Kubisches und biquadratisches Reziprozitätsgesetz

Bachelorarbeit

vorgelegt von

Helena Bergold

an der

Universität Konstanz

Fachbereich Mathematik und Statistik

Betreuer: Prof. Dr. Claus Scheiderer

Konstanz, 2015

Inhaltsverzeichnis

Kapitel 1

Einleitung

Seit Leonhard Euler (1707-1783) beschäftigen sich Mathematiker mit Reziprozitätsgesetzen. Doch was ist ein Reziprozitätsgesetz? Wird in der Mathematik von einem Reziprozitätsgesetz gesprochen, so ist eine Verallgemeinerung des quadratischen Reziprozitätsgesetzes gemeint. Das quadratische Reziprozitätsgesetz war historisch gesehen das erste Reziprozitätsgesetz. Dieses wurde von Euler formuliert und erstmals vollständig von Gauß bewiesen. Mit Hilfe des quadratischen Reziprozitätsgesetzes und dessen Ergänzungssätze ist es möglich quadratische Reste in endlichen Körpern zu bestimmen, d.h. zu einer vorgegebenen Primzahl p und einer ganzen Zahl a die Lösbarkeit der Gleichung $x^2 \equiv a \pmod{p}$ zu untersuchen. An dieser Stelle zur Erinnerung, die Aussage des quadratischen Reziprozitätsgesetzes für zwei verschiedene Primzahlen $p, q > 2$:

Gilt $p \equiv q \equiv 3 \pmod{4}$, so ist p genau dann ein quadratischer Rest modulo q, wenn q ein quadratischer Nichtrest modulo p ist.
Gilt jedoch $p \equiv 1 \pmod{4}$ oder $q \equiv 1 \pmod{4}$, so ist p genau dann ein quadratischer Rest modulo q, wenn q ein quadratischer Rest modulo p ist.

Für eine leichtere Untersuchung wurde das Legendre-Symbol $\left(\frac{a}{p}\right)_2$ eingeführt, an dessen Wert man direkt ablesen kann, ob a ein quadratischer Rest modulo p ist oder nicht. Mit dem Legendre-Symbol erhält man folgende Form des quadratischen Reziprozitätsgesetzes:

1.0.1 Satz (Quadratisches Reziprozitätsgesetz, QRG)**.** [1]
Für ungerade Primzahlen $p \neq q$ gilt:

$$\left(\frac{p}{q}\right)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)_2.$$

Um quadratische Reste auch für negative Zahlen, das heißt Primzahlen multipliziert mit einer Einheit in $\mathbb{Z}$, zu berechnen, benötigt man die Ergänzungssätze zum quadratischen Reziprozitätsgesetz.

1.0.2 Satz (Ergänzungssätze)**.** [2]
Für eine Primzahl $p > 2$ gilt:

(1) $\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$

(2) $\left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}}$

[1] siehe [ZT14, Kap.5, 2.8]
[2] siehe [ZT14, Kap.5, 2.9]

Wie bereits erwähnt, wurde das quadratische Reziprozitätsgesetz erstmals von Gauß vollständig bewiesen. Dieser versuchte direkt einen Beweis zu finden, der sich auch auf höhere Potenzen übertragen lässt, um Aussagen über Lösbarkeit von Gleichungen $x^n \equiv a \pmod{p}$ für ein $a \in \mathbb{Z}$ und eine Primzahl p treffen zu können. So kam es, dass Gauß sechs Beweise des quadratischen Reziprozitätsgesetz veröffentlichte. Die Frage der Lösbarkeit von Gleichungen $x^n \equiv a \pmod{p}$ oder allgemeiner die Lösbarkeit von Gleichungen $x^n = \alpha$ in einem endlichen Körper F für ein $\alpha \in F$ zu beantworten, stellte sich jedoch als schwierig heraus und ist Ziel der Untersuchung von Reziprozitätsgesetzen. In dieser Arbeit wird die Gleichung für $n = 3$ (kubisches Reziprozitätsgesetz) und $n = 4$ (biquadratisches Reziprozitätsgesetz) näher betrachtet. Die ersten vollständigen Beweise des kubischen und des biquadratischen Reziprozitätsgesetzes mit dessen Ergänzungssätzen wurde von Eisenstein im Jahr 1844 veröffentlicht. Eisenstein war es auch, der Kummers Versuch von einem allgemeinen Reziprozitätsgesetz in Kreisteilungskörpern weiterentwickelte und somit einen Spezialfall des allgemeinen Reziprozitätsgesetzes formulieren konnte.[3] Dieser Spezialfall wird auch für kubische und biquadratische Reste in den jeweiligen Kapiteln dieser Arbeit betrachtet werden.

Um biquadratische rationalen Gleichungen, d.h. Gleichungen der Form $x^4 \equiv a \pmod{p}$ mit $a \in \mathbb{Z}$ und einer Primzahl $p > 0$ auf Lösbarkeit zu untersuchen, reicht es nicht aus, sich auf den Ring $\mathbb{Z}$ der ganzen Zahlen zu beschränken. Man benötigt eine endliche Erweiterung dieses Ringes, wie nachfolgendes Beispiel aus [Lem00, S.185f] illustrieren soll.

1.0.3 Beispiel. Für eine ungerade, ganze Zahl $q \geq 3$, ist die ganze Zahl $S_q := 2^{2q} + 1$ niemals prim in $\mathbb{Z}$, denn es existiert eine Zerlegung

$$S_q = 2^{2q} + 1 = \underbrace{\left(2^q - 2^{\frac{q+1}{2}} + 1\right)}_{=: A_q} \cdot \underbrace{\left(2^q + 2^{\frac{q+1}{2}} + 1\right)}_{=: B_q}.$$

Fixiere im Folgenden eine ungerade, ganze Zahl $q \geq 3$, sodass $p = 4q + 1$ eine Primzahl ist. Insbesondere ist für ein solches q die ganze Zahl S_q nicht prim. Weiterhin gilt $p = 4q + 1 \equiv 5 \pmod{8}$, denn es ist $p \equiv 1 \pmod{4}$ nach Voraussetzung und $p \equiv 1 \pmod{8}$ ist nur für eine gerade Zahl q möglich. Mit dem bereits bekanntem quadratischen Reziprozitätsgesetz und dessen Ergänzungssatz gilt:

$$\begin{aligned} S_q = 2^{2q} + 1 &= 2^{\frac{p-1}{2}} + 1 \\ &\equiv \left(\frac{2}{p}\right)_2 + 1 && \text{(Eulers Kriterium)} \\ &= (-1)^{\frac{p^2-1}{8}} + 1 && \text{(nach Ergänzungssatz zu QRG 1.0.2)} \\ &= -1 + 1 = 0 \qquad (\text{mod } p). \end{aligned}$$

Also folgt mit Hilfe des quadratischen Reziprozitätsgesetzes, dass $S_q = A_q B_q$ durch p teilbar ist. Da p eine Primzahl ist, muss schon $p \mid A_q$ oder $p \mid B_q$ gelten.
Wie später in Satz 2.3.4 gezeigt werden wird, gibt es für Primzahlen p mit $p \equiv 1 \pmod{4}$ eine Darstellung als Summe zweier Quadrate. Sei $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ und $a \equiv 1 \pmod{2}$, sowie

[3] siehe [Lem00, S. vii]

$b \equiv 0 \pmod 2$.
Betrachte nun für einige kleine, ungerade ganze Zahlen $q \geq 3$, sodass $p = 4q + 1$ eine Primzahl ist, die Tabelle zur Untersuchung, welcher der beiden Fälle eintritt.

q	p	A	B	a	b	p teilt A_q ?	p teilt B_q ?
3	13	5	13	3	2	NEIN	JA
7	29	113	145	5	2	NEIN	JA
9	37	481	545	1	6	JA	NEIN
13	53	8065	8321	7	2	NEIN	JA
15	61	32513	33025	5	6	JA	NEIN
25	101	33546241	33562625	1	10	JA	NEIN
27	109	134201345	134234113	3	10	JA	NEIN
49	197	562949919866881	562949986975745	1	14	NEIN	JA

Nach genauerer Betrachtung dieser Tabelle, kann man einen Zusammenhang zwischen der Teilbarkeit von A_q und B_q mit der Restklasse von $\frac{b}{2}$ modulo 8 erkennen. Es liegt also folgende Vermutung nahe:

$$p \mid A_q \;\Leftrightarrow\; \frac{b}{2} \equiv \pm 3 \pmod 8 \quad \text{und} \tag{1.1}$$

$$p \mid B_q \;\Leftrightarrow\; \frac{b}{2} \equiv \pm 1 \pmod 8 \tag{1.2}$$

Um diese Vermutung zu zeigen, muss man die Restklasse von A_q und B_q modulo p berechnen. Dabei gilt:

$$2^q = 2^{\frac{p-1}{4}} = \left(2^{\frac{p-1}{2}}\right)^{\frac{1}{2}}$$

und $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}} = -1 \pmod p$ (vgl. Satz 1.0.2). Bis jetzt wurde nur die Teilbarkeit in $\mathbb{Z}$ untersucht. Damit man die Restklasse von $2^{\frac{p-1}{4}}$ modulo p berechnen kann, müssen wir den Ring $\mathbb{Z}$ der ganzen Zahlen erweitern, und betrachten im Weiteren die Teilbarkeit in dem Ring $\mathbb{Z}[i]$. Es folgt $2^{\frac{p-1}{4}} \equiv i \pmod \pi$ oder $2^{\frac{p-1}{4}} \equiv -i \pmod \pi$ für einen Teiler $\pi = a + bi$ von $p = \pi\overline{\pi}$.

Offensichtlich benötigt man, um die Restklasse von $2^{\frac{p-1}{4}}$ modulo p zu bestimmen, eine Erweiterung der ganzen Zahlen, die Gaußschen Zahlen $\mathbb{Z}[i]$. Der Ring $\mathbb{Z}[i]$ ist der Ganzheitsring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Im Kapitel zum biquadratischen Reziprozitätsgesetz wird die Lösbarkeit von Gleichung $x^4 = \alpha$ für ein $\alpha \in \mathbb{Z}[i]$ in einem endlichen Restklassenkörper $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ für ein Primelement π von $\mathbb{Z}[i]$ analysiert.

Auch im kubischen Fall genügt der Ring der ganzen Zahlen zur Untersuchung zunächst nicht aus. Zur Untersuchung des kubischen Reziprozitätsgesetzes wird der Ganzheitsring $\mathbb{Z}[\omega]$, genannt die Eisenstein-Zahlen, des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{(-3)}) = \mathbb{Q}(\omega)$ verwendet. Dabei ist $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ eine primitive dritte Einheitswurzel. Die Lösbarkeit der Gleichung $x^3 = \alpha$ wird dementsprechend für ein $\alpha \in \mathbb{Z}[\omega]$ in endlichen Restklassenkörpern der Form $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$

mit einem Primelement π von $\mathbb{Z}[\omega]$ betrachtet.

Für die Beweise der beiden hier untersuchten Reziprozitätsgesetze benötigen wir Gauß- und Jacobi-Summen als Hilfsmittel. Diese werden im ersten Kapitel eingeführt. In Kapitel 3 widmen wir uns dann dem kubischen Reziprozitätsgesetz und zum Abschluss in Kapitel 4 dem biquadratischen Reziprozitätsgesetz. Die Kapitel zu den beiden Reziprozitätsgesetzen sind ähnlich aufgebaut. Zunächst werden einige einfache Aussagen zu den Ganzheitsringen $\mathbb{Z}[\omega]$ und $\mathbb{Z}[i]$ gemacht, mit dessen Hilfe wir dann die jeweiligen Restsymbole definieren können. Im Anschluss werden dann die Reziprozitätsgesetze und deren Ergänzungssätze bewiesen. Zum Abschluss werden noch einige Anwendungen der Reziprozitätsgesetze gegeben, darunter auch der Beweis der Vermutung aus Beispiel 1.0.3.

Ich werde in dieser Arbeit Kenntnisse aus der algebraischen Zahlentheorie aus der Vorlesung [ZT14] von Prof. Dr. Claus Scheiderer voraussetzen und auch weitgehend die Notation daraus übernehmen.

Kapitel 2

Gauß- und Jacobi-Summen

Für die Beweise des kubischen und biquadratischen Reziprozitätsgesetzes in Kapitel 3.4 und 4.4 benötigen wir als Hilfsmittel die Theorie der Gauß- und Jacobi-Summen. Als Grundlage für diese beiden Summen dienen Charaktere auf endlichen Gruppen. Zur Vereinfachung werden in dieser Arbeit nur Charaktere auf endlichen Körpern $\mathbb{F}_p$, für eine Primzahl p, betrachtet. Üblicherweise wird ein Charakter jedoch allgemeiner auf endlichen abelschen Gruppen definiert (siehe [ZT14, Kap.6, 1.1]). Mit Hilfe von Charakteren ist es im Anschluss möglich, Gauß- und Jacobi-Summen zu definieren. Im Allgemeinen dienen die Theorien, die in diesem Kapitel untersucht werden, oft der Bestimmung der Anzahl von Lösungen einer Gleichung mit Koeffizienten in einem endlichen Körper. Diese Anwendungen werden hier jedoch nicht genauer betrachtet, da die Gauß- und Jacobi-Summen nur als Hilfsmittel für die Beweise des kubischen und des biquadratischen Reziprozitätsgesetzes dienen. Das gesamte erste Kapitel orientiert sich an [IR93, Kap. 8].

2.1 Charaktere auf $\mathbb{F}_p$

Charaktere sind Abbildungen, die auf einer endlichen abelschen Gruppe definiert sind. Im Rahmen dieser Arbeit ist es ausreichend, diese auf den Einheitengruppen endlicher Körper $\mathbb{F}_p$ mit p Elementen zu definieren. Dabei ist $p > 0$ eine Primzahl.
Mit Hilfe von Charakteren kann man die Anzahl von Lösungen einer Gleichung der Form $x^n = a$ untersuchen. Beispielsweise erhält man für die Anzahl N_a der Lösungen von $x^2 = a$: $N_a = 1 + \left(\frac{a}{p}\right)_2$. Ist a ein quadratischer Rest, so hat diese Gleichung zwei Lösungen, sonst ist sie nicht lösbar.
Im Weiteren werden Anwendungen der Charaktere nicht weiter berücksichtigt, da der Fokus dieser Arbeit auf der Bestimmung von kubischen und biquadratischen Resten liegt.

2.1.1 Definition. Ein *(multiplikativer) Charakter* auf $\mathbb{F}_p$ ist eine Abbildung $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ mit der Eigenschaft

$$\chi(ab) = \chi(a)\chi(b) \quad \text{für alle } a, b \in \mathbb{F}_p^*.$$

2.1.2 Beispiele.

(a) Das bereits aus der Zahlentheorie bekannte Legendre-Symbol $\left(\frac{\cdot}{p}\right)_2$ für eine ungerade Primzahl $p > 0$ ist ein Charakter von $\mathbb{F}_p^*$ in die Menge $\{-1, +1\}$ der zweiten Einheitswurzeln. Die multiplikative Eigenschaft wurde in [ZT14, Kap.2, 3.7] gezeigt.

(b) In Kapitel 3 und 4 werden als weitere Beispiele der kubische und der biquadratische Charakter eingeführt.

(c) Die Abbildung $\epsilon\colon \mathbb{F}_p^* \to \mathbb{C}^*$ mit $\epsilon(a) = 1$ für alle $a \in \mathbb{F}_p^*$ ist ein Charakter, genannt der *triviale Charakter* auf $\mathbb{F}_p$.

2.1.3 Bemerkung. Oft ist es hilfreich, den Definitionsbereich eines Charakters auf den gesamten endlichen Körper $\mathbb{F}_p$ zu erweitern. Setze die Abbildung χ eines Charakters dazu wie folgt fort

$$\chi(0) = 0, \text{ falls } \chi \neq \epsilon \qquad \text{und}$$
$$\epsilon(0) = 1.$$

Im Folgenden benötigen wir den kleinen Satz von Fermat aus [Alg13, Kap.3, 2.13], dessen Aussage als bekannt vorausgesetzt wird.

2.1.4 Satz (Kleiner Satz von Fermat)**.** *Für $a \in \mathbb{Z}$ und eine Primzahl $p > 0$ mit $p \nmid a$ gilt*

$$a^{p-1} \equiv 1 \pmod{p}.$$

2.1.5 Satz. *Sei χ ein Charakter auf $\mathbb{F}_p$ und $a \in \mathbb{F}_p^*$ beliebig. Dann gilt*

(a) $\chi(1) = 1$

(b) $\chi(a)$ *ist $(p-1)$-te Einheitswurzel*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

Beweis.

(a) Es gilt $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Da nach Definition $\chi(1) \neq 0$gilt, muss bereits $\chi(1) = 1$ sein.

(b) Wegen $a \neq 0$ in $\mathbb{F}_p$ gilt nach Fermats kleinem Satz 2.1.4 bereits $a^{p-1} = 1$ in $\mathbb{F}_p$ und folglich

$$1 \overset{(a)}{=} \chi(1) \overset{2.1.4}{=} \chi(a^{p-1}) = \chi(a)^{p-1}.$$

Damit ist $\chi(a)$ eine $(p-1)$-te Einheitswurzel.

(c) Mit (a) folgt: $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$ und somit $\chi(a)^{-1} = \chi(a^{-1})$. Außerdem gilt nach (b): $\chi(a) \in \mathbb{C}^*$ mit $1 = |\chi(a)| = \chi(a)\overline{\chi(a)}$, wodurch die zweite Gleichheit folgt.

□

2.1.6 Satz. *Sei χ ein Charakter auf $\mathbb{F}_p$, dann gilt:*

$$\sum_{t \in \mathbb{F}_p} \chi(t) = \begin{cases} 0, & \text{falls } \chi \neq \epsilon \\ p, & \text{falls } \chi = \epsilon \end{cases}$$

Beweis. Sei zunächst $\chi = \epsilon$. Dann ist $\sum\limits_{t \in \mathbb{F}_p} \chi(t) = \sum\limits_{t \in \mathbb{F}_p} 1 = p$.
Für $\chi \neq \epsilon$ existiert ein $a \in \mathbb{F}_p$ mit $\chi(a) \neq 1$. Setze $T := \sum\limits_{t \in \mathbb{F}_p} \chi(t)$. Dann folgt:

$$\chi(a)T = \sum_{t \in \mathbb{F}_p} \chi(at) = T.$$

Da $\chi(a) \neq 1$list, muss schon $T = 0$ gelten. □

2.1.7 Satz. *Die Charaktere auf $\mathbb{F}_p$ bilden eine Gruppe mit der Verknüpfung*

$$(\chi\lambda)(a) := \chi(a)\lambda(a)$$

für Charaktere χ und λ. Das neutrale Element ist der triviale Charakter ϵ und zu einem Charakter $\chi \neq \epsilon$ ist das inverse Element χ^{-1} in der Gruppe der Charakter durch $\chi^{-1}\colon \mathbb{F}_p^* \to \mathbb{C}^*$, $a \mapsto \chi(a)^{-1}$ gegeben.

Beweis. Der Satz wurde bereits in [ZT14, Kap. 6, 1.2] in allgemeinerer Form bewiesen. □

2.1.8 Satz. *Die Gruppe der Charaktere auf $\mathbb{F}_p$ ist zyklisch von Ordnung $p-1$.*
Insbesondere existiert für jedes $a \in \mathbb{F}_p^*$ mit $a \neq 1$ ein Charakter χ auf $\mathbb{F}_p$ mit $\chi(a) \neq 1$.

Beweis. Nach [ZT14, Kap.6, 1.4] ist die Gruppe der Charaktere auf $\mathbb{F}_p$ isomorph zu $\mathbb{F}_p^*$ und ist damit zyklisch von Ordnung $p-1$.
Für ein $a \in \mathbb{F}_p^*$ mit $a \neq 1$ ist $a = g^l$ für ein $l \in \mathbb{N}$ und einen Erzeuger g von $\mathbb{F}_p^*$. Wegen $a \neq 1$ gilt $(p-1) \nmid l$. Sei weiterhin $\chi_0(g^k) := e^{\frac{2\pi ik}{p-1}}$ für $0 \leq k < p$, dann ist χ_0 ein Erzeuger der Gruppe der Charaktere auf $\mathbb{F}_p$ und es folgt:

$$\chi_0(a) = \chi_0(g^l) = e^{\frac{2\pi il}{p-1}} \neq 1 \qquad (\text{denn } (p-1) \nmid l).$$

□

2.1.9 Korollar. *Sei G die Gruppe der Charaktere auf $\mathbb{F}_p$. Dann gilt für $a \in \mathbb{F}_p^*$ mit $a \neq 1$ die Gleichung $\sum\limits_{\chi \in G} \chi(a) = 0$.*

Beweis. Setze $S := \sum\limits_{\chi \in G} \chi(a)$. Da $a \neq 1$ existiert nach Satz 2.1.8 ein Charakter $\lambda \in G$ mit $\lambda(a) \neq 1$. Dann gilt

$$\lambda(a)S = \sum_{\chi \in G} (\lambda\chi)(a) \overset{2.1.8}{=} \sum_{\chi \in G} \chi(a) = S$$

und wegen $\lambda(a) \neq 1$ folgt $S = 0$. □

2.2 Die Gauß-Summe

Unter einer Gauß-Summe versteht man eine endliche Summe von Einheitswurzeln. Im Unterschied zu der Notation g_a von [IR93] für Gauß-Summen, werden hier Gauß-Summem mit G_a bezeichnet.

2.2.1 Definition. Sei χ ein Charakter auf $\mathbb{F}_p$ und $a \in \mathbb{F}_p$. Dann definieren wir die *Gauß-Summe auf $\mathbb{F}_p$ zum Charakter χ* durch

$$G_a(\chi) := \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at} \qquad \text{mit der primitven } p\text{-ten Einheitwurzel } \zeta = e^{\frac{2\pi i}{p}}.$$

Im Folgenden spielen die Gauß-Summen für $a = 1$ eine wichtige Rolle. Deshalb setzt man zur Abkürzung $G := G_1$.

Die Gauß-Summe kann man durch die folgenden Eigenschaften genauer bestimmen.

2.2.2 Satz. *Für einen nichttrivialen Charakter χ auf $\mathbb{F}_p$ und den trivialen Charakter ϵ gilt*

$$G_a(\chi) = \begin{cases} \chi(a^{-1})G(\chi), & \text{falls } a \neq 0 \\ 0, & \text{falls } a = 0 \end{cases}$$

und

$$G_a(\epsilon) = \begin{cases} 0, & \text{falls } a = 0 \\ p, & \text{falls } a \neq 0 \end{cases}.$$

Beweis. Sei $a \neq 0$ und $\chi \neq \epsilon$. Dann gilt:

$$\chi(a)G_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(at)\zeta^{at} = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta^t = G_1(\chi) = G(\chi)$$

und somit folgt $G_a(\chi) = \chi(a)^{-1}G(\chi) = \chi(a^{-1})G(\chi)$, denn es ist $\chi(a) \neq 0$.
Ist nun $a = 0$, so folgt:

$$G_0(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta^{0t} = \sum_{t\in\mathbb{F}_p} \chi(t) \overset{2.1.6}{=} 0.$$

Zeige nun die Behauptung für den trivialen Charakter $\chi = \epsilon$. Sei zunächst $a \neq 0$, so folgt:

$$G_a(\epsilon) = \sum_{t\in\mathbb{F}_p} \epsilon(t)\zeta^{at} = \sum_{t\in\mathbb{F}_p} \zeta^{at} = 0.$$

Dabei wurde im letzten Schritt verwendet das ζ eine primitive p-te Einheitswurzel ist, also die Identität $1 + \zeta + \ldots + \zeta^{p-1} = 0$ erfüllt. Für $a = 0$ folgt:

$$G_0(\epsilon) = \sum_{t\in\mathbb{F}_p} \epsilon(t)\zeta^{0t} = \sum_{t\in\mathbb{F}_p} 1 = p.$$

□

2.2.3 Satz. *Sei $\chi \neq \epsilon$ ein Charakter auf $\mathbb{F}_p$. Dann gilt $|G(\chi)| = \sqrt{p}$.*

Beweis. Wir werden die Summe $\sum_{a\in\mathbb{F}_p} G_a(\chi)\overline{G_a(\chi)}$ mit zwei verschiedenen Ansätzen berechnen und anschließend die Ergebnisse vergleichen.
Für $a \neq 0$ gilt nach Satz 2.2.2:

$$\overline{G_a(\chi)} \overset{2.2.2}{=} \overline{\chi(a^{-1})G(\chi)} = \chi(a)\overline{G(\chi)} \quad \text{und} \quad G_a(\chi) \overset{2.2.2}{=} \chi(a^{-1})G(\chi).$$

Durch Multiplikation beider Gleichungen folgt

$$G_a(\chi)\overline{G_a(\chi)} = \chi(a^{-1})G(\chi)\chi(a)\overline{G(\chi)} = G(\chi)\overline{G(\chi)} = |G(\chi)|^2.$$

Somit folgt für die Summe über alle Elemente $a \in \mathbb{F}_p$:

$$\sum_{a\in\mathbb{F}_p} G_a(\chi)\overline{G_a(\chi)} = \underbrace{G_0(\chi)\overline{G_0(\chi)}}_{=0 \text{ (nach 2.2.2)}} + (p-1)|G(\chi)|^2$$
$$= (p-1)|G(\chi)|^2. \tag{2.1}$$

Für die andere Variante gehen wir direkt über die Definition der Gauß-Summe. Es gilt:

$$G_a(\chi)\overline{G_a(\chi)} = \left(\sum_{x\in\mathbb{F}_p} \chi(x)\zeta^{ax}\right) \cdot \left(\overline{\sum_{y\in\mathbb{F}_p} \chi(y)\zeta^{ay}}\right)$$
$$= \sum_{x,y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Für die Summe über alle $a \in \mathbb{F}_p$ gilt:

$$\sum_{a\in\mathbb{F}_p} G_a(\chi)\overline{G_a(\chi)} = \sum_{a\in\mathbb{F}_p}\sum_{x,y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$$
$$= \sum_{x,y\in\mathbb{F}_p} \underbrace{\left(\sum_{a\in\mathbb{F}_p} \zeta^{a(x-y)}\right)}_{\substack{=p, \quad \text{für } y=x;\\ =0, \quad \text{für } y\neq x}} \chi(x)\overline{\chi(y)}$$
$$= p\sum_{x\in\mathbb{F}_p} \chi(x)\overline{\chi(x)}$$
$$= p\sum_{0\neq x\in\mathbb{F}_p} \chi(x)\chi(x)^{-1}$$
$$= p(p-1). \tag{2.2}$$

Nun führen wir die beiden Umformungen (2.1) und (2.2) zusammen, und erhalten

$$(p-1)|G(\chi)|^2 = (p-1)p \quad \Rightarrow \quad |G(\chi)| = \sqrt{p}.$$

□

Um den obigen Satz in Zukunft bei Rechnungen gut verwenden zu können, ist es hilfreich den Zusammenhang zwischen $\overline{G(\chi)}$ und $G(\overline{\chi})$ zu bestimmen. Dabei bezeichnet $\overline{\chi}$ den Charakter

$$\overline{\chi}: \mathbb{F}_p^* \to \mathbb{C}^*, a \mapsto \overline{\chi(a)}.$$

Da $\chi(a)$ für jedes $a \in \mathbb{F}_p^*$ eine $(p-1)$-te Einheitswurzel ist, gilt $\overline{\chi(a)} = \chi^{-1}(a)$ für jedes $a \in \mathbb{F}_p^*$ und folglich ist $\overline{\chi} = \chi^{-1}$.

2.2.4 Satz. *Für einen Charakter $\chi \neq \epsilon$ auf $\mathbb{F}_p$ gilt*

$$\overline{G(\chi)} = \chi(-1)G(\overline{\chi}).$$

Beweis. Aufgrund der Gleichung $1 = \chi(1) = \chi(-1)^2$ gilt $\chi(-1) = \pm 1$ und damit ist offensichtlich $\overline{\chi(-1)} = \chi(-1)$. Somit folgt

$$\overline{G(\chi)} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)\zeta^t} = \sum_{t\in\mathbb{F}_p} \chi(-1)\overline{\chi(-t)}\zeta^{-t} = \chi(-1)\sum_{t\in\mathbb{F}_p} \overline{\chi}(t)\zeta^t = \chi(-1)G(\overline{\chi}).$$

□

Als direkte Folgerung aus den letzten beiden Sätzen erhalten wir folgendes Korollar.

2.2.5 Korollar. *Sei $\chi \neq \epsilon$ ein Charakter auf $\mathbb{F}_p$. Dann gilt $G(\chi)G(\overline{\chi}) = \chi(-1)p$.*

2.3 Die Jacobi-Summe

Jacobi-Summen werden in Kapitel 3 ein nützliches Mittel sein, um das kubische Reziprozitätsgesetz zu beweisen. Dort werden wir jedoch die allgemeinere Version aus dem nächsten Abschnitt verwenden. Die Jacobi-Summen, wie sie in diesem Abschnitt zunächst eingeführt werden, ist eine endliche Summe vom Produkt zweier $(p-1)$-ten Einheitswurzeln. In den folgenden Sätzen werden die wichtigsten Zusammenhänge gezeigt, um später mit den Summen arbeiten zu können.

2.3.1 Definition. Seien χ, λ Charaktere auf $\mathbb{F}_p$. Definiere die *Jacobi-Summe zu* χ, λ wie folgt

$$J(\chi,\lambda) := \sum_{\substack{a,b\in\mathbb{F}_p,\\ a+b=1}} \chi(a)\lambda(b).$$

2.3.2 Satz. *Seien χ, λ zwei nichttriviale Charaktere und ϵ der triviale Charakter auf $\mathbb{F}_p$. Dann gilt:*

(a) $J(\epsilon,\epsilon) = p$

(b) $J(\epsilon,\chi) = 0$

(c) $J(\chi,\chi^{-1}) = -\chi(-1)$

(d) Falls $\chi\lambda \neq \epsilon$, so ist $J(\chi,\lambda) = \dfrac{G(\chi)G(\lambda)}{G(\chi\lambda)}$

Beweis.

(a) Es ist $J(\epsilon,\epsilon) = \sum_{a+b=1} \epsilon(a)\epsilon(b) = \sum_{a+b=1} 1 = p.$
Denn für ein festes $a \in \mathbb{F}_p$ ist durch die Gleichung $a + b = 1$ das Element $b \in \mathbb{F}_p$ eindeutig bestimmt.

(b) Es gilt $J(\epsilon,\chi) = \sum_{a+b=1} \epsilon(a)\chi(b) = \sum_{b\in\mathbb{F}_p} \chi(b) \overset{2.1.6}{=} 0.$

(c) $J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1\\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right) = \sum_{c\neq -1} \chi(c) \overset{2.1.6}{=} -\chi(-1).$
Dabei wurde im vorletzten Schritt $c = \frac{a}{1-a}$ substituiert. Für $a \in \mathbb{F}_p\backslash\{1\}$ ist $c \in \mathbb{F}_p\backslash\{-1\}$.

(d) Gelte $\chi\lambda \neq \epsilon$, dann folgt:

$$\begin{aligned} G(\chi)G(\lambda) &= \left(\sum_{x\in\mathbb{F}_p} \chi(x)\zeta^x\right) \cdot \left(\sum_{y\in\mathbb{F}_p} \lambda(y)\zeta^y\right) \\ &= \sum_{x,y\in\mathbb{F}_p} \chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_{t\in\mathbb{F}_p} \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t. \end{aligned} \tag{2.3}$$

Berechne nun die innere Summe zunächst für $t = 0$:

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_{x\in\mathbb{F}_p} \chi(x)\lambda(-x) = \lambda(-1)\sum_{x\in\mathbb{F}_p} (\chi\lambda)(x) \overset{\chi\lambda\neq\epsilon}{=} 0 = (\chi\lambda)(0)J(\chi,\lambda). \tag{2.4}$$

Berechne nun noch die innere Summe für $t \neq 0$. Dazu substituiere x und y durch x' und y', sodass wir obige Summe auf die Jacobi-Summe zurückführen können. Durch $x = tx'$ und $y = ty'$ sind x' und y' eindeutig bestimmt und es gilt $x + y = t \Leftrightarrow x' + y' = 1$. Folglich gilt

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = (\chi\lambda)(t) \sum_{x'+y'=1} \chi(x')\lambda(y') = (\chi\lambda)(t)J(\chi,\lambda). \tag{2.5}$$

Man erhält nun insgesamt durch Einsetzen der Gleichungen (2.4) und (2.5) in die Gleichung (2.3):

$$G(\chi)G(\lambda) = \sum_{t\in\mathbb{F}_p} (\chi\lambda)(t)J(\chi,\lambda)\zeta^t = J(\chi,\lambda)G(\chi\lambda).$$

Die Behauptung folgt, da wegen $\chi\lambda \neq \epsilon$ nach Satz 2.2.3 bereits $G(\chi\lambda) \neq 0$ gilt.

□

Wir können nun auch leicht den Betrag der Jacobi-Summe bestimmen.

2.3.3 Korollar. *Seien $\chi, \lambda \neq \epsilon$ zwei Charaktere auf $\mathbb{F}_p$ mit $\chi\lambda \neq \epsilon$. Dann ist $|J(\chi,\lambda)| = \sqrt{p}$.*

Beweis. Es ist

$$|J(\chi,\lambda)| \overset{2.3.2(d)}{=} \left|\frac{G(\chi)G(\lambda)}{G(\chi\lambda)}\right| \overset{2.2.3}{=} \frac{(\sqrt{p})^2}{\sqrt{p}} = \sqrt{p}.$$

□

Aus diesem Korollar erhalten wir zwei wichtige Konsequenzen für die Darstellungsform von Primzahlen.

2.3.4 Satz. *Sei p eine Primzahl.*

- *Ist* $p \equiv 1 \pmod 4$*, so kann man* p *als Summe zweier Quadrate schreiben, d.h. es existieren* $a, b \in \mathbb{Z}$*, sodass* $p = a^2 + b^2$*.*

- *Ist* $p \equiv 1 \pmod 3$*, so existiert eine Darstellung* $p = a^2 - ab + b^2$ *der Primzahl* p *für ganze Zahlen* $a, b \in \mathbb{Z}$*.*

Beweis.

- Sei $p \equiv 1 \pmod 4$, dann gilt $4|(p-1)$. Somit existiert ein Charakter χ der Ordnung 4 (z.B. $\chi = \lambda^{\frac{p-1}{4}}$ für den Erzeuger λ der Gruppe der Charaktere). Daher bildet χ in die Einheitengruppe $\{\pm 1, \pm i\}$ von $\mathbb{Z}[i]$ ab. Folglich gilt $J(\chi, \chi) = \sum_{s+t=1} \chi(s)\chi(t) \in \mathbb{Z}[i]$, also existiert eine Darstellung $J(\chi, \chi) = a + bi$ mit $a, b \in \mathbb{Z}$ und nach Korollar 2.3.3 folgt, dass $p = |J(\chi, \chi)|^2 = a^2 + b^2$ gilt.

- Für Primzahlen $p \equiv 1 \pmod 3$ funktioniert die Argumentation analog. Es existiert ein Charakter χ' mit Wertebereich $\{\pm 1, \pm\omega, \pm\omega^2\}$, wobei $\omega = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist. Somit erhalten wir anstelle von $J(\chi, \chi) \in \mathbb{Z}[i]$ bereits $J(\chi', \chi') \in \mathbb{Z}[\omega]$, also eine Darstellung $J(\chi', \chi') = a + b\omega$ mit $a, b \in \mathbb{Z}$. Folglich gilt $p = |a + b\omega|^2 = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$.

□

2.3.5 Bemerkung. Der erste Teil der obigen Aussage geht auf Fermat zurück, der zeigte, dass Primzahlen $p \equiv 1 \pmod 4$ als Summe zweier Quadratzahlen geschrieben werden können. Diese Darstellung ist eindeutig, falls $a, b > 0$, a ungerade und b gerade gefordert wird. Dies sieht man wie folgt:
Angenommen $p = a^2+b^2 = c^2+d^2$ für positive, ganze Zahlen a, b, c, d mit $a \equiv c \equiv 1 \pmod 2$ und $b \equiv d \equiv 0 \pmod 2$. Es gilt offensichtlich $\mathrm{ggT}(a, b) = \mathrm{ggT}(c, d) = 1$ und $0 < a, b, c, d < \sqrt{p}$. Weiterhin ist $(ad-bc)(ad+bc) = a^2d^2 - b^2c^2 = (p-b^2)d^2 - b^2c^2 = pd^2 - pb^2$. Dementsprechend folgt $p \mid (ad-bc)$ oder $p \mid (ad+bc)$. Angenommen $p \mid (ad+bc)$. Dann würde $p = ad+bc$ folgen, denn es gilt $0 < ad+bc < 2p$. Folglich wäre $p^2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2+(ac-bd)^2 = p^2+(ac-bd)^2$, also $ac - bd = 0$. Dies steht im Widerspruch zu $ac - bd \equiv 1 \pmod 2$.
Somit gilt $p \mid (ad - bc)$, woraus $ad - bc = 0$ folgt. Also $a = c$ und $b = d$.

Im Gegensatz dazu, ist für $p \equiv 1 \pmod 3$ keine Eindeutigkeit gegeben, denn

$$a^2 - ab + b^2 = (b-a)^2 - (b-a)b + b^2 = a^2 - a(a-b) + (a-b)^2.$$

So ist beispielsweise $7 = 2^2 - 2 \cdot 3 + 3^2 = 1^2 - 3 + 3^2$.
Diese Darstellung von Primzahlen $p \equiv 1 \pmod 3$ werden in Kapitel 3 noch eine wichtige Rolle spielen, ebenso wie die der Primzahlen $p \equiv 1 \pmod 4$ im Kapitel zu dem biquadratischen Reziprozitätsgesetz.

Für solche Primzahlen und allgemein für Primzahlen $p \equiv 1 \pmod n$ erhält man einen wichtigen Satz über die n-te Potenz der Gauß-Summe. Diesen werden wir später oft für den Fall $n = 3$ und $n = 4$ verwenden.

