

Vortrag 14 – Die Dedekindsche Zetafunktion

Primzahlen der Form $x^2 + ny^2$

Seminar im WS 2021/2022

Vinzenz Baumann

Zusammenfassung

Wir führen die Dedekindsche Zetafunktion ζ_K eines Zahlkörpers K (als Eulerprodukt) ein, zeigen, dass sie eine holomorphe Funktion auf $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}$ definiert, und leiten ihre Dirichletreihenentwicklung her. Anschließend beweisen wir, dass ζ_K im Falle eines quadratischen Zahlkörpers K als Produkt der Riemannschen Zetafunktion ζ mit einer gewissen L -Funktion geschrieben werden kann. Ist K imaginär quadratisch, so erhalten wir auf diese Weise eine handliche Formel für die Anzahl der Darstellungen einer natürlichen Zahl $n \in \mathbb{N}$ als $n = f(x, y)$, wobei f eine reduzierte quadratische Form $f \in \mathbb{Z}[X, Y]$ mit Diskriminante Δ_K ist.

Definition 1.1 (Riemannsche Zetafunktion). Die *Riemannsche Zetafunktion* ist definiert als

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

mit

$$\zeta : \{s \in \mathbb{C} : \operatorname{Re}(s) > 1\} \rightarrow \mathbb{C}$$

Dabei ist $\prod_p \frac{1}{1 - p^{-s}}$ die Definition als Eulerprodukt über Primzahlen und $\sum_{n=1}^{\infty} \frac{1}{n^s}$ die Definition als Dirichletreihe.

Definition 1.2 (Zahlkörper). Ein (*algebraischer*) *Zahlkörper* ist eine endliche Körpererweiterung der rationalen Zahlen \mathbb{Q} . Sei im Folgenden K ein Zahlkörper. Man nennt einen Zahlkörper *quadratisch*, wenn er die Grad 2 über \mathbb{Q} hat.

Definition 1.3 (Ganzheitsring). Sei K ein Zahlkörper. Dann definiert $\mathcal{O}_K := K \cap \mathbb{A}$ den *Ganzheitsring* des Zahlkörpers K , wobei \mathbb{A} als Ring der ganz algebraischen Zahlen definiert ist.

Definition 1.4 (Idealnorm). Sei K ein Zahlkörper mit Ganzheitsring

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

welches ungleich dem Nullideal ist. So ist die *Idealnorm* definiert durch

$$N_{K|\mathbb{Q}}(\mathfrak{a}) := [O_K : \mathfrak{a}] = |O_K/\mathfrak{a}|$$

Bemerkung. (1) Ist \mathfrak{a} ein Hauptideal $\langle a \rangle$, dann ist

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

(2) Die Norm ist multiplikativ. Es ist $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$

Definition 1.5 (Dedekindsche Zetafunktion). Sei K ein Zahlkörper. Wir definieren die *Dedekindsche Zetafunktion* ζ_K zum Zahlkörper K durch

$$\zeta_K(s) := \prod_{\mathfrak{p}} \frac{1}{1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{-s}}$$

wobei sich das Produkt über alle Primideale $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ erstreckt.

Satz 1.1. Für $K = \mathbb{Q}$ stimmt die Dedekindsche Zetafunktion mit der Riemanschen Zetafunktion überein.

Beweis. Es ist $O_K = \mathbb{Z}$, also sind die Primideale $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ gerade jene Hauptideale $\langle p \rangle \subseteq \mathbb{Z}$, die von Primzahlen p erzeugt werden. Führen wir diesen Gedanken weiter so gilt $N_{\mathbb{Q}|\mathbb{Q}}(\langle p \rangle) = |\mathbb{Z}/\langle p \rangle| = p$, also erhalten wir

$$\zeta_{\mathbb{Q}}(s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s)$$

□

Definition 1.6 (Unendliches Produkt). Sei $(a_\nu) \subset \mathbb{C}$. Das *unendliche Produkt* $\prod_{\nu=1}^{\infty} (a_\nu)$ existiert, falls gilt:

- (1) Entweder sind alle $a_\nu \neq 0$, es existiert der Grenzwert $a := \lim_{n \rightarrow \infty} \prod_{\nu=1}^n a_\nu$ und es ist $a \neq 0$
- (2) Oder es gibt ein ν_0 , so dass $a \neq 0$ für alle $\nu \geq \nu_0$ ist, und es existiert $a^* := \prod_{\nu=\nu_0}^{\infty} a_\nu$ im obigen Sinne. Dann setzen wir $a := a^* \cdot \prod_{\nu=1}^{\nu_0-1} a_\nu$.

Bemerkung (Konvergenz von unendlichen Produkten). Das unendliche Produkt $\prod_{\nu=1}^{\infty} (a_\nu)$ existiere. Dann gilt:

- (1) $\prod_{\nu=1}^{\infty} a_\nu = 0$ genau dann, wenn mindestens ein a_ν gleich Null ist.
- (2) Die Folge (a_ν) ist "1-Folge", das heißt es ist $\lim_{\nu \rightarrow \infty} a_\nu = 1$.

Bemerkung (Konstruktion des Logarithmus im Komplexen). Durch die Einschränkung der Exponentialfunktion auf den Streifen $S = \{z \in \mathbb{C} : \operatorname{Im}(z) \in (-\pi, \pi)\}$ wird sie injektiv und der Satz der Umkehrfunktion ist anwendbar. Daraus folgt:

$$\operatorname{Log}(z) := \log(r) + \phi$$

mit $r = |z|$ mit $\arg(z) = \phi$. Hierbei bezeichnet \log den reellen und Log den Hauptzweig des komplexen Logarithmus.

Bemerkung (Cauchy-Riemann-Differentialgleichung in Polarkoordinaten (CRDFG)). Durch die Darstellung einer komplexen Zahl als $z = r \cdot e^{i\phi}$ folgt eine besondere Form der CRDFG. Es ist:

$$(1) \frac{\delta u}{\delta r} = \frac{1}{r} \frac{\delta v}{\delta \phi}$$

und

$$(2) \frac{\delta v}{\delta r} = -\frac{1}{r} \frac{\delta u}{\delta \phi}$$

mit $f := u + iv$.

