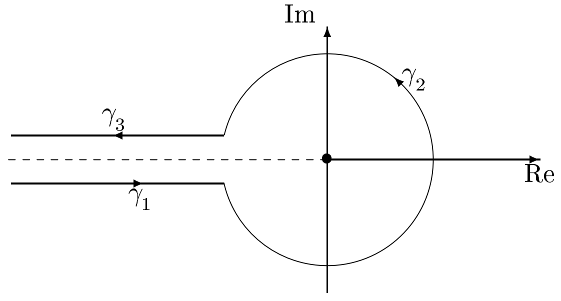
Analytische Zahlentheorie

Vorlesung im WS 2003/2004 nach Prof. Dr. P. Schmid

Aufgeschrieben von Hörern der Vorlesung



Vorwort

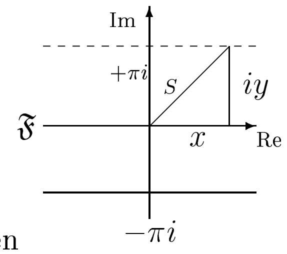
Aus dem kommentierten Vorlesungsverzeichnis:
Die Analytische Zahlentheorie ist der Teil der Zahlentheorie, in welchem neben rein algebraischen Argumenten Methoden der Analysis eine zentrale Rolle spielen. So werden gewisse funktionentheoretische Grundkenntnisse (Analysis III) vorausgesetzt, ebenso wie algebraische (Algebra I). Ziele der Vorlesung sind der Beweis des Primzahlsatzes, des Satzes über die Primzahlen in arithmetischer Progression (Dirichlet) sowie eine Einführung in die Theorie ganzzahliger binärer quadratischer Formen und quadratischer Zahlkörper (Gauss). Die Verbindung zu algebraischen Gegenständen wird durch Zeta-Funktionen (Riemann) und Dirichlet-Reihen hergestellt. Die Vorlesung ist so konzipiert, dass sie als Prüfungsgebiet sowohl in Richtung Algebra wie auch Analysis gelten kann. Sie wendet sich sowohl an Diplomkandidaten in Mathematik wie auch an Staatsexamenskandidaten. Je nach Interessenlage soll im kommenden Sommer ein Seminar folgen, das auf Arbeiten in diesem Bereich hinführen könnte.

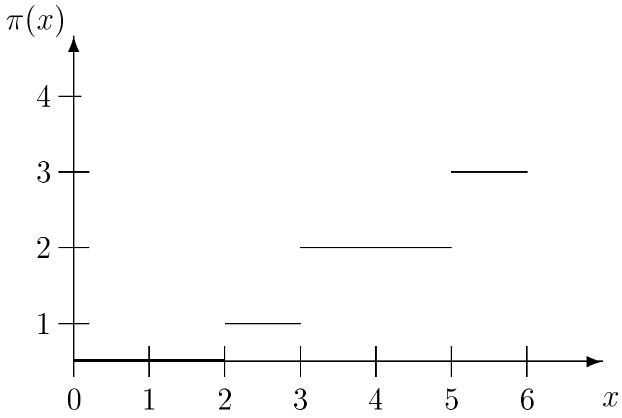
Dieses Vorlesungsskript ist aus einer im Wintersemester 2003/2004 an der Universität Tübingen von Prof. Dr. Peter Schmid gehaltenen Vorlesung zur Analytischen Zahlentheorie entstanden.
Unter sorgfältiger Ausarbeitung des handschriftlich mitgeschriebenen Skriptes ist dann dieses in LaTeX gesetzte Skript entstanden. Erfahrungsgemäß sind noch an der ein oder anderen Stelle Fehler enthalten. Für Hinweise auf Fehler oder aber auf Dinge, die besser gemacht werden können, bin ich dankbar.

