1. Erster Beweis des quadratischen Reziprozitätssatzes

(1.1) **Definition/Notation** $\zeta \in \mathbb{C}$ heißt n-te Einheitswurzel falls $\zeta^n = 1$ für $n \in \mathbb{N}_{>0}$. Ist n kleinste natürliche Zahl mit dieser Eigenschaft, heißt ζ primitive n-te Einheitswurzel. Die n-ten Einheitswurzeln sind 1, $e^{\frac{2\pi i}{n}k}$ mit $k = 1, ..., n-1$. Für k, n teilerfremd ist $e^{\frac{2\pi i}{n}k}$ primitive n-te Einheitswurzel.
Ist ζ n-te Einheitswurzel und $m \equiv l\ (n) \Rightarrow \zeta^m = \zeta^l$
Ist ζ primitive n-te Einheitswurzel und $\zeta^m = \zeta^l \Rightarrow m \equiv l\ (n)$
Sei im Folgenden $f(z) := e^{2\pi iz} - e^{-2\pi iz}$ $(= 2i\sin(2\pi z))$ Es gilt:
(i) $f(z+1) = f(z)$
(ii) $f(-z) = -f(z)$
(iii) r $\in \mathbb{R}$, 2r $\notin \mathbb{Z} \Rightarrow f(r) \neq 0$

(1.2) **Aussage** Für $n > 0$ ungerade, $\zeta = e^{\frac{2\pi i}{n}}$ und $x, y \in \mathbb{C}$ gilt

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)$$

Beweis 1,$\zeta, \zeta^2, ..., \zeta^{n-1}$ sind die n paarweise verschiedenen Nullstellen von $z^n - 1$ das heißt $z^n - 1 = \prod_{n=0}^{n-1}(z - \zeta^k)$. Ersetzt man z durch $\frac{x}{y}$ und multipliziert mit y^n durch, ergibt sich

$$x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k y)$$

k läuft 0,...,n-1 ab; da n ungerade ist, läuft $-2k$ mod n ebenfalls 0,...,n-1 ab

$$\Leftrightarrow \quad x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^{-2k} y)$$

$$\Leftrightarrow \quad x^n - y^n = \prod_{k=0}^{n-1} \zeta^{-k}(\zeta^k x - \zeta^{-k} y)$$

$$\Leftrightarrow \quad x^n - y^n = \zeta^{-(0+1+...+n-1)} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)$$

$$\Leftrightarrow \quad x^n - y^n = \zeta^{-\frac{(n-1)}{2}n} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)$$

$$\Leftrightarrow \quad x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)$$

□

(1.3) **Aussage** Für $n > 0$ ungerade, z keine Nullstelle von f gilt

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$$

Beweis Aus (1.2) folgt mit $x = e^{2\pi iz}$ und $y = e^{-2\pi iz}$

$$f(nz) = \left(e^{2\pi iz}\right)^n - \left(e^{-2\pi iz}\right)^n \overset{(1.2)}{=} \prod_{k=0}^{n-1} \left(\zeta^k e^{2\pi iz} - \zeta^{-k} e^{-2\pi iz}\right)$$

$$= \prod_{k=0}^{n-1} \left(e^{\frac{2\pi i}{n}k} e^{2\pi iz} - e^{-\frac{2\pi i}{n}k} e^{-2\pi iz}\right) = \prod_{k=0}^{n-1} \left(e^{2\pi i(\frac{k}{n}+z)} - e^{-2\pi i(\frac{k}{n}+z)}\right) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right)$$

Außerdem gilt $f\left(z + \frac{k}{n}\right) \overset{(i)}{=} f\left(z + \frac{k}{n} - 1\right) = f\left(z - \frac{n-k}{n}\right) =: (*)$

Es folgt

$$\frac{f(nz)}{f(z)} = \frac{f(z)}{f(z)} \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z + \frac{k}{n}\right)$$

$$\overset{(*)}{=} \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z - \frac{n-k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$$

Zur letzten Gleichheit: Wenn k von $\frac{n+1}{2}, ..., n-1$ läuft, läuft $n-k$ von $\frac{n-1}{2}, ..., 1$. Im letzten Schritt wird das zweite Produkt mit dem ersten zusammengefasst indem $n-k$ durch k ersetzt wird. Dabei ändert sich zwar die Reihenfolge der Faktoren, aber (da das Produkt endlich ist) nicht das Ergebnis.

