

Satz 1. *Es seien $a \neq b$ und $c \neq d$ komplexe Zahlen.*

- *Der Durchschnitt $K_{a,b} \cap \mathfrak{g}_{c,d}$ enthält höchstens zwei Elemente. Im Fall $c \neq a$ enthält auch $K_{a,b} \cap K_{c,d}$ höchstens zwei Elemente.*
- *Sei $K \subseteq \mathbb{C}$ ein Unterkörper, welcher a, b, c und d enthält und invariant unter komplexer Konjugation ist. Dann gibt es eine Erweiterung L von K vom Grade ≤ 2 mit $K_{a,b} \cap \mathfrak{g}_{c,d} \subseteq L$. Im Fall $a \neq c$ gibt es auch eine Erweiterung L von K vom Grade ≤ 2 mit $K_{a,b} \cap K_{c,d} \subseteq L$.*

Beweis. Beim Beweis des ersten Punktes kann man wegen (1) ähnlich wie beim Beweis von Satz 5.2 voraussetzen, daß $a = 0$ und $b = 1$ gilt. Dies gilt auch beim Beweis des zweiten Punktes, denn die dort betrachteten quadratischen Erweiterungskörper L sind alle invariant unter $T_{b-a,a}$.

Wir haben

$$K_{0,1} = \big\{ z \in \mathbb{C} \;\big|\; |z| = 1 \big\} = \big\{ z \in \mathbb{C} \;\big|\; z \cdot \overline{z} = 1 \big\}.$$

Aus $z \in K_{0,1} \cap \mathfrak{g}_{c,d}$ folgt insbesondere $z \neq 0$ und, wegen (5.1),

$$(\overline{d} - \overline{c})(z-c) = (d-c)(\overline{z} - \overline{c}) = (d-c)\Big(\frac{1}{z} - \overline{c}\Big)$$

und z löst die quadratische Gleichung

$$(\overline{d} - \overline{c})z^2 + \Big(c(\overline{c} - \overline{d}) + (d-c)\overline{c}\Big)z + (c-d) = 0,$$

welche maximal zwei komplexe Lösungen hat[3]. In der Situation des zweiten sind die Koeffizienten der quadratischen Gleichung in K enthalten, so daß die Lösungen entweder in K oder in einer quadratischen Erweiterung von K enthalten sind.

[3]Wobei zwar die Existenz von Lösungen garantiert ist, deren Betrag aber nicht automatisch 1 ist, so daß $K_{0,1} \cap \mathfrak{g}_{c,d}$ auch leer sein kann.

Für $c \neq 0$ folgt aus $z \in K_{0,1} \cap K_{c,d}$ ähnlich wie zuvor

$$(d-c)(\overline{d}-\overline{c}) = (z-c)(\overline{z}-\overline{c}) = (z-c)\Big(\frac{1}{z}-\overline{c}\Big)$$

und die quadratische Gleichung

$$\overline{c}z^2 + \Big((d-c)(\overline{d}-\overline{c}) - c\overline{c} - 1\Big)z + c = 0,$$

und eine Wiederholung der vorigen Argumente beendet den Beweis. □

Sei nun $\mathfrak{M}$ eine endliche Teilmenge von $\mathbb{C}$. Wir wollen induktiv die Menge $\mathfrak{M}_k$ aller in höchstens k Schritten aus den Elementen von $\mathfrak{M}$ konstruierbaren Zahlen definieren, wobei wir natürlich $\mathfrak{M}_0 = \mathfrak{M}$ setzen. Wenn $\mathfrak{M}_k$ definiert ist, so sei $\mathfrak{B}_k$ die Menge aller Quadrupel (a,b,c,d) von Elementen von $\mathfrak{M}_k$ mit $a \neq b$ und $c \neq d$. Weiter sei $\mathfrak{A}_k$ (bzw. $\mathfrak{C}_k$) die Menge aller Elemente von $\mathfrak{B}_k$ mit $\mathfrak{g}_{a,b} \neq \mathfrak{g}_{c,d}$ (bzw. $a \neq c$). Wir setzen dann

$$\mathfrak{M}_{k+1} = \mathfrak{M}_k \cup \Big(\bigcup_{(a,b,c,d)\in\mathfrak{A}_k} \mathfrak{g}_{a,b} \cap \mathfrak{g}_{c,d}\Big) \cup \Big(\bigcup_{(a,b,c,d)\in\mathfrak{B}_k} K_{a,b} \cap \mathfrak{g}_{c,d}\Big) \cup \Big(\bigcup_{(a,b,c,d)\in\mathfrak{C}_k} K_{a,b} \cap K_{c,d}\Big).$$

Aus der Endlichkeit von $\mathfrak{M}$ und Satz 5.2 sowie Satz 1 folgt induktiv die Endlichkeit von $\mathfrak{M}_k$. Wir setzen

$$\mathfrak{M}_\infty = \bigcup_{k=0}^{\infty} \mathfrak{M}_k.$$

Im Fall $\mathfrak{M} = \{0;1\}$ wollen wir für die Zwecke dieses Seminares die Elemente von $\mathfrak{M}_\infty$ *konstruierbare Zahlen* nennen.

Satz 2. *Wenn K ein Unterkörper von $\mathbb{C}$ ist, welcher $\mathfrak{M}$ enthält und invariant unter komplexer Konjugation ist, so existieren Folgen $K = K_0 \subseteq K_1 \subseteq \ldots$ sowie $K_k = K_{k,0} \subseteq K_{k,1} \subseteq \ldots \subseteq K_{k,n_k} = K_{k+1}$ von Unterkörpern von C, so daß die K_k invariant unter komplexer Konjugation sind und $\mathfrak{M}_k$ enthalten und so daß die Erweiterungen $K_{k,j+1}/K_{k,j}$ für $0 \leq j < n_k$ quadratisch sind. Insbesondere ist $[K_k : K]$ eine Zweierpotenz.*

Beweis. Wir gehen durch Induktion nach k vor und bezeichnen mit $(z_l)_{l=1}^{N_k}$ eine Auflistung aller Elemente von $\mathfrak{M}_{k+1} \setminus \mathfrak{M}_k$. Sei $K_{k,0} = K_k$ und $j_0 = 0$. Wir nehmen an, daß $l \geq 1$ gilt und $K_{k,j}$ mit $0 \leq j \leq j_{l-1}$ schon so konstruiert ist, daß die Behauptungen gelten und zusätzlich $K_{k,j_{l-1}}$ invariant unter komplexer Konjugation ist. In jedem der drei möglichen Fälle

- $z_l \in \mathfrak{g}_{a,b} \cap \mathfrak{g}_{c,d}$ mit $(a,b,c,d) \in \mathfrak{A}_k$
- $z_l \in K_{a,b} \cap \mathfrak{g}_{c,d}$ mit $(a,b,c,d) \in \mathfrak{B}_k$
- $z_l \in K_{a,b} \cap K_{c,d}$ mit $(a,b,c,d) \in \mathfrak{C}_k$

gibt es nach Satz 5.2 oder Satz 1 eine Erweiterung L von K vom Grade ≤ 2 mit $z_l \in L$. Im Falle $L = K$ setzen wir $j_l = j_{l-1}$. Andernfalls ist $L = K(\sqrt{\kappa})$ eine quadratische Erweiterung

von K. Falls $\sqrt{\kappa} \in K_{k,j_{l-1}}$ ist,[4] setzen wir $j_l = j_{l-1}$. Andernfalls sei

$$K_{k,j_{l-1}+1} = K_{k,j_{l-1}}(\sqrt{\kappa}).$$

Falls auch $\overline{\sqrt{\kappa}} \in K_{k,j_{l-1}+1}$ ist, ist dieser Unterkörper von $\mathbb{C}$ invariant unter komplexer Konjugation und wir setzen $j_l = j_{l-1} + 1$. Andernfalls setzen wir $j_l = j_{l-1} + 2$. Weil $K_{k,j_{l-1}}$ invariant unter komplexer Konjugation ist, ist auch $\overline{\kappa}$ Element dieses Körpers und

$$K_{k,j_{l-1}+2} = K_{k,j_{l-1}+1}(\overline{\sqrt{\kappa}}) = K_{k,j_{l-1}}(\sqrt{\kappa}, \overline{\sqrt{\kappa}})$$

ist eine quadratische Erweiterung von $K_{k,j_{l-1}+1}$ und invariant unter komplexer Konjugation.