Folgerung (Log ist holomorph). Mit obiger Gleichung folgt mit $\text{Log}(r \cdot e^{i\phi}) := \log(r) + i\phi$, dass

$$\frac{\delta u}{\delta r} = \frac{1}{r} = \frac{1}{r} \frac{\delta v}{\delta \phi}$$

und

$$\frac{\delta v}{\delta r} = 0 = -\frac{1}{r} \frac{\delta u}{\delta \phi}$$

mit $f = \log(r) + i\phi = u + iv$.

Bemerkung (Potenzreihe des Logarithmus auf $\mathbb{C} \setminus \{0\}$). Es gilt

$$\text{Log}(1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{(n-1)}}{n} (z-1)^n$$

für alle $z \in \mathbb{C}$ mit $|z| < 1$.

Definition 1.7 (Normale Konvergenz). Eine Reihe von Funktionen $f_1 + f_2 + f_3 + \dots$ $f_n : D \rightarrow \mathbb{C}$ für $D \subset \mathbb{C}$ und $n \in \mathbb{N}_0$ heißt *normal konvergent* in D , falls es zu jedem Punkt $a \in D$ eine Umgebung U und eine Folge $(M_n)_{n \geq 0}$ nicht negativer reeller Zahlen gibt, so dass gilt

$$|f_n(z)| \leq M_n$$

für alle $z \in U \cap D$, für alle $n \in \mathbb{N}_0$ und $\sum_{n=0}^{\infty} M_n$ konvergiert.

Bemerkung (Identitätssatz). Seien f und g holomorphe Funktionen auf einer Umgebung U von z_0 und sei z_0 ein Häufungspunkt der Koinzidenzmenge $\{z \in U | f(z) = g(z)\}$, dann existiert eine Umgebung V von z_0 mit $f(z) = g(z)$ für alle $z \in V$.

Lemma 1.2. Sei $\sum_{n=1}^{\infty} f_n$ eine normal konvergente Reihe von holomorphen Funktionen $f_n : D \rightarrow \mathbb{C}$ auf einem Gebiet $D \subseteq \mathbb{C}$. Dann existiert für jeden Punkt $z \in \mathbb{C}$ eine offene Umgebung $z \in U \subseteq \mathbb{C}$ so wie eine natürliche Zahl $N \in \mathbb{N}$, sodass $|f_n(z)| \leq \frac{1}{2}$ für alle $z \in U$ und alle $n \geq N$ gilt. In diesem Fall ist durch

$$F_N(z) := \sum_{n=N}^{\infty} \text{Log}(1 + f_n(z))$$

eine holomorphe Funktion $F_N : U \rightarrow \mathbb{C}$ definiert. Weiter gilt

$$\lim_{m \rightarrow \infty} \prod_{n=1}^m (1 + f_n(z)) = \prod_{n=1}^{N-1} (1 + f_n(z)) \cdot e^{F_N(z)}$$

für alle $z \in U$. Insbesondere stellt das unendliche Produkt

$$\prod_{n=1}^{\infty} (1 + f_n(z)) := \lim_{m \rightarrow \infty} \prod_{n=1}^m (1 + f_n(z))$$

eine holomorphe Funktion auf D dar.

Beweis. Für den Beweis benötigen wir zunächst zwei Hilfslemmata.

Hilfslemma 1. Aus $|f_n(z)| \leq \frac{1}{2}$ folgt $1 + f_n(z) \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$.

Beweis. Es ist $|f_n(z)| \geq 0$, daher ist die Anwendung der Wurzelfunktion und das Quadrieren eine Äquivalenzumformung. So folgt mit der Definition des komplexen Betrags direkt:

$$|(f_n(z))|^2 = \sqrt{f_n(z) \cdot \overline{f_n(z)}}^2 = \sqrt{f_n(z)}^2 \cdot \sqrt{\overline{f_n(z)}}^2 = f_n(z) \cdot \overline{f_n(z)}$$

und wegen der Positiven Definitheit des Betrags gilt bereits, dass jeweils beide Ausdrücke größer oder gleich Null sind. Die Null wird aber durch die Addition mit der 1 ausgeschlossen. So folgt $1 + f_n(z) \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$

Insbesondere:

Es ist $\text{Log}(1 + f_n(z))$ für alle $z \in U$ und $n \geq N$ definiert, da aus der obiger Betrachtung hervorgeht, dass $1 + f_n(z)$ für alle z im Definitionsbereich von Log enthalten ist. \square

Hilfslemma 2. Abschätzung $|\text{Log}(1 + z)| \leq 2|z|$ für alle $z \in \mathbb{C}$ mit $|z| \leq \frac{1}{2}$

Beweis.

$$\begin{aligned} |\text{Log}(1 + z)| &= \left| \sum_{n=1}^{\infty} (-1)^{(n-1)} \frac{z^n}{n} \right| \leq |z| \sum_{n=0}^{\infty} \frac{|z|^n}{n+1} \\ &< |z| \cdot \left(\frac{1}{1} + \frac{1}{2 \cdot 2} + \frac{1}{3 \cdot 2^2} + \dots + \frac{1}{(n+1) \cdot 2^{(n)}} + \dots \right) = 2 \cdot |z| \end{aligned}$$

wobei bei dem letzten Gleichheitszeichen der Wert der geometrischen Reihe benutzt wurde. Nämlich

$$\sum_{n=0}^{\infty} \frac{1}{(n+1) \cdot 2^{(n)}} < \sum_{n=0}^{\infty} \frac{1}{2^{(n)}} = \sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1 - (\frac{1}{2})} = 2$$

\square

Beweis zu Lemma ??. Aus Hilfslemma ?? folgt $(1 + f_n(z)) \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$.