□

Wiederholung Zum besseren Verständnis rufe man sich die Definition des Legendre-Symbols und die Formulierung des Gauß-Lemmas in Erinnerung, insbesondere die aus dem Beweis gewonnene Einsicht, dass zu gegebener Primzahl p gilt $\{m_1, ..., m_{\frac{(p-1)}{2}}\} = \{1, ..., \frac{(p-1)}{2}\} =: (\nmid)$, wobei m_l den Betrag des kleinsten Rests von la für $l \in \{1, ..., \frac{(p-1)}{2}\}$ bezeichnet.

(1.4) **Aussage** Sei p ungerade Primzahl, $a \in \mathbb{Z}, p \nmid a$. Dann gilt

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right)$$

Beweis Sei für $l = 1, ..., \frac{p-1}{2}$ $\quad la \equiv \pm m_l \ (p)$ wobei $m_l \in \left\{1, ..., \frac{p-1}{2}\right\}$, dh $\exists\, t_l \in \mathbb{Z}$:
$la = \pm m_l + t_l p \Leftrightarrow \frac{la}{p} = \frac{\pm m_l}{p} + t_l$. Es folgt $f\left(\frac{la}{p}\right) = f\left(\frac{\pm m_l}{p} + t_l\right) \overset{(i)}{=} f\left(\frac{\pm m_l}{p}\right) \overset{(ii)}{=} \pm f\left(\frac{m_l}{p}\right)$

Betrachte nun

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} \pm f\left(\frac{m_l}{p}\right) = (-1)^{\mu} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{m_l}{p}\right) \overset{Gauß}{=} \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{m_l}{p}\right) \overset{(\dagger)}{=} \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right)$$

□

(1.5) **Satz** (Quadratischer Reziprozitätssatz) Seien p, q zwei voneinander verschiedene, ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Beweis Nach (1.4) gilt

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right) \quad \Leftrightarrow \quad \left(\frac{q}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} \frac{f(lq/p)}{f(l/p)}$$

Nach (1.3) (mit q als n und $\frac{l}{p}$ als z) gilt

$$\frac{f(lq/p)}{f(l/p)} = \prod_{m=1}^{\frac{q-1}{2}} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right)$$

Insgesamt folgt

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right)$$

und mit analogen Überlegungen

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right)$$

Es gilt $f\left(\frac{m}{q} - \frac{l}{p}\right) = f\left(-\left(\frac{l}{p} - \frac{m}{q}\right)\right) \overset{(i)}{=} -f\left(\frac{l}{p} - \frac{m}{q}\right)$

Da das negative Vorzeichen $\frac{q-1}{2}\frac{p-1}{2}$ mal aus dem hinteren Faktor rausgezogen wird, folgt mit anschließendem Gleichsetzen

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

Mit einer Fallunterscheidung folgt die Aussage:

Da $p \neq q$, sind $\left(\frac{q}{p}\right), \left(\frac{p}{q}\right) \neq 0$. Da 1 keine Primzahl ist, wird der Ausdruck $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ebenfalls nie Null. Ist $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$, so haben $\left(\frac{q}{p}\right)$ und $\left(\frac{p}{q}\right)$ das gleiche Vorzeichen und ergeben miteinander

multipliziert 1. Ist $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$, so haben $\left(\frac{q}{p}\right)$ und $\left(\frac{p}{q}\right)$ unterschiedliche Vorzeichen und ergeben miteinander multipliziert -1. □

Wiederholung/Hilfsaussagen Für p Primzahl, $a, b \in \mathbb{Z}$ gilt

(H1) $a \equiv b \ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (H2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (H3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(1.6) **Aussage** Seien p, q zwei voneinander verschiedene, ungerade Primzahlen, $1 \leqslant a \in \mathbb{Z}$. Dann sind die folgenden Aassagen äquivalent:

(I) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

(II) Falls $p \equiv \pm q \ (4a), p \nmid a \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

Beweis "(I) $\Rightarrow$ (II)" Wegen Multiplikativität genügt es, die Aussage für a Primzahl zu beweisen (siehe unten).

