Das Kubische und das Biquadratische Reziprozitätsgesetz

Bachelorarbeit

Naturwissenschaftlich-Technische Fakultät I
Universität des Saarlandes

zur Erlangung des akademischen Grades

Bachelor of Science
(B. Sc.)

betreut von **Prof. E.-U. Gekeler**

vorgelegt von **Simon Balthasar Jäger**
geboren am 02.05.1992 in Neunkirchen

Saarbrücken, den 19.07.2013

Eidesstaatliche Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Saarbrücken, den

Ort, Datum

Simon Balthasar Jäger

Inhaltsverzeichnis

1 Einleitung **4**

2 Das n-te Potenzrestsymbol **6**

3 Charaktere, Gaußsummen und Jacobisummen **15**

4 Das Kubische Reziprozitätsgesetz **23**

5 Das Biquadratische Reziprozitätsgesetz **30**

6 Beispiele und Schlusswort **43**

1 Einleitung

Was ist ein Reziprozitätsgesetz? Im Grunde geht diese Frage auf Euler zurück, der als erstes ein Quadratisches Reziprozitätsgesetz formulierte. Nachdem sich ein Beweis von Legendre als lückenhaft herausstellte, konnte als erster Gauß das Quadratische Reziprozitätsgesetz beweisen. Seitdem gibt es bis heute mehr als 200 Beweise für dieses Gesetz, von denen allein Gauß mehrere beisteuerte. Eine Chronik der Beweise für das Quadratische Reziprozitätsgesetz wurde von Franz Lemmermeyer in seinem Buch *Reciprocity Laws From Euler to Eisenstein* ([Lem]) zusammengestellt. Diese Chronik kann auch online eingesehen werden ([chron]).
Ein Reziprozitätsgesetz in der Mathematik befasst sich mit einer Verallgemeinerung des Quadratischen Reziprozitätsgesetzes. Letzteres braucht man, um in endlichen Körpern der Primzahlordnung $p \in \mathbb{P}$ quadratische Reste zu identifzieren. Das heißt, wir geben uns ein Element aus einem endlichen Körper vor und wollen entscheiden, ob es zu diesem Element eine Quadratwurzel gibt. Eine mögliche Verallgemeinerung ist: wir geben uns ein Element aus einem endlichen Körper vor und wollen entscheiden, ob es zu diesem Element eine n-te Wurzel gibt. Tatsächlich ist dies genau das, was wir in der Arbeit für den Fall $n = 4$ und $n = 3$ machen werden. Diese Idee ist natürlich nichts Neues. Sie ist vielmehr historisch eine der ersten Verallgemeinerungen des Quadratischen Reziprozitätsgesetzes. Die erste weitreichende Verallgemeinerung gelang Eisenstein mit dem Eisensteinschen Reziprozitätsgesetz, welches noch deutlich allgemeinere Aussagen trifft, als ich in dieser Arbeit machen werde. Er bewies dieses Reziprozitätsgesetz um 1850, aber seit dieser Zeit steht die Entwicklung allgemeinerer Reziprozitätsgesetze keinesfalls still. Weitere Verallgemeinerungen lieferten auch Furtwängler und Hasse (vgl. [Has],[Furt]). Und spätestens seitdem Hilbert im Jahre 1900 unter seinen berühmten 23 Problemen der Mathematik auch die Frage nach einer Verallgemeinerung des Reziprozitätsgesetzes für beliebige algebraische Zahlkörper stellte, sind Reziprozitätsgesetze in der Mathematik ein wichtiges Forschungsgebiet. Einen Meilenstein in der algebraischen Zahlentheorie und auch eine Teillösung des 9. Problems von Hilbert lieferte Artin. Das Artinsche Reziprozitätsgesetz wird wegen seiner Wichtigkeit als der Hauptsatz der Klassenkörpertheorie tituliert und liefert eine sehr elegante Beschreibung der endlichen abelschen Körpererweiterungen von algebraischen Zahlkörpern. Auch heute ist das Thema Reziprozitätsgesetz noch sehr aktuell. Das Langlands-Programm beschäftigt sich mit noch allgemeineren Reziprozitätsgesetzen die aber größtenteils noch unbewiesen sind.
Wir wollen uns aber mit den wohl deutlich einfacheren Reziprozitätsgesetzen beschäftigen, wie man sie schon im 19. Jahrhundert beschreiben konnte. Allerdings ist der Ausgangspunkt deutlich aktueller. Die Grundlagen für diese Arbeit sind Grundverständnisse in algebraischer Zahlentheorie. In der Arbeit werden Begriffe wie algebraische Zahlkörper, Ganzheitsringe, Galoisgruppen, Primideale und auch speziellere Dinge, wie Frobeniusautomorphismen, Trägheitsindex, Verzweigungsindex und Zerfällungsindex als bekannt vorausgesetzt. Meine Kenntnisse und größtenteils alle Notationen im folgenden Kapitel ziehe ich aus der Vorlesung zur Algebraischen Zahlentheorie I ([Gek]) von E.-U. Gekeler. Allerdings sind diese Begrifflichkeiten auch in den meisten Lehrbüchern zur algebraischen Zahlentheorie zu finden. Beispielsweise werden diese Begriffe im Buch von Neukirch ([Neu]) in den ersten Kapiteln erklärt. Besonders für die Beweise der Reziprozitätsgesetze und die Relationen der Gaußsummen empfehle ich die Bücher von Lemmermeyer ([Lem]; Kapitel 4.5 und 4.6, sowie Kapitel 6 und Kapitel 7) und Ireland, Rosen ([IR]; Kapitel 9). Letzteres

verlangt vom Leser auch weniger Grundkenntnisse in algebraischer Zahlentheorie. Da die Reziprozitätsgesetze über Kreisteilungskörpern bewiesen werden, empfiehlt sich auch ein Blick in das Buch von Washington ([Wash]; Kapitel 1, Kapitel 2 und Kapitel 3).
Bevor wir mit den eigentlichen Aussagen anfangen, möchte ich noch kurz das Vorgehen erklären. Wir werden im folgenden Kapitel das Potenzrestsymbol einführen und einige elementare Aussagen für dieses beweisen. Dabei versuche ich an elementare Aussagen der algebraischen Zahlentheorie zu erinnern, wenn wir diese für Beweise brauchen. Im Kapitel 3 kommen wir dann auf Gaußsummen, die einen sehr schönen Zusammenhang zu speziellen Kummererweiterungen haben. In den Kapiteln 4 und 5 beweisen wir dann das Kubische und das Biquadratische Reziprozitätsgesetz. Nachdem wir einige weitgehend triviale Aussagen über die zugrunde liegenden Ganzheitsringe gemacht haben, berechnen wir die Gaußsummen zu den Potenzrestsymbolen. Im Beweis der Reziprozitätsgesetze wird die Wirkung des Frobeniusautomorphismus einer Primzahl auf der Gaußsumme untersucht. Dies wird der Hauptteil des Beweises sein. Die endgültigen Aussagen folgen dann durch teils mühsame Rechnungen, die leider der Forderung nach Eleganz nicht völlig gerecht werden. Im Buch von Ireland, Rosen wird der Beweis des Biquadratischen Reziprozitätsgesetz deshalb auch wie folgt beendet: *This completes the Proof, a monument to ingenuity and persistence!* ([IR]; S.127)

2 Das n-te Potenzrestsymbol

Bezeichnungen: Wir führen zuerst ein paar Bezeichnungen ein, die in der gesamten Arbeit benutzt werden.

- $\mathbb{N} = \{1, 2, 3, ...\}$
- $K =$ algebraischer Zahlkörper
- $\overline{K} =$ algebraischer Abschluss von K
- $O_K =$ Ganzheitsring von K
- $Gal(L|K)$ =Galoisgruppe der Körpererweiterung $L|K$
- $\mathbb{P} =$ Menge der positiven Primzahlen $= \{2, 3, 5, ...\}$
- $a|b$ heißt a teilt b
- $K^* =$ multiplikative Gruppe von K
- $\mathbb{F}_q =$ Isomorphieklasse des endlichen Körpers mit $q = p^f$ Elementen

Vorbemerkung: Im ganzen Kapitel sei K ein algebraischer Zahlenkörper, ω_n eine primitive n-te Einheitswurzel, wobei $n \in \mathbb{N}$ eine natürliche Zahl ist. Im Folgenden sei $\mathfrak{p} \subset O_K$ ein ganzes Primideal mit $\mathfrak{p} \nmid nO_K$ und wir setzen voraus $\omega_n \in K$.

Proposition 2.1. *Sei μ_n die Menge der n-ten Einheitswurzeln in O_K. Dann definiert*

$$\begin{aligned} \mu_n &\longrightarrow (O_K/\mathfrak{p}O_K)^* \\ \zeta_n &\longmapsto \zeta_n \ mod\ \mathfrak{p} = \zeta_n(\mathfrak{p}) \end{aligned}$$

einen injektiven Gruppenhomomorphismus. Wir können also die n-ten Einheitswurzeln in O_K eineindeutig mit den n-ten Einheitswurzeln in $O_K/\mathfrak{p}O_K$ identifizieren.

Beweis: Dass die Abbildung wohldefiniert und ein Gruppenhomomorphismus ist, ist klar. Wir zeigen nur die Injektivität. Für diese reicht es zu zeigen, dass ω_n (ein Erzeuger von μ_n) in $O_K/\mathfrak{p}O_K$ auch eine primitive n-te Einheitswurzel ist. Sei also $k \in \mathbb{N}$ und $\omega_n^k \equiv 1(\mathfrak{p})$ bzw. $1 - \omega_n^k \equiv 0(\mathfrak{p})$. Betrachte weiter

$$f(X) = \frac{X^n - 1}{X - 1} = \sum_{i=0}^{n-1} X^i.$$

Dann ist

$$f(X) = \sum_{i=0}^{n-1} X^i = \prod_{i=1}^{n-1} (X - \omega^i),$$

da jede n-te Einheitswurzel außer 1 Nullstelle von $f(X)$ ist. Somit ergibt sich

$$\prod_{i=1}^{n-1} (1 - \omega^i) = f(1) = n.$$

Dies zeigt, dass $1 - \omega^k \not\equiv 0(\mathfrak{p})$ für $k \lneq n$, da sonst $\mathfrak{p} \mid nO_K$ gelten müsste. □

Definition/Proposition 2.2. *Sei $\mathfrak{a} \subset O_K$ ein ganzes Ideal. Wir definieren die Absolutnorm von $\mathfrak{a}$ mit*

$$\mathcal{N}(\mathfrak{a}) := \#(O_K/\mathfrak{a}O_K) < \infty.$$

Seien jetzt $\mathfrak{a}$ und $\mathfrak{b}$ zwei ganze Ideale; dann ist

$$\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Beweis: Sei $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ die eindeutige Primfaktorzerlegung von $\mathfrak{a}$. Wir wollen zeigen, dass

$$\mathcal{N}(\mathfrak{a}) = \prod_{i=1}^{s} \mathcal{N}(\mathfrak{p}_i)^{e_i}$$

gilt. Dies impliziert direkt die Behauptung. Nach dem chinesischen Restsatz ist

$$O_K/\mathfrak{a}O_K \cong \prod_{i=1}^{s} O_K/\mathfrak{p}_i^{e_i}O_K,$$

und es reicht zu zeigen, dass $\mathcal{N}(\mathfrak{p}^e) = \mathcal{N}(\mathfrak{p})^e$ für Primideale $\mathfrak{p}$ gilt. Betrachte dazu $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ mit $i \in \mathbb{N}$. Die Gruppe $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ bildet einen $O_K/\mathfrak{p}O_K$ Vektorraum der Dimension 1. Insbesondere ist jede Restklasse eines $a \in \mathfrak{p}^i - \mathfrak{p}^{i+1}$ ein Erzeuger des Vektorraums. Dies zeigt

$$\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong O_K/\mathfrak{p}O_K$$

und folglich

$$\mathcal{N}(\mathfrak{p}^e) = \#(O_K/\mathfrak{p}^eO_K) = \prod_{i=0}^{e-1} \#(\mathfrak{p}^iO_K/\mathfrak{p}^{i+1}O_K) = \#(O_K/\mathfrak{p}O_K)^e = \mathcal{N}(\mathfrak{p})^e.$$

□

Korollar 2.3. *Ist $\mathfrak{p}$ ein Primideal von O_K über dem Primideal in $\mathbb{Z}$, das von $p \in \mathbb{P}$ erzeugt wird, so ist $\mathcal{N}(\mathfrak{p}) = p^f$, wobei f der Trägheitsindex von $\mathfrak{p}$ über p ist.*

Beweis: Dies ist klar, da $O_K/\mathfrak{p}O_K$ gerade die Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ vom Grad f ist. □

Bemerkungen 2.4. Sei K ein beliebiger Zahlkörper mit Ganzheitsring O_K und L eine endliche Erweiterung von K mit Ganzheitsring O_L. Da $L|K$ separabel ist, gilt

- $[L:K]_{sep} = \#\{\sigma : L \to \overline{K} | \sigma \text{ ist } K - \text{Einbettung von } L \text{ in } \overline{K}\} = [L:K]$.
- Sei $Aut(L|K) := \{\sigma : L \to \overline{K} | \sigma \text{ ist } K - \text{Einbettung von } L \text{ in } \overline{K}\}$. Dann ist die Relativnorm definiert durch

  $$N_K^L : L \to K, x \longmapsto \prod_{\sigma \in Aut(L|K)} \sigma(x).$$

  Eine andere (äquivalente) Möglichkeit die Relativnorm eines $x \in L$ zu definieren, ist als Determinante der K-linearen Abbildung m_x, wobei

  $$m_x : L \to L, a \mapsto xa.$$

- Die Idealnorm eines Primideals $\mathfrak{q} \subset O_L$ über einem Primideal $\mathfrak{p} \subset O_K$ mit Trägheitsindex $f := f_{\mathfrak{q}|\mathfrak{p}}$ wird definiert als
$$N_K^L(\mathfrak{q}) = \mathfrak{p}^f.$$
Die Idealnorm wird auf beliebige gebrochene Ideale in L durch ihre Primidealzerlegung und vollständige Multiplikativität fortgesetzt.

- In dieser Situation sei jetzt $\mathfrak{a} = (a)$, das von $a \in L$ erzeugte Hauptideal. Dann stimmt die Idealnorm von $\mathfrak{a}$ mit dem Ideal, das von der Relativnorm von a erzeugt wird, überein. Es gilt also
$$N_K^L(\mathfrak{a}) = (N_K^L(a)).$$

Korollar 2.5. *Sei nun zusätzlich O_K ein Hauptidealring und $N_{\mathbb{Q}}^K$ die Relativnorm von K über $\mathbb{Q}$. Ist dann $\mathfrak{a} = (a)$, so gilt*

$$|N_{\mathbb{Q}}^K(a)| = \mathcal{N}(\mathfrak{a}).$$

Beweis: Wegen der Multiplikativität beider Normen, reicht es, dies für Primideale $\mathfrak{p}$ zu zeigen. Sei also $\mathfrak{p} = (\pi)$ ein Primideal über $p \in \mathbb{P}$ mit Trägheitsindex f, so ist $\mathcal{N}(\mathfrak{p}) = p^f$. Weiter ist $N_{\mathbb{Q}}^K(\pi)O_K = N_{\mathbb{Q}}^K(\mathfrak{p}) = (p)^f$, wobei letzteres die Idealnorm von K über $\mathbb{Q}$ ist. Dies zeigt, dass $N_{\mathbb{Q}}^K(\pi)$ ein Erzeuger von $(p)^f$ ist, was aber bedeutet, dass $|N_{\mathbb{Q}}^K(\pi)| = p^f$ sein muss. □

Bemerkung 2.6. Das vorangegangene Korollar gilt nicht nur für Hauptidealringe, sondern auch für beliebige Hauptideale in Ganzheitsringen. Wir benötigen in dieser Arbeit aber nur diese schwächere Version, da die Ganzheitsringe, die wir später betrachten, Hauptidealringe sind. Um die allgemeinere Aussage zu beweisen, benötigt man die Lokalisierung eines Ganzheitsrings, die im weiteren Verlauf dieser Arbeit nicht benötigt wird. Deshalb möchte ich auf den Beweis der allgemeineren Aussage verzichten.

Korollar 2.7. *Ist $\mathfrak{a}$ ein ganzes Ideal von O_K, welches teilerfremd zu nO_K ist, so gilt $n \mid \mathcal{N}(\mathfrak{a}) - 1$. Ist $\mathfrak{a} = \prod_{i=1}^s \mathfrak{p}_i^{e_i}$ die eindeutige Zerlegung, so ist*

$$\frac{\mathcal{N}(\mathfrak{a}) - 1}{n} \equiv \sum_{i=1}^{s} e_i \frac{\mathcal{N}(\mathfrak{p}_i) - 1}{n} (mod\ n).$$

Beweis: Vermöge der injektiven Abbildung von $\mu_n \longrightarrow (O_K/\mathfrak{p}O_K)^*$ gilt bereits $n \mid \mathcal{N}(\mathfrak{p})-1$ für Primideale $\mathfrak{p}$. Sind $\mathfrak{p}$ und $\mathfrak{q}$ mit $n \mid \mathcal{N}(\mathfrak{p}) - 1$ sowie $n \mid \mathcal{N}(\mathfrak{q}) - 1$ nicht notwendigerweise Primideale, so gilt auch

$$(\mathcal{N}(\mathfrak{p}) - 1)(\mathcal{N}(\mathfrak{q}) - 1) = \mathcal{N}(\mathfrak{pq}) - \mathcal{N}(\mathfrak{q}) - \mathcal{N}(\mathfrak{p}) + 1 \equiv 0 (mod\ n^2),$$

insbesondere ist also

$$\frac{\mathcal{N}(\mathfrak{q}) - 1}{n} + \frac{\mathcal{N}(\mathfrak{p}) - 1}{n} \equiv \frac{\mathcal{N}(\mathfrak{pq}) - 1}{n} (mod\ n).$$

Mehrfaches Anwenden dieser Identität zeigt die Behauptung. □

Definition 2.8. *Ist $\alpha \in O_K$ und α teilerfremd zu $\mathfrak{p}$, so definieren wir mit den gleichen Bezeichnungen wie vorher das n-te Potenzrestsymbol durch die eindeutige n-te Einheitswurzel, die die Kongruenz*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,n} := \left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} (\mathfrak{p})$$

erfüllt. Sind α und $\mathfrak{p}$ nicht teilerfremd, so setzen wir $\left(\frac{\alpha}{\mathfrak{p}}\right) = 0$.