Zeige weiter $F_N(z) := \sum_{n=N}^{\infty} \text{Log}(1 + f_n(z))$ ist normal konvergent auf U . Dies folgt daraus, dass $|\text{Log}(1 + z)| \leq 2|z|$ für $z \in \mathbb{C}$ mit $|z| \leq \frac{1}{2}$ nach Hilfslemma ?? und der Tatsache, dass mit der Abschätzung von $|\text{Log}(1 + z)| \leq 2|z|$ mit $|f_n(z)| \leq \frac{1}{2}$ $F_N(z)$ genau der Definition der normalen Konvergenz entspricht. Insbesondere stellen F_N und e^{F_N} holomorphe Funktionen dar, da Holomorphie

unter Bildung von Summen, Produkten und Verkettungen erhalten bleibt. Für beliebige $z \in \mathbb{C}$ und $m \leq N$ gilt, dass

$$\begin{aligned} \prod_{n=1}^m (1+f_n(z)) &= \prod_{n=1}^{N-1} (1+f_n(z)) \cdot \prod_{n=N}^m (1+f_n(z)) = \prod_{n=1}^{N-1} (1+f_n(z)) \cdot \prod_{n=N}^m (e^{\text{Log}(1+f_n(z))}) \\ &= \prod_{n=1}^{N-1} (1+f_n(z)) \cdot \prod_{n=N}^m (e^{\sum_{n=N}^m \text{Log}(1+f_n(z))}) \end{aligned}$$

wobei hier benutzt wurde, dass e^{F_N} auf der bereits oben angesprochenen Einschränkung konform mit dem komplexen Logarithmus agiert. Mit der Stetigkeit der Exponentialfunktion folgt

$$\lim_{m \rightarrow \infty} \prod_{n=1}^m (1+f_n(z)) = \prod_{n=1}^{N-1} (1+f_n(z)) \cdot e^{F_N(z)}$$

für alle $z \in U$ gilt. Durch die Holomorphie von $1+f_n$ für $1 \leq n \leq N-1$ und e^{F_N} und dem Umstand, dass endliche Produkte holomorpher Funktionen wiederum holomorph sind, stellt

$$\prod_{n=1}^{\infty} (1+f_n(z))$$

als unendliches Produkt eine holomorphe Funktion - nicht nur für alle z_0 auf U , sondern aufgrund der Offenheit der Umgebung U auf ganz D - dar.

□

Proposition 1.3. *Sei K ein Zahlkörper. Dann konvergiert das unendliche Produkt*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{-s}}$$

für $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$. Des weiteren stellt $\zeta_K(s): \{s \in \mathbb{C}: \text{Re}(s) > 1\} \rightarrow \mathbb{C}$ eine holomorphe Funktion dar.

Beweis. Das unendliche Produkt

$$\zeta *_{K}(s) = \prod_{\mathfrak{p}} (1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{-s})$$

für $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$ konvergiert, beziehungsweise ist auf diesem Gebiet holomorph. Zunächst ist es wichtig zu sehen, dass keiner der Faktoren $1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{-s}$ eine Nullstelle in der Menge $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$ besitzt.

Dies folgt schnell über:

Angenommen $1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)}$ hat eine Nullstelle in der Menge $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$, so folgt $1 = N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)}$. Das bedeutet nach der Norm $|O_K/\mathfrak{p}| = 1$, d. h. $\mathfrak{p} = O_K$. Dann ist aber \mathfrak{p} nicht echt in O_K und daher kein Primideal.

Trifft die Behauptung auf $\zeta *_{K}$ zu, so gilt zusätzlich $\zeta *_{K} \neq 0$ für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$. Denn wäre $\zeta *_{K} = 0$, so wäre nach oben stehendem Satz mindestens ein Faktor gleich Null. Dies haben wir aber eben ausgeschlossen. So ist

auch ζ_K^{-1} holomorph auf diesem Gebiet.
Es genügt nun zu zeigen, dass $\zeta_K^{-1} = \zeta_K$. Es ist

$$\begin{aligned}\zeta_K^{-1} &= \left(\prod_{\mathfrak{p}} (1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)}) \right)^{-1} \\ &= \prod_{\mathfrak{p}} (1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)})^{-1} = \prod_{\mathfrak{p}} \frac{1}{1 - N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)}} = \zeta_K\end{aligned}$$

Damit folgt ζ_K ist holomorph auf $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}$, falls wir zeigen können, dass ζ_K holomorph ist. Der Nachweis der normalen Konvergenz der Funktionenreihe

$$\sum_{\mathfrak{p}} N_{K|\mathbb{Q}}(\mathfrak{p})^{-s}$$

auf $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}$ folgt aus

$$\sum_{\mathfrak{p}} |e^{\operatorname{Log}(N_{K|\mathbb{Q}}(\mathfrak{p})^{(-s)})}| = \sum_{\mathfrak{p}} |e^{-s \cdot \operatorname{Log}(N_{K|\mathbb{Q}}(\mathfrak{p}))}|$$

und unter der Verwendung von Folgendem:
Es ist mit $z = x + iy$

$$|e^z| = e^x$$

da

$$\begin{aligned}|e^z| &= |e^{x+iy}| = |e^x \cdot e^{iy}| = |e^x| \cdot |e^{iy}| = e^x \cdot |e^{iy}| = e^x \cdot |\cos(y) + i \cdot \sin(y)| \\ &= e^x \cdot \sqrt{\cos^2(x) + \sin^2(x)} = e^x \cdot 1\end{aligned}$$

und mithilfe der folgenden Betrachtung:

Jedes Primideal $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ in $\mathfrak{p} \in O_K$ enthält eine Primzahl p und \mathfrak{p} tritt in diesem Fall in der Primidealzerlegung (siehe Vortrag 5) des Hauptideals $\langle p \rangle = p \cdot O_K$ auf. Somit gibt es zu jeder Primzahl p nur endlich viele Primideale $\mathfrak{p} \subset O_K$, die p enthalten. Präziser gilt: Für fast alle Primzahlen p gibt es höchstens $[K : \mathbb{Q}]$ verschiedene Primideale $\mathfrak{p} \subset O_K$, die p enthalten.

So folgt:

$$\sum_{\mathfrak{p}, p \in \mathfrak{p}, p > C} (N_{K|\mathbb{Q}}(\mathfrak{p}))^{-\operatorname{Re}(s)} \leq [K : \mathbb{Q}] \cdot \sum_{p > C} p^{-\operatorname{Re}(s)}$$

Den letzten Ausdruck kann man mithilfe der Geometrischen Reihe abschätzen. \square

Definition 1.8 (Dirichletreihe). Eine (formale) *Dirichletreihe* ist eine Reihe der Form

$$\mathbb{D}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

wobei $(a_n)_{n \in \mathbb{N}}$ eine beliebige Folge komplexer Zahlen beschreibt.