Damit ist die Konstruktion der Körpertürme mit den behaupteten Eigenschaften abgeschlossen. Durch induktive Anwendung von Satz 3.1 haben wir $[K_{k+1} : K_k] = 2^{j_l}$, also $[K_k : K] = 2^{d_k}$ mit $d_k = \sum_{l=1}^{k-1} j_l$. Die Körpergrade sind also Zweierpotenzen wie behauptet. □

Im Fall $\mathfrak{M} = \{0; 1\}$ kann $K = \mathbb{Q}$ genommen werden, und wir erhalten

Folgerung 1. *Alle konstruierbaren Zahlen sind algebraisch von Zweierpotenzordnung.*

Beweis. Sei $z \in \mathbb{C}$ konstruierbar. Nach dem Satz gibt es eine endliche Erweiterung K von $\mathbb{Q}$ mit $z \in K$, so daß $[K : \mathbb{Q}]$ eine Zweierpotenz ist. Also ist z algebraisch über $\mathbb{Q}$, und die Ordnung $[\mathbb{Q}(z) : \mathbb{Q}]$ von z ist als Teiler der Zweierpotenz $[K : \mathbb{Q}]$ nach Folgerung 2.2 ebenfalls eine Zweierpotenz. □

Bemerkung 1. Die Umkehrung ist nicht richtig. (CAVE) $z^4 - 4z + 2 = 0$.

7. Die Verdoppelung des Würfels

Wir wollen zeigen, daß $\mathbb{Q}(\sqrt[3]{2})$ eine kubische Erweiterung von $\mathbb{Q}$ ist, wobei die reelle Kubikwurzel betrachtet werden soll. Nach Folgerung 6.1 ist dann die Zahl $\sqrt[3]{2}$ nicht konstruierbar und die Verdoppelung des Würfels nicht mit Zirkel und Lineal lösbar. Wir beginnen mit dem folgenden allgemeinen Fakt.

Satz 1. *Sei L ein Erweiterungskörper von K und $l \in L$ Lösung der kubischen Gleichung*

$$(+) \qquad x^3 + px^2 + qx + r = 0$$

mit $p, q, r \in K$. Wenn (+) keine Lösung mit $x \in K$ hat, so gilt $[K(l) : K] = 3$.

Beweis. Weil l eine Lösung von (+) ist, ist l algebraisch vom Grade 1, 2 oder 3 über K. Im ersten Fall hat (+) die Lösung $x = l \in K$ und im letzten gilt $[K(l) : K] = 3$. Wir zeigen, daß (+) auch dann eine Lösung in K hat, wenn l den Grad 2 über K hat. In diesem Fall gilt nämlich

$$T^3 + pT^2 + qT + r = \mathrm{Min}_{l/K}(T) \cdot Q(T)$$

mit einem $Q \in K[T]$ nach Satz 4.3, wobei $\mathrm{Min}_{l/K}(T)$ quadratisch ist. Der Grad von Q ist daher 1, also $Q(T) = T - a$ mit $a \in K$, und $x = a$ löst (+). □

[4]Was entweder für alle oder gar keine Quadratwurzeln aus κ gilt, weil diese sich nur um das Vorzeichen unterscheiden.

Bemerkung 1. Wenn l eine Gleichung vom Grad $n > 3$ löst, wird es schwieriger, $[K(l) : K] = n$ zu zeigen. Beispielsweise hat $x^4 = 4$ keine Lösung $x \in \mathbb{Q}$. Trotzdem ist für jede komplexe Lösung z von $z^4 = 4$ die Erweiterung $\mathbb{Q}(z) \,/\, \mathbb{Q}$ quadratisch statt quartisch, denn $z^2 = \pm 2$.

Wir müssen noch ausschließen, daß $z^3 = 2$ eine rationale Lösung hat. Generell gilt der folgende Satz:

Satz 2. *Sei $z \in \mathbb{Q}$ eine Lösung von*

$$z^n = \sum_{k=0}^{n-1} a_k z^k$$

mit ganzen Zahlen a_k. Dann ist z eine ganze Zahl, und a_0 ist ein ganzzahliges Vielfaches von z.

Beweis. Sei $z = \frac{p}{q}$ eine Darstellung als teilerfremder Bruch mit positivem Nenner. Es gilt

$$p^n = \sum_{k=0}^{n-1} a_k p^k q^{n-k}.$$

Also ist p^n durch q teilbar und es muß $q = 1$ gelten, weil p^n und q nach Folgerung 1.3 teilerfremd sind. Folglich ist z eine ganze Zahl, und

$$a_0 = z^n - \sum_{k=1}^{n-1} a_k z^k$$

ist durch z teilbar. □

Für die Gleichung $z^3 = 2$ kommen also nur ± 1 und ± 2 als rationale Lösungen in Frage. Da keine dieser Zahlen die Gleichung wirklich löst, gibt es gar keine rationale Lösung. Aus Satz 1 folgt nun

Theorem 1 (Wantzel, 1837)**.** *Die Zahl $\sqrt[3]{2}$ ist nicht konstruierbar.*

Das klassische Problem der Verdoppelung des Würfels ist also mit Zirkel und Lineal nicht lösbar.

8. Das regelmässige Neuneck und die Drittelung des Winkels

Der erste vollständige Beweis der Unlösbarkeit des klassischen Problemes der Winkeldrittelung mit Zirkel und Lineal wurde ebenfalls 1837 von P. Wantzel publiziert. Der damalige Entwicklungsstand der Theorie der algebraischen Zahlen war freilich nach Resultaten von Gauß, Abel und Galois schon ziemlich hoch. Es ist jedoch unwahrscheinlich, daß Wantzel im Jahre 1837 die Resultate von Galois gekannt hat.

Sei $\zeta_n = e^{\frac{2\pi i}{n}}$. Offenbar haben alle diese komplexen Zahlen den Betrag 1. Die Multiplikation mit ζ_n kann gemoetrisch als Drehung um den Winkel $\frac{2\pi}{n}$, also $360^o/n$, gedeutet werden. Die Zahlen ζ_n^i mit $0 \leq i < n$ bilden also die Ecken eines regelmäßigen n-Eckes. Dabei gilt $\zeta_n^n = 1$.

Lösungen der Gleichung $z^n = 1$ nennt man *n-te Einheitszwurzeln*. Wenn n minimal ist, also $z^m \neq 1$ für $0 < m < n$ gilt, spricht man von einer *primitiven n-ten Einheitswurzeln*. Die aus der Analysis bekannten Resultate über die Exponentialfunktion im Komplexen zeigen, daß ζ_n eine primitive n-te Einheitszurzel ist und

$$\overline{\zeta_n} = \zeta_n^{-1} = \zeta_n^{n-1} \tag{1}$$

gilt.

Weiter gilt

$$s = \sum_{j=0}^{n-1} \zeta_n^j = 0, \tag{2}$$

denn es gilt

$$\zeta_n s = \sum_{j=0}^{n-1} \zeta_n^{j+1} = \sum_{j=1}^{n} \zeta_n^j = \Big(\sum_{j=1}^{n-1} \zeta_n^j\Big) + 1 = \sum_{j=0}^{n-1} \zeta_n^j = s$$

und $\zeta_n \neq 1$.

Wir betrachten zunächst

$$\zeta_3 = \cos(120^o) + i\sin(120^o) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Aus (2) folgt

$$\zeta_3^2 + \zeta_3 + 1 = 0. \tag{3}$$

und mit (1) folgt

$$|1 + \zeta_3|^2 = (1 + \zeta_3)(1 + \overline{\zeta_3}) = (1 + \zeta_3)(1 + \zeta_3^2) = 2 + \zeta_3 + \zeta_3^2 = 1.$$

Es folgt $K_{0,1} \cap K_{1,0} = \big\{1 \pm \zeta_3\big\}$ nach Satz 6.1, denn die angegeben Zahlen sind in der Tat im Durschnitt enthalten. Die Zahl

$$1 + \zeta_3 = \frac{1}{2} + \frac{\sqrt{3}}{2}i = \cos(60^o) + \sin(60^o)i = \zeta_6$$

ist also konstruierbar, entsprechend der aus der Schule bekannten Konstruktion des regelmäßigen Sechseckes. Wir haben weiter $K_{0,1} \cap K_{\zeta_6,1} = \{\zeta_3; 1\}$ nach Satz 6.1, denn aus der vorigen Gleichung folgt, daß beide Zahlen in der Tat im Durchschnitt enthalten sind. Also ist auch ζ_3 konstruierbar.

Wir betrachten nun ζ_9 und wollen zeigen, daß diese Zahl nicht konstruierbar ist. Daraus folgt die Nichtkonstruierbarkeit des regelmäßigen Neuneckes mit Zirkel und Lineal und die Unmöglichkeit der Drittelung des Winkels mit diesen Mitteln. Könnte nämlich der Winkel, den 1 und ζ_3 mit 0 als Ecke bilden, mit diesen Mitteln gedrittelt werden, so gäbe es eine komplexe Zahl $z = r\zeta_9$ mit reellem $r > 0$, welche konstruierbar ist. Wegen $\mathfrak{g}_{0,z} \cap K_{0,1} = \{\pm\zeta_9\}$ wäre dann auch ζ_9 konstruierbar.