Proposition 2.9. *Das n-te Potenzrestsymbol erfüllt folgende Relationen*

(i) $\alpha \equiv \beta(\mathfrak{p}) \Rightarrow \left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\beta}{\mathfrak{p}}\right)$,

(ii) $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1 \Leftrightarrow \alpha$ *ist n-ter Potenzrest*,

(iii) $\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right)$.

Beweis:

(i) Dies ist direkt wegen der Definition des Symbols klar.

(ii) "$\Leftarrow$":
Sei α n-ter Potenzrest, d.h. es gibt ein $\gamma \in O_K$, sodass $\alpha \equiv \gamma^n(\mathfrak{p})$. Es ist dann

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\gamma^n}{\mathfrak{p}}\right) \equiv \gamma^{\mathcal{N}(\mathfrak{p})-1}(\mathfrak{p}) \equiv 1(\mathfrak{p}).$$

Wegen der letzten Kongruenz ist dann auch

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 1.$$

"$\Rightarrow$":
Sei jetzt

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 1,$$

d.h.

$$\alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \equiv 1(\mathfrak{p}).$$

Da $(O_K/\mathfrak{p}O_K)^* \cong \mathbb{F}_{p^f}^*$ mit $\mathfrak{p} \mid p$ und Trägheitsindex f zyklisch ist, gibt es einen zyklischen Erzeuger γ von $(O_K/\mathfrak{p}O_K)^*$ und eine natürliche Zahl k mit $\gamma^k \equiv \alpha(\mathfrak{p})$. Weiter ist dann

$$\gamma^{k\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \equiv 1(\mathfrak{p}),$$

und da γ ein Erzeuger von $(O_K/\mathfrak{p}O_K)^*$ ist, muss $n \mid k$ gelten. Somit ist

$$(\gamma^{\frac{k}{n}})^n \equiv \alpha(\mathfrak{p})$$

n-ter Potenzrest modulo $\mathfrak{p}$.

(iii) Dies ist wieder klar, wegen $(\alpha\beta)^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \equiv \alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \beta^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} (\mathfrak{p})$. □

Definition/Korollar 2.10. *Ist $\mathfrak{a}$ ein ganzes zu nO_K teilerfremdes Ideal in O_K und*

$$\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i},$$

so definieren wir

$$\left(\frac{\alpha}{\mathfrak{a}}\right) = \prod_{i=1}^{s} \left(\frac{\alpha}{\mathfrak{p}_i}\right)^{e_i}.$$

Dieses Symbol erfüllt

(i) $\left(\frac{\alpha\beta}{\mathfrak{a}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\beta}{\mathfrak{a}}\right)$,

(ii) $\left(\frac{\alpha}{\mathfrak{ab}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right)$,

(iii) $\left(\frac{\zeta}{\mathfrak{a}}\right) = \zeta^{\frac{\mathcal{N}(\mathfrak{a})-1}{n}}, \forall \zeta \in \mu_n$.

Beweis:

(i),(ii) Diese Relationen sind durch obige Proposition und durch die Definition direkt klar.

(iii) Wegen der Definition des n-ten Potenzrestsymbols ist

$$\left(\frac{\zeta}{\mathfrak{p}_i}\right) \equiv \zeta^{\frac{\mathcal{N}(\mathfrak{p}_i)-1}{n}} (\mathfrak{p}_i),$$

also sogar

$$\left(\frac{\zeta}{\mathfrak{p}_i}\right) = \zeta^{\frac{\mathcal{N}(\mathfrak{p}_i)-1}{n}}.$$

Dies zeigt aber, dass

$$\left(\frac{\zeta}{\mathfrak{a}}\right) = \zeta^{\sum_{i=1}^{s} e_i \frac{\mathcal{N}(\mathfrak{p}_i)-1}{n}} = \zeta^{\frac{\mathcal{N}(\mathfrak{a})-1}{n}},$$

da das Resultat nur von der Restklasse des Exponenten modulo n abhängt und da $\frac{\mathcal{N}(\mathfrak{a})-1}{n} \equiv \sum_{i=1}^{s} e_i \frac{\mathcal{N}(\mathfrak{p}_i)-1}{n} (n)$ gilt. □

Bemerkung 2.11. Sei jetzt $K|\mathbb{Q}$ galoissch mit Galoisgruppe G und $\mathfrak{p} \subset O_K$ ein ganzes Primideal mit $\mathfrak{p}|p$.Man definiert die Zerlegungsgruppe

$$Z(\mathfrak{p}) = \{\sigma \in G | \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

und die Trägheitsgruppe durch

$$T(\mathfrak{p}) = \{\sigma \in G | \sigma(x) \equiv x(\mathfrak{p}), \forall x \in O_K\}.$$

Ist $\mathfrak{q}$ ein weiteres Ideal über p, so sind die jeweiligen Gruppen $Z(\mathfrak{q})$ bzw. $T(\mathfrak{q})$ zu den Gruppen $Z(\mathfrak{p})$ bzw. $T(\mathfrak{p})$ konjugiert. Die zu den Gruppen gehörenden Fixkörper $K^{Z(\mathfrak{p})}$ und $K^{T(\mathfrak{p})}$ heißen Zerlegungskörper bzw. Trägheitskörper. Wir definieren dazu die Primideale $\mathfrak{r} := \mathfrak{p} \cap O_{K^{Z(\mathfrak{p})}}$ und $\mathfrak{s} := \mathfrak{p} \cap O_{K^{T(\mathfrak{p})}}$. In dieser Situation ist $\mathfrak{p}|\mathfrak{s}$ vollverzweigt und $\mathfrak{s}|\mathfrak{r}$ träge. Es ist also

$$[K : K^{T(\mathfrak{p})}] = \#T(\mathfrak{p}) = e_{\mathfrak{p}|\mathfrak{s}} = e\ _{mathfrakp|p} =: e$$

der Verweigungsindex und da die Trägheitsgruppe normal in der Zerlegungsgruppe liegt ist

$$[K^{T(\mathfrak{p})} : K^{Z(\mathfrak{p})}] = \#(Z(\mathfrak{p})/T(\mathfrak{p})) = f_{\mathfrak{s}|\mathfrak{r}} = f_{\mathfrak{p}|p} =: f$$

der Trägheitsindex von $\mathfrak{p}|p$. Dabei ist der Trägheitsindex definiert durch

$$f_{\mathfrak{p}|p} = [K(\mathfrak{p}) : K(p)]$$

und der Verzweigungsindex $e_{\mathfrak{p}|p}$ ist die maximale Potenz, in der $\mathfrak{p}$ in der Primfaktorzerlegung von pO_K auftritt. Beachte dabei, dass der Trägheitsindex und der Verzweigungsindex nicht von dem Primideal $\mathfrak{p}$ über p abhängt. Dies liegt daran, dass die Erweiterung galoissch ist. Die zugehörigen endlichen Körper sind

$$K(\mathfrak{p}) = O_K/\mathfrak{p}O_K, K(\mathfrak{s}) = O_{K^{T(\mathfrak{p})}}/\mathfrak{s}O_{K^{T(\mathfrak{p})}}, K(\mathfrak{r}) = O_{K^{Z(\mathfrak{p})}}/\mathfrak{r}O_{K^{Z(\mathfrak{p})}} \text{ und } K(p) = \mathbb{Z}/p\mathbb{Z}.$$

Da die einzelnen Körper $K(\mathfrak{p})$, $K(\mathfrak{s})$, $K(\mathfrak{r})$und $K(p)$ endliche Körper sind, sind die jeweiligen Erweiterungen galoissch und es gilt sogar

$$Z(\mathfrak{p})/T(\mathfrak{p}) \cong Gal(K(\mathfrak{s})|K(\mathfrak{r})) \cong Gal(K(\mathfrak{p})|K(p)),$$

wobei die letzte Isomorphie gilt, da $\mathfrak{r}|p$ und $\mathfrak{p}|\mathfrak{s}$ Trägheitsindex 1 haben und die jeweiligen Restkörper somit isomorph sind. Ist nun $\mathfrak{p} \mid p$ unverzweigt, dann ist $T(\mathfrak{p})$ trivial und $Z(\mathfrak{p})/T(\mathfrak{p}) = Z(\mathfrak{p})$. Durch den Isomorphismus

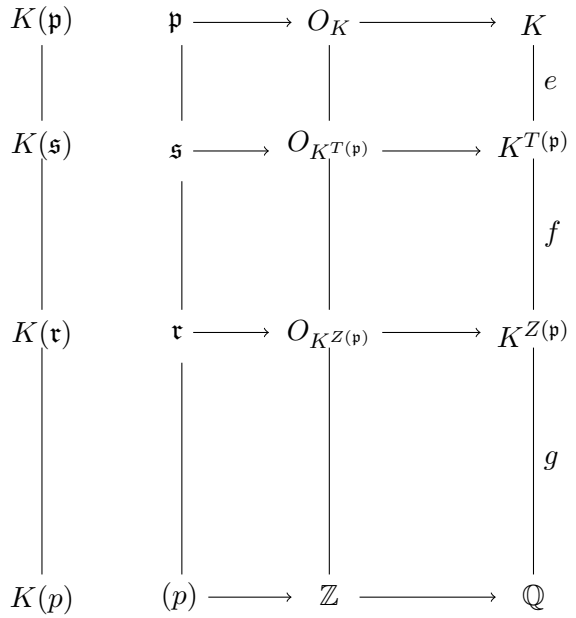
$$Z(\mathfrak{p})/T(\mathfrak{p}) = Z(\mathfrak{p}) \cong Gal(K(\mathfrak{p})|K(p))$$

existiert dann ein Frobeniusautomorphismus $\varphi_{\mathfrak{p}}$ in G. Dieser Automorphismus ist durch die Kongruenz

$$\varphi_{\mathfrak{p}}(x) \equiv x^p(\mathfrak{p}), \forall x \in O_K$$

wohlbestimmt. Der Zerlegungsindex $g = g_p$ ist die Anzahl der Primideale über p. Es gilt in diesem Kontext

$$e \cdot f \cdot g = [K : \mathbb{Q}].$$



Ist jetzt G abelsch, so ist die Konjugation trivial und die Gruppen $Z(\mathfrak{p}) =: Z(p)$ und $T(\mathfrak{p}) =: T(p)$ hängen nicht von den Primidealen über p ab, sondern nur von der Primzahl p selbst. Gleiches gilt für den Frobeniusautomorphismus. Wir betrachten jetzt noch spezieller $K = \mathbb{Q}(\omega_n)$; dann ist auch der Ganzheitsring $O_K = \mathbb{Z}[\omega_n]$. Die Galoisgruppe ist

$$G \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Der Isomorphismus ist durch

$$\begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & G \\ a & \longmapsto & \sigma_a \end{array}$$

gegeben, wobei die Körperautomorphismen σ_a durch $\sigma_a(\omega_n) = \omega_n^a$ definiert sind. Eine Primzahl p ist jetzt genau dann verzweigt, wenn $p \mid n$ gilt. Dementsprechend existiert ein Frobeniusautomorphismus zu einer Primzahl p genau dann, wenn $p \nmid n$. Der zugehörige Frobeniusautomorphismus ist dann einfach $\varphi_p = \sigma_p$. Da jetzt der Frobeniusautomorphismus zu einer Primzahl p die primitive Einheitswurzel in die p-te Potenz setzt, hängt die Wirkung des Frobeniusautomorphismus nur von der Restklasse der Primzahl p modulo n ab. Insbesondere ist $\varphi_p = 1$ genau dann der triviale Automorphismus, wenn $p \equiv 1(n)$. Und da dann auch $f = \#Z(p) = 1$ gilt, ist p vollständig zerfallend.

Korollar 2.12. *Betrachte $\mathbb{Q}(\omega_p)|L|\mathbb{Q}$ mit $p \equiv 1(n)$, $[L : \mathbb{Q}] = n$ und $q \neq p \in \mathbb{P}$ eine Primzahl. Dann gilt:*

$$q \text{ ist } n\text{-ter Potenzrest modulo } p \Leftrightarrow q \text{ zerfällt vollständig in } L \Leftrightarrow n \mid g$$

Dabei ist $g = g_q$ der Zerfällungsindex von q in $\mathbb{Q}(\omega_p)$.

Beweis: Es gilt q ist genau dann n-ter Potenzrest modulo p, wenn $q^{\frac{p-1}{n}} \equiv 1(p)$. Das Frobeniuselement φ_q existiert in $G = Gal(\mathbb{Q}(\omega_p)|\mathbb{Q})$, da p und q teilerfremd sind. Ist dann $f = f_q$ der Trägheitsindex von q in der Erweiterung, so gilt f ist minimal mit der Eigenschaft, dass $\varphi_q^f = 1$. Das heißt aber f ist minimal mit der Eigenschaft $q^f \equiv 1(p)$. Aus dieser Überlegung folgt:

$$q \text{ ist } n\text{-ter Potenzrest modulo } p \Leftrightarrow f|\frac{p-1}{n} \Leftrightarrow n|\frac{p-1}{f}$$

Da q unverzweigt ist, gilt zudem $\frac{p-1}{f} = g$. Dies zeigt also $n|g$. Da die Galoisgruppe

$$Gal(\mathbb{Q}(\omega_p)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$$

zyklisch ist, gibt es genau eine Untergruppe der Ordnung $\frac{p-1}{n}$. Das bedeutet, es gibt genau einen Körper L mit $[L : \mathbb{Q}] = n$. Die Tatsache, dass n den Zerlegungsindex g teilt, ist damit gleichbedeutend, dass q in L vollständig zerlegt ist. Dies folgt aus der Multiplikativität der Trägheits-, Verzweigungs- und Zerlegungsindizes in Körpertürmen. □

Korollar 2.13 (Quadratisches Reziprozitätsgesetz)**.** *Wir betrachten den Fall $n = 2$ und $K = \mathbb{Q}$. Das Quadratische Symbol für $a \in \mathbb{Z}$ wird durch*

$$\left(\frac{a}{p}\right) := \left(\frac{a}{(p)}\right)_{\mathbb{Q},2}$$

definiert, wobei $2 \neq p \in \mathbb{P}$ *der eindeutige positive Erzeuger des Primideals* (p) *ist. Sind jetzt* p *und* q *Primzahlen mit* $p \neq q \neq 2$*, so gilt*

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

Beweis: Betrachte wieder die Körper $\mathbb{Q}(\omega_p)|L|\mathbb{Q}$, wobei L der wohlbestimmte quadratische Körper in dieser Erweiterung ist. Da nur die Primzahl p selbst verzweigt, darf auch in L nur p verzweigen. Um die wohlbestimmte quadratische Teilerweiterung L zu finden, müssen wir also die wohlbestimmte quadratische Erweiterung von $\mathbb{Q}$ finden, die nur genau in p verzweigt ist. Diese geben wir einfach an. Ist $p \equiv 1(4)$, so ist ein Minimalpolynom des Ganzheitsrings O_L

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

Man beachte, dass $\frac{1-p}{4}$ eine ganze Zahl ist. Die Diskriminante dieses Polynoms ist gerade p also nur verzweigt in p. Dies zeigt, dass $L = \mathbb{Q}(\sqrt{p})$ und $O_L = Z[\frac{1-\sqrt{p}}{2}]$. Ist $p \equiv 3(4)$, so ist ein Minimalpolynom von O_L

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

mit Diskriminante $-p$. Wieder ist $\frac{1+p}{4}$ eine ganze Zahl. Dies zeigt, dass $L = \mathbb{Q}(\sqrt{-p})$ und $O_L = \mathbb{Z}[\frac{1-\sqrt{-p}}{2}]$. Insgesamt haben wir also $L = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$. Es gilt jetzt:

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 \quad &\Leftrightarrow \\ q \text{ zerfällt vollständig in } L \quad &\Leftrightarrow \\ (-1)^{\frac{p-1}{2}}p \text{ ist ein Quadrat modulo } q \quad &\Leftrightarrow \quad \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1 \end{aligned}$$

