Das biquadratische Reziprozitätsgesetz

Harald Kümmerle

8. Juni 2010

Abstract

Die kanonische Übertragung des altbekannten quadratischen Reziprozitätsgesetzes auf den Fall der vierten Potenz ergibt sich, indem man $\mathbb{Z}$ verlässt und stattdessen die Gauschen Zahlen $\mathbb{Z}[i]$ betrachtet. In diesem Vortrag soll das biquadratische Reziprozitätsgesetz für diesen Fall bewiesen werden. Hierbei wird eine Idee von Eisenstein aufgegriffen, dies mit elliptischen Funktionen durchzuführen; jedoch wird hier der modernere Zugang über die Weierstrasche Theorie den ursprünglichen Berechnungen auf der Lemniskate vorgezogen.

1 Vorbereitung

Sei O_K der Ganzheitsring eines Zahlkörpers K, der die n-ten Einheitswurzeln $\mu_n = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ enthält und $\mathfrak{p} \nmid nO_K$ ein Primideal. Weil O_K ein Dedekindring ist, d.h. alle Primideale maximal sind, ist $O_K/\mathfrak{p}$ ein (endlicher) Körper. Für jedes zu $\mathfrak{p}$ teilerfremde Element $\alpha \in O_K$ gilt also $\alpha^{N\mathfrak{p}-1} \equiv 1 \mod \mathfrak{p}$, wenn N die Normfunktion bezeichnet. Weil die von $\zeta_n \mod \mathfrak{p}$ erzeugte Untergruppe von $(O_K/\mathfrak{p})^*$ die Mächtigkeit n besitzt, gilt $n \mid N\mathfrak{p} - 1$.

Deswegen lässt sich definieren:

Definition 1 *Das n-te Restklassensymbol ist definiert durch*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{\frac{N\mathfrak{p}-1}{n}} \mod \mathfrak{p}$$

Hierbei werden die Einheitswurzeln als Repräsentanten gewählt.

Proposition 2 *Es gilt:*

1. $\alpha \equiv \beta$ *impliziert* $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\beta}{\mathfrak{p}}\right)_n$.
2. $\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \left(\frac{\beta}{\mathfrak{p}}\right)_n$
3. $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$ *gilt genau dann, wenn es ein* $\xi \in O_K \backslash \mathfrak{p}$ *gibt, das* $\alpha \equiv \xi^n \mod \mathfrak{p}$ *erfüllt.*

Beweis: 1) und 2) sind offensichtlich. Für 3) sei zunächst angenommen, dass $\alpha = \xi^n \mod p$ ist. Potenzieren ergibt

$$\alpha^{\frac{N\mathfrak{p}-1}{n}} = \xi^{N\mathfrak{p}-1} = 1.$$

Für die andere Richtung sei $\left(\frac{\alpha}{p}\right)_n = 1$ angenommen. Weil $(O_K/\mathfrak{p})^*$ zyklisch ist, sei $\alpha = \gamma^j \mod \mathfrak{p}$ dargestellt. Es gilt

$$1 = \alpha^{\frac{N\mathfrak{p}-1}{n}} = \xi^{j\frac{N\mathfrak{p}-1}{n}},$$

also $N\mathfrak{p}-1 \mid j\frac{N\mathfrak{p}-1}{n}$. Daraus folgt $n \mid j$, indesbesondere ist $\alpha = \xi^{nm} \mod \mathfrak{p}$ für ein $m \in \mathbb{Z}$.

Definition 3 *Sei $\mathfrak{a}$ ein zu nO_K teilerfremdes Ideal; der kanonische Homomorphismus*

$$\mu_n \to (O_K/\mathfrak{a})^*, \zeta_n, \mapsto \zeta_n \mod a$$

ist dann injektiv. Ein Repräsentantensystem $A = \alpha_1, \ldots, \alpha_m$ von $(O_K/\mathfrak{a})^*/\mu_n$ wird $\frac{1}{n}$-System mod $\mathfrak{a}$ genannt. Ist $\mathfrak{a}$ ein Primideal, so ist m notwendigerweise $\frac{N\mathfrak{a}-1}{n}$.