Theorem 2. *Sei $\zeta = \zeta_9$. Wir betrachten die reelle Zahl $s = \zeta + \overline{\zeta} = \zeta + \zeta^8$.*[5]

[5]Die Gleichungen folgen aus (1), und aus $s = \overline{s}$ folgt $s \in \mathbb{R}$

- *s löst die kubische Gleichung*

$$s^3 - 3s + 1 = 0. \tag{4}$$

- *$\mathbb{Q}(s)$ ist eine kubische Erweiterung von $\mathbb{Q}$.*
- *$\mathbb{Q}(\zeta)$ hat den Grad 6 über $\mathbb{Q}$.*
- *ζ ist nicht konstruierbar.*

Beweis. Aus (3) und $\zeta_3 = \zeta^3$ folgt

$$\zeta^6 + \zeta^3 + 1 = 0 \tag{5}$$

und aus der Definition von s ergibt sich unter Anwendung des kubischen binomischen Satzes

$$s^3 - 3s + 1 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} - 3\zeta - 3\zeta^{-1} + 1 = \zeta^3 + \zeta^{-3} + 1 = \zeta^{-3}\big(\zeta^6 + \zeta^3 + 1\big) = 0.$$

Also ist s wirklich Lösung von (4). Diese Gleichung hat keine rationalen Lösungen, denn nach Satz 7.2 kommen nur die ganzen Zahlen ± 1 als rationale Lösungen in Frage, welche die Gleichung nicht erfüllen. Nach Satz 7.1 ist s kubisch über $\mathbb{Q}$.

Wegen $\mathbb{Q}(s) \subseteq \mathbb{Q}(\zeta)$ und nach Satz 3.1 ist $d = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ durch $[\mathbb{Q}(s) : \mathbb{Q}] = 3$ teilbar. Weiterhin ist $d > 3$, denn sonst wäre $\mathbb{Q}(\zeta) = \mathbb{Q}(s) \subseteq \mathbb{R}$, was wegen $\zeta \notin \mathbb{R}$ nicht der Fall sein kann. Wegen (5) kann d nicht größer sein als 6. Also gilt $d = 6$ wie behauptet. Die letzte Behauptung folgt nun aus Folgerung 6.1. □

9. Irrationalität von e und transzendente Zahlen.

Als letztes der drei großen klassischen geometrischen Konstruktionsprobleme verbleibt das Problem der Quadratur des Kreises. Das Problem läuft hinaus auf die Frage der Konstruierbarkeit von $\sqrt{\pi}$ und ist negativ gelöst, sobald die Transzendenz von π gezeigt ist. Wäre nämlich $\sqrt{\pi}$ algebraisch, so wäre auch das Quadrat dieser Zahl, also π, algebraisch.

Durch die Beziehung $e^{i\pi} = -1$ sind die Transzendenzbeweise für e und π eng miteinander verwandt. Da die Beweise für die Zahl e einfacher sind, beginnen wir mit der Betrachtung dieses Falles, auch wenn dies einen kleinen Umweg bedeutet. Wir beginnen mit dem sehr einfachen Beweis der Irrationalität von e.

Satz 1 (Euler, 1744)**.** *Die Zahl e ist irrational.*

Der folgende Beweis stammt von Fourier.

Beweis. Andernfalls gäbe es eine positive ganze Zahl n, so daß ne ganzzahlig ist. Dann ist auch $n!e = (n-1)!(ne)$ ganzzahlig. Auf der anderen Seite gilt

$$n!e = \sum_{k=0}^{n} \frac{n!}{k!} + \sum_{k=n+1}^{\infty} \frac{n!}{k!}.$$

Weil der erste Summand ganzzahlig ist, muß auch das Restglied

$$R = \sum_{k=n+1}^{\infty} \frac{n!}{k!}$$

ganzzahlig sein. Für $k > n \geq 1$ gilt aber $k! \geq 2^{k-n}n!$ mit Gleichheit nur für $k = 2$ und $n = 1$. Also gilt

$$0 < R < \sum_{k=n+1}^{\infty} 2^{n-k} = 1,$$

im Widerspruch zur Ganzzahligkeit von R. □

Die Idee des Beweises beruht also darauf, daß die Exponentialreihe, ohne abzubrechen, sehr schnell konvergiert und ihre Nenner ab einem gewissen Summanden durch jede vorgegebene positive ganze Zahl teilbar sind. Lambert gelang 1761 — angeblich bis auf eine Lücke, die von Legendre geschlossen wurde — der Beweis der Irrationalität von π. Wir wollen hier aber nicht auf diesen Beweis eingehen, weil dieser länger ist als der Irrationalitätsbeweis von e und wir ohnehin einen Beweis der von Lambert vermuteten Transzendenz von π anstreben. Dieser Transzendenzbeweis erfordert aber, wie wir sehen werden, andere Ideen.

Es gibt freilich eine Art von Transzendenzbeweisen für manche Zahlen, welche ähnlich wie unser Irrationalitätsbeweis von e auf der Existenz guter Annäherungen durch rationale Zahlen beruhen. Algebraische Irrationalzahlen sind nämlich relativ schlecht durch rationale Zahlen approximierbar, wie die folgenden Sätze zeigen:

Satz 2 (Liouville, 1844)**.** *Sei $\alpha \in \mathbb{R}$ eine irrationale Zahl, welche algebraisch vom Grade n ist. Dann existiert eine Zahl $\delta > 0$ mit*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{\delta}{q^n}$$

für alle ganzen Zahlen p und q mit $q > 0$.

Der Satz von Liouville ist also eine untere Schranke für das Problem der *diophantischen Approximation*, der möglichst guten Approximation reeller Zahlen x durch rationale Zahlen $\frac{p}{q}$ mit $p \in \mathbb{Z}$ und möglichst kleinen positiven ganzen Zahlen q als Nenner, für den Fall einer algebraischen Zahl x. Um die Mitte des vorigen Jahrhunderts wurde dann der folgende Satz bewiesen:

Satz 3 (K. F. Roth, 1955)**.** *Sei $\alpha \in \mathbb{R}$ eine algebraische Irrationalzahl und $\varepsilon > 0$, dann existieren nur endlich viele Paare (p, q) ganzer Zahlen mit $q > 0$ und*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}}.$$

Offenbar ist der Satz von Roth eine Verschärfung des Satzes von Liouville, ausgenommen im Fall quadratischer Irrationalzahlen α. Weil die Theorie der Kettenbrüche für beliebige reelle Zahlen α unendlich viele Näherungsbrüche mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

liefert, kann dieser Satz nicht mehr wesentlich verschärft werden. Zwischenresultate auf dem Weg zwischen den Sätzen von Liouville und Roth stammen von A. Thue, C. L. Siegel und von dem bekannten Physiker F. Dyson.

Wir gehen nicht auf die Beweise ein, zumal diese mit Ausnahme des Liouvilleschen Beweises etwas länger sind. Übrigens sind rationale Zahlen in dem hier studierten Sinne besonders schlecht durch andere rationale Zahlen approximierbar, denn es gilt

$$\left|\frac{a}{b}-\frac{p}{q}\right| = \frac{|aq-bp|}{bq} \geq \frac{1}{bq},$$

falls die beiden Brüche nicht gleich sind. Folglich gibt es für jedes $x \in \mathbb{Q}$ ein $\delta > 0$ mit

$$\left|x-\frac{p}{q}\right| \geq \frac{\delta}{q}$$

für alle Paare (p, q) ganzer Zahlen mit $q > 0$ und $x \neq \frac{p}{q}$. Es handelt sich hierbei gewissermaßen um die Aussage, die das Liouvillesche Beweisprinzip für die diophantische Approximation algebraischer Zahlen vom Grade 1, also rationaler Zahlen, liefert.

Aus dem Liouvielleschen Satz und der soeben gebrachten Überlegung über rationale Zahlen folgt die Transzendenz des Limes der extrem schnell konvergierenden Summe

$$\sum_{n=0}^{\infty} b^{-n!}$$

mit jeder natürlichen Zahl $b > 1$ als Basis. Wird der Satz von Roth benutzt, kann man auch die Transzendenz von

$$\sum_{n=0}^{\infty} b^{-3^n}$$

zeigen. Die Exponentialreihe konvergiert aber nicht schnell genug für die Anwendung eines dieser Sätze.