1) Sei $a = 2$, dann folgt die Aussage aus 5.1.3[1]:

Vorüberlegung: Für $l, s \in \mathbb{Z}$ mit l=$8s$+[1,3,5,7] gilt $-l$=$-8(s$+$1)$+[7,5,3,1] (soll heißen für l=$8s$+1 ist $-l$=$-8(s$+$1)$+7 usw.)

– Falls $\left(\frac{a}{p}\right) = 1 \overset{5.1.3}{\Rightarrow}$ p hat die Form $8k+1$ oder $8k+7$ für ein $k \in \mathbb{Z}$. Wegen $p \equiv \pm q \ (8)$ folgt, dass es ein $t \in \mathbb{Z}$ gibt, sodass q die Form $8t+1$ oder $8t+7$ hat $\overset{5.1.3}{\Rightarrow} \left(\frac{a}{q}\right) = 1$

– Falls $\left(\frac{a}{p}\right) = -1 \overset{5.1.3}{\Rightarrow}$ p hat die Form $8k+3$ oder $8k+5$ für ein $k \in \mathbb{Z}$. Wegen $p \equiv \pm q \ (8)$ folgt, dass es ein $t \in \mathbb{Z}$ gibt, sodass q die Form $8t+3$ oder $8t+5$ hat $\overset{5.1.3}{\Rightarrow} \left(\frac{a}{q}\right) = -1$

2) Sei a eine ungrade Primzahl.

Fall 1: $p \equiv q \ (4a)$

Für geeignetes $t \in \mathbb{Z}$ gilt $p = q + 4at$ also gilt auch $p \equiv q \ (a)$. Mit (H1) folgt $\left(\frac{p}{a}\right) = \left(\frac{q}{a}\right)$. Es gilt

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{p}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{q}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}(-1)^{\frac{a-1}{2}\frac{q-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\frac{p+q-2}{2}}\left(\frac{a}{q}\right)$$

$p + q - 2 = q + q + 4at - 2 = 2(q-1) + 4at = 4(\frac{q-1}{2} + at)$ also $p + q - 2 \equiv 0 \ (4)$

Da $a - 1$ grade, $\frac{p+q-2}{4} \in \mathbb{Z}$ folgt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

Fall 2: $p \equiv -q \ (4a)$

Es gilt auch $p \equiv -q \ (a)$. Mit (H1) folgt $\left(\frac{p}{a}\right) = \left(\frac{-q}{a}\right)$. Es gilt

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{p}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{-q}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{-1}{a}\right)\left(\frac{q}{a}\right)$$

$$\overset{(H3)}{=} (-1)^{\frac{a-1}{2}\frac{p-1}{2}}(-1)^{\frac{a-1}{2}}\left(\frac{q}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}(-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}\frac{q-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\frac{p+q}{2}}\left(\frac{a}{q}\right)$$

$p + q = q - q + 4at = 4at$ also $p + q \equiv 0 \ (4)$ Da $a - 1$ grade, $\frac{p+q}{4} \in \mathbb{Z}$ folgt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

Zur Multiplikativität: Sei $a = \prod_{i=1}^{m} p_i^{e_i}$ die Primfaktorzerlegung von a. Dann gilt mit (H2) und (II)

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{m} \left(\frac{p_i}{p}\right)^{e_i} = \prod_{i=1}^{m} \left(\frac{p_i}{q}\right)^{e_i} = \left(\frac{a}{q}\right)$$

"(II) $\Rightarrow$ (I)" Sei oBdA $p > q$.
Vorüberlegung: Es gilt $\left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right)$ und $\left(\frac{a}{q}\right) = \left(\frac{4a}{q}\right)$
Fall 1: Sei $p \equiv q \ (4)$ dh $\exists\, a \geqslant 1 : \ p = q + 4a \Leftrightarrow p - q = 4a$. Betrachte nun