Analog zum klassischen Beweis des quadratischen Reziprozitätsgesetzes gelten zwei Lemmata:

Lemma 4 *Sei $A = \{\alpha_1, \ldots, \alpha_m\}$ ein $\frac{1}{n}$-System mod $\mathfrak{p}$. Dann gibt es eine Permutation $\pi \in Sym(m)$ und eine Funktion $a : \{1, \ldots, m\} \to \{0, \ldots, n-1\}$, so dass*

$$\alpha\alpha_i \equiv \zeta_n^{a(i)}\alpha_{\pi(i)} \mod \mathfrak{p} \quad (\forall i).$$

Weiterhin gilt mit $\mu = \sum a(i)$:

$$\left(\frac{\alpha}{p}\right)_n = \zeta_n^{\mu}.$$

Beweis: (Es wird im folgenden nicht strikt zwischen α und dem Repräsentanten α mod $\mathfrak{p}$ unterschieden).

Für jedes α_i ist auch $\alpha\alpha_i \in (O_K/p)^*$, und liegt deswegen in genau einer μ_n-Nebenklasse. Also gibt es solche Funktionen a und π. π ist zudem injektiv (und damit auch bijektiv):

Angenommen, $\pi(i) = \pi(j)$. Dann ist $\alpha\alpha_i\zeta_n^{-a(i)} \equiv \alpha\alpha_j\zeta_n^{-a(j)}$, und somit $\alpha_i \equiv \zeta_n^{a(i)-a(j)}\alpha_j$. Weil die α_k Repräsentanten von μ_n-Klassen sind, folgt $i = j$. Die Behauptung folgt aus:

$$\alpha^{\frac{N\mathfrak{p}-1}{n}} \prod_{i=1}^{m} \alpha_i = \prod_{i=1}^{m} \alpha\alpha_i \equiv \prod_{i=1}^{m} \zeta_n^{a(i)}\alpha_{\pi(i)} = \zeta_n^{\mu} \prod_{i=1}^{m} \alpha_{\pi(i)}$$

Lemma 5 *Sei pO_K ein Hauptprimideal mit $pO_K \nmid nO_K$ und $f : K \to \mathbb{C}$ eine O_K-periodische Funktion mit*

1. *$f(\zeta_n z) = \zeta_n f(z)$ für alle $z \in K \backslash O_K$;*
2. *$f(\frac{\alpha}{p}) \neq 0$ für alle $\alpha \in O_K \backslash pO_K$.*

Dann gilt für jedes $\frac{1}{n}$-System A mod pO_K:

$$\left(\frac{\gamma}{p}\right)_n = \prod_{\alpha \in A} \frac{f(\gamma\alpha/p)}{f(\alpha/p)}$$

Beweis: Seien a, π wie in Lemma 4 gewählt.

$$f\Big(\frac{\gamma\alpha_i}{p}\Big) = f\Big(\frac{\zeta_n^{a(i)}\alpha_{\pi(i)} + \lambda p}{p}\Big) = f\Big(\frac{\zeta_n^{a(i)}\alpha_{\pi(i)}}{p}\Big) = \zeta_n^{a(i)} f\Big(\frac{\alpha_{\pi(i)}}{p}\Big)$$

Vom gesamten Produkt bleibt also nur noch folgendes übrig, und das ist nach Wahl von a:

$$\prod_{i=1}^{m} \zeta_n^{a(i)} = \zeta^{\mu} = \Big(\frac{\gamma}{p}\Big)_n.$$

2 Elliptische Funktionen - Allgemeines

Zur Erinnerung: eine elliptische Funktion ist eine meromorphe Funktion, die doppeltperiodisch bezüglich einem Gitter $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$ ist. definiert. Desweiteren:

Definition 6 *Das Fundamentalparallelogramm eines Gitters Λ ist*

$$F = F_\Lambda = \omega_1[0,1) + \omega_2[0,1).$$

Der Divisor (f) einer elliptischen Funktion f ist definiert als die formale (endliche) Summe

$$(f) = \sum_{p \in F} n_p(p).$$

Satz 7 *(1. und 2. Liouvillescher Satz)*

1. *Elliptische Funktionen ohne Pole sind konstant. Aus $(f) = (g)$ folgt $f = c \cdot g$ für ein konstantes c.*

2. *Elliptische Funktionen haben nur endlich viele Pole in F, die Summe der Residuen ist 0. Insbesondere hat jede mindestens zwei Pole, Vielfachheiten eingerechnet.*

Beweis: Zu 1): Hat f keine Pole in F, so ist f auf ganz $\mathbb{C}$ beschränkt, weil nur die Werte aus dem Kompaktum $\overline{F}$ angenommen werden. Nach dem allgemeinen Satz von Liouville ist f damit konstant. Ist $(f) = (g)$, dann ist der Divisor von $\frac{f}{g}$ leer, da sich die überall gleichen Vielfachheiten die Null- und Polstellen wegheben.

Zu 2) Integration auf ∂F mit dem Residuensatz (evtl wird der den endlich vielen Polstellen 'passend' ausgewichen):

$$0 = \int_{\partial F} f(z) = 2\pi i \sum_{p \in F} \mathrm{res}_p f$$

Wäre genau ein Pol vorhanden, so wäre das Residuum nur dort $\neq 0$.

Satz 8 *Die Weierstraßsche σ-Funktion ist für ein vorgegebenes Gitter Λ definiert durch*

$$\sigma(z) = z \prod_{\lambda \in \Lambda \setminus 0} \Big(1 - \frac{z}{\lambda}\Big) \exp\Big(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}\Big).$$

Sie konvergiert, wie sich zeigen lässt, normal und hat damit offensichtlich Nullstellen bei jedem Gitterpunkt $\lambda \in \Lambda$. Es gibt desweiteren für jedes $\lambda \in \Lambda$ Konstanten a, b mit

$$\sigma(z+\lambda) = \mathrm{e}^{az+b}\sigma(z) \quad (\forall z \in \mathbb{C}).$$

Satz 9 *(von Abel) Seien $u_1, \ldots, u_r, v_1, \ldots, v_s \in \mathbb{C}$, $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbb{N}$ und $\sum m_i = \sum n_j$. Genau dann gibt es eine elliptische Funktion f mit $(f) = \sum m_i(u_i) - \sum n_j(v_j)$, wenn*

$$\sum m_i u_i = \sum n_j v_j \mod \Lambda.$$

Beweis: Wir benötigen nur die Rückrichtung. Seien $a_1, \ldots a_n$ die evtl. mehrfach vorkommenden Null- und $b_1, \ldots, b_n$ die evtl. mehrfach vorkommenden Polstellen. Nach Annahme darf o.B.d.A

$$\sum a_k - \sum b_k = 0$$

angenommen werden, da man z.B. a_1 passend abändert, wenn nötig. Man definiere:

$$f(z) = \prod_{k=1}^{n} \frac{\sigma(z-a_j)}{\sigma(z-b_j)}$$

Für beliebiges, aber festes λ gilt:

$$f(z+\lambda) = \prod_{k=1}^{n} \frac{\sigma(z+\lambda-a_k)}{\sigma(z+\lambda-b_k)} = \prod_{k=1}^{n} \frac{\exp(a(z-a_k)+b)\sigma(z-a_k)}{\exp(a(z-b_k)+b)\sigma(z-b_k)}$$

$$= f(z)\exp\left(a\sum_{k=1}^{n}(z-a_k-(z-b_k)) + \sum_{k=1}^{n}(b_k-b_k)\right) = f(z)\exp\left(a\sum_{j=1}^{n}(b_k-a_k)\right)$$

Letzterer Faktor ist 1. Weil die σ-Funktion Nullstellen auf Λ hat, folgt nach Konstruktion, dass die Null- und Polstellen passend liegen.