Wenn man lediglich die Existenz transzendenter Zahlen zeigen möchte, kann man einfach die von Cantor entwickelten Methoden der unendlichen Kombinatorik benutzen: Weil jedes Polynom n-ten Grades mit rationalen Koeffizienten maximal n komplexe Nullstellen hat und die Menge dieser Polynome nach dem ersten Cantorschen Diagonalprinzip abzählbar ist, kann es nur abzählbar unendlich viele algebraische Zahlen geben. Da $\mathbb{R}$ überabzählbar ist, muß es transzendente reelle Zahlen geben. Im Unterschied zu dem historisch früheren Argument von Liouville ist dieser Beweis offenbar nicht konstruktiv: Von keiner einzigen explizit angegebenen rellen Zahl kann unter alleiniger Ausnutzung des Cantorschen Arguments die Transzendenz gezeigt werden.

10. Die Transzendenz von e

Die im vorigen Abschnitt beschriebenen Argumente liefern keine Ideen für den Beweis der Transzendenz von π, welcher in diesem Seminar entwickelt werden soll. Sie wurden nur deswegen gebracht, weil es sich um wichtige Elemente der mathematischen Allgemeinbildung handelt, welche damit verwandte Fragestellungen betreffen. Im Unterschied dazu kann der folgende Transzendenzbeweis von e zum Beweis einer allgemeineren Aussage ausgebaut werden, aus welcher in der Tat die Transzendenz von π folgt.

Theorem 3 (Hermite, 1873)**.** *Die Zahl e ist transzendent.*

Der Beweis wird den ganzen Rest dieses Abschnittes beanspruchen. Wir bringen einen Beweis von Hurwitz, den dieser aufbauend auf einer Vereinfachung des ursprünglichen Hermiteschen Beweises durch Hilbert 1893 publiziert hat.

Für ein Polynom $f \in \mathbb{C}[T]$ sei $F = F_f$ durch

$$F_f = \sum_{k=0}^{\infty} f^{(k)} \tag{1}$$

definiert, wobei die Reihe in Wahrheit endlich ist, weil $f^{(k)}$ für genügend große k verschwindet. Für den Transzendenzbeweis von e sind wir nur an dem Fall $f \in \mathbb{R}[T]$ interessiert. Dies soll also im Rest dieses Abschnittes vorausgesetzt werden.

Lemma 1. *Für alle $x \in [0, \infty)$ gilt $F(x) = e^x F(0) - xe^{x-y} f(y)$ mit einem $y \in [0, x]$.*

Beweis. Sei $g(x) = e^{-x} F(x)$, dann gilt $g'(x) = -e^{-x} f(x)$. Die Behauptung folgt aus dem Mittelwertsatz der Differentialrechnung:

$$F(x) - e^x F(0) = e^x \big(g(x) - g(0)\big) = xe^x g'(y) = -xe^{x-y} f(y),$$

wobei y im angegebenen Intervall liegt. □

Angenommen, e erfüllt eine algebraische Gleichung

$$\sum_{i=0}^{n} C_i e^i = 0 \tag{2}$$

mit rationalen Zahlen C_i und $C_n \neq 0$. Wir nehmen an, daß n minimal ist. Dann gilt $C_0 \neq 0$, denn sonst würde e die nichttrivale Gleichung

$$\sum_{i=0}^{n-1} C_{i+1} e^i = 0$$

von kleinerem Grad erfüllen. Durch Multiplikation mit einem gemeinsamen Nenner können wir voraussetzen, daß die C_i ganze Zahlen sind.

Wir betrachten für große p das Polynom

$$f_p(T) = \frac{1}{(p-1)!} T^{p-1} \prod_{i=1}^{n} (T - i)^p.$$

und definieren $F_p = F_{f_p}$ durch (1).

Lemma 2. *Es gilt*

$$\lim_{p \to \infty} \sum_{i=0}^{n} C_i F_p(i) = 0. \tag{3}$$

Beweis. In der Tat, nach Lemma 1 und (2) gilt

$$\sum_{i=0}^{n} C_i F_p(i) = -\sum_{i=1}^{n} iC_i e^{i-y_i} f_p(y_i)$$

mit $y_i \in [0, i]$, und die Summe ist betragsmäßig

$$\leq \frac{L \cdot K^p}{(p-1)!} \to 0 \qquad (\text{für } p \to \infty)$$

mit $L = \sum_{i=1}^{n} ie^i \left|C_i\right|$ und $K = (n+1)^{n+1}$. □

Das folgende Lemma führt nun unsere Annahme (2) ad absurdum.

Lemma 3.
- *Für $1 \leq i \leq n$ ist $F_p(i)$ eine durch p teilbare ganze Zahl.*
- *Für Primzahlen $p > n$ ist $F_p(0)$ eine nicht durch p teilbare ganze Zahl.*

Für Primzahlen $p > \max\big(\left|C_0\right|, n\big)$ ist also das p-te Glied in (3) eine nicht durch p teilbare und damit von 0 verschiedene ganze Zahl. Da es nach Folgerung 2.3 beliebig große Primzahlen gibt, ist dies ein Widerspruch zu (3). Es verbleibt der Beweis des Lemmas.

Beweis. Da Verwechslungen ausgeschlossen sind, unterdrücken wir umwillen kürzerer Bezeichnungen den Index p in $f = f_p$ und $F = F_p$. Für den ersten Punkt zerlegen wir

$$(+) \qquad f(T) = \frac{1}{(p-1)!} g(T) h(T)$$

mit $g(T) = (T-i)^p$ und

$$h(T) = T^{p-1} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (T-j)^p.$$

Dann hat h ganzzahlige Koeffizienten, und

$$g^{(k)}(i) = \begin{cases} p! & k = p \\ 0 & k \neq p. \end{cases}$$

Also

$$f^{(k)}(i) = \begin{cases} p\binom{k}{p} h^{(k-p)}(i) & k \geq p \\ 0 & k < p, \end{cases}$$

und dies ist eine durch p teilbare ganze Zahl. Dasselbe trifft dann auch für die Summe $F(i)$ dieser Zahlen zu.

Für den zweiten Punkt zerlegen wir f als $(+)$ mit $g(T) = T^{p-1}$ und $h(T) = \eta(T)^p$ mit $\eta(T) = \prod_{i=1}^{n}(T-i)$, einem Polynom mit ganzzahligen Koeffizienten. Ähnlich wie zuvor haben wir

$$g^{(k)}(0) = \begin{cases} (p-1)! & k = p-1 \\ 0 & k \neq p-1, \end{cases}$$

und

$$f^{(k)}(0) = \begin{cases} \binom{k}{p-1} h^{(k+1-p)}(0) & k \geq p-1 \\ 0 & k < p-1. \end{cases}$$

Insbesondere ist

$$f^{(p-1)}(0) = h(0) = (-1)^{np}(n!)^p$$

für Primzahlen $p > n$ eine nicht durch p teilbare ganze Zahl. Wegen

$$h'(T) = p\eta'(T)\eta(T)^{p-1}$$

sind die Koeffizienten von h' durch p teilbare ganze Zahlen. Dasselbe trifft dann auch auf die Koeffizienten der höheren Ableitungen von h zu. Also ist $f^{(k)}(0)$ für $k \neq p-1$ eine durch p teilbare ganze Zahl. In der (in Wahrheit endlichen) Summe

$$F(0) = \sum_{k=0}^{\infty} f^{(k)}(0)$$

treten also nur ganze Zahlen auf, und der k-te Summand ist genau für $k \neq p-1$ durch p teilbar. Die Summe ist also nicht durch p teilbar. □

11. Polynome in mehreren Variablen

Der in diesem Seminar präsentierte Transzendenzbeweis von π wird letztlich darauf beruhen, daß statt (10.2) die Gleichung

$$C + \sum_{i=1}^{n} e^{\alpha_i} = 0$$

ad absurdum geführt wird, wobei über alle Nulltellen eines durch T nicht teilbaren Polynomes $P \in \mathbb{Q}[T]$ summiert wird und C eine positive ganze Zahl ist. Für $\alpha_i = i$ würde man also (10.2) mit $C_0 = C$ sowie $C_i = 1$ für $1 \leq i \leq n$ erhalten. Die α_i sind aber nunmehr algebraische komplexe Zahlen. Um ein Analogon zu Lemma 10.3 anwenden zu können, benötigen wir den generell sehr wichtigen Hauptsatz über elementarsymmetrische Polynome. Wir beginnen mit der Definition von Polynomen in mehreren Veränderlichen, wobei wir uns in den Beweisen der Einfachheit halber auf Polynome mit Koeffizienten aus Unterringen von $\mathbb{C}$ beschränken.

Definition 1. Ein *Multiindex* in Dimension n ist eine Folge $\alpha = (\alpha_1, \ldots, \alpha_n)$ natürlicher Zahlen, also ein Element von $\mathbb{N}^n$. Man setzt

$$|\alpha| = \sum_{i=1}^{n} \alpha_i$$

$$\alpha! = \prod_{i=1}^{n} \alpha_i!$$

sowie, für n-Tupel $x = (x_1, \ldots, x_n)$ von Elementen eines kommutativen Ringes,

$$x^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i}.$$

Die Summe zweier Multiindizes wird komponentenweise gebildet.