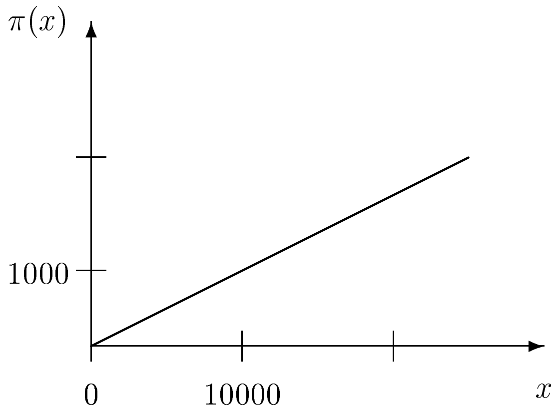
Markus Baur — Rottenburg, im März 2004

Inhaltsverzeichnis

Notation. $\mathbb{R}_{>0}$; $\mathbb{C}^*$; $s = x + iy \in \mathbb{C}$ $(x = \mathrm{Re}(s), y = \mathrm{Im}(s))$
$z \mapsto e^z = \exp(z) = \sum\limits_{n=0}^{\infty} \frac{z^n}{n!}$ ist biholomorph vom
Streifen $\mathfrak{F} = \{z \in \mathbb{C} | -\pi \leq \mathrm{Im}(z) < \pi\}$ auf $\mathbb{C}^*$
Umkehrfunktion: $\log = \ln : \mathbb{C}^* \xrightarrow{\sim} \mathfrak{F}$
(Hauptzweig des Logarithmus)
$\log(1+z) = \sum\limits_{n=0}^{\infty} (-1)^{n+1} \frac{z^n}{n}$ $(|z| < 1)$
$\overline{\mathbb{P}} = \mathbb{P}_{\mathbb{Q}} = \{2, 3, 5, 7, \ldots\}$ Menge der rationalen Primzahlen
$\pi : \mathbb{R}_{>0} \to \mathbb{N}, \quad \pi(x) = \sum\limits_{\substack{p \in \mathbb{P} \\ p \leq x}} 1$ Anzahl der Primzahlen $\leq x$.







Primzahlsatz. $\pi(x) \sim \frac{x}{\log x}$ *(für $x \to \infty$)*
Für reelle Funktionen f, g schreibe $f(x) \sim g(x)$ [für $x \to \infty$], falls

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

1 Euklid - Euler - Riemann

(1.1) Satz (Euklid). $\mathbb{P}$ *ist unendlich.*

Beweis. Annahme $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ endlich.
$2 = p_1 < 3 = p_2 < \cdots < p_n$
Betrachte $a = p_1 \cdot \cdots \cdot p_n + 1$; $a \notin \mathbb{P}$ $(a > p_j \ \forall j)$
Finde Primzahl p mit $p | a$; etwa $p = p_i$. Dann

$$\left.\begin{array}{r} a = p_i \cdot q \text{ für ein } q \in \mathbb{N} \\ a = p_i \cdot q' + 1 \text{ für ein } q' \in \mathbb{N} \end{array}\right\}$$

$\Rightarrow p_i q = p_i \cdot q' + 1;\ p_i(q - q') = 1$ (Wds) ■

(1.2) Satz (Euler). *Für $x \in \mathbb{R}_{>0}$ gilt*

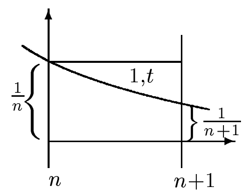
(a) $\pi(x) > \log x - 1$

(b) $\sum\limits_{\substack{p \in \mathbb{P} \\ p \leq 1}} \frac{1}{p} > \log\log x - 1$

(c) $\sum\limits_{p \in \mathbb{P}} \frac{1}{p}$ *divergent*

Beweis. (a) $\prod\limits_{p \leq x} \frac{1}{1-\frac{1}{p}} = \prod\limits_{p \leq x} \left(\sum\limits_{i=0}^{\infty} \frac{1}{p_i} \right) = \sum\limits_{n}{}' \frac{1}{n}$, wobei die Summation über alle $n \in \mathbb{N}$ erfolgt, die nur durch Primfaktoren $\leq x$ teilbar sind.