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) \overset{(H1)}{=} \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) \overset{(II)}{=} \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p-q}{p}\right) \overset{(H1)}{=} \left(\frac{-q}{p}\right) \overset{(H3)}{=} (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

– Falls $p \equiv 1 \ (4)$ ist $\frac{p-1}{2}$ gerade und daher gilt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. Da außerdem $p \equiv q \ (4)$, ist auch $\frac{q-1}{2}$ gerade und daher gilt $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$.
– Falls $p \equiv 3 \ (4)$ ist $\frac{p-1}{2}$ ungerade und daher gilt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. Da außerdem $p \equiv q \ (4)$, ist auch $\frac{q-1}{2}$ ungerade und daher gilt $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$.

Fall 2: Sei $p \equiv -q \ (4)$ dh $\exists\, a \geqslant 1 : \ p = -q + 4a \Leftrightarrow p + q = 4a$. Betrachte nun

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) \overset{(H1)}{=} \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) \overset{(II)}{=} \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) \overset{(H1)}{=} \left(\frac{q}{p}\right)$$

Also $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. Wegen $p \equiv -q \ (4)$ ist entweder $p \equiv 1 \ (4)$ oder, falls $p \equiv 3 \ (4) \Rightarrow -q \equiv 3 \ (4) \Rightarrow q \equiv 1 \ (4)$ also ist entweder $\frac{p-1}{2}$ oder $\frac{q-1}{2}$ gerade, also ergibt sich $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$.

In beiden Fällen wurde also die Gültigkeit der Formel $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ nachgewiesen. □

Bemerkung Für $r \in Z$ mit $r, 4a$ teilerfremd ist der quadratische Charakter von a (also der Wert des Legendre-Symbols) gleich für alle Primzahlen der Form $r + 4at, t \in Z$. In Kapitel 16[1] wird gezeigt, dass es unendlich viele Primzahlen dieser From gibt. Auch ist der quadratische Charakter der Primzahl $r + 4at$ identisch mit dem der Primzahl $-r + 4a$.
Die Formulierung des Gesetzes der quadratischen Reziprozität wie es in (1.5) bewiesen wurde, geht auf Eisenstein zurück. Durch ähnliches Vorgehen mit einer elliptischen statt einer trigonometrischen Funktion bewies er die kubische und bikubische Reziprozität.

2. Algebraische Zahlen und Integer

(2.1) **Definition** Eine algebraische Zahl ist eine Nullstelle $\alpha \in \mathbb{C}$ eines Polynoms
$$a_0x^n + a_1x^{n-1} + ... + a_n \text{ mit } a_0, ..., a_n \in \mathbb{Q},\ a_0 \neq 0$$
Ein algebraischer Integer ist eine Nullstelle $\alpha \in \mathbb{C}$ eines Polynoms
$$x^n + b_1x^{n-1} + ... + b_n \text{ mit } b_1, ..., b_n \in \mathbb{Z}$$

(2.2) **Aussage** Eine rationale Zahl $r \in \mathbb{Q}$ ist ein algebraischer Integer genau dann wenn $r \in \mathbb{Z}$
Beweis "$\Leftarrow$" Sei $r \in \mathbb{Z}$, dann ist r Nullstelle des Polynoms $x - r$ und somit algebraischer Integer.
"$\Rightarrow$" Sei $r \in \mathbb{Q}$ ein algebraischer Integer, dh die löse die Gleichung $x^n + b_1x^{n-1} + ... + b_n = 0$ mit $b_1, ..., b_n \in \mathbb{Z}$ Für geeignete $c, d \in \mathbb{Z}$ teilerfremd gilt $r = \frac{c}{d}$. Einsetzen in die Gleichung liefert

$\frac{c^n}{d^n} + b_1\frac{c^{n-1}}{d^{n-1}} + b_2\frac{c^{n-2}}{d^{n-2}} ... + b_n = 0 \qquad | * d^n$

$\Leftrightarrow \quad c^n + b_1c^{n-1}d + b_2c^{n-2}d^2 + ... + b_nd^n = 0$

$\Leftrightarrow \quad c^n = (-b_1c^{n-1} - b_2c^{n-2}d - ... - b_nd^{n-1})d$

Also teilt d c^n und wegen d, c teilerfremd, folgt $d \in \{\pm 1\}$, also $r \in \{\pm c\}$ also $r \in \mathbb{Z}$ □