Bemerkung 1. Der binomische Satz nimmt für Potenzen, deren Basis n-Tupel von Ringelementen und deren Exponenten Multiindizes sind, die Gestalt

$$(x \pm y)^\alpha = \sum_{\alpha=\beta+\gamma} \frac{\alpha!}{\beta!\gamma!} (\pm 1)^{|\gamma|} x^\beta y^\gamma \tag{1}$$

an, wobei über alle Darstellungen von α als Summe zweier Multiindizes summiert wird. Ferner gilt

$$x^{\alpha+\beta} = x^\alpha \cdot x^\beta.$$

Definition 2. Sei R ein Ring. Ein *Polynom in n Variablen* mit Koeffizienten aus R ist eine Folge $(p_\alpha)_{\alpha\in\mathbb{N}^n}$ von Elementen von R, so daß nur endlich viele $\alpha \in \mathbb{N}^n$ mit $p_\alpha \neq 0$ existieren. Wir bevorzugen normalerweise die Schreibweise als formale Linearkombination $P = \sum_{\alpha\in\mathbb{N}^n} p_\alpha X^\alpha$ mit einem fest gewählten n-Tupel $(X_1, \ldots, X_n)$ von Variablennamen und bezeichnen den Polynomring in diesen Veränderlichen dann mit $R[X_1, \ldots, X_n]$. Die Ringoperationen sind dabei durch

$$\begin{aligned}
(\sum_{\alpha\in\mathbb{N}^n} p_\alpha X^\alpha) + (\sum_{\alpha\in\mathbb{N}^n} q_\alpha X^\alpha) &= \sum_{\alpha\in\mathbb{N}^n} (p_\alpha + q_\alpha) X^\alpha \\
(\sum_{\alpha\in\mathbb{N}^n} p_\alpha X^\alpha) \cdot (\sum_{\alpha\in\mathbb{N}^n} q_\alpha X^\alpha) &= \sum_{\alpha\in\mathbb{N}^n} \Big(\sum_{\alpha=\beta+\gamma} p_\beta q_\gamma \Big) X^\alpha
\end{aligned}$$

gegeben. Den Funktionswert bildet man als

$$P(s) = \sum_{\alpha\in\mathbb{N}^n} p_\alpha s^\alpha, \tag{2}$$

wobei s ein n-Tupel von Elementen eines Erweiterungsringes von R ist. Der *Grad* von P ist

$$\deg P = \max\big\{ |\alpha| \;\big|\; p_\alpha \neq 0 \big\}$$

oder $-\infty$, wenn diese Menge leer ist. Ein Polynom ist *homogen von Grade d*, wenn $p_\alpha = 0$ für $|\alpha| \neq d$ gilt.

Bemerkung 2. Aus den Definitionen und aus der Gleichung $|\alpha + \beta| = |\alpha| + |\beta|$ für Multiindezes α und β folgt, daß das Produkt zweiter homogener Polynome vom Grad d und e homogen vom Grad $d + e$ ist. Die Summe zweier homogener Polynome vom Grad d ist homogen vom Grad d.

Bemerkung 3. Wenn P homogen vom Grad d ist, so gilt

$$P(\lambda s) = \lambda^d P(s). \tag{3}$$

Bemerkung 4. In der Definition von „Grad“ ist es oft nützlich, die einzelnen Variablen unterschiedlich zu gewichten. Sei $w = (w_1, \dots, w_n)$ eine Folge natürlicher Zahlen, wir setzen

$$|\alpha|_w = \sum_{i=1}^{n} w_i \alpha_i$$
$$\deg_w(P) = \max\{|\alpha|_w \mid p_\alpha \neq 0\}$$

wobei wie zuvor $\max \emptyset = -\infty$ genommen wird. Wir nennen P w-homogen vom Grad d, wenn $p_\alpha = 0$ für $|\alpha|_w \neq d$ gilt. In diesem Fall gilt

$$P(\lambda^{w_1} s_1, \dots, \lambda^{w_n} s_n) = \lambda^d P(s_1, \dots, s_n).$$

Im Fall $w = (1, \dots, 1)$ erhält man den normalen („ungewichteten“) Polynomgrad.

Bemerkung 5. Aus den Definitionen folgt ziemlich leicht

$$\deg_w(P_1 + P_2) \leq \max\big(\deg_w(P_1), \deg_w(P_2)\big)$$

mit Gleichheit, wenn die beiden Argumente von max verschieden sind. Insbesondere gilt dies für den gewöhnlichen Polynomgrad.

Wir sind vor allem an dem Fall interessiert, wo R ein Unterring von $\mathbb{C}$ und s in (2) ein Element von $\mathbb{C}^n$ ist. Wir merken aber an, daß die drei letzten Punkte des folgenden Satzes auch dann gelten, wenn Polynome mit Koeffizienten aus einem nullteilerfreien Ring betrachtet werden.

Satz 1. *Seien P und Q Elemente von $\mathbb{C}[X_1, \dots, X_n]$.*

- *Wenn P nicht verschwindet, ist*

$$\{z \in \mathbb{C}^n \mid P(z) \neq 0\} \tag{4}$$

  eine offene dichte Teilmenge von $\mathbb{C}^n$.
- *Wenn P und Q beide nicht verschwinden, so verschwindet auch PQ nicht.*
- *Es gilt*

$$\deg(PQ) = \deg(P) + \deg(Q). \tag{5}$$

- *Allgemeiner gilt*

$$\deg_w(PQ) = \deg_w(P) + \deg_w(Q). \tag{6}$$

Beweis. Aus den grundlegenden Resultaten über stetige Funktionen aus Analysis 1 und 2 folgt, daß $s \to P(s)$ eine stetige Funktion auf $\mathbb{C}$ und (4) offen ist. Es genügt also, die Dichtigkeit dieser Menge zu zeigen. Wir gehen durch Induktion nach n vor. Für $n = 1$ folgt die Behauptung aus der aus Lineare Algebra 1 bekannten Tatsache, daß P nur endlich viele Nullstellen hat. Sei $n > 1$, die Behauptung für Polynome in $n - 1$ Variablen gezeigt und $\varepsilon > 0$ sowie $x \in \mathbb{C}^n$ gegeben, wir müssen ein $y \in \mathbb{C}^n$ mit $|x - y| < \varepsilon$ und $P(y) \neq 0$ finden. Wir schreiben Elemente

von $\mathbb{C}^n$ als Paare (y', y_n) mit $y' = (y_1, \ldots, y_{n-1})$, verwenden eine analoge Schreibweise für Multi-Indizes und haben

$$P(y) = \sum_{k=0}^{\infty} P'_k(y') y_n^k \tag{@}$$

mit

$$P'_k(y') = \sum_{\alpha' \in \mathbb{N}^{n-1}} p_{(\alpha',k)} y'^{\alpha'}.$$

Dabei handelt es um ein Element von $\mathbb{C}[X_1, \ldots, X_{n-1}]$, welches wegen $P \neq 0$ für wenigstens ein $k \in \mathbb{N}$ von Null verschieden ist. Nach der Induktionsannahme gibt es ein $y' \in \mathbb{C}^{n-1}$ mit $|x' - y'| < \varepsilon/2$ und $P'_k(y') \neq 0$. Wird y' so gewählt, so gibt es wegen (@) und der Induktionsannahme ein y_n mit $P(y', y_n) \neq 0$ und $|x_n - y_n| < \varepsilon/2$. Die erste Behauptung ist damit gezeigt.

Die zweite Behauptung folgt aus der ersten und der Tatsache, daß der Durchschnitt zweier offener dichter Teilmengen eines metrischen Raumes M eine offene dichte Teilmenge von M ist.

Die dritte Behauptung ist ein Spezialfall der vierten. Um diese aus der zweiten herzuleiten, zerlegen wir Polynome als

$$P = \sum_{d=0}^{\infty} P_{d,w} \tag{7}$$

in w-homogene Komponenten, mit

$$P_{d,w}(X) = \sum_{|\alpha|_w = d} p_\alpha X^\alpha.$$

Wir haben

$$\deg_w P = \max\bigl\{ d \;\bigm|\; P_{d,w} \neq 0 \bigr\}$$

wobei $-\infty$ genommen wird, wenn die Menge leer ist.