Proposition 1.4. *Sei K ein Zahlkörper. Dann gilt für alle $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > 1$, dass*

$$\zeta_K(s) = \sum_{\mathfrak{J}} \frac{1}{N_{K|\mathbb{Q}}(\mathfrak{J})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

wobei sich die Summation in $\sum_{\mathfrak{J}}$ über alle Ideale $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ erstreckt und a_n für $n \in \mathbb{N}$ die Anzahl der Ideale $\mathfrak{J} \subseteq O_K$ mit $N_{K|\mathbb{Q}}(\mathfrak{J}) = n$ bezeichnet. Insbesondere gilt:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Beweis. Zur Vereinfachung, führt man eine beliebige Nummerierung auf der Menge aller Primideale $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ ein. Diese hat die Form

$$\{\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K\} = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots\}$$

Die Abzählbarkeit dieser Menge folgt aus:

Jedes Primideal $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ in O_K enthält eine Primzahl p . Die Primideale, die in O_K sind und p enthalten, sind genau die Primideale, die in der Faktorisierung des Hauptideals pO_K auftreten (nach Vortrag 5). In der Faktorisierung von pO_K treten aber nur endlich viele Primideale auf, das heißt zu jeder Primzahl p gibt es nur endlich viele Primideale, die p enthalten. Somit besteht die Menge der Primzahlen, die p enthalten, aus einer abzählbaren Vereinigung von abzählbaren Mengen - nämlich die Vereinigung über alle Primzahlen und die Vereinigung aller Primideale, die p enthalten. Abzählbare Vereinigungen abzählbarer Mengen sind wiederum abzählbare Mengen.

Sei weiter $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > 1$ beliebig, dann ist mit $N_{K|\mathbb{Q}} \geq 2$ für jedes $m \in \mathbb{N}$, siehe Beweis Proposition ???. So folgt:

$$\prod_{m=1}^n \frac{1}{1 - N_{K|\mathbb{Q}}(\mathfrak{p}_m)^{-s}} = \prod_{m=1}^n \sum_{k=0}^{\infty} (N_{K|\mathbb{Q}}(\mathfrak{p}_m))^{-k \cdot s} = \prod_{m=1}^n \sum_{k=0}^{\infty} (N_{K|\mathbb{Q}}(\mathfrak{p}_m^k))^{(-s)}$$

Daraus resultiert mit Anwendung der Geometrischen Reihe auf $(N_{K|\mathbb{Q}}(\mathfrak{p}_m^k))^{(-s)} < 1$, dass das Produkt absolut konvergiert, da es Produkt absolut konvergenter Reihen ist. Mithilfe des Umordnungssatzes für absolut konvergente Reihen und der Multiplikativität der Norm spricht dann:

$$\begin{aligned} \prod_{m=1}^n \sum_{k=0}^{\infty} (N_{K|\mathbb{Q}}(\mathfrak{p}_m^k))^{(-s)} &= 1 + \sum_{j=1}^n \sum N_{K|\mathbb{Q}}(\mathfrak{p}_{m_1}^{\alpha_1})^{(-s)} \cdots N_{K|\mathbb{Q}}(\mathfrak{p}_{m_j}^{\alpha_j})^{(-s)} \\ &= 1 + \sum_{j=1}^n \sum N_{K|\mathbb{Q}}(\mathfrak{p}_{m_1}^{\alpha_1} \cdots \mathfrak{p}_{m_j}^{\alpha_j})^{(-s)} \end{aligned}$$

wobei sich die unbeschriftete Summe über alle Teilmengen $\{m_1, \dots, m_j\} \subseteq \{1, \dots, n\}$ und alle $(\alpha_1, \dots, \alpha_j)$ erstreckt. Mit $n \rightarrow \infty$ folgt mit der vorherigen Proposition, dass

$$1 + \sum_{j=1}^{\infty} \sum N_{K|\mathbb{Q}}(\mathfrak{p}_{m_1}^{\alpha_1} \cdots \mathfrak{p}_{m_j}^{\alpha_j})^{(-s)}$$

Aufgrund der eindeutigen Primidealzerlegung in O_K und dass $N_K(O_K)^{-s} = 1$ tritt jedes Ideal $\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq O_K$ genau einmal als $\mathfrak{p}_{m_1}^{\alpha_1} \cdots \mathfrak{p}_{m_j}^{\alpha_j}$ genau einmal auf. Wieder aufgrund der Umordnung folgt daraus

$$\zeta_K(s) = \sum_{\mathfrak{p}} \frac{1}{(N_{K|\mathbb{Q}}(\mathfrak{p}))^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

und im Falle $K = \mathbb{Q}$ gibt es für jede natürliche Zahl genau ein Ideal mit Norm n , nämlich $\langle n \rangle = n\mathbb{Z} \subseteq \mathbb{Z}$, daher gilt $a_n = 1$ für alle $n \in \mathbb{N}$. So folgt insbesondere:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

□

Bemerkung. Der aus Vortrag 8 existierende Gruppenhomomorphismus ist als Funktion aufgefasst $\chi_K: \mathbb{N} \rightarrow \{-1, 0, 1\}$, wobei man für $n \in \mathbb{N}$ schreibt, dass

$$\chi_K = \begin{cases} 0 & \text{falls } \text{ggT}(n, \Delta_K) > 1, \\ \chi_K(\bar{n}) & \text{falls } \text{ggT}(n, \Delta_K) = 1 \end{cases}$$

Theorem 1.5. Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. Dann definiert das Eulerprodukt

$$L(s, \chi_K) := \prod_p \frac{1}{1 - \chi_K(p)p^{(-s)}}$$

eine holomorphe Funktion $L(s, \chi_K): \{s \in \mathbb{C}: \text{Re}(s) > 1\} \rightarrow \mathbb{C}$ und es gilt

$$\zeta_K(s) = \zeta(s) \cdot L(s, \chi_K)$$

für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$. Man nennt $L(\cdot, \chi_K)$ die L -Funktion zum Gruppenhomomorphismus χ_K .