Da das Quadratische Symbol nur zwei Werte annimmt ist dann

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

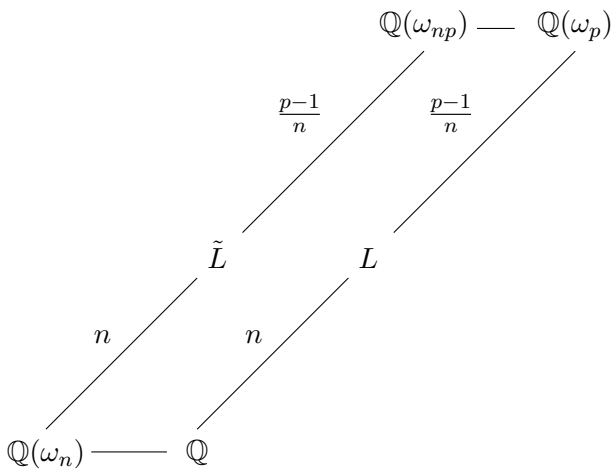
□

Bemerkung 2.14. Um mögliche Beweise für andere Reziprozitätsgesetze zu finden, nehmen wir uns wieder eine natürliche Zahl n, und betrachten die Erweiterungen $\mathbb{Q}(\omega_n)|\mathbb{Q}$, $\mathbb{Q}(\omega_p)|\mathbb{Q}$ mit einer Primzahl $p \nmid n$ und $p \equiv 1(n)$. Da die Primzahl p in $\mathbb{Q}(\omega_p)$ vollverzweigt und in $\mathbb{Q}(\omega_n)$, wegen $p \nmid n$, unverzweigt bleibt, sind $\mathbb{Q}(\omega_p)$ und $\mathbb{Q}(\omega_n)$ linear disjunkt. Deshalb ist insbesondere $\mathbb{Q}(\omega_n)\mathbb{Q}(\omega_p) = \mathbb{Q}(\omega_{np})$. Wegen $n|p-1$ gibt es wohlbestimmte Teilkörper $L, \tilde{L}$ mit

$$\mathbb{Q}(\omega_p)|L|\mathbb{Q} \text{ und } \mathbb{Q}(\omega_{np})|\tilde{L}|\mathbb{Q}(\omega_n)$$

sowie

$$[\tilde{L} : \mathbb{Q}(\omega_n)] = [L : \mathbb{Q}] = n.$$



Da jetzt die Galoisgruppen der Erweiterungen $\mathbb{Q}(\omega_p)|\mathbb{Q}$ bzw. $\mathbb{Q}(\omega_{np})|\mathbb{Q}(\omega_n)$ zyklisch sind, müssen auch die Teilerweiterungen $L|\mathbb{Q}$ bzw. $\tilde{L}|\mathbb{Q}(\omega_n)$ zyklisch sein. Die Erweiterung $\tilde{L}|\mathbb{Q}(\omega_n)$ ist folglich eine Kummererweiterung. Es gibt also ein $\mu \in \mathbb{Q}(\omega_n)$, sodass

$$\tilde{L} = \mathbb{Q}(\omega_n)(\sqrt[n]{\mu}).$$

Sei jetzt $p \neq q \in \mathbb{P}$ mit $q \equiv 1(n)$ und $\mathfrak{q}|q$ ein Primideal in $\mathbb{Q}(\omega_n)$. Dann gilt q zerfällt in L vollständig genau dann, wenn $\mathfrak{q}$ in $\tilde{L}$ vollständig zerfällt. Denn wegen der Bedingung $q \equiv 1(n)$ ist q vollständig zerlegt in $\mathbb{Q}(\omega_n)|\mathbb{Q}$. Das heißt der Zerlegungskörper von q in der Erweiterung $\mathbb{Q}(\omega_n)|\mathbb{Q}$ ist $\mathbb{Q}(\omega_n)$. Der Zerlegungskörper von q in $\mathbb{Q}(\omega_{np})|\mathbb{Q}$ setzt sich aus dem Zerlegungskörper von q in $\mathbb{Q}(\omega_p)|\mathbb{Q}$ und aus dem Zerlegungskörper von q in $\mathbb{Q}(\omega_n)|\mathbb{Q}$ zusammen. Dies ist eine direkte Folgerung aus der Tatsache, dass alle Teilkörper von $\mathbb{Q}(\omega_p)|\mathbb{Q}$ und $\mathbb{Q}(\omega_n)|\mathbb{Q}$ linear disjunkt sind und, dass sich Zerlegungsindizes multiplikativ in Körpertürmen verhalten. Folglich ist der Zerlegungskörper von q in $\mathbb{Q}(\omega_{np})|\mathbb{Q}$ gleich dem Zerlegungskörper von $\mathfrak{q}$ in $\mathbb{Q}(\omega_{np})|\mathbb{Q}(\omega_n)$. Dies ist gleichbedeutend dazu, dass die Zerlegungsgruppen $Z(q)$ und $Z(\mathfrak{q})$, der Galoisgruppen $Gal(\mathbb{Q}(\omega_{np})|\mathbb{Q}(\omega_n))$ und $Gal(\mathbb{Q}(\omega_p)|\mathbb{Q})$, isomorph sind. Weiter gilt, ein Element in $\mathfrak{q}$ zerfällt in $\tilde{L}$ genau dann, wenn μ ein n-ter Potenzrest modulo $\mathfrak{q}$ ist. Wir können also schreiben:

$$q \text{ ist } n\text{-ter Potenzrest modulo } p \Leftrightarrow \left(\frac{\mu}{\mathfrak{q}}\right) = 1$$

Dies verallgemeinert einen Beweis des Quadratischen Reziprozitätsgesetzes, liefert aber kein vergleichbares Reziprozitätsgesetz für n-te Potenzreste. Die Probleme sind dabei, dass (μ) natürlich eine Primfaktorzerlegung hat, die von allen Primidealen über p abhängt und vorallem, dass das Potenzrestsymbol mehr als zwei Werte annimmt.

3 Charaktere, Gaußsummen und Jacobisummen

Definition/Proposition 3.1. *Sei G eine endliche abelsche Gruppe. Ein Charakter χ ist eine Gruppenhomomorphismus*

$$\chi : G \to \mathbb{C}^*.$$

Die Menge aller Charaktere X_G bildet eine Gruppe mit punktweiser Multiplikation. Es gilt $X_G \cong G$ als Gruppen.

Beweis: Dass X_G eine Gruppe bildet ist klar! Es bleibt also die Isomorphie der beiden Gruppen zu zeigen. Nach dem Hauptsatz endlicher abelscher Gruppen, lässt sich G als direktes Produkt zyklischer Gruppen beschreiben. Ein Charakter auf G ist jetzt einfach als Produkt der Charaktere der zyklischen Komponenten von G gegeben. Es reicht also, die Behauptung nur für zyklische Gruppen zu zeigen. Wir nehmen also an G sei zyklisch mit Erzeuger g und $\#G = n$. Für ein beliebiges Element $\chi \in X_G$ gilt $1 = \chi(g^n) = \chi(g)^n$ dies zeigt also $\chi(g)$ ist eine n-te Einheitswurzel. Wir definieren χ_n durch $\chi_n(g) = \omega_n$, mit einer primitive Einheitswurzel ω_n. Desweiteren setzen wir χ_n auf beliebigen $h = g^k$ durch $\chi_n(h) = \chi_n(g)^k = \omega_n^k$ fort. Dann definiert χ_n einen Charakter auf G. Da ω_n eine primitive Einheitswurzel ist, erzeugt χ_n eine zyklische Untergruppe von X_G der Ordnung n. Wegen der Zyklizität von G ist ein Charakter schon durch das Bild von g festgelegt. Wir wissen bereits, dass für ein $\chi \in X_G$ $\chi(g)$ eine n-te Einheitswurzel sein muss. Von denen gibt es aber nur n viele, also ist auch $\#X(G) \leq n$. Somit haben wir gezeigt, dass $X(G)$ eine zyklische Gruppe der Ordnung n ist. Aus diesem Grund sind G und $X(G)$ zwangsläufig isomorph. □

Korollar 3.2. *Sei G eine endliche abelsche Gruppe mit $\#G = n$. Wir bezeichnen mit 1_G die Eins in G und mit 1_{X_G} die Eins in X_G, so gelten*

(i) $\sum_{g\in G} \chi(g) = \begin{cases} \#G, \text{ falls } \chi = 1_{X_G}, \\ 0, \text{ sonst.} \end{cases}$

(ii) $\sum_{\chi\in X_G} \chi(g) = \begin{cases} \#G, \text{ falls } g = 1_G, \\ 0, \text{ sonst.} \end{cases}$

(iii) $\chi(g) \in \mu_n, \forall g \in G \forall \chi \in X_G$.

Beweis:

(i) Ist $\chi = 1_{X_G}$, so ist die Aussage klar. Ist $\chi \neq 1$, so gibt es ein $a \in G$ mit $\chi(a) \neq 1$. Dann ist

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(ag) = \chi(a) \sum_{g\in G} \chi(g),$$

was nur sein kann, wenn $\sum_{g\in G} \chi(g) = 0$ ist.

(ii) Ist $g = 1_G$, so ist die Aussage wieder klar. Ist $g \neq 1$, so gibt es ein $\psi \in X_G$ mit $\psi(g) \neq 1$. Dies folgt aus der Isomorphie der beiden Gruppen. Weiter ist wieder

$$\sum_{\chi\in X_G} \chi(g) = \sum_{\chi\in X_G} \psi\chi(g) = \psi(g) \sum_{\chi\in X_G} \chi(g),$$

woraus wieder folgt, dass $\sum_{\chi\in X_G} \chi(g) = 0$.

(iii) Ist $g \in G$, so gilt $g^n = 1_G$. Deshalb ist $\chi(g)^n = 1$, also $\chi(g) \in \mu_n$. $\square$

Bemerkung 3.3. Wir betrachtet ab jetzt spezielle abelsche Gruppen. Dazu sei K ein algebraischer Zahlkörper, der die n-ten Einheitswurzeln beinhaltet. Weiter sei $\mathfrak{p} \subset O_K$ ein Primideal über einer Primzahl $p \in \mathbb{P}$ mit Trägheitsindex f. Dann ist

$$O_K/\mathfrak{p}O_K \cong \mathbb{F}_{p^f}$$

eine Körpererweiterung von $\mathbb{F}_p$ mit $q := p^f$ Elementen. Ist $G = Gal(\mathbb{F}_q|\mathbb{F}_p)$, so wird die Spur von $\mathbb{F}_q|\mathbb{F}_p$ definiert durch

$$\begin{aligned} Tr : \mathbb{F}_q &\longrightarrow \mathbb{F}_p \\ x &\longmapsto Tr(x) = \sum_{\sigma \in G} \sigma(x). \end{aligned}$$

Die Spur ist offensichtlich $\mathbb{F}_p$-linear. Ist weiter χ ein Charakter von $\mathbb{F}_q^*$, so setzen wir diesen auf $\mathbb{F}_q$ durch $\chi(0) = 0$ fort.

Definition 3.4. *In dieser Situation definieren wir*

(i) die Abbildung

$$\begin{aligned} \psi : \mathbb{F}_q &\longrightarrow \mathbb{C}^* \\ t &\longmapsto \omega_p^{Tr(t)}, \end{aligned}$$

die einen additiven Charakter der Gruppe $\mathbb{F}_q$ definiert und anschließend

(ii) mit einem multiplikativen Charakter χ die Gaußsumme

$$G_\alpha(\chi) = -\sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t).$$

Definition 3.5. *Sind χ_1 und χ_2 multiplikative Charakter von $\mathbb{F}_q$, so wird die Jacobisumme $J(\chi_1, \chi_2)$ definiert durch*

$$J(\chi_1, \chi_2) = -\sum_{t \in \mathbb{F}_q} \chi_1(t)\chi_2(1-t).$$

Proposition 3.6. *Seien jetzt $1 \neq \chi = \chi_1$ und χ_2 Charaktere der Ordnung $k \mid n$, d.h insbesondere $\chi_1^n = \chi_2^n = 1$. Weiter setzen wir voraus $\chi_1\chi_2 \neq 1$. Dann gelten*

1. $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$,
2. $J(\chi_1, \chi_2) \in \mathbb{Z}[\omega_n]$,
3. $G_\alpha(\chi) \in \mathbb{Z}[\omega_n, \omega_p]$,
4. $G_\alpha(\chi) = \chi(\alpha^{-1})G(\chi)$,
5. $G(\chi_1)G(\chi_2) = G(\chi_1\chi_2)J(\chi_1, \chi_2)$,
6. $\chi(-1)G(\chi^{-1}) = \overline{G(\chi)}$,

7. $G(\chi)G(\chi^{-1}) = \chi(-1)q$,
8. $G(\chi)\overline{G(\chi)} = q$,

wobei $G(\chi) := G_1(\chi)$.

Beweis:

1. Dies folgt aus der Tatsache, dass $t \mapsto 1-t$ bijektiv $\mathbb{F}_q$ nach $\mathbb{F}_q$ abbildet.
2. Dies ist wegen $\chi_1(a), \chi_2(a) \in \mathbb{Z}[\omega_n], \forall a \in \mathbb{F}_q$ klar.
3. Es gilt $\chi(a) \in \mathbb{Z}[\omega_n]$ und $\psi(a) \in \mathbb{Z}[\omega_p]$ für alle $a \in \mathbb{F}_q$ und deshalb ist die Behauptung klar.
4. Wir wissen $G_\alpha(\chi) = -\sum_{t\in\mathbb{F}_q} \chi(t)\psi(\alpha t)$. Lassen wir die Summe anstatt über t über $u = \alpha t$ laufen, so wird
$$G_\alpha(\chi) = -\sum_{t\in\mathbb{F}_q} \chi(t)\psi(\alpha t) = -\sum_{u\in\mathbb{F}_q} \chi(\alpha^{-1}u)\psi(u)$$
und es folgt
$$G_\alpha(\chi) = \chi(\alpha^{-1})(-\sum_{u\in\mathbb{F}_q} \chi(u)\psi(u)) = \chi(\alpha^{-1})G(\chi).$$
5. Es gilt
$$G(\chi_1)G(\chi_2) = \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q} \chi_1(a)\chi_2(b)\psi(a)\psi(b) = \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q} \chi_1(a)\chi_2(b)\psi(a+b).$$
Wir setzen jetzt $c = a + b$ und summieren über c und a, dies ändert nur etwas an der Summationsreihenfolge, aber nichts am Ergebnis. Es ist also
$$G(\chi_1)G(\chi_2) = \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q} \chi_1(a)\chi_2(b)\psi(a+b) = \sum_{a\in\mathbb{F}_q}\sum_{c\in\mathbb{F}_q} \chi_1(a)\chi_2(c-a)\psi(c).$$
Die Summation über c spalten wir auf in $c = 0$ und $c \neq 0$. Also wird $G(\chi_1)G(\chi_2) = A + B$, wobei wir
$$A = \sum_{a\in\mathbb{F}_q}\sum_{0\neq c\in\mathbb{F}_q} \chi_1(a)\chi_2(c-a)\psi(c) \text{ und } B = \sum_{a\in\mathbb{F}_q} \chi_1(a)\chi_2(-a)$$
setzen. Wir behandeln nun beide Ausdrücke getrennt. Ist $c \neq 0$, so ist die Zuordnung $t \mapsto ct$ bijektiv in $\mathbb{F}_q$ und wir können $a = ct$ setzen und anstatt über a über t summieren. Dies gibt
$$\begin{aligned}
A &= \sum_{a\in\mathbb{F}_q}\sum_{0\neq c\in\mathbb{F}_q} \chi_1(a)\chi_2(c-a)\psi(c) \\
&= \sum_{t\in\mathbb{F}_q}\sum_{0\neq c\in\mathbb{F}_q} \chi_1(ct)\chi_2(c-ct)\psi(c) \\
&= \sum_{t\in\mathbb{F}_q}\sum_{0\neq c\in\mathbb{F}_q} \chi_1(c)\chi_2(c)\chi_1(t)\chi_2(1-t)\psi(c) \\
&= \left(-\sum_{t\in\mathbb{F}_q} \chi_1(t)\chi_2(1-t)\right)\left(-\sum_{0\neq c\in\mathbb{F}_q} \chi_1(c)\chi_2(c)\psi(c)\right) \\
&= J(\chi_1,\chi_2)G(\chi_1\chi_2).
\end{aligned}$$

Für den Ausdruck B erhalten wir

$$B = \sum_{a\in\mathbb{F}_q} \chi_1(a)\chi_2(-a) = \chi_2(-1)\sum_{a\in\mathbb{F}_q} (\chi_1\chi_2)(a) = 0,$$

wobei die letzte Gleichheit wegen $\chi_1\chi_2 \neq 1$ gilt. Letztendlich also

$$G(\chi_1)G(\chi_2) = A = J(\chi_1,\chi_2)G(\chi_1\chi_2).$$

6. Durch einfaches Umformen erhalten wir

$$\begin{aligned}
\overline{G(\chi)} &= \overline{-\sum_{a\in\mathbb{F}_q} \chi(a)\psi(a)} \\
&= -\sum_{a\in\mathbb{F}_q} \overline{\chi(a)}\psi(-a) \\
&\overset{b=-a}{=} -\sum_{b\in\mathbb{F}_q} \overline{\chi(-b)}\psi(b) \\
&= -\chi(-1)\sum_{b\in\mathbb{F}_q} \overline{\chi(b)}\psi(b) \\
&= \chi(-1)G(\chi^{-1}).
\end{aligned}$$

Dabei wurde ausgenutzt, dass $\chi(-1) \in \{\pm 1\}$ und $\overline{\chi} = \chi^{-1}$ gilt.