2.3.6 Satz. *Für eine Primzahl $p \equiv 1 \pmod{n}$ und einen Charakter χ auf $\mathbb{F}_p$ mit Ordnung $n > 2$ gilt*

$$G(\chi)^n = \chi(-1)p \prod_{i=1}^{n-2} J(\chi, \chi^i).$$

Beweis. Durch die Voraussetzung $p \equiv 1 \pmod{n}$ folgt die Existenz eines Charakters χ auf $\mathbb{F}_p$ mit Ordnung n. Nach Satz 2.3.2 (d) folgt $G(\chi)^2 = J(\chi, \chi)G(\chi^2)$, da nach Voraussetzung χ ein Charakter von Ordnung $n > 2$ ist, also $\chi, \chi^2 \neq \epsilon$. Durch Multiplikation der Gleichung mit $G(\chi)$ erhält man $G(\chi)^3 = J(\chi, \chi)G(\chi^2)G(\chi)$. Für $n = 3$ folgt nun die Behauptung, da $G(\chi)G(\chi^2) = G(\chi)G(\overline{\chi}) \overset{2.2.5}{=} \chi(-1)p$ gilt. Ist $n > 3$, so wende Satz 2.3.2 (d) auf χ und χ^2 an:

$$G(\chi)^3 = J(\chi, \chi)J(\chi, \chi^2)G(\chi^3).$$

Durch Iteration folgt

$$G(\chi)^{n-1} = J(\chi, \chi) \cdot \ldots \cdot J(\chi, \chi^{n-2})G(\chi^{n-1}).$$

Da $\chi^{n-1} = \chi^{-1} = \overline{\chi}$ gilt $G(\chi)G(\chi^{n-1}) = G(\chi)G(\overline{\chi}) \overset{2.2.5}{=} \chi(-1)p$. Also folgt die Behauptung durch Multiplikation der Gleichung mit $G(\chi)$. □

Eine ähnliche Aussage erhält man auch für die quadratische Gauß-Summe, d.h. die Gauß-Summe $G(\chi)$ mit einem Charakter χ der Ordnung 2 auf $\mathbb{F}_p$.

2.3.7 Satz. [1] *Sei χ ein nichttrivialer Charakter von Ordnung 2 auf $\mathbb{F}_p$ für eine ungerade Primzahl $p > 0$ (d.h. χ ist das Legendre-Symbol). Dann gilt:*

$$G(\chi)^2 = \chi(-1)p = (-1)^{\frac{p-1}{2}}p.$$

Beweis. Die zweite Gleichheit gilt nach den Ergänzungssätzen des quadratischen Reziprozitätsgesetz (siehe Satz 1.0.2). Zeige also nur die erste Gleichheit.
Berechne die Summe $\sum_{a \in \mathbb{F}_p} G_a(\chi)G_{-a}(\chi)$ auf zwei verschiedene Arten ähnlich wie im Beweis von Satz 2.2.3. Für $a \not\equiv 0 \pmod{p}$ gilt

$$G_a(\chi)G_{-a}(\chi) \overset{2.2.2}{=} \underbrace{\chi(a^{-1})\chi(-a^{-1})}_{=\chi(-1)\text{ , da }\chi\text{ Ordnung 2}} G(\chi)^2.$$

Für $a \neq 0$ in $\mathbb{F}_p$ gilt nach Satz 2.2.2: $G_0(\chi)^2 = 0$. Summieren über alle $a \in \mathbb{F}_p$ zeigt, dass

$$\sum_{a \in \mathbb{F}_p} G_a(\chi)G_{-a}(\chi) = \underbrace{G_0(\chi)^2}_{=0} + (p-1)\chi(-1)G(\chi)^2 = (p-1)\chi(-1)G(\chi)^2 \tag{2.6}$$

gilt. Außerdem ist

$$G_a(\chi)G_{-a}(\chi) = \sum_{x,y \in \mathbb{F}_p} \chi(x)\chi(y)\zeta^{ax-ay}.$$

[1] Dieser Satz ist abweichend von dem restlichen Kapitel aus [IR93, Kap.6, 3.2]

Für die Summe folgt nun

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} G_a(\chi)G_{-a}(\chi) &= \sum_{x,y\in\mathbb{F}_p} \underbrace{\left(\sum_{a\in\mathbb{F}_p} \zeta^{a(x-y)}\right)}_{\substack{=p, \text{ für } y=x;\\ =0, \text{ für } y\neq x}} \chi(x)\chi(y)\\ &= \sum_{x\in\mathbb{F}_p} p \underbrace{\chi(x)^2}_{=1 \text{ für } x\neq 0}\\ &= (p-1)p. \end{aligned} \tag{2.7}$$

Aus den Gleichungen (2.6) und (2.7) folgt

$$(p-1)p = (p-1)\chi(-1)G(\chi)^2$$

und da χ ein Charakter von Ordnung 2 ist, gilt $G(\chi)^2 = \chi(-1)^{-1}p = \chi(-1)p$. □

2.4 Verallgemeinerung der Jacobi-Summe

In dem vorhergehendem Abschnitt wurde die Jacobi-Summe für zwei Charaktere definiert. Nun wollen wir auch mehr als zwei Charaktere als Argumente der Jacobi-Summe zulassen, und verallgemeinern somit die Definition 2.3.1. Die Jacobi-Summe mit l Argumenten wird im Folgenden mit J^l bezeichnet.

2.4.1 Definition. Zu $l \in \mathbb{N}_{\geq 2}$ und den Charakteren $\chi_1, \ldots, \chi_l$ auf $\mathbb{F}_p$ definiere die verallgemeinerte Jacobi-Summe

$$J^l(\chi_1, \ldots, \chi_l) := \sum_{\substack{t_1,\ldots,t_l\in\mathbb{F}_p\\ t_1+\ldots+t_l=1}} \prod_{i=1}^{l} \chi_i(t_i) = \sum_{t_1+\ldots+t_l=1} \chi_1(t_1)\cdots\chi_l(t_l).$$

Für $l = 2$ stimmt diese Definition mit der früheren Definition 2.3.1 überein, d.h. es gilt $J^2(\chi_1, \chi_2) = J(\chi_1, \chi_2)$. Definiere außerdem

$$J_0^l(\chi_1, \ldots, \chi_l) := \sum_{\substack{t_1,\ldots,t_l\in\mathbb{F}_p\\ t_1+\ldots+t_l=0}} \prod_{i=1}^{l} \chi_i(t_i).$$

2.4.2 Satz. *Seien $\chi_1, \ldots, \chi_l$ Charaktere auf $\mathbb{F}_p$. Dann gilt:*

(a) $J_0^l(\epsilon, \ldots, \epsilon) = J^l(\epsilon, \ldots, \epsilon) = p^{l-1}$

(b) Falls als Argument der Jacobi-Summe J^l mindestens einmal der triviale Charakter ϵ und einmal ein nichttrivialer Charakter vorkommt, also falls es $i, j \in \{1, \ldots, l\}$ gibt, sodass $\chi_i = \epsilon$ und $\chi_j \neq \epsilon$ gilt. Dann ist:

$$J_0^l(\chi_1, \ldots, \chi_l) = J^l(\chi_1, \ldots, \chi_l) = 0.$$

(c) Gilt $\chi_l \neq \epsilon$, so ist

$$J_0^l(\chi_1, \ldots, \chi_l) = \begin{cases} 0, & \text{falls } \prod_{i=1}^{l} \chi_i \neq \epsilon \\ \chi_l(-1)(p-1)J^{l-1}(\chi_1, \ldots, \chi_{ll-1}), & \text{falls } \prod_{i=1}^{l} \chi_i = \epsilon \end{cases}$$

Beweis.

(a) Für $t_1, \ldots, t_{l-1} \in \mathbb{F}_p$ beliebig, aber fest, ist durch die Identität $t_1 + \ldots + t_l = 1$ oder $t_1 + \ldots + t_l = 0$ der l-te Summand t_l eindeutig bestimmt. Somit gilt

$$J_0^l(\epsilon, \ldots, \epsilon) = \sum_{t_1+\ldots+t_l=0} 1 = p^{l-1}.$$

Analog folgt

$$J^l(\epsilon, \ldots, \epsilon) = \sum_{t_1+\ldots+t_l=1} 1 = p^{l-1}.$$

(b) Da die Jacobi-Summe in ihren Argumenten symmetrisch ist, können wir ohne Einschränkung $\chi_1, \ldots, \chi_s$ nichttrivial und $\chi_{s+1} = \ldots = \chi_l = \epsilon$ für ein $0 < s < l$ annehmen. Erhalte somit

$$\begin{aligned} J_0^l(\chi_1, \ldots, \chi_l) &= \sum_{t_1+\ldots+t_l=0} \prod_{i=1}^{l} \chi_i(t_i) \\ &= \sum_{t_1+\ldots+t_l=0} \prod_{i=1}^{s} \chi_i(t_i) \\ &= p^{l-1-s} \sum_{t_1,\ldots,t_s \in \mathbb{F}_p} \prod_{i=1}^{s} \chi_i(t_i) \\ &= p^{l-1-s} \underbrace{\left(\sum_{t_1 \in \mathbb{F}_p} \chi_1(t_1) \right)}_{=0} \cdots \underbrace{\left(\sum_{t_s \in \mathbb{F}_p} \chi_s(t_s) \right)}_{=0} \\ &= 0 \qquad \text{(nach Satz 2.1.6).} \end{aligned}$$

Analog folgt

$$J^l(\chi_1, \ldots, \chi_l) = p^{l-1-s} \sum_{t_1,\ldots,t_s \in \mathbb{F}_p} \prod_{i=1}^{s} \chi_i(t_i) = 0.$$

(c) Es ist $J_0^l(\chi_1, \ldots, \chi_l) = \sum_{s \in \mathbb{F}_p} \left(\sum_{t_1+\ldots+t_{l-1}=-s} \prod_{i=1}^{l-1} \chi_i(t_i) \right) \chi_l(s)$. Ist $s = 0$, so ist $\chi_l(s) = 0$, da $\chi_l \neq \epsilon$ und somit verschwindet der gesamte Summand. Für $s \neq 0$ setze nun $t_i = -st_i'$.

Dann folgt

$$\sum_{t_1+\ldots+t_{l-1}=-s} \prod_{i=1}^{l-1} \chi_i(t_i) = \Big(\prod_{j=1}^{l-1} \chi_j\Big)(-s) \cdot \underbrace{\left(\sum_{t_1'+\ldots+t_{l-1}'=1} \prod_{i=1}^{l-1} \chi_i(t_i')\right)}_{=J^{l-1}(\chi_1,\ldots,\chi_{l-1})}.$$

Also ist

$$\begin{aligned} J_0^l(\chi_1,\ldots,\chi_l) &= J^{l-1}(\chi_1,\ldots,\chi_{l-1}) \sum_{s\neq 0} \chi_l(s) \cdot \prod_{i=1}^{l-1} \chi_i(-s) \\ &= J^{l-1}(\chi_1,\ldots,\chi_{l-1}) \Big(\prod_{i=1}^{l-1} \chi_i\Big)(-1) \sum_{s\neq 0} \Big(\prod_{i=1}^{l} \chi_i\Big)(s). \end{aligned}$$

Ist $\prod_{i=1}^{l} \chi_i \neq \epsilon$, so gilt nach Satz 2.1.6: $\sum_{s\neq 0} \Big(\prod_{i=1}^{l} \chi_i\Big)(s) = 0$, also folgt $J_0^l(\chi_1,\ldots,\chi_l) = 0$. Gilt andererseits $\prod_{i=1}^{l} \chi_i = \epsilon$, so ist $\sum_{s\neq 0} \Big(\prod_{i=1}^{l} \chi_i\Big)(s) = \sum_{s\neq 0} 1 = p-1$ und $\Big(\prod_{i=1}^{l-1} \chi_i\Big)(-1) = \chi_l^{-1}(-1) = \chi_l(-1)$. Folglich gilt $J_0^l(\chi_1,\ldots,\chi_l) = \chi_l(-1)(p-1)J^{l-1}(\chi_1,\ldots,\chi_{l-1})$.

□

2.4.3 Theorem. *Seien $\chi_1,\ldots,\chi_r$ nichttriviale Charaktere auf $\mathbb{F}_p$, sodass $\prod_{i=1}^{r} \chi_i \neq \epsilon$ gilt. Dann ist*

$$\prod_{i=1}^{r} G(\chi_i) = J^r(\chi_1,\ldots,\chi_r) G\Big(\prod_{i=1}^{r} \chi_i\Big).$$

Beweis. Es gilt

$$\begin{aligned} \prod_{i=1}^{r} G(\chi_i) &= \prod_{i=1}^{r} \left(\sum_{t_i\in\mathbb{F}_p} \chi_i(t_i)\zeta^{t_i}\right) \\ &= \sum_{t_1,\ldots,t_r\in\mathbb{F}_p} \left(\prod_{i=1}^{r} \chi_i(t_i)\right) \zeta^{t_1+\ldots+t_r} \\ &= \sum_{s\in\mathbb{F}_p} \left(\sum_{t_1+\ldots+t_r=s} \prod_{i=1}^{r} \chi_i(t_i)\right) \zeta^s. \end{aligned} \tag{2.8}$$

Für $s=0$ und mit der Voraussetzung $\prod_{i=1}^{r} \chi_i \neq \epsilon$ und nach Satz 2.4.2 (c) folgt:

$$\sum_{t_1+\ldots+t_r=0} \prod_{i=1}^{r} \chi(t_i) = J_0^r(\chi_1,\ldots,\chi_r) = 0.$$

Für $s \neq 0$ ersetze $t_i = st_i'$. Genau dann, wenn $\sum_{i=1}^{r} t_i = s$ gilt, ist $\sum_{i=0}^{r} t_i' = 1$. Somit gilt

$$\sum_{t_1+\ldots+t_r=s} \prod_{i=1}^{r} \chi_i(t_i) = \left(\prod_{i=1}^{r} \chi_i(s)\right) \cdot \sum_{t_1'+\ldots+t_r'=1} \prod_{i=1}^{r} \chi_i(t_i') = \left(\prod_{i=1}^{r} \chi_i\right)(s) \cdot J^r(\chi_1, \ldots, \chi_r).$$

Einsetzen in die Umformung (2.8) liefert

$$\prod_{i=1}^{r} G(\chi_i) = J^r(\chi_1, \ldots, \chi_r) \cdot \sum_{s\neq 0} \left(\prod_{i=1}^{r} \chi_i\right)(s)\, \zeta^s = J^r(\chi_1, \ldots, \chi_r) \cdot G\left(\prod_{i=1}^{r} \chi_i\right),$$

denn nach Voraussetzung gilt $\prod_{i=1}^{r} \chi_i \neq \epsilon$. □

2.4.4 Korollar. *Es seien $r > 2$ und $\chi_1, \ldots, \chi_r$ nichttriviale Charaktere mit $\prod_{i=1}^{r} \chi_i = \epsilon$. Dann gilt:*

$$\prod_{i=1}^{r} G(\chi_i) = \chi_r(-1) p J^{r-1}(\chi_1, \ldots, \chi_{r-1}).$$

Beweis. Nach Theorem 2.4.3 angewandt auf $\chi_1, \ldots, \chi_{r-1}$ mit $\prod_{i=1}^{r-1} \chi_i \neq \epsilon$ gilt

$$\prod_{i=1}^{r-1} G(\chi_i) = J^{r-1}(\chi_1, \ldots, \chi_{r-1}) G\Big(\underbrace{\prod_{i=1}^{r-1} \chi_i}_{=\chi_r^{-1}=\overline{\chi_r}} \Big).$$

Somit erhält man durch Multiplikation mit $G(\chi_r)$

$$\prod_{i=1}^{r} G(\chi_i) = G(\chi_r) G(\overline{\chi_r}) J^{r-1}(\chi_1, \ldots, \chi_{r-1}) \overset{2.2.5}{=} \chi_r(-1) p J^{r-1}(\chi_1, \ldots, \chi_{r-1}).$$

□

2.4.5 Korollar. *Seien wie zuvor $r > 2$, $\chi_1, \ldots, \chi_r \neq \epsilon$ Charaktere auf $\mathbb{F}_p$ und $\prod_{i=1}^{r} \chi_i = \epsilon$. Dann gilt:*

$$J^r(\chi_1, \ldots \chi_r) = -\chi_r(-1) J^{r-1}(\chi_1, \ldots \chi_{r-1}).$$

Beweis. Verwende die Gleichung (2.8) aus dem Beweis zu Theorem 2.4.3. Dabei ist zu beachten, dass diese auch ohne die Voraussetzung $\prod_{i=1}^{r} \chi_i \neq \epsilon$ des Theorems gilt. Zusammen mit der

Voraussetzung $\prod_{i=1}^{r} \chi_i = \epsilon$, führt dies zu

$$\begin{aligned}\prod_{i=1}^{r} G(\chi_i) &= J_0^r(\chi_1,\dots,\chi_r) + J^r(\chi_1,\dots,\chi_r) \sum_{s\neq 0} \left(\prod_{i=1}^{r} \chi_i\right)(s)\, \zeta^s \\ &= J_0^r(\chi_1,\dots,\chi_r) + J^r(\chi_1,\dots,\chi_r) \underbrace{\sum_{s\neq 0} \zeta^s}_{=-1} \\ &= \chi_r(-1)(p-1)J^{r-1}(\chi_1,\dots,\chi_{r-1}) - J^r(\chi_1,\dots,\chi_r) \quad \text{(nach Theorem 2.4.2 (c))}.\end{aligned}$$

Durch Anwendung von Korollar 2.4.4 folgt

$$\chi_r(-1)pJ^{r-1}(\chi_1,\dots,\chi_{r-1}) = \chi_r(-1)(p-1)J^{r-1}(\chi_1,\dots,\chi_{r-1}) - J^r(\chi_1,\dots,\chi_r)$$

und somit $J^r(\chi_1,\dots,\chi_r) = \chi_r(-1)J^{r-1}(\chi_1,\dots,\chi_{r-1})(p-1-p) = -\chi_r(-1)J^{r-1}(\chi_1,\dots\chi_{r-1})$. □

2.4.6 Satz. *Für Charaktere $\chi_1,\dots,\chi_r \neq \epsilon$ auf $\mathbb{F}_p$ gilt:*

(a) Falls $\prod_{i=1}^{r} \chi_i \neq \epsilon$, so ist $|J^r(\chi_1,\dots,\chi_r)| = p^{\frac{r-1}{2}}$

(b) Falls $\prod_{i=1}^{r} \chi_i = \epsilon$, so $|J^r(\chi_1,\dots,\chi_r)| = p^{\frac{r}{2}-1}$ und $|J_0^r(\chi_1,\dots,\chi_r)| = (p-1)p^{\frac{r}{2}-1}$

Beweis.

(a) Durch Betrachtung der Beträge folgt mit Theorem 2.4.3:

$$\left|\prod_{i=1}^{r} G(\chi_r)\right| = |J^r(\chi_1,\dots,\chi_r)| \left|G\left(\prod_{i=1}^{r} \chi_i\right)\right|.$$

Weiter gilt für $i \in \{1,\dots,n\}$: $\chi_i \neq \epsilon$ und somit nach Satz 2.2.3 $|G(\chi_i)| = \sqrt{p}$. Ebenso folgt

$$\left|G\left(\prod_{i=1}^{r} \chi_i\right)\right| = \sqrt{p}$$

aufgrund der Voraussetzung $\prod_{i=1}^{r} \chi_i \neq \epsilon$. Also gilt

$$|J^r(\chi_1,\dots,\chi_r)| = \sqrt{p}^{r-1} = p^{\frac{r-1}{2}}.$$

(b) Da nach Voraussetzung $\prod_{i=1}^{r} \chi_i = \epsilon$ und $\chi_r \neq \epsilon$ gilt, folgt $\prod_{i=1}^{r-1} \chi_i \neq \epsilon$. Folglich gilt nach Korollar 2.4.5 und Teilaussage (a):

$$|J^r(\chi_1,\dots,\chi_r)| \overset{2.4.5}{=} \underbrace{|\chi_r(-1)|}_{=1} \left|J^{r-1}(\chi_1,\dots,\chi_{r-1})\right| \overset{(a)}{=} p^{\frac{(r-1)-1}{2}} = p^{\frac{r}{2}-1}.$$

Weiterhin ist nach Satz 2.4.2

$$|J_0^r(\chi_1,\dots,\chi_r)| \overset{2.4.2}{=} |\chi_r(-1)(p-1)J^{r-1}(\chi_1,\dots,\chi_{r-1})| \overset{(a)}{=} (p-1)p^{\frac{r}{2}-1}.$$

□

Kapitel 3

Das kubische Reziprozitätsgesetz

In diesem Kapitel widmen wir uns dem kubischen Reziprozitätsgesetz. Dazu reicht im Gegensatz zum quadratischen Fall der Ring $\mathbb{Z}$ nicht aus. Dies haben wir für den biquadratischen Fall schon in dem Beispiel 1.0.3 der Einleitung gesehen und es lässt sich auch auf den kubischen Fall übertragen. Wir müssen somit den Ring $\mathbb{Z}$ erweitern und betrachten für $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ den Ganzheitsring $\mathbb{Z}[\omega]$ des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-3})$. Nachdem wir einige wichtige Eigenschaftes dieses Ringes $\mathbb{Z}[\omega]$ untersucht haben, können wir das kubische Restsymbol definieren und mit dessen Hilfe das kubische Reziprozitätsgesetz formulieren. Für den Beweis des kubischen Reziprozitätsgesetzes benötigen wir Gauß- und Jacobisummen von kubischen Charakteren, wie sie in Kapitel 2 eingeführt wurden. Das quadratische Reziprozitätsgesetz wurde in [ZT14] bewiesen, indem die Zerlegung von Primzahlen in einer zyklischen Erweiterung mit der Zerlegung in einer quadratischen Erweiterung verglichen wurden. Dieses Verfahren kann man auch im kubischen Fall anwenden, wie im letzten Abschnitt dieses Kapitels zu sehen ist. Allerdings führt dieses Verfahren nicht zu einem vollständigen Beweis des kubischen Reziprozitätsgesetzes.

3.1 Der Ring $\mathbb{Z}[\omega]$

Betrachte im Folgenden den Ganzheitsring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-3})$. Dieser hat die Form $\mathbb{Z}[\omega]$ für $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. Dabei ist ω eine primitive dritte Einheitswurzel, erfüllt also die Gleichung $\omega^2 + \omega + 1 = 0$. In diesem Abschnitt werden wir, wie in [IR93, Kap.9, §1 und §2] einige wichtige Eigenschaften dieses Ganzheitsringes zeigen. Die Beweise sind jedoch oft kürzer, da die Resultate aus [ZT14] verwendet werden.

3.1.1 Bemerkung.

(a) Der Ganzheitsring $\mathbb{Z}[\omega]$ ist ein euklidischer Ring mit der Norm

$$N : \mathbb{Z}[\omega] \to \mathbb{N}_0,\ \alpha = a + b\omega \mapsto a^2 - ab + b^2 = \alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{N}_0$$

als Wertefunktion. (Dies wurde in [ZT14, Aufg. 25] gezeigt.)
Insbesondere ist $\mathbb{Z}[\omega]$ ein Hauptidealring und somit auch faktoriell.

(b) Die Einheitengruppe des Ganzheitsringes $\mathbb{Z}[\omega]$ ist endlich und besteht aus der Menge $\mathcal{O}^*_{\mathbb{Q}(\sqrt{-3})} = \{\pm 1, \pm\omega, \pm\omega^2\}$ (siehe [ZT14, Aufg. 13]).

Im Folgenden wollen wir die Zerlegung von Primzahlen $p \in \mathbb{Z}$ in dem imaginär-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{-3})$ untersuchen. Zur Erinnerung nun ein Satz aus [ZT14, Kap.2, 3.10] zur Zerlegung von Primzahlen in quadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d})$ mit $d \equiv 1 \pmod 4$.

3.1.2 Satz. *Für $K = \mathbb{Q}(\sqrt{d})$ mit $d = 4k+1 \equiv 1 \pmod 4$ und für $d \in \mathbb{Z}$ quadratfrei gilt für die Zerlegung der Primzahl $p > 0$ in K:*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & (p \text{ verzweigt}), \quad \textit{falls } p \mid d \\ \mathfrak{p}_1\mathfrak{p}_2 & (p \text{ zerlegt}), \quad \textit{falls } p \nmid 2d \ \textit{ mit } \left(\frac{d}{p}\right)_2 = +1 \textit{ oder } p = 2 \textit{ mit } d \equiv 1 \pmod 8 \\ \mathfrak{p} & (p \text{ träge}), \quad \textit{falls } p \nmid 2d \textit{ mit } \left(\frac{d}{p}\right)_2 = -1 \textit{ oder } p = 2 \textit{ mit } d \equiv 5 \pmod 8 \end{cases}.$$

Daraus erhalten wir für die Zerlegung der Primzahlen in $K = \mathbb{Q}(\sqrt{-3})$:

3.1.3 Bemerkung. Sei p eine Primzahl. Dann gilt für die Zerlegung von p in $K/\mathbb{Q}$:

- $p = 3$ ist verzweigt, denn $p = 3 \mid d = -3$. Folglich können wir $p = u\pi^2$ schreiben für eine Einheit u und ein Primelement π. Es gilt $3 = -\omega^2(1-w)^2$. Dabei folgt aus der Eindeutigkeit der Primfaktorzerlegung, dass $1-\omega$ prim in $\mathbb{Z}[\omega]$ ist.
- Für $p \equiv 1 \pmod 3$ ist p zerlegt, denn es gilt $p \nmid 6 = -2d$ und $\left(\frac{-3}{p}\right)_2 = \left(\frac{-1}{p}\right)_2\left(\frac{3}{p}\right)_2 = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right)_2 = \left(\frac{1}{3}\right)_2 = 1$. Somit existiert $\pi \in \mathbb{Z}[\omega]$ prim mit $p = \pi\overline{\pi}$. Wobei $\pi \not\sim \overline{\pi}$.
- Primzahlen $p \equiv 2 \pmod 3$ sind träge und somit auch prim in $\mathbb{Z}[\omega]$. (Folgt aus Satz 3.1.2 und da für $p = 2$ die Kongruenz $d = -3 \equiv 5 \pmod 8$ gilt, und für $p \neq 2$ die Teilbarkeitsrelation $p \nmid 6 = -2d$ gilt, sowie $\left(\frac{-3}{p}\right)_2 = \left(\frac{-1}{p}\right)_2(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right)_2 = \left(\frac{2}{3}\right)_2 = -1$.)

Da jedes Primelement aus $\mathbb{Z}[\omega]$ über einer Primzahl aus $\mathbb{Z}$ liegt, sind die oben aufgeführten Primelemente alle Primelemente von $\mathbb{Z}[\omega]$.

3.1.4 Definition. [1] Eine Nichteinheit $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ heißt *primär*, falls $\alpha \equiv \pm 1 \pmod 3$ (in $\mathbb{Z}[\omega]$) ist.

3.1.5 Bemerkung. In dem gesamten Kapitel sind Teilbarkeitsrelationen immer bezüglich der Teilbarkeit in $\mathbb{Z}[\omega]$. Sind dabei alle beteiligten Elemente ganzzahlig, z.B. $a \equiv b \pmod c$ für $a, b, c \in \mathbb{Z}$, dann ist die Teilbarkeit in $\mathbb{Z}[\omega]$ äquivalent zu der in $\mathbb{Z}$.
Denn aus $a \equiv b \pmod c$ folgt $a - b = c\alpha$ für ein $\alpha = x + y\omega \in \mathbb{Z}[\omega]$, also $a - b = cx + cy\omega$. Folglich ist $y = 0$. Also auch $a \equiv b \pmod c$ in $\mathbb{Z}$. Aus der Teilbarkeit in $\mathbb{Z}$, folgt offensichtlich auch die Teilbarkeit in $\mathbb{Z}[\omega]$.

3.1.6 Satz. *Ein Element $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ ist genau dann primär, falls $a \equiv \pm 1 \pmod 3$ und $b \equiv 0 \pmod 3$ gilt.*

Beweis. Zeige die Behauptung nur für $\alpha \equiv 1 \pmod 3$, die Rechnung folgt analog für $\alpha \equiv -1 \pmod 3$. Es gibt also ein $\beta = c + d\omega \in \mathbb{Z}[\omega]$, sodass $\alpha - 1 = 3\beta$ gilt. Somit gilt

$$a - 1 + b\omega = 3c + 3d\omega.$$

Koeffizientenvergleich zeigt, dass $a \equiv 1 \pmod 3$ und $b \equiv 0 \pmod 3$ gilt. Die Rückrichtung ist klar. □

[1] Diese Definition und die nachfolgenden Sätze sind in [IR93] erst später (Seite 113f) aufgeführt.

3.1.7 Bemerkung. Ist $p \equiv 2 \pmod 3$ eine träge Primzahl, dann ist p bereits ein primäres Primelement von $\mathbb{Z}[\omega]$.

3.1.8 Satz. *Für $\alpha \in \mathbb{Z}[\omega]$ mit $\mathrm{ggT}(\alpha, 3) = 1$ sind genau zwei der zu α assoziierten Elementen primär.*
Insbesondere finden wir immer eine Einheit u, sodass $u\alpha \equiv 1 \pmod 3$ gilt.

Beweis. Sei nun $\alpha = a+b\omega \in \mathbb{Z}[\omega]$ beliebig mit $\mathrm{ggT}(\alpha, 3) = 1$. Dann gibt es die sechs assoziierten Elemente von α:

$$\begin{array}{llrcrcr}
(a) & \alpha & = & a & + & b\omega \\
(b) & \omega\alpha & = & -b & - & (b-a)\omega \\
(c) & \omega^2\alpha & = & -(a-b) & - & a\omega \\
(d) & -\alpha & = & -a & - & b\omega \\
(e) & -\omega\alpha & = & b & + & (b-a)\omega \\
(f) & -\omega^2\alpha & = & (a-b) & + & a\omega
\end{array}$$

Ist α primär, so gilt $a \equiv \pm 1 \pmod 3$ und $b \equiv 0 \pmod 3$. Dann ist auch $-\alpha$ primär, aber keines der anderen Assoziierten.
Sei nun α nicht primär, d.h. $3 \mid a$ oder $3 \nmid b$.
Ist $a \equiv b \equiv 0 \pmod 3$, so erhalten wir einen Widerspruch zur Voraussetzung $\mathrm{ggT}(\alpha, 3) = 1$. Ist $a \equiv 0 \pmod 3$ und $b \equiv \pm 1 \pmod 3$, so ist auch $b - a \equiv \pm 1 \pmod 3$ und somit sind genau $\omega^2\alpha$ und $-\omega^2\alpha$ primär.
Betrachte nun den Fall $a \equiv \pm 1$ und $b \equiv \pm 1 \pmod 3$. Ist $a \equiv b \equiv \pm 1 \pmod 3$, so ist $a - b \equiv 0 \pmod 3$, also genau $\omega\alpha, -\omega\alpha$ primär. Ist jedoch $a \equiv -b \pmod 3$. Dann ist $\alpha = a + b\omega \equiv a - a\omega \equiv a(1-\omega) \equiv \pm(1-\omega) \pmod 3$ und wir erhalten einen Widerspruch zur Voraussetzung $\mathrm{ggT}(\alpha, 3) = 1$. □

3.1.9 Bemerkung. In [IR93] wird eine andere Definition von primär verwendet. Dort wird ein Element $\alpha \in \mathbb{Z}[\omega]$ primär genannt, falls $\alpha \equiv -1 \pmod 3$. Dadurch bekommt man die Eindeutigkeit des assoziierten primären Elements zu einem beliebigen $\beta \in \mathbb{Z}[\omega]$ mit $\mathrm{ggT}(\beta, 3) = 1$.

3.1.10 Satz. *Für ein Primelement π von $\mathbb{Z}[\omega]$ ist der Restklassenkörper $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ ein endlicher Körper mit $N(\pi)$ Elementen.*

Beweis. Diese Aussage folgt direkt aus der Idealnorm (siehe [ZT14, Kap.2, 4.1]). □

Nun folgt eine zu Fermats kleinem Satz analoge Aussage in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

3.1.11 Korollar. [2] *Die Einheitengruppe $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ ist zyklisch von Ordnung $N(\pi) - 1$.*
Insbesondere gilt für $\alpha \in \mathbb{Z}[\omega]$ mit $\pi \nmid \alpha$:

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

Beweis. Folgt direkt aus Satz 3.1.10. □

[2] Dieses Korollar stammt im Gegensatz zu dem restlichen Abschnitt aus [IR93, Prop.9.3.2]

3.2 Das kubische Restsymbol

In diesem Abschnitt, der sich nach [IR93, Kap.9, §3] richtet, werden wir das kubische Restsymbol, welches das Pendant zu dem Legendre-Symbol im quadratischen Fall bildet, definieren. Dazu ist es notwendig, zunächst die Restklassen aller dritten Einheitswurzeln $1, \omega, \omega^2$ modulo eines Primelements $\pi \in \mathbb{Z}[\omega]$ mit $N(\pi) \neq 3$ zu betrachten.

3.2.1 Lemma. *Sei $\pi \in \mathbb{Z}[\omega]$ prim mit $N(\pi) \neq 3$, d.h. $\pi \not\sim 1-\omega$. Dann sind $1, \omega, \omega^2$ paarweise verschieden in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.*

Beweis. Angenommen $1 \equiv \omega \pmod{\pi}$. Dann gilt $\pi \mid 1-\omega$ und da $1-\omega$ prim und somit irreduzibel ist, muss $\pi \sim (1-\omega)$ gelten. Dies ist ein Widerspruch zur Voraussetzung $N(\pi) \neq 3$. Die beiden anderen Fälle $1 \equiv \omega^2 \pmod{\pi}$ und $\omega \equiv \omega^2 \pmod{\pi}$ können durch Multiplikation mit ω bzw. ω^2 auf den oben gezeigten Fall zurückgeführt werden. □

3.2.2 Bemerkung. Für $\pi \in \mathbb{Z}[\omega]$ prim mit $N(\pi) \neq 3$ ist $\{1, \omega, \omega^2\}$ eine zyklische Untergruppe von $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ mit Ordnung 3. Somit enthält $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ ein Element der Ordnung 3 und nach dem Satz von Lagrange gilt $3 \mid N(\pi) - 1$.

3.2.3 Satz. *Sei $\pi \in \mathbb{Z}[\omega]$ prim mit $N(\pi) \neq 3$ und $\alpha \in \mathbb{Z}[\omega]$ mit $\pi \nmid \alpha$. Dann existiert ein eindeutiges $m \in \{0,1,2\}$ mit:*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi}.$$

Beweis. Wegen $\pi \nmid \alpha$ gilt nach Korollar 3.1.11

$$\pi \mid \alpha^{N(\pi)-1} - 1. \tag{3.1}$$

Außerdem gilt, da ω eine primitive dritte Einheitswurzel ist, die Gleichheit
$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$. Setze $x = \alpha^{\frac{N(\pi)-1}{3}}$ in die Gleichung ein. Dann ist die linke Seite nach (3.1) durch π teilbar und da π prim ist, teilt π einen der Faktoren auf der rechten Seite. Also gilt $\pi \mid (\alpha^{\frac{N(\pi)-1}{3}} - \omega^m)$ für ein $m \in \{0,1,2\}$. Somit ist die Existenz gezeigt.
Die Eindeutigkeit von m folgt aus Lemma 3.2.1. □

3.2.4 Definition. Für ein Primelement $\pi \in \mathbb{Z}[\omega]$ mit $N(\pi) \neq 3$ und $\alpha \in \mathbb{Z}[\omega]$ definieren wir das kubische Restsymbol durch

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0, & \text{falls } \pi \mid \alpha \\ \omega^m \text{ mit } m \in \{0,1,2\}, \text{ sodass } \omega^m \equiv \alpha^{\frac{N(\pi)-1}{3}} \pmod{\pi}, & \text{falls } \pi \nmid \alpha \end{cases}.$$

Dies ist wohldefiniert nach dem vorhergehenden Satz 3.2.3.

Im Folgenden betrachten wir stets das kubische Restsymbol $\left(\frac{\cdot}{\pi}\right)_3$ für ein Primelement π von $\mathbb{Z}[\omega]$. Dabei ist das Restsymbol nur für Primelemente π mit $N(\pi) \neq 3$ (oder äquivalent: $\pi \not\sim (1-\omega)$) definiert. Sei im Folgenden, falls nicht anders vorausgesetzt, stets π ein solches Primelement aus $\mathbb{Z}[\omega]$ mit $N(\pi) \neq 3$.

3.2.5 Satz (Eigenschaften)**.** *Seien $\alpha, \beta \in \mathbb{Z}[\omega]$ und $\pi \in \mathbb{Z}[\omega]$ prim (mit $N(\pi) \neq 3$). Dann gilt:*

(a) $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \pmod{\pi}$

(b) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$

(c) $\alpha \equiv \beta \pmod{\pi} \Rightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

(d) Für $\pi' \sim \pi$ *gilt* $\left(\frac{\alpha}{\pi'}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3$

(e) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$

Beweis.

(a) Für $\pi \nmid \alpha$ folgt die Aussage direkt aus der Definition. Gilt $\pi \mid \alpha$, so ist $\left(\frac{\alpha}{\pi}\right)_3 = 0$ und $\alpha^{\frac{N(\pi)-1}{3}} \equiv 0 \pmod{\pi}$.

(b) Aus Teilaussage (a) erhält man:

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \overset{(a)}{\equiv} (\alpha\beta)^{\frac{N(\pi)-1}{3}} \equiv \alpha^{\frac{N(\pi)-1}{3}} \beta^{\frac{N(\pi)-1}{3}} \overset{(a)}{\equiv} \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$$

und aufgrund der Eindeutigkeit aus Satz 3.2.3 folgt die Gleichheit $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$ der Behauptung.