Beweis. Wenn wir zeigen können, dass

$$\prod_{\mathfrak{p}, p \in \mathfrak{p}} \frac{1}{(1 - N_{K|\mathbb{Q}}(\mathfrak{p}))^{(-s)}} = \frac{1}{1 - p^{-s}} \cdot \frac{1}{1 - \chi_K(p)p^{-s}}$$

für jede Primzahl p gilt, dann folgt daraus, dass

$$L(s, \chi_K) = \zeta_K(s) \cdot \zeta(s)^{-1}$$

für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$ gilt, da $\zeta(s) \neq 0$. Dadurch ist

$$L(\cdot, \chi_K) = \zeta_K \cdot \zeta^{-1}: \{s \in \mathbb{C}: \text{Re}(s) > 1\} \rightarrow \mathbb{C}$$

eine holomorphe Funktion.

Fall 1. $O_K = \mathbb{Z}[\sqrt{-d}]$

Betrachte also $d \equiv 2, 3 \pmod{4}$. Die Primideale $\mathfrak{p} \subseteq O_K$, die p enthalten, entsprechen genau den Primidealen im Ring

$$O_K/\langle p \rangle \cong \mathbb{Z}[X]/\langle X^2 - d, p \rangle \cong (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 - \bar{d} \rangle$$

Dies folgt aus Vortrag 3, Beweis Proposition 1, aus dem Isomorphiesatz.

Fall 1.1. Angenommen $p \mid \Delta_K$. Das bedeutet im Fall $d \equiv 2, 3 \pmod{4}$, dass entweder $p = 2$ oder $p \mid d$. Im ersten Fall ist $X^2 - \bar{d} = (X - \bar{d})^2 \in (\mathbb{Z}/2\mathbb{Z})[X]$. Im zweiten Fall ist $X^2 - \bar{d} = X^2 \in (\mathbb{Z}/p\mathbb{Z})[X]$, also hat das Polynom $X^2 - \bar{d} \in (\mathbb{Z}/p\mathbb{Z})$ auf jeden Fall eine doppelte Nullstelle in $\mathbb{Z}/p\mathbb{Z}$. Vermöge des Isomorphismus von oben bedeutet das einerseits, dass $\langle p \rangle \subseteq O_K$ kein Primideal ist und andererseits, dass es ein eindeutiges Primideal $\mathfrak{p} \subseteq O_K$ mit $p \in \mathfrak{p}$ gibt. Dies folgt daraus, dass eine Primzahl genau dann prim in O_K ist, wenn das Polynom keine Nullstellen in $(\mathbb{Z}/p\mathbb{Z})[X]$ hat. Des Weiteren ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Das einzige maximale und damit prime Ideal ist das Nullideal, welches p enthält.

In Anbetracht der eindeutigen Primfaktorzerlegung kann das nur bedeuten, dass $\langle p \rangle = \mathfrak{p}^k$ für ein $k \geq 2$ gilt. Da aber $p^2 = N_{K|\mathbb{Q}}(\langle p \rangle) = N_{K|\mathbb{Q}}(\mathfrak{p}^k) = N_{K|\mathbb{Q}}(\mathfrak{p})^k$ gilt, folgt aus der eindeutigen Primfaktorzerlegung in \mathbb{Z} , dass $k = 2$ und $N_{K|\mathbb{Q}}(\mathfrak{p}) = p$. So ist die linke Seite gegeben durch $\frac{1}{1-p^{-s}}$ und die rechte Seite

$$\frac{1}{1-p^{-s}} \cdot \frac{1}{1-0 \cdot p^{-s}} = \frac{1}{1-p^{-s}}$$

also die Gleichheit beider Seiten.

Fall 1.2. Angenommen $p \nmid \Delta_K$ und $\chi_K(\bar{p}) = \left(\frac{\Delta_K}{p}\right) = 1$. Da $\Delta_K = 4d$, folgt daraus, dass

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^2 \cdot \left(\frac{d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{\Delta_K}{p}\right) = 1$$

Dann liefert die Definition des Legendre Symbols, dass $\bar{d} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ein Quadrat ist, sagen wir $\bar{d} = \bar{y}^2$ für ein $y \in \mathbb{Z}$, $p \nmid y$. Das ergibt, dass

$$X^2 - \bar{d} = (X - \bar{y})(X + \bar{y})$$

in $(\mathbb{Z}/p\mathbb{Z})[X]$ gilt, also dass $X^2 - \bar{d}$ zwei verschiedene Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ hat. Das bedeutet, dass es genau zwei verschiedene Primideale in O_K gibt, die p enthalten, und wie in Fall 1.1, dass diese Norm p haben. Somit ist die linke Seite gegeben durch $\left(\frac{1}{1-p^{-s}}\right)^2$, die rechte Seite durch

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

und damit wiederum gleich.

Fall 1.3. Angenommen $p \nmid \Delta_K$ und $\chi_K(\bar{p}) = \left(\frac{\Delta_K}{p}\right) = -1$. Wie in Fall 1.2 folgt $\left(\frac{d}{p}\right) = -1$, also dass $\bar{d} \in (\mathbb{Z}/p\mathbb{Z})^\times$ kein Quadrat ist. Das bedeutet aber, dass das Polynom $X^2 - \bar{d} \in (\mathbb{Z}/p\mathbb{Z})[X]$ keine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt. Bei einem Polynom von Grad 2 ist das wiederum äquivalent dazu, dass es keine Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ besitzt. Damit ist das Polynom irreduzibel. Daraus folgt aber $(\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 - \bar{d} \rangle$ ist ein Körper. Also trifft wegen des Isomorphismus Selbiges auf $O_K/\langle p \rangle$ zu. Das macht das von p erzeugte Ideal in O_K zu einem maximalen und insbesondere zu einem Primideal. Somit haben wir wieder für die linke Seite $\frac{1}{1-(p^2)}^{-s} = \frac{1}{1-(p)}^{-2s}$ und die rechte Seite stimmt damit überein

durch

$$\frac{1}{1 - (p^{-s})} \cdot \frac{1}{(1 - (-1)1p^{-s})} = \frac{1}{(1 - p^{-s}(1 + p^{-s}))} = \frac{1}{1 - p^{-2s}}$$

Fall 2. $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Betrachte also $d \equiv 1 \pmod{4}$

Fall 2.1. Angenommen $p \mid \Delta_K$. Im Falle $d \equiv 1 \pmod{4}$ bedeutet das $p \mid d$ da $\Delta_K = d$. Das folgt aus dem Bilden der Diskriminante aus dem Polynom $4 \cdot (X^2 - X + \frac{1-d}{4})$. So folgt direkt $2(X-1)^2 - d$ hat zwei Nullstellen in $\mathbb{Z} \setminus p\mathbb{Z}[X]$ und wie in Fall 1.1 folgt Gleichheit der beiden Seiten.