7. Zuerst halten wir fest, dass die Zerlegung von $G(\chi_1)G(\chi_2) = A + B$ nicht von der Eigenschaft $\chi_1\chi_2 \neq 1$ Gebrauch gemacht hat. Dementsprechend müssen wir nur die Summanden A und B neu bestimmen, für die $G(\chi)G(\chi^{-1}) = A + B$ gilt. Es ist

$$B = \sum_{a\in\mathbb{F}_q} \chi(a)\chi^{-1}(-a) = \chi(-1)\sum_{a\in\mathbb{F}_q} (\chi\chi^{-1})(a) = \chi(-1)(q-1),$$

da der Summand für $a = 0$ wegfällt. Bei der Betrachtung von A spielte die Bedingung $\chi_1\chi_2 \neq 1$ auch keine Rolle. Wir brauchen also nur die Ausdrücke

$$-\sum_{0\neq c\in\mathbb{F}_q} \psi(c) \text{ und } -\sum_{t\in\mathbb{F}_q} \chi(t)\chi^{-1}(1-t)$$

betrachten. Wir erhalten

$$-\sum_{0\neq c\in\mathbb{F}_q} \psi(c) = \psi(0) = 1,$$

da

$$-\sum_{c\in\mathbb{F}_q} \psi(c) = 0$$

ist. Für den anderen Ausdruck halten wir zuerst fest, dass für $t \neq 1$, die Gleichheit $\chi^{-1}(1-t) = \chi((1-t)^{-1})$ gilt, wodurch wir

$$-\sum_{t\in\mathbb{F}_q} \chi(t)\chi^{-1}(1-t) = -\sum_{t\in\mathbb{F}_q-\{1\}} \chi(t(1-t)^{-1})$$

erhalten. Der Summand mit $t = 1$ verschwindet ohnehin. Setzen wir nun

$$u = t(1-t)^{-1},$$

so erhalten wir durch Umformen:

$$u = t(1-t)^{-1} \Leftrightarrow u - ut = t \Leftrightarrow t = u(1+u)^{-1}$$

Dies zeigt, die Abbildung $t \mapsto t(1-t)^{-1}$ bildet $\mathbb{F}_q - \{1\}$ bijektiv auf $\mathbb{F}_q - \{-1\}$ ab. Es folgt also

$$-\sum_{t \in \mathbb{F}_q - \{1\}} \chi(t(1-t)^{-1}) = -\sum_{u \in \mathbb{F}_q - \{-1\}} \chi(u) = \chi(-1).$$

Wir folgern die Behauptung, denn

$$G(\chi)G(\chi^{-1}) = A + B = \chi(-1)(q-1) + \chi(-1) = \chi(-1)q.$$

8. Dies ist eine leichte Folgerung:

$$G(\chi)\overline{G(\chi)} \overset{6.}{=} \chi(-1)G(\chi)G(\chi^{-1}) \overset{7.}{=} q$$

□

Korollar 3.7. *Sei jetzt χ ein Charakter n-ter Ordnung, d.h. $\chi^n = 1$, aber $\chi^k \neq 1$ für $k \leq n-1$. Es gilt dann*

$$G(\chi)^k = G(\chi^k) \prod_{i=1}^{k-1} J(\chi, \chi^i), \text{ für alle } 1 \leq k \leq n-1$$

und

$$G(\chi)^n = \chi(-1)q \prod_{i=1}^{n-2} J(\chi, \chi^i) \in \mathbb{Z}[\omega_n].$$

Beweis: Wir zeigen die erste Aussage per Induktion.
I.A. Für $k = 1$ ist die Behauptung klar.
I.V. Sei die Behauptung für $k-1$ mit $2 \leq k \leq n-1$ gezeigt.
I.S. Wir machen den Induktionsschritt von $k-1 \rightsquigarrow k$. Wir erhalten

$$G(\chi)^k = G(\chi)G(\chi)^{k-1} \overset{\text{I.V.}}{=} G(\chi)G(\chi^{k-1}) \prod_{i=1}^{k-2} J(\chi, \chi^i).$$

Nun nutzen wir die Relation 5. aus vorhergegangener Proposition aus. Es gilt dann nämlich

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

da $\chi\chi^{k-1} = \chi^k \neq 1$. Setzen wir dies ein, so ergibt sich

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

Dies zeigt die erste Gleichung. Die zweite Gleichung ist eine direkte Folgerung, denn

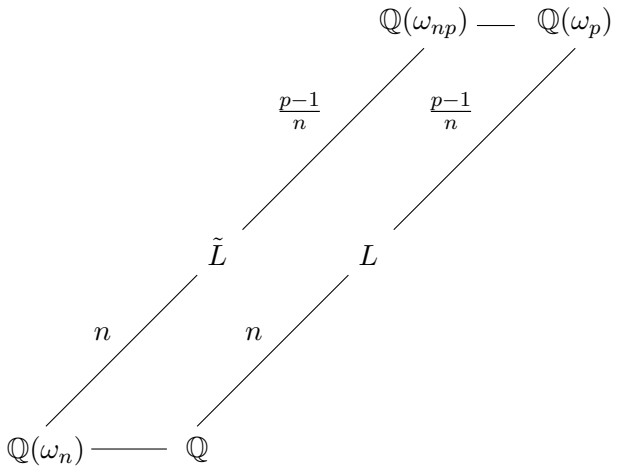
$$\begin{aligned} G(\chi)^n &= G(\chi)G(\chi)^{n-1} \\ &= G(\chi)G(\chi^{n-1})\prod_{i=1}^{n-2} J(\chi,\chi^i) \\ &= G(\chi)G(\chi^{-1})\prod_{i=1}^{n-2} J(\chi,\chi^i) \\ &= \chi(-1)q\prod_{i=1}^{n-2} J(\chi,\chi^i). \end{aligned}$$

Bei der letzten Gleicheit wird 7. aus der vorangegangenen Proposition verwendet. □

Bemerkung 3.8. Wenn wir den trivialen Charakter der multiplikativen Gruppe $\mathbb{F}_q^*$, $\chi = 1$, benutzen, macht es meist Sinn, auch diesen durch $\chi(0) = 0$ fortzusetzen. Wir sind im weiteren Vorgehen allerdings nicht wirklich an diesem Charakter interessiert, weshalb dieser Spezialfall außer Acht gelassen worden ist. Charaktere der Ordnung n sind gerade deshalb interessant, da das n-te Potenzrestsymbol einen solchen definiert. Sei nun K wieder ein algebraischer Zahlkörper, der die n-ten Einheitswurzeln enthält und weiter $\mathfrak{p} \subset O_K$ wieder ein Primideal. Wir fassen $O_K/\mathfrak{p}O_K \cong \mathbb{F}_q$ auf mit $q = p^f$ und $p \in \mathbb{P}$. Wir definieren dann

$$\chi(\alpha) := \left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}}(\mathfrak{p}).$$

Dies ist offensichtlich ein multiplikativer Charakter von $\mathbb{F}_q$. Durch die eindeutige Identifizierung der n-ten Einheitswurzeln in $\mathbb{F}_q$ und K können wir χ auch durch die Kongruenz rechts auffassen. Insbesondere zeigt es, dass $\chi^n = 1$ ist und somit χ eine Ordnung $k \mid n$ hat. Der Charakter χ hat aber auch exakt die Ordnung n, da für einen Erzeuger γ der Gruppe $\mathbb{F}_q^*$ die Zahl $\chi(\gamma)$ eine primitive n-te Einheitswurzel ist. Es gelten für χ also die vorangegangenen Aussagen über Charaktere. Speziell betrachten wir jetzt wieder $K = \mathbb{Q}(\omega_n)$ und das folgende Diagramm mit einer Primzahl $p \equiv 1(n)$ mit $\mathfrak{p} \mid p$. Dabei sind $L, \tilde{L}$ die wohlbestimmten Teilkörper der Erweiterungen $\mathbb{Q}(\omega_p)|\mathbb{Q}$ bzw. $\mathbb{Q}(\omega_{np})|\mathbb{Q}(\omega_p$ mit $[L:\mathbb{Q}] = [\tilde{L}:\mathbb{Q}] = n$.



Die Zahl $G(\chi) \in \mathbb{Z}[\omega_{np}]$ erzeugt eine Kummererweiterung von $\mathbb{Q}(\omega_n)$, da eben $G(\chi)^n \in \mathbb{Z}[\omega_n]$ gilt. Aus gleichem Grund gilt auch, dass $\mathbb{Q}(\omega_n, G(\chi))$ eine Teilerweiterung von $\tilde{L}|\mathbb{Q}(\omega_n)$ ist. Ist jetzt

$$\sigma_a \in Gal(\mathbb{Q}(\omega_{np})|\mathbb{Q}(\omega_n)) \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^*$$

zugehörig zu einem $a \in (\mathbb{Z}/p\mathbb{Z})^*$, sodass $\sigma_a(\omega_p) = \omega_p^a$. Dann gilt

$$\sigma_a(G(\chi)) = \sigma_a(-\sum_{t\in\mathbb{F}_q} \chi(t)\psi(t)) = -\sum_{t\in\mathbb{F}_q} \chi(t)\sigma_a(\psi(t)) = -\sum_{t\in\mathbb{F}_q} \chi(t)\psi(at) = G_a(\chi).$$

Wir wissen $G_a(\chi) = \overline{\chi(a)}G(\chi)$. Insbesondere ist $\sigma_a(G(\chi)) = G(\chi)$ genau dann, wenn a ein n-ter Potenzrest ist. Dies zeigt, dass $G(\chi)$ im Fixkörper der $\frac{p-1}{n}$ elementigen Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^*$ ist und diesen sogar erzeugt. Es ist also $\tilde{L} = \ mathbbQ(\omega_n, G(\chi))$. Wie schon erwähnt, liefert dies leider kein Reziprozitätsgesetz. Die Gaußsumme ist dennoch von enormer Bedeutung für den Beweis höherer Reziprozitätsgesetze.

Proposition 3.9. *Sei K ein algebraischer Zahlkörper und $\mathfrak{p} \subset O_K$ ein Primideal. Setzen wir $O_K/\mathfrak{p}O_K = K(\mathfrak{p})$, so gilt mit $1 \leq k \leq \mathcal{N}(\mathfrak{p}) - 1$*

$$\sum_{a\in K(\mathfrak{p})} a^k \equiv \begin{cases} 0(\mathfrak{p}), \text{ für } 1 \leq k \leq \mathcal{N}(\mathfrak{p}) - 2, \\ -1(\mathfrak{p}), \text{ für } k = \mathcal{N}(\mathfrak{p}) - 1. \end{cases}$$

Beweis: Wegen

$$a^{\mathcal{N}(\mathfrak{p})-1} \equiv 1(\mathfrak{p}) \text{ und } \mathcal{N}(\mathfrak{p}) - 1 \equiv -1(\mathfrak{p})$$

ist der Fall $k = \mathcal{N}(\mathfrak{p}) - 1$ direkt klar. Ist $1 \leq k \leq \mathcal{N}(\mathfrak{p}) - 2$, so gibt es ein $b \in K(\mathfrak{p})$ mit $b^k \not\equiv 1(\mathfrak{p})$. Es gilt dann

$$b^k \sum_{a\in K(\mathfrak{p})} a^k = \sum_{a\in K(\mathfrak{p})} (ab)^k \equiv \sum_{a\in K(\mathfrak{p})}^{p-1} a^k(\mathfrak{p}).$$

Dies zeigt

$$\sum_{a\in K(\mathfrak{p})} a^k \equiv 0(\mathfrak{p}).$$

□

Korollar 3.10. *Sei K ein algebraischer Zahlkörper, der die n-ten Einheitswurzeln beinhaltet und $\mathfrak{p} \subset O_K$ ein Primideal. Das n-te Potenzrestsymbol*

$$\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_{K,n}$$

definiert einen multiplikativen Charakter der Ordnung n auf $K(\mathfrak{p})^*$, wobei $K(\mathfrak{p}) = O_K/\mathfrak{p}O_K$ wie vorher ist. Seien $1 \leq a, b$ mit $(a, p) = (b, p) = 1$ und $a + b \leq n - 1$, so ist

$$J(\chi^a, \chi^b) \equiv 0(\mathfrak{p}).$$

Beweis: Dass χ einen multiplikativen Charakter von $K(\mathfrak{p})$ der Ordnung n definiert, haben wir bereits festgestellt. Wir berechnen also die Jacobisumme

$$J(\chi^a, \chi^b) = -\sum_{t \in K(\mathfrak{p})} \chi^a(t)\chi^b(1-t) \equiv -\sum_{t \in K(\mathfrak{p})} t^{a\frac{\mathcal{N}(\mathfrak{p})-1}{n}}(1-t)^{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}}(\mathfrak{p}).$$

Es ist weiter

$$(1-t)^{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}} = \sum_{k=0}^{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \binom{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}}{k}(-1)^k t^k,$$

und deshalb

$$\begin{aligned} J(\chi^a, \chi^b) &\equiv -\sum_{t \in K(\mathfrak{p})} t^{a\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \sum_{k=0}^{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \binom{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}}{k}(-1)^k t^k(\mathfrak{p}) \\ &\equiv -\sum_{k=0}^{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \binom{b\frac{\mathcal{N}(\mathfrak{p})-1}{n}}{k}(-1)^k \sum_{t \in K(\mathfrak{p})} t^{a\frac{\mathcal{N}(\mathfrak{p})-1}{n}+k}(\mathfrak{p}). \end{aligned}$$

Wegen $1 \leq a\frac{\mathcal{N}(\mathfrak{p})-1}{n} + k \leq a\frac{\mathcal{N}(\mathfrak{p})-1}{n} + b\frac{\mathcal{N}(\mathfrak{p})-1}{n} = (a+b)\frac{\mathcal{N}(\mathfrak{p})-1}{n} \leq \mathcal{N}(\mathfrak{p}) - 2$ ist dann

$$\sum_{t \in K(\mathfrak{p})} t^{a\frac{\mathcal{N}(\mathfrak{p})-1}{n}+k} \equiv 0(\mathfrak{p}) \text{ also auch } J(\chi^a, \chi^b) \equiv 0(\mathfrak{p}).$$

□

Bemerkung 3.11. Während in den anderen Formeln für die Gauß- und Jacobisummen der Körper nur als Isomorphieklasse $\mathbb{F}_q$ benötigt wurde, wird in den letzten Formeln der Körper in der bestimmten Form $K(\mathfrak{p})$ benutzt. Dies liegt daran, dass in dem Körper wirklich die Kongruenz mod $\mathfrak{p}$ wichtig ist. Es zeigt nämlich die wichtige Eigenschaft, dass das Ideal, welches von der Jacobisumme erzeugt wird, durch das Ideal $\mathfrak{p}$ teilbar ist und nicht zwangsläufig auch durch andere Primideale über p. Wegen

$$G(\chi)^n = \chi(-1)q\prod_{i=1}^{n-2} J(\chi, \chi^i) \in \mathbb{Z}[\omega_n],$$

erhalten wir zudem, dass $\mathfrak{p}^{(f\cdot g+n-2)} \mid (G(\chi)^n)$, wobei f der Trägheitsindex und g der Verzweigungsindex von p ist.

4 Das Kubische Reziprozitätsgesetz

Bemerkung 4.1. Es sei ab jetzt $\omega := \omega_3$ eine (primitive) dritte Einheitswurzel. Das zugehörige Minimalpolynom ist $X^2 + X + 1$, d.h ω erfüllt $\omega^2 + \omega + 1 = 0$. Wir betrachten den zugehörigen algebraischen Zahlkörper $\mathbb{Q}(\omega)$ und dessen Ganzheitsring $\mathbb{Z}[\omega]$. Da das Minimalpolynom Grad 2 hat, ist dies eine Erweiterung vom Grad 2 über $\mathbb{Q}$ und wir können jedes $z \in \mathbb{Z}[\omega]$ durch $z = a + b\omega$, mit $a, b \in \mathbb{Z}$, darstellen. Die Galoisgruppe dieser Erweiterung ist isomorph zu $(\mathbb{Z}/3\mathbb{Z})^*$ und das nicht triviale Element in der Galoisgruppe ist σ_2, wobei dieses definiert ist durch $\sigma_2(\omega) = \omega^2$. Da $\mathbb{Q}(\omega)|\mathbb{Q}$ eine komplexe Erweiterung vom Grad 2 ist, ist σ_2 als komplexe Konjugation zu verstehen. Die Relativnorm $N(z) := N_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(z) = z\overline{z}$ ist positiv. Und weiter gilt

$$N(z) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

Da $\mathbb{Z}[\omega]$ zusätzlich ein Hauptidealring ist, lässt sich für ein Ideal $\mathfrak{z} = (z)$ die Relativnorm und die Absolutnorm gleichsetzen. Es gilt also

$$\mathcal{N}((z)) = N(z).$$

Wir wissen auch bereits, dass jedes Primideal $\neq (3)$ unverzweigt ist. Für das von 3 erzeugte Ideal in $\mathbb{Z}[\omega]$ gilt

$$(3) = ((1 - \omega))^2.$$

Im Folgenden werden wir das kubische Reziprozitätsgesetz herleiten. Der erste Schritt den wir machen ist einen bestimmten Erzeuger aus den Primidealen auszuwählen.

Definition/Proposition 4.2. *Ein $z = a + b\omega \in \mathbb{Z}[\omega]$ mit $N(z) \not\equiv 0(3)$ heißt **primär**, wenn $z \equiv \pm 1(3)$. Dies ist äquivalent dazu, dass $a \equiv \pm 1(3)$ und $b \equiv 0(3)$. Des weiteren erfüllt für ein beliebiges $z \in \mathbb{Z}[\omega]$ mit $N(z) \not\equiv 0(3)$ genau eine Zahl*

$$x \in \{z, -z, \omega z, -\omega z, \omega^2 z, -\omega^2 z\}$$

eine der Kongruenzen $x \equiv 1(3)$ oder $x \equiv -1(3)$ und dann genau eine dieser Kongruenzen.