(c) Mit der Voraussetzung $\alpha \equiv \beta \pmod{\pi}$ folgt

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \equiv \beta^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}.$$

(d) Die Behauptung folgt direkt aus $N(\pi) = N(\pi')$.

(e) Da $N(\pi) = N(\overline{\pi})$ gilt, ist:

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} \equiv \overline{\alpha^{\frac{N(\pi)-1}{3}}} = \overline{\alpha}^{\frac{N(\pi)-1}{3}} = \overline{\alpha}^{\frac{N(\overline{\pi})-1}{3}} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3 \pmod{\overline{\pi}}.$$

□

3.2.6 Bemerkung. Für ein festes, echt-komplexes Primelement $\pi \in \mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi} \equiv 1 \pmod 3$ sieht man mit Hilfe der Identifizierung von $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ mit $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, dass $\chi_\pi := \left(\frac{\cdot}{\pi}\right)_3$ ein Charakter auf $\mathbb{F}_p$ ist. Ein solcher Charakter hat Ordnung 3 und wird *kubischer Charakter* genannt. Da $\chi_\pi^3 = \epsilon$ ist, ist die Ordnung von χ_π entweder 3 oder χ_π ist der triviale Charakter. Angenommen χ_π wäre ein trivialer Charakter, dann wäre die Abbildung

$$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega], x \mapsto x^3 \tag{3.2}$$

surjektiv. Der Restklassenkörper $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ ist nach Satz 3.1.10 ein endlicher Körper mit $N(\pi) = p$ Elementen. Es folgt direkt die Injektivität der Abbildung (3.2). Dies ist jedoch nicht möglich, da 1 und ω nach Lemma 3.2.1 in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ verschiedene Elemente sind, aber beide durch die Abbildung (3.2) auf 1 abgebildet werden.

3.2.7 Satz. [3] *Für einen endlichen Körper F mit $|F| = q$, $n \in \mathbb{N}$, $\alpha \in F^*$ und $d := \mathrm{ggT}(n, q-1)$ gilt:*

$$x^n = \alpha \text{ hat eine Lösung in } F^* \Leftrightarrow \alpha^{\frac{q-1}{d}} = 1 \text{ in } F.$$

Beweis. Da F ein endlicher Körper ist, ist F^* zyklisch erzeugt. Sei g der Erzeuger von F^* und setze $\alpha = g^a$ für ein $a \in \mathbb{N}$. Nun gilt:

$$\begin{aligned} x^n = \alpha \text{ hat Lösung in } F^* &\Leftrightarrow \exists\, y \in \mathbb{N} :\ g^{yn} = g^a \\ &\Leftrightarrow \exists\, y \in \mathbb{N} :\ yn \equiv a \pmod{(q-1)} \\ &\overset{(\star)}{\Leftrightarrow} d \mid a \\ &\Leftrightarrow \alpha^{\frac{q-1}{d}} = \left(g^{\frac{a}{d}}\right)^{q-1} = 1. \end{aligned}$$

Dabei gilt die Äquivalenz $(\star)$, denn: Existiert ein y, sodass $yn \equiv a \pmod{(q-1)}$, so gibt es eine Darstellung $yn - m(q-1) = a$ für ein $m \in \mathbb{N}$. Nach Wahl von d ist sowohl n, als auch $q-1$ durch d teilbar und folglich auch a.
Ist umgekehrt a durch d teilbar, so existiert ein $c \in \mathbb{Z}$ mit $dc = a$. Außerdem können wir den größten gemeinsamen Teiler d durch den euklidischen Algorithmus darstellen als $n\tilde{y} - m(q-1) = d$ für $\tilde{y}, m \in \mathbb{N}$. Durch Multiplikation mit c erhalte die Gleichung $n\tilde{y}c - mc(q-1) = a$, also existiert ein $y = \tilde{y}c \in \mathbb{N}$, sodass die behauptete Kongruenz modulo $q-1$ erfüllt ist. □

Damit folgt nun als Spezialfall:

3.2.8 Korollar. *Für $\alpha \in \mathbb{Z}[\omega]$ und $\pi \in \mathbb{Z}[\omega]$ prim mit $\pi \nmid \alpha$ gilt:*

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \Leftrightarrow x^3 \equiv \alpha \pmod{\pi} \text{ hat eine Lösung } x \in \mathbb{Z}[\omega].$$

Beweis. Die Behauptung folgt als Spezialfall aus Satz 3.2.7 mit $F = \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega], q = N(\pi), n = 3$ und somit $d = 3$. □

3.2.9 Bemerkung. Satz 3.2.8 zeigt, dass die Definition des kubischen Restsymbols ein Pendant zum Legendre-Symbols ist. Denn im quadratischen Fall wurde das Legendre-Symbol zunächst durch

$$\left(\frac{a}{p}\right)_2 = \begin{cases} 1, & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist.} \\ -1, & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

definiert. Dies entspricht der gerade für das kubische Restsymbol gezeigten Äquivalenz in Satz 3.2.8. Für das Legendre-Symbol gilt das Euler-Kriterium:

[3] siehe [IR93, 7.1.2]

Sei $p > 2$ eine Primzahl. Dann gilt für eine ganze Zahl $a \in \mathbb{Z}$ mit $p \nmid a$:

$$\left(\frac{a}{p}\right)_2 \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{3.3}$$

Dieses wurde in [ZT14, Auf.47] bewiesen. Dies entspricht der Kongruenz, durch die wir nun das kubische Restsymbol definiert haben.
Beachte: Beim Legendre-Symbol erhält man direkt die Lösbarkeit in $\mathbb{Z}$ und im kubischen Fall mit dem kubischen Restsymbol zunächst nur die Lösbarkeit in $\mathbb{Z}[\omega]$. Wir werden später noch die Lösbarkeit der Gleichung $x^3 \equiv a \pmod{p}$ für $a \in \mathbb{Z}$ und Primzahl p für ein $x \in \mathbb{Z}$ untersuchen. Außerdem gilt im quadratischen Fall, dass die Anzahl der quadratischen Nichtreste gleich der Anzahl der quadratischen Reste modulo einer ungeraden Primzahl p ist, und somit wird die zyklische Gruppe $\mathbb{F}_p^*$ in zwei gleich große Teile unterteilt wird. Auch dies lässt sich auf den kubischen Fall übertragen. Durch den kubischen Restklassencharakter $\left(\frac{\cdot}{\pi}\right)_3$ für ein komplexes Primelement $\pi \in \mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi} \equiv 1 \pmod 3$ wird die Einheitengruppe $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ in drei gleich große Teile unterteilt. Davon sind ein Drittel kubische Reste und zwei Drittel kubische Nichtreste. Dabei gibt es zwei verschiedene Arten von Nichtresten, die Elemente für die das kubische Restsymbol gleich ω und die, für die das kubische Restsymbol gleich ω^2 ist.[4]

3.3 Die kubische Jacobi-Summe

Da das kubische Restsymbol für ein komplexes Primelement $\pi \in \mathbb{Z}[\omega]$ ein Charakter ist, können wir auch Aussagen über die Gauß- und Jacobi-Summe dieses Charakters treffen. Betrachte dazu in diesem Abschnitt den kubischen Charakter $\chi_\pi := \left(\frac{\cdot}{\pi}\right)_3 \neq \epsilon$ für ein echt-komplexes Primelement π von $\mathbb{Z}[\omega]$. Die Aussagen dieses Abschnitts sind aus [IR93, S.115f].

3.3.1 Satz. *Sei $p = \pi\overline{\pi} \equiv 1 \pmod 3$ eine Primzahl, und χ ein kubischer Charakter auf $\mathbb{F}_p$ (z.B $\chi = \chi_\pi$). Dann ist $J(\chi,\chi) = a + b\omega$ mit $a, b \in \mathbb{Z}$ und $a \equiv -1 \pmod 3, b \equiv 0 \pmod 3$. Also ist $J(\chi,\chi)$ insbesondere primär.*

Beweis. Nach Voraussetzung ist χ ein kubischer Charakter auf $\mathbb{F}_p$, hat also Werte in $\{1, \omega, \omega^2\}$. Dabei folgt die Existenz eines kubischen Charakters auf $\mathbb{F}_p$ aus der Voraussetzung $p \equiv 1 \pmod 3$. Für die Jacobi-Summe gilt $J(\chi,\chi) = \sum_{s+t=1} \chi(s)\chi(t) \in \mathbb{Z}[\omega]$. Somit existieren $a, b \in \mathbb{Z}$ mit $J(\chi,\chi) = a + b\omega$. Nach Satz 2.3.6 und mit dem Frobenius-Automorphismus von $\mathbb{Q}(\omega)$ gilt für $\zeta = e^{\frac{2\pi i}{p}}$:

$$pJ(\chi,\chi) \overset{2.3.6}{=} G(\chi)^3 \overset{\text{Def.}}{=} \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta^t\right)^3 \equiv \sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta^{3t} \pmod 3. \tag{3.4}$$

Es gilt $\chi(0) = 0$ und für alle $t \neq 0$ gilt $\chi(t)^3 = 1$. Also gilt nach (3.4) bereits

$$pJ(\chi,\chi) \equiv \sum_{t\neq 0} \zeta^{3t} = \sum_{t\neq 0} \zeta^t = -1 \pmod 3.$$

[4] siehe [Cox89, S. 79]

Dabei wurde im letzten Schritt verwendet, dass ζ eine primitive p-te Einheitswurzel ist. Außerdem gilt wegen $p \equiv 1 \pmod 3$ auch

$$-1 \equiv pJ(\chi,\chi) \equiv J(\chi,\chi) = a + b\omega \pmod 3.$$

Damit ist $b \equiv 0 \pmod 3$ und $a \equiv -1 \pmod 3$, also ist insbesondere $J(\chi,\chi)$ primär. □

3.3.2 Satz. *Sei $\pi \in \mathbb{Z}[\omega]$ ein echt-komplexes primäres Primelement mit $\pi \equiv -1 \pmod 3$. Dann gilt für die Jacobi-Summe*

$$J(\chi_\pi, \chi_\pi) = \pi.$$

Gilt $\pi \equiv 1 \pmod 3$, so ist

$$J(\chi_\pi, \chi_\pi) = -\pi.$$

Beweis. Sei $\chi := \chi_\pi$. Aus Satz 3.3.1 ist bekannt, dass $J(\chi,\chi)$ primär ist und $N(J(\chi,\chi)) = |J(\chi,\chi)|^2 = p \equiv 1 \pmod 3$. Sei $J(\chi,\chi) = \pi'$ für ein primäres, echt-komplexes Primelement $\pi' \in \mathbb{Z}[\omega]$. Somit gilt $\pi'\overline{\pi'} = p = \pi\overline{\pi}$ und wegen π prim muss $\pi \mid \pi'$ oder $\pi \mid \overline{\pi'}$ gelten. Da alle beteiligten Elemente $\pi, \pi', \overline{\pi}, \overline{\pi'}$ primär und prim sind, gilt $\pi' = \pm\pi$ oder $\overline{\pi'} = \pm\pi$. Wir wollen Letzteres ausschließen und zeigen dazu, dass $J(\chi,\chi)$ durch π teilbar ist.
Betrachte dazu die Jacobi-Summe des kubischen Charakters χ

$$J(\chi,\chi) = \sum_{x\in\mathbb{F}_p} \chi(x)\chi(1-x) \equiv \sum_{x=0}^{p-1} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \pmod \pi. \tag{3.5}$$

Nun gilt für ein allgemeines Polynom $P(x) = \sum_{i=0}^{k} \alpha_i x^i$ von Grad $k < p-1$ mit ganzzahligen Koeffizienten $\alpha_i \in \mathbb{Z}$, dass $\sum_{x\in\mathbb{F}_p} P(x) \equiv 0 \pmod p$ ist. Denn für $0 < k < p-1$ gilt insbesondere $p-1 \nmid k$ und somit ist $x^k \neq 1$ für alle $1 \neq x \in \mathbb{F}_p$ und da p eine ungerade Primzahl ist, gilt die Kongruenz

$$\sum_{x\in\mathbb{F}_p} x^k = \sum_{x=0}^{p-1} x = \frac{(p-1)}{2}\cdot p \equiv 0 \pmod p. \tag{3.6}$$

Wir erhalten also für das Polynom mit (3.6)

$$\sum_{x\in\mathbb{F}_p} P(x) = \sum_{x\in\mathbb{F}_p}\sum_{i=0}^{k} \alpha_i x^i = \sum_{i=0}^{k} \alpha_i \sum_{x=0}^{p-1} x^i \overset{(3.6)}{\equiv} 0 \pmod p.$$

Da $x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}}$ ein Polynom von Grad $\frac{2}{3}(p-1) < p-1$ ist, folgt

$$\sum_{x=0}^{p-1} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \equiv 0 \pmod p.$$

Wegen $p = \pi\overline{\pi}$ und Gleichung (3.5) gilt dann

$$J(\chi,\chi) \equiv 0 \pmod \pi.$$

Somit sind wir in dem Fall $\pi \mid J(\chi,\chi) = \pi'$ und erhalten für $\pi = a + b\omega \equiv -1 \pmod 3$ die Identität $J(\chi,\chi) = \pi$. Die Aussage für $\pi \equiv 1 \pmod 3$ folgt analog. □

3.3.3 Korollar. [5] *Sei $p = 3m+1 = a^2 - ab + b^2 = \frac{1}{4}(L^2 + 27M^2)$ eine Primzahl mit $L = 2a - b$ und $M = \frac{b}{3}$. Für $L \equiv 2 \pmod 3$ gilt*

$$2a - b = L \equiv \binom{2m}{m} \pmod p.$$

Beweis. Sei $\pi = a + b\omega = \frac{1}{2}(L + 3M\sqrt{-3})$ ein primäres Primelement von $\mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi}$. Es ist $2a - b = L = \pi + \overline{\pi} \equiv \overline{\pi} \pmod \pi$. Nach Voraussetzung ist $L \equiv 2 \pmod 3$ und somit folgt $a \equiv 1 \pmod 3$. Folglich gilt $\pi \equiv 1 \pmod 3$. Damit folgt auch $\overline{\pi}$ primär mit $\overline{\pi} \equiv 1 \pmod 3$. Satz 3.3.2 führt zu:

$$-\overline{\pi} = J(\chi_{\overline{\pi}}, \chi_{\overline{\pi}}) = \sum_{t \in \mathbb{F}_p} \chi_{\overline{\pi}}(t)\chi_{\overline{\pi}}(1-t) = \sum_{t \in \mathbb{F}_p} \overline{\chi_\pi(t)\chi_\pi(1-t)} = J(\overline{\chi_\pi}, \overline{\chi_\pi}) = J(\chi_\pi^2, \chi_\pi^2). \quad (3.7)$$

Für den kubischen Charakter χ_π folgt $\chi_\pi(t) \equiv t^{\frac{p-1}{3}} = t^m \pmod \pi$ für jedes $t \in \mathbb{F}_p$. Mit der Gleichung (3.7) erhält man:

$$\begin{aligned} L \equiv \overline{\pi} = -J(\chi_\pi^2, \chi_\pi^2) &\equiv -\sum_{t \in \mathbb{F}_p} t^{2m}(1-t)^{2m} \\ &= -\sum_{t \in \mathbb{F}_p} t^{2m} \sum_{j=0}^{2m} \binom{2m}{j} t^{2m-j}(-1)^{2m-j} \\ &= -\sum_{j=0}^{2m} \binom{2m}{j}(-1)^j \sum_{t=0}^{p-1} t^{4m-j} \qquad \pmod \pi. \end{aligned}$$

Die Summe $\sum_{t=0}^{p-1} t^{4m-j}$ verschwindet für $j \neq m$ und für $j = m$ ist $\sum_{t=0}^{p-1} t^{3m} = \sum_{t=0}^{p-1} t^{p-1} \equiv -1 \pmod p$. Damit gilt insgesamt

$$L \equiv \binom{2m}{m}(-1)^m \pmod \pi.$$

Da m gerade ist (denn $p - 1 = 3m$ ist durch 2 teilbar), gilt $(-1)^m = 1$. Da auf beiden Seiten der Kongruenz ganzzahlige Elemente stehen, gilt die Kongruenz auch modulo p und damit ist die Behauptung gezeigt. □

3.4 Das kubische Reziprozitätsgesetz

In diesem Abschnitt werden wir das kubische Reziprozitätsgesetz beweisen. Dabei gehen wir wie im zweiten, eleganteren Beweis aus [IR93, Kap.9, §5] vor. Für mögliche andere Beweise siehe auch [IR93, Kap.9, §4] oder [Lem00, S.213ff].

3.4.1 Theorem (Kubisches Reziprozitätsgesetz)**.** *Seien $\pi_1, \pi_2 \in \mathbb{Z}[\omega]$ primäre, teilerfremde Primelemente mit $N(\pi_i) \neq 3$ für $i \in \{1, 2\}$ und $N(\pi_1) \neq N(\pi_2)$. Dann gilt:*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

[5] siehe [Lem00, Kor. 7.6]

Zunächst noch einige Beispiele kubischer Reste.

3.4.2 Beispiel.

(i) Für jedes Primelement $\pi \in \mathbb{Z}[\omega]$ ist -1 ein kubischer Rest modulo π, denn $(-1)^3 = -1$.

(ii) 3 ist ein kubischer Rest modulo 11, denn $9^3 \equiv (-2)^3 = -8 \equiv 3 \pmod{11}$.

(iii) Für zwei verschiedene Primzahlen $p \equiv q \equiv 2 \pmod 3$, kann man durch wiederholte Anwendung des kubischen Reziprozitätsgesetzes, schnell berechnen, ob p ein kubischer Rest modulo q ist, ähnlich wie es auch mit Hilfe des quadratischen Reziprozitätsgesetzes funktioniert.
Seien dazu $p = 11, q = 149$. Dann gilt:

$$\left(\frac{11}{149}\right)_3 \overset{\text{kub. RG}}{=} \left(\frac{149}{11}\right)_3 = \left(\frac{6}{11}\right)_3 = \left(\frac{2}{11}\right)_3\left(\frac{3}{11}\right)_3 \overset{(ii)}{=} \left(\frac{2}{11}\right)_3 \overset{\text{kub. RG}}{=} \left(\frac{11}{2}\right)_3 = \left(\frac{1}{2}\right)_3 = 1.$$

Das bedeutet, dass 11 ein kubischer Rest modulo 149 ist. Eine Lösung der Gleichung $x^3 \equiv 11 \pmod{149}$ ist $x = 99$, denn es gilt $99^3 = 970299 = 6512 \cdot 149 + 11 \equiv 11 \pmod{149}$.

(iv) $2-3\omega$ ist ein kubischer Rest modulo 11, denn die Norm von $2-3\omega$ ist $N(2-3\omega) = 4+6+9 = 19$ und somit sind $2-3\omega$ und 11 primäre Primelemente in $\mathbb{Z}[\omega]$. Die Voraussetzungen für das kubische Reziprozitätsgesetz sind erfüllt und es gilt

$$\left(\frac{2-3\omega}{11}\right)_3 = \left(\frac{11}{2-3\omega}\right)_3.$$

Damit sind äquivalent:

$$\begin{aligned} &(i) \quad x^3 \equiv 2-3\omega \pmod{11} \text{ ist lösbar mit } x \in \mathbb{Z}[\omega] \\ &(ii) \quad x^3 \equiv 11 \pmod{(2-3\omega)} \text{ ist lösbar mit } x \in \mathbb{Z}[\omega] \end{aligned}$$

Wegen der Isomorphie $\mathbb{Z}[\omega]/(2-3\omega)\mathbb{Z}[\omega] \cong \mathbb{Z}/19\mathbb{Z}$ ist (ii) äquivalent zu: $x^3 \equiv 11 \pmod{19}$ ist lösbar in $\mathbb{Z}$. Die letzte Kongruenz ist etwa für $x = 5, x = 16$ und $x = 17$ erfüllt ist. Eine Lösung der Gleichung $x^3 \equiv 2 - 3\omega \pmod{11}$ ist $x = 7 + 10\omega$, denn
$x^3 \equiv (-4)^3 + 3 \cdot (-4)^2 \cdot (-\omega) - 3 \cdot 7 - 3 \cdot 7\omega + (-1)^3 \equiv 2 - 3\omega \pmod{11}$.

(v) [6] Die Gleichung $x^3 \equiv 2 + 3\omega \pmod{11}$ ist nicht in lösbar, d.h.

$$\left(\frac{2+3\omega}{11}\right)_3 \neq 1.$$

Denn es gilt $2+3\omega \equiv 2 \pmod 3$ und $N(2+3\omega) = 4-6+9 = 7$. Damit sind 11 und $2-3\omega$ primäre Primelemente in $\mathbb{Z}[\omega]$. Mit Hilfe des kubischen Reziprozitätsgesetzes 3.4.1 erhält man nun

$$\left(\frac{2+3\omega}{11}\right)_3 = \left(\frac{11}{2+3\omega}\right)_3.$$

[6] Dieses und das vorhergehende Beispiel (iv) gehen aus [IR93, Kap.9, Aufg.16] hervor. Dort ist ein Fehler in der Aufgabenstellung. Betrachte hier $2+3\omega$ anstelle von $2-3\omega$. Denn wie wir in dem Beispiel (iv) gesehen haben, ist die Gleichung für $2 - 3\omega$ lösbar

Also ist $x^3 \equiv 2 + 3\omega \pmod{11}$ genau dann für ein $x \in \mathbb{Z}[\omega]$ lösbar, wenn die Kongruenz $x^3 \equiv 11 \pmod{(2+3\omega)}$ für ein $x \in \mathbb{Z}[\omega]$ lösbar ist. Da $\mathbb{Z}[\omega]/(2+3\omega)\mathbb{Z}[\omega] \cong \mathbb{Z}/7\mathbb{Z}$ ist dies genau dann der Fall, wenn $x^3 \equiv 11 \equiv 4 \pmod{7}$ für ein $x \in \mathbb{Z}$ gilt. Die Gleichung $x^3 \equiv a \pmod{7}$ ist allerdings nur lösbar, falls $a \equiv 1 \pmod{7}$ oder $a \equiv 6 \pmod{7}$ gilt. Somit ist die Gleichung $x^3 \equiv 2 + 3\omega \pmod{11}$ für kein $x \in \mathbb{Z}[\omega]$ erfüllt.

3.4.3 Bemerkung.

- Im Gegensatz zu dem quadratischen Reziprozitätsgesetz und auch zu dem biquadratischen Reziprozitätsgesetz (siehe Kapitel 4), tritt beim kubischen Reziprozitätsgesetz kein Faktor $(-1)^a$, $a \in \mathbb{Z}$ auf. Dies macht die Aussage des kubischen Reziprozitätsgesetzes unabhängig von weiteren Eigenschaften der Elemente π_1 und π_2. Das kubische Reziprozitätsgesetz besagt für Primelemente π_1 und π_2 wie in Theorem 3.4.1:

  π_1 ist ein kubischer Rest modulo π_2 genau dann, wenn π_2 kubischer Rest modulo π_1 ist.

  Und wir erhalten sogar mehr als diese Äquivalenz, die nur Aussagen macht, falls eines der beiden Restsymbole gleich eins ist. Auch falls π_1 kein kubischer Rest modulo π_2 ist, das heißt, falls $\left(\frac{\pi_1}{\pi_2}\right)_3 \neq 1$, so sind die beiden Restsymbole trotzdem noch gleich. Das heißt π_1 und π_2 sind von derselben „Art“ kubischer Nichtreste.

- Die Betrachtung ausschließlich primärer Elemente ist keine wesentliche Einschränkung und entspricht in etwa der Einschränkung auf positive Primzahlen im quadratischen Reziprozitätsgesetz. Ein beliebiges Primelement unterscheidet sich maximal um eine Einheit von einem primären Primelement oder es ist assoziiert zu $1 - \omega$. Somit kann man mit Hilfe der Ergänzungssätze zum kubischen Reziprozitätsgesetz alle kubischen Restsymbole berechnen.

Nun zu dem Beweis des kubischen Reziprozitätsgesetzes.

Beweis von Theorem 3.4.1.
Mache eine Fallunterscheidung für alle Möglichkeiten der verschiedenen Primelemente in $\mathbb{Z}[\omega]$.

1. Sei $\pi_1 = q \equiv 2 \pmod{3}$ eine träge Primzahl und $\pi_2 = \pi$ ein komplexes Primelement mit $p = \pi\overline{\pi} \equiv 1 \pmod{3}$. Setze $\chi := \left(\frac{\cdot}{\pi}\right)_3 \neq \epsilon$.

   Betrachte die Jacobi-Summe $J^q(\chi, \ldots, \chi) = \sum_{t_1+\ldots+t_q=1} \prod_{i=1}^{q} \chi(t_i)$. Teile die Summe nun in die Summanden auf, bei denen alle t_i gleich sind, und in die restlichen Summanden. Für die Summanden mit $t_1 = \ldots = t_q =: t$ erhalte $qt = 1$, also $\chi(q)\chi(t) = \chi(1) = 1$ durch potenzieren der Gleichung mit q erhalte

   $$\chi(q)^q \chi(t)^q = 1.$$

   Mit der Voraussetzung $q \equiv 2 \pmod{3}$ gilt dann

   $$\chi(q)^2 \chi(t)^q = 1 \quad \text{bzw.} \quad \chi(t)^q = \chi(q)^{-2} = \chi(q). \tag{3.8}$$

Betrachte nun die Summanden mit $t_1 + \ldots + t_q = 1$ und $t_i \neq t_j$ für mindestens ein Paar $(i,j) \in \{1,\ldots,q\}^2$. Zu jedem q-Tupel $(t_1,\ldots,t_q)$ gibt es q zyklische Permutationen. Für jede solche Permutation verändert sich der Wert des Summanden nicht. Folglich gilt

$$J^q(\chi,\ldots,\chi) \equiv \chi(t)^q \overset{(3.8)}{=} \chi(q) \pmod{q}. \tag{3.9}$$

Nach Voraussetzung gilt außerdem $3 \mid (q+1)$ und χ ist ein Charakter der Ordnung 3, also ist $\prod_{i=1}^{q+1} \chi = \epsilon$. Somit gilt nach Korollar 2.4.4

$$G(\chi)^{q+1} = \underbrace{\chi(-1)}_{=1} pJ^q(\chi,\ldots,\chi).$$

Außerdem gilt nach Satz 2.3.6 und Satz 3.3.2: $G(\chi)^3 = \chi(-1)pJ(\chi,\chi) = \pm p\pi$ und somit

$$G(\chi)^{q+1} = (\pm p\pi)^{\frac{q+1}{3}}.$$

Nun ist $\frac{q+1}{3}$ eine gerade ganze Zahl, falls $q > 2$ ist und falls $q = 2$ ist das Vorzeichen unwichtig, da wir dann die Gleichung modulo $q = 2$ betrachten werden.
Es gilt also

$$(\pm p\pi)^{\frac{q+1}{3}} \equiv (p\pi)^{\frac{q+1}{3}} \equiv pJ^q(\chi,\ldots,\chi) \overset{(3.9)}{\equiv} p\chi(q) \pmod{q}$$

und somit

$$p^{\frac{q-2}{3}} \pi^{\frac{q+1}{3}} \equiv \chi(q) \pmod{q}.$$

Durch potenzieren mit $q - 1 \equiv 1 \pmod 3$ erhält man

$$\left(p^{\frac{q-2}{3}}\right)^{q-1} \pi^{\frac{q^2-1}{3}} \equiv \chi(q)^{q-1} = \chi(q) = \left(\frac{q}{\pi}\right)_3 \pmod{q}.$$

Weiterhin gilt nach dem kleinen Satz von Fermat (Satz 2.1.4):

$$\left(p^{\frac{q-2}{3}}\right)^{q-1} \equiv 1 \pmod{q}$$

und nach Definition des kubischen Restsymbols $\pi^{\frac{q^2-1}{3}} \equiv \left(\frac{\pi}{q}\right)_3 \pmod{q}$. Es folgt

$$\left(\frac{\pi}{q}\right)_3 = \left(\frac{q}{\pi}\right)_3.$$

2. Seien nun π_1 und π_2 zwei verschiedene, nicht-assoziierte, echt-komplexe primären Primelemente mit $p_i = \pi_i\overline{\pi_i} \equiv 1 \pmod 3$ für $i = 1, 2$. Mit π_i primär ist auch $\overline{\pi_i}$ primär, denn es ist $1 \equiv p_i = \pi_i\overline{\pi_i} \equiv \pm\overline{\pi_i} \pmod 3$. Sei nun $\chi_1 := \left(\frac{\cdot}{\overline{\pi_1}}\right)_3 \neq \epsilon$.
Da $p_2 \equiv 1 \pmod 3$ gilt, ist $\chi_1^{p_2} = \chi_1 \neq \epsilon$ und damit gilt nach Theorem 2.4.3

$$G(\chi_1)^{p_2} = J^{p_2}(\chi_1,\ldots,\chi_1)G(\chi_1^{p_2}) = J^{p_2}(\chi_1,\ldots,\chi_1)G(\chi_1).$$

Es folgt

$$J^{p_2}(\chi_1,\ldots,\chi_1) = G(\chi_1)^{p_2-1} = \left(G(\chi_1)^3\right)^{\frac{p_2-1}{3}} = (\pm p_1\overline{\pi_1})^{\frac{p_2-1}{3}} = (p_1\overline{\pi_1})^{\frac{p_2-1}{3}}. \tag{3.10}$$

Im letzten Schritt wurde verwendet, dass p_2 eine ungerade Primzahl ist und somit $\frac{p_2-1}{3}$ gerade ist. Berechne nun die Summanden der Jacobi-Summe

$$J^{p_2}(\chi_1,\ldots,\chi_1) = \sum_{t_1+\ldots+t_{p_2}=1} \prod_{i=1}^{p_2} \chi_1(t_i).$$

Für $t_1 = \ldots = t_{p_2} =: t$ ist $tp_2 = 1$, also $\chi_1(t)\chi_1(p_2) = 1$ und damit gilt $\chi_1(t) = \chi_1(p_2)^{-1} = \chi_1(p_2)^2$. Analoges Vorgehen wie in Fall 1 ergibt

$$J^{p_2}(\chi_1,\ldots,\chi_1) \equiv \chi_1(t)^{p_2} = \chi_1(t) = \chi_1(p_2)^2 \pmod{p_2}. \tag{3.11}$$

Weiterhin ist

$$\left(\frac{p_1\overline{\pi_1}}{\pi_2}\right)_3 \equiv (p_1\overline{\pi_1})^{\frac{p_2-1}{3}} \overset{(3.10)}{=} J^{p_2}(\chi_1,\ldots,\chi_1) \overset{(3.11)}{\equiv} \chi_1(p_2)^2 = \left(\frac{p_2}{\overline{\pi_1}}\right)_3^2 \pmod{p_2}$$

und da π_2 ein Teiler von p_2 ist, folgt

$$\left(\frac{p_1\overline{\pi_1}}{\pi_2}\right)_3 \equiv \left(\frac{p_2}{\overline{\pi_1}}\right)_3^2 \pmod{\pi_2}.$$

Folglich ist

$$\left(\frac{p_1\overline{\pi_1}}{\pi_2}\right)_3 = \left(\frac{p_2}{\overline{\pi_1}}\right)_3^2. \tag{3.12}$$

Analog erhält man

$$\left(\frac{p_2\pi_2}{\pi_1}\right)_3 = \left(\frac{p_1}{\pi_2}\right)_3^2. \tag{3.13}$$

Somit ergibt sich insgesamt

$$\begin{aligned}\left(\frac{\pi_2}{\pi_1}\right)_3\left(\frac{p_1\overline{\pi_1}}{\pi_2}\right)_3 &\overset{(3.12)}{=} \left(\frac{\pi_2}{\pi_1}\right)_3\left(\frac{p_2}{\overline{\pi_1}}\right)_3^2 \overset{3.2.5(e)}{=} \left(\frac{\pi_2}{\pi_1}\right)_3\overline{\left(\frac{p_2}{\pi_1}\right)_3}^2 \\ &= \left(\frac{\pi_2}{\pi_1}\right)_3\left(\frac{p_2}{\pi_1}\right)_3 = \left(\frac{p_2\pi_2}{\pi_1}\right)_3 \overset{(3.13)}{=} \left(\frac{p_1}{\pi_2}\right)_3^2 = \left(\frac{\pi_1}{\pi_2}\right)_3\left(\frac{\overline{\pi_1}p_1}{\pi_2}\right)_3.\end{aligned}$$

Durch Multiplikation mit dem Inversen $\left(\frac{\overline{\pi_1}p_1}{\pi_2}\right)_3^{-1}$ folgt die Behauptung.

3. Der letzte noch verbleibende Fall, dass beide Primelemente träge Primzahlen sind, also $\pi_1 \equiv \pi_2 \equiv 2 \pmod 3$ folgt aus dem nachfolgenden Satz.

□

3.4.4 Satz. *Sei* $q \equiv 2 \pmod 3$, $n \in \mathbb{N}$ *mit* $\mathrm{ggT}(n,q) = 1$. *Dann gilt:*

$$\left(\frac{n}{q}\right)_3 = 1.$$

Beweis. Es gilt $\overline{n} = n, \overline{q} = q$ und somit

$$\left(\frac{n}{q}\right)_3 = \left(\frac{\overline{n}}{\overline{q}}\right)_3 \overset{3.2.5(e)}{=} \overline{\left(\frac{n}{q}\right)_3}.$$

Nun folgt die Behauptung, da $\mathrm{ggT}(n,q) = 1$ gilt und somit $\left(\frac{n}{q}\right)_3 \neq 0$. Außerdem ist $\omega^m = \overline{\omega}^m$ nur für $m \equiv 0 \pmod 3$ erfüllt. □

3.4.5 Bemerkung. Aus Satz 3.4.4 folgt insbesondere für zwei verschiedene Primzahlen $q_1 \equiv q_2 \equiv 2 \pmod 3$ die Gleichheit

$$\left(\frac{q_1}{q_2}\right)_3 = 1 = \left(\frac{q_2}{q_1}\right)_3$$

und vervollständigt damit den Beweis des kubischen Reziprozitätsgesetzes (Theorem 3.4.1).

3.5 Die Ergänzungssätze

Die Ergänzungssätze werden wir wie in [Lem00, S.215ff] betrachten. Ebenso wie die Ergänzungssätze zum quadratischen Reziprozitätsgesetz, dienen die Ergänzungssätze zum kubischen Reziprozitätsgesetz der Berechnung des kubischen Restsymbols für Elemente, die durch das Reziprozitätsgesetz nicht abgedeckt werden. Mit Hilfe der Ergänzungssätze und der Tatsache, dass -1 immer ein kubischer Rest ist, kann man somit alle kubischen Restsymbole berechnen. Durch die Ergänzungssätze erhalten wir die Werte des kubischen Restsymbols für alle Einheiten und für das Primelement $(1-\omega)$.

3.5.1 Satz (Ergänzungssätze)**.** *Sei* $\pi = a + b\omega$ *ein primäres Primelement, sodass* $\pi \equiv 1 \pmod 3$ *gilt. Sei dann* $a = 3m+1$ *und* $b = 3n$. *(Für* $\pi \equiv -1 \pmod 3$ *setze* $-\pi = a + b\omega \equiv 1 \pmod 3$*). Dann gilt:*

(1) $\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{1-(a+b)}{3}} = \omega^{-m-n}$

(2) $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{\frac{a-1}{3}} = \omega^m$

(3) $\left(\frac{3}{\pi}\right)_3 = \omega^{\frac{b}{3}} = \omega^n$

Beweis. (1) Es gilt $\left(\frac{\omega}{\pi}\right)_3 \equiv \omega^{\frac{N(\pi)-1}{3}} \pmod \pi$. Da dies bereits eine Potenz von ω ist, folgt auch die Gleichheit. Wegen

$$\begin{aligned}\frac{N(\pi)-1}{3} &= \frac{9m^2+6m+1-9mn-3n+9n^2-1}{3} \\ &= 3m^2-3mn+3n^2+2m-n \\ &\equiv -m-n \pmod 3\end{aligned}$$

folgt dann $\left(\frac{\omega}{\pi}\right)_3 = \omega^{-m-n}$.
Die Beweise der beiden anderen Ergänzungssätze sind komplizierter und man benötigt zunächst noch eine Verallgemeinerung des kubischen Restsymbols. □

3.5.2 Lemma. [7] *Sei $\gamma \in \mathbb{Z}[\omega]$ primär, dann existieren primäre Primelemente $\pi_1, \ldots, \pi_r \in \mathbb{Z}[\omega]$, sodass eine sogenannte primäre Primfaktorzerlegung der Form $\gamma = \pm \prod_{i=1}^{r} \pi_i$ von γ existiert.*

Beweis. Offensichtlich ist die Multiplikation zweier primärer Elemente wieder primär. Wir können ohne Einschränkung den Fall $\gamma \equiv -1 \pmod 3$ betrachten. (Denn: ist $\gamma \equiv 1 \pmod 3$, so ist $-\gamma \equiv -1 \pmod 3$, ändert also nichts an einer Existenz der gewünschten Form.)
Da $\mathbb{Z}[\omega]$ ein faktorieller Ring ist, existiert bis auf Assoziiertheit eine eindeutige Primfaktorzerlegung, etwa $\gamma = u \cdot \prod_{i=1}^{r} \widetilde{\pi}_i$ mit Primelementen $\widetilde{\pi}_i$ und einer Einheit u von $\mathbb{Z}[\omega]$ für $i = 1, \ldots, r$.
Wegen γ primär ist insbesondere $\mathrm{ggT}(\gamma, 3) = 1$ und keiner der Primfaktoren $\widetilde{\pi}_i$ ist assoziiert zu $(1-\omega)$. Es existiert also für jedes $i \in \{1, \ldots, r\}$ eine Einheit u_i von $\mathbb{Z}[\omega]$, sodass $\pi_i := u_i \widetilde{\pi}_i$ primär ist. Wähle u_i so, dass $\pi_i \equiv 1 \pmod 3$ gilt.
Somit gibt es eine Primfaktorzerlegung $\gamma = v \cdot \prod_{i=1}^{r} \pi_i$ für eine Einheit v von $\mathbb{Z}[\omega]$. Es bleibt zu zeigen, dass $v = \pm 1$ gilt. Dies folgt aus $-1 \equiv \gamma = v \cdot \prod_{i=1}^{r} \pi_i \equiv v \pmod 3$. □

Nun können wir das kubische Restsymbol auf alle primären Elemente verallgemeinern. Diese Definition ist das Pendant zu dem Jacobi-Symbol im quadratischen Fall.