Falls einer der Faktoren P oder Q verschwindet, sind beide Seiten der zu beweisenden Gleichung (5) gleich $-\infty$. Sei also $P \neq 0$ und $Q \neq 0$. Wir haben

$$(PQ)_{c,w} = \sum_{c=d+e} P_{d,w} Q_{e,w},$$

was für $c > \deg p + \deg q$ verschwindet und für $c = \deg p + \deg q$ zu

$$(PQ)_{\deg p + \deg q, w} = P_{\deg p, w} \cdot Q_{\deg q, w} \neq 0$$

führt, wobei die zweite Behauptung benutzt wurde. □

12. Der Hauptsatz über elementarsymmetrische Polynome

Ein Polynom $P = \sum_{\alpha\in\mathbb{N}^n} p_\alpha X^\alpha$ in n Variablen wird *symmetrisch* gennant, wenn

$$p_{\alpha_{\pi(1)},\dots,\alpha_{\pi(n)}} = p_\alpha$$

für alle Permutationen $\pi \in S_n$ und alle Multiindizes α gilt. Wir sind vor allem an Polynomen mit Koeffizienten aus Unterringen von $\mathbb{C}$ interessiert. In diesem Fall ist die Symmetrie äquivalent zu

$$P(z_{\pi(1)},\dots,z_{\pi(n)}) = P(z_1,\dots,z_n)$$

für alle $z \in \mathbb{C}^n$ und alle Permutationen π äquivalent.

Sei $0 \le k \le n$. Offenbar sind die Polynome

$$\sigma_k(X_1,\dots,X_n) = \sum_{\substack{S\subseteq\{1;\dots,n\}\\ \#(S)=k}} \prod_{i\in S} X_i$$

symmetrisch und homogen vom Grade k. Aus der Definition ergibt sich $\sigma_0 = 1$.

Satz 1. *Sei R ein kommutativer Ring und $P \in R[X_1,\dots,X_n]$ ein symmetrisches Polynom. Dann gibt es genau ein Polynom $Q \in R[X_1,\dots,X_n]$ mit*

$$P(X_1,\dots,X_n) = Q\big(\sigma_1(X_1,\dots,X_n),\dots,\sigma_n(X_1,\dots,X_n)\big), \tag{1}$$

und es gilt $\deg_w Q = \deg P$, mit dem Gewicht $w = (1,\dots,n)$.

Beweis. Der Einfachheit halber betrachten wir nur Unterringe $R \subseteq \mathbb{C}$, so daß der Polynomring mit einem Unterring des Ringes der $\mathbb{C}$-wertigen Funktionen auf $\mathbb{C}$ identifiziert werden kann, was die Interpretation von Gleichungen wie der obigen erleichtert. Wir beweisen nur die Existenz von Q mit $\deg_w(Q) \le \deg P$, die Eindeutigkeit und der genaue gewichtete Grad von Q werden für den Transzendenzbeweis von π nicht benötigt. Grundsätzlich gehen die untigen Betrachtungen aber für beliebige Ringe durch und können leicht zu einem Eindeutigkeitsbeweis von Q sowie zu einer Bestimmung von $\deg_w(Q)$. ergänzt werden.

Der Beweis erfolgt durch Induktion nach n. Für $n = 1$ kann $Q = P$ genommen werden. Sei $n > 1$ und die Behauptung für symmetrische Polynome in $n-1$ Variablen gezeigt.

Wir führen den Beweis für symmetrische Polynome in n Variablen durch Induktion nach dem Grad des Polynomes P. Ist dieser ≤ 0, so ist $P(z) = p_0$ eine Konstante für Q kann dieselbe Konstante p_0 genommen werden. Sei also $\deg P$ positiv und die Behauptung für symmetrische Polynome von kleinerem Grad in n Variablen gezeigt. Zunächst betrachten wir

$$P'(X_1,\dots,X_{n-1}) = P(X_1,\dots,X_{n-1},0) = \sum_{\alpha'\in\mathbb{N}^{n-1}} p_{\alpha',0} {X'}^{\alpha'},$$

ein symmetrisches Polynom in $n-1$ Variablen vom Grade $\le \deg P$. Nach der Induktionsannahme kann P' als

$$P'(X') = Q'\big(\sigma_1(X'),\dots,\sigma_{n-1}(X')\big) \tag{+}$$

dargestellt werden, wobei der mit $w' = (1, \dots, n-1)$ gewichtete Grad von Q' mit dem Grad von P' übereinstimmt und daher $\leq \deg P$ ist. Sei $Q_1(Y_1, \dots, Y_n) = Q'(Y_1, \dots, Y_{n-1}, 0)$ und

$$P_1(X_1, \dots, X_n) = Q_1\big(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)\big).$$

Aus der Definition folgt $\deg_w(Q) = \deg_{w'}(Q') \leq \deg P$. Dieses Polynom ist darstellbar als Summe

$$\sum_{\alpha \in \mathbb{N}^n} q_{1,\alpha} \prod_{i=1}^{n} \sigma_i(X)^\alpha.$$

Dabei ist $\prod_{i=1}^n \sigma_i(X)_i^\alpha$ ein Polynom vom Grad

$$\sum_{i=1}^{n} \alpha_i \deg(\sigma_i) = \sum_{i=1}^{n} \alpha_i \cdot i = |\alpha|_w ,$$

und wenn $q_{1,\alpha}$ nicht verschwindet, ist dieser Grad $\leq \deg P$. Also gilt $\deg P_1 \leq \deg P$ und auch der Grad von $P_2 := P - P_1$ ist $\leq \deg P$. Wegen $\sigma_n(X_1, \dots, X_{n-1}, 0) = 0$ sowie

$$\sigma_i(X_1, \dots, X_{n-1}, 0) = \sigma_i(X_1, \dots, X_{n-1})$$

für $0 \leq i < n$ gilt für $z' \in \mathbb{C}^{n-1}$ und $z = (z', 0)$

$$\begin{aligned} P(z) = P(z', 0) &= Q'(\sigma_1(z'), \dots, \sigma_{n-1}(z')) = Q_1(\sigma_1(z'), \dots, \sigma_{n-1}(z'), 0) \\ &= Q_1(\sigma_1(z), \dots, \sigma_n(z)) = P_1(z). \end{aligned}$$

Also verschwindet $P_2(z) = P(z) - P_1(z)$ für derartige z. Wegen

$$P_2(z', 0) = \sum_{\alpha' \in \mathbb{N}^{n-1}} p_{2,(\alpha',0)} {z'}^{\alpha'}$$

und Satz 11.1 folgt $p_{2,\alpha} = 0$ für alle α mit $\alpha_n = 0$. Auf Grund der Symmetrie des Polynomes gilt auch $p_{2,\alpha} = 0$, falls irgendein α_i mit $1 \leq i \leq n$ verschwindet. Es folgt

$$P_2(X) = (X_1 \cdot \ldots \cdot X_n)\tilde{P}_2(X) = \sigma_n(X)\tilde{P}_2(X)$$

mit $\deg \tilde{P}_2 = \deg P_2 - n \leq \deg P - n$. Insbesondere kann die innere Induktionsannahme auf $\tilde{P}_2$ angewendet werden:

$$\tilde{P}_2(X) = \tilde{Q}_2\big(\sigma_1(X), \dots, \sigma_n(X)\big)$$

mit $\deg_w \tilde{Q}_2 \leq \deg P - n$. Also gilt (1) mit

$$Q(Y_1, \dots, Y_n) = Q_1(Y_1, \dots, Y_n) + Y_n \tilde{Q}_2(Y_1, \dots, Y_n),$$

mit $\deg_w Q \leq \deg P$. □

Der soeben bewiesene Satz ist generell ziemlich wichtig. Für unsere Betrachtungen sind vor allem die beiden folgenden Folgerungen von Interesse.

Folgerung 1. *Seien $(\alpha_1, \dots, \alpha_n)$ komplexe Zahlen, so daß das Polynom*

$$F(T) = \prod_{i=1}^{n} (T - \alpha_i) \tag{2}$$

rationale (bzw. ganzzahlige) Koeffizienten hat. Wenn $P(X_1, \dots, X_n)$ ein symmetrisches Polynom mit rationalen (bzw. ganzzahligen) Koeffizienten ist, so ist $P(\alpha_1, \dots, \alpha_n)$ eine rationale (bzw. ganze) Zahl.