3 Biquadratisches Reziprozitätsgesetz

Nun wird mit der Theorie der elliptischen Funktionen das biquadratische Reziprozitätsgesetz bewiesen, d.h. das Restklassensymbol für den Fall $n = 4$ in $K = \mathbb{Q}[i]$.

Statt der expliziten geometrischen Überlegungen, die zu einer elliptischen Funktion mit den folgenden Eigenschaften führen, benutzen wir die bisher aufgebaute Theorie. Die Lösung kann aber nicht auf Restklassensymbole höheren Grades übertragen werden; lediglich im kubischen Fall $n = 3$ kann man recht analog vorgehen.

Proposition 10 *Es gibt eine elliptische Funktion Φ mit:*

1. *Φ hat Periodengitter $\mathbb{Z}[i]$ und Divisor $(\Phi) = (0) + (\frac{1+i}{2}) - (\frac{1}{2}) - (\frac{i}{2})$.*
2. *$\Phi(iz) = i\Phi(z), \Phi(\frac{1+i}{4}) = 1, \Phi(z)\Phi(z-\frac{1}{2}) = i$.*

3. *Sei $\nu \in \mathbb{Z}[i]$ mit $\gcd(2,\nu) = 1$, und sei ϵ die eindeutig bestimmte Einheitswurzel, so dass $\nu \equiv \epsilon \mod 2-2i$. Dann ist*

$$\Phi(\nu z) = \epsilon \prod_{\alpha} \Phi\Big(z - \frac{\alpha}{\nu}\Big),$$

wobei α ein vollständiges Restklassensystem mod ν läuft.

Beweis: Zu 1): Wegen

$$0 + \frac{1+i}{2} = -\frac{1}{2} - \frac{i}{2} \mod \mathbb{Z}[i]$$

gibt es nach 9 eine Funktion zum gewünschten Divisor.

Zu 2): Es kann nach Satz 7(1) festgelegt werden, dass $\Phi(\frac{1+i}{4}) = 1$ ist. Nach Wahl des Divisors von $\Phi(z)$ hat $\Phi(iz)$ den selben, also ist der Quotient konstant. Taylorentwicklung um 0 ergibt:

$$c\Phi(z) = \sum_{n \geqslant 0} a_n c z^n$$

$$\Phi(iz) = \sum_{n \geqslant 0} a_n i^n z^n$$

Somit gilt $c = i^n$ falls $a_n \neq 0$.Weil die Nullstelle in 0 einfach ist, ist $a_1 \neq 0$, also $c = i$. Nach Wahl des Gitters ist $\big(z \mapsto \Phi(z)\big) = -\big(z \mapsto \Phi(z - \frac{1}{2})\big)$, das Produkt also konstant. Und:

$$\Phi\Big(\frac{1+i}{4}\Big)\Phi\Big(\frac{-1+i}{4}\Big) = i\Phi\Big(\frac{1+i}{4}\Big)^2 = i$$

Zu 3): Die Funktion $\Psi(z) = \Phi(\nu z)$ hat den Divisor $(\Psi) = \sum(\frac{\alpha}{\nu}) + \sum(\frac{\alpha}{\nu} + \frac{1+i}{2}) - \sum(\frac{\alpha}{\nu} + \frac{1}{2}) - \sum(\frac{\alpha}{\nu} + \frac{i}{2})$, wenn α ein vollständiges Repräsentantensystem mod ν durchläuft (wegen $\gcd(1+i,\nu) = 1$ kommt dabei keine Überlappung zustande). Das gleiche gilt für $\prod \Phi(z - \frac{\alpha}{\nu})$. γ bezeichne $\frac{1+i}{4}$. Mit 2) gilt:

$$\Phi\Big(\gamma + \frac{\alpha}{\nu}\Big)\Phi\Big(\gamma - \frac{i\alpha}{\nu}\Big) = -i\Phi\Big(\gamma + \frac{\alpha}{\nu}\Big)\Phi\Big(i\gamma + \frac{\alpha}{\nu}\Big)$$

$$-i\Phi\Big(\gamma + \frac{\alpha}{\nu}\Big)\Phi\Big(\gamma - \frac{1}{2} + \frac{\alpha}{\nu}\Big) = -i \cdot i = 1$$