Fall 2.2. Angenommen $p \nmid \Delta_K$ und $\chi_K(\bar{p}) = (\frac{\Delta_K}{p}) = 1$. So folgt direkt $(\frac{d}{p}) = 1$ mit Definition des Legendre Symbol, dass $\bar{d} \in (\mathbb{Z} \setminus p\mathbb{Z})^\times$ ein Quadrat ist und somit hat $(2x-1)^2 - d$ zwei Nullstellen in $\mathbb{Z} \setminus p\mathbb{Z}$. Der Rest folgt analog dem Beweis von Fall 1.2.

Fall 2.3 Angenommen $p \nmid \Delta_K$ und $\chi_K(\bar{p}) = (\frac{\Delta_K}{p}) = -1$. So ist \bar{d} wie in Fall 1.3 kein Quadrat und hat in $\mathbb{Z} \setminus p\mathbb{Z}$ keine Nullstellen. Der Beweis schließt analog wie in Fall 1.3.

□

Theorem 1.6. Sei $K = \mathbb{Q}(\sqrt{d})$ ein imaginär quadratischer Zahlkörper. Für jede natürliche Zahl $n \in \mathbb{N}$ bezeichnen wir mit $r_k(n)$ die Anzahl der Paare $(x, y) \in \mathbb{Z}^2$, sodass $n = f(x, y)$ für eine reduzierte quadratische Form $f \in \mathbb{Z}[X, Y]$ mit Diskriminante Δ_K gilt. Dann ist

$$r_k(b) \stackrel{(1)}{=} |O_K^\times| \cdot a_n \stackrel{(2)}{=} |O_K^\times| \cdot \sum_{d|n} \chi_K(n)$$

wobei $(a_n)_{n \in \mathbb{N}}$ die Folge der Koeffizienten der Dirichletreihe zu ζ_K ist, und

$$|O_K^\times| = \begin{cases} 4, & \text{falls } d = -1 \\ 6, & \text{falls } d = -3 \\ 2, & \text{sonst} \end{cases}$$

gilt.

Beweis. Die Aussage über $|O_K^\times|$ wurde in Vortrag 3 bewiesen. Somit verbleibt es die Gleichheitszeichen (1) und (2) zu zeigen. Beginne mit (2). Es ist

$$L(s, \chi_K) = \sum_{n=1}^{\infty} \frac{\chi_K(n)}{n^s}$$

für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$. Dies folgt aus dem folgenden Hilfslemma ??.

Hilfslemma 3. Sei f eine multiplikative Funktion, sodass die $\sum f_n(n)$ absolut konvergiert. So kann der Wert der Reihe als ein absolut konvergentes Produkt ausgedrückt werden. Im Spezialfall der strikten Multiplikativität von f erhält man $\sum_{n=1}^{\infty} f_n = \prod_p$.

Beweis. Sei

$$P(x) = \prod_{p \leq x} \{1 + f(p) + f(p^2) + \dots\}$$

welches sich über alle Primzahlen p erstreckt. Da es ein Produkt einer endlichen Anzahl von absolut konvergenter Reihen ist, ist es erlaubt die Reihen zu multiplizieren und gegebenenfalls umzuordnen ohne den Wert zu verändern. Hierbei wählt man die Form

$$f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot f(p_3^{a_3}) \cdot \dots \cdot f(p_r^{a_r}) = f(p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \dots \cdot p_r^{a_r})$$

Dies folgt aus der Multiplikativität von f . Benutzt man nun die Eindeutigkeit der Primfaktorzerlegung, so folgt, dass $P(x) = \sum_{n \in A} f(n)$ wobei A aus allen n besteht mit Primfaktoren, welche kleiner oder gleich x sind. Daraus folgt

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n)$$

wobei B die Menge derjenigen n ist, die mindestens einen Primfaktor strikt größer x besitzen. Hieraus resultiert

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|$$

Läuft jetzt $x \rightarrow \infty$, so geht der ganz rechte Ausdruck gegen Null, da $\sum |f(n)|$ konvergent ist. So konvergiert $P(x)$ gegen $\sum f(n)$ für $x \rightarrow \infty$. Hier ist es noch wichtig zu sehen, dass das unendliche Produkt der Form $\prod 1 + a_n$ absolut konvergiert, wenn $\sum a_n$ absolut konvergiert. In diesem Fall folgt:

$$\sum_{p \leq x} |f(p) + f(p^2) + \dots| \leq \sum_{p \leq x} (|f(p)| + |f(p^2)| + \dots) \leq \sum_{n=2}^{\infty} |f(n)|$$

Da alle Partialsummen beschränkt sind, folgt, dass $\sum_p |f(p) + f(p^2) + \dots|$ konvergiert und daraus folgt die absolute Konvergenz des oben genannten unendlichen Produktes.

Im strikt multiplikativem Fall folgt sogar $f(p^n) = f(p)^n$ und jede Reihe im unendlichen Produkt (von oben) ist eine konvergente geometrische Reihe mit dem Wert $(1 - f(p))^{-1}$.

In diesem Fall erhält man

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}}$$

für $\sum f(n)n^{-s}$ absolut konvergent. Nun setze $f(n) = \chi_K(n)$ und man erhält

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

und damit die Behauptung.

Dafür ist die Beobachtung notwendig, dass $\chi_K: \rightarrow \{-1, 0, 1\}$ strikt multiplikativ ist. Das heißt es gilt $\chi(mn) = \chi(m) \cdot \chi(n)$ für beliebige $m, n \in \mathbb{N}$.