(2.3) **Definition** Eine Teilmenge $V \subset \mathbb{C}$ heißt $\mathbb{Q}$-Modul falls
(a) $\gamma_1, \gamma_2 \in V \Rightarrow \gamma_1 \pm \gamma_2 \in V$ (b) $\gamma \in V, r \in \mathbb{Q} \Rightarrow r\gamma \in V$
(c) Es gibt $\gamma_1, ..., \gamma_l \in V$ sodass sich jedes $\gamma \in V$ schreiben lässt als $\gamma = \sum_{i=1}^{l} r_i\gamma_i$ mit $r_i \in \mathbb{Q}$

Bemerkung Insbesondere ist $V \subset \mathbb{C}$ ein $\mathbb{Q}$-Modul, falls V ein endlichdimensionaler Vektorraum über $\mathbb{Q}$ ist. Für $\gamma_1, ..., \gamma_l \in \mathbb{C}$ ist $\left\{ \sum_{i=1}^{l} r_i\gamma_i | r_1, ..., r_l \in \mathbb{Q} \right\}$ ein $\mathbb{Q}$-Modul. Schreibweise: $[\gamma_1, ..., \gamma_l]$

(2.4) **Aussage** Sei V=$[\gamma_1, ..., \gamma_l]$, $\alpha \in \mathbb{C}$ mit der Eigenschaft $\alpha\gamma \in V$ für alle $\gamma \in V$. Dann ist α eine algebraische Zahl.
Beweis Wegen $\alpha\gamma_i \in V$ für i=1,...,l folgt für geeignete $a_{ij} \in \mathbb{Q}$
$\alpha\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j \Leftrightarrow \sum_{j=1}^{l} a_{ij}\gamma_j - \alpha\gamma_i = 0 \Leftrightarrow \sum_{j=1}^{l} (a_{ij} - \delta_{ij}\alpha)\gamma_j$ für i=1,...,l
das heißt det((a_{ij})-$\alpha\mathbb{I}_l$)=0, also ist α Nullstelle des Polynoms l-ten Grades p(λ):=det((a_{ij})-$\lambda\mathbb{I}_l$) mit rationalen Koeffizienten. □

(2.5) **Aussage** Die Menge der algebraischen Zahlen bildet einen Körper.
Beweis Seien α_1, α_2 algebraische Zahlen.
1) Zeige: $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2$ sind algebraische Zahlen.
Da α_1, α_2 algebraische Zahlen sind, gibt es $r_i, s_j \in \mathbb{Q}$ sodass $\alpha_1^n + r_1\alpha_1^{n-1} + r_2\alpha_1^{n-2} + ... + r_n = 0$ und $\alpha_2^m + s_1\alpha_2^{m-1} + s_2\alpha_2^{m-2} + ... + s_m = 0$. Sei V das $\mathbb{Q}$-Modul, das von allen $\mathbb{Q}$-Linearkombinationen der Elemente $\alpha_1^i\alpha_2^j$ für $0 \leqslant i < n, 0 \leqslant j < m$ erzeugt wird. Zeige zunächst: für $\gamma \in V$ gilt $\alpha_1\gamma \in V$. Es gilt

$$\gamma = \sum_{k=1}^{mn} q_k\alpha_1^{i_k}\alpha_2^{j_k} \qquad \text{für geeignete } q_k \in \mathbb{Q}, i_k \in \{0, ..., n-1\}, j_k \in \{0, ..., m-1\}$$