Beweis: Da 3 in $\mathbb{Z}$ liegt und deshalb genau die Koeffizienten der $\mathbb{Z}$-Basisvektoren 1 und ω von $\mathbb{Z}[\omega]$ modulo 3 reduziert werden, ist die Äquivalenz von $z \equiv \pm 1(3)$ zu $a \equiv \pm 1(3)$ und $b \equiv 0(3)$ klar. Es gilt:

$$\begin{aligned} z &= a + b\omega \\ -z &= -a - b\omega \\ \omega z &= -b + (a - b)\omega \\ -\omega z &= b + (b - a)\omega \\ \omega^2 z &= (b - a) - a\omega \\ -\omega^2 z &= (a - b) + a\omega \end{aligned}$$

Wir wollen zeigen, dass eine dieser Zahlen kongruent zu 1 mod 3 ist. Die Fälle $a \equiv 1(3)$ und $b \equiv 2(3)$, $a \equiv 2(3)$ und $b \equiv 1(3)$, sowie $a \equiv b \equiv 0(3)$ können wir ausschließen, da dann $a^2 - ab + b^2 \equiv 0(3)$ wäre. Wenn $a \equiv b(3)$ gilt, so liefert eine der unteren vier Gleichungen eine Zahl mit Koeffizienten $a' \equiv 0(3)$ und $b' \equiv \pm 1(3)$ bzw. $a' \equiv \pm 1(3)$ und $b' \equiv 0(3)$. Es reicht also, die Behauptung für eine dieser beiden Fälle zu zeigen. Gilt letzteres, so sind wir fertig. Wäre $a \equiv 0(3)$ und $b \equiv \pm 1(3)$ so liefern die letzten beiden Gleichungen das Gewünschte. □

Bemerkung 4.3. Da sich die Erzeuger der Primideale in Hauptidealringen nur um Einheiten unterscheiden, können wir, um die Wahl des Erzeugers einzuschränken, diesen primär wählen. Wir werden später, anstatt das Primideal selbst im 3-ten Potenzrestsymbol zu verwenden, einfach primäre Erzeuger wählen. Dies ist vergleichbar mit dem quadratischen Fall, bei dem man den Erzeuger einfach durch die Eigenschaft größer Null eindeutig festlegt. Dabei ist hier zu beachten, dass die Wahl eines primären Erzeugers nicht wirklich eindeutig ist, da dieser eben eine der beiden Bedingungen $z \equiv 1(3)$ oder $z \equiv -1(3)$ erfüllen darf. Dies liefert aber im späteren Reziprozitätsgesetz keine Probleme, da eben $-1 = (-1)^3$ automatisch ein kubischer Rest ist. Wir bekommen die obige Aussage auch leichter, indem wir feststellen, dass ein Element z mit $N(z) \not\equiv 0(3)$ in $\mathbb{Z}[\omega]/3\mathbb{Z}[\omega]$ invertierbar ist. Es ist also $z \in (\mathbb{Z}[\omega]/3\mathbb{Z}[\omega])^*$. Für die Anzahl der Elemente gilt

$$\#((\mathbb{Z}[\omega]/3\mathbb{Z}[\omega])^*) = N(3) - N(1-\omega) = 9 - 3 = 6,$$

da eben

$$\mathbb{Z}[\omega]/3\mathbb{Z}[\omega] \cong \mathbb{Z}[\omega]/(1-\omega)^2\mathbb{Z}[\omega].$$

Dies zeigt, dass jedes Element z mit $N(z) \not\equiv 0(3)$ mit einer Einheit multipliziert genau einer der beiden Äquivalenzklassen 1 bzw. -1 in $\mathbb{Z}[\omega]/3\mathbb{Z}[\omega]$ entsprechen muss. Also eine einfache Folgerung aus der Tatsache, dass es sechs Einheiten gibt und auch sechs Äquivalenzklassen in $(\mathbb{Z}[\omega]/3\mathbb{Z}[\omega])^*$.

Korollar 4.4. *Sind $x, y \in \mathbb{Z}[\omega]$ primär, so sind auch xy und $\overline{x}$ primär.*

Beweis: Dies ist wegen der Kongruenzbedingungen direkt klar. □

Proposition 4.5. *Ist $3 \neq p \in \mathbb{P}$, so ist (p) für $p \equiv 2(3)$ träge und für $p \equiv 1(3)$ vollständig zerfallend. Wir schreiben für zerfallendes p dann $p = \pi\overline{\pi}$.*

Beweis: Da $p \neq 3$ unverzweigt ist, gibt es ein Frobeniuselement φ_p in $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$. Dieses Frobeniuselement setzt eine 3-te Einheitswurzel in die p-te Potenz. Für das Potenzieren von 3-ten Einheitswurzeln, ist aber nur die Restklasse der Potenz modulo 3 von Bedeutung. Ist $p \equiv 1(3)$, so ist das Frobeniuselement trivial, also auch die Zerlegungsgruppe. D.h. p zerfällt vollständig. Ist $p \equiv 2(3)$, so erzeugt φ_p die Galoisgruppe, d.h. Zerlegungsgruppe und Galoisgruppe stimmen überein. Dementsprechend ist p dann träge. □

Definition 4.6. *Sei π ein Erzeuger des Primideals (π). Wir definieren das Kubische Symbol durch*

$$\chi_\pi(t) := \left(\frac{t}{\pi}\right) := \left(\frac{t}{(\pi)}\right)_{\mathbb{Q}(\omega),3}.$$

Für beliebige Ideale $\mathfrak{z}$ mit Erzeugern z lässt sich dieses Symbol durch Multiplikation fortsetzen und wir erhalten

$$\left(\frac{t}{z}\right) := \left(\frac{t}{\mathfrak{z}}\right)_{\mathbb{Q}(\omega),3}.$$

Proposition 4.7. *Ist z in $\mathbb{Z}[\omega]$, so gelten*

1. $\overline{\chi_z(t)} = \chi_{\overline{z}}(\overline{t})$,
2. $\overline{\chi_z(t)} = \chi_z(t)^2$.

Beweis: Es reicht, diese Behauptungen für Primzahlen $z = \pi$ zu beweisen.

1. Ist $\chi_\pi(t) = \zeta$ eine 3-te Einheitswurzel, so gilt

$$\zeta = t^{\frac{N(\pi)-1}{3}} + k\pi$$

mit einem $k \in \mathbb{Z}[\omega]$. Dann ist

$$\overline{\zeta} = \overline{t}^{\frac{N(\pi)-1}{3}} + \overline{k}\overline{\pi},$$

also

$$\overline{\chi_\pi(t)} = \chi_{\overline{\pi}}(\overline{t}).$$

2. Da $\chi_\pi(t)$ eine 3-te Einheitswurzel ist, entspricht die komplexe Konjugation gerade dem Quadrieren.

□

Proposition 4.8. *Sei $\pi \equiv 1(3)$ eine primäre Primzahl in $\mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi}$. Dann definiert $\chi := \chi_\pi$ einen Charakter auf $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ und es gilt*

$$G(\chi)^3 = \pi^2\overline{\pi}$$

und

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

Beweis: Wir wissen

$$G(\chi)^3 = \chi(-1)pJ(\chi, \chi) = pJ(\chi, \chi).$$

Außerdem haben wir auch noch

$$G(\chi)\overline{G(\chi)} = |G(\chi)|^2 = p.$$

Betrachten wir den Absolutbetrag der ersten Gleichung, so ergibt sich

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

Dies zeigt also insbesondere $|J(\chi, \chi)| = \sqrt{p}$. Da jetzt schon $\pi \mid J(\chi, \chi)$ reicht es zu zeigen, dass $J(\chi, \chi)$ primär ist. Wir erhalten durch weitere Umformungen:

$$\begin{aligned} J(\chi, \chi) \equiv G(\chi)^3 &= \left(-\sum_{t \neq 0} \chi(t)\psi(t) \right)^3 \\ &\equiv -\sum_{t \neq 0} \chi^3(t)\psi(3t) \\ &= -\sum_{t \neq 0} \psi(3t) \\ &= 1 \end{aligned}$$

Dabei sind die Kongruenzen immer modulo 3 zu lesen. Dies zeigt also

$$J(\chi, \chi) = \pi$$

und damit auch

$$G(\chi)^3 = p\pi.$$

□

Satz 4.9 (Kubisches Reziprozitätsgesetz)**.** *Sind $\alpha, \beta \in \mathbb{Z}[\omega]$ primär, so gilt*

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

Beweis: Es reicht, die Relation für Primzahlen in $\mathbb{Z}[\omega]$ zu zeigen, da der Rest aus der Multiplikativität des Symbols folgt. Sindπ, λ diese Primzahlen, so zeigen wir $\chi_\pi(\lambda) = \chi_\lambda(\pi)$.

1.Fall: Seien $\lambda = q \in \mathbb{P}$ und $\pi = p \in \mathbb{P}$ bereits Primzahlen in $\mathbb{Z}$ die träge in $\mathbb{Q}(\omega) \mid \mathbb{Q}$ sind. Dann gilt

$$\chi_p(q)^2 = \overline{\chi_p(q)} = \chi_{\overline{p}}(\overline{q}) = \chi_p(q)$$

und deshalb, da $\chi_p(q)$ eine dritte Einheitswurzel ist,

$$\chi_p(q) = 1 = \chi_q(p).$$

2.Fall: Sei jetzt $p \in \mathbb{P}$ mit $p = \pi\overline{\pi}$ mit primärem π und o.B.d.A. $\pi \equiv 1(3)$, ansonsten ersetzte π durch $-\pi$. Weiter sei wie im letzten Fall $\lambda = q \in \mathbb{P}$, also insbesondere $\lambda = q \equiv 2(3)$. Wir wollen die Wirkung des Frobeniuselements φ_q auf $G(\chi)$ ausnutzen. Setzen wir nun $\chi := \chi_\pi$, so gilt:

$$\begin{aligned}
(-G(\chi))^q = -G(\chi)^q &\equiv \sum_{t\neq 0} \chi(t)^q \psi(qt) \\
&= \sum_{t\neq 0} \chi(t)^2 \psi(qt) \\
&= \sum_{t\neq 0} \overline{\chi(q^{-1}t)}\psi(t) \\
&= -\chi(q)G(\overline{\chi})
\end{aligned}$$

Dabei sind die auftretenden Kongruenzen modulo q zu betrachten. Jetzt ist wegen $\chi(-1) = 1$ auch

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

Dies zeigt also

$$G(\chi)^{q+1} \equiv \chi(q)G(\chi)\overline{G(\chi)} = \chi(q)p.$$

Weiter ist jetzt $G(\chi)^{q+1} = (\pi^2\overline{\pi})^{\frac{q+1}{3}}$. Da q träge ist, entspricht das Frobeniuselement φ_q in der Galoisgruppe der komplexen Konjugation und es ist $\overline{\pi} \equiv \pi^q$. Es gilt weiter

$$G(\chi)^{q+1} = (\pi^2\overline{\pi})^{\frac{q+1}{3}} \equiv (\pi^{q+2})^{\frac{q+1}{3}} \equiv \chi_\pi(q)\pi^{q+1}$$

oder äquivalent dazu

$$\chi_\pi(q) \equiv \pi^{\frac{q^2+3q+2-3q-3}{3}} = \pi^{\frac{q^2-1}{3}} \equiv \chi_q(\pi).$$

3.Fall: Seien jetzt $p, q \in \mathbb{P}$ mit $q \neq p$ und $p \equiv q \equiv 1(3)$ zerfallen in $\mathbb{Q}(\omega) \mid \mathbb{Q}$. Wir zerlegen dann $p = \pi\overline{\pi}$ und $q = \lambda\overline{\lambda}$ mit primären π, λ und wir nehmen zusätzlich wieder o.B.d.A. $\pi \equiv 1(3)$ an. Wir betrachten erneut die Wirkung des Frobeniuselements φ_q, und alle

auftretenden Kongruenzen sind modulo λ zu verstehen. Es gilt dann mit der Bezeichnung $\chi := \chi_\pi$:

$$\begin{aligned}(-G(\chi))^q = -G(\chi)^q &\equiv \sum_{t\neq 0}\chi(t)^q\psi(qt)\\ &= \sum_{t\neq 0}\chi(t)\psi(qt)\\ &= \sum_{t\neq 0}\chi(q^{-1}t)\psi(t)\\ &= -\chi(q^{-1})G(\chi)\end{aligned}$$

Es ist wieder $\overline{G(\chi)} = G(\overline{\chi})$ und weiter $G(\chi)\overline{G(\chi)} = p$. Wegen $p \neq q$ ist p modulo λ invertierbar und wir erhalten $G(\chi)^{-1} \equiv G(\overline{\chi})p^{-1}$. Wir können also auch

$$G(\chi)^q \equiv \chi(q)^{-1}G(\chi)$$

äquivalent zu

$$G(\chi)^{q-1} \equiv \chi(q)^{-1} = \chi(q)^2$$

umformen. Durch die Berechnung der Gaußsumme erhalten wir zudem $G(\chi)^{q-1} = (\pi^2\overline{\pi})^{\frac{q-1}{3}}$. Also insgesamt

$$\chi_\pi(q)^2 \equiv (\pi^2\overline{\pi})^{\frac{q-1}{3}} \equiv \chi_\lambda(\pi^2\overline{\pi}).$$

Indem wir die Rollen von λ und π vertauschen, erhalten wir

$$\chi_\lambda(p)^2 = \chi_\pi(\lambda^2\overline{\lambda}).$$

Multiplizieren wir die beiden Gleichungen so ergibt sich

$$\chi_\lambda(\pi^2\overline{\pi})\chi_\lambda(p)^2 = \chi_\pi(\lambda^2\overline{\lambda})\chi_\pi(q)^2.$$

Zuerst die linke Seite:

$$\begin{aligned}\chi_\lambda(\pi^2\overline{\pi})\chi_\lambda(p)^2 &= \chi_\lambda(\pi^2\overline{\pi})\chi_\lambda(\pi^2\overline{\pi^2})\\ &= \chi_\lambda(\pi^4)\chi_\lambda(\overline{p\imath}^3)\\ &= \chi_\lambda(\pi)\end{aligned}$$

Und jetzte die rechte Seite:

$$\begin{aligned}\chi_\pi(\lambda^2\overline{\lambda})\chi_\pi(q)^2 &= \chi_\pi(\lambda^2\overline{\lambda})\chi_\pi(\lambda^2\overline{\lambda^2})\\ &= \chi_\pi(\lambda^4)\chi_\pi(\overline{\lambda}^3)\\ &= \chi_\pi(\lambda)\end{aligned}$$

Es gilt also letztendlich

$$\chi_\lambda(\pi) = \chi_\pi(\lambda).$$

4.Fall: Für den letzten Fall muss $p = q \in \mathbb{P}$ sein und dementsprechend $\overline{\pi} = \lambda$. Wir rechnen dazu kurz:

$$\begin{aligned}\chi_\pi(\overline{\pi}) &= \chi_\pi(\overline{\pi}+\pi)\\ &= \chi_{\pi+\overline{\pi}}(\pi)\\ &= \chi_{\pi+\overline{\pi}}(-\overline{\pi})\\ &= \chi_{\overline{\pi}}(\pi+\overline{\pi})\\ &= \chi_{\overline{\pi}}(\pi)\end{aligned}$$

Dabei wurde das Reziprozitätsgesetz im 1.Fall, 2.Fall und 3.Fall ausgenutzt mit der Tatsache, dass $\overline{\pi} + \pi \in \mathbb{Z}$ primär ist. Des weiteren wurde die Eigenschaft ausgenutzt, dass man bei $\chi_\pi(\lambda)$ das Argument λ modulo π reduzieren kann. □

Korollar 4.10 (Ergänzungssätze zum Kubischen Reziprozitätsgesetz)**.** *Sei $\alpha \in \mathbb{Z}[\omega]$ primär und sei $\alpha \equiv 1(3)$. Wir setzen $\alpha = a + b\omega$, mit $a \equiv 1(3)$ und $b \equiv 0(3)$. Es gilt dann*

(i) $\chi_\alpha(\omega) = \omega^{\frac{1-a-b}{3}}$,

(ii) $\chi_\alpha(1-\omega) = \omega^{\frac{a-1}{3}}$,

(iii) $\chi_\alpha(3) = \omega^{\frac{b}{3}}$.

Beweis: Wir zeigen diese Aussagen jeweils für $b = 0$ und $b \neq 0$.

(i) Ist $b = 0$, so gilt

$$\chi_\alpha(\omega) = \omega^{\frac{a^2-1}{3}} = \omega^{(a+1)\frac{a-1}{3}} = \omega^{2\frac{a-1}{3}} = \omega^{\frac{1-a}{3}}.$$

Dabei gilt die letzte Gleichung wegen $a + 1 \equiv 2 \equiv -1(3)$.
Sei nun allgemeiner

$$\chi_\alpha(\omega) = \omega^{\frac{a^2-ab+b^2-1}{3}}.$$

Wir halten fest $a - 1 \equiv 0(3)$ und $b \equiv 0(3)$ und somit

$$ab - b = (a-1)b \equiv 0(9),$$

$$a^2 - 2a + 1 = (a-1)^2 \equiv 0(9)$$

und

$$b^2 \equiv 0(9).$$

Dies zeigt dann

$$a^2 - ab + b^2 - 1 \equiv 2a - 2 - b(9),$$

durch das Einsetzen der obigen Identitäten. Also auch

$$\frac{a^2 - ab + b^2 - 1}{3} \equiv \frac{2a - 2 - b}{3} \equiv \frac{1 - a - b}{3}(3)$$

und deshalb

$$\chi_\alpha(\omega) = \omega^{\frac{1-a-b}{3}}.$$

(ii),(iii) Die beiden anderen Identitäten zeigen wir parallel. Sei zuerst $b = 0$. Dann gilt

$$\chi_\alpha(3) = \overline{\chi_\alpha(3)} = \chi_\alpha(3)^2,$$

also insbesondere auch

$$\chi_\alpha(3) = 1.$$

Wir wissen bereits

$$(1-\omega)^2 = -3\omega.$$

Dies zeigt

$$\chi_\alpha(1-\omega)^2 = \chi_\alpha(3)\chi_\alpha(\omega) = \chi_\alpha(\omega) = \omega^{\frac{1-a}{3}},$$

also durch Quadrieren

$$\chi_\alpha(1-\omega) = \omega^{\frac{a-1}{3}}.$$

Wir führen nun die Berechnung von $\chi_\alpha(1-\omega)$ für beliebiges $\alpha \in \mathbb{Z}[\omega]$ mit $\alpha \equiv 1(3)$ zurück auf den Fall $b = 0$. Durch Ausnutzen des Reziprozitätsgesetzes berechnet man:

$$\begin{aligned}\chi_\alpha(1-\omega)^2 = \chi_\alpha(-3\omega) &= \chi_\alpha(\alpha - 3\omega)\\ &= \chi_{\alpha-3\omega}(\alpha)\\ &= \chi_{\alpha-3\omega}(3\omega)\end{aligned}$$

Dies zeigt, dass wir α um ganzzahlige Vielfache von 3ω reduzieren können. Da jetzt $b \equiv 0(3)$ nach Voraussetzung gilt, haben wir die Berechnung von $\chi_\alpha(1-\omega)$ auf den Fall $b = 0$ zurückgeführt. Es bleibt also noch die Berechnung von $\chi_\alpha(3)$ für beliebige α wie oben. Es ist

$$3 = -\omega^2(1-\omega)^2$$

und deshalb

$$\chi_\alpha(3) = \chi_\alpha(\omega)^2\chi_\alpha(1-\omega)^2 = \omega^{\frac{1-a+a+b-1}{3}} = \omega^{\frac{b}{3}}.$$

□

5 Das Biquadratische Reziprozitätsgesetz

Bemerkung 5.1. Wir definieren nun im klassischen Sinne eine primitive 4-te Einheitswurzel mit $\omega_4 = i$. Das Minimalpolynom ist dann $X^2 + 1$ und die entsprechende Erweiterung vom Grad 2 ist $\mathbb{Q}(i)$ mit Ganzheitsring $\mathbb{Z}[i]$. Die Zahl i erfüllt die Gleichung $i^2 = -1$ und jedes $z \in \mathbb{Z}[i]$ lässt sich durch $z = a + bi$ darstellen. Die Galoisgruppe dieser Erweiterung ist $(\mathbb{Z}/4\mathbb{Z})^*$ und das nichttriviale Element ist σ_3, wobei σ_3 durch $\sigma_3(i) = i^3 = -i$ eindeutig definiert ist. Diese Erweiterung ist komplex, weshalb wir σ_3 als komplexe Konjugation auffassen können. Dies liefert uns wiederum, dass die Relativnorm $N(z) := N_{\mathbb{Q}}^{\mathbb{Q}(i)}(z) = z\overline{z}$ positiv ist. Die Relativnorm von einem Element $z = a + bi$ ist gegeben durch

$$N(z) = (a + bi)(a - bi) = a^2 + b^2.$$

Der Ring $\mathbb{Z}[i]$ ist euklidisch, also insbesondere auch ein Hauptidealring, weshalb hier für ein Ideal $\mathfrak{z} = (z)$ wieder

$$\mathcal{N}((z)) = N(z)$$

gilt. Die verzweigten Primideale dieser Erweiterung müssen Teiler von 4 sein, weshalb nur das Ideal über 2 verzweigt. Für dieses gilt

$$(2) = ((1 - i))^2.$$

Es soll jetzt in gleicher Manier wie im kubischen Fall der Grundstein für das Biquadratisches Reziprozitätsgesetz gelegt werden.