Die Fallunterscheidung nach o.B.d.A. $\text{ggT}(n, \Delta_K) > 1$ hat direkt zur Folge, dass $\text{ggT}(nm, \Delta_K) > 1$ und daraus resultiert $\chi_K(nm) = 0 = 0 \cdot \chi(m) = \chi(m) \cdot \chi(n)$. Nun bleibt $\text{ggT}(n, \Delta_K) = 1$ so wie $\text{ggT}(m, \Delta_K) = 1$. So folgt nach der Definition der Abbildung für beliebige natürliche Zahlen als Gruppenhomomorphismus

$$\chi(mn) = \chi(\bar{n}) \cdot \chi(\bar{m}) = \chi(m) \cdot \chi(n)$$

□

Fortsetzung Beweis zu Theorem ??. Das führt zur Behauptung

$$\zeta(s) \cdot L(s, \chi_K) = \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_K(d) \right) \frac{1}{n^s}$$

für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$, wobei die Summe $\sum_{d|n}$ über alle positiven Teiler $d \in \mathbb{N}$ von n durchläuft, da die beiden Dirichletreihen

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}$$

und

$$L(s, \chi_K) = \sum_{d=1}^{\infty} \frac{\chi_K(d)}{d^s}$$

für alle $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$ absolut konvergieren. Dies folgt für beide direkt nach Anwendung der Geometrischen Reihe.

So konvergiert auch das Produkt aus beiden mit der Form

$$\zeta(s) \cdot L(s, \chi_K) = \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \frac{\chi_K(d)}{(md)^s}$$

absolut. Dadurch ist die Umordnung der Summation beliebig veränderbar zu

$$\zeta(s) \cdot L(s, \chi_K) = \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \frac{\chi_K(d)}{(md)^s} = \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_K(d) \right) \frac{1}{n^s}$$

Im letzten Schritt nutzt es, dass $n \cdot m = n$ wiederum in \mathbb{N} durch ein beliebiges $n \in \mathbb{N}$ dargestellt werden kann.

Um nun auch (1) zu beweisen, muss zunächst folgendes Lemma betrachtet werden.

Motivation. Die Identität $\zeta_K(s) = \zeta(s) \cdot L(s, \chi_K)$ aus vorigem Theorem liefert nun eine also eine Identität von absolut konvergenten Dirichletreihen für $s \in \mathbb{C}$ mit $\text{Re}(s) > 1$

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_K(d) \right) \frac{1}{n^s}$$

wobei $a_n = \sum_{d|n} \chi_K(d)$ für beliebige $n \in \mathbb{N}$ aus dem nächsten Lemma folgt.

Lemma 1.7. Sei $N \in \mathbb{N}_0$ und $f: \{s \in \mathbb{C}: \operatorname{Re}(s) > N\} \rightarrow \mathbb{C}$ eine holomorphe Funktion. Falls f für alle $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > N$ durch eine absolut konvergente Dirichletreihe

$$f(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

gegeben ist, dann ist die Koeffizientenfolge $(b_n)_{n \in \mathbb{N}}$ eindeutig durch f festgelegt. Dies ist äquivalent zur Einzigartigkeit der Darstellung von f als absolut konvergente Dirichletreihe, sofern die Darstellung überhaupt existiert.

Beweis. Es bietet sich ein induktives Vorgehen an. Zunächst steht die Behauptung

$$b_1 = \lim_{k \rightarrow \infty} f(k)$$

also, dass b_1 Grenzwert der Folge

$$(f(N+1), f(N+2), f(N+3), \dots)$$

ist. Denn dadurch ist b_1 eindeutig durch f festgelegt. Dies gilt, da

$$f(s) = b_1 + \sum_{n=1}^{\infty} \frac{b_n}{n^s} \xrightarrow{s \rightarrow \infty} b_1 + 0 = b_1$$

Dadurch ist b_1, \dots, b_m für ein $m \in \mathbb{N}$ eindeutig durch f festgelegt. Ersetze $f(s)$ durch $f(s) - \sum_{n=1}^m \frac{b_n}{n^s}$. Daraus folgt die Annahme, dass $b_1 = \dots = b_m = 0$ gilt. Mit selbigem Argument wie oben folgt

$$b_{m+1} = \lim_{k \rightarrow \infty} (m+1)^k f(k)$$

also ist auch b_{m+1} eindeutig durch f festgelegt.

Damit ist erreicht, was in der Motivation gefordert war. □

Fortsetzung Beweis zu Theorem ??. Nun folgt der Beweis zur Rechtfertigung des ersten Gleichheitszeichens des Theorems ??. Zuerst ist

$$\zeta_K(s) = \sum_{C \in Cl_K} \sum_{\mathfrak{J} \in C} \frac{1}{N_{K|\mathbb{Q}}(\mathfrak{J})^s}$$

wobei sich die Summe $\sum_{\mathfrak{J} \in C}$ über alle Ideale $\langle 0 \rangle \subsetneq \mathfrak{J} \subseteq O_K$ aus der Idealklasse $C \in Cl_K$ erstreckt. Das erste Summenzeichen ist nach Vortrag 7 bereits eine endliche Summe. Man fixiere ein beliebiges Ideals $\langle 0 \rangle \subsetneq \mathfrak{L} \subseteq O_K$ mit $\mathfrak{L} \in C^{-1}$, wobei C^{-1} die inverse Idealklasse zu C in Cl_K bezeichnet. Die Behauptung liegt nahe, dass

$$\{\text{Ideale } \langle 0 \rangle \subsetneq \mathfrak{J} \subseteq O_K \text{ mit } \mathfrak{J} \in C\} \rightarrow (\mathfrak{L} \setminus \{0\})/O_K^\times = \{\beta \cdot O_K^\times : \beta \in \mathfrak{L} \setminus \{0\}\}$$

gegeben durch

$$\mathfrak{J} \mapsto \text{„Erzeuger des Hauptideals“ } \mathfrak{J} \cdot \mathfrak{L} \cdot O_K^\times$$

eine wohldefinierte Bijektion darstellt.