$\sum\limits_{n}{}' \frac{1}{n} \geq \sum\limits_{\substack{n \leq x \\ (n \in \mathbb{N})}} \frac{1}{n} > \sum\limits_{n}^{[x]} \int\limits_{n}^{n+1} \frac{dt}{t} \geq \log x$



Andererseits:

$$\prod_{p \leq x} \frac{1}{1-\frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1} \leq \prod_{n \leq x} \frac{n}{n-1} \leq \prod_{n=2}^{\pi(x)+1} \frac{n}{n-1} = \frac{1 \cdot 2 \cdot \cdots \cdot (\pi(x)+1)}{2 \cdots \pi(x)} = \pi(x)+1$$

$\Rightarrow \quad \pi(x) + 1 > \log(x)$

(b) Nach (a) gilt [reeller Logarithmus streng monoton wachsend, unbeschränkt, mit $\log(a \cdot b) = \log a + \log b$];

$\sum\limits_{p \leq x} \log \left(\frac{1}{1-\frac{1}{p}} \right) > \log\log x$

Andererseits:

$$\begin{aligned} \log \left(\frac{1}{1-\frac{1}{p}} \right) = -\log(1-\frac{1}{p}) &= \frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \ldots \\ &< \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots \\ &= \frac{1}{p} \cdot \frac{1}{1-\frac{1}{p}} = \frac{1}{p-1} = \frac{1}{p} + \frac{1}{p(p-1)} \end{aligned}$$

Folglich: $\sum\limits_{p \leq x} \frac{1}{p} > \log\log x - \underbrace{\sum\limits_{p \leq x} \frac{1}{p(p-1)}}_{< \sum\limits_{n=2}^{\infty} \frac{1}{n(n-1)} = 1}$

$$> \log\log(x) - 1$$

(c) folgt aus (b) [wegen Eigenschaften vom Logarithmus]

∎

(1.3) Definition. Sei $n \in \mathbb{N}_{>0}$. Dann $s \mapsto n^s = e^{s \log n}$ holomorph ($s \in \mathbb{C}$)
Es gilt $|n^s| = |e^{s \cdot \log n}| = |e^{(x+iy)\log n}|, x = \mathrm{Re}(s), y = \mathrm{Im}(s)$
$= |e^{x \log n} \cdot e^{iy \log n}| = |e^{x \log n}| \cdot \underbrace{|e^{iy \log n}|}_{1} = |e^{\mathrm{Re}\, s \log n}|$
$= |n^{\mathrm{Re}(s)}|$
Sei $a \in \mathbb{R}_{>0}$; $\sum\limits_{n=1}^{\infty} \frac{1}{n^a}$ konvergiert $\Leftrightarrow$ $a > 1$ (Analysis I)
Für $\mathrm{Re}(s) > 1$ ist daher die Reihe

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\mathrm{Re}(s) > 1)$$

absolut konvergent (Riemannsche Zetafunktion)

(1.4) Satz (Weierstraß). *Sei $U \underset{\text{offen}}{\subseteq} \mathbb{C}$ und (f_n) eine Folge holomorpher Funktionen auf U. Konvergiert (f_n) auf jeder kompakten Teilmenge $D \subseteq U$ gleichmäßig gegen eine Funktion f, so ist f holomorph und (f'_n) konvergiert kompakt gegen f'.*

Beweis. Sei $D \subseteq U$ eine abgeschlossene Kreisscheibe mit orientiertem Rand C.
Cauchy-Integralsatz

$$f_n = \frac{1}{2\pi i} \int_C \frac{f_n(z)}{z - s}\, dz \quad (s \in \overset{\circ}{\mathrm{D}} \text{ Inneres von D})$$