Definition/Proposition 5.2. *Ein Element $z = a + bi \in \mathbb{Z}[i]$ mit $N(z) \not\equiv 0(2)$ heißt **primär**, wenn $z \equiv 1(mod\ 2 + 2i) =: 1((2 + 2i))$. Dies ist äquivalent zu $a - b \equiv 1(4)$ und $b \equiv 0(2)$. Für ein beliebiges $z \in \mathbb{Z}[i]$ mit $N(z) \not\equiv 0(2)$ gibt es genau ein*

$$x \in \{z, -z, iz, -iz\},$$

welches primär ist.

Beweis: Sei jetzt z primär. Wegen $a^2 + b^2 \not\equiv 0(2)$ muss $a \not\equiv b(2)$ gelten. Angenommen $a \equiv 0(2)$ und $b \equiv 1(2)$, so ist $z \equiv i(2)$. Das würde bedeuten, es gibt ein $k \in \mathbb{Z}[i]$, sodass $i + k \cdot (2 + 2i) = 1$, Widerspruch! Es ist also $a \equiv 1(2)$ und $b \equiv 0(2)$. Da $\frac{b}{2} \in \mathbb{Z}$ gilt

$$a + bi \equiv a + bi - \frac{b}{2} \cdot (2 + 2i) \equiv a - b((2 + 2i)).$$

Dies bedeutet wiederum $a - b \equiv 1((2+2i))$, also auch $a - b \equiv 1(4)$, wegen $a, b \in \mathbb{Z}$. Sei jetzt umgekehrt $a - b \equiv 1(4)$ und $b \equiv 0(2)$ und betrachte $z = a + bi$. Wegen $a - b \equiv 1(4)$ muss auch schon $a - b \equiv 1((2 + 2i))$ gelten, weshalb wieder wegen $\frac{b}{2} \in \mathbb{Z}$ auch $z \equiv 1((2 + 2i))$ gilt. Dies zeigt, dass z genau dann primär ist, wenn die beiden Kongruenzen $b \equiv 0(2)$ und $a - b \equiv 1(4)$ erfüllt sind. Sei nun z mit $N(z) = a^2 + b^2 \not\equiv 0(2)$ beliebig, so können wir o.B.d.A. annehmen $b \equiv 0(2)$, ansonsten betrachte $iz = -b + ai$. Aus diesem Grund kann entweder $a - b \equiv 1(4)$ oder $a - b \equiv -1(4)$ gelten. Falls das Erste gilt sind wir fertig, falls Letzteres gilt, so erfüllt $-z$ das Gewünschte. □

Bemerkung 5.3. Die Definition eines primären Elements erlaubt es uns wie auch im kubischen Fall das Ideal durch seinen primären Erzeuger zu repräsentieren. Der kleine Unterschied ist hierbei, dass das primäre Element eindeutig festgelegt ist. Wir können

wieder durch Abzählen den obigen Beweis kürzer fassen. Ist nämlich $z \not\equiv 0(2)$, so gilt $z \in (\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i])^* \cong (\mathbb{Z}[i]/(1-i)^3\mathbb{Z}[i])^*$. Die vier Zahlen $z, -z, iz, -iz$ sind alle unterschiedlich in $(\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i])^*$ und wegen

$$\#((\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i])^*) = N(2+2i) - N((1+i)^2) = 8-4 = 4,$$

erfüllt genau eines die Kongruenz zu 1 modulo $2+2i$.

Korollar 5.4. *Sind $x, y \in \mathbb{Z}[i]$ primär, so sind auch xy und $\overline{x}$ primär.*

Beweis: Die Kongruenzbedingung impliziert dies wieder direkt. □

Proposition 5.5. *Ist $2 \neq p \in \mathbb{P}$ eine Primzahl, so ist p träge in $\mathbb{Q}(i) \mid \mathbb{Q}$, falls $p \equiv 3(4)$ und p zerfällt vollständig, wenn $p \equiv 1(4)$.*

Beweis: Wegen der Bedingung $2 \neq p$ ist p unverzweigt und das zugehörige Frobeniuselement φ_p exisitiert. Ist jetzt $p \equiv 1(4)$, so ist φ_p trivial und somit auch die Zerlegungsgruppe. Das heißt aber der Trägheitsindex ist 1 und p zerfällt vollständig in $\mathbb{Q}(i) \mid \mathbb{Q}$. Gilt $p \equiv 3(4)$, so erzeugt φ_p die gesamte Galoisgruppe und der Trägheitsindex ist 2. In diesem Fall bleibt p träge in $\mathbb{Q}(i) \mid \mathbb{Q}$. □

Definition 5.6. *Für einen Erzeuger π des Primideals (π) definieren wir das Biquadratische Symbol durch*

$$\chi_\pi(t) := \left(\frac{t}{\pi}\right) := \left(\frac{t}{(\pi)}\right)_{\mathbb{Q}(i),4}.$$

Dieses wird auf beliebigen Idealen $\mathfrak{z}$ mit Erzeugern z multiplikativ fortgesetzt und es ist

$$\left(\frac{t}{z}\right) := \left(\frac{t}{\mathfrak{z}}\right)_{\mathbb{Q}(i),4}.$$

Proposition 5.7. *Ist z in $\mathbb{Z}[i]$, so gelten*

1. $\overline{\chi_z(t)} = \chi_{\overline{z}}(\overline{t})$,
2. $\overline{\chi_z(t)} = \chi_z(t)^3$.

Beweis:

1. Dies zeigt man genau wie im kubischem Fall.
2. Der nichttriviale Automorphismus von $\mathbb{Q}(i) \mid \mathbb{Q}$ erhebt eine 4-te Einheitswurzel in die dritte Potenz. Dieser Automorphismus entspricht auch gleichzeitig der komplexen Konjugation. Da $\chi(t)$ eine 4-te Einheitswurzel ist, gilt somit $\overline{\chi_z(t)} = \chi_z(t)^3$.

□

Proposition 5.8. *Sei $p \in \mathbb{P}$ mit $p \equiv 1(4)$. Sei weiter $\pi \in \mathbb{Z}[i]$ primär mit $\pi\overline{\pi} = p$. Wir bezeichnen $\chi = \chi_\pi$. Dann ist*

$$J(\chi, \chi^2) = \chi(-1)J(\chi, \chi),$$

$$J(\chi, \chi) = \chi(-1)\pi$$

und

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

Beweis: Wir erhalten leicht

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

und somit

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

Weiter ist

$$G(\chi)^4 = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2),$$

wegen $p \equiv 1(4)$ und da somit p Trägheitsindex 1 hat. Da χ ein Charakter der Ordnung 4 ist, muss χ^2 ein Charakter der Ordnung 2 sein und wir erhalten zudem

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

Durch Einsetzen dieser Identitäten wird

$$J(\chi,\chi)^2 = \frac{G(\chi)^4}{G(\chi^2)^2} = \chi(-1)J(\chi,\chi)J(\chi,\chi^2)$$

und deshalb

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

Wir setzen nun $p = 2m-1$ mit einer natürlichen Zahl m und wir identifizieren $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ eindeutig mit $\mathbb{Z}/p\mathbb{Z}$. Es gilt dann

$$\begin{aligned} -J(\chi,\chi) &= \sum_{t=1}^{p-1} \chi(t)\chi(1-t) \\ &= \sum_{t=1}^{2m-2} \chi(t)\chi(1-t) \\ &= \sum_{t=1}^{m-1} \chi(t)\chi(1-t) + \chi(m)\chi(1-m) + \sum_{t=m+1}^{2m-2} \chi(t)\chi(1-t). \end{aligned}$$

Da χ in dieser Notation ein Charakter von $\mathbb{Z}/p\mathbb{Z}$ ist, können wir die Argumente von χ modulo p reduzieren. Es ist dann

$$1 - m \equiv 1 - m + 2m - 1 \equiv m(p)$$

und weiter sogar

$$1 - m - k \equiv 1 - m - k + 2m - 1 \equiv m - k(p).$$

Dies zeigt $\chi(m)\chi(1-m) = \chi(m)^2$ und

$$\sum_{t=m+1}^{2m-2} \chi(t)\chi(1-t) = \sum_{t=2}^{m-1} \chi(t)\chi(1-t) = \sum_{t=1}^{m-1} \chi(t)\chi(1-t).$$

Wir erhalten also

$$-J(\chi,\chi) = 2\sum_{t=1}^{m-1} \chi(t)\chi(1-t) + \chi(m)^2.$$

Wir untersuchen zunächst $\chi(m)^2$. Es gilt

$$\chi(1) = \chi(p+1) = \chi(2m) = \chi(2)\chi(m),$$

also insbesondere auch $\chi(m)^2 = \chi(2)^2 = \chi(4) = \chi(-(1+i)^4) = \chi(-1)$. Da der Körper $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ zwei Elemente hat, ist jede 4-te Einheitswurzel kongruent zu 1 modulo $1+i$. Dies zeigt $\chi(t) \equiv 1(mod\ 1+i)$ und auch $2\chi(t) \equiv 2((2+2i))$. Kommen wir nun zu $2\sum_{t=1}^{m-1} \chi(t)\chi(1-t)$. Es ist dann

$$\begin{aligned} 2\sum_{t=1}^{m-1} \chi(t)\chi(1-t) &= \sum_{t=1}^{m-1} 2\chi(t)\chi(1-t) \\ &= \sum_{t=1}^{m-1} 2\chi(t(1-t)) \\ &\equiv \sum_{t=2}^{m-1} 2 \\ &\equiv 2m - 4((2+2i)). \end{aligned}$$

Wegen $p \equiv 1(4)$ und $p = 2m-1$ ist dann $2m-4 \equiv p+1((2+2i)) \equiv 2((2+2i))$. Wir erhalten also

$$J(\chi,\chi) \equiv -\chi(-1) - 2$$

oder durch Multiplikation mit $\chi(-1)$

$$\chi(-1)J(\chi,\chi) \equiv -2\chi(-1) - 1 \equiv 1((2+2i)),$$

wieder wegen $2\chi(t) \equiv -2\chi(t) \equiv 2((2+2i))$.
Dies zeigt also:

$$\chi(-1)J(\chi,\chi) \text{ ist primär.}$$

Es ist

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

und somit

$$|G(\chi)|^2 = |J(\chi,\chi)||G(\chi^2)|,$$

also

$$p = |J(\chi,\chi)|\sqrt{p},$$

damit auch

$$|J(\chi,\chi)| = \sqrt{p}.$$

Dies zeigt also

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

und damit die Behauptung. □

Bemerkung 5.9. Schon die Berechnung der Jacobisummmen und der Gaußsumme des Charakters $\chi := \chi_\pi$ ist deutlich technischer. Dies spiegelt auch das weitere Vorgehen im Beweis des Biquadratischen Reziprozitätsgesetzes wider. Bisher war die Vorgehensweise im Beweis der beiden Reziprozitätsgesetze weitgehend identisch. Dies wird sich nun

etwas ändern. Bevor wir aber das entscheidende Korollar für das Biquadratische Reziprozitätsgesetz festhalten, versuchen wir, die Berechnung der Jacobisumme im kubischem Fall zu imitieren. Wir berechnen also die vierte Potenz der Gaußsumme, und es ist

$$G(\chi)^4 = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2) = pJ(\chi,\chi)^2,$$

weshalb wir niemals eine Kongruenz für $J(\chi,\chi)$ erhalten. Die Tatsache, dass in dieser Gleichung $J(\chi,\chi)^2$ auftritt, lässt nämlich nicht darauf schließen, welche Kongruenz $J(\chi,\chi)$ erfüllt. Deshalb war in der hier verwendeten Berechnung leider ein viel aufwendigerer Weg nötig.

Proposition 5.10. *Seien $\alpha \in \mathbb{Z}[i]$ und $a \in \mathbb{Z}$ teilerfremd und primär, d.h. $\alpha \equiv 1((2+2i))$ und $a \equiv 1(4)$. Es gilt*

(i) $\chi_a(\alpha) = \chi_\alpha(a)$,

(ii) $\chi_a(i) = (-1)^{\frac{a-1}{4}}$

(iii) $\chi_a(1+i) = i^{\frac{a-1}{4}}$.

Beweis:

(i) Wir beweisen diese Identität für Primzahlen $a \in \mathbb{Z}$ und Primzahlen $\alpha = \pi \in \mathbb{Z}[i]$, die allgemeine Aussage folgt wieder aus der Multiplikativität des Symbols. Dabei ist mit einer Primzahl a gemeint, dass entweder $a \in \mathbb{P}$ oder $-a \in \mathbb{P}$ gilt. Es soll aber stets die entsprechende Kongruenz $a \equiv 1(4)$ erfüllt sein.

1.Fall: Wir nehmen zuerst an $\pi = -p$ mit $p \equiv 3(4)$ und $p \in \mathbb{P}$. Zusätzlich sei $a = -q$ mit $q \equiv 3(4)$ und $q \in \mathbb{P}$. Dann gilt

$$\chi_{-p}(a) \equiv a^{\frac{p^2-1}{4}} = a^{(p-1)\frac{p+1}{4}} \equiv 1(p).$$

Dies zeigt $\chi_{-p}(a) = 1$. Genauso erhält man auch $\chi_a(-p) = 1$. Also insbesondere auch

$$\chi_{-p}(a) = \chi_a(-p).$$

2.Fall: Sei jetzt wieder $\pi = -p$ wie oben, aber $a = q \equiv 1(4)$ zerfällt $a = \lambda\overline{\lambda}$ mit primärem $\lambda \in \mathbb{Z}[i]$. Es gilt wieder

$$\chi_{-p}(a) \equiv a^{\frac{p^2-1}{4}} = a^{(p-1)\frac{p+1}{4}} \equiv 1(p).$$

Also ist $\chi_{-p}(a) = 1$. Und weiter ist

$$\chi_q(-p) = \chi_\lambda(-p)\chi_{\overline{\lambda}}(-p) = \chi_\lambda(-p)\overline{\chi_\lambda(-p)} = 1.$$

Wir haben somit wieder

$$\chi_a(-p) = \chi_{-p}(a).$$

3.Fall: Sei $a = -q$ mit $q \in \mathbb{P}$ und $q \equiv 3(4)$. Zusätzlich sei $\alpha = \pi$ mit $\pi\overline{\pi} = p \in \mathbb{P}$. Wir berechnen dann für $\chi := \chi_\pi$:

$$\begin{aligned}(-G(\chi))^q = -G(\chi)^q &= \left(\sum_{t\neq 0}\chi(t)\psi(t)\right)^q \\ &\equiv \sum_{t\neq 0}\chi(t)^3\psi(qt) \\ &= -\chi(q^{-1})^3 G(\chi^3) = -\chi(q)G(\overline{\chi})\end{aligned}$$

Die Kongruenz ist dabei modulo q. Wir wissen, es ist

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

und

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

. Deshalb ist

$$G(\chi)^{q+1} \equiv \chi(q)\chi(-1)p = \chi(-q)p.$$

Aus der Berechnung der Gaußsumme wissen wir

$$G(\chi)^{q+1} = (\pi^3\overline{\pi})^{\frac{q+1}{4}}.$$

Jetzt ist $q \equiv 3(4)$ und deshalb ist der Frobeniusautomorphismus die komplexe Konjugation in $\mathbb{Q}(i) \mid \mathbb{Q}$, d.h

$$x^q \equiv \overline{x}(q)$$

für $x \in \mathbb{Q}(i)$. Deshalb berechnen wir weiter:

$$\begin{aligned}\chi(-q)p &\equiv G(\chi)^{q+1} = (\pi^3\overline{\pi})^{\frac{q+1}{4}} \\ \chi(-q)\pi^{q+1} &\equiv \pi^{\frac{(q+3)(q+1)}{4}} \\ \Leftrightarrow \chi(-q) &\equiv \pi^{\frac{q^2+4q+3-4q-4}{4}} \\ \chi(-q) &\equiv \pi^{\frac{q^2-1}{4}} = \chi_{-q}(\pi)\end{aligned}$$