3.5.3 Definition. Definiere für ein primäres $\gamma \in \mathbb{Z}[\omega]$ mit primärer Primfaktorzerlegung $\gamma = \pm\pi_1 \cdot \ldots \cdot \pi_r$ und einem beliebigen $\beta \in \mathbb{Z}[\omega]$ das verallgemeinerte Restsymbol

$$\left(\frac{\beta}{\gamma}\right)_3 := \prod_{i=1}^{r} \left(\frac{\beta}{\pi_i}\right)_3.$$

3.5.4 Bemerkung.

1. Das verallgemeinerte Restsymbol aus Definition 3.5.3 ist wohldefiniert, da γ primär ist und somit $N(\pi_i) \neq 3$ für alle primären Primfaktoren π_i von γ gilt (siehe Beweis von 3.5.2).
2. Gilt $\mathrm{ggT}(\beta, \gamma) \neq 1$, so ist $\left(\frac{\beta}{\gamma}\right)_3 = 0$ nach der Definition des kubischen Restsymbols (siehe 3.2.4), denn es existiert ein Primfaktor π von γ, sodass π ein Teiler von β ist.
3. Für das kubische Restsymbol für Primelemente (siehe Definition 3.2.4) und das verallgemeinerte kubische Restsymbol (siehe Definition 3.5.3) wird das gleiche Symbol verwendet. Im Fall eines Primelements $\pi \neq 1 - \omega$, stimmen die beiden Definitionen überein.

3.5.5 Bemerkung. Wir haben in [ZT14] festgestellt, dass für das Jacobi-Symbol $\left(\frac{a}{b}\right)_2$ aus $\left(\frac{a}{b}\right)_2 = 1$ für $a, b \in \mathbb{Z}$ im Allgemeinen nicht folgt, dass a ein quadratischer Rest modulo b ist. Dasselbe Problem erhält man nun bei der Verallgemeinerung des kubischen Restsymbols. Hat

[7] Aussage vgl. [IR93][Aufg 17]

das verallgemeinerte kubische Restsymbol den Wert 1, so kann man nicht darauf schließen, dass es sich um einen kubischen Rest handelt.
Wie in Beispiel 3.4.2 (v) bereits gezeigt wurde, ist $x^3 \equiv a \pmod 7$ nur für $a \equiv 1$ oder $a \equiv 6 \pmod 7$ lösbar. Für $a \equiv 4 \pmod 7$ jedoch nicht. Da $7 \equiv 1 \pmod 3$ ist, zerfällt die Primzahl 7 in $\mathbb{Z}[\omega]$ in zwei Primfaktoren. Mit der Primfaktorzerlegung $7 = (2+3\omega)\overline{(2+3\omega)}$ folgt

$$\left(\frac{4}{7}\right)_3 = \left(\frac{4}{2+3\omega}\right)_3 \left(\frac{4}{\overline{2+3\omega}}\right)_3 = \left(\frac{4}{2+3\omega}\right)_3 \overline{\left(\frac{4}{2+3\omega}\right)_3} = \left(\frac{4}{2+3\omega}\right)_3 \left(\frac{4}{2+3\omega}\right)_3^{-1} = 1,$$

obwohl 4 kein kubischer Rest modulo 7 ist.

Einige Eigenschaften des kubischen Restsymbols übertragen sich auf das verallgemeinerte kubische Restsymbol:

3.5.6 Satz (Eigenschaften)**.** [8] *Sei $\gamma = \pm \prod_{i=1}^{r} \pi_i$ die primäre Primfaktorzerlegung des primären Elements $\gamma \in \mathbb{Z}[\omega]$. Für $\alpha, \beta \in \mathbb{Z}[\omega]$ gilt:*

(a) Ist $\alpha \equiv \beta \pmod \gamma$, so gilt auch $\left(\frac{\alpha}{\gamma}\right)_3 = \left(\frac{\beta}{\gamma}\right)_3$.

(b) $\left(\frac{\alpha\beta}{\gamma}\right)_3 = \left(\frac{\alpha}{\gamma}\right)_3 \left(\frac{\beta}{\gamma}\right)_3$

(c) $\left(\frac{\overline{\alpha}}{\overline{\gamma}}\right)_3 = \overline{\left(\frac{\alpha}{\gamma}\right)_3}$

Beweis.

(a) Gelte $\alpha \equiv \beta \pmod \gamma$. Dann folgt auch für jeden Teiler π_i von γ die Kongruenz $\alpha \equiv \beta \pmod{\pi_i}$ $(i = 1, \ldots, r)$. Mit den Eigenschaften des kubischen Restsymbols (siehe Satz 3.2.5) gilt $\left(\frac{\alpha}{\pi_i}\right)_3 = \left(\frac{\beta}{\pi_i}\right)_3$ für alle $i = 1, \ldots, r$. Folglich gilt für das verallgemeinerte Restsymbol

$$\left(\frac{\alpha}{\gamma}\right)_3 = \prod_{i=1}^{r} \left(\frac{\alpha}{\pi_i}\right)_3 \overset{3.2.5}{=} \prod_{i=1}^{r} \left(\frac{\beta}{\pi_i}\right)_3 = \left(\frac{\beta}{\gamma}\right)_3.$$

(b) Durch Anwendung der Eigenschaft für das kubische Restsymbol aus Satz 3.2.5 folgt

$$\left(\frac{\alpha\beta}{\gamma}\right)_3 = \prod_{i=1}^{r} \left(\frac{\alpha\beta}{\pi_i}\right)_3 \overset{3.2.5}{=} \prod_{i=1}^{r} \left(\frac{\alpha}{\pi_i}\right)_3 \left(\frac{\beta}{\pi_i}\right)_3 = \left(\frac{\alpha}{\gamma}\right)_3 \left(\frac{\beta}{\gamma}\right)_3.$$

(c) Die primäre Primfaktorzerlegung von $\overline{\gamma}$ ist $\overline{\gamma} = \pm \prod_{i=1}^{r} \overline{\pi_i}$ für die primäre Primfaktorzerlegung $\gamma = \pm \prod_{i=1}^{r} \pi_i$. Es folgt

$$\left(\frac{\overline{\alpha}}{\overline{\gamma}}\right)_3 = \prod_{i=1}^{r} \left(\frac{\overline{\alpha}}{\overline{\pi_i}}\right)_3 \overset{3.2.5}{=} \prod_{i=1}^{r} \overline{\left(\frac{\alpha}{\pi_i}\right)_3} = \overline{\left(\frac{\alpha}{\gamma}\right)_3}.$$

□

[8] Aussage vgl. [IR93] Aufgabe 18

Wie im Folgenden gezeigt wird, gelten die Aussagen des kubischen Reziprozitätsgesetzes und der Ergänzungssätze ebenso für das verallgemeinerte kubische Restsymbol. Beachte dabei, dass bis jetzt nur der erste Ergänzungssatz für ω bewiesen ist. Es werden nun die allgemeinen Ergänzungssatz bewiesen werden (ohne die noch nicht bewiesenen Ergänzungssätze für Primelemente zu verwenden). Der Spezialfall für das kubische Restsymbol mit Primelemente folgt dann aus dem allgemeinen Fall. Zunächst aber die Verallgemeinerung des kubischen Reziprozitätsgesetzes.

3.5.7 Theorem. [9] *Seien γ, ϱ primär. Dann gilt*

$$\left(\frac{\gamma}{\varrho}\right)_3 = \left(\frac{\varrho}{\gamma}\right)_3.$$

Beweis. Falls γ und ϱ einen gemeinsamen Primteiler haben, so verschwinden beide Restsymbole und die Gleichung ist erfüllt. Sei nun $\mathrm{ggT}(\gamma, \varrho) = 1$ und seien $\gamma = \pm \prod_{i=1}^{r} \pi_i$ und $\varrho = \pm \prod_{j=1}^{s} \lambda_j$ die primären Primfaktorzerlegungen von γ und ϱ. Da die primären Primteiler von γ und ϱ paarweise teilerfremd sind folgt mit dem kubischen Reziprozitätsgesetz

$$\left(\frac{\gamma}{\varrho}\right)_3 \overset{\text{Def.}}{=} \prod_{j=1}^{s} \left(\frac{\gamma}{\lambda_j}\right)_3 \overset{3.5.6}{=} \prod_{i=1}^{r}\prod_{j=1}^{s} \left(\frac{\pi_i}{\lambda_j}\right)_3 \overset{\text{kub. RG}}{=} \prod_{i=1}^{r}\prod_{j=1}^{s} \left(\frac{\lambda_j}{\pi_i}\right)_3 = \left(\frac{\varrho}{\gamma}\right)_3.$$

□

3.5.8 Satz. *Für ein primäres ganzzahliges Element $a \equiv \pm 1 \pmod 3$ und ein $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, a) = 1$ gilt*

$$\left(\frac{n}{a}\right)_3 = 1.$$

Beweis. Der Beweis folgt analog wie im Fall für Primelemente (siehe Satz 3.4.4), denn nach Satz 3.5.6 gilt

$$\left(\frac{n}{a}\right)_3 = \left(\frac{\overline{n}}{\overline{a}}\right)_3 = \overline{\left(\frac{n}{a}\right)_3}.$$

Da nach Voraussetzung $\left(\frac{n}{a}\right)_3 \neq 0$ gilt, folgt bereits $\left(\frac{n}{a}\right)_3 = 1$. □

Das zeigt, dass bei Betrachtung ganzzahliger, teilerfremder Elemente, das kubische Restsymbol immer gleich 1 ist. Nun zu den allgemeinen Ergänzungssätzen.

3.5.9 Satz. *Seien $\gamma = A + B\omega$ primär, sodass $\gamma \equiv 1 \pmod 3$ gilt. Setze $A = 3M + 1$ und $B = 3N$. Dann gilt:*

(1) $\left(\frac{\omega}{\gamma}\right)_3 = \omega^{\frac{1-(A+B)}{3}} = \omega^{-M-N}$

(2) $\left(\frac{1-\omega}{\gamma}\right)_3 = \omega^{\frac{A-1}{3}} = \omega^{M}$

[9] Aussage vgl. [IR93][Aufg. 20]

(3) $\left(\frac{3}{\gamma}\right)_3 = \omega^{\frac{B}{3}} = \omega^N$

Beweis.

(1) Sei $\gamma = \pm\prod_{i=1}^{s}\pi_i$ die primäre Primfaktorzerlegung mit $\pi_i = a_i + b_i\omega = 3m_i + 1 + 3n_i\omega$ für $i = 1, \ldots, s$. Dann gilt nach Definition des allgemeinen kubischen Restsymbols

$$\left(\frac{\omega}{\gamma}\right)_3 = \prod_{i=1}^{s}\left(\frac{\omega}{\pi_i}\right)_3 \overset{3.5.1(1)}{=} \prod_{i=1}^{s}\omega^{-m_i-n_i} = \omega^{-\sum_{i=1}^{s} m_i+n_i}.$$

Es genügt also zu zeigen, dass $M + N \equiv \sum_{i=1}^{s} m_i + n_i \pmod 3$ gilt. Zeige dies per Induktion nach s. Der Fall $s = 1$ ist klar. Betrachte nun $s = 2$. Es ist

$$\begin{aligned}\gamma &= \pi_1\pi_2\\ &= (3m_1 + 1 + 3n_1\omega)(3m_2 + 1 + 3n_2\omega)\\ &= 3\underbrace{(3m_1m_2 + m_1 + m_2 - 3n_1n_2)}_{=M} + 1 + 3\underbrace{(3m_1n_2 + 3n_1m_2 - 3n_1n_2 + n_1 + n_2)}_{=N}\omega.\end{aligned}$$

Offensichtlich gilt

$$(3m_1m_2 - 3n_1n_2 + 3m_1n_2 + 3n_1m_2 - 3n_1n_2) \equiv 0 \pmod 3$$

und somit

$$M + N \equiv m_1 + n_1 + m_2 + n_2 \pmod 3.$$

Der Fall $\gamma = -\pi_1\pi_2$ folgt analog. Der Induktionsschritt folgt direkt durch die Induktionsvoraussetzung und aus dem Fall $s = 2$.

(2) Betrachte zunächst den Fall $B = 0$. Dann ist $\gamma = A \in \mathbb{Z}$ und aufgrund der Primfaktorzerlegung $3 = -\omega^2(1-\omega)^2$ gilt

$$\left(\frac{1-\omega}{\gamma}\right)_3^2 = \underbrace{\left(\frac{-1}{\gamma}\right)_3}_{=1}\underbrace{\left(\frac{3}{\gamma}\right)_3}_{=1}\left(\frac{\omega}{\gamma}\right)_3 \overset{(1)}{=} \omega^{-M}.$$

Durch Quadrieren der Gleichung folgt $\left(\frac{1-\omega}{\gamma}\right)_3 = \left(\frac{1-\omega}{\gamma}\right)_3^4 = \omega^M$.

Sei nun $B \neq 0$. Dann gilt

$$\left(\frac{3\omega}{\gamma}\right)_3 = \left(\frac{-3\omega}{\gamma}\right)_3 \overset{3.5.6(a)}{=} \left(\frac{\gamma - 3\omega}{\gamma}\right)_3 \overset{\text{kub. RG}}{=} \left(\frac{\gamma}{\gamma - 3\omega}\right)_3 = \left(\frac{3\omega}{\gamma - 3\omega}\right)_3. \tag{3.14}$$

Das kubische Reziprozitätsgesetz kann angewendet werden, da sowohl γ als auch $\gamma - 3\omega$ primär sind. N-maliges Wiederholen dieser Rechnung in (3.14) führt auf den bereits gezeigten Fall für $B = 0$. Insgesamt gilt

$$\left(\frac{3\omega}{\gamma}\right)_3 \overset{(3.14)}{=} \left(\frac{3\omega}{A}\right)_3 = \underbrace{\left(\frac{3}{A}\right)_3}_{=1 \text{ nach } 3.5.8}\left(\frac{\omega}{A}\right)_3 \overset{(1)}{=} \omega^{-M}. \tag{3.15}$$

Nun folgt die Behauptung, denn:

$$\left(\frac{1-\omega}{\gamma}\right)_3 = \left(\frac{1-\omega}{\gamma}\right)_3^4 = \left(\frac{3\omega}{\gamma}\right)_3^2 \overset{(3.15)}{=} \omega^{-2M} = \omega^M.$$

(3) Durch Anwenden der Ergänzungssätze (1) und (2) folgt der letzte Teil des Satzes:

$$\left(\frac{3}{\gamma}\right)_3 = \left(\frac{\omega}{\gamma}\right)_3^2 \left(\frac{1-\omega}{\gamma}\right)_3^2 \overset{(1),(2)}{=} \omega^{-2M-2N}\omega^{2M} = \omega^N.$$

□

3.5.10 Bemerkung. Die fehlenden Beweise von Satz 3.5.1 folgen direkt aus Satz 3.5.9. Diese allgemeiner Version des Ergänzungssatzes und die dazu benötigten Sätze wurde bewiesen, ohne die bis dorthin noch nicht bewiesenen Aussagen zu verwenden. Als Spezialfall folgen somit die restlichen Aussagen des Ergänzungssatzes 3.5.1 für Primelemente.

Die Aussage des kubischen Reziprozitätsgesetzes 3.4.1 gilt ebenso für Primelemente mit derselben Norm. Somit kann bei der Formulierung des kubischen Reziprozitätsgesetzes für Primelemente (Theorem 3.4.1) auf die Voraussetzung $N(\pi_1) \neq N(\pi_2)$ verzichtet werden (so wie es in [Lem00, Thm. 7.8] gehandhabt wird.). Sind π_1 und π_2 zueinander assoziiert, so ist die Aussage des kubischen Reziprozitätsgesetzes klar, denn die Elemente teilen sich gegenseitige und somit verschwinden beide kubische Restsymbole. Es genügt somit ein echt-komplexes Primelement $\pi \in \mathbb{Z}[\omega]$ und dessen komplex Konjugiertes zu betrachten.

3.5.11 Satz. [10] *Für ein primäres Primelement $\pi \in \mathbb{Z}[\omega]$ mit $N(\pi) \neq 3$ gilt*

$$\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3.$$

Beweis. Es gilt

$$\left(\frac{\overline{\pi}}{\pi}\right)_3 = \left(\frac{\overline{\pi}+\pi}{\pi}\right)_3 = \left(\frac{\pi}{\overline{\pi}+\pi}\right)_3 = \left(\frac{-\overline{\pi}}{\overline{\pi}+\pi}\right)_3 = \left(\frac{\overline{\pi}+\pi}{\overline{\pi}}\right)_3 = \left(\frac{\pi}{\overline{\pi}}\right)_3.$$

Das kubische Reziprozitätsgesetz ist anwendbar, da π und $\overline{\pi}$ primär sind und weiterhin $\pi + \overline{\pi}$ wegen $\pi + \overline{\pi} = 2a - b \equiv -a \equiv \pm 1 \pmod 3$ primär ist. □

Ein Spezialfall des allgemeinen kubischen Reziprozitätsgesetzes ist das von Eisenstein formulierte Reziprozitätsgesetz (siehe [Lem00, Proposition 7.7]). Für den Beweis des kubischen Reziprozitätsgesetzes kann man auch zunächst diesen Spezialfall beweisen und daraus leicht den allgemeinen Fall herleiten (siehe dazu auch [Lem00, S.213f]).

3.5.12 Theorem (Eisensteins kubisches Reziprozitätsgesetz)**.** *Seien $\alpha \in \mathbb{Z}[\omega]$ und $a \in \mathbb{Z}$ mit $\alpha \equiv 1 \equiv a \pmod 3$. Dann gilt das Reziprozitätsgesetz*

$$\left(\frac{\alpha}{a}\right)_3 = \left(\frac{a}{\alpha}\right)_3$$

mit den zugehörigen Ergänzungssätzen

[10] siehe [Lem00, S.215]

(1) $\left(\frac{\omega}{a}\right)_3 = \omega^{\frac{1-a}{3}}$

(2) $\left(\frac{1-\omega}{a}\right)_3 = \omega^{\frac{a-1}{3}}$.

Beweis. Spezialfall des verallgemeinerten kubischen Reziprozitätsgesetzes. □

3.6 Anwendungen

In den vorangehenden Abschnitten wurden alle Untersuchungen in $\mathbb{Z}[\omega]$ durchgeführt. Nun soll auch die Lösbarkeit von $x^3 \equiv a \pmod{p}$ für ein $x \in \mathbb{Z}$ betrachtet werden. Im Anschluss werden Anwendungen aus [IR93] zum kubischen Reziprozitätsgesetz gegeben.

Für $p \mid a$ ist die Kongruenz $x^3 \equiv 0 \pmod{0}$ immer lösbar, da $0^3 = 0$ gilt. Gelte im Folgenden $p \nmid a$.

- Ist $p = 3$, so gilt für jedes $a \in \mathbb{Z}$ die Kongruenz $a^3 \equiv a \pmod{3}$ (nach Satz 2.1.4). Die obige Gleichung hat somit für jedes $a \in \mathbb{Z}$ eine ganzzahlige Lösung $x \in \mathbb{Z}$.
- Für Primzahlen $p \equiv 1 \pmod{3}$ mit $p = \pi\overline{\pi}$ für ein Primelement $\pi \in \mathbb{Z}[\omega]$ sind nach Satz 3.1.10 die Körper $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ zueinander isomorph. Somit gilt für jedes $a \in \mathbb{Z}$ mit $p \nmid a$:

$$x^3 \equiv a \pmod{p} \text{ lösbar in } \mathbb{Z} \Leftrightarrow x^3 \equiv a \pmod{\pi} \text{ lösbar in } \mathbb{Z}[\omega]$$
$$\overset{3.2.8}{\Leftrightarrow} \left(\frac{a}{\pi}\right)_3 = 1.$$

- Gilt $p \equiv 2 \pmod{3}$, also insbesondere $3 \nmid p$, so enthält $\mathbb{Z}/p\mathbb{Z}$ kein Element der Ordnung 3, also ist $a \mapsto a^3$ ein Automorphismus auf $(\mathbb{Z}/p\mathbb{Z})^*$. Da wir die Lösbarkeit der Gleichung für ein $a \in \mathbb{Z}$ betrachten, erhalten wir auch für diesen Fall, dass die Kongruenz immer lösbar ist.

Im Folgenden werden wir Eulers Vermutung bezüglich Primzahlen der Form $p = x^2 + 27y^2$ als Anwendung des kubischen Reziprozitätsgesetzes aus [IR93, Kap.9, §6] beweisen.

3.6.1 Theorem. *Sei $p > 0$ eine Primzahl. Dann gilt:*

$$\exists x, y \in \mathbb{Z} : \; p = x^2 + 27y^2 \;\Leftrightarrow\; p \equiv 1 \pmod{3} \text{ und } 2 \text{ ist ein kubischer Rest modulo } p.$$

Für den Beweis dieses Theorems benötigen wir zunächst ein Lemma.

3.6.2 Lemma. *Für ein echt-komplexes primäres Primelement $\pi = a + b\omega \in \mathbb{Z}[\omega]$ gilt die Äquivalenz:*

$$\left(\frac{2}{\pi}\right)_3 = 1 \;\Leftrightarrow\; \pi \equiv 1 \pmod{2} \;\Leftrightarrow\; a \equiv 1 \pmod{2} \text{ und } b \equiv 0 \pmod{2}.$$

Beweis. Sei $p = \pi\overline{\pi}$. Ohne Einschränkung sei π primär, denn für $\pi' \sim \pi$ gilt:

$$x^3 \equiv 2 \pmod{\pi} \text{ ist lösbar } \Leftrightarrow\ x^3 \equiv 2 \pmod{\pi'} \text{ ist lösbar.}$$

Für $\pi \not\sim 1-\omega$ gilt nach dem kubischen Reziprozitätsgesetz

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3. \tag{3.16}$$

Außerdem gilt:

$$\pi = \pi^{\frac{4-1}{3}} = \pi^{\frac{N(2)-1}{3}} \equiv \left(\frac{\pi}{2}\right)_3 \pmod{2}. \tag{3.17}$$

Mit (3.16) und (3.17) folgt:

$$\left(\frac{2}{\pi}\right)_3 = 1 \overset{(3.16)}{\Leftrightarrow} \left(\frac{\pi}{2}\right)_3 = 1 \overset{(3.17)}{\Leftrightarrow} \pi \equiv 1 \pmod{2}.$$

□

Nun zu dem Beweis von Theorem 3.6.1.

Beweis von Theorem 3.6.1. Gelte $p = x^2 + 27y^2$. Es gilt $p \neq 3$, denn 3 besitzt keine solche Darstellung. Somit ist x nicht durch 3 teilbar. Außerdem gilt $p \equiv x^2 \pmod{3}$. Da 1 der einzige von 0 verschiedene quadratische Rest modulo 3 ist, folgt $p \equiv 1 \pmod{3}$.
Es bleibt nun noch zu zeigen, dass 2 ein kubischer Rest modulo p ist. Sei $\pi = x + 3\sqrt{-3}y$. Dann gilt $p = \pi\overline{\pi}$. Nach Lemma 3.6.2 genügt es die Kongruenz $\pi \equiv 1 \pmod{2}$ zu zeigen. Es gilt $\sqrt{-3} = 1 + 2\omega$ und somit ist $\pi = x + 3(1+2\omega)y = x + 3y + 6\omega y \in \mathbb{Z}[\omega]$. Mit dieser Darstellung von π folgt $\pi \equiv x + y \pmod{2}$. Wären x und y gerade, so wäre p durch 2 teilbar. Wären beide ungerade, so wäre p ebenso gerade. (Es gilt $p \neq 2$, da $p \equiv 1 \pmod{4}$ ist.) Also sind x und y in verschiedenen Restklassen modulo 2. Somit gilt $\pi \equiv x + y \equiv 1 \pmod{2}$.
Gelte nun umgekehrt $p \equiv 1 \pmod{3}$. Es existiert ein primäres Primelement $\pi = a + b\omega \in \mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi}$. Wegen π primär ist b durch 3 teilbar, etwa $b = 3n$. Damit ist

$$4p = 4(a^2 - 3an + 9n^2) = (2a - 3n)^2 + 27n^2. \tag{3.18}$$

Da 2 ein kubischer Rest modulo p ist, gilt nach Lemma 3.6.2 bereits $\pi \equiv 1 \pmod{2}$. Dann ist b gerade und somit ist auch $n \equiv 0 \pmod{2}$. Folglich gilt mit Gleichung (3.18):

$$p = \Bigg(\underbrace{\frac{2a-3n}{2}}_{=:x\in\mathbb{Z}}\Bigg)^2 + 27\Bigg(\underbrace{\frac{n}{2}}_{=:y\in\mathbb{Z}}\Bigg)^2.$$

□

3.6.3 Beispiel.

(1) Für $p = 7$ existiert keine Darstellung $7 = x^2 + 27y^2$. Somit ist die Gleichung $x^3 \equiv 2 \pmod{7}$ nicht lösbar.

(2) Es gilt $p = 31 = 2^2 + 27 \cdot 1^2$. Daher ist 2 ein kubischer Rest modulo 31.

3.6.4 Satz. [11] *Sei γ ein beliebiges primäres Element, sodass γ keine Kubikzahl in $\mathbb{Z}[\omega]$ ist.*[12] *Dann gibt es unendlich viele primären Primelemente π, sodass $x^3 \equiv \gamma \pmod{\pi}$ nicht lösbar ist (d.h. $\left(\frac{\gamma}{\pi}\right)_3 \neq 1$ für unendlich viele primären Primelemente π).*

Beweis. Sei $\gamma = \pm \prod_{i=1}^{s} \lambda_i^{e_i}$ die Primfaktorzerlegung mit paarweise verschiedenen primären Primelementen λ_i und $e_i \in \mathbb{N}$ für $i = 1, \ldots, s$. Da γ keine Kubikzahl in $\mathbb{Z}[\omega]$ ist, gibt es ein e_i ($i \in \{1, \ldots, s\}$), welches nicht durch 3 teilbar ist. Sei dies ohne Einschränkung e_s.
Wähle nun eine beliebige, endliche Menge von paarweise verschiedenen primären Primelementen $\pi_1, \ldots, \pi_n$, sodass $x^3 \equiv \gamma \pmod{\pi_i}$ für alle $i = 1, \ldots, n$ nicht lösbar ist. Es gilt zu zeigen, dass dann ein weiteres primäres Primelement θ existiert, sodass auch die Kongruenz $x^3 \equiv \gamma \pmod{\theta}$ nicht lösbar ist. Dann folgt die Behauptung, da die Kongruenz dann für unendlich viele primäre Primelemente nicht lösbar ist.
Sei weiterhin α ein kubischer Nichtrest modulo λ_s. Die Ideale $(\lambda_1), \ldots, (\lambda_s), (\pi_1), \ldots, (\pi_n)$ sind paarweise verschieden. Denn wäre $(\lambda_j) = (\pi_k)$ für ein $j \in \{1, \ldots, s\}$ und ein $k \in \{1, \ldots, n\}$, so wäre $\gamma \equiv 0 \pmod{\pi_k}$ und damit wäre die Kongruenz $x^3 \equiv \gamma \pmod{\pi_k}$ lösbar. Weiterhin sind alle Ideale jeweils relativ prim zu dem von 3 in $\mathbb{Z}[\omega]$ erzeugtem Ideal, da alle beteiligten Elemente primär sind. Nach dem Chinesischen Restsatz existiert eine Lösung der folgenden Kongruenzen.

$$\begin{aligned}
&(a) \quad x \equiv 1 \pmod{\lambda_i} \quad \text{für } i = 1, \ldots, s-1 \\
&(b) \quad x \equiv \alpha \pmod{\lambda_s} \\
&(c) \quad x \equiv 1 \pmod{\pi_i} \quad \text{für } i = 1, \ldots, n \\
&(d) \quad x \equiv 1 \pmod{3}
\end{aligned}$$

Sei β eine Lösung der Kongruenzen (a)-(d). Dann ist β nach (d) primär. Da auch λ_i für alle $i = 1, \ldots, s$ primär ist, gilt nach dem kubischen Reziprozitätsgesetz

$$\left(\frac{\lambda_i}{\beta}\right)_3 = \left(\frac{\beta}{\lambda_i}\right)_3 \quad \text{für } i = 1, \ldots, s. \tag{3.19}$$

Durch die Multiplikativität des kubischen Restsymbols folgt

$$\left(\frac{\gamma}{\beta}\right)_3 = \prod_{i=1}^{s} \left(\frac{\lambda_i}{\beta}\right)_3^{e_i} \overset{(3.19)}{=} \prod_{i=1}^{s} \left(\frac{\beta}{\lambda_i}\right)_3^{e_i} \overset{(a)}{=} \left(\frac{\beta}{\lambda_s}\right)_3^{e_s} \cdot \underbrace{\prod_{i=1}^{s-1} \left(\frac{1}{\lambda_i}\right)_3^{e_i}}_{=1} \overset{(b)}{=} \left(\frac{\alpha}{\lambda_s}\right)_3^{e_s} \neq 1.$$

Der letzte Schritt folgt, da α ein kubischer Nichtrest modulo λ_s und e_s nicht durch 3 teilbar ist. Da β primär ist, existiert eine primäre Primfaktorzerlegung $\beta = \pm \prod_{i=1}^{m} \varrho_i$. Somit gilt nach Definition des allgemeinen kubischen Restsymbols

$$1 \neq \left(\frac{\gamma}{\beta}\right)_3 = \prod_{i=1}^{m} \left(\frac{\gamma}{\varrho_i}\right)_3.$$

[11] Die Aussage von diesem und dem nächsten Satz ist aus [IR93, Aufg. 21]

[12] Die zusätzliche Voraussetzung $\gamma \neq x^3$ für alle $x \in \mathbb{Z}[\omega]$ wird hier benötigt, denn es gilt $\gamma = (4+\omega)^3 \equiv -1 \pmod{3}$ und damit ist γ primär. Die Gleichung $x^3 \equiv \gamma \pmod{\pi}$ ist somit für alle Primelemente gültig.

Folglich existiert ein $k \in \{1, \dots, m\}$, sodass $\left(\frac{\gamma}{\varrho_k}\right)_3 \neq 1$ gilt. Mit der Kongruenz (c) gilt $\pi_i \nmid \beta$ für alle $i = 1, \dots, n$. Damit ist $\theta := \varrho_k$ jeweils von $\pi_1, \dots, \pi_n$ verschieden. Somit ist θ ein weiteres primäres Element, sodass die gewünschte Kongruenz nicht lösbar ist. □

Dieselbe Aussage gilt auch für ω und $1 - \omega$ anstelle eines primären Elements γ.

3.6.5 Satz.

(a) Es gibt unendlich viele primären Primelemente π, sodass $x^3 \equiv \omega \pmod{\pi}$ nicht lösbar ist.

(b) Ebenso gibt es unendlich viele primären Primelemente π, sodass $x^3 \equiv 1 - \omega \pmod{\pi}$ nicht lösbar ist.

Beweis.

(a) Sei $\{\lambda_1, \dots, \lambda_r\}$ eine endliche Menge von primären Primelementen mit $\lambda_i = 3m_i + 1 + 3n_i\omega \equiv 1 \pmod 3$, sodass die Kongruenz $x^3 \equiv \omega \pmod{\lambda_i}$ für alle $i = 1, \dots, r$ nicht lösbar ist. Dann ist $\beta = 3\lambda_1 \cdots \lambda_r + 1$ primär, denn $\beta \equiv 1 \pmod 3$. Da alle λ_i $(i = 1, \dots, r)$ primär sind, ist auch das Produkt $\prod_{i=1}^{r} \lambda_i$ primär mit $\prod_{i=1}^{r} \lambda_i \equiv 1 \pmod 3$. Folglich existieren $n, m \in \mathbb{Z}$, sodass $\lambda_1 \cdots \lambda_r = 3m + 1 + 3n\omega$ gilt. Dann ist $\beta = 3(3m + 1 + 3n\omega) + 1 = 3\underbrace{(3m+1)}_{=:M} + 1 + 3\underbrace{(3n)}_{=:N}\omega$ und mit dem Ergänzungssatz 3.5.9 des kubischen Reziprozitätsgesetzes gilt

$$\left(\frac{\omega}{\beta}\right)_3 = \omega^{-M-N} = \omega^{-3m-1-3n} = \omega^2 \neq 1.$$

Sei $\beta = \pm \prod_{i=1}^{s} \varrho_i$ die primäre Primfaktorzerlegung von β mit $\varrho_i \equiv 1 \pmod 3$. Dann ist

$$1 \neq \left(\frac{\omega}{\beta}\right)_3 = \prod_{i=1}^{s} \left(\frac{\omega}{\varrho_i}\right)_3.$$

Folglich gilt $\left(\frac{\omega}{\varrho_k}\right)_3 \neq 1$ für ein $k \in \{1, \dots, s\}$. Da β nach Definition durch keines der λ_i teilbar ist, gilt $\varrho_k \notin \{\lambda_1, \dots, \lambda_r\}$. Das heißt zu jeder endlichen Menge $\{\lambda_1, \dots, \lambda_r\}$, gibt es noch ein weiteres Element ϱ_k, sodass $x^3 \equiv \omega \pmod{\varrho_k}$ nicht lösbar ist. Somit ist die Kongruenz für unendlich viele primäre Primelemente nicht erfüllt.

(b) Der Beweis funktioniert analog zu dem in (a) geführten Beweis. Denn für das in (a) gewählte β gilt

$$\left(\frac{1+\omega}{\beta}\right)_3 = \omega^M = \omega^{3m+1} = \omega \neq 1.$$

□

3.6.6 Satz. [13] *Gilt für ein $\gamma \in \mathbb{Z}[\omega]$, dass die Kongruenz $x^3 \equiv \gamma \pmod{\pi}$ für alle bis auf endlich viele primären Primelemente π lösbar ist, so ist γ bereits eine dritte Potenz in $\mathbb{Z}[\omega]$ (d.h. $\gamma = x^3$ für ein $x \in \mathbb{Z}[\omega]$).*

Beweis. Sei $\gamma = \pm u\lambda_1^{e_1} \cdots \lambda_s^{e_s}$ eine Primfaktorzerlegung von γ mit paarweise verschiedenen Primelementen λ_i $(i = 1, \ldots, s)$ von $\mathbb{Z}[\omega]$ und einer Einheit u der Form $u = \omega^{e_0}$. Weiterhin sei $e_0, \ldots, e_s \in \mathbb{N}_0$, $\lambda_1 = (1 - \omega)$ und λ_i für alle $i = 2, \ldots, s$ primär.
Angenommen γ wäre keine dritte Potenz in $\mathbb{Z}[\omega]$, d.h. für mindestens ein $i \in \{0, 1, \ldots, s\}$ ist e_i nicht durch 3 teilbar. Wir wissen aus Satz 3.6.4 und 3.6.5, dass

1. $x^3 \equiv \omega \pmod{\pi}$
2. $x^3 \equiv \lambda_1 = 1 - \omega \pmod{\pi}$
3. $x^3 \equiv \lambda_i \pmod{\pi} \qquad i = 2, \ldots, s$

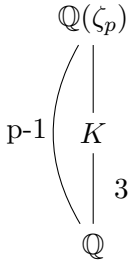
jeweils für unendlich viele primären Primelemente π nicht lösbar sind. Da mindestens ein Faktor $\lambda \in \{u, \lambda_1, \ldots, \lambda_s\}$ von γ in einer nicht durch drei teilbaren Potenz vorkommt, ist für diesen Faktor λ mit zugehörigem Exponent $e = e_i$ für ein $i = 0, \ldots, e_s$ die Kongruenz $x^3 \equiv \lambda^e \pmod{\pi}$ für unendlich viele primären Primelemente π_i nicht lösbar. Dann ist auch die Kongruenz $x^3 \equiv \gamma \pmod{\pi}$ für unendlich viele primären Primelement π nicht lösbar. Denn da $\mathbb{Z}[\omega]$ ein faktorieller Ring ist, gilt bereits $\lambda_i \not\equiv \lambda_j \pmod{\pi}$ für $i \neq j$ $(i, j \in \{1, \ldots, s\})$ und unendlich viele primären Primelemente π. Angenommen es würde $\lambda_i \equiv \lambda_j \pmod{\pi}$ für alle bis auf endlich viele primären Primelemente gelten, dann hätte die Differenz $\lambda_i - \lambda_j$ unendlich viele Primteiler. Dies ist allerdings für $0 \neq \lambda_i - \lambda_j$ nicht möglich.
Folglich muss γ eine Kubikzahl in $\mathbb{Z}[\omega]$ sein. □

3.7 Zerlegung von Primzahlen

Die Untersuchung des kubischen Reziprozitätsgesetzes ist auch mit einer anderen Herangehensweise möglich. Die in diesem Abschnitt betrachtete Methode ist durch einen Beweis des quadratischen Reziprozitätsgesetzes motiviert. Bei diesem Beweis werden die Zerlegungen von Primzahlen in einer quadratischen Erweiterung mit den Zerlegungen in einer Kreisteilungskörpererweiterung verglichen (siehe [ZT14]). Im Unterschied zum quadratischen Fall, kann man mit dieser Herangehensweise das kubische Reziprozitätsgesetz nicht vollständig beweisen.
Dieser Abschnitt wird ohne die bisher gezeigten Sätze auskommen mit Ausnahme der Sätze über die Eigenschaften des Ganzheitsringes $\mathbb{Z}[\omega]$ aus dem Abschnitt 3.1. Dabei wird das Vorgehen analog zu [Lem00, 7.1] sein.
Wir betrachten weiterhin den imaginär-quadratischen Zahlkörper $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ für $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und dessen Ganzheitsring $\mathbb{Z}[\omega]$. Im Folgenden sei p stets eine in $\mathbb{Q}(\omega)$ zerlegte Primzahl mit $p = \pi\overline{\pi} \equiv 1 \pmod{3}$. Wir können annehmen, dass π primär ist und für $p = a^2 - ab + b^2$ ist $\pi = a + b\omega$ mit $a \equiv 1 \pmod{3}$ und $b \equiv 0 \pmod{3}$ ein solches Element. Eine andere Darstellung von π ist $\pi = \frac{1}{2}(L + 3M\sqrt{-3})$ mit $L = 2a - b$ und $M = \frac{b}{3}$.