Weil ein Halbsystem so wählbar ist, dass für jeden Repräsentanten entweder α oder $-i\alpha$ darin liegt, folgt $\prod_\alpha \phi(\gamma + \frac{\alpha}{\gamma}) = 1$, somit auch $\prod_\alpha \phi(\gamma - \frac{\alpha}{\gamma})$. Somit kann die Quotienten-Konstante an der Stelle $\nu\gamma$ bestimmt werden:

$$\Phi(\gamma\nu) = \Phi(\epsilon\gamma + (\gamma - \epsilon)\nu) = \Phi(\epsilon\gamma) = \epsilon\Phi(\gamma) = \epsilon$$

Hierbei wurde benutzt, dass $(2-2i)\gamma \in \mathbb{Z}[i]$ und dass Φ $\mathbb{Z}[i]$-peridiosch ist.

Satz 11 *Für primäre (d.h. $\equiv 1$ mod $2-2i$) Primelemente gilt:*

$$\Big(\frac{\nu}{\mu}\Big)_4 = (-1)^{\frac{N\nu-1}{4}\cdot\frac{N\mu-1}{4}}\Big(\frac{\mu}{\nu}\Big)_4$$

Beweis: Zu solchen μ, ν bezeichne A_μ bzw A_ν jeweils $\frac{1}{4}$-Systeme, sowie R_ν ein Repräsentantensystem mod ν. Weiterhin definiere man

$$P(x,y) = \prod_{k=1}^{4} \Phi(x + i^k y)$$

und bemerke $P(x,y) = -P(y,x)$. Dann ist nach Lemma 5 und Proposition 10(3):

$$\left(\frac{\nu}{\mu}\right)_4 = \prod_{\alpha \in A_\mu} \frac{\Phi(\nu\alpha/\mu)}{\Phi(\alpha/\mu)} = \prod_{\alpha \in A_\mu} \frac{\prod_{\beta \in R_\nu} \Phi(\alpha/\mu - \beta/\nu)}{\Phi(\alpha/\mu)}$$

$$= \prod_{\alpha \in A_\mu} \prod_{\beta \in R_\nu \setminus 0} \Phi(\alpha/\mu - \beta/\nu) = \prod_{\alpha \in A_\mu} \prod_{\beta \in \alpha_\nu} P(\alpha/\mu, \beta/\nu)$$

Vertauscht man ν und μ, so erhält man das gleiche Ergebnis, allerdings mit $|A_\mu| \cdot |A_\nu|$ mal dem Faktor (-1). Daraus folgt die Behauptung.

Die Einschränkung 'primär' vereinfacht lediglich die Notation, da sich jede Nichteinheit α mit $1 + i \nmid \alpha$ nur um eine Einheit davon unterscheidet.

Für das kubische Reziprozitätsgesetz im Ring der Eisensteinzahlen $\mathbb{Z}[\zeta_3]$ kann man ein ähnliches Φ konstruieren, mit dem man sehr analog vorgeht.

Literatur

[1] F. Lemmermeyer, "Reciprocity Laws" *Springer-Verlag Berlin Heidelberg* (2000)

[2] E. Freitag, R. Busam, "Funktionentheorie" *Springer-Verlag Berlin Heidelberg* (1993)

[3] K. Ireland, M. Rosen, "A Classical Introduction to Modern Number Theory" *Spring-Verlag New York* (1990)

[4] T. Kubota, "Some arithmetical applications of an elliptic function" *J. Reine Angew. Math.* **214/215** (1964), 141-145

[5] G. Eisenstein, "Application de l'algèbre à l'arithmétique transcendante" *J. Reine Angew. Math.* **29** (1845), 177-184