Die letzte Gleichung zeigt also die behauptete Gleichung

$$\chi_\pi(-q) = \chi_{-q}(\pi).$$

4.Fall: Sei jetzt $a = q = \lambda\overline{\lambda}$ mit $q \equiv 1(4)$ und $q \in \mathbb{P}$. Und wie im letzten Fall sei $\alpha = \pi$ mit $\pi\overline{\pi} \in \mathbb{P}$. Wir setzen wieder $\chi = \chi_\pi$ und rechnen modulo λ:

$$\begin{aligned}(-G(\chi))^q = -G(\chi)^q &= \left(\sum_{t\neq 0}\chi(t)\psi(t)\right)^q \\ &\equiv \sum_{t\neq 0}\chi(t)\psi(qt) \\ &= -\chi(q^{-1})G(\chi) = -\chi(q)^{-1}G(\chi)\end{aligned}$$

Wegen $q \neq p$ ist $G(\chi)$ modulo λ invertierbar und wir haben

$$G(\chi)^{q-1} \equiv \chi(q)^{-1}.$$

Nun ist wieder

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

und deshalb auch

$$(\pi^3\overline{\pi})^{\frac{q-1}{4}} = G(\chi)^{q-1} \equiv \chi(q)^{-1}.$$

Weiter ist

$$(\pi^3\overline{\pi})^{\frac{q-1}{4}} \equiv \chi_\lambda(\pi)^3\chi_\lambda(\overline{\pi}) = \chi_\lambda(\pi)^3\overline{\chi_{\overline{\lambda}}(\pi)} = \chi_\lambda(\pi)^3\chi_{\overline{\lambda}}(\pi)^3 = \chi_q(\pi)^3.$$

Also haben wir zuletzt

$$\chi_\pi(q)^{-1} = \chi_\pi(q)^3 = \chi_q(\pi)^3,$$

also auch

$$\chi_\pi(q) = \chi_q(\pi).$$

Man beachte bei diesen Beweisen, dass die Primzahlen λ und π und sogar q und p als unterschiedlich angenommen wurden. Dies liegt daran, dass nach der Voraussetzung die Zahlen a und α teilerfremd sind und zusätzlich $a \in \mathbb{Z}$ liegt.

(ii) Da $a \in \mathbb{Z}$, ist $N(a) = a^2$. Es gilt also

$$\chi_a(i) = i^{\frac{a^2-1}{4}}.$$

Wegen $a \equiv 1(4)$ erhalten wir weiter

$$\chi_a(i) = i^{\frac{a^2-1}{4}} = i^{(a+1)\frac{a-1}{4}} = (-1)^{\frac{a-1}{4}}.$$

(iii) Für diese Rechnung unterscheiden wir zunächst die Fälle $a = -q$ mit $q \in \mathbb{P}$ und $a = q = \lambda\overline{\lambda}$ wieder mit $q \in \mathbb{P}$ und zwei Primzahlen $\lambda, \overline{\lambda} \in \mathbb{Z}[i]$. Dies entspricht also wieder $q \equiv 3(4)$ und $q \equiv 1(4)$.

1.Fall Sei $a = -q$ mit $q \equiv 3(4)$ und $q \in \mathbb{P}$. Es gilt

$$\chi_{-q}(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} = (1+i)^{(q-1)\frac{q+1}{4}}.$$

Jetzt ist weiter

$$(1+i)^{q-1} = \frac{(1+i)^q}{1+i} \equiv \frac{1+i^q}{1+i} = \frac{1-i}{1+i} = -i(q).$$

Also erhalten wir

$$(1+i)^{(q-1)\frac{q+1}{4}} \equiv (-i)^{\frac{q+1}{4}} = i^{\frac{-q-1}{4}}(q).$$

Somit auch die Behauptung

$$\chi_{-q}(1+i) = i^{\frac{-q-1}{4}}.$$

2.Fall Sei $a = q = \lambda\overline{\lambda}$ mit $q \equiv 1(4)$ und $q \in \mathbb{P}$. Dazu rechnen wir:

$$\begin{aligned}\chi_q(1+i) &= \chi_\lambda(1+i)\chi_{\overline{\lambda}}(1+i)\\ &= \chi_\lambda(1+i)\overline{\chi_\lambda(\overline{1+i})}\\ &= \chi_\lambda(1+i)\chi_\lambda(1-i)^3\\ &= \chi_\lambda(i)\chi_\lambda(1+i)^4\\ &= \chi_\lambda(i) = i^{\frac{q-1}{4}}\end{aligned}$$

Damit ist die Behauptung für $\pm a \in \mathbb{P}$ gezeigt. Die endgültige Behauptung folgt aus der Multiplikativität des Ausdrucks. Seien $a, b \in \mathbb{Z}$ mit $a \equiv 1(4)$ und $b \equiv 1(4)$; dann ist

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

Und wegen $(a-1)(b-1) \equiv 0(16)$ ist dann auch $ab - 1 \equiv a + b - 2(16)$, weshalb letztendlich

$$i^{\frac{a+b-2}{4}} = i^{\frac{ab-1}{4}}$$

gilt. □

Bemerkung 5.11. Der Beweis der letzten Proposition ähnelt stark dem Beweis des kubischen Reziprozitätsgesetzes, liefert aber wegen der Einschränkung $a \in \mathbb{Z}$ ein weniger starkes Ergebnis. Im kubischem Fall erhielten wir das Reziprozitätsgesetz für zwei Primzahlen $\pi, \lambda \in \mathbb{Z}[\omega]$, die nicht zugleich in $\mathbb{Z}$ liegen, durch die Multiplikation zweier Ausdrücke

$$\chi_\lambda(\pi^2\overline{\pi}) = \chi_\pi(q)^2$$

und

$$\chi_\pi(\lambda^2\overline{\lambda}) = \chi_\lambda(p)^2.$$

Hier haben wir ähnliche Relationen im 4.Fall des Beweises der ersten Aussage, nämlich

$$\chi_\lambda(\pi^3\overline{\pi}) = \chi_\pi(q)^3$$

und

$$\chi_\pi(\lambda^3\overline{\lambda}) = \chi_\lambda(p)^3.$$

Multiplizieren wir diese beiden Gleichungen, erhalten wir

$$\chi_\lambda(\pi^3\overline{\pi})\chi_\lambda(p)^3 = \chi_\pi(\lambda^3\overline{\lambda})\chi_\pi(q)^3$$

oder durch leichtes Umformen

$$\chi_\lambda(\pi^2) = \chi_\pi(\lambda^2).$$

Das gleiche Vorgehen wie im Kubischen Reziprozitätsgesetz liefert also kein Biquadratisches Reziprozitätsgesetz, sondern eine Art Quadratisches Reziprozitätsgesetz für den Ganzheitsring $\mathbb{Z}[i]$ von $\mathbb{Q}(i)$. Um nun das Biquadratische Reziprozitätsgesetz zu beweisen, werden lediglich obige Proposition und einige Eigenschaften des Symbols benutzt.

Satz 5.12 (Biquadratisches Reziprozitätsgesetz)**.** *Seien $\alpha, \beta \in \mathbb{Z}[i]$ primär. Wir setzen $\alpha = a + bi$ und $\beta = c + di$. Es gilt dann*

$$\begin{aligned}\chi_\alpha(\beta) &= (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}}\chi_\beta(\alpha)\\ &= (-1)^{\frac{a-1}{2}\frac{c-1}{2}}\chi_\beta(\alpha)\\ &= (-1)^{\frac{bd}{4}}\chi_\beta(\alpha).\end{aligned}$$

Beweis: Wir zeigen erst, weshalb die letzten beiden Gleichheiten gelten. Da α primär ist, gilt $a - b \equiv 1(4)$ und $b \equiv 0(2)$, also auch $a - 1 \equiv b(4)$, und da beide Seiten durch 2 teilbar sind, gilt sogar

$$\frac{a-1}{2} \equiv \frac{b}{2}(2).$$

Gleiches gilt für β. Dies zeigt die letzte Gleichung. Es ist jetzt $N(\alpha) = a^2+b^2$. Wir erhalten dann wegen $a-b \equiv 1(4)$ oder $a-b-1 \equiv 0(4)$, dass $(a-b-1)^2 \equiv 0(16)$ ist. Aus Letzterem folgt

$$(a-b-1)^2 = a^2 + b^2 + 1 - 2ab - 2a + 2b \equiv 0(16)$$

oder durch Umformen

$$a^2 + b^2 - 1 \equiv 2(ab + a - b - 1) = 2(a-1)(b+1)(16).$$

Da beide Seiten durch 4 teilbar sind, gilt auch schon

$$\frac{N(\alpha)-1}{4} = \frac{a^2+b^2-1}{4} \equiv \frac{(a-1)(b+1)}{2}(2).$$

Zuletzt wissen wir, $a - 1 \equiv 0(2)$ und $b \equiv 0(2)$, also $(a-1)b \equiv 0(4)$, und wir erhalten dann

$$\frac{N(\alpha)-1}{4} \equiv \frac{(a-1)b}{2} + \frac{(a-1)}{2} \equiv \frac{a-1}{2}(2).$$

Kommen wir nun zum eigentlichen Beweis. Wir nehmen an, dass

$$(a, b) = 1 = (c, d)$$

ansonsten könnten wir ganze Zahlen bei α bzw. β ausklammern und diese mit der letzten Proposition behandeln. Wir nehmen zusätzlich an, dass α und β teilerfremd sind, sonst gilt ohnehin $\chi_\alpha(\beta) = \chi_\beta(\alpha) = 0$. Es ist jetzt $\beta = c + di$ oder äquivalent $i\beta = ic - d$. Wir haben also

$$ic \equiv d(\beta).$$

Wir rechnen weiter: Es ist

$$c\alpha = ca + icb \equiv ac + db(\beta).$$

Wir haben also

$$\chi_\beta(\alpha) = \chi_\beta(c^{-1}c\alpha) = \chi_\beta(c)^3\chi_\beta(ac + bd).$$

In gleicher Art erhalten wir auch

$$\chi_\alpha(\beta) = \chi_\alpha(a^{-1}a\beta) = \chi_\alpha(a)^3\chi_\alpha(ac + bd).$$

Insgesamt haben wir

$$\chi_\beta(\alpha)\chi_\alpha(\beta)^{-1} = \chi_\alpha(a)\chi_\beta(c)^3\chi_\alpha(ac + bd)^3\chi_\beta(ac + bd)(*)$$

durch Multiplikation und invertieren der zweiten Gleichung. Der Rest der Behauptung beruht auf einer Fallunterscheidung.

1.Fall Ist $a \equiv c \equiv 1(4)$, so ist

$$\chi_\beta(c) = \chi_c(\beta) = \chi_c(di) = \chi_c(i).$$

Dabei gilt dies wegen $\beta = c + di \equiv di(c)$ und $\chi_c(d) = 1$. Mit gleicher Rechnung ist auch

$$\chi_\alpha(a) = \chi_a(i).$$

Weiter ist wegen der Voraussetzung $ac \equiv 1(4)$ und $bd \equiv 0(4)$, also auch

$$ac + bd \equiv 1(4).$$

Dabei ist $ac + bd \in \mathbb{Z}$ und deshalb

$$\chi_\alpha(ac + bd)^3 = \chi_{\overline{\alpha}}(ac + bd).$$

Wir rechnen:

$$\begin{aligned}
\chi_\alpha(ac + bd)^3\chi_\beta(ac + bd) &= \chi_{\overline{\alpha}}(ac + bd)\chi_\beta(ac + bd) \\
&= \chi_{ac+bd}(\overline{\alpha}\beta) \\
&= \chi_{ac+bd}((a - bi)(c + di)) \\
&= \chi_{ac+bd}((ac + bd) + (ad - bc)i) \\
&= \chi_{ac+bd}(i)
\end{aligned}$$

Dabei beachte man, dass $\overline{\alpha}\beta$ primär ist. Setzen wir dies in die Gleichung $(*)$ ein, erhalten wir:

$$\begin{aligned}
\chi_\alpha(a)\chi_\beta(c)^3\chi_\alpha(ac + bd)^3\chi_\beta(ac + bd) &= \chi_a(i)\chi_c(i)^3\chi_{ac+bd}(i) \\
&= (-1)^{\frac{a-1}{4}}(-1)^{\frac{1-c}{4}}(-1)^{\frac{ac+bd-1}{4}} \\
&= (-1)^{\frac{bd+ac+a-c-1}{4}}
\end{aligned}$$

Weiter ist wegen $(a - 1)(c + 1) = ac + a - c - 1 \equiv 0(8)$ auch

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

2.Fall Ist jetzt $a \equiv c \equiv 3(4)$, so ist auch $-a \equiv -b \equiv 1(4)$ und wir erhalten wie vorhin

$$\chi_\beta(-c) = \chi_{-c}(i)$$

und

$$\chi_\alpha(-a) = \chi_{-a}(i).$$

Genauso wie vorher ist wieder $ac \equiv 1(4)$ und $bd \equiv 0(4)$, also auch $ac + bd \equiv 1(4)$. Und wir erhalten wieder mit gleichen Rechnungen

$$\chi_{\overline{\alpha}}(ac + bd)\chi_\beta(ac + bd) = \chi_{ac+bd}(i).$$

Dabei ist wieder zu beachten, dass $\overline{\alpha}\beta$ primär ist. Wir setzen dies erneut in die Gleichung $(*)$ ein:

$$\begin{aligned}\chi_\alpha(a)\chi_\beta(c)^3\chi_\alpha(ac+bd)^3\chi_\beta(ac+bd) &= \chi_\alpha(-1)\chi_\beta(-1)\chi_{-a}(i)\chi_{-c}(i)^3\chi_{ac+bd}(i)\\ &= (-1)^{\frac{a^2+b^2-1}{4}}(-1)^{\frac{c^2+d^2-1}{4}}(-1)^{\frac{bd+ac+c-a-1}{4}}\end{aligned}$$

Wegen $a \equiv 3(4)$ und somit $b \equiv 2(4)$ gilt $(a-1)(a+1) = a^2 - 1 \equiv 0(8)$ und $(b-2)b = b^2 - 2b \equiv 0(8)$. Des weiteren ist dann auch $2b \equiv 4(8)$ und wir haben

$$a^2 - 1 + b^2 - 2b \equiv a^2 + b^2 - 1 - 4 \equiv 0(8)$$

oder

$$\frac{a^2+b^2-1}{4} \equiv 1(2).$$

Dies zeigt

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

Wir haben also

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

Jetzt ist

$$(a+1)(c-1) = ac + c - a - 1 \equiv 0(8),$$

also

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

<u>3.Fall</u> Sei $a \equiv 1(4)$ und $c \equiv 3(4)$. Wir wissen bereits:

$$\begin{aligned}\chi_\alpha(a) &= \chi_a(i)\\ \chi_\beta(-c) &= \chi_{-c}(a)\\ \chi_\beta(-1) &= -1\end{aligned}$$

Wegen $ac \equiv 3(4)$ gilt dann

$$-(ac+bd) \equiv 1(4),$$

weshalb auch

$$\chi_{\overline{\alpha}}(-(ac+bd))\chi_\beta(-(ac+bd)) = \chi_{-(ac+bd)}(i)$$

ist. Dies gilt, da auch diesmal $(ac+bd) - (ad-bc) \equiv 1(4)$, also $\overline{\alpha}\beta$ primär ist. Wir stellen weiter fest: Es ist $ac + bd \equiv 3(4)$ und $ad - bd \equiv 2(4)$, also

$$\chi_{\overline{\alpha}\beta}(-1) = -1.$$

Wir setzen nun wieder in $(*)$ ein und erhalten:

$$\begin{aligned}\chi_\alpha(a)\chi_\beta(c)^3\chi_\alpha(ac+bd)^3\chi_\beta(ac+bd) &= (-1)^{\frac{a-1}{2}}(-1)(-1)^{\frac{c+1}{2}}(-1)(-1)^{\frac{-ac-bd-1}{2}}\\ &= (-1)^{\frac{-bd-ac+a+c-1}{2}}\end{aligned}$$

Wir haben $-\frac{bd}{2} \equiv \frac{bd}{2}(2)$ und $-(a-1)(c-1) = -ac + a + c - 1 \equiv 0(8)$ und deshalb wieder

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

Damit sind alle Fälle behandelt und der Satz bewiesen. □

Korollar 5.13 (Ergänzungssätze zum Biquadratischen Reziprozitätsgesetz)**.** *Ist $\alpha \in \mathbb{Z}[i]$ primär mit $\alpha = a + bi$, so gilt*

(i) $\chi_\alpha(i) = i^{\frac{1-a}{2}}$,

(ii) $\chi_\alpha(1+i) = i^{\frac{a-b-b^2-1}{4}}$,

(iii) $\chi_\alpha(2) = i^{-\frac{b}{2}}$.