Nach Voraussetzung konvergiert $z \mapsto \frac{f_n(z)}{z-s}$ auf dem Kompaktum $\mathrm{D} \setminus \overset{\circ}{\mathrm{D}}$ glm. gegen $\frac{f(z)}{z-s}$.
Folglich $f(s) = \frac{1}{2\pi i} \int_C \frac{f(z)}{z-s}\, dz$
Für $s \neq s'$ in $\overset{\circ}{\mathrm{D}}$ gilt $\frac{f(s)-f(s')}{s-s'} = \frac{1}{2\pi i} \int_C \frac{f(z)}{s-s'} \left[\frac{1}{z-s} - \frac{1}{z-s'}\right] dz = \frac{1}{2\pi i} \int_C \frac{f(z)\, dz}{(z-s)(z-s')}$
Also ist f holomorph in $\overset{\circ}{\mathrm{D}}$ und $f'(s) = \frac{1}{2\pi i} \int_C \frac{f(z)}{(z-s)^2}\, dz$
Rest folgt durch Betrachten der Integralformel für (f'_n).
Zusatz: Konvergiert die Reihe $\sum\limits_n f_n$ normal auf jedem Kompaktum $D \subseteq U$,
d.h $\sum \|f_n\|_D$ konvergiert $(\|f_n\|_D = \sup\limits_{z \in D} |f_n(z)|)$
so ist die Grenzfunktion holomorph (Weierstraß). ∎

(1.5) Lemma. *Sei $z_n \in \mathbb{C}$, $z_n \neq -1$ $(n \in \mathbb{N}_{>0})$. Äquivalent:*

(i) $\prod\limits_{n=1}^{\infty} (1 + z_n) = \lim\limits_{n \to \infty} [(1 + z_1)(1 + z_2) \cdots (1 + z_n)]$ *existiert in* $\mathbb{C}^*$ *(etwa b)*

(ii) $\sum\limits_{n=1}^{\infty} \log(1 + z_n)$ *konvergiert in* $\mathbb{C}$ *(gegen* β*)*

Beweis. Eigenschaften des Hauptzweiges log $[b = e^{\beta}]$. ■

(1.6) Satz. $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ *ist holomorph für* $\mathrm{Re}(s) > 1$, *und es gilt das* Euler-Produkt
$\zeta(s) = \prod\limits_{p \in \mathbb{P}} \frac{1}{1-\frac{1}{p^s}} \quad (\mathrm{Re}(s) > 1)$
Insbesondere hat $\zeta(s)$ *keine Nullstelle für* $\mathrm{Re}(s) > 1$.

Beweis. Für $a > 1$ und $\mathrm{Re}(s) \geq a$ gilt:

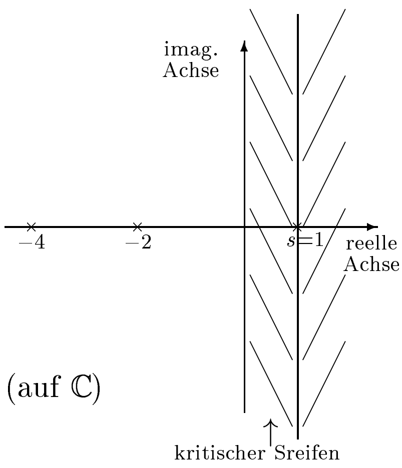
(a) $\left|\frac{1}{n^s}\right| = \left|\frac{1}{n^{\mathrm{Re}(s)}}\right| \leq \frac{1}{n^a}$; $\sum\limits_{n=1}^{\infty} \frac{1}{n^a}$ konvergiert, da $a > 1$.
$\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ normal konvergierende Reihe für $\mathrm{Re}(s) \geq a$ holomorpher Funktionen. Wende 1.4 an.