[13] Aussage siehe [IR93, S.135, Aufg 22]

3.7.1 Konstruktion.



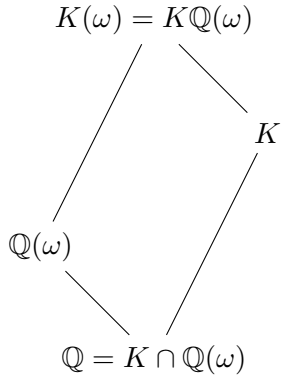
Die Primzahl $p = \pi\overline{\pi} \equiv 1 \pmod 3$ ist in $\mathbb{Q}(\omega)/\mathbb{Q}$ zerlegt.
Wir betrachten nun den Kreisteilungskörper $\mathbb{Q}(\zeta_p)$ für eine primitive p-te Einheitswurzel ζ_p. Wir identifizieren $G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ mit $\mathbb{F}_p^*$. Mit Hilfe der Galoistheorie erhalten wir eine Bijektion

$$\{\text{Teiler von } p-1\} \leftrightarrow \{\text{Untergruppen von } \mathbb{F}_p^*\} \leftrightarrow \{\text{Zwischenkörper von } \mathbb{Q}(\zeta_p)/\mathbb{Q}\}$$

Wegen $3 \mid (p-1)$ existiert eine Untergruppe H von $\mathbb{F}_p^*$ mit $[G : H] = 3$. Somit gibt es nach dem Hauptsatz der Galoistheorie auch einen Zwischenkörper K von $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ mit $[K : \mathbb{Q}] = 3$.

3.7.2 Satz. *Die Körpererweiterung $K/\mathbb{Q}$ ist zyklisch und somit ist auch die Körpererweiterung $K(\omega)/\mathbb{Q}(\omega)$ zyklisch mit* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega))$.

Beweis.



Da $\mathbb{F}_p^*$ zyklisch ist, ist auch jede Untergruppe von $\mathbb{F}_p^*$ zyklisch. Insbesondere ist $\mathrm{Gal}(K/\mathbb{Q})$ zyklisch. Daher ist auch $K/\mathbb{Q}$ zyklische Galoiserweiterung. Mit dem Translationssatz [Alg13, Kap.4, 3.10] folgt, dass auch die Körpererweiterung $K(\omega)/\mathbb{Q}(\omega)$ galoissch und zyklisch ist, da $\mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega)) \cong \mathrm{Gal}(K/\mathbb{Q})$ gilt.

□

3.7.3 Bemerkung. Hierin liegt ein Unterschied zu dem Vorgehen im quadratischen Fall. Beim Beweis des quadratischen Reziprozitätsgesetzes verwendet man direkt einen quadratischen Zwischenkörper. Im Gegensatz dazu muss man im kubischen Fall die Translation $K(\omega)/\mathbb{Q}(\omega)$ des kubischen Zwischenkörpers K betrachten.

Im Folgenden wird ein primitives Element der Körpererweiterung $K(\omega)/\mathbb{Q}(\omega)$ bestimmt werden.

3.7.4 Satz. *Es existiert ein $\mu \in \mathbb{Z}[\omega]$, sodass $K(\omega) = \mathbb{Q}(\omega, \sqrt[3]{\mu})$ gilt.*

Für den Beweis benötigen wir Hilberts Theorem 90 in der folgenden Form :

3.7.5 Satz. [14] *Sei E/F eine endliche zyklische Galoiserweiterung und* $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. *Dann gilt für jedes $\beta \in E$:*

$$N_{E/F}(\beta) = 1 \;\Leftrightarrow\; \beta = \frac{\alpha}{\sigma(\alpha)} \text{ für ein } \alpha \in E^*.$$

[14] siehe [Bos09, S. 200]

Beweis. Gelte $\beta = \frac{\alpha}{\sigma(\alpha)}$. Dann gilt

$$N_{E/F}(\beta) = \prod_{i=0}^{n-1} \sigma^i(\beta) = \prod_{i=0}^{n-1} \frac{\sigma^i(\alpha)}{\sigma^{i+1}(\alpha)} = 1.$$

Umgekehrt sei nun $N_{E/F}(\beta) = 1$. Betrachte die Abbildung von E nach F definiert durch

$$\mathrm{id} + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}. \tag{3.20}$$

Da die Automorphismen der Galoisgruppe linear unabhängig sind, ist dies nicht die Nullabbildung. Deswegen existiert ein $\theta \in E$, sodass

$$\theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta) = \alpha \in E^*$$

gilt. Man erhält nun durch Anwendung von σ und anschließender Multiplikation mit β die Gleichung

$$\beta\sigma(\alpha) = \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta) + \underbrace{\beta\sigma(\beta)\cdots\sigma^{n-1}(\beta)}_{=N_{E/F}(\beta)=1}\theta = \alpha.$$

Folglich ist $\beta = \frac{\alpha}{\sigma(\alpha)}$. □

Nun zurück zu dem Beweis von Satz 3.7.4.

Beweis. Sei σ ein Erzeuger der Galoisgruppe $\mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega))$. Wir wollen Hilberts Theorem 90 auf die dritte primitive Einheitswurzel $\omega \in \mathbb{Q}(\omega) \subseteq K(\omega)$ anwenden. Dazu berechne die $K(\omega)/\mathbb{Q}(\omega)$-Norm von ω. Es gilt

$$N_{K(\omega)/\mathbb{Q}(\omega)}(\omega) = \omega^3 = 1.$$

Folglich existiert nach Hilberts Theorem 90 ein $y \in L^*$, sodass $\omega = \frac{y}{\sigma(y)}$ gilt. Oder anders gesagt $\sigma(y) = \omega^{-1}y$. Weiterhin gilt $\sigma^2(y) = \omega^{-2}y$. Dann hat y schon 3 verschiedene $\mathbb{Q}(\omega)$-Konjugierte. Außerdem ist $\tilde{\mu} := y^3 \in \mathbb{Q}(\omega)$, denn es gilt

$$\sigma^i(\tilde{\mu}) = (\sigma^i(y))^3 = (w^{-i}y)^3 = y^3 = \tilde{\mu}.$$

Damit ist gezeigt, dass $\tilde{\mu}$ fix unter σ^i für $i = 0, 1, 2$ ist. Folglich liegt $\tilde{\mu}$ in dem Grundkörper $\mathbb{Q}(\omega)$. Damit ist y ein primitives Element, sodass $K(\omega) = \mathbb{Q}(\omega, y)$ gilt.
Nun ist noch zu zeigen, dass es ein $\mu \in \mathbb{Z}[\omega]$ mit $K(\omega) = \mathbb{Q}(\omega, \sqrt[3]{\mu})$ gibt. Da $\tilde{\mu} \in \mathbb{Q}(\omega)$ ist, existiert eine Darstellung $\tilde{\mu} = \frac{\mu_1}{\mu_2}$ mit $\mu_1, \mu_2 \in \mathbb{Z}[\omega]$. Für $\mu := \tilde{\mu}\mu_2^3 \in \mathbb{Z}[\omega]$ gilt $\mathbb{Q}(\omega, \sqrt[3]{\mu}) = \mathbb{Q}(\omega, \sqrt[3]{\tilde{\mu}})$. □

Im Folgenden wird das Element $\mu \in \mathbb{Z}[\omega]$ aus Satz 3.7.4 genauer bestimmt.

3.7.6 Konstruktion. In $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ist nur p verzweigt (siehe [ZT14, 5.1.8]), alle anderen Primzahlen sind unverzweigt. Insbesondere ist $3 \neq p$ in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ unverzweigt und wegen der Multiplikativität des Verzweigungsindex ist 3 auch in der Teilerweiterung $K/\mathbb{Q}$ unverzweigt. Es gilt daher $1-\omega \notin K$ und wir können annehmen, dass μ nicht durch 3 teilbar ist. Denn wäre μ durch 3 teilbar, so würde $\frac{\mu}{3}$ dieselbe Körpererweiterung erzeugen. dadurch kann erreicht werden, dass $1-\omega$ kein Teiler von μ ist.

Weiterhin ist klar, dass μ keine Einheit in $\mathbb{Z}[\omega]$ ist, denn sonst wäre $K(\omega)/\mathbb{Q}(\omega)$ keine echte Erweiterung.
In Satz 3.1.8 wurde gezeigt, dass eine Einheit u von $\mathbb{Z}[\omega]$ existiert, sodass $u\mu$ primär ist, das heißt $u\mu \equiv \pm 1 \pmod 3$. Da $u\mu$ dieselbe Körpererweiterung wie μ erzeugt, können wir $\mu \equiv \pm 1 \pmod 3$ annehmen.
Da außerhalb von $p = \pi\overline{\pi}$ die Körpererweiterung $K/\mathbb{Q}$ unverzweigt ist, können wir weiterhin annehmen, dass μ durch keine Primzahl $q \neq p$ teilbar ist. Außerdem können wir alle dritten Potenzen eliminiert werden. Damit ist $\mu \in \{\pi, \overline{\pi}, \pi\overline{\pi}, \pi^2\overline{\pi}, \pi\overline{\pi}^2\}$.
Sei σ der nichttriviale Automorphismus von $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$, also ist σ die komplexe Konjugation. Da $K(\omega)/\mathbb{Q}$ abelsch ist, folgt mit [Lem00, Kor.4.17], dass $\omega^\sigma = \omega^{a(\sigma)}$ für ein $a(\sigma) \in \mathbb{N}$ gilt. Da ω eine dritte Einheitswurzel ist, muss $a(\sigma) = 2$ gelten. Außerdem ist $a(\sigma)$ so gewählt, dass $\mu^\sigma \mu^{-a(\sigma)} = \xi^3$ für ein $\xi \in \mathbb{Z}[\omega]$ (nach [Lem00, Prop. 4.14]). Somit muss $\mu^\sigma\mu = \xi^3$ für ein $\xi \in \mathbb{Z}[\omega]$ gelten. Nun kann man überprüfen, welche Kandidaten von μ diese Bedingung erfüllen.

1.	$\mu = \pi$:	$\mu^\sigma\mu = \overline{\pi}\pi = p$	keine dritte Potenz in $\mathbb{Z}[\omega]$
2.	$\mu = \overline{\pi}$:	$\mu^\sigma\mu = \pi\overline{\pi} = p$	analog zu 1.
3.	$\mu = \pi\overline{\pi}$:	$\mu^\sigma\mu = \pi^2\overline{\pi}^2$	keine dritte Potenz in $\mathbb{Z}[\omega]$
4.	$\mu = \pi^2\overline{\pi}$:	$\mu^\sigma\mu = \overline{\pi}^2\pi\pi^2\overline{\pi} = p^3$	
5.	$\mu = \pi\overline{\pi}^2$:	$\mu^\sigma\mu = p^3$	

Die ersten 3 Möglichkeiten können ausgeschlossen werden und es bleiben nur die letzten beiden Möglichkeiten übrig. Diese unterscheiden sich nur durch komplexe Konjugation. Folglich können wir ohne Einschränkung annehmen, dass $\mu = \pi^2\overline{\pi}$ gilt.

Sei nun $\alpha := \sqrt[3]{\mu} + \sqrt[3]{\overline{\mu}}$ so gewählt, dass α reell ist. Da α auch in $K(\omega)$ enthalten ist, gilt $\alpha \in K(\omega) \cap \mathbb{R} = K$. Wir können nun das Minimalpolynom von α über $\mathbb{Q}$ bestimmen.

3.7.7 Konstruktion. Es gilt

$$\begin{aligned}\alpha^3 &= (\sqrt[3]{\mu} + \sqrt[3]{\overline{\mu}})^3 = \mu + 3\sqrt[3]{\mu^2\overline{\mu}} + 3\sqrt[3]{\overline{\mu}^2\mu} + \overline{\mu} \\ &= \mu + \overline{\mu} + 3p(\sqrt[3]{\mu} + \sqrt[3]{\overline{\mu}}) \\ &= p(\underbrace{\pi + \overline{\pi}}_{=p(2a-b)=pL}) + 3p\alpha\end{aligned}$$

Somit ist das Minimalpolynom von α über $\mathbb{Q}$ durch $f_\alpha(x) = x^3 - 3px - pL$ gegeben. Dabei ist das Vorzeichen von L abhängig von der Wahl von α. Denn ist α eine Nullstelle von f_α, so ist wegen

$$(-\alpha)^3 - 3p(-\alpha) - pL = -(\alpha^3 - 3p\alpha) - pL = 0$$

$-\alpha$ eine Nullstelle von $x^3 - pLx + pL$.

Für die folgenden Untersuchungen benötigen wir zunächst noch ein rationales kubisches Restsymbol, das zur Identifizierung von n-ten Potenzen in $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p dienen soll. Dazu definieren wir eine allgemeine Form eines n-ten rationalen Restsymbols, jedoch nur in vereinfachter Weise. Wir werden nur angeben, wann dieses Restsymbol gleich 1 ist, jedoch keine weiteren Werte festlegen.

3.7.8 Definition. [15] Definiere für $a \in \mathbb{Z}$ und eine Primzahl $p \equiv 1 \pmod{2n}$ für ein $n \in \mathbb{N}$ das *n-te rationale Restsymbol* $\left[\frac{a}{p}\right]_n$ durch:

$$\left[\frac{a}{p}\right]_n \begin{cases} = 1, & \text{falls } a^{\frac{p-1}{n}} \equiv 1 \pmod{p} \\ \neq 1, & \text{sonst} \end{cases}.$$

Im Folgenden wird der Satz [ZT14, Kap.5, 2.11] verwendet werden.

3.7.9 Satz. *Seien p, q voneinander verschiedene Primzahlen. Sei m ein Teiler von $p-1$ und $K_m \subseteq \mathbb{Q}(\zeta_p)$ der Teilkörper mit $[K_m : \mathbb{Q}] = m$. Dann gilt:*

$$q \text{ ist } m\text{-te Potenz in } \mathbb{F}_p^* \Leftrightarrow q \text{ ist in } K_m \text{ total zerlegt.}$$

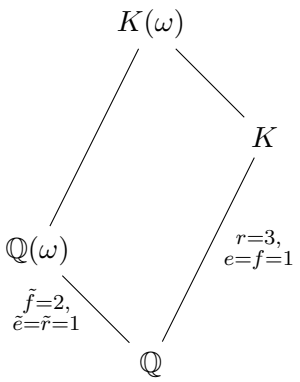
Mit Hilfe des eben eingeführten rationalen Restsymbols, das hier nur für $n = 3$ verwendet wird, können wir nun rationale Kriterien für kubische Reste untersuchen. Dazu werden zunächst die in $\mathbb{Q}(\omega)/\mathbb{Q}$ trägen Primzahlen $q \equiv 2 \pmod 3$ betrachtet.

3.7.10 Satz. *Sei $q \equiv 2 \pmod 3$ eine Primzahl. Dann ist q träge in $\mathbb{Q}(\omega)$ und es gilt*

$$\left[\frac{q}{p}\right]_3 = 1 \Leftrightarrow \mu \equiv \xi^3 \pmod{q} \text{ für ein } \xi \in \mathbb{Z}[\omega].$$

Beweis. In Bemerkung 3.1.1 wurde bereits festgestellt, das Primzahlen $q \equiv 2 \pmod 3$ in $\mathbb{Q}(\omega)$ träge sind. Wir erhalten somit

$$\begin{aligned} \left[\frac{q}{p}\right]_3 = 1 &\overset{\text{Def.}}{\Leftrightarrow} q^{\frac{p-1}{3}} \equiv 1 \pmod{p} \\ &\overset{3.2.7}{\Leftrightarrow} x^3 \equiv q \pmod{p} \text{ ist lösbar für ein } x \in \mathbb{Z} \\ &\overset{3.7.9}{\Leftrightarrow} q \text{ ist in } K/\mathbb{Q} \text{ zerlegt} \\ &\Leftrightarrow q \text{ ist in } K(\omega)/\mathbb{Q}(\omega) \text{ zerlegt} \\ &\Leftrightarrow \exists \xi \in \mathbb{Z}[\omega] : \mu \equiv \xi^3 \pmod{q} \end{aligned}$$



Dabei wird im vorletzten Schritt die Multiplikativität des Trägheitsindex (in dem Schaubild mit f bzw. $\tilde{f}$ gekennzeichnet) und des Verzweigungsindex (e bzw. $\tilde{e}$) verwendet. In dem Schaubild bezeichnet r bzw. $\tilde{r}$ die Anzahl der Primfaktoren von q in der jeweiligen Körpererweiterung.

□

Damit ist es bereits möglich Eulers Vermutung (siehe Theorem 3.6.1) zu beweisen.

3.7.11 Satz. *2 ist genau dann ein kubischer Rest modulo $p = \frac{1}{4}(L^2 + 27M^2)$, wenn $L \equiv M \equiv 0 \pmod 2$ gilt.*

[15] siehe [Lem00, S.154f]. Die Notation stimmt nicht mit der Notation in [Lem00] überein.

Beweis. Sei $q = 2$, dann gilt nach Satz 3.7.10:

$$\left[\frac{2}{p}\right]_3 = 1 \;\Leftrightarrow\; \mu \equiv \xi^3 \pmod 2 \text{ für ein } \xi \in \mathbb{Z}[\omega].$$

Da μ teilerfremd zu 2 ist, muss auch ein solches $\xi = a+b\omega$ teilerfremd zu 2 sein. Für jedes solche ξ gilt $\xi^3 \equiv 1 \pmod 2$, denn

$$(a+b\omega)^3 = a^3 + 3ab(a\omega + b\omega^2) + b^3 = a^3 + b^3 + 3ab(a-b)\omega - 3ab^2 \equiv 1 \pmod 2,$$

falls $2 \nmid a$ oder $2 \nmid b$ gilt. Man erhält nun insgesamt

$$\left[\frac{2}{p}\right]_3 = 1 \;\Leftrightarrow\; \mu \equiv 1 \pmod 2 \overset{\mu=p\pi}{\Leftrightarrow} \pi \equiv 1 \pmod 2.$$

Die Behauptung folgt nun durch die Darstellung $\pi = \frac{1}{2}(L + 3M\sqrt{-3})$ des Primelements π. □

Im folgenden benötigen wir eine weitere Aussage aus der Zahlentheorie.

3.7.12 Lemma. [16] *Sei K ein quadratischer Zahlkörper mit Diskriminante d_K und $p > 2$ eine Primzahl mit $p \nmid d_K$. Dann gilt für alle $\alpha \in K$*

$$\alpha^p \equiv \begin{cases} \alpha \pmod p, & \text{falls } \left(\frac{d_K}{p}\right)_2 = 1 \\ \alpha' \pmod p, & \text{falls } \left(\frac{d_K}{p}\right)_2 = -1 \end{cases}$$

Dabei bezeichnet $\alpha \mapsto \alpha'$ den nichttrivialen $\mathbb{Q}$-Automorphismus von K (bei imaginär-quadratischen Zahlkörpern entspricht dies der komplexen Konjugation).

Beweis. Sei $K = \mathbb{Q}(\sqrt{d})$ mit $1 \neq d \in \mathbb{Z}$ quadratfrei. Dann gilt für die Diskriminante

$$d_K = \begin{cases} 4d, & \text{falls } d \equiv 2,3 \pmod 4 \\ d, & \text{falls } d \equiv 1 \pmod 4 \end{cases}.$$

Setze nun $\varrho = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2,3 \pmod 4 \\ \frac{1}{2}(1+\sqrt{d}), & \text{falls } d \equiv 1 \pmod 4 \end{cases}$.
Sei $\alpha = a + b\varrho \in \mathcal{O}_K = \mathbb{Z}[\varrho]$ beliebig mit $a, b \in \mathbb{Z}$. Dann gilt mit dem Frobenius-Automorphismus

$$\alpha^p \equiv a^p + b^p\varrho^p \equiv a + b\varrho^p \pmod p.$$

Ist $d \equiv 2,3 \pmod 4$, also $d_K \equiv 0 \pmod 4$, so ist p ungerade, da nach Voraussetzung $p \nmid d_K$ gilt. Mit dem Euler-Kriterium (3.3) folgt:

$$\varrho^p = \sqrt{d}^p = d^{\frac{p-1}{2}}\sqrt{d} \equiv \left(\frac{d}{p}\right)_2 \sqrt{d} = \left(\frac{d_K}{p}\right)_2 \varrho \pmod p.$$

Ist $\left(\frac{d_K}{p}\right)_2 = 1$, so ist $\alpha^p \equiv a + b\varrho = \alpha \pmod p$. Ist andernfalls $\left(\frac{d_K}{p}\right)_2 = -1$, so ist $\alpha^p \equiv a - b\varrho = \alpha' \pmod p$.

[16] siehe [Lem00, Satz 2.21]

Sei nun $d_K = d \equiv 1 \pmod 4$. Da $p > 2$ eine ungerade Primzahl ist, folgt die Behauptung analog, denn es gilt $\sqrt{d}^p \equiv \left(\frac{d_K}{p}\right)_2 \sqrt{d} \pmod p$ und somit

$$\varrho^p \equiv \frac{1}{2}(1+\sqrt{d}^p) \equiv \begin{cases} \frac{1}{2}(1+\sqrt{d}) = \varrho, & \text{falls } \left(\frac{d_K}{p}\right)_2 = 1 \\ \frac{1}{2}(1-\sqrt{d}) = \varrho', & \text{falls } \left(\frac{d_K}{p}\right)_2 = -1 \end{cases}.$$

□

Wir werden einen Spezialfall von diesem Lemma benötigen.

3.7.13 Korollar. *Für eine in $\mathbb{Q}(\omega)$ träge Primzahl $q \equiv 2 \pmod 3$ gilt $\pi^q \equiv \overline{\pi} \pmod q$ für ein $\pi \in \mathbb{Z}[\omega]$.*

Beweis. Die Diskriminante des Zahlkörpers $K = \mathbb{Q}(\omega)$ ist $d_K = -3$. Außerdem gilt

$$\left(\frac{-3}{q}\right)_2 = \left(\frac{-1}{q}\right)_2 \left(\frac{3}{q}\right)_2 = (-1)^{\frac{q-1}{2}} (-1)^{\frac{q-1}{2}\frac{3-1}{2}} \left(\frac{q}{3}\right)_2 = \left(\frac{2}{3}\right)_2 = -1.$$

Damit gilt nach Satz 3.7.12 für $\pi \in \mathbb{Z}[\omega]$ bereits $\pi^q \equiv \overline{\pi} \pmod q$. □

Für Primzahlen $q > 2$ mit $q \equiv 2 \pmod 3$ können wir auch genauer angeben, wann $\left[\frac{q}{p}\right]_3 = 1$ gilt.

3.7.14 Satz. *Sei $q > 2$ eine träge Primzahl in $\mathbb{Q}(\omega)$. Dann gilt:*

$$\left[\frac{q}{p}\right]_3 = 1 \Leftrightarrow \pi^{\frac{q+1}{3}} \equiv \overline{\pi}^{\frac{q+1}{3}} \pmod q.$$

Beweis. Für $q \equiv 2 \pmod 3$ mit $q > 2$ gilt $p^{\frac{q^2-1}{3}} = \left(p^{q-1}\right)^{\frac{q+1}{3}} \equiv 1 \pmod q$. Somit ist $\mu = p\pi$ genau dann eine dritte Potenz modulo q, wenn π eine solche dritte Potenz ist. Außerdem folgt nach Korollar 3.7.13, dass $\pi^q \equiv \overline{\pi} \pmod q$ gilt. Folglich ist

$$\overline{\pi}^{\frac{q+1}{3}} \equiv (\pi^q)^{\frac{q+1}{3}} = \pi^{\frac{q+1}{3}} \pi^{\frac{(q+1)(q-1)}{3}} \pmod q. \tag{3.21}$$

Dann folgt:

$$\begin{aligned} \left[\frac{q}{p}\right]_3 = 1 &\overset{3.7.10}{\Leftrightarrow} \mu \equiv \xi^3 \pmod q \\ &\overset{\mu = p\pi}{\Leftrightarrow} \pi \equiv \xi^3 \pmod q \text{ für ein } \xi \in \mathbb{Z}[\omega] \\ &\overset{3.2.7}{\Leftrightarrow} \pi^{\frac{q^2-1}{3}} \equiv 1 \pmod q \\ &\overset{(3.21)}{\Leftrightarrow} \pi^{\frac{q+1}{3}} \equiv \overline{\pi}^{\frac{q+1}{3}} \pmod q. \end{aligned}$$

□

3.7.15 Definition. Definiere für ungerade Primzahlen $q \equiv 2 \pmod 3$ und $n := \frac{q+1}{3}$ die Summe $g_q := \sum_{\substack{j=1 \\ j \equiv 1 \pmod 2}}^{n} \binom{n}{j} 3^j (-3)^{\frac{j-1}{2}} L^{n-j} M^j$.

3.7.16 Satz. *Für $q \equiv 2 \pmod 3$ mit $q > 2$ und $\pi = \frac{1}{2}(L + 3M\sqrt{-3})$ folgt*

$$\left[\frac{q}{p}\right]_3 = 1 \Leftrightarrow g_q \equiv 0 \pmod q.$$

Beweis. Nach Satz 3.7.14 gilt $\left[\frac{q}{p}\right]_3 = 1 \Leftrightarrow \pi^{\frac{q+1}{3}} \equiv \overline{\pi}^{\frac{q+1}{3}} \pmod q$. Setze $\pi = \frac{1}{2}(L+3M\sqrt{-3})$ ein. Dann gilt

$$\begin{aligned}
\left[\frac{q}{p}\right]_3 = 1 &\Leftrightarrow \left(\frac{1}{2}(L + 3M\sqrt{-3})\right)^{\frac{q+1}{3}} \equiv \left(\frac{1}{2}(L - 3M\sqrt{-3})\right)^{\frac{q+1}{3}} \pmod q \\
&\Leftrightarrow \sum_{i=1}^{n} \binom{n}{i} L^{n-i} 3^i M^i \sqrt{-3}^i \equiv \sum_{i=1}^{n} \binom{n}{i} L^{n-i} 3^i M^i (-\sqrt{-3})^i \pmod q \\
&\Leftrightarrow 2 \sum_{\substack{i=1 \\ i \equiv 1 \pmod 2}}^{n} \binom{n}{i} L^{n-i} 3^i M^i \sqrt{-3}^i \equiv 0 \pmod q \\
&\Leftrightarrow g_q \equiv 0 \pmod q.
\end{aligned}$$

Der letzte Schritt ist möglich, da nach Voraussetzung q eine von 2 verschiedene Primzahl ist und somit $\mathrm{ggT}(q, 2) = 1$. □

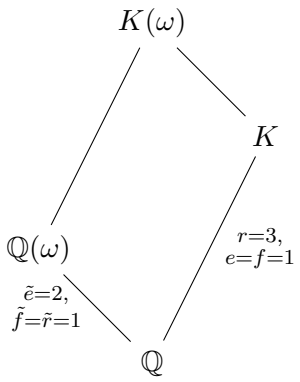
Betrachte nun die in $\mathbb{Q}(\omega)$ verzweigte Primzahl $q = 3 = -\omega^2(1-\omega)^2$.
Sei $\mathfrak{q} = \sqrt{-3}\mathbb{Z}[\omega] = (1-\omega)\mathbb{Z}[\omega]$ das von $(1-\omega)$ in $\mathbb{Z}[\omega]$ erzeugte Ideal. (Die Gleichheit der Ideale folgt aus $(1-\omega) = \sqrt{-3}\omega^2$ und $\sqrt{-3} = \omega(1-\omega)$.)

3.7.17 Satz. *Es gilt:*

$$\left[\frac{3}{p}\right]_3 = 1 \Leftrightarrow \mu \equiv \xi^3 \pmod{3\mathfrak{q}} \text{ für ein } \xi \in \mathbb{Z}[\omega].$$

Beweis.

$$\begin{aligned}
\left[\frac{3}{p}\right]_3 = 1 &\Leftrightarrow 3^{\frac{p-1}{3}} \equiv 1 \pmod p \\
&\overset{3.2.7}{\Leftrightarrow} 3 \text{ ist in } K/\mathbb{Q} \text{ zerlegt} \\
&\Leftrightarrow \mathfrak{q} \text{ ist in } K(\omega)/\mathbb{Q}(\omega) \text{ zerlegt} \\
&\Leftrightarrow \mu = \xi^3 \pmod{3\mathfrak{q}} \text{ für ein } \xi \in \mathbb{Z}[\omega]
\end{aligned}$$



Im letzten Schritt wurde dabei die Zerlegung von Primzahlen in Kummer-Erweiterungen [Lem00, Thm. 4.12] verwendet.
(In dem Schaubild kennzeichnen e bzw. $\tilde{e}$ den Verzweigungsindex von 3 in der jeweiligen Körpererweiterung und f bzw. $\tilde{f}$ steht für den jeweiligen Trägheitsindex. Die Zahl r bzw. $\tilde{r}$ entspricht der Anzahl der Primfaktoren von 3 in den Körpererweiterungen.) □

3.7.18 Satz. *Sei $p = \frac{1}{4}(L^2 + 27M^2)$. Dann ist 3 ist eine dritte Potenz modulo p genau dann, wenn $M \equiv 0 \pmod 3$ gilt.*

Beweis. Sei $\xi \in \mathbb{Z}[\omega]$ so gewählt, dass $\xi = \frac{1}{2}(r + s\sqrt{-3})$ mit $\mathrm{ggT}(r, 3) = 1$ gilt. Dann ist

$$\xi^3 = \frac{1}{8}(\underbrace{r^3 - 9rs^2}_{=:u} + \underbrace{3s(r^2 - s^2)}_{=:v}\sqrt{(-3)}) = \frac{1}{8}(u + v\sqrt{-3}).$$

Da $\mathrm{ggT}(r, 3) = 1$ gilt, ist $s(r^2 - s^2) = s(r + s)(r - s) \equiv 0 \pmod 3$ und somit $v \equiv 0 \pmod 9$. Weiterhin gilt für ein $\alpha \in \mathbb{Z}[\omega]\backslash\mathfrak{q}$ mit $\alpha \equiv \xi^3 \pmod{3\mathfrak{q}}$ nach obiger Rechnung

$$\alpha \equiv \frac{1}{8}(u + v\sqrt{-3}) \equiv \frac{1}{8}u \pmod{3\mathfrak{q}}.$$

Dabei ist u kein Vielfaches von $\sqrt{-3}$, da $\alpha \notin \mathfrak{q}$. Somit ist dies äquivalent zu $\alpha \equiv a \pmod 9$ für ein $a \in \mathbb{Z}\backslash 3\mathbb{Z}$.
Insgesamt folgt die Äquivalenz

$$\begin{aligned}
3 \text{ ist dritte Potenz modulo } p \quad &\Leftrightarrow \left[\frac{3}{p}\right]_3 = 1 \\
&\overset{3.7.17}{\Leftrightarrow} p\pi = \mu \equiv \xi^3 \pmod{3\mathfrak{q}} \text{ für ein } \xi \in \mathbb{Z}[\omega] \\
&\Leftrightarrow \pi \equiv \xi^3 \pmod{3\mathfrak{q}} \text{ für ein } \xi \in \mathbb{Z}[\omega] \\
&\Leftrightarrow \pi = \frac{1}{2}(L + 3M\sqrt{-3}) \equiv a \pmod 9 \text{ für ein } a \in \mathbb{Z}\backslash 3\mathbb{Z} \\
&\Leftrightarrow M \equiv 0 \pmod 3.
\end{aligned}$$

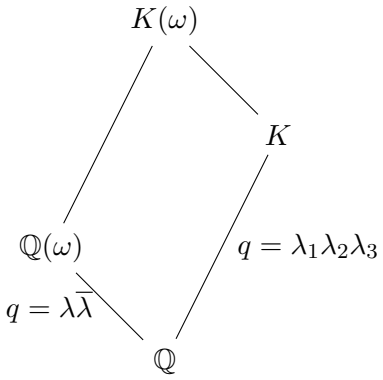
□

Betrachte nun abschließend noch in $\mathbb{Q}(\omega)$ zerlegte Primzahlen $q \equiv 1 \pmod 3$.

3.7.19 Satz. *Sei $q = \lambda\overline{\lambda} \equiv 1 \pmod 3$. Dann gilt*

$$\left[\frac{q}{p}\right]_3 = 1 \Leftrightarrow \overline{\pi}^{\frac{q-1}{3}} \equiv \pi^{\frac{q-1}{3}} \pmod{\lambda}.$$

Beweis.



Es gilt

$$\begin{aligned}
\left[\frac{q}{p}\right]_3 = 1 &\Leftrightarrow q^{\frac{p-1}{3}} \equiv 1 \pmod p \\
&\Leftrightarrow q \text{ ist in } K/\mathbb{Q} \text{ zerlegt} \\
&\Leftrightarrow \lambda \text{ ist in } K(\omega)/\mathbb{Q}(\omega) \text{ zerlegt} \\
&\Leftrightarrow \mu = p\overline{\pi} \equiv \xi^3 \pmod{\lambda} \text{ für ein } \xi \in \mathbb{Z}[\omega] \\
&\Leftrightarrow \mu^{\frac{q-1}{3}} = (\pi^2\overline{\pi})^{\frac{q-1}{3}} \equiv 1 \pmod{\lambda} \\
&\Leftrightarrow \overline{\pi}^{\frac{q-1}{3}} \equiv (\pi^{-2})^{\frac{q-1}{3}} \pmod{\lambda} \\
&\Leftrightarrow \overline{\pi}^{\frac{q-1}{3}} \equiv \pi^{\frac{q-1}{3}} \pmod{\lambda}.
\end{aligned}$$

Dabei wurde im letzten Schritt verwendet, dass $\pi^{\frac{q-1}{3}} \equiv \left(\frac{\pi}{\lambda}\right)_3 \pmod{\lambda}$ eine Potenz von ω modulo λ ist und daher eine dritte Einheitswurzel ist. Damit ist $\left(\pi^{\frac{q-1}{3}}\right)^{-2} \equiv \pi^{\frac{q-1}{3}} \pmod{\lambda}$.
Dabei ist $q = \lambda_1\lambda_2\lambda_3$ (siehe Schaubild) die Primfaktorzerlegung von q in der Körpererweiterung K □

Analog zu dem Fall $q \equiv 2 \pmod 3$ definieren wir die Summe g_q.

3.7.20 Definition. Sei $q \equiv 1 \pmod 3$ eine Primzahl und $n := \frac{q-1}{3}$. Dann definiere die Summe g_q durch $g_q = \sum\limits_{\substack{j=1 \\ j\equiv 1 \pmod 2}}^{n} \binom{n}{j} 3^j (-3)^{\frac{j-1}{2}} L^{n-j} M^j$.

3.7.21 Satz. *Sei $p = \frac{1}{4}(L^2 + 27M^2)$ und $q \equiv 1 \pmod 3$ eine Primzahl. Sei $n = \frac{q-1}{3}$. Dann gilt*

$$\left[\frac{q}{p}\right]_3 = 1 \;\Leftrightarrow\; g_q \equiv 0 \pmod{q}.$$

Beweis. Man erhält analog zu dem Beweis von Satz 3.7.16 die Äquivalenz

$$\left[\frac{q}{p}\right]_3 = 1 \;\Leftrightarrow\; g_q \equiv 0 \pmod{\lambda}$$

für $q = \lambda\overline{\lambda}$. Da auf beiden Seiten der Kongruenz $g_q \equiv 0 \pmod{\lambda}$ ganzzahlige Elemente stehen ist dies äquivalent zu der Kongruenz $g_q \equiv 0 \pmod{q}$. □

Aus den Sätzen 3.7.16 und 3.7.21 folgt:

3.7.22 Satz. *Sei $p = \frac{1}{4}(L^2 + 27M^2)$ und $q > 3$ eine Primzahl. Sei $n = \frac{1}{3}(q - \left(\frac{-3}{q}\right)_2)$. Dann gilt*

$$\left[\frac{q}{p}\right]_3 = 1 \;\Leftrightarrow\; g_q \equiv 0 \pmod{q}.$$

Beweis. Die Behauptung ist genau die Zusammensetzung der beiden Sätze 3.7.16 und 3.7.21, denn ist $q > 3$, so bleibt nur $q \equiv 2 \pmod 3$ und $q \equiv 1 \pmod 3$. Im ersten Fall ist $\left(\frac{-3}{q}\right)_2 = -1$ (siehe auch Beweis von Korollar 3.7.13) und im Letzteren $\left(\frac{-3}{q}\right)_2 = 1$. □

3.7.23 Beispiele. Sei $p = \frac{1}{4}(L^2 + 27M^2)$ und sei $q \neq 3$ eine von p verschiedene Primzahl.

(i) Sei $q = 5 \equiv 2 \pmod 3$, somit ist mit der Notation aus Satz 3.7.22 die Zahl n gegeben durch $n = \frac{q+1}{3} = 2$. Man erhält die Äquivalenz

$$\left[\frac{5}{p}\right]_3 = 1 \;\Leftrightarrow\; g_5 \equiv 0 \pmod 5 \;\Leftrightarrow 3\binom{2}{1} LM \equiv 0 \pmod 5 \;\Leftrightarrow LM \equiv 0 \pmod 5.$$

(ii) Sei nun $q = 11 \equiv 2 \pmod 3$. Dann ist $n = 4$. Mit Satz 3.7.22 folgt:

$$\begin{aligned}\left[\frac{11}{p}\right]_3 = 1 \;\Leftrightarrow\; 0 \equiv g_{11} &= 12L^3M - 4 \cdot 3^4 LM^3 = LM(12L^2 - 4 \cdot 9^2 M^2) \\ &\equiv LM(L - 4M)(L + 4M) \pmod{11}.\end{aligned}$$

Betrachte nun im Folgenden noch Primzahlen $q \equiv 1 \pmod 3$:

(iii) Für $q = 7$ erhalte $n = 2$. Dann gilt:

$$\left[\frac{7}{p}\right]_3 = 1 \Leftrightarrow 0 \equiv g_7 = 6LM \pmod 7 \Leftrightarrow LM \equiv 0 \pmod 7.$$

(iv) Ist $q = 13$, so erhalte für g_{13} zwei Summanden, da $n = 4$ ist. Es gilt:

$$\begin{aligned}\left[\frac{13}{p}\right]_3 = 1 \Leftrightarrow 0 \equiv g_{13} &= LM(12L^2 - 12 \cdot 27M^2) \\ &\equiv LM(M^2 - L^2) = LM(M - L)(M + L) \pmod{13}.\end{aligned}$$

Kapitel 4

Das biquadratische Reziprozitätsgesetz

In diesem Kapitel wird das biquadratische Reziprozitätsgesetz in ähnlicher Weise wie zuvor das Kubische untersucht. Im kubischen Fall haben wir den Ring $\mathbb{Z}[\omega]$ als Erweiterung von $\mathbb{Z}$ betrachtet. Auch für vierte Potenzen, genügt der Ring der ganzen Zahlen nicht. Dies wurde schon in Beispiel 1.0.3 der Einleitung festgestellt. Im Folgenden werden wir nun die Gaußschen Zahlen $\mathbb{Z}[i]$ betrachten. Dies entspricht dem Ganzheitsring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(i)$. Dabei bezeichne i die imaginäre Einheit mit $i^2 = -1$.
Zunächst werden einige wichtige Eigenschaften des Ganzheitsringes $\mathbb{Z}[i]$ aufgeführt, mit dessen Hilfe dann das biquadratische Restsymbol definiert werden kann. Im Anschluss wird dann mit der Theorie der Gauß- und Jacobisummen aus Kapitel 2 das biquadratische Reziprozitätsgesetz und dessen Ergänzungssätzen bewiesen werden.