Also ist

$$\alpha_1\gamma = \sum_{k=1}^{mn} q_k\alpha_1^{i_k+1}\alpha_2^{j_k}$$

Falls alle $i_k < n-1$ ist $\alpha_1\gamma \in V$ klar.
Sei jetzt $l \in \{0, ..., mn\}$ einziger Index mit $i_l = n-1$.
Es gilt $\alpha_1^n = -r_1\alpha_1^{n-1} - r_2\alpha_1^{n-2} - ... - r_n$. Eingesetzt liefert dies (wegen $i_l + 1 = n - 1 + 1 = n$)

$$\alpha_1\gamma = \sum_{\substack{k=1\\k\neq l}}^{mn} q_k\alpha_1^{i_k+1}\alpha_2^{j_k} \quad + \quad q_l(-r_1\alpha_1^{n-1} - r_2\alpha_1^{n-2} - ... - r_n)\alpha_2^{j_l}$$

$$= \sum_{\substack{k=1\\k\neq l}}^{mn} q_k\alpha_1^{i_k+1}\alpha_2^{j_k} \quad + \quad \underbrace{\sum_{f=1}^{n} \underbrace{(-q_l r_f)}_{\in\mathbb{Q}} \alpha_1^{n-f}\alpha_2^{j_l}}_{\in V} \qquad \in V$$

Mit (2.3)(a) folgt $\alpha_1\gamma \in V$.
Falls für mehrere Indizes i_k den Wert $n-1$ annimmt, werden entsprechend mehrere Summen rausgezogen und (2.3)(a) wiederholt angewendet. $\alpha_2\gamma \in V$ für $\gamma \in V$ folgt analog.
Insgesamt gilt $\alpha_1(\alpha_2\gamma) = (\alpha_1\alpha_2)\gamma \in V$ und $\alpha_1\gamma + \alpha_2\gamma = (\alpha_1 + \alpha_2)\gamma \in V$ für alle $\gamma \in V$. Mit (2.4) folgt, dass $\alpha_1\alpha_2$ und $\alpha_1 + \alpha_2$ algebraische Zahlen sind.

2) Zeige: Für $\alpha \neq 0$ algebraische Zahl ist α^{-1} ebenfalls algebraische Zahl.
Es existieren $a_0, ..., a_n \in \mathbb{Q}$ sodass $a_0\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0$. Dabei ist nach Definition $a_0 \neq 0$, es kann aber ohne Beschränkung auch $a_n \neq 0$ angenommen werden. (Falls $a_n = 0$ teilt man die Gleichung so lange durch α, bis das absolute Glied $\neq 0$ ist.) Durchmultiplizieren dieser Gleichung mit α^{-n} liefert $a_0 + a_1\alpha^{-1} + ... + a_n\alpha^{-n} = 0$. Somit ist α^{-1} ebenfalls eine algebraische Zahl. □

Um jetzt zu zeigen, dass die algebraischen Integer einen Ring bilden, werden die Beweise von (2.4) und (2.5) leicht variiert.

(2.6) **Definition** Die Teilmenge $W \subset \mathbb{C}$ heißt $\mathbb{Z}$-Modul falls
(a) $\gamma_1, \gamma_2 \in W \Rightarrow \gamma_1 \pm \gamma_2 \in W$
(c) Es gibt $\gamma_1, ..., \gamma_l \in W$ sodass sich jedes $\gamma \in W$ schreiben lässt als $\gamma = \sum_{i=1}^{l} b_i\gamma_i$ mit $b_i \in \mathbb{Z}$

(2.7) **Aussage** Sei W ein $\mathbb{Z}$-Modul, sei $\beta \in \mathbb{C}$ mit der Eigenschaft $\beta\gamma \in V$ für alle $\gamma \in W$. Dann ist β ein algebraischer Integer.
Beweis Analog zum Beweis von (2.4), mit $a_{ij} \in \mathbb{Z}$. (Ausschreiben der Determinante $\det((a_{ij})\text{-}\delta_{ij}\beta)=0$ zeigt, dass β Nullstelle eines normierten Polynoms vom Grad l mit ganzzahligen Koeffizienten ist.)