(b) $\prod\limits_{\substack{p \leq a \\ (p \in \mathbb{P})}} \frac{1}{1-\frac{1}{p^s}} = \prod\limits_{p \leq a} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \sum\limits_{n}{}' \frac{1}{n^s}$,
wobei die Summation über die $n \in \mathbb{N}_{>0}$, deren Primfaktoren $\leq a$ sind (Cauchy-Produkt)
Euler-Produkt folgt bei Übergang $a \to \infty$.
zu zeigen: $\sum\limits_{p \in \mathbb{P}} \log \frac{1}{1-\frac{1}{p^s}}$ konvergiert ($\overset{1.5}{\Rightarrow} \zeta(s) \neq 0$ für $\mathrm{Re}(s) > 0$)
$\left|\log \frac{1}{1-\frac{1}{p^s}}\right| = \left|\frac{1}{p^s} + \frac{1}{2p^{2s}} + \cdots\right| \leq \frac{1}{p^a} + \frac{1}{p^{2a}} + \frac{1}{p^{3a}} + \cdots = \frac{\frac{1}{p^a}}{1-\frac{1}{p^a}} = \frac{1}{p^a - 1} \leq \frac{2}{p^a}$
Reihe $\sum\limits_{p \in \mathbb{P}} \frac{2}{p^a}$ konvergiert. Die Behauptung folgt.

■

(1.7) Satz. *Es gibt eine eindeutig bestimmte holomorphe Funktion* $f(s)$ *für* $\mathrm{Re}(s) > 0$, *so dass*

$$\zeta(s) = \frac{1}{s-1} + f(s) \quad (\mathrm{Re}(s) > 1)$$



Beweis. Für $\mathrm{Re}(s) > 1$ gilt $\lim\limits_{\substack{t \to \infty \\ (t \in \mathbb{R})}} \frac{1}{t^{s-1}} = 0$; also

$$\sum_{n=1}^{\infty} \int_n^{n+1} \frac{dt}{t^s} = \int_1^{\infty} \frac{dt}{t^s} = \left[-\frac{1}{s-1}\frac{1}{t^{s-1}}\right]_1^{\to\infty} = \frac{1}{s-1}$$

Folglich $\zeta(s) = \frac{1}{s-1} + \sum\limits_{n=1}^{\infty} \int\limits_n^{n+1} \left[\frac{1}{n^s} - \frac{1}{t^s}\right] dt \quad (\mathrm{Re}(s) > 1)$

Betrachte $f_n(s) = \int\limits_n^{n+1} \left[\frac{1}{n^s} - \frac{1}{t^s}\right] dt$; $(n \in \mathbb{N}_{>0})$; f_n holomorph (auf $\mathbb{C}$)

(„Differentiation unter dem Integralzeichen“, (18.4) Analysis I, WS 2002/2003)
Zeige: $\sum\limits_{n=1}^{\infty} f_n(s)$ konvergiert normal in jedem Kompaktum in $\mathrm{Re}(s) > 0$
(stellt dort also nach 1.4 eine holomorphe Funktion f dar).
Sei $a > 0$ und $\mathrm{Re}(s) \geq a$. Es gilt

$$|f_n(s)| \leq \sup_{n \leq t \leq n+1} \left| \frac{1}{n^2} - \frac{1}{t^2} \right| \underset{\substack{\text{Schranken-}\\\text{satz}}}{\leq} \sup_{n \leq t \leq n+1} |n-t| \cdot \left| \frac{d}{dt} \frac{1}{t^s} \right|$$

$$\leq |s| \cdot \left\| \frac{1}{t^{s+1}} \right\|_{[n,n+1]} \leq \frac{|s|}{n^{a+1}} \; ; \; \sum_{n=1}^{\infty} \frac{1}{n^{a+1}} \text{ konvergiert}$$

Behauptung folgt. (Eindeutigkeit von f folgt aus dem Identitätssatz für Potenzreihen und dem einfachen Zusammenhang von $\{s \in \mathbb{C} | \, \mathrm{Re}(s) > 0\}$) ■

(1.8) Folgerungen. Durch $s \mapsto \frac{1}{s-1} + f(s)$ wird die Zetafunktion auf $\mathrm{Re}(s) > 0$ erklärt.
Durch $s \mapsto \frac{1}{s-1} + f(s)$ ist $\zeta(s)$ meromorph fortgesetzt auf $\mathrm{Re}(s) > 0$.
Dort ist $\zeta(s)$ holomorph mit der einzigen Singularität bei $s = 1$, nämlich einem einfachen Pol mit Residuum 1.
Notation: Für meromorphe Funktion $g(s), h(s)$ erklärt in Umgebung von $s = s_0$ schreibe