Analog zu Abschnitt 3.7 gibt es auch beim biquadratischen Reziprozitätsgesetz die Möglichkeit die Untersuchung der biquadratischen Reste durch den Vergleich der Zerlegung von Primzahlen in verschiedenen Körpererweiterungen durchzuführen. Dabei vergleicht man die Zerlegung von Primzahlen in K/k mit der Zerlegung in einem Kreisteilungskörper. Dabei ist der betrachtete Grundkörper $k = \mathbb{Q}(i)$ mit dem Oberkörper $K = k(\sqrt[4]{\pi})$. Schon beim kubischen Reziprozitätsgesetz ist es nicht gelungen, mit dieser Herangehensweise, das kubische Reziprozitätsgesetz vollständig zu beweisen (vgl. Abschnitt 3.7). Dies gelingt auch beim biquadratischen Reziprozitätsgesetz nicht. Das Vorgehen ist ähnlich wie im kubischen Fall. Man muss jedoch noch zusätzlich beachten, dass die Erweiterung $K/\mathbb{Q}$ nicht normal ist und somit nicht abelsch sein kann. Deshalb betrachtet man den maximal abelschen Teilkörper K^{ab} der normalen Hülle N von $K/\mathbb{Q}$. Zur näheren Betrachtung siehe [Lem00, S.186ff].

4.1 Der Ring $\mathbb{Z}[i]$

Im Folgenden betrachten wir den Ganzheitsring $\mathbb{Z}[i]$ des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-1})$. Dabei ist i die imaginäre Einheit mit $i^2 = -1$, insbesondere ist i eine primitive vierte Einheitswurzel. Dieser Abschnitt ist an [IR93, Kap.9, §7] orientiert.

4.1.1 Bemerkung. Zu Beginn einige Eigenschaften des Rings $\mathbb{Z}[i]$, die bei der weiteren Betrachtung benötigt werden und bereits in [ZT14] in einer allgemeineren Form gezeigt wurden.

(a) Genauso wie $\mathbb{Z}[\omega]$ ist auch $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der Normfunktion als Wertefunktion. In $\mathbb{Z}[i]$ ist die Norm durch

$$N\colon \mathbb{Z}[i] \to \mathbb{N}_0, N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2, \quad \text{für ein } \alpha = a + bi \in \mathbb{Z}[i]$$

bestimmt (siehe dazu auch [ZT14, Aufg. 25]).

(b) Die Einheitengruppe von $\mathbb{Z}[i]$ ist endlich und besteht aus allen vierten Einheitswurzeln, d.h. $\mathcal{O}^*_{\mathbb{Q}(i)} = \{\pm 1, \pm i\}$.

Für Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit $d \equiv 2, 3 \pmod 4$, kann man nach [ZT14, Kap.2, 3.10] leicht die Zerlegung von Primzahlen bestimmen. Dazu folgendes Resultat aus der Zahlentheorie.

4.1.2 Satz. *Falls $d \equiv 2, 3 \pmod 4$ zerlegt sich die Primzahl p in $K = \mathbb{Q}(\sqrt{d})$ wie folgt:*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & (p \text{ verzweigt}), \quad \textit{falls } p \mid 2d \\ \mathfrak{p}_1\mathfrak{p}_2 & (p \text{ zerlegt}), \quad \textit{falls } p \nmid 2d \ \textit{ und } \ \left(\frac{d}{p}\right)_2 = +1 \\ \mathfrak{p} & (p \text{ träge}), \quad \textit{falls } p \nmid 2d \ \textit{ und } \ \left(\frac{d}{p}\right)_2 = -1 \end{cases}.$$

Folglich gilt für die Zerlegung von Primzahlen im Zahlkörper $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$.

4.1.3 Bemerkung. Sei $p > 0$ eine Primzahl.

- Die Primzahl $p = 2$ ist verzweigt mit $2 = -i(1+i)^2$. Dabei ist $(1+i)$ ein Primelement von $\mathbb{Z}[i]$ (siehe Satz 4.1.2).
- Ist $p \equiv 3 \pmod 4$, so ist p eine träge Primzahl, d.h. p ist auch prim in $\mathbb{Z}[i]$, denn es gilt $\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}} = -1$.
- Primzahlen $p \equiv 1 \pmod 4$ sind zerlegt, denn $\left(\frac{-1}{p}\right)_2 = 1$. Somit existiert ein Primelement $\pi \in \mathbb{Z}[i]$ mit $p = \pi\overline{\pi}$ und $\pi \not\sim \overline{\pi}$.

Analog zum kubischen Fall definieren wir nun, wann ein Element aus $\mathbb{Z}[i]$ primär heißt. Dabei ist im Folgenden bei Teilbarkeitsrelationen immer die Teilbarkeit in $\mathbb{Z}[i]$ gemeint.

4.1.4 Definition. Eine Nichteinheit $\alpha \in \mathbb{Z}[i]$ heißt *primär*, falls $\alpha \equiv 1 \pmod{(2+2i)}$ gilt.

4.1.5 Bemerkung. In [IR93, 9.7] wird ein primäres Element α durch $\alpha \equiv 1 \pmod{(1+i)^3}$ definiert. Diese Definition ist äquivalent zu der hier eingeführten Definition, die in [Lem00, S. 191] und [Cox89, S. 82] verwendet wird.
Denn: Sei $\alpha \in \mathbb{Z}[i]$ primär im Sinne der hier verwendeten Definition, d.h. $\alpha \equiv 1 \pmod{(2+2i)}$. dann folgt die Existenz eines $\beta \in \mathbb{Z}[i]$, sodass

$$\alpha - 1 = (2+2i)\beta = \underbrace{i(2+2i)}_{=-2+2i=(1+i)^3} \cdot \underbrace{i^3\beta}_{\in\mathbb{Z}[i]}$$

gilt. Dies entspricht der Definition von primär in [IR93]. Die Rückrichtung gilt ebenfalls nach der obigen Umformung.
Es gibt auch noch andere Möglichkeiten primäre Elemente in $\mathbb{Z}[i]$ zu definieren. Eine weitere Definition wird später noch gezeigt. Diese ist jedoch nicht äquivalent zu den bereits genannten Möglichkeiten.

4.1.6 Lemma. [1] *Eine Nichteinheit $\alpha = a + bi$ ist primär genau dann, wenn $a \equiv 1 \pmod 4$ und $b \equiv 0 \pmod 4$ oder $a \equiv 3 \pmod 4$ und $b \equiv 2 \pmod 4$.*

[1] Die Aussage ist aus [IR93, 9.7, Lemma 6] und ist nach der Äquivalenz beider Definitionen, siehe Bemerkung 4.1.5 auch für die hier verwendete Definition gültig.

Beweis. Eine Nichteinheit $\alpha = a + bi \in \mathbb{Z}[i]$ ist genau dann primär, wenn

$$\mathbb{Z}[i] \ni \frac{a+bi-1}{2+2i} = \frac{(a-1+bi)(2-2i)}{8} = \frac{a-1+bi-(a-1)i+b}{4}$$
$$= \frac{a+b-1}{4} + \frac{b-a+1}{4}i$$

gilt. Dies ist äquivalent zu

$$\Leftrightarrow\ a+b \equiv 1 \pmod 4 \text{ und } b-a \equiv -1 \pmod 4.$$

Oder äquivalent dazu, dass $2b \equiv 0 \pmod 4$ und $a + b \equiv 1 \pmod 4$ gilt. Daraus folgt die Äquivalenz der Behauptung. □

4.1.7 Bemerkung.

- Jedes Element $\alpha = a + bi \equiv 1 \pmod 4$ in $\mathbb{Z}[i]$ ist primär. Denn aufgrund der Kongruenz gilt $a \equiv 1 \pmod 4$ und $b \equiv 0 \pmod 4$. Das Resultat folgt also nach Lemma 4.1.6.
- Ist $p \equiv 3 \pmod 4$ eine zerlegte Primzahl, so ist $-p$ primär in $\mathbb{Z}[i]$.

4.1.8 Lemma. *Ist $\alpha \in \mathbb{Z}[i]$ eine Nichteinheit mit $(1+i) \nmid \alpha$. Dann gibt es eine eindeutige Einheit u von $\mathbb{Z}[i]$, sodass $u\alpha$ primär ist.*

Beweis. Sei $\alpha = a + bi \in \mathbb{Z}[i]$ eine Nichteinheit mit $(1+i) \nmid \alpha$. Dann ist entweder a oder b gerade und das jeweils andere Element ist ungerade. Denn wären sowohl a als auch b gerade, so würde $2 \mid \alpha$ gelten. und wegen $2 = -i(1+i)^2$ würde auch $(1+i) \mid \alpha$ folgen. Dies steht im Widerspruch zur Voraussetzung. Wären a und b beide ungerade, etwa $a = 2c+1$ und $b = 2d+1$ für $c, d \in \mathbb{Z}$, so wäre $\alpha = (2c+1) + (2d+1)i = 2(c+di) + (1+i)$. Dies ist erneut widersprüchlich zur Voraussetzung $(1+i) \nmid \alpha$.
Falls a gerade ist, multipliziere mit der Einheit $\tilde{u} = i$, sodass $\tilde{u}\alpha = \tilde{a} + \tilde{b}i$ mit $\tilde{a} = -b$ ungerade und $\tilde{b} = a$ gerade gilt. Falls a bereits ungerade ist, wähle $\tilde{u} = 1$. Falls nötig, multipliziere nun noch mit -1. Denn für eine gerade ganze Zahl $\tilde{b}$ bleibt die Restklasse modulo 4 nach Multiplikation mit -1 erhalten. Jedoch verändert sich die Restklasse von einem ungeraden $\tilde{a}$ modulo 4. Damit erhalte nach Lemma 4.1.6 eine Einheit $u = \pm\tilde{u}$, sodass $u\alpha$ primär ist.
Zeige nun noch die Eindeutigkeit einer solchen Einheit. Seien dazu u_1 und u_2 Einheiten, sodass $u_1\alpha \equiv u_1\alpha \equiv 1 \pmod{(2+2i)}$ gilt. Nach Voraussetzung ist α nicht durch $(1+i)$ teilbar, also insbesondere $\alpha \not\equiv 0 \pmod{(2+2i)}$. Es folgt $u_1 \equiv u_2 \pmod{(2+2i)}$. Wären die Einheiten verschiedenen, so hätten sie auch verschiedene Restklassen modulo $(2+2i)$, denn aus $1 \equiv -i \pmod{(2+2i)}$ folgt die Existenz von $a, b \in \mathbb{Z}$ mit $1 + i = (2+2i)(a+bi) = 2(a-b) + 2(a+b)i$. Dann müsste schon $2a - 2b = 1$ und $2a + 2b = 1$ gelten. Dies bedeutet $4a = 1$. Dies ist ein Widerspruch, da ein solches a nicht in $\mathbb{Z}$ liegen kann. Die anderen Fälle führen analog zu einem Widerspruch. Folglich gilt $u_1 = u_2$. □

4.1.9 Satz. *Jedes primäre Element kann als Produkt von primären Primelementen geschrieben werden.*

Beweis. Sei $\alpha \in \mathbb{Z}[i]$ primär. Da $\mathbb{Z}[i]$ ein faktorieller Ring ist, existiert eine Primfaktorzerlegung $\alpha = u\pi_1 \cdot \ldots \cdot \pi_s q_1 \cdot \ldots \cdot q_r$ mit einer Einheit u, komplexen Primelementen π_i mit $N(\pi_i) \equiv 1$

(mod 4) für $i = 1, \dots s$ und ganzzahlige zerlegte Primzahlen $q_j \equiv 3 \pmod 4$ für $j = 1, \dots r$. Das Primelement $1 + i$ ist nicht in der Primfaktorzerlegung enthalten, denn für ein Element $\alpha = a + bi \in \mathbb{Z}[i]$, ist $(1 + i)\alpha = (a - b) + (a + b)i$ nicht primär.
Nach Bemerkung 4.1.7 ist $-q_j$ für $j = 1, \dots, r$ primär und nach Lemma 4.1.8 existiert zu jedem π_i $(i = 1, \dots, s)$ eine eindeutige Einheit u_i, sodass $u_i\pi_i$ primär ist. Wir erhalten somit für eine Einheit $\tilde{u}$ die Gleichung $\alpha = \tilde{u}u_1\pi_1 \cdots u_s\pi_s(-q_1) \cdots (-q_r)$, welche durch Betrachtung modulo $(2 + 2i)$ die Kongruenz

$$1 \equiv \alpha = \tilde{u}u_1\pi_1 \cdots u_s\pi_s(-q_1) \cdots (-q_r) \equiv \tilde{u} \pmod{(2 + 2i)}$$

zur Folge hat. Mit demselben Argument wie im Beweis von Lemma 4.1.8 folgt $\tilde{u} = 1$. Folglich ist α Produkt von primären Primelementen. □

Analog zum kubischen Fall erhalten wir nun für den Restklassenkörper $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ eine Aussage über die Anzahl der Elemente. Die zwei folgenden Aussagen dieses Abschnittes sind in [IR93, Prop.9.8.1 & Kor] zu finden.

4.1.10 Satz. *Sei $\pi \in \mathbb{Z}[i]$ prim, dann ist $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ ein endlicher Körper mit $N(\pi)$ Elementen.*

Beweis. Folgt direkt aus der Idealnorm (siehe [ZT14, Kap.2, 4.1]). □

Als direkte Folgerung erhalte nun eine Aussage, analog zum kleinen Satz von Fermat.

4.1.11 Korollar. *Für $\pi \in \mathbb{Z}[i]$ prim ist die Einheitengruppe $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ zyklisch von Ordnung $N(\pi) - 1$ und für ein $\alpha \in \mathbb{Z}[i]$ beliebig mit $\pi \nmid \alpha$ gilt*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

4.2 Das biquadratische Restsymbol

Mit den in Kenntnissen aus dem vorhergehenden Abschnitt, können wir nun das biquadratische Restsymbol definieren. Dabei gehen wir ähnlich wie bei der Definition des kubischen Restsymbols vor und orientieren uns an [IR93, Kap.9, §8].

4.2.1 Satz. *Sei $\pi \in \mathbb{Z}[i]$ mit $\pi \not\sim (1 + i)$ (oder äquivalent: $N(\pi) \neq 2$) und $\alpha \in \mathbb{Z}[i]$ mit $\pi \nmid \alpha$. Dann existiert ein eindeutiges $m \in \{0, 1, 2, 3\}$, sodass*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv i^m \pmod \pi$$

gilt.

Beweis. Da $\langle i \rangle = \{\pm i, \pm 1\}$ eine Untergruppe der Einheitengruppe $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ ist, enthält $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ ein Element der Ordnung 4. Folglich ist $\frac{N(\pi)-1}{4} \in \mathbb{N}$.
Die Restklassen der Einheiten $+1, -1, +i, -i$ sind modulo π paarweise verschieden, denn wäre $1 \equiv -i \pmod \pi$, so würde $\pi \mid (1 + i)$ folgen, was im Widerspruch zur Voraussetzung $\pi \not\sim (1 + i)$ steht. Die anderen Fälle folgen analog. Somit ist die Eindeutigkeit gezeigt, falls ein solches m existiert.
Die vierten Einheitswurzeln $+1, -1, +i, -i$ sind paarweise verschiedene Lösungen der Gleichung $x^4 \equiv 1 \pmod \pi$. Nach Korollar 4.1.11 ist auch $\alpha^{\frac{N(\pi)-1}{4}}$ eine Lösung. Da es maximal vier Lösungen der Gleichung gibt, gilt $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^m \pmod \pi$ für ein $m \in \{0, 1, 2, 3\}$. □

Ebenso, wie bei der Definition des kubischen Restsymbols, können wir obige Eigenschaft nutzen, um das biquadratische Restsymbol zu definieren.

4.2.2 Definition. Sei $\pi \in \mathbb{Z}[i]$ prim mit $N(\pi) \neq 2$, so definiere für $\alpha \in \mathbb{Z}[i]$ das *biquadratische Restsymbol* durch

$$\left(\frac{\alpha}{\pi}\right)_4 := \begin{cases} 0, & \text{falls } \pi \mid \alpha \\ i^m, \text{ sodass } i^m \equiv \alpha^{\frac{N(\pi)-1}{4}} \pmod{\pi}, & \text{falls } \pi \nmid \alpha \end{cases}.$$

4.2.3 Bemerkung. Für ein Primelement $\pi \in \mathbb{Z}[i]$ mit $N(\pi) = p$ für eine Primzahl $p > 2$ ist das biquadratische Restsymbol $\left(\frac{\cdot}{\pi}\right)_4$ ein Charakter auf $\mathbb{F}_p$ mit Ordnung 4 , im Folgenden auch *biquadratischer Charakter* genannt.
Der biquadratische Charakter ist nicht trivial. Angenommen er wäre trivial, so ist jedes Element des endlichen Körpers $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ mit $N(\pi) = p$ ein Biquadrat, also die Abbildung

$$\mathbb{Z}[i]/\pi\mathbb{Z}[i] \to \mathbb{Z}[i]/\pi\mathbb{Z}[i], x \mapsto x^4 \tag{4.1}$$

surjektiv. Aufgrund der Endlichkeit des Körpers $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ müsste die Abbildung (4.1) auch injektiv sein. Dies ist nicht der Fall, denn für ein $x \neq 0$ in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ ist $x \neq ix$ (in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$), aber beide Elemente x und ix werden durch die Abbildung (4.1) auf x abgebildet.
Weiterhin kann die Ordnung des biquadratischen Charakters nicht 2 sein, denn dann wären alle Elemente von $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ Quadrate und wegen der Isomorphie $\mathbb{Z}[i]/\pi\mathbb{Z}[i] \cong \mathbb{Z}/p\mathbb{Z}$ wären auch alle Elemente von $\mathbb{Z}/p\mathbb{Z}$ Quadrate. Dies ist nicht der Fall, denn $(\mathbb{Z}/p\mathbb{Z})^*$ besteht zur Hälfte aus Quadraten und zur anderen Hälfte aus Nichtquadraten. Weiterhin ist $\chi_\pi^4 = \epsilon$. Folglich hat der biquadratische Charakter, wie behauptet, Ordnung 4.

Im Folgenden sei ein Primelement $\pi \in \mathbb{Z}[i]$ stets mit $N(\pi) \neq 2$, falls es nicht anders vorausgesetzt wird.

4.2.4 Satz (Eigenschaften)**.** *Seien $\pi, \alpha, \beta \in \mathbb{Z}[i]$ und π ein Primelement (mit $N(\pi) \neq 2$). Dann gilt:*

(a) $\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N(\pi)-1}{4}} \pmod{\pi}$

(b) $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$

(c) $\alpha \equiv \beta \pmod{\pi} \Rightarrow \left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$

(d) $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\pi'}\right)_4$, *falls* $\pi \sim \pi'$

(e) $\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4$

Beweis. Der Beweis der hier aufgeführten Eigenschaften folgt direkt aus der Definition des biquadratischen Restsymbols analog zum kubischen Fall (siehe Beweis von 3.2.5). □

Man kann nun auch einfach bestimmen, wann -1 ein Biquadrat modulo π für ein primäres Primelement π ist. Der nächste Satz ist aus [IR93, Aufg. 38].

4.2.5 Satz. *Für ein primäres Primelement $\pi = a + bi \in \mathbb{Z}[i]$ gilt*

$$\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{1-a}{2}}.$$

Beweis. Nach Definition des biquadratischen Restsymbols und Eigenschaft (a) von Satz 4.2.4 erhalte

$$\left(\frac{-1}{\pi}\right)_4 \equiv (-1)^{\frac{a^2+b^2-1}{4}} \pmod{\pi}.$$

Nach Lemma 4.1.6 gibt es zwei mögliche Fälle für das primäre Element π:

- Ist $a \equiv 1 \pmod 4$ und $b \equiv 0 \pmod 4$, so ist $a^2 + b^2 \equiv 1 \pmod 8$ und somit $\frac{a^2+b^2-1}{4} \equiv 0 \pmod 2$. Ebenso gilt $\frac{1-a}{2} \equiv 0 \pmod 2$.
- Gilt andererseits $a \equiv 3 \pmod 4$ und $b \equiv 2 \pmod 4$, so ist $0 \equiv (a-3)^2 + (b-2)^2 \equiv a^2 + b^2 + 2a - 4b - 3 \pmod 8$ und somit

$$\frac{a^2+b^2-1}{4} \equiv \frac{-2a+4b+2}{4} = b + \frac{1-a}{2} \equiv \frac{1-a}{2} \pmod 2.$$

Es wurde nun gezeigt, dass $\frac{a^2+b^2-1}{4} \equiv \frac{1-a}{2} \pmod 2$ gilt. □

4.2.6 Satz. *Für $\alpha \in \mathbb{Z}[i]$ und ein Primelement $\pi \in \mathbb{Z}[i]$ teilerfremd zu α gilt die Äquivalenz:*

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \;\Leftrightarrow\; x^4 \equiv \alpha \pmod{\pi} \text{ hat eine Lösung in } \mathbb{Z}[i].$$

Beweis. Die Aussage ist ein Spezialfall von Satz 3.2.7 mit $F = \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, $q = N(\pi)$, $n = 4$ und somit $d = \mathrm{ggT}(n, q-1) = 4$. □

4.2.7 Bemerkung. Das biquadratische Restsymbol teilt die zyklische Gruppe $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ für ein Primelement π aus $\mathbb{Z}[i]$ in vier gleich große Teile auf. Ein Viertel dieser Menge besteht aus den biquadratischen Reste modulo π. Ein biquadratischer Rest ist offensichtlich auch ein quadratischer Rest. Jedoch ist nicht jeder quadratische Rest auch ein biquadratischer Rest. Somit besteht ein weiteres Viertel aus quadratischen Resten, die keine biquadratischen Reste sind. Insgesamt ist die Hälfte von $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ quadratische Reste. Die andere Hälfte besteht aus quadratischen Nichtresten. Dies sind auch biquadratische Nichtreste.
Wir haben insgesamt drei verschiedene Arten von biquadratischen Nichtresten. Die Nichtreste, die quadratischen Rest sind (das Restsymbol nimmt den Wert -1 an) und die Nichtreste, bei denen das biquadratische Restsymbol den Wert i bzw. $-i$ hat.

Das biquadratische Restsymbol lässt sich auf beliebige Elemente wie folgt verallgemeinern:

4.2.8 Definition. Sei $\gamma \in \mathbb{Z}[i]$ eine Nichteinheit mit $(1+i) \nmid \gamma$ und $\beta \in \mathbb{Z}[i]$. Sei $\gamma = \prod_{i=1}^{s} \lambda_i$ eine Primfaktorzerlegung von γ. Dann wird das allgemeine biquadratische Restsymbol $\left(\frac{\beta}{\gamma}\right)_4$ definiert durch:

$$\left(\frac{\beta}{\gamma}\right)_4 := \prod_{i=1}^{s} \left(\frac{\beta}{\lambda_i}\right)_4.$$

Dies ist nach Eigenschaft (d) von Satz 4.2.4 wohldefiniert. Falls $\mathrm{ggT}(\beta, \gamma) \neq 1$ gilt, so ist $\left(\frac{\beta}{\gamma}\right)_4 = 0$, da einer der Faktoren nach der Definition des biquadratischen Restsymbols 4.2.2 verschwindet.

4.2.9 Satz. *Seien $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ mit $(1+i) \nmid \gamma$. Dann gilt:*

(a) $\left(\frac{\alpha\beta}{\gamma}\right)_4 = \left(\frac{\alpha}{\gamma}\right)_4 \left(\frac{\beta}{\gamma}\right)_4$

(b) $\alpha \equiv \beta \pmod{\gamma} \Rightarrow \left(\frac{\alpha}{\gamma}\right)_4 = \left(\frac{\beta}{\gamma}\right)_4$

(c) $\overline{\left(\frac{\alpha}{\gamma}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\gamma}}\right)_4$

Beweis. Die Eigenschaften folgen direkt aus den Eigenschaften des biquadratischen Restsymbols 4.2.4 und der Definition des verallgemeinerten biquadratischen Restsymbols. □

4.3 Die biquadratischen Gauß- und Jacobi-Summen

Für den Beweis des biquadratischen Reziprozitätsgesetzes benötigen wir Gauß- und Jacobi-Summen eines biquadratischen Charakters. Für ein primäres Primelement π mit $N(\pi) = p \equiv 1 \pmod 4$ ist das biquadratische Restsymbol $\left(\frac{\cdot}{\pi}\right)_4$ ein Charakter auf $\mathbb{Z}[i]/\pi\mathbb{Z}[i] \cong \mathbb{Z}/p\mathbb{Z}$ von Ordnung 4 (siehe Bemerkung 4.2.3). Setze dazu zur Vereinfachung im Folgenden $\chi_\pi := \left(\frac{\cdot}{\pi}\right)_4$. In diesem Abschnitt, der sich an [IR93, 9.9.1-9.9.5] orientiert, werden die Gauß- und Jacobi-Summe dieses biquadratischen Charakters berechnet.

4.3.1 Satz. *Sei $\pi \in \mathbb{Z}[i]$ prim und primär mit $N(\pi) = p \equiv 1 \pmod 4$, so gilt:*

$$J(\chi_\pi, \chi_\pi) = \chi_\pi(-1) J(\chi_\pi, \chi_\pi^2).$$

Beweis. Fixiere $\pi \in \mathbb{Z}[i]$ und setze $\chi := \chi_\pi$ und $\psi := \chi_\pi^2$. Dann ist ψ ein nichttrivialer Charakter von Ordnung 2, entspricht also dem Legendre-Symbol und es gilt nach Satz 2.3.2 (d)

$$J(\chi, \chi) = \frac{G(\chi)^2}{G(\chi^2)} = \frac{G(\chi)^2}{G(\psi)} \neq 0.$$

Für die Gauß-Summe von ψ gilt nach Satz 2.3.7 $G(\psi)^2 = \psi(-1)p = p$, denn nach Voraussetzung ist $p \equiv 1 \pmod 4$ eine ungerade Primzahl. Daraus folgt $\psi(-1) = (-1)^{\frac{p-1}{2}} = 1$. Somit erhalte insgesamt durch Anwendung von Satz 2.3.6 auf den Charakter χ:

$$J(\chi,\chi)^2 = \frac{G(\chi)^4}{G(\psi)^2} \overset{2.3.6}{=} \frac{1}{G(\psi)^2}\chi(-1)pJ(\chi,\chi)J(\chi,\psi) = \chi(-1)J(\chi,\chi)J(\chi,\psi).$$

Die Behauptung folgt durch Division der obigen Gleichung durch $J(\chi,\chi) \neq 0$. □

4.3.2 Satz. *Für $\pi \in \mathbb{Z}[i]$ prim und primär mit $p = N(\pi)$ eine zerlegte Primzahl. Dann ist $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)$ primär.*

Beweis. Betrachte zu dem Charakter $\chi := \chi_\pi$ die Jacobi-Summe $J(\chi,\chi)$. Da nach Voraussetzung $p \equiv 1 \pmod 4$ gilt, ist insbesondere $p \neq 2$. Somit folgt:

$$\begin{aligned} J(\chi,\chi) &= \sum_{t\in\mathbb{F}_p} \chi(t)\chi(1-t) \\ &= \underbrace{\chi(0)}_{=0}\chi(1) + \chi(1)\underbrace{\chi(0)}_{=0} + \sum_{t=2}^{\frac{p-1}{2}} \chi(t)\chi(1-t) + \chi\left(\frac{p+1}{2}\right)^2 + \sum_{t=\frac{p+3}{2}}^{p-1} \chi(t)\chi(1-t) \\ &= 2\sum_{t=2}^{\frac{p-1}{2}} \chi(t)\chi(1-t) + \chi\left(\frac{p+1}{2}\right)^2. \end{aligned} \tag{4.2}$$

Im letzten Schritt wurde dabei die Summationsreihenfolge der zweiten Summe verändert. Weiterhin gilt mit $2 = -i(1+i)^2$:

$$\chi\left(\frac{p+1}{2}\right)^2 = \chi\left(\frac{1}{2}\right)^2 = \chi(2)^{-2} = \chi(2)^2 = \chi(-i)^2\chi(i+1)^4 = \chi(-1).$$

Außerdem ist jede Einheit von $\mathbb{Z}[i]$ in derselben Restklasse wie 1 modulo $(1+i)$ und es gilt $p \equiv 1 \pmod{(2+2i)}$. Somit folgt bei Betrachtung der Summe aus (4.2) modulo $(2+2i)$:

$$2\sum_{t=2}^{\frac{p-1}{2}} \chi(t)\chi(1-t) \equiv 2\sum_{t=2}^{\frac{p-1}{2}} 1 = \frac{2(p-3)}{2} \equiv -2 \pmod{(2+2i)}.$$

Insgesamt ergibt sich nun für die Jacobi-Summe

$$J(\chi,\chi) = 2\sum_{t=2}^{\frac{p-1}{2}} \chi(t)\chi(1-t) + \chi(-1) \equiv -2 + \chi(-1) \pmod{(2+2i)}.$$

Durch Multiplikation mit $-\chi(-1)$ folgt

$$-\chi(-1)J(\chi,\chi) \equiv 2\chi(-1) - \underbrace{\chi(-1)^2}_{=\chi(1)=1} \equiv 1 \pmod{(2+2i)}.$$

Der letzte Schritt gilt, da $\chi(-1)$ nach Definition eine Einheit in $\mathbb{Z}[i]$ ist und damit $2\chi(-1) \equiv 2 \pmod{(2+2i)}$ gilt.
Aus der letzten Gleichung folgt nun, dass $-\chi(-1)J(\chi,\chi)$ primär ist. □

4.3.3 Korollar. *Sei $\pi \in \mathbb{Z}[i]$ ein primäres Primelement mit $N(\pi) = p \equiv 1 \pmod 4$. Dann gilt $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = \pi$.*

Beweis. Es genügt zu zeigen, dass $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod \pi$ gilt. Dann folgt die Behauptung, da $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ nach Satz 4.3.2 primär ist und $N(J(\chi_\pi, \chi_\pi)) = J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = p$ gilt. Mit der Eindeutigkeit des primären Elements unter den Assoziierten folgt dann bereits die behauptete Gleichheit.
Wir argumentieren wie in dem Beweis zu Satz 3.3.2 und erhalten mit gleichem Argument

$$J(\chi_\pi, \chi_\pi) = \sum_{x \in \mathbb{F}_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x \in \mathbb{F}_p} x^{\frac{p-1}{4}}(1-x)^{\frac{p-1}{4}} \equiv 0 \pmod \pi.$$

Dabei wurde verwendet, dass $x^{\frac{p-1}{4}}(1-x)^{\frac{p-1}{4}}$ ein Polynom von Grad $\frac{p-1}{2} < p-1$ ist. □

Mit Hilfe dieses Korollars, können wir nun auch etwas über die Gauß-Summe eines biquadratischen Charakters aussagen.

4.3.4 Korollar. *Wir erhalten nun insgesamt für jedes primäre Primelement $\pi \in \mathbb{Z}[i]$:*

$$G(\chi_\pi)^4 = \pi^3\overline{\pi}.$$

Beweis. Aus Satz 2.3.6 folgt

$$\begin{aligned} G(\chi_\pi)^4 &= \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, \chi_\pi^2) \\ &\overset{4.3.1}{=} \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)\chi_\pi(-1)^{-1}J(\chi_\pi, \chi_\pi) \\ &= \pi\overline{\pi} \cdot \pi^2 \\ &= \pi^3\overline{\pi}. \end{aligned}$$

Dabei wurde im letzten Schritt das Ergebnis aus dem vorhergehenden Korollar verwendet, denn $J(\chi_\pi, \chi_\pi)^2 = \underbrace{(-1)^2\chi_\pi(-1)^2}_{=1} J(\chi_\pi, \chi_\pi)^2 = \pi^2$. □

Gauß entdeckte eine einfache Folgerung bezüglich der $\mathbb{Q}(i)/\mathbb{Q}$-Spur von π. Die Spur $\mathrm{tr}_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) = \pi + \overline{\pi} = 2a$ ist durch einen Binominialkoeffizienten bestimmt (siehe [Lem00, Kor. 6.6]).

4.3.5 Korollar (Gauß' Kongruenz)**.** *Sei $p = a^2 + b^2 = 4m+1$ eine Primzahl und $\pi := a + bi \equiv 1 \pmod{(2+2i)}$ (d.h. π primär). Dann gilt*

$$2a \equiv (-1)^m \binom{2m}{m} \pmod p.$$

Beweis. Setze $\chi := \chi_\pi$. Wenn π primär ist, dann ist auch $\overline{\pi}$ primär, denn nach Voraussetzung gilt $p \equiv 1 \pmod 4$. Da $(2+2i) \mid 4$ gilt, folgt $1 \equiv p = \pi\overline{\pi} \equiv \overline{\pi} \pmod{(2+2i)}$. Weiterhin ist $\chi_\pi(-1) = \chi_{\overline{\pi}}(-1)$ und

$$J(\chi^3, \chi^3) = J(\overline{\chi_\pi}, \overline{\chi_\pi}) = \sum_{t \in \mathbb{F}_p} \overline{\chi_\pi(t)\chi_\pi(1-t)} = \sum_{t \in \mathbb{F}_p} \chi_{\overline{\pi}}(t)\chi_{\overline{\pi}}(1-t) = J(\chi_{\overline{\pi}}, \chi_{\overline{\pi}}).$$

Folglich gilt

$$\begin{aligned} J(\chi^3,\chi^2) &= J(\chi^{-1},(\chi^{-1})^2) \\ &\overset{4.3.1}{=} \chi(-1)^{-1}J(\chi^{-1},\chi^{-1}) \\ &= \chi(-1)J(\chi^3,\chi^3) \\ &= \chi_{\overline{\pi}}(-1)J(\chi_{\overline{\pi}},\chi_{\overline{\pi}}) \\ &\overset{4.3.3}{=} -\overline{\pi}. \end{aligned}$$

Für beliebiges $t \in \mathbb{F}_p$ ist nach Definition des biquadratischen Charakters $\chi(t) \equiv t^{\frac{p-1}{4}} = t^m \pmod{\pi}$. Somit folgt

$$\begin{aligned} J(\chi^3,\chi^2) &= \sum_{t=0}^{p-1}\chi(t)^3\chi(1-t)^2 \equiv \sum_{t=0}^{p-1}t^{3m}(1-t)^{2m} = \sum_{t=0}^{p-1}t^{3m}(t-1)^{2m} \\ &= \sum_{t=0}^{p-1}t^{3m}\sum_{j=0}^{2m}\binom{2m}{j}(-1)^j t^{2m-j} \\ &= \sum_{j=0}^{2m}(-1)^j\binom{2m}{j}\sum_{t=0}^{p-1}t^{5m-j} \qquad \pmod{\pi}. \end{aligned}$$

Die innere Summe $\sum\limits_{t=0}^{p-1} t^{5m-j}$ verschwindet für $j \neq m$ und für $j = m$ gilt

$$\sum_{t=0}^{p-1}t^{5m-m} = \sum_{t=0}^{p-1}t^{p-1} \equiv p-1 \equiv -1 \pmod{p}.$$

Somit ist

$$J(\chi^3,\chi^2) \equiv (-1)^{m+1}\binom{2m}{m} \pmod{\pi}.$$

Damit folgt

$$2a = \pi + \overline{\pi} \equiv \overline{\pi} \equiv -J(\chi^3,\chi^2) \equiv (-1)^{m+2}\binom{2m}{m} = (-1)^m\binom{2m}{m} \pmod{\pi}.$$

Da auf beiden Seiten der Kongruenz ganzzahlige Elemente stehen, gilt dann auch

$$2a \equiv (-1)^m\binom{2m}{m} \pmod{p}.$$

□

4.3.6 Bemerkung. [2] In [Lem00, Kap. 6.2] werden Gauß- und Jacobi-Summe für biquadratische

[2] siehe [Lem00, S. 193]

Charaktere χ mit anderem Vorzeichen definiert, also

$$G'(\chi^r) = -\sum_{t=1}^{p-1} \chi(t)^r \zeta^t, \quad \text{anstelle von } G(\chi^r) = \sum_{t=1}^{p-1} \chi(t)^r \zeta^t \tag{4.3}$$

und $$J'(\chi, \chi^r) = -\sum_{t=1}^{p-1} \chi(t)\chi(1-t)^r, \quad \text{anstelle von } J(\chi,\chi) = \sum_{t=1}^{p-1} \chi(t)\chi(1-t)^r. \tag{4.4}$$

Mit dieser Definition erhält man eine etwas schönere Aussage bezüglich des Jacobi-Summe, denn somit fällt in Korollar 4.3.3 das negative Vorzeichen weg, d.h. man erhält $\chi(-1)J'(\chi_\pi, \chi_\pi) = \pi$. Der zusätzliche, etwas unschöne, Faktor $\chi(-1)$ bleibt auch mit der Definition aus (4.3) erhalten. Würde man Kummers Rat folgen, der sagte, dass Jacobi-Summen primär sein müssen, so dürfte man keinen solchen Faktor haben. Tatsächlich kann man dies erreichen, falls man zusätzlich zu dem Vorzeichen in der Jacobi-Summe noch eine andere Definition für primär wählt, hier im Folgenden *J-primär* genannt.
Eine Nichteinheit $\pi = a + bi$ heißt *J-primäre*, falls $a \equiv 1 \pmod 4$ gilt.
Mit dieser Definition folgt, dass $J'(\chi_\pi, \chi_\pi) = \pi$ für ein J-primäres Primelement $\pi = a + bi$ gilt. Dies sieht man wie folgt:
Da $\pi = a + bi$ nach Voraussetzung J-primär ist, gilt $a \equiv 1 \pmod 4$. Dann ist b gerade. Wir unterscheiden zwei Fälle:

(a) Ist $b \equiv 0 \pmod 4$, so ist π auch primär und es gilt

$$J'(\chi_\pi, \chi_\pi) = \chi_\pi(-1)\pi = \left(\frac{-1}{\pi}\right)_4 \pi \overset{4.2.5}{=} (-1)^{\frac{1-a}{2}}\pi = \pi.$$

(b) Ist andernfalls $b \equiv 2 \pmod 4$, so ist $-\pi$ primär. Außerdem gilt $\chi_\pi = \chi_{-\pi}$ nach Satz 4.2.4(d). Folglich gilt

$$J'(\chi_\pi, \chi_\pi) = J'(\chi_{-\pi}, \chi_{-\pi}) = -\chi_{-\pi}(-1)(-\pi) = -(-1)^{\frac{1+a}{2}}\pi = \pi.$$

Mit der Voraussetzung, dass $\pi = a + bi$ J-primär (anstelle von primär) ist, verändert sich auch die Aussage von Korollar 4.3.5 zu: $2a \equiv \binom{2m}{m} \pmod p$.
Denn: Mit analoger Rechnung wie im Beweis von 4.3.5 gilt

$$J'(\chi^3, \chi^2) = \chi_\pi(-1)\overline{\pi}.$$

Damit folgt

$$2a \equiv \overline{\pi} \equiv \chi(-1)(-1)^m \binom{2m}{m} = (-1)^{\frac{p-1}{4}}(-1)^m \binom{2m}{m} = (-1)^{2m}\binom{2m}{m} = \binom{2m}{m} \pmod \pi.$$

Da beide Seiten ganzzahlig sind, gilt die Kongruenz auch bezüglich p.