Beweis. Durch Ausmultiplizieren erhält man die folgende, generell sehr wichtige Beziehung zwischen den Koeffizienten f_i von F und den elementarsymmetrischen Polynomen:

$$f_i = (-1)^{n-i} \sigma_{n-i}(\alpha_1, \dots, \alpha_n). \tag{3}$$

Nach dem Hauptsatz über elementarsymmetrische Polynome gilt nun

$$\begin{aligned} P(\alpha_1, \dots, \alpha_n) &= Q\big(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)\big) \\ &= Q\big(-f_{n-1}, f_{n-2}, \dots, (-1)^{n-1} f_1, (-1)^n f_0\big), \end{aligned}$$

wobei das Polynom Q rationale (bzw. ganzzahlige) Koeffizienten hat und die f_i rationale (bzw. ganze) Zahlen sind. Die Behauptung folgt. □

Manchmal hat das Polynom F aus (2) rationale und das symmetrische Polynom P ganze Koeffizienten, und man möchte den Nenner der rationalen Zahl $P(\alpha_1, \dots, \alpha_n)$ kontrollieren. Dies leistet das folgende Ergebnis:

Folgerung 2. *Seien $(\alpha_1, \dots, \alpha_n)$ komplexe Zahlen, so daß das Polynom (2) rationale Koeffizienten hat, also*

$$\prod_{i=1}^{n} (T - \alpha_i) = T^n + \sum_{i=0}^{n-1} f_i T^i$$

mit $f_i \in \mathbb{Q}$. Wir setzen voraus, daß M eine positive ganze Zahl ist, so daß $M^{n-i} f_i \in \mathbb{Z}$ gilt. Zum Beispiel ist dies dann der Fall, wenn M ein gemeinsamer Nenner der rationalen Zahlen $f_0, \dots, f_{n-1}$ ist. Sei $P(X_1, \dots, X_n)$ ein symmetrisches Polynom mit ganzen Koeffizienten vom Grade $\leq d$. Dann ist $M^d P(\alpha_1, \dots, \alpha_n)$ eine ganze Zahl.

Beweis. Sei $\tilde{\alpha}_i = M\alpha_i$. Aus unseren Voraussetzungen folgt, daß $\tilde{F}(T) = \prod_{i=1}^{n} (T - \tilde{\alpha}_i)$ ganzzahlige Koeffizienten (nämlich $M^{n-i} f_i$ bei T^i) hat. Nach (11.7) existiert eine Zerlegung

$$P(X_1, \dots, X_n) = \sum_{e=0}^{d} P_e(X_1, \dots, X_n)$$

in Polynome P_e mit ganzzahligen Koeffizienten, die homogen vom Grade e sind. Weil eine Permutation der Indizes von α die Zahl $|\alpha|$ nicht ändert und P_e alle Polynomkoeffizienten

p_α von P mit $|\alpha| = e$ zusammenfaßt, ist P_e ein symmetrisches Polynom. Nach (11.3) und Folgerung 1 ist

$$M^d P(\alpha_1, \dots, \alpha_n) = \sum_{e=0}^{d} M^d P(\alpha_1, \dots, \alpha_n) = \sum_{e=0}^{d} M^{d-e} P(\tilde{\alpha}_1, \dots, \tilde{\alpha}_n)$$

ganzzahlig. □

13. Die Transzendenz von π, Teil I

Unser Ziel in den folgenden beiden Abschnitten ist der Beweis des folgenden Satzes:

Satz 1. *Sei $G \in \mathbb{Q}[T]$ ein normiertes Polynom mit $G(0) \neq 0$, und seien $(x_i)_{i=1}^n$ die komplexen Nullstellen von G, wobei mehrfache Nullstellen entsprechend ihrer Vielfachheit mehrfach aufgelistet sind, so daß*

$$G(T) = \prod_{i=1}^{n} (T - x_i) \tag{1}$$

gilt. Dann gilt

$$C + \sum_{i=1}^{n} e^{x_i} \neq 0$$

für alle positiven ganzen Zahlen C.

Aus dem Satz folgt

Theorem 4 (Lindemann, 1882)**.** *Die Zahl π ist transzendent. Insbesondere ist π nicht konstruierbar, und das klassische Problem der Quadratur des Kreises ist nicht mit Zirkel und Lineal lösbar.*

Beweis. Wegen $i^2 = -1$ ist die komplexe Zahl i algebraisch. Wenn π algebraisch wäre, so wäre also auch πi algebraisch. Angenommen, $Q \in \mathbb{Q}[T]$ ist ein nicht identisch verschwindendes Polynom mit $Q(i\pi) = 0$. Wir setzen voraus, daß der führende Koeffizient von Q gleich 1 ist. Dann hat Q die Form

$$Q = \prod_{i=1}^{m} (T - \theta_i)$$

mit komplexen Zahlen θ_i. Es gilt

$$\prod_{i=1}^{m} (1 + e^{\theta_i}) = 0, \tag{+}$$

denn unter den Faktoren taucht $1 + e^{i\pi} = 0$ auf. Andererseits stimmt (+) überein mit

$$\sum_{S \subseteq \{1;\dots;m\}} e^{\sum_{i \in S} \theta_i} = \sum_{j=1}^{2^m} e^{\alpha_j} \tag{@}$$

wobei wir annehmen, daß $(M_j)_{j=1}^{2^m}$ eine vollständige Auflistung aller Teilmengen von $\{1;\dots;m\}$ ist und

$$\alpha_j = \sum_{i\in M_j} \theta_i$$

setzen. Sei C die Zahl aller j mit $1 \le j \le 2^m$ und $\alpha_j = 0$. Wir haben $C > 0$, denn für $M_j = \emptyset$ gilt $\alpha_j = 0$. Wir dürfen annehmen, daß die Numerierung der M_j so vorgenommen wurde, daß $\alpha_j = 0$ genau für $2^m - C < j \le 2^m$ gilt. Wir haben $C > 0$, denn für $M_j = \emptyset$ gilt $\alpha_j = 0$. Dann nimmt (@) die Form

$$C + \sum_{j=1}^{2^m-C} e^{\alpha_j} \tag{\%}$$

Sei $G(T) = \prod_{j=1}^{2^m-C}(T-\alpha_j)$. Wir behaupten, daß G rationale Koeffizienten hat. Wenn dies der Fall ist, so steht das Verschwinden von (%) im Widerspruch zu Satz 1, und die Algebraizität von π ist ad absurdum geführt.

Es genügt, die Rationalität der Koeffizienten von

$$\tilde{G}(T) = T^C G(T) = \prod_{j=1}^{2^m}(T-\alpha_j)$$

zu zeigen. Dazu benutzen wir $\tilde{G}(T) = \sum_{i=0}^{n} \tilde{p}_i T^i$ mit Koeffizienten $\tilde{p}_i$, die nach (12.3) durch

$$\tilde{p}_i = (-1)^{n-i}\sigma_{n-i}(\alpha_1,\dots,\alpha_{2^m}) = (-1)^{n-i}\sigma_{n-i}\big(R_1(\theta_1,\dots,\theta_m),\dots,R_{2^m}(\theta_1,\dots,\theta_m)\big) \tag{\#}$$

mit den Polynomen

$$R_j(X_1,\dots,X_m) = \sum_{i\in M_j} X_i.$$

gegeben sind. Sei $\pi \in S_m$, dann gibt es eine Permutation $\rho \in S_{2^m}$ mit

$$M_{\rho(j)} = \big\{\pi(i) \;\big|\; i \in M_j\big\},$$

und wir haben $R_j(X_{\pi(1)},\dots,X_{\pi(m)}) = R_{\rho(j)}(X_1,\dots,X_m)$. Daraus folgt

$$\begin{aligned}\sigma_{n-i}\big(R_1(T_{\pi(1)},\dots,T_{\pi(m)}),\dots,R_{2^m}(T_{\pi(1)},\dots,T_{\pi(m)})\big)\\ = \sigma_{n-i}\big(R_{\rho(1)}(T_1,\dots,T_m),\dots,R_{\rho(2^m)}(T_1,\dots,T_m)\big)\\ = \sigma_{n-i}\big(R_1(T_1,\dots,T_m),\dots,R_{2^m}(T_1,\dots,T_m)\big).\end{aligned}$$

Die rechte Seite von (#) ist also ein symmetrisches Polynom mit rationalen Koeffizienten in $\theta_1,\dots,\theta_m$. Die behauptete Rationalität von $\tilde{p}_i$ folgt nun aus Folgerung 12.1. □

Es verbleibt der Beweis von Satz 1. Dieser wird neben dem Rest dieses Vortrages den ganzen nächsten Vortrag beanspruchen. Wir nehmen an, daß unter den Voraussetzungen des Satzes

$$C + \sum_{i=1}^{n} e^{x_i} = 0 \tag{2}$$

gilt, im Widerspruch zur Behauptung des Satzes. Um (2) ad absurdum zu führen, betrachten wir ähnlich wie beim Beweis von Theorem 3 für große p das Polynom

$$f_p(T) = \frac{T^{p-1}}{(p-1)!} \prod_{i=1}^{n} (T - x_i)^p \tag{3}$$

und definieren $F_p = F_{f_p}$ durch (10.1). Der in Lemma 10.1 benutzte Mittelwertsatz der Differentialrechnung ist nur für reellwertige Funktionen und $x \in \mathbb{R}$ richtig. Statt dessen haben wir

Lemma 1. *Die Beziehung zwischen f und $F = F_f$ sei durch (10.1) gegeben, dann gilt*

$$F(x) = e^x F(0) - x \int_0^1 e^{(1-\lambda)x} f(\lambda x)\, d\lambda$$

für alle komplexen Zahlen x.