Zunächst die Wohldefiniertheit: Es ist $\mathfrak{J} \cdot \mathfrak{L} \subseteq O_K$ ein Hauptideal mit Namen $\langle \alpha \rangle = \mathfrak{J} \cdot \mathfrak{L}$, weil $\mathfrak{J} \cdot \mathfrak{L} \in C \cdot C^{-1} = P_K$, wobei $P_K \in Cl_K$ die Klasse aller gebrochenen Hauptideale, also das neutrale Element bezeichnet. Darüber hinaus ist $\alpha \in \langle \alpha \rangle = \mathfrak{J} \cdot \mathfrak{L} \subseteq \mathfrak{L}$. Es folgt leicht, dass genau dann $\langle \alpha \rangle = \langle \beta \rangle$ für beliebige $\beta \in \mathfrak{L}$, wenn α und β assoziiert sind. Denn sei $\alpha = \beta \cdot y$ mit $y \in O_K^\times$, so folgt $\alpha \mid \beta$ und damit unmittelbar $\beta \in \langle \alpha \rangle$ und $\langle \beta \rangle \subseteq \langle \alpha \rangle$. Dasselbe gilt für $y := y^{-1}$, da y eine Einheit ist. Also analog für die Vertauschung von α und β . Die Rückrichtung nutzt, dass O_K ein Hauptidealring ist. Sei weiter $\langle \alpha \rangle = \langle \beta \rangle$. Nach Wahl der Darstellungen für $\beta = \alpha \cdot c$ und $\alpha = \beta \cdot d$ folgt $\alpha = c \cdot d \cdot \alpha$ und daraus unmittelbar $1 - cd = 0$. Da O_K auch noch Integritätsring und somit nullteilerfrei ist, folgt $\alpha = 0$ ($\beta = 0$) oder $1 - cd = 0$. Dies spricht dafür, dass $b, c \in O_K^\times$ also Einheiten sind. So sind α und β assoziiert. So ist obige Abbildung wohldefiniert und injektiv.

Beweis der Surjektivität: Seien dazu $\beta \in \mathfrak{L} \setminus 0$ und $\langle 0 \rangle \subsetneq \mathfrak{J} \subseteq O_K$ mit $\mathfrak{J} \in C$ beliebig und weiter $\mathfrak{J} \cdot \mathfrak{L} = \langle \alpha \rangle$ für ein $\alpha \in \mathfrak{L}$. Dann gilt $\frac{\beta}{\alpha} \cdot \mathfrak{J} \in C$ und $\frac{\beta}{\alpha} \cdot \mathfrak{J} \cdot \mathfrak{L} = \langle \beta \rangle$. Diese Darstellung ist richtig, da für $\frac{\beta}{\alpha} \cdot \mathfrak{J} \subseteq K$ tatsächlich gilt $\frac{\beta}{\alpha} \cdot \mathfrak{J} \subseteq O_K$. Dies folgt daraus, dass $\beta \in \mathfrak{L}$ und damit $\langle \beta \rangle \subseteq \mathfrak{L}$. Das wiederum hat zur Folge, dass $\mathfrak{L} \mid \langle \beta \rangle$ ist. Dies bedeutet, dass ein Ideal $\mathfrak{L}' \subseteq O_K$ mit $\mathfrak{L} \cdot \mathfrak{L}' = \langle \beta \rangle$. Durch Einsetzen in $\frac{\beta}{\alpha} \cdot \mathfrak{J} \cdot \mathfrak{L} = \langle \beta \rangle$ ist $\frac{\beta}{\alpha} \cdot \mathfrak{J} \cdot \mathfrak{L} = \mathfrak{L} \cdot \mathfrak{L}'$ und nach Multiplikation mit \mathfrak{L}^{-1} folgt $\frac{\beta}{\alpha} \cdot \mathfrak{L}' \subseteq O_K$. Daraus folgt die Surjektivität.

Die Eigenschaften der Norm

$$N(\alpha) = N_{K|\mathbb{Q}}(\langle \alpha \rangle) = N_{K|\mathbb{Q}}(\mathfrak{J} \cdot \mathfrak{L}) = N_{K|\mathbb{Q}}(\mathfrak{J}) \cdot N_{K|\mathbb{Q}}(\mathfrak{L})$$

ermöglichen, die Bijektion umzuschreiben. Aus Vortrag 5 ist bekannt, dass stets $\gamma, \delta \in \mathfrak{L}$ mit

$$\mathfrak{L} = \mathbb{Z}\gamma + \mathbb{Z}\delta = \{x\gamma + y\delta : x, y \in \mathbb{Z}\}$$

gefunden werden können. Weiter ist aus Vortrag 7 gegeben, dass

$$f := \frac{N(\gamma X + \delta Y)}{N_{K|\mathbb{Q}}(\mathfrak{L})} = \frac{(\gamma X + \delta Y) \cdot \iota((\gamma)X + \iota(\delta)Y)}{N_{K|\mathbb{Q}}(\mathfrak{L})} \in \mathbb{Z}[X, Y]$$

eine primitive, positiv definite quadratische Form mit Diskriminante Δ_K ist, die unter der Bijektion $C(\Delta_K) \rightarrow Cl_K$ auf C^{-1} (die Klasse von \mathfrak{L} in Cl_K) abgebildet wird. Hieraus folgt, dass

$$\sum_{\mathfrak{J} \in C} \frac{1}{N_{K|\mathbb{Q}}(\mathfrak{J})^s} = \frac{1}{|O_K^\times|} \sum_{(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{f(x,y)^s}$$

wobei sich dies durch das Ersetzen von f durch eine reduzierte quadratische Form, die eigentlich äquivalent zu f ist, nicht ändert. Das folgt aus der Bemerkung nach Cox [?] [S. 23], dass äquivalente Formen dieselben ganzen Zahlen repräsentieren.

Seien also $f_1, \dots, f_k \in \mathbb{Z}[X, Y]$ reduzierte quadratische Formen, die die Äquivalenzklassen aus $C(\Delta_K)$ repräsentieren. Dann erhalten wir aufgrund absoluter

Konvergenz, dass

$$\zeta_K(s) = \sum_{j=1}^k \frac{1}{|O_K^\times|} \sum_{(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{f_j(x,y)^s} = \frac{1}{|O_K^\times|} \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s}$$

Das Gleichheitszeichen folgt dann analog mit dem vorherigen Lemma. \square

Literatur

- [1] J. Neukirch: *Algebraische Zahlentheorie*. Springer, 1. Auflage (1992)
- [2] F. Modler, M. Kreh: *Tutorium Algebra*. Springer, 3. Auflage (2013)
- [3] D. A. Marcus: *Number Fields*. Springer, 2. Auflage (2018)
- [4] E. Freitag, R. Busam: *Funktionentheorie 1*. Springer, 4. Auflage (2006)
- [5] D. A. Cox: *Primes of the Form $x^2 + ny^2$* . Wiley, 2. Auflage (2013)
- [6] C. Baxa: *Vorlesungsskript Zahlentheorie*. Universität Wien