Beweis:

(i) Sei $\alpha = a + bi$ primär, d.h. $a - b \equiv 1(4)$. Dann gilt

$$(a - b - 1)^2 \equiv a^2 + b^2 + 1 - 2ab - 2a + 2b \equiv 0(16)$$

oder auch

$$a^2 + b^2 - 1 \equiv 2(ab + a - b - 1) = 2(a-1)b + 2(a-1)(16).$$

Dies zeigt auch

$$\frac{a^2 + b^2 - 1}{4} \equiv \frac{1-a}{2}(-b-1)(4)$$

Unterscheidet man jetzt für die letzte Gleichung die Fälle $a \equiv 1(4)$ und $b \equiv 0(4)$ bzw. $a \equiv 3(4)$ und $b \equiv 2(4)$, so erhält man leicht

$$\frac{1-a}{2}(-b-1) \equiv \frac{1-a}{2}(4).$$

(ii) Wir setzen zunächst $\gamma = (1+i)^3 = -2 + 2i$. Deshalb gilt wegen $\gamma - i(2+2i) = 0$ auch

$$\lambda \equiv 0((2+2i)).$$

Somit ist

$$\gamma - \alpha \equiv -\alpha \equiv -1((2+2i)),$$

also ist $\alpha - \gamma$ primär. Wir rechnen dann:

$$\begin{aligned} \chi_\alpha(\gamma) &= \chi_\alpha(\gamma - \alpha) \\ &= \chi_\alpha(-1)\chi_\alpha(\alpha - \gamma) \\ &= \chi_\alpha(-1)\chi_{\alpha-\gamma}(\alpha) \\ &= \chi_\alpha(-1)\chi_{\alpha-\gamma}(\gamma) \end{aligned}$$

Es lässt sich also α immer modulo γ reduzieren mit Berücksichtigung des Faktors $\chi_\alpha(-1)$ im ersten Schritt bzw. eines Faktors $\chi_{\alpha-k\gamma}(-1)$ im k-ten Schritt. Wir schreiben deshalb $\alpha = a + bi = c + d\gamma$ mit

$$d = \frac{b}{2}$$

und

$$c = a + b.$$

Wir rechnen zuerst den aufretenden Faktor aus:

$$\begin{aligned}\chi_{\alpha-k\gamma}(-1) &= \chi_{c+(d-k)\gamma}(-1)\\ &= \chi_{c+(d-k)\gamma}(i)^2\\ &\overset{(i)}{=} (-1)^{\frac{a-2k-1}{2}}\end{aligned}$$

Jetzt ist wegen $a-b\equiv 1(4)$ auch

$$\frac{a-1}{2}\equiv\frac{b}{2}(2),$$

also auch

$$(-1)^{\frac{a-2k-1}{2}}=(-1)^{\frac{b-2k}{2}}=(-1)^{d-k}.$$

Wir können nun also den Wert für $\chi_\alpha(\lambda)$ berechnen durch:

$$\begin{aligned}\chi_\alpha(\gamma) &= \chi_\alpha(-1)\chi_{\alpha-\gamma}(\gamma)\\ &= (-1)^d\chi_{\alpha-\gamma}(\gamma)\\ &= (-1)^{\sum_{k=0}^{d}(d-k)}\chi_{\alpha-d\gamma}(\gamma)\\ &= (-1)^{\frac{d(d+1)}{2}}\chi_c(\gamma)\\ &= (-1)^{\frac{d(d+1)}{2}}i^{\frac{c-1}{4}}\\ &= i^{\frac{b(b+2)}{4}+\frac{a+b-1}{4}}\\ &= i^{\frac{a+3b+b^2-1}{4}}\end{aligned}$$

Es ist jetzt $2b(b+2)=2b^2+4b\equiv 0(16)$ und deshalb auch

$$\frac{b^2+3b}{4}\equiv\frac{-b^2-b}{4}(4).$$

Dies zeigt

$$\chi_\alpha(\gamma)=i^{\frac{a+3b+b^2-1}{4}}=i^{\frac{a-b-b^2-1}{4}}.$$

(iii) Wir wissen $(1+i)^2=2i$ und somit:

$$\begin{aligned}\chi(2i) &= \chi_\alpha(1+i)^2\\ \chi_\alpha(2)\chi_\alpha(i) &= i^{\frac{a-b-b^2-1}{2}}\\ \chi_\alpha(2)i^{\frac{1-a}{2}} &= i^{\frac{a-b-b^2-1}{2}}\\ \chi_\alpha(2) &= i^{\frac{2a-b-b^2-2}{2}}\end{aligned}$$

Es ist $2(a-b-1)=2a-2b-2\equiv 0(8)$, also auch

$$\frac{2a-2b-2}{2}\equiv 0(4)$$

und deshalb

$$i^{\frac{2a-b-b^2-2}{2}}=i^{\frac{b-b^2}{2}}=i^{\frac{-b}{2}}.$$

Dabei gilt die letzte Gleichung wegen $b(b-2)=b^2-2b\equiv 0(8)$.

□

6 Beispiele und Schlusswort

Die bewiesenen Reziprozitätsgesetze erlauben uns, die Biquadratischen und Kubischen Symbole schnell auszuwerten. Dies liegt vor allem daran, dass genau wie beim Legendre-Symbol die explizite Primfaktorzerlegung der beteiligten Zahlen in $\mathbb{Z}[\omega]$ bzw. $\mathbb{Z}[i]$ keine Rolle spielen. Die Eigenschaft, dass das Symbol 1 ist genau dann, wenn der "Zähler" ein kubischer bzw. biquadratischer Rest modulo dem "Nenner" ist, geht dabei aber im Allgemeinen verloren. Diese Aussage ist nur dann richtig, wenn der "Nenner" eine Primzahl im jeweiligen Ganzheitsring ist. Im Folgenden werden wir noch jeweils ein Beispiel für die entsprechenden Ganzheitsringe $\mathbb{Z}[\omega]$ und $\mathbb{Z}[i]$ durchführen.

Beispiel 6.1. Um Primzahlen in $\mathbb{Z}[\omega]$ zu erhalten, können wir Primzahlen in $\mathbb{Z}$ betrachten und wie diese in $\mathbb{Z}[\omega]$ zerfallen. Wir betrachten $p = 19 \in \mathbb{P}$ und $q = 103 \in \mathbb{P}$. Offensichtlich ist $p = 19 \equiv 1(3)$ und $q = 103 \equiv 1(3)$, weshalb beide Primzahlen zerfallen. Wir setzen wie gewohnt $p \equiv \pi\overline{\pi}$ und $q \equiv \lambda\overline{\lambda}$. Das Finden einer Primzahl $\pi = a + b\omega$ bzw. $\lambda = c + d\omega$ läuft auf das Lösen der Gleichungen

$$a^2 - ab + b^2 = 19$$

bzw.

$$c^2 - cd + d^2 = 103$$

hinaus. Wir wissen bereits wir können unseren Erzeuger stets primär wählen also setzen wir $b \equiv d \equiv 0(3)$ und $c \equiv a \equiv \pm 1(3)$. Eine einfache Umformung ergibt

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

Da nun ab durch 3 teilbar ist, verändern wir 19 solange um einen Summanden 3, bis wir eine Quadratzahl erhalten. Anschließend schauen wir dann, ob die obige Formel erfüllbar ist. Wir beginnen mit den Quadratzahlen kleiner als 19. Von denen liegen nur 16 und 4 in derselben Kongruenzklasse modulo 3. Angenommen 16 wäre das gewünschte Quadrat, so müsste $ab = 3$ gelten. Dann kann aber unmöglich $(a - b)^2 = 16$ gleichzeitig wahr sein. Die Zahl 4 ist hingegen das gewünschte Quadrat, denn

$$(3 - 5)^2 + 3 \cdot 5 = 4 + 15 = 19.$$

Wir erhalten also $a = 5$ und $b = 3$. Gleiches machen wir für 103. Es gibt 10 Quadratzahlen unter 103, von denen aber nur 6 in Frage kommen ($1^2, 3^2, 6^2, 9^2$ kommen nicht in Frage!). Das zugehörige Quadrat ist wieder 4 und es gilt

$$(11 - 9)^2 + 11 \cdot 9 = 4 + 99 = 103.$$

Die Tatsache, dass das Quadrat immer kleiner als die entsprechende Zahl ist, ist kein Zufall. Dazu betrachten wir nochmal den allgemeinen Fall. Ist

$$p = a^2 - ab + b^2,$$

so kann offensichtlich nur dann

$$(a - b)^2 > p = a^2 - ab + b^2 = (a - b)^2 + ab$$

gelten, falls $ab < 0$ gilt. Dies ist erfüllt, wenn $a < 0$ und $b > 0$ oder wenn $a > 0$ und $b < 0$ ist. Sei jetzt o.B.d.A. $a > 0$ und $b < 0$, sonst gehe zu $-a$ und $-b$ über. Die zugehörige Primzahl in $\mathbb{Z}[\omega]$ ist $a + b\omega$. Die Zahl

$$a + b\omega^2 = a - b - b\omega$$

hat als Norm dieselbe Primzahl in $\mathbb{P}$ wie $a + b\omega$ und erfüllt zudem

$$a - b > 0 \text{ und } -b > 0.$$

Insbesondere ist

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

und wir haben ein gesuchtes kleineres Quadrat als die Primzahl p gefunden. Um eine Primzahl in $\mathbb{Z}[\omega]$ über einer Primzahl $p \in \mathbb{P}$ zu finden, reicht es also, die Quadrate zu untersuchen, die kleiner als die Primzahl p sind. Kommen wir zurück zum Zahlenbeispiel. Wir hatten nun

$$\pi = 5 + 3\omega$$

und

$$\lambda = 11 + 9\omega.$$

Wir wollen nun das Symbol $\chi_\lambda(\pi)$ mit dem kubischen Reziprozitätsgesetz berechnen. Es ist:

$$\begin{aligned}
\left(\frac{5+3\omega}{11+9\omega}\right) &= \left(\frac{11+9\omega}{5+3\omega}\right) \\
&= \left(\frac{-4}{5+3\omega}\right) \\
&= \left(\frac{4}{5+3\omega}\right) \\
&= \left(\frac{5+3\omega}{4}\right) \\
&= \left(\frac{1-\omega}{4}\right) \\
&= \omega^{\frac{4-1}{3}} \\
&= \omega
\end{aligned}$$

Betrachten wir noch $\overline{\pi} = 2 - 3\omega$ und das Symbol $\chi_\lambda(\overline{\pi})$:

$$\begin{aligned}
\left(\frac{2-3\omega}{11+9\omega}\right) &= \left(\frac{11+9\omega}{2-3\omega}\right) \\
&= \left(\frac{17}{2-3\omega}\right) \\
&= \left(\frac{-2}{2-3\omega}\right) \\
&= \left(\frac{2-3\omega}{-2}\right) \\
&= \left(\frac{\omega}{-2}\right) \\
&= \omega^{\frac{1-(-2)}{3}} \\
&= \omega
\end{aligned}$$

Wir erhalten dann auch $\chi_{\overline{\lambda}}(\overline{\pi}) = \omega^2 = \chi_{\overline{\lambda}}(\pi)$ durch komplexe Konjugation.

Beispiel 6.2. Wir betrachten nun den Ganzheitsring $\mathbb{Z}[i]$. Genau wie im vorhergehenden Beispiel können wir die Primzahlen in $\mathbb{Z}[i]$ durch das Zerfällungsverhalten der Primzahlen aus $\mathbb{Z}$ beschreiben. Wir betrachten jetzt beispielsweise $p = 37$ und $q = 113$, zwei Primzahlen in $\mathbb{Z}$. Für diese gilt $p = 37 \equiv 1(4)$ und $q = 113 \equiv 1(4)$. Deshalb zerfallen beide Primzahlen in $\mathbb{Z}[i]$ und wir setzen $p = \pi\overline{\pi}$ und $q = \lambda\overline{\lambda}$. Um die Primzahlen $\pi = a + bi$ und $\lambda = c + di$ zu finden, müssen wir die Gleichungen

$$a^2 + b^2 = p = 37$$

und

$$c^2 + d^2 = q = 113$$

lösen. Wir wollen unseren Erzeuger primär wählen, d.h. wir setzen $a - b \equiv 1(4)$ und $b \equiv 0(2)$ und ebenso $c - d \equiv 1(4)$ $d \equiv 0(2)$. Um die Gleichung $a^2 + b^2 = p$ zu lösen, können wir also wegen $b^2 \equiv 0(4)$ die Primzahl um Vielfache von 4 verkleinern, um dann eine Quadratzahl a^2 zu erhalten. Wenn das Vielfache der 4 noch ein Quadrat ist, so ist die Lösung der Gleichung gefunden. Wir betrachten also die Primzahl $p = 37$. Die Quadrate die unter 37 liegen und dieselbe Äquivalenzklasse modulo 4 haben sind $1, 9, 25$ und die zugehörigen Vielfachen der 4 sind $36, 28, 12$. Wir erhalten deshalb $a = -1$ und $b = 6$ da nur

$$-1 - 6 = -7 \equiv 1(4)$$

erfüllt. Also ist

$$\pi = -1 + 6i.$$

Gleiches machen wir für $q = 113$ und erhalten $c = -7$ und $d = 8$ denn dann ist

$$-7 - 8 = -15 \equiv 1(4)$$

und

$$7^2 + 8^2 = 49 + 64 = 113.$$

Und es gilt

$$q = -7 + 8i.$$

Wie auch im kubischem Fall wollen wir noch das Symbol $\chi_\lambda(\pi)$ berechnen:

$$\begin{aligned}
\left(\frac{-1+6i}{-7+8i}\right) &= (-1)^{\frac{8\cdot 6}{4}}\left(\frac{-7+8i}{-1+6i}\right) \\
&= \left(\frac{-6+2i}{-1+6i}\right) \\
&= \left(\frac{2}{-1+6i}\right)\left(\frac{-3+i}{-1+6i}\right) \\
&= \left(\frac{2}{-1+6i}\right)\left(\frac{1+i}{-1+6i}\right)\left(\frac{-1+2i}{-1+6i}\right) \\
&= i^{\frac{-6}{2}} i^{\frac{-1-6-36-1}{4}}(-1)^{\frac{2\cdot 6}{4}}\left(\frac{-1+6i}{-1+2i}\right) \\
&= i\cdot i\cdot(-1)\left(\frac{2}{-1+2i}\right) \\
&= \left(\frac{2}{-1+2i}\right) \\
&= -i
\end{aligned}$$

Ebenso soll noch $\chi_\lambda(\overline{\pi})$ berechnet werden:

$$\begin{aligned}
\left(\frac{-1-6i}{-7+8i}\right) &= \left(\frac{-7+8i}{-1-6i}\right) \\
&= \left(\frac{-8+2i}{-1-6i}\right) \\
&= \left(\frac{2}{-1-6i}\right)\left(\frac{i}{-1-6i}\right)\left(\frac{1+4i}{-1-6i}\right) \\
&= i^{\frac{6}{2}} i^{\frac{1+1}{2}}\left(\frac{-1-6i}{1+4i}\right) \\
&= \left(\frac{-2i}{1+4i}\right) \\
&= i^{\frac{-4}{2}}(i^{\frac{1-1}{2}})^3 \\
&= -1
\end{aligned}$$

Letzteres ist jetzt so zu interpretieren, dass $\overline{\pi}$ quadratischer Rest modulo λ ist, aber kein biquadratischer Rest.

Die Beispiele geben eine Vorstellung, wie man diese Symbole sinnvoll berechnet. Um einen kleinen Ausblick für mögliche Erweiterungen dieser Beweise auch für höhere Reziprozitätsgesetze zu geben verweise ich auf die Stickelberg-Relation. Da der Ganzheitsring von Kreisteilungskörpern im Allgemeinen kein Hauptidealring ist, betrachtet man anstelle der Gaußsumme das von der Gaußsumme erzeugte Ideal. Die Stickelberg-Relation gibt das Zerfällungsverhalten dieses Ideals in Primideale an (vgl. [IR] Kapitel 14 oder [Lem] Kapitel 11). Unter Zuhilfenahme dieser Relation lässt sich dann das Eisensteinsche Reziprozitätsgesetz beweisen.

Danksagung

Zunächst sei meinem Betreuer Prof. E.-U. Gekeler für seine fachkundige Unterstützung gedankt. Die Vorlesung zur Algebraischen Zahlentheorie I legt den Grundstein für diese Arbeit und weckte meine Interesse für eine Bachelorarbeit auf diesem Gebiet. Ebenfalls möchte ich Philipp Stopp danken, der in den begleitenden Übungen zu den Vorlesungen Algebraische Zahlentheorie I und Algebraische Zahlentheorie II stets hilfsbereit war und auch auf spezifische Fragen zu meiner Bachelorarbeit einging. Ich bedanke mich auch bei meinen Kommilitonen, die sich für Fragen meinerseits Zeit genommen haben. Besonders bedanke ich mich bei Lukas Theis, Marius Schöndorf, Michael Kaicher und Tobias Chasseur, die mir während dem Schreiben der Bachelorarbeit geholfen haben.

Literatur

[chron] http://www.rzuser.uni-heidelberg.de/ hb3/fchrono.html

[Furt] Ph. Furtwängler, *Über die Reziprozitätsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet.* Mathematische Annalen 1903, Volume 58, Issue 1-2, pp1-50

[Gek] E.-U. Gekeler, Mitschrift zu den Vorlesungen: Algebraische Zahlentheorie I und Algebraische Zahlentheorie II, WS2012/13 und SS2013 an der Universität des Saarlandes.

[Has] H. Hasse: *Das Eisensteinsche Reziprozitätsgesetz der n-ten Potenzreste.* Mathematische Annalen 1927, Volume 97, Issue 1, pp 599-623.

[IR] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory.* Second Edition, Springer-Verlag, 1990 New York.

[Lem] F. Lemmermeyer: *Reciprocity Laws From Euler to Eisenstein.* Springer Monographs in Mathematics, Berlin Heidelberg 2000.

[Neu] J. Neukirch: *Algebraische Zahlentheorie.* Unveränderter Nachdruck der 1.Auflage, Springer-Verlag, Berlin Heidelberg 2007.

[Wash] L.C. Washington: *Introduction to Cyclotomic Fields.* 1.Auflage, Springer-Verlag, 1982 New York.