(2.8) **Aussage** Die Menge der algebraischen Integer bildet einen Ring.
Beweis Analog zum Beweis von (2.5) 1)

Bemerkung Bezeichne den Ring der algebraischen Integer mit Ω. Für $\omega_1, \omega_2, \gamma \in \Omega$ schreibe $\omega_1 \equiv \omega_2 \ (\gamma)$ falls $\omega_1 - \omega_2 = \gamma\alpha$ für ein $\alpha \in \Omega$. Diese Kongruenzbezeichnung steht nicht in Konflikt mit der üblichen Kongruenzbezeichnung in $\mathbb{Z}$, da man zeigen kann, dass aus $\omega_1, \omega_2, \gamma \in \mathbb{Z}$ folgt, dass α ebenfalls aus $\mathbb{Z}$ sein muss: Aus $a, b, c \in \mathbb{Z}, c \neq 0$ mit $a \equiv_\Omega b \ (c)$, das heißt $a - b = c\alpha$ für ein

$\alpha \in \Omega$, folgt, dass $\frac{a-b}{c} = \alpha \in \mathbb{Q}$ und daher nach (2.2) $\alpha \in \mathbb{Z}$.

(2.9) **Aussage** Für $\omega_1, \omega_2 \in \Omega, p \in \mathbb{Z}$ Primzahl gilt $(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \ (p)$
Beweis Für $k = 1, ..., p-1$ gilt $p \mid \binom{p}{k}$, denn $\binom{p}{k} = \frac{p!}{k!(p-k)!} \Leftrightarrow p! = \binom{p}{k} \ k!(p-k)!$
p teilt $p!$, aber p teilt nicht $k!(p-k)!$ da dies ein Produkt ganzer Zahlen ist, die echt kleiner p (und somit zu p teilerfremd) sind. Also teilt muss p $\binom{p}{k}$ teilen.
Mit dem binomischen Lehrsatz (dem man anwenden kann, da Ω ein Ring mit 1 ist) folgt
$(\omega_1 + \omega_2)^p = \sum_{k=0}^{p} \binom{p}{k} \ \omega_1^k \omega_2^{p-k} = \binom{p}{0} \ \omega_1^0 \omega_2^p + \sum_{k=1}^{p-1} \binom{p}{k} \ \omega_1^k \omega_2^{p-k} + \binom{p}{p} \ \omega_1^p \omega_2^0 \equiv \omega_1^p + \omega_2^p \ (p)$ □

Bemerkung Eine n-te Einheitswurzel ist eine Lösung der Gleichung $x^n - 1$, daher sind alle Einheitswurzeln (und alle $\mathbb{Z}$-Linearkombinationen von Einheitswurzeln) algebraische Integer.

(2.10) **Aussage** Sei α algebraische Zahl, dann ist α Nullstelle eines eindeutig bestimmten, normierten, irreduziblen Polynoms $f(x) \in \mathbb{Q}[x]$. Für $g(x) \in \mathbb{Q}[x]$ mit $g(\alpha) = 0$ gilt $f(x) | g(x)$.
Beweis Zeige zunächst den zweiten Teil: Sei f beliebiges irreduzibles, normiertes Polynom mit $f(\alpha) = 0, g(x) \in \mathbb{Q}[x]$ beliebig mit $g(\alpha) = 0$.
Widerspruchsannahme: Es gelte $f(x) \nmid g(x)$. Dann ist 1 ggT von $f(x)$ und $g(x)$, für geeignete $h(x), t(x) \in \mathbb{Q}[x]$ gilt $f(x)h(x) + g(x)t(x) = 1$. Setzt man $x = \alpha$ ein, erhält man $0 = 1$ eine falsche Aussage, also muss $f(x) | g(x)$ gelten.
Damit folgt auch die Eindeutigkeit von f: Sei $\hat{f}(x) \in \mathbb{Q}[x]$ normiertes, irreduzibles Polynom mit $\hat{f}(\alpha) = 0$, dann gilt $f(x) | \hat{f}(x)$ und $\hat{f}(x) | f(x)$, also $f = \pm \hat{f}$. Da beide Polynome den führenden Koeffizienten 1 haben, muss $f = \hat{f}$ gelten. □