Beweis. In der Tat, die Funktion $g(t) = e^{-tx} F(tx)$ hat die Ableitung $g'(t) = -xe^{-tx} f(tx)$, also

$$F(x) = e^x g(1) = e^x g(0) - e^x \int_0^1 g'(\lambda)\, d\lambda = e^x F(0) + x \int_0^1 e^{(1-\lambda)x} f(\lambda x)\, d\lambda$$

wie behauptet. □

Lemma 2. *Für jede natürliche Zahl N gilt*

$$\lim_{p\to\infty} N^p \Big(C F_p(0) + \sum_{i=1}^{n} F_p(x_i) \Big) = 0. \tag{4}$$

Der Term N^p mit $N > 1$ wird sich im Unterschied zu (10.3) dann als erforderlich erweisen, wenn die Koeffizienten von G keine ganzen Zahlen sind.

Beweis. Auf Grund von (2) und nach Lemma 1 ist das p-ten Folgenglied durch

$$-N^p \sum_{i=1}^{n} x_i \int_0^1 e^{(1-\lambda)x_i} f_p(\lambda x_i)\, d\lambda \tag{+}$$

gegeben. Sei $R = \max\big(1, |x_1|, \ldots, |x_n|\big)$. Der Betrag von (+) ist durch

$$\frac{L \cdot K^p}{(p-1)!} \to 0 \qquad \text{für } p \to \infty$$

beschränkt, mit $K = N 2^n R^{n+1}$ und $L = \sum_{i=1}^{n} e^{\max(\Re x_i, 0)}\, |x_i|$. □

14. Die Transzendenz von π, Teil 2

Wir nehmen weiterhin an, daß C und $(x_i)_{i=1}^n$ die Voraussetzungen von Satz 13.1 erfüllen und trotzdem (13.2) gilt, im Widerspruch zu Satz 13.1. Wir behalten die nach (13.2) eingeführten Bezeichnungsweisen f_p und F_p bei. Wir zeigen nun, daß sich ein Widerspruch zu (13.4) ergibt.

Zur Formulierung des Analogons von Lemma 10.3 geben wir zunächst unsere Voraussetzung über (13.1) auf und betrachten (13.3) mit beliebigen komplexen Zahlen $x_1, \ldots, x_n$. Zunächst bemerken wir, daß

$$f_p(T) = \frac{T^{p-1}}{(p-1)!} \prod_{i=1}^{n} (T - x_i)^p = \sum_{i=0}^{np+p-1} \phi_{p,i}(x_1, \ldots, x_n) T^i$$

gilt, wobei die $\phi_{p,i}$ symmetrische Polynome vom Grade $\leq np$ mit rationalen Koeffizienten in n Variablen $X_1, \ldots, X_n$ sind. Daraus ergibt sich

$$F_p(T) = \sum_{i=0}^{np+p-1} f_p^{(i)}(T) = \sum_{i=0}^{np+p-1} \Phi_{p,i}(x_1, \ldots, x_n) T^i,$$

wobei $\Phi_{p,i}(X_1, \ldots, X_n)$ ebenfalls ein symmetrisches Polynom vom Grade $\leq np$ mit rationalen Koeffizenten ist. Es folgt

$$CF_p(0) = A_p(x_1, \ldots, x_n)$$
$$\sum_{i=1}^{n} F_p(x_i) = B_p(x_1, \ldots, x_n),$$

wobei die Polynome $A_p(X_1, \ldots, X_n)$ (bzw. $B_p(X_1, \ldots, X_n)$) symmetrisch mit rationalen Koeffizenten und vom Grad $\leq np$ (bzw. $\leq 2np + p - 1$) sind. Sie sind eindeutig bestimmt durch die Forderung, daß die obigen Gleichungen für beliebige komplexe Zahlen $x_1, \ldots, x_n$ gelten, wenn f_p durch (13.3) und F_p durch (10.1) gegeben ist. Die Rolle von Lemma 10.3 wird nun von dem folgenden Lemma gespielt:

Lemma 1. *Wir haben*

$$A_p(X_1, \ldots, X_n) = (-1)^{np} C(X_1 \cdot \ldots \cdot X_n)^p + D_p(X_1, \ldots, X_n),$$

wobei D_p ein symmetrisches Polynom mit durch p teilbaren, ganzzahligen Koeffizienten in den X_i ist. Die Koeffizienten von B_p sind durch p teilbare ganze Zahlen.

Wenn das Lemma geglaubt wird, kann der Beweis von Satz 13.1 wie folgt beendet werden: Wir setzen nun wieder voraus, daß $(x_1, \ldots, x_n)$ die Voraussetzungen von Satz 13.1 über (13.1) erfüllen. Sei die positive ganze Zahl M ein gemeinsamer Nenner der Koeffizienten des Polynomes G. Wir wenden Lemma 1 an, wobei p eine Primzahl und hinreichend groß ist, nämlich größer als die natürlichen Zahlen C, M und $M\,|G(0)|$. Sei $N = M^{2n+1}$. Aus Folgerung 12.2 folgt dann, daß

$$N^p CF_p(0) = CM^{(2n+1)p} G(0)^p + M^{(2n+1)p} D_p(x_1, \ldots, x_n)$$

ganzzahlig ist, wobei der zweite Summand, nicht aber der erste Summand, durch p teilbar ist. Weiterhin ist

$$N^p \sum_{i=1}^{n} F_p(x_i) = M^{(2n+1)p} B_p(x_1, \dots, x_n)$$

eine durch p teilbare ganze Zahl. Die Summe

$$N^p \Big(C F_p(0) + \sum_{i=1}^{n} F_p(x_i) \Big)$$

dieser beiden Ausdrücke ist also eine nicht durch p teilbare ganze Zahl und daher betragsmäßig ≥ 1. Nach Folgerung 2.3 ist dies ein Widerspruch zu (13.4).

Es verbleibt der Beweis des letzten Lemmas. Von nun ab dürfen die x_i wieder beliebige komplexe Zahlen sein.

Beweis. Der Einfachheit halber unterdrücken wir den Index p und schreiben $f = f_p$, $F = F_p$, $A = A_p$ und $B = B_p$. Ähnlich dem Beweis von Lemma 10.3 betrachten wir zunächst $F(x_i)$ und zerlegen

$$f(T) = \frac{1}{(p-1)!} g_i(T) h_i(T)$$

mit $g_i(T) = (T - x_i)^p$ und

$$h_i(T) = T^{p-1} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (T - x_j)^p = \sum_{d=0}^{np-1} H_{i,d}(x_1, \dots, x_n) T^d,$$

wobei $H_{i,d} \in \mathbb{Z}[X_1, \dots, X_n]$ ist. Wegen

$$g_i^{(k)}(x_i) = \begin{cases} 0 & k \neq p \\ p! & k = p \end{cases}$$

folgt

$$f^{(k)}(x_i) = \begin{cases} 0 & k < p \\ p \binom{k}{p} h_i^{(k-p)}(x_i), & \end{cases}$$

und die rechte Seite ist ein (meistens unsymmetrisches) Polynom mit durch p teilbaren ganzzahligen Koeffizienten in den x_j. Durch Summation über k und i ergibt sich unsere Behauptung über die Polynome B.

Weiterhin haben wir $f(T) = \frac{1}{(p-1)!} g(T) h(T)$ mit $g(T) = T^{p-1}$ und

$$h(T) = \prod_{i=1}^{n} (T - x_i)^p = \sum_{d=0}^{\infty} H_d(x_1, \dots, x_n) T^d,$$

wobei $H_d \in \mathbb{Z}[X_1, \ldots, X_n]$ für $d > np$ verschwindet und

$$(+) \qquad H_0(X_1, \ldots, X_n) = (-1)^{np} \prod_{i=1}^{n} X_i^p$$

gilt. Wir haben $g^{(k)}(0) = 0$ für $k \neq p-1$ und $g^{(p-1)}(0) = (p-1)!$, also

$$f^{(k)}(0) = \begin{cases} 0 & k < p-1 \\ \binom{k}{p-1} h^{(k+1-p)}(0) = \frac{k!}{(p-1)!} H_{k+1-p}(x_1, \ldots, x_n) & k \geq p-1. \end{cases}$$

Für $k = p-1$ ist dies $H_0(x_1, \ldots, x_n)$ mit dem durch $(+)$ gegebenen Polynom H_0, für $k > p-1$ ist der Vorfaktor $\frac{k!}{(p-1)!}$ durch p teilbar und $H_{k+1-p}(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$. Die Behauptung über die C-fache Summe $A(X_1, \ldots, X_n)$ dieser Ausdrücke folgt. □