4.4 Das biquadratische Reziprozitätsgesetz und die Ergänzungssätze

Nun sind alle Vorbereitungen getroffen um das biquadratische Reziprozitätsgesetz zu formulieren und zu beweisen. Das biquadratische Reziprozitätsgesetz wird in zwei äquivalenten Versionen

vorkommen. Die klassische Formulierung von Gauß und Eisenstein ist analog zu den bereits bekannten quadratischen und kubischen Reziprozitätsgesetzen. Die zweite Version stammt von Jacobi und Kaplan. Im Gegensatz zu dem Vorgehen in Kapitel 3 wird das biquadratische Reziprozitätsgesetz mit Hilfe von Eisensteins Reziprozitätsgesetz in der biquadratischen Variante bewiesen. Mit diesem Spezialfall wird im Anschluss das allgemeine biquadratische Reziprozitätsgesetz gezeigt. Dieser Abschnitt richtet sich nach [Lem00, 6.3].

4.4.1 Theorem (Biquadratisches Reziprozitätsgesetz, Gauß und Eisenstein)**.** *Seien $\pi = a + bi$, $\lambda = c + di$ zwei teilerfremde primäre Primelemente in $\mathbb{Z}[i]$. Dann gilt:*

$$\left(\frac{\lambda}{\pi}\right)_4 \left(\frac{\pi}{\lambda}\right)_4^{-1} = (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\pi)-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}.$$

Wir werden zuerst die letzten Gleichheiten zeigen. Damit erhalten wir verschiedene Möglichkeiten zur Berechnung des Vorzeichens.

4.4.2 Lemma. *Für primäre, teilerfremde Elemente $\pi = a + bi$ und $\lambda = c + di$, wie in den Voraussetzungen für das biquadratische Reziprozitätsgesetz von Gauß und Eisenstein, gilt:*

$$(-1)^{\frac{a^2+b^2-1}{4}\frac{c^2+d^2-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}.$$

Beweis. Für die erste Gleichheit reicht es zu zeigen, dass $\frac{a-1}{2} \equiv \frac{a^2+b^2-1}{4} \pmod 2$ gilt. Dies wurde bereits in dem Beweis von 4.2.5 gezeigt.
Analog folgt dann auch: $\frac{c-1}{2} \equiv \frac{c^2+d^2-1}{4} \pmod 2$.
Für die zweite Gleichheit genügt es die Kongruenz $\frac{a^2+b^2-1}{4} \equiv \frac{b}{2} \pmod 2$ zu zeigen. Diese gilt, denn $\frac{a^2+b^2-1}{4} = \frac{(a+1)(a-1)}{4} + \frac{b^2}{4}$. Da $\pi = a+bi$ primär ist, ist a ungerade und somit ist $(a+1)(a-1)$ durch 8 teilbar. Der erste Bruch ist somit irrelevant für die Kongruenz modulo 2. Weiterhin gilt $\frac{b^2}{4} \equiv \frac{b}{2} \pmod 2$ für eine gerade ganze Zahl b. Denn für $b \equiv 0 \pmod 4$ ist die Aussage trivial. Ist $b \equiv 2 \pmod 4$, so ist $\frac{b}{2} \equiv 1 \pmod 2$ und $0 \equiv (b-2)^2 = b^2 - 4b + 4 \pmod{16}$. Es folgt $\frac{b^2}{4} \equiv b - 1 \equiv 1 \pmod 2$. □

Eine andere Formulierung des biquadratischen Reziprozitätsgesetzes stammt von Jacobi und Kaplan:

4.4.3 Theorem (Biquadratisches Reziprozitätsgesetz, Jacobi und Kaplan)**.** *Seien $\alpha = a + bi$ und $\beta = c + di$ aus $\mathbb{Z}[i]$ teilerfremd und so gewählt, dass $a \equiv c \equiv 1 \pmod 4$ gilt, dann ist*

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

4.4.4 Bemerkung. Wie später gezeigt wird, sind die beiden Versionen des biquadratischen Reziprozitätsgesetzes (Theorem 4.4.1 und 4.4.3) äquivalent.

Im Folgenden Beweis wird ein Spezialfall von Satz 3.7.12 benötigt.

4.4.5 Korollar. *Für $\pi = a + bi \in \mathbb{Z}[i]$ und eine Primzahl $p \equiv 3 \pmod 4$ gilt $\pi^p \equiv \overline{\pi} \pmod p$.*

Beweis. Folgt direkt aus Lemma 3.7.12, denn für $K = \mathbb{Q}(i)$ ist $d_K = -4$ und
$\left(\frac{-4}{p}\right)_2 = \left(\frac{-1}{p}\right)_2 \left(\frac{2}{p}\right)_2^2 = (-1)^{\frac{p-1}{2}} = -1$. □

Aus der Primfaktorzerlegung der Gauß-Summe von Korollar 4.3.4 erhalten wir einen Spezialfall des biquadratischen Reziprozitätsgesetz, das Reziprozitätsgesetz von Eisenstein für vierte Potenzen.

4.4.6 Theorem (Eisensteins biquadratisches Reziprozitätsgesetz)**.** *Seien $\alpha \in \mathbb{Z}[i]$ und $a \in \mathbb{Z}$ teilerfremd und primär. Dann gilt*

$$\left(\frac{\alpha}{a}\right)_4 = \left(\frac{a}{\alpha}\right)_4.$$

Beweis. Nach Voraussetzung sind sowohl α als auch a primär, d.h. $\alpha \equiv 1 \pmod{(2+2i)}$ und nach Satz 4.1.6 gilt $a \equiv 1 \pmod 4$.
Sei $\alpha = (-q_1)\cdots(-q_s)\lambda_1\cdots\lambda_r$ die primäre Primfaktorzerlegung von α mit trägen Primzahlen $q_j \equiv 3 \pmod 4$ $(j = 1,\ldots,s)$ und echt-komplexen primären Primelementen $\lambda_k \neq 1+i$, $k = 1,\ldots,r$. Weiterhin sei $a = (-p_1)\cdots(-p_n)p_{n+1}\cdots p_m$ die Primfaktorzerlegung von $a \in \mathbb{Z}$ mit ungeraden Primzahlen $p_l \equiv 3 \pmod 4$ für $l = 1,\ldots,n$ und $p_l \equiv 1 \pmod 4$ für $l = n+1,\ldots m$. Wegen der Multiplikativität des biquadratischen Restsymbols und der verallgemeinerten Definition genügt es für ungerade Primzahlen p (d.h. $p \equiv 1 \pmod 4$ oder $p \equiv 3 \pmod 4$), Primzahlen $q \equiv 3 \pmod 4$ und echt-komplexe primäre Primelemente λ die folgenden 4 Gleichungen zu zeigen

(1) $\left(\frac{-p}{-q}\right)_4 = \left(\frac{-q}{-p}\right)_4$, falls $p \equiv 3 \pmod 4$

(2) $\left(\frac{p}{-q}\right)_4 = \left(\frac{-q}{p}\right)_4$, falls $p \equiv 1 \pmod 4$

(3) $\left(\frac{-p}{\lambda}\right)_4 = \left(\frac{\lambda}{-p}\right)_4$, falls $p \equiv 3 \pmod 4$

(4) $\left(\frac{p}{\lambda}\right)_4 = \left(\frac{\lambda}{p}\right)_4$, falls $p \equiv 1 \pmod 4$.

Sei zunächst $q \equiv 3 \pmod 4$ und unterscheide die beiden möglichen Fälle für p:

(1) Für eine beliebige ganze Zahl a teilerfremd zu p und $p \equiv 3 \pmod 4$ gilt $\left(\frac{a}{p}\right)_4 = 1$, denn

$$\left(\frac{a}{p}\right)_4 \equiv a^{\frac{p^2-1}{4}} = \left(a^{p-1}\right)^{\frac{p+1}{4}} \equiv 1 \pmod p.$$

Somit gilt $\left(\frac{-p}{-q}\right)_4 = \left(\frac{-p}{q}\right)_4 = 1 = \left(\frac{-q}{p}\right)_4 = \left(\frac{-q}{-p}\right)_4$.

(2) Sei $p \equiv 1 \pmod 4$ mit $p = \pi\overline{\pi}$ für ein Primelement π von $\mathbb{Z}[i]$. Dann gilt $\left(\frac{-q}{p}\right)_4 = 1$, denn

$$\left(\frac{-q}{p}\right)_4 = \left(\frac{-q}{\pi}\right)_4\left(\frac{-q}{\overline{\pi}}\right)_4 = \left(\frac{-q}{\pi}\right)_4\left(\frac{-q}{\pi}\right)_4^{-1} = 1.$$

Aus dem Beweis von (1) folgt $\left(\frac{p}{-q}\right)_4 = 1$.

Zeige nun noch die letzten beiden Gleichungen. Sei $l := N(\lambda) \equiv 1 \pmod 4$ und $\chi := \chi_\lambda := \left(\frac{\cdot}{\lambda}\right)_4$.

(3) Sei $p \equiv 3 \pmod 4$. Dann folgt mit dem Frobenius-Automorphismus

$$\begin{aligned} G(\chi)^p &= \left(\sum_{t=0}^{l-1} \chi(t)\zeta^t\right)^p \equiv \sum_{t=0}^{l-1} \chi(t)^p \zeta^{pt} = \chi(p)^4 \sum_{t=0}^{l-1} \chi(t)^p \zeta^{pt} \\ &= \chi(p) \sum_{t=0}^{l-1} \chi(pt)^3 \zeta^{pt} = \left(\frac{p}{\lambda}\right)_4 G(\chi^3) \pmod p. \end{aligned}$$

Somit folgt

$$\begin{aligned} G(\chi)^{p+1} &\equiv \left(\frac{p}{\lambda}\right)_4 G(\chi^3)G(\chi) = \left(\frac{p}{\lambda}\right)_4 G(\chi^{-1})G(\chi) \\ &\overset{2.2.5}{=} \left(\frac{p}{\lambda}\right)_4 \chi(-1)l = \left(\frac{-p}{\lambda}\right)_4 l \pmod p. \end{aligned} \tag{4.5}$$

Nach Korollar 4.4.5 gilt $\overline{\lambda} \equiv \lambda^p \pmod p$ und folglich $l = \lambda\overline{\lambda} \equiv \lambda^{p+1} \pmod p$. Zusammen mit Korollar 4.3.4 folgt

$$\begin{aligned} G(\chi)^{p+1} &= \left(G(\chi)^4\right)^{\frac{p+1}{4}} = \left(\lambda^3\overline{\lambda}\right)^{\frac{p+1}{4}} = \left(\lambda^{p+3}\right)^{\frac{p+1}{4}} \\ &= \lambda^{p+1}\lambda^{\frac{(p+1)(p-1)}{4}} \equiv \lambda^{p+1}\left(\frac{\lambda}{p}\right)_4 \equiv l\left(\frac{\lambda}{p}\right)_4 \pmod p. \end{aligned} \tag{4.6}$$

Mit den Kongruenzen (4.5) und (4.6) gilt

$$\left(\frac{-p}{\lambda}\right)_4 l \equiv l\left(\frac{\lambda}{p}\right)_4 \pmod p$$

also

$$\left(\frac{-p}{\lambda}\right)_4 = \left(\frac{\lambda}{p}\right)_4 = \left(\frac{\lambda}{-p}\right)_4.$$

(4) Sei nun $p = \pi\overline{\pi} \equiv 1 \pmod 4$. Dann ist

$$G(\chi)^p \equiv \sum_{t=0}^{l-1} \chi(t)^p \zeta^{pt} = \chi(p)^3 \sum_{t=0}^{l-1} \chi(tp)\zeta^{tp} = \chi(p)^{-1}G(\chi) \pmod p.$$

Erneut mit Korollar 4.3.4 folgt

$$\left(\frac{p}{\lambda}\right)_4^{-1} = \chi(p)^{-1} \equiv G(\chi)^{p-1} = \left(G(\chi)^4\right)^{\frac{p-1}{4}} = \left(\lambda^3\overline{\lambda}\right)^{\frac{p-1}{4}} = \lambda^{\frac{3(p-1)}{4}}\overline{\lambda}^{\frac{p-1}{4}} \pmod p$$

also

$$\left(\frac{p}{\lambda}\right)_4^{-1} \equiv \left(\frac{\lambda}{\pi}\right)_4^3 \left(\frac{\overline{\lambda}}{\pi}\right)_4 \pmod \pi.$$

Dies führt zu

$$\left(\frac{p}{\lambda}\right)_4 = \left(\frac{\lambda}{\pi}\right)_4 \left(\frac{\overline{\lambda}}{\pi}\right)_4^3 = \left(\frac{\lambda}{\pi}\right)_4 \left(\frac{\lambda}{\overline{\pi}}\right)_4 = \left(\frac{\lambda}{p}\right)_4.$$

□

Direkt aus dem Beweis von (1) folgt:

4.4.7 Korollar. *Für alle ungeraden $a, b \in \mathbb{Z}$ mit* $\mathrm{ggT}(a,b) = 1$ *gilt*

$$\left(\frac{a}{b}\right)_4 = 1.$$

Zu dem Reziprozitätsgesetz von Eisenstein gibt es noch die Ergänzungssätze zu ganzzahligen Elementen. Wir werden zunächst nur den Fall von primären Primelementen betrachten und anschließend auf alle primären Elemente von $\mathbb{Z}[i]$ erweitern.

4.4.8 Satz. *Sei $a \in \mathbb{Z}$ primär (d.h. $a \equiv 1 \pmod 4$) und prim in $\mathbb{Z}$. Dann gilt*

(1) $\left(\frac{i}{a}\right)_4 = (-1)^{\frac{a-1}{4}}$

(2) $\left(\frac{1+i}{a}\right)_4 = i^{\frac{a-1}{4}}$

(3) $\left(\frac{2}{a}\right)_4 = 1$

Beweis. Für ein ganzzahliges, primäres Element a, welches prim in $\mathbb{Z}$ ist, gibt es zwei Möglichkeiten. Entweder ist $-a = p \equiv 3 \pmod 4$ oder $a = p \equiv 1 \pmod 4$ jeweils für eine Primzahl p.

(a) Sei $-a = p \equiv 3 \pmod 4$ für eine Primzahl p. Dann ist nach Definition $\left(\frac{i}{p}\right)_4 \equiv i^{\frac{p^2-1}{4}} \pmod p$. Da dies aber bereits eine Potenz von i ist, folgt direkt die Gleichheit. Insgesamt gilt

$$\left(\frac{i}{a}\right)_4 = \left(\frac{i}{p}\right)_4 = (i^{p-1})^{\frac{p+1}{4}} = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{a-1}{4}}.$$

(b) Ist $a = p = \pi\overline{\pi} \equiv 1 \pmod 4$. So gilt mit demselben Argument wie in (a)

$$\left(\frac{i}{a}\right)_4 = \left(\frac{i}{p}\right)_4 = \left(\frac{i}{\pi}\right)_4 \left(\frac{i}{\overline{\pi}}\right)_4 = i^{\frac{p-1}{4}} i^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{a-1}{4}}.$$

Nun zu dem zweiten Ergänzungssatz.

(a) Sei $-a = p \equiv 3 \pmod 4$. Dann gilt $(1+i)^p \equiv 1^p + i^p = 1 - i \pmod p$. Somit folgt $(1+i)^{p-1} \equiv \frac{1-i}{1+i} = -i \pmod p$ und insgesamt gilt

$$\left(\frac{1+i}{a}\right)_4 = \left(\frac{1+i}{p}\right)_4 \equiv \left((1+i)^{p-1}\right)^{\frac{p+1}{4}} \equiv (-i)^{\frac{p+1}{4}} = i^{\frac{-p-1}{4}} = i^{\frac{a-1}{4}} \pmod p.$$

(b) Sei nun wieder $a = p = \pi\overline{\pi} \equiv 1 \pmod 4$. Dann gilt

$$\begin{aligned}\left(\frac{1+i}{a}\right)_4 &= \left(\frac{1+i}{p}\right)_4 = \left(\frac{1+i}{\pi}\right)_4\left(\frac{1+i}{\overline{\pi}}\right)_4 = \left(\frac{1+i}{\pi}\right)_4\overline{\left(\frac{1-i}{\pi}\right)}_4 \\ &= \left(\frac{i(1-i)}{\pi}\right)_4\left(\frac{1-i}{\pi}\right)_4^3 = \left(\frac{i}{\pi}\right)_4\left(\frac{1-i}{\pi}\right)_4^4 = \left(\frac{i}{\pi}\right)_4 = i^{\frac{p-1}{4}} = i^{\frac{a-1}{4}}.\end{aligned}$$

Der Beweis des letzten Ergänzungssatzes, folgt direkt aus den zwei eben bewiesenen durch

$$\left(\frac{2}{a}\right)_4 = \left(\frac{i}{a}\right)_4^3\left(\frac{1+i}{a}\right)_4^2 \overset{(1),(2)}{=} (-1)^{\frac{a-1}{4}}(-1)^{\frac{a-1}{4}} = 1.$$

□

Die Ergänzungssätze kann man nun auch verallgemeinern. Die Gültigkeit für ein beliebiges primäres $a \in \mathbb{Z}$ folgt direkt aus folgendem Lemma.

4.4.9 Lemma. [3] *Für ganze Zahlen $m_1, \ldots, m_s \in \mathbb{Z}$ mit $m_i \equiv 1 \pmod 4$ gilt*

$$\sum_{i=1}^{s} \frac{m_i - 1}{4} \equiv \frac{1}{4}\left(\prod_{i=1}^{s} m_i - 1\right) \pmod 4.$$

Beweis. Betrachte zunächst den Fall $s = 2$: Zeige für $m \equiv n \equiv 1 \pmod 4$ die Kongruenz $\frac{m-1}{4} + \frac{n-1}{4} \equiv \frac{mn-1}{4} \pmod 4$ oder äquivalent $m+n-1 \equiv mn \pmod{16}$. Es gilt $0 \equiv (m-1)(n-1) = mn - m - n + 1 \pmod{16}$. Damit folgt schon die Gleichheit für $s = 2$. Die Behauptung folgt nun induktiv. □

Mit Hilfe dieses Lemmas kann man nun die Ergänzungssätze für ein beliebiges ganzzahliges Element beweisen.

4.4.10 Satz. *Sei $a \in \mathbb{Z}$ primär (d.h. $a \equiv 1 \pmod 4$). Dann gilt*

(1) $\left(\frac{i}{a}\right)_4 = (-1)^{\frac{a-1}{4}}$

(2) $\left(\frac{1+i}{a}\right)_4 = i^{\frac{a-1}{4}}$

(3) $\left(\frac{2}{a}\right)_4 = 1$

Beweis. Sei $a = p_1 \cdots p_s(-q_1)\cdots(-q_r)$ die Primfaktorzerlegung von a mit Primzahlen $p_j \equiv 1 \pmod 4$ für $j = 1, \ldots, s$ und $q_k \equiv 3 \pmod 4$ für $k = 1, \ldots, r$. Da alle Faktoren der Zerlegung nun primär sind, folgt nach Satz 4.4.8 zusammen mit Lemma 4.4.9:

$$\begin{aligned}\left(\frac{i}{a}\right)_4 &= \prod_{j=1}^{s}\left(\frac{i}{p_j}\right)_4 \prod_{k=1}^{r}\left(\frac{i}{q_k}\right)_4 \overset{4.4.8}{=} \prod_{j=1}^{s}(-1)^{\frac{p_j-1}{4}} \prod_{k=1}^{r}(-1)^{\frac{(-q_k)-1}{4}} \\ &= (-1)^{\sum_{j=1}^{s}\frac{p_j-1}{4} + \sum_{k=1}^{r}\frac{(-q_k)-1}{4}} \overset{4.4.9}{=} (-1)^{\frac{1}{4}\left(\prod_{j=1}^{s} p_j \prod_{k=1}^{r}(-q_k)-1\right)} = (-1)^{\frac{a-1}{4}}.\end{aligned}$$

[3] Aussage siehe [IR93, Kap.9 Aufg. 44]

Für den zweiten Ergänzungssatz folgt die Rechnung analog und der dritte folgt wieder aus den ersten beiden wie im Beweis von Satz 4.4.8. □

4.4.11 Korollar. *Für teilerfremde Elemente $a, b \in \mathbb{Z}$ mit $b \equiv 1 \pmod 2$, dann gilt*

$$\left(\frac{a}{b}\right)_4 = 1.$$

Beweis. Sind a und b beide ungerade, so folgt die Behauptung nach Korollar 4.4.7. Ist a gerade, etwa $a = 2^l c$ für $l \geq 1$ und $2 \nmid c$. Dann folgt nach Satz 4.4.10, dass $\left(\frac{2}{b}\right)_4 = 1$ gilt und daher folgt

$$\left(\frac{a}{b}\right)_4 = \underbrace{\left(\frac{2}{b}\right)_4^l}_{=1} \left(\frac{c}{b}\right)_4 \overset{4.4.7}{=} 1.$$

□

Nun zurück zu dem Beweis des biquadratischen Reziprozitätsgesetzes. Mit Hilfe von Eisensteins Reziprozitätsgesetz (Theorem 4.4.6) können wir folgenden Spezialfall des Reziprozitätsgesetzes von Jacobi und Kaplan beweisen.

4.4.12 Lemma. *Seien $\alpha = a + bi$ und $\beta = c + di$ zwei teilerfremde Elemente von $\mathbb{Z}[i]$, sodass $a \equiv c \equiv 1 \pmod 4$ und $\mathrm{ggT}(a, b) = \mathrm{ggT}(c, d) = 1$ gilt. Dann gilt*

$$\left(\frac{\beta}{\alpha}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\alpha}{\beta}\right)_4.$$

Beweis. Aus der Voraussetzung $\mathrm{ggT}(a, b) = 1$ folgt auch $\mathrm{ggT}(a, \alpha) = \mathrm{ggT}(b, \alpha) = 1$. Ebenso folgt $\mathrm{ggT}(c, \beta) = \mathrm{ggT}(d, \beta) = 1$ aus der Voraussetzung $\mathrm{ggT}(c, d) = 1$. Weiterhin gilt

$$c\alpha = ac + bci = ac + bi(\beta - di) \equiv ac + bd \pmod \beta. \tag{4.7}$$

Da β und α teilerfremd sind und $\mathrm{ggT}(c, \beta) = 1$ ist, folgt $\mathrm{ggT}(ac + bd, \beta) = 1$. Außerdem folgt aus Gleichung (4.7)

$$\left(\frac{c}{\beta}\right)_4 \left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{ac + bd}{\beta}\right)_4. \tag{4.8}$$

Analog erhalte $a\beta \equiv ac + bd \pmod \alpha$, sowie $\mathrm{ggT}(ac + bd, \alpha) = 1$ und

$$\left(\frac{a}{\alpha}\right)_4 \left(\frac{\beta}{\alpha}\right)_4 = \left(\frac{ac + bd}{\alpha}\right)_4. \tag{4.9}$$

Aus den Gleichungen (4.8) und (4.9) folgt

$$\left(\frac{c}{\beta}\right)_4 \overline{\left(\frac{a}{\alpha}\right)_4} \left(\frac{\alpha}{\beta}\right)_4 \overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{c\alpha}{\beta}\right)_4 \overline{\left(\frac{a\beta}{\alpha}\right)_4} = \left(\frac{ac + bd}{\beta}\right)_4 \overline{\left(\frac{ac + bd}{\alpha}\right)_4} = \left(\frac{ac + bd}{\beta\overline{\alpha}}\right)_4.$$

Nach Multiplikation der Gleichung mit $\left(\frac{c}{\beta}\right)_4^{-1}\left(\frac{a}{\alpha}\right)_4$ gilt dann:

$$\left(\frac{\alpha}{\beta}\right)_4\left(\frac{\beta}{\alpha}\right)_4^{-1} = \left(\frac{c}{\beta}\right)_4^{-1}\left(\frac{a}{\alpha}\right)_4\left(\frac{ac+bd}{\beta\overline{\alpha}}\right)_4. \tag{4.10}$$

Berechne nun die einzelnen Restsymbole auf der rechten Seite der Gleichung (4.10). Wegen $c \equiv 1 \pmod 4$ ist entweder β oder $-\beta$ primär. Ist $-\beta$ primär, so folgt

$$\left(\frac{c}{\beta}\right)_4 = \left(\frac{c}{-\beta}\right)_4 \overset{4.4.6}{=} \left(\frac{-\beta}{c}\right)_4 = \left(\frac{-1}{c}\right)_4\left(\frac{\beta}{c}\right)_4 = (-1)^{\frac{c-1}{2}}\left(\frac{\beta}{c}\right)_4 = \left(\frac{\beta}{c}\right)_4.$$

Falls β primär ist, so kann man Theorem 4.4.6 direkt anwenden, sodass in beiden Fällen die Gleichheit

$$\left(\frac{c}{\beta}\right)_4 = \left(\frac{\beta}{c}\right)_4 \tag{4.11}$$

gilt. Mit $\beta \equiv di \pmod c$ und $\mathrm{ggT}(c,\beta) = 1$ folgt dann

$$\left(\frac{c}{\beta}\right)_4 \overset{(4.11)}{=} \left(\frac{\beta}{c}\right)_4 = \left(\frac{di}{c}\right)_4 = \underbrace{\left(\frac{d}{c}\right)_4}_{=1}\left(\frac{i}{c}\right)_4. \tag{4.12}$$

Analog folgt

$$\left(\frac{a}{\alpha}\right)_4 = \left(\frac{i}{a}\right)_4. \tag{4.13}$$

Da $\mathrm{ggT}(ac+bd,\alpha) = \mathrm{ggT}(ac+bd,\beta) = 1$ ist und b,d beide gerade sind, gilt $ac+bd \equiv 1 \pmod 4$. Analog zu (4.11) erhält man auch

$$\left(\frac{ac+bd}{\overline{\alpha}\beta}\right)_4 = \left(\frac{\overline{\alpha}\beta}{ac+bd}\right)_4.$$

Mit $\overline{\alpha}\beta = (a-bi)(c+di) = ac+bd+(ad-bc)i$ gilt:

$$\left(\frac{ac+bd}{\overline{\alpha}\beta}\right)_4 = \left(\frac{\overline{\alpha}\beta}{ac+bd}\right)_4 = \left(\frac{ac+bd+(ad-bc)i}{ac+bd}\right)_4 = \underbrace{\left(\frac{ad-bc}{ac+bd}\right)_4}_{=1}\left(\frac{i}{ac+bd}\right)_4.$$

Aus den Gleichungen (4.10), (4.12) und (4.13) folgt nach Anwendung des Ergänzungssatzes 4.4.10

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)_4\left(\frac{\beta}{\alpha}\right)_4^{-1} &= \left(\frac{i}{c}\right)_4^{-1}\left(\frac{i}{a}\right)_4\left(\frac{i}{ac+bd}\right)_4 \\ &\overset{4.4.10}{=} (-1)^{-\frac{c-1}{4}}(-1)^{\frac{a-1}{4}}(-1)^{\frac{ac+bd-1}{4}} \\ &= (-1)^{\frac{c-1}{4}+\frac{a-1}{4}}(-1)^{\frac{ac-1}{4}}(-1)^{\frac{bd}{4}} \\ &\overset{4.4.9}{=} (-1)^{\frac{ac-1}{4}}(-1)^{\frac{ac-1}{4}}(-1)^{\frac{bd}{4}} \\ &= (-1)^{\frac{bd}{4}}.\end{aligned}$$

□

Aus diesem Lemma kann man nun das biquadratischen Reziprozitätsgesetzes von Jacobi und Kaplan (Theorem 4.4.3) folgern. Das heißt die Voraussetzung $\mathrm{ggT}(a,b) = \mathrm{ggT}(c,d) = 1$ von Lemma 4.4.12 wird nicht benötigt. Es soll folgendes Theorem gezeigt werden:

Theorem. *Seien $\alpha = a + bi$, $\beta = c + di$ zwei teilerfremde Elemente mit $a \equiv c \equiv 1 \pmod 4$. Dann gilt*

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

Beweis von Theorem 4.4.3. Sei $\alpha = a+bi = m(\tilde{a}+\tilde{b}i)$ und $\beta = c+di = n(\tilde{c}+\tilde{d}i)$ mit $m \equiv n \equiv 1 \pmod 4$ und $\mathrm{ggT}(\tilde{a},\tilde{b}) = 1 = \mathrm{ggT}(\tilde{c},\tilde{d})$ (Dies ist möglich, da α, β nicht durch 2 teilbar sind). In den vorangehenden Sätzen sind bereits folgende Gleichheiten gezeigt:

(a) Da nach Voraussetzung $\mathrm{ggT}(\alpha,\beta) = 1$ ist, ist auch $\mathrm{ggT}(n,m) = 1$ und nach Korollar 4.4.7 gilt

$$\left(\frac{n}{m}\right)_4 = 1 = \left(\frac{m}{n}\right)_4. \tag{4.14}$$

(b) Da $m \equiv 1 \pmod 4$ und β oder $-\beta$ primär ist, folgt mit Satz 4.4.6

$$\left(\frac{\beta}{m}\right)_4 = \left(\frac{m}{\beta}\right)_4. \tag{4.15}$$

(c) Aus $n \equiv 1 \pmod 4$ und wegen $\tilde{a} \equiv 1 \pmod 4$ ist auch $\tilde{a} + \tilde{b}i$ oder $-(\tilde{a} + \tilde{b}i)$ primär. Erneute Anwendung von Korollar 4.4.6 zeigt:

$$\left(\frac{n}{\tilde{a}+\tilde{b}i}\right)_4 = \left(\frac{\tilde{a}+\tilde{b}i}{n}\right)_4. \tag{4.16}$$

Fügen wir nun die obigen Gleichungen zusammen und wenden den bereits bewiesenen Spezialfall (Lemma 4.4.12) auf $\tilde{a} + \tilde{b}i$ und $\tilde{c} + \tilde{d}i$ an, so folgt

$$\begin{aligned}
\left(\frac{\alpha}{\beta}\right)_4 &= \left(\frac{\tilde{a}+\tilde{b}i}{\beta}\right)_4 \left(\frac{m}{\beta}\right)_4 \\
&= \left(\frac{\tilde{a}+\tilde{b}i}{\tilde{c}+\tilde{d}i}\right)_4 \left(\frac{\tilde{a}+\tilde{b}i}{n}\right)_4 \left(\frac{m}{\beta}\right)_4 \\
&\overset{4.4.12}{=} (-1)^{\frac{\tilde{b}\tilde{d}}{4}} \left(\frac{\tilde{c}+\tilde{d}i}{\tilde{a}+\tilde{b}i}\right)_4 \left(\frac{\tilde{a}+i\tilde{b}}{n}\right)_4 \left(\frac{m}{\beta}\right)_4 \\
&\overset{(4.15)}{=} (-1)^{\frac{\tilde{b}\tilde{d}}{4}} \left(\frac{\tilde{c}+\tilde{d}i}{\tilde{a}+\tilde{b}i}\right)_4 \left(\frac{\tilde{a}+\tilde{b}i}{n}\right)_4 \left(\frac{\beta}{m}\right)_4 \\
&\overset{(4.16)}{=} (-1)^{\frac{\tilde{b}\tilde{d}}{4}} \left(\frac{\tilde{c}+\tilde{d}i}{\tilde{a}+\tilde{b}i}\right)_4 \left(\frac{n}{\tilde{a}+\tilde{b}i}\right)_4 \left(\frac{\beta}{m}\right)_4 \\
&= (-1)^{\frac{m\tilde{b}n\tilde{d}}{4}} \left(\frac{\beta}{\tilde{a}+\tilde{b}i}\right)_4 \left(\frac{\beta}{m}\right)_4 \qquad (\text{Da } m \equiv n \equiv 1 \pmod 4) \\
&= (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.
\end{aligned}$$

□

Nun ist also das biquadratische Reziprozitätsgesetz in der Variante von Jacobi und Kaplan bewiesen. Wir wollen nun zeigen, dass die beiden Theoreme äquivalent sind. Dazu benötigen wir noch einige kleine Lemmata. Das folgende Lemma entspricht dem ersten Ergänzungssatz des biquadratischen Reziprozitätsgesetz.

4.4.13 Lemma. *Sei $\alpha = a + bi$ primär in $\mathbb{Z}[i]$. Dann gilt:*

$$\left(\frac{i}{\alpha}\right)_4 = i^{\frac{1-a}{2}}.$$

Beweis. Nehme zunächst an, dass $\alpha = \pi = a + bi \equiv 1 \pmod{(2+2i)}$ ein primäres Primelement ist. Unterscheide die zwei möglichen Fälle für α:

1. Sei $a \equiv 1 \pmod 4$ und $b \equiv 0 \pmod 4$. Dann gilt

$$\left(\frac{i}{\alpha}\right)_4 = i^{\frac{N(\alpha)-1}{4}} = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{a^2-1}{4}} = i^{\frac{1-a}{2}}.$$

   Dabei gilt die letzte Gleichung, denn $a \equiv 1 \pmod 8$ ist äquivalent zu $\frac{a-1}{2} \equiv 0 \pmod 4$. Dafür folgt $\frac{a^2-1}{4} = \frac{a-1}{2}\frac{a+1}{2} \equiv 0 \equiv -\frac{a-1}{2} = \frac{1-a}{2} \pmod 4$. Ist $a \equiv 5 \pmod 8$, so ist $\frac{a+1}{2} \equiv 3 \pmod 4$ und damit $\frac{a^2-1}{4} \equiv -\frac{a-1}{2} \pmod 4$.

2. Gilt $a \equiv 3 \pmod 4$ und $b \equiv 2 \pmod 4$, so ist $0 \equiv (b-2)^2 = b^2 - 4b + 4 \pmod{16}$ und somit $\frac{b^2}{4} \equiv 1 \pmod 4$. Dann gilt

$$\left(\frac{i}{a}\right)_4 = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{a^2+4-1}{4}} = i^{\frac{(a+1)^2+2-2a}{4}} = i^{\frac{1-a}{2}},$$

   denn $(a+1)^2 \equiv 0 \pmod{16}$.