Bemerkung/Definition Das in (2.10) eindeutig definierte Polynom f hängt nur von α ab; es wird Minimalpolynom von α genannt. Hat f Grad n, bezeichnet man α als algebraische Zahl vom Grad n. Ein irreduzibeles Polynom $f(x) \in \mathbb{Q}$ vom Grad n ist Minimalpolynom seiner n paarweise verschiedenen Nullstellen. Sind α, β Nullstellen von f, bezeichnet man sie als zueinander konjugiert.
Sei nun $\mathbb{Q}[\alpha] := \{g(\alpha) \mid g(x) \in \mathbb{Q}[x]\}$ und $\mathbb{Q}(\alpha) := \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(x), h(x) \in \mathbb{Q}[x], h(\alpha) \neq 0 \right\}$

(2.11) **Aussage** Für $\alpha \in \Omega$ gilt $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$
Beweis $\mathbb{Q}[\alpha] \subset \mathbb{Q}(\alpha)$ ist klar. zzg: $\mathbb{Q}(\alpha) \subset \mathbb{Q}[\alpha]$. Sei $0 \neq h(\alpha) \in \mathbb{Q}[\alpha], f(x)$ das Minimalpolynom von α dann gilt nach (2.10) dass $f(x) \nmid h(x)$. Also ist 1 ggT von $f(x), h(x)$ und für geeignete $s(x), t(x) \in \mathbb{Q}[x]$ gilt $s(x)f(x) + t(x)h(x) = 1$. Für $x = \alpha$ ergibt sich (wegen $f(\alpha) = 0$) $t(\alpha)h(\alpha) = 1$, das heißt $h(\alpha)^{-1} = t(\alpha) \in \mathbb{Q}[\alpha]$. Betrachte jetzt ein beliebiges $\beta \in \mathbb{Q}(\alpha)$, dann existieren $g(x), h(x) \in \mathbb{Q}[x]$ sodass $\beta = g(\alpha)h(\alpha)^{-1} \in \mathbb{Q}[\alpha]$. □

(2.12) **Korollar** Ist α algebraische Zahl vom Grad n, dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$
Beweis Nach (2.11) ist dies gleichbedeutend mit $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$.
Zeige dazu, dass $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ eine Basis von $\mathbb{Q}[\alpha]$ über $\mathbb{Q}$ bilden. Zeige dazu, dass
1) $Spann_{\mathbb{Q}}\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\} = \mathbb{Q}[\alpha]$.
"$\subset$" ist klar.
"$\supset$" Sei $\beta \in \mathbb{Q}[\alpha]$ beliebig, dh $\exists\, g(x) \in \mathbb{Q}[x]$ sd $\beta = g(\alpha)$.
Es gilt $g(x) = f(x)p(x) + q(x)$ für f Minimalpolynom von α und geeignete $p, q \in \mathbb{Q}[x]$ wobei Grad(q)<Grad(f)=n gilt.
$\beta = g(\alpha) = f(\alpha)p(\alpha) + q(\alpha) \overset{f(\alpha)=0}{=} q(\alpha) \overset{q \in \mathbb{Q}[x]}{=} c_{n-1}\alpha^{n-1} + ... + c_0$ für geeignete $c_i \in \mathbb{Q}$, also liegt β in $Spann_{\mathbb{Q}}\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$

2) $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ sind linear unabhängig über $\mathbb{Q}$.
Angenommen sie sind nicht unabhängig, dann existieren $c_0, ..., c_n - 1 \in \mathbb{Q}$ von denen mindestens eins ungleich 0 ist, sodass $c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1} = 0$. Für $g(x) := c_0 + c_1 x + ... + c_{n-1}x^{n-1}$ gilt also $g(\alpha) = 0$. Nach (2.10) gilt $f(x)|g(x)$, dies kann aber nicht gelten, da $\text{Grad}(g) \leqslant n - 1 < n = \text{Grad}(f)$.
Also sind $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ linear unabhängig über $\mathbb{Q}$ und es gilt $n = \dim_{\mathbb{Q}}(\mathbb{Q}[\alpha]) = [\mathbb{Q}[\alpha] : \mathbb{Q}]$ $\square$

---

[1] Diese Angaben beziehen sich auf das unten genannte Buch, dessen Kapitel 5 §3 und 6 §1 als Vorlage für dieses Skript dienten:

Ireland, Kenneth & Rosen, Michael: A Classical Introduction to Modern Number Theory (Second Edition), New York, Springer-Verlag, 1990