Nun zu einem allgemeinen primären Element $\alpha = a + bi$ mit primärer Primfaktorzerlegung $\alpha = \prod_{j=1}^{s} \gamma_j$ für primäre Primelemente $\gamma_j = a_j + b_j i$ von $\mathbb{Z}[i]$. Für α folgt

$$\left(\frac{i}{\alpha}\right)_4 = \prod_{j=1}^{s} \left(\frac{i}{\gamma_j}\right)_4 = \prod_{j=1}^{s} (-1)^{\frac{a_j-1}{2}}.$$

Für $k := \prod_{j=1}^{s} a_j$ ist k ungerade, da jedes a_j ungerade ist. Es gilt

$$\sum_{j=1}^{s} \frac{a_j - 1}{2} \equiv |\{j \in \{1, \ldots, s\} \colon a_j \equiv 3 \pmod 4\}| \equiv \frac{k-1}{2} \pmod 2, \tag{4.17}$$

denn die Summanden $\frac{a_j-1}{2}$ für $a_j \equiv 1 \pmod 4$ verschwinden modulo 2. Die zweite Gleichheit gilt, denn ob $k \equiv 1 \pmod 4$ oder $k \equiv 3 \pmod 4$ ist, hängt nur davon ab, ob es eine gerade oder eine ungerade Anzahl an Faktoren a_j mit $a_j \equiv 3 \pmod 4$ gibt.

Es genügt zu zeigen, dass $\sum_{j=1}^{s} \frac{a_j-1}{2} \overset{(4.17)}{\equiv} \frac{1}{2}(\prod_{j=1}^{s} a_j - 1) \equiv \frac{a-1}{2} \pmod 2$ gilt. Für $s = 2$ ist Produkt von γ_1 und γ_2 durch

$$\gamma_1\gamma_2 = (a_1 + b_1 i)(a_2 + b_2 i) = a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)i$$

gegeben. Daher ist $a = a_1a_2 - b_1b_2$ und da b_1 und b_2 gerade sind, ist $a \equiv a_1a_2 \pmod 4$. Nun folgt wie gewünscht $\frac{a_1a_2-1}{2} \equiv \frac{a-1}{2} \pmod 2$. Der allgemeine Fall folgt induktiv. □

Mit dem eben bewiesenem ersten Ergänzungssatz erhalte nun eine einfache Folgerung für den biquadratischen Rest von -1.

4.4.14 Korollar. *Für $\alpha = a + bi$ primär in $\mathbb{Z}[i]$ gilt*

$$\left(\frac{-1}{\alpha}\right)_4 = (-1)^{\frac{a-1}{2}}.$$

Beweis. Nach dem ersten Ergänzungssatz gilt

$$\left(\frac{-1}{\alpha}\right)_4 = \left(\frac{i}{\alpha}\right)_4^2 = (i^2)^{\frac{1-a}{2}} = (-1)^{\frac{1-a}{2}} = (-1)^{\frac{a-1}{2}}.$$

□

4.4.15 Lemma. *Für primäre Elemente $a_j + b_j i$ für $j = 1, \ldots, s$ und $\prod_{j=1}^{s}(a_j + b_j i) = a + bi$ gilt*

$$\sum_{j=1}^{s} \frac{b_j}{2} \equiv \frac{b}{2} \pmod 2.$$

Beweis. Es genügt die Behauptung für $s = 2$ zu zeigen, der allgemeine Fall folgt per Induktion. Es gilt $b = a_1b_2 + a_2b_1$. Zu zeigen ist, dass

$$a_1b_2 + a_2b_1 \equiv b_1 + b_2 \pmod 4$$

gilt. Dies ist der Fall, denn nach Voraussetzung sind π_i primär und somit ist $a_i \equiv b_i + 1 \pmod 4$ für $i = 1, 2$. Es folgt

$$b = a_1b_2 + a_2b_1 \equiv (b_1 + 1)b_2 + (b_2 + 1)b_1 = 2b_1b_2 + b_1 + b_2 \equiv b_1 + b_2 \pmod 4.$$

□

4.4.16 Satz. *Im Folgenden bezeichne*

(i) das Reziprozitätsgesetz von Gauß und Eisenstein für primäre Primelemente (siehe Theorem 4.4.1) und

(ii) das Reziprozitätsgesetz nach Jacobi und Kaplan (siehe Theorem 4.4.3) .

Dann gilt (i) ⇔ (ii).

Beweis. Zeige „$(ii) \Rightarrow (i)$“:
Seien $\pi = a + bi$ und $\lambda = c + di$ zwei teilerfremde primäre Primelemente. Da beide primär sind, sind a und c ungerade. Untersuche nun die einzelnen Fälle:

(a) Ist $a \equiv c \equiv 1 \pmod 4$, so folgt die Behauptung direkt.

(b) Ist $a \equiv 1 \pmod 4$ und $c \equiv 3 \pmod 4$, so ist $d \equiv -d \equiv 2 \pmod 4$ und somit folgt

$$\left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{\pi}{-\lambda}\right)_4 \overset{(ii)}{=} (-1)^{\frac{-bd}{4}} \left(\frac{-\lambda}{\pi}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\lambda}{\pi}\right)_4,$$

denn nach Satz 4.2.5 gilt $\left(\frac{-1}{\pi}\right)_4 \overset{4.2.5}{=} (-1)^{\frac{a-1}{2}} = 1$.

(c) Der Fall $a \equiv 3 \pmod 4$ und $c \equiv 1 \pmod 4$ folgt analog.

(d) Gilt $a \equiv c \equiv 3 \pmod 4$, dann folgt

$$\left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{-1}{\lambda}\right)_4 \left(\frac{-\pi}{-\lambda}\right)_4 \overset{(ii)}{=} -(-1)^{\frac{bd}{4}} \left(\frac{-\lambda}{-\pi}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\lambda}{\pi}\right)_4.$$

Dabei wurde verwendet, dass nach Korollar 4.2.5 $\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{a-1}{2}} = -1$ gilt und ebenso $\left(\frac{-1}{\lambda}\right)_4 = -1$.

„$(i) \Rightarrow (ii)$“:
Seien $\alpha = a + bi$ und $\beta = c + di$ so gewählt, dass $a \equiv c \equiv 1 \pmod 4$ gilt. Folglich ist α oder $-\alpha$ primär und ebenso entweder β oder $-\beta$ primär. Unterscheide erneut alle möglichen Kombinationen:

(a) Sind α und β primär, so gilt $b \equiv d \equiv 0 \pmod 4$. Sei nun $\alpha = \prod_{j=1}^{r} \pi_j$ die primäre Primfaktorzerlegung von α und $\beta = \prod_{k=1}^{s} \lambda_k$ die von β mit primären Primelementen $\pi_j = a_j + b_j i$ und $\lambda_k = c_k + d_k i$ von $\mathbb{Z}[i]$ für $j = 1, \ldots, r$ und $k = 1, \ldots, s$. Es gilt

$$\left(\frac{\alpha}{\beta}\right)_4 = \prod_{j=1}^{r}\prod_{k=1}^{s} \left(\frac{\pi_j}{\lambda_k}\right)_4 \overset{(i)}{=} \prod_{j=1}^{r}\prod_{k=1}^{s} (-1)^{\frac{b_j d_k}{4}} \left(\frac{\lambda_k}{\pi_j}\right)_4 \overset{4.4.15}{=} (-1)^{\frac{bd}{4}} \prod_{j=1}^{r}\prod_{k=1}^{s} \left(\frac{\lambda_k}{\pi_j}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

(b) Ist α und $-\beta$ primär und $\alpha = \prod_{j=1}^{r} \pi_j$, sowie $-\beta = \prod_{k=1}^{s} \lambda_k$ die primäre Primfaktorzerlegungen mit π_j und λ_k für $j = 1, \ldots, r$ und $k = 1, \ldots, s$ wie in (a). Mit $\frac{-b}{2} \equiv \frac{b}{2} \pmod 2$ folgt

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{-\beta}\right)_4 \overset{(a)}{=} (-1)^{-\frac{bd}{4}} \left(\frac{-\beta}{\alpha}\right)_4 \overset{4.4.14}{=} (-1)^{-\frac{bd}{4}} \underbrace{(-1)^{\frac{a-1}{2}}}_{=1} \left(\frac{\beta}{\alpha}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

(c) Ist $-\alpha$ und β primär, so folgt die Behauptung analog.

(d) Nun fehlt noch der Fall, dass $-\alpha$ und $-\beta$ primär sind. Betrachte dazu die primären Primfaktorzerlegungen $-\alpha = \prod_{j=1}^{r} \pi_j$ und $-\beta = \prod_{k=1}^{s} \lambda_k$. Wobei π_j und λ_k für $j = 1, \ldots, r$ und $k = 1, \ldots, s$ wie in (a) gewählt sind. Dann ist

$$\left(\frac{-1}{\alpha}\right)_4 = \left(\frac{-1}{-\alpha}\right)_4 \overset{4.4.14}{=} (-1)^{\frac{-a-1}{2}} = -1.$$

Analog folgt $\left(\frac{-1}{\beta}\right)_4 = (-1)^{\frac{-c-1}{2}} = -1$. Erhalte nun insgesamt

$$\left(\frac{\alpha}{\beta}\right)_4 = -\left(\frac{-\alpha}{-\beta}\right)_4 \overset{(a)}{=} -(-1)^{\frac{bd}{4}} \left(\frac{-\beta}{-\alpha}\right)_4 = (-1)^{\frac{bd}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

□

Damit ist der Beweis des biquadratischen Reziprozitätsgesetzes abgeschlossen. Da die Version von Jacobi und Kaplan bewiesen wurde und die Äquivalenz beider biquadratischen Reziprozitätsgesetze gezeigt wurde, ist auch die Version von Gauß und Eisenstein bewiesen. Nun ist es möglich die fehlenden, allgemeinen Ergänzungssätze zum biquadratischen Reziprozitätsgesetz zu beweisen.

4.4.17 Satz (Ergänzungssätze)**.** *Sei $\alpha = a + bi$ primär in $\mathbb{Z}[i]$. Dann gilt:*

(1) $\left(\frac{i}{\alpha}\right)_4 = i^{\frac{1-a}{2}}$

(2) $\left(\frac{1+i}{\alpha}\right)_4 = i^{\frac{a-b-b^2-1}{4}}$

(3) $\left(\frac{2}{\alpha}\right)_4 = i^{\frac{ab}{2}} = i^{-\frac{b}{2}}$

Beweis.

(1) siehe Satz 4.4.13

(2) Sei $\lambda := (1+i)^3 = -2+2i$, dann ist $\left(\frac{\lambda}{\alpha}\right)_4^3 = \left(\frac{1+i}{\alpha}\right)_4^9 = \left(\frac{1+i}{\alpha}\right)_4$. Somit genügt es $\left(\frac{\lambda}{\alpha}\right)_4$ zu berechnen.
Da $\alpha = a + bi$ nach Voraussetzung primär ist, existiert eine Darstellung $\alpha = c + d\lambda = c + d(-2+2i) = c - 2d + 2di$. Also folgt nach Koeffizientenvergleich $b = 2d$ und $a = c - 2d$, somit $d = \frac{b}{2}$ und $c = a + b$. Nun zu der Berechnung von $\left(\frac{\lambda}{\alpha}\right)_4$.
Wenn α primär ist, so ist auch $\alpha - \lambda = a+2+(b-2)i$ primär, also ist das Reziprozitätsgesetz

4.4.1 anwendbar. Es gilt

$$\begin{aligned}\left(\frac{\lambda}{\alpha}\right)_4 &= \left(\frac{\lambda-\alpha}{\alpha}\right)_4 = \left(\frac{-1}{\alpha}\right)_4\left(\frac{\alpha-\lambda}{\alpha}\right)_4 \\ &\overset{\text{biqu. RG}}{=} (-1)^{\frac{b(b-2)}{4}}\left(\frac{-1}{\alpha}\right)_4\left(\frac{\alpha}{\alpha-\lambda}\right)_4 \\ &\overset{4.4.14}{=} (-1)^{\frac{b(b-2)}{4}}(-1)^{\frac{a-1}{2}}\left(\frac{\alpha}{\alpha-\lambda}\right)_4 \\ &= (-1)^{\frac{b}{2}}\left(\frac{\lambda}{\alpha-\lambda}\right)_4 \\ &= (-1)^{d}\left(\frac{\lambda}{\alpha-\lambda}\right)_4.\end{aligned}$$

Dabei wurde verwendet, dass $\alpha \equiv \lambda \pmod{(\alpha-\lambda)}$ ist und da b gerade ist, folgt $\frac{b(b-2)}{4} \equiv 0 \pmod 2$. Außerdem gilt, da α primär ist, $a-1 \equiv b \pmod 4$. Dies ist äquivalent zu $\frac{a-1}{2} \equiv \frac{b}{2} \pmod 2$. Durch wiederholen dieses Schrittes folgt

$$\left(\frac{\lambda}{\alpha}\right)_4 = (-1)^{d+(d-1)}\left(\frac{\lambda}{\alpha-2\lambda}\right)_4.$$

Nach weiteren Iterationen gilt dann:

$$\left(\frac{\lambda}{\alpha}\right)_4 = (-1)^{\sum_{j=1}^{d} j}\left(\frac{\lambda}{\alpha-d\lambda}\right)_4 = (-1)^{\frac{d(d+1)}{2}}\left(\frac{\lambda}{c}\right)_4.$$

Wegen α primär, ist $c = a+b \equiv 1 \pmod 4$ und somit gilt $\left(\frac{1+i}{c}\right)_4 = i^{\frac{c-1}{4}}$ nach Satz 4.4.10. Also folgt insgesamt

$$\begin{aligned}\left(\frac{1+i}{\alpha}\right)_4 &= \left(\frac{\lambda}{\alpha}\right)_4^3 \\ &= \left((-1)^{\frac{d(d+1)}{2}}\left(\frac{\lambda}{c}\right)_4\right)^3 \\ &= \left((-1)^3\right)^{\frac{d(d+1)}{2}}\left(\frac{1+i}{c}\right)_4^9 \\ &= (-1)^{\frac{d(d+1)}{2}}\left(\frac{1+i}{c}\right)_4 \\ &= i^{d(d+1)}i^{\frac{c-1}{4}} \\ &= i^{\frac{b^2+2b}{4}+\frac{a+b-1}{4}} \\ &= i^{\frac{a-b-b^2-1}{4}}.\end{aligned}$$

Dabei wurde im letzten Schritt verwendet, dass $2b^2+4b = 2b(b+2) \equiv 0 \pmod{16}$ ist und somit $b^2+3b \equiv -b^2-b \pmod{16}$. Dies ist gleichbedeutend mit $\frac{b^2+3b}{4} \equiv \frac{-b^2-b}{4} \pmod 4$.

(3) Nun zu dem letzten Ergänzungssatze, der aufgrund der Primfaktorzerlegung von 2, direkt aus den ersten beiden folgt. Es ist

$$\begin{aligned}\left(\frac{2}{\pi}\right)_4 &= \left(\frac{i}{\pi}\right)_4^3 \left(\frac{1+i}{\pi}\right)_4^2 \\ &= \left(i^{\frac{1-a}{2}}\right)^3 \left(i^{\frac{a-b-b^2-1}{4}}\right)^2 \\ &= i^{\frac{a-1+a-b-1-b^2}{2}} \\ &= i^{-\frac{b}{2}} i^{a-1-\frac{b^2}{2}} \\ &= i^{-\frac{b}{2}} \\ &= i^{\frac{ab}{2}},\end{aligned}$$

denn es gilt $a-1 \equiv b \pmod 4$, also folgt $a-1-\frac{b^2}{2} \equiv b-\frac{b^2}{2} \equiv 0 \pmod 4$. Außerdem gilt $\frac{b}{2}(b+2) \equiv 0 \pmod 4$ und somit $-\frac{b}{2} \equiv \frac{b}{2}(b+1) \equiv \frac{ab}{2} \pmod 4$.

□

Das nachfolgende Beispiel soll die Berechnung eines biquadratischen Restsymbols mit Hilfe des biquadratischen Reziprozitätsgesetzes und dessen Ergänzungssätze verdeutlichen.

4.4.18 Beispiel. Betrachte die primären Primelemente $\pi = 3+2i$ und $\lambda = -1-6i$. Die beiden Elemente sind prim, da die Normen $N(\pi) = 13$ und $N(\lambda) = 37$ Primzahlen sind. Wir werden sehen, dass π kein kubischer Rest modulo λ ist:

$$\begin{aligned}\left(\frac{3+2i}{-1-6i}\right)_4 &\overset{\text{biqu. RG}}{=} (-1)^{\frac{3-1}{2}\frac{-1-1}{2}} \left(\frac{-1-6i}{3+2i}\right)_4 \\ &= -\left(\frac{5-2i}{3+2i}\right)_4 \\ &= -\left(\frac{-1}{3+2i}\right)_4 \left(\frac{-5+2i}{3+2i}\right)_4 \\ &= -(-1)^{\frac{3-1}{2}} \left(\frac{-5+2i}{3+2i}\right)_4 \\ &= \left(\frac{-5+2i}{3+2i}\right)_4 \\ &\overset{\text{biqu. RG}}{=} (-1)^{\frac{-5-1}{2}\frac{3-1}{2}} \left(\frac{3+2i}{-5+2i}\right)_4 \\ &= -\left(\frac{8}{-5+2i}\right)_4 \\ &= -\left(\frac{2}{-5+2i}\right)_4^3 \\ &\overset{\text{3. ES}}{=} -(i^{-\frac{2}{2}})^3 \\ &= -i.\end{aligned}$$

4.5 Anwendungen

In diesem Abschnitt soll das biquadratische Reziprozitätsgesetz verwendet werden einige Problemstellungen zu lösen. Im Folgenden wird Eulers Vermutung bezüglich Primzahlen der Form $x^2 + 64y^2$ bewiesen werden und zum Abschluss des Kapitels folgt der Beweis der Vermutungen (1.1) und (1.2) des einführenden Beispiels 1.0.3. Weiterhin wird die Lösbarkeit rationaler Gleichungen $x^4 \equiv a \pmod{p}$ für verschiedene ungerade Primzahlen p untersucht werden.
Zunächst zu Eulers Vermutung für Primzahlen $p = x^2 + 64y^2$. Für den Beweis dieser Vermutung wird der dritte Ergänzungssatz des biquadratischen Reziprozitätsgesetzes verwendet.

4.5.1 Theorem. [4] *Sei $p > 0$ eine Primzahl. Dann gilt die Äquivalenz:*

$$\exists x, y \in Z : \ p = x^2 + 64y^2 \ \Leftrightarrow \ p \equiv 1 \pmod{4} \text{ und } 2 \text{ ist ein biquadratischer Rest modulo } p.$$

Beweis. Aus der Darstellung $p = x^2+64y^2$ folgt direkt $p \equiv 1 \pmod{4}$, da das Quadrat ungerader Zahlen immer kongruent zu 1 modulo 4 ist (Wenn x gerade wäre, so wäre p keine ungerade Primzahl). Für $p \equiv 1 \pmod{4}$ können wir eine Darstellung $p = a^2 + b^2 = \pi\overline{\pi}$ wählen mit einem primären Primelement $\pi = a + bi$ von $\mathbb{Z}[i]$. Mit der Isomorphie $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$ und mit dem dritten Ergänzungssatz zum biquadratischen Reziprozitätsgesetz (Satz 4.4.17) folgt: 2 ist ein biquadratischer Rest genau dann, wenn $i^{-\frac{b}{2}} = 1$ ist und das ist genau dann der Fall, wenn b durch 8 teilbar ist. □

Sei im Folgenden $p \equiv 1 \pmod{4}$ eine Primzahlen, π ein Primelement von $\mathbb{Z}[i]$ mit $p = \pi\overline{\pi}$ und $a \in \mathbb{Z}$ ein zu p teilerfremdes ganzzahliges Element. Wir haben bereits in Satz 4.2.6 gesehen, dass die Äquivalenz

$$\left(\frac{a}{\pi}\right)_4 = 1 \ \Leftrightarrow \ x^4 \equiv a \pmod{\pi} \text{ hat eine Lösung } x \in \mathbb{Z}[i]$$

gilt. Wir wollen nun eine Aussage über die Lösbarkeit der Gleichung $x^4 \equiv a \pmod{p}$ in $\mathbb{Z}$ treffen.

4.5.2 Satz. [5] *Es gilt*

$$\left(\frac{a}{\pi}\right)_4 = 1 \ \Leftrightarrow \ x^4 \equiv a \pmod{p} \text{ hat eine Lösung } x \in \mathbb{Z}.$$

Beweis. Jedes Element aus $\mathbb{Z}[i]$ ist modulo $\pi = c + di$ kongruent zu einer ganzen Zahl. Denn d und p sind teilerfremd. Mit dem euklidischen Algorithmus folgt die Existenz eines $b \in \mathbb{Z}$, sodass $bd \equiv m \pmod{p}$ gilt. Sei $\lambda = m + ni$ ein beliebiges Element aus $\mathbb{Z}[i]$. Dann ist

$$\mu \equiv \mu - b\pi = \mu - bc - bdi \equiv \mu - bc - mi = \underbrace{n - bc}_{\in\mathbb{Z}} \pmod{\pi}.$$

Folglich gilt die Äquivalenz

$$\left(\frac{a}{\pi}\right)_4 = 1 \ \Leftrightarrow \ x^4 \equiv a \pmod{\pi} \text{ hat eine Lösung } x \in \mathbb{Z}.$$

[4] siehe [Cox89, S.83, Thm. 4.23]
[5] siehe [IR93, S.128, Lemma 1]

Da auf beiden Seiten der Kongruenz $x^4 \equiv a \pmod{\pi}$ ganzzahlige Elemente stehen, ist die ganzzahlige Lösbarkeit dieser Kongruenz gleichbedeutend mit der Lösbarkeit von $x^4 \equiv a \pmod{p}$ in $\mathbb{Z}$. □

Wir können nun auch den Zusammenhang zwischen dem Legendre-Symbol und dem biquadratischen Restsymbol untersuchen. Es ist offensichtlich, dass die Lösbarkeit von $x^4 \equiv a \pmod{p}$ in $\mathbb{Z}$ bereits die Lösbarkeit der Gleichung $x^2 \equiv a \pmod{p}$ impliziert. Also gilt

4.5.3 Satz. *Es gilt:*

$$\left(\frac{a}{\pi}\right)_4 = 1 \;\Rightarrow\; \left(\frac{a}{p}\right)_2 = 1.$$

Die Umkehrung gilt im Allgemeinen nicht, denn 4 ist ein quadratischer Rest modulo 5 ($2^2 \equiv 4 \pmod{5}$) aber kein biquadratischer Rest. Für $x \in \mathbb{F}_5^*$ ist $x^4 = 1$ in $\mathbb{F}_5$.
Die quadratischen Reste in einem endlichen Körper $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ für ein beliebiges Primelement π von $\mathbb{Z}[i]$, sind die Element, für die das biquadratische Restsymbol $\left(\frac{\cdot}{\pi}\right)_4$ die werte 1 oder -1 annimmt. Dies wird im folgenden Satz gezeigt.

4.5.4 Satz. [6] *Ist* $\left(\frac{a}{p}\right)_2 = 1$*, so gilt* $\left(\frac{a}{\pi}\right)_4 = \pm 1$.

Beweis. Nach Eulers Kriterium (3.3) ist $\left(\frac{a}{p}\right)_2 = 1$ gleichbedeutend mit $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Wegen $p = \pi\overline{\pi}$ gilt diese Kongruenz auch bezüglich π. Es folgt

$$\left(\frac{a}{\pi}\right)_4^2 \equiv \left(a^{\frac{p-1}{4}}\right)^2 = a^{\frac{p-1}{2}} \equiv 1 \pmod{\pi}.$$

Also gilt $\left(\frac{a}{\pi}\right)_4^2 = 1$. Dies impliziert $\left(\frac{a}{\pi}\right)_4 = \pm 1$. □

Im Weiteren werden Primzahlen $p \equiv 3 \pmod 4$ und ein zu p teilerfremdes Element $a \in \mathbb{Z}$ betrachtet. Auch für solche Primzahlen, können wir eine Aussage zur Lösbarkeit rationaler Gleichungen $x^4 \equiv a \pmod{p}$ in $\mathbb{Z}$ machen.

4.5.5 Satz. [7] *Für eine träge Primzahl* $p \equiv 3 \pmod 4$ *ist die Gleichung* $x^4 \equiv a \pmod{p}$ *für jedes zu* p *teilerfremdes* $a \in \mathbb{Z}$ *lösbar, d.h.* $\left(\frac{a}{p}\right)_4 = 1$.

Beweis. Nach Voraussetzung ist $p-1$ nicht durch 4 teilbar. Somit existiert ein Automorphismus $a \mapsto a^4$ auf $(\mathbb{Z}/p\mathbb{Z})^*$. Da die Gleichung nur für ganzzahlige $a \in \mathbb{Z}$ betrachtet wird, gibt es immer eine ganzzahlige Lösung. □

Als weitere Anwendung des biquadratischen Reziprozitätsgesetzes und dessen Ergänzungssätze, kann man nun noch für ein primäres Primelement $\pi = a+bi$ von $\mathbb{Z}[i]$ mit $b \neq 0$ das biquadratische Restsymbol $\left(\frac{\overline{\pi}}{\pi}\right)_4$ berechnen. Da π und $\overline{\pi}$ teilerfremd sind, ist das Symbol nicht 0.

[6] siehe [IR93, S.128, Lemma 2]
[7] siehe [Cox89, S.92, Aufg.. 4.20]

4.5.6 Satz. [8] *Sei $\pi = a + bi$ ein primäres Primelement von $\mathbb{Z}[i]$ mit $b \neq 0$. Dann gilt*

$$\left(\frac{\overline{\pi}}{\pi}\right)_4 = \left(\frac{-2}{\pi}\right)_4 (-1)^{\frac{a^2-1}{8}}.$$

Beweis. Es gilt $\overline{\pi} = a - bi \equiv 2a \pmod{\pi}$ und somit

$$\left(\frac{\overline{\pi}}{\pi}\right)_4 = \left(\frac{2}{\pi}\right)_4 \left(\frac{a}{\pi}\right)_4 \tag{4.18}$$

(vgl. Aufgabe 28 von [IR93, S.136]). Um $\left(\frac{\overline{\pi}}{\pi}\right)_4$ genauer zu bestimmen, ist es ausreichend, die beiden Restsymbole der rechten Seite zu berechnen. Das erste biquadratische Restsymbol $\left(\frac{2}{\pi}\right)_4$ lässt sich direkt aus dem dritten Ergänzungssatz (Satz 4.4.17) bestimmen. Wir wollen nun auch noch den Wert des Restsymbols $\left(\frac{a}{\pi}\right)_4$ genauer bestimmen. Um das biquadratische Reziprozitätsgesetz anwenden zu können, wird eine Einheit u benötigt, sodass ua primär ist. Zeige dazu, dass $a \equiv (-1)^{\frac{p-1}{4}} \pmod 4$ gilt (siehe [IR93, Aufg.28]).
Ist $a \equiv 1 \pmod 4$, so folgt wegen π primär, bereits $b \equiv 0 \pmod 4$ und $a^2 + b^2 \equiv 1 \pmod 8$. Dies impliziert

$$(-1)^{\frac{a^2+b^2-1}{4}} = 1 \equiv a \pmod 4.$$

Ist andernfalls $a \equiv 3 \equiv -1 \pmod 4$, so ist $b \equiv 2 \pmod 4$ und $a^2 + b^2 \equiv 5 \pmod 8$. Damit folgt

$$(-1)^{\frac{a^2+b^2-1}{4}} = -1 \equiv a \pmod 4.$$

Folglich ist $(-1)^{\frac{p-1}{4}} a \equiv 1 \pmod 4$ und Eisensteins biquadratisches Reziprozitätsgesetz (Theorem 4.4.6) ist anwendbar. Dann folgt

$$\left(\frac{(-1)^{\frac{p-1}{4}} a}{\pi}\right)_4 = \left(\frac{\pi}{(-1)^{\frac{p-1}{4}} a}\right)_4 = \left(\frac{\pi}{a}\right)_4 = \left(\frac{ib}{a}\right)_4 = \left(\frac{i}{a}\right)_4 \left(\frac{b}{a}\right)_4 = \left(\frac{i}{a}\right)_4 = i^{\frac{a^2-1}{4}} = (-1)^{\frac{a^2-1}{8}}. \tag{4.19}$$

Dabei ist $a^2 - 1 = (a-1)(a+1)$ durch 8 teilbar.

[8] Aussage siehe [IR93, S.136, Aufg. 30]; für den Beweis werden auch [IR93, S.136, Aufg. 27-30] gezeigt

Mit den Gleichungen (4.18) und (4.19) gilt

$$\begin{aligned}\left(\frac{\overline{\pi}}{\pi}\right)_4 &\overset{(4.18)}{=} \left(\frac{2}{\pi}\right)_4\left(\frac{a}{\pi}\right)_4\\ &= \left(\frac{-2}{\pi}\right)_4\left(\frac{-1}{\pi}\right)_4\left(\frac{-1}{\pi}\right)_4^{\frac{p-1}{4}}\left(\frac{(-1)^{\frac{p-1}{4}}a}{\pi}\right)_4\\ &= \left((-1)^{\frac{a-1}{2}}\right)^{\frac{p+3}{4}}\left(\frac{-2}{\pi}\right)_4\left(\frac{(-1)^{\frac{p-1}{4}}a}{\pi}\right)_4\\ &\overset{(4.19)}{=} (-1)^{\frac{a-1}{2}\frac{p+3}{4}}\left(\frac{-2}{\pi}\right)_4(-1)^{\frac{a^2-1}{8}}\\ &= \left(\frac{-2}{\pi}\right)_4(-1)^{\frac{a^2-1}{8}}.\end{aligned}$$

Im letzten Schritt wurde verwendet, dass wegen $a \equiv (-1)^{\frac{p-1}{4}} \pmod 4$

$$\frac{1-a}{2}\cdot\frac{p+3}{4} \equiv \frac{1-(-1)^{\frac{p-1}{4}}}{2}\cdot\left(\frac{p-1}{4}+1\right) \equiv 0 \pmod 2$$

gilt. Denn es ist $\frac{p-1}{4} \equiv 0 \pmod 2$ oder $\frac{p-1}{4} \equiv 1 \pmod 2$. Damit folgt $(-1)^{\frac{a-1}{2}\frac{p+3}{4}} = 1$. □

Nun als letzten Satz noch den Beweis der Vermutungen (1.1) und (1.2) der Einleitung. Es wird eine allgemeinere Form bewiesen werden, sodass die Vermutungen (1.1) und (1.2) als Spezialfall folgen.

4.5.7 Satz. *Seien q und u zwei ungerade ganze Zahlen, sodass $p = 4qu+1 = a^2+4b^2$ eine Primzahl ist. Falls $S_q = 2^{2q}+1 = A_q \cdot B_q$ mit $A_q = 2^q - 2^{\frac{q+1}{2}}+1$, $B_q = 2^q + 2^{\frac{q+1}{2}}+1$ durch p teilbar ist, so gilt*

$$\begin{array}{llllllll} b \equiv & \pm 3u & \pmod 8 & \Leftrightarrow & A_q \equiv & 0 & \pmod p & \text{und } B_q \equiv \quad 2(1+2^q) \pmod p \\ b \equiv & \pm u & \pmod 8 & \Leftrightarrow & A_q \equiv & 2(1+2^q) & \pmod p & \text{und } B_q \equiv \quad 0 \pmod p \end{array}.$$

Beweis. Gelte $p \mid (2^{2q}+1)$, dann ist $2^{2q} = 2^{\frac{p-1}{2u}} \equiv -1 \pmod p$. Dies ist äquivalent zu $2^{\frac{p-1}{u}} \equiv 1 \pmod p$.
Denn durch Quadrieren der ersten Kongruenz erhalte direkt $2^{\frac{p-1}{u}} \equiv 1 \pmod p$. Gilt umgekehrt $2^{\frac{p-1}{u}} \equiv 1 \pmod p$, so folgt $2^{\frac{p-1}{2u}} \equiv \pm 1 \pmod p$. Wir müssen also nur das positive Vorzeichen ausschließen. Wäre $2^{\frac{p-1}{2u}} \equiv +1 \pmod p$, so würde durch potenzieren mit u die Kongruenz

$$1 \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}} \pmod p$$

folgen. Damit gilt die Äquivalenz

$$2^{\frac{p-1}{2}} \equiv 1 \pmod p \Leftrightarrow \frac{p^2-1}{8} \equiv 0 \pmod 2.$$

Dies zeigt, dass $p \equiv \pm 1 \pmod 8$ wäre. Wegen $p = 4qu + 1$ gilt jedoch $p \equiv 5 \pmod 8$, denn qu ist ungerade und somit ist $qu - 1$ durch 2 teilbar. Damit gilt $p - 5 = 4qu - 4 = 4(qu - 1) \equiv 0 \pmod 8$. Folglich ist $2^{\frac{p-1}{2u}} \equiv -1 \pmod p$ wie gewünscht.

Um die Restklassen von A_q und B_q modulo p bestimmen zu können, berechne zunächst die Restklassen von 2^q und $2^{\frac{q+1}{2}}$ modulo π.
Sei dazu $2^{\frac{p-1}{2u}} \equiv -1 \pmod p$ für $p = \pi\overline{\pi}$ mit $\pi = a + 2bi$. Dann gilt die Kongruenz auch modulo π und somit ist $2^q = 2^{\frac{p-1}{4u}} \equiv i^k$ für $k \in \{1, 3\}$. Da u ungerade ist, gilt $u^2 \equiv 1 \pmod 4$ und es folgt

$$2^{\frac{p-1}{4u}} \equiv i^k = \left(i^k\right)^{u^2} \equiv 2^{\frac{p-1}{4}u} \pmod \pi.$$

Mit dem Ergänzungssatz 4.4.17 zum biquadratischen Reziprozitätsgesetz gilt dann

$$2^{\frac{p-1}{4}} \equiv \left(\frac{2}{\pi}\right)_4 = i^{-b}.$$

Es ist nun gezeigt, dass

$$2^q = 2^{\frac{p-1}{4u}} \equiv i^{-bu} \pmod \pi \tag{4.20}$$

gilt. In ähnlicher Weise kann auch die Restklasse von $2^{\frac{q+1}{2}} = 2^{\frac{p-1+4u}{8u}}$ bestimmt werden. Dabei ist

$$\frac{2^{\frac{p-1+4u}{8u}}}{(1+i)} = \frac{(-i(1+i)^2)^{\frac{p-1+4u}{8u}}}{(1+i)} = (-i)^{\frac{p-1+4u}{8u}}(1+i)^{\frac{p-1+4u}{4u}-1} = (-i)^{\frac{-(p-1)+4u}{8u}}2^{\frac{p-1}{4u}} \equiv i^k \pmod \pi.$$

Somit bleibt die Restklasse nach potenzieren mit $u^2 \equiv 1 \pmod 4$ erhalten. Es folgt nach einiger Rechnung, die hier im Detail nicht ausgeführt werden wird:

$$\begin{aligned}\frac{2^{\frac{p-1+4u}{8u}}}{(1+i)} \equiv \frac{2^{\frac{p-1+4u}{8}u}}{(1+i)^{u^2}} &= \left(\frac{2^{\frac{p+3}{8}} \cdot 2^{\frac{u-1}{2}}}{(1+i)^u}\right)^u = \left(\frac{2^{\frac{p+3}{8}}}{(1+i)}\right)^u \left(\frac{2^{\frac{u-1}{2}}}{(1+i)^{u-1}}\right)^u \\ &= \left((-i)^{\frac{p+3}{8}}(1+i)^{\frac{p+3}{4}-1}\right)^u \left((-i)^{\frac{u-1}{2}}(1+i)^{u-1-(u-1)}\right)^u \\ &= i^{\frac{3-bu}{2}} \pmod \pi\end{aligned}$$

Da b und u beide ungerade sind, muss $b \equiv \pm u \pmod 8$ oder $b \equiv \pm 3u \pmod 8$ gelten. Unterscheide nun die einzelnen Fälle:

(a) Gilt $b \equiv u \pmod 8$. Dann gilt $bu \equiv 1 \pmod 8$, denn alle Quadrate ungerader Zahlen sind kongruent zu 1 modulo 8. Somit folgt

$$B_q = 2^q + 2^{\frac{q+1}{2}} + 1 \equiv i^{-bu} + (1+i)i^{\frac{3-bu}{2}} + 1 = i^3 + (1+i)i + 1 = 0 \pmod \pi.$$

Da auf beiden Seiten nur ganzzahlige Elemente stehen, gilt die Kongruenz auch modulo p. Wegen $A_q + B_q = 2(2^q + 1)$ folgt dann

$$A_q \equiv 2(2^q + 1) \pmod p.$$

(b) Ist $b \equiv -u \pmod 8$, so $bu \equiv -1 \pmod 8$ und daher $B_q \equiv i+(1+i)(-1)+1 \equiv 0 \pmod \pi$. Die Argumentation für A_q folgt analog.

(c) Sei nun $b \equiv 3u \pmod 8$ und somit $bu \equiv 3 \pmod 8$. Dann folgt

$$A_q = 2^q - 2^{\frac{q+1}{2}} + 1 \equiv i^{-bu} - (1+i)i^{\frac{3-bu}{2}} + 1 = i - (1+i) + 1 = 0 \pmod \pi.$$

Damit gilt $A_q \equiv 0 \pmod p$ und mit $A_q + B_q = 2(1+2^q)$ folgt auch $B_q \equiv 2(1+2^q) \pmod p$.

(d) Ist $b \equiv -3u \pmod 8$, so $bu \equiv -3 \pmod 8$. Dann folgt $A_q \equiv i^3 - (1+i)i^3 + 1 \equiv 0 \pmod \pi$.

□

Literaturverzeichnis

[Bos09] Bosch, Siegfried: *Algebra*. 7. Aufl. Springer Verlag, 2009

[Cox89] Cox, David A.: *Primes of the Form $x^2 + ny^2$*. Wiley, 1989

[IR93] Ireland, Kenneth ; Rosen, Michael: *A Classical Introduction to Modern Number Theory*. 2. Aufl. Springer Verlag, 1993

[Lem00] Lemmermeyer, Franz: *Reciprocity Laws: From Euler to Eisenstein*. Springer Verlag, 2000

[Alg13] Scheiderer, Prof. Dr. C.: *Algebra*. Universität Konstanz : Vorlesung, WS13/14

[ZT14] Scheiderer, Prof. Dr. C.: *Zahlentheorie*. Universität Konstanz : Vorlesung, SS14