$$g(s) \sim h(s) \qquad \text{für } s \to s_0$$

falls $g(s) - h(s)$ holomorph (fortsetzbar) in s_0.
Damit: $\zeta(s) \sim \frac{1}{s-1}$ für $s \to 1$
$\lim\limits_{s \to 1} (s-1)\zeta(s) = 1 + \lim\limits_{s \to 1} (s-1) f(s) = 1$
oder $\log \zeta(s) \sim \log \frac{1}{s-1}$ für $s \to 1$
Behauptung: $\sum\limits_{p \in \mathbb{P}} \frac{1}{p^s} \sim \log \frac{1}{s-1}$ für $s \to 1$.

Beweis. Für $\mathrm{Re}(s) > 1$ gilt nach dem Eulerprodukt (1.6):

$$\begin{aligned} \log \zeta(s) = \sum_{p \in \mathbb{P}} \log \left(\frac{1}{1 - \frac{1}{p^s}} \right) &= \sum_{p \in \mathbb{P}} \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots \right) \\ &= \sum_{p} \frac{1}{p^s} + \sum_{p, k \geq 2} \frac{1}{kp^{ks}} \end{aligned}$$

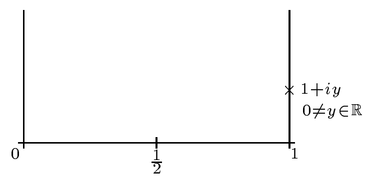
Sei $a > \frac{1}{2}$ und $\mathrm{Re}(s) \geq a$, zeige: $\sum\limits_{p,k \geq 2} \frac{1}{kp^{ks}}$ konvergiert normal für $\mathrm{Re}(s) \geq a$.
$(\overset{1.4}{\Rightarrow} \sum\limits_{p} \frac{1}{p^s} \sim \log \zeta(s) \sim \log \frac{1}{s-1}$ für $s \to 1)$

Setze

$$\begin{aligned}
\psi_p(s) &= \sum_{k=2}^{\infty} \frac{1}{kp^{ks}} \quad (p \in \mathbb{P}, \mathrm{Re}(s) \geq a); \\
|\psi_p(s)| &\leq \sum_{k=2}^{\infty} \frac{1}{kp^{ka}} \leq \sum_{k=2}^{\infty} \frac{1}{p^{ka}} = \sum_{k=2}^{\infty} \frac{1}{p^{ak}} = \frac{\frac{1}{p^{2a}}}{1-\frac{1}{p^a}} = \frac{1}{p^{2a}-p^a} \leq \frac{4}{p^{2a}} \\
\text{Reihe} & \quad \sum_{p\in\mathbb{P}} \frac{4}{p^{2a}} \text{ konvergiert.}
\end{aligned}$$

■

(1.9) Riemannsche Vermutung. (B. Riemann, 1826-1866)
Wir werden $\zeta(s)$ auf $\mathbb{C}$ meromorph erklären (3), $\zeta(s)$ ist holomorph außer für $s = 1$, hat Nullstellen für $s = -2n, n \in \mathbb{N}_{>0}$, sonst nur im „kritischen Streifen“ $0 < \mathrm{Re}(s) < 1$ (unendlich viele Nullstellen dort).
Vermutung: Alle Nullstellen von $\zeta(s)$ im kritischen Streifen liegen auf der Geraden $\mathrm{Re}(s) = \frac{1}{2}$.



(1.10) Satz. $\zeta(s)$ *hat keine Nullstelle für* $\mathrm{Re}(s) = 1, s \neq 1$.

Beweis. (Mertens,1898). Für $t \in \mathbb{R}$ gilt

$$3 + 4\cos t + \cos 2t = 2(1 + \cos t)^2 \geq 0$$

Für $\mathrm{Re}(s) > 1$ gilt nach dem Euler-Produkt (1.6):

$$\begin{aligned}
\log|\zeta(s)| &= \mathrm{Re}\left(\sum_{p\in\mathbb{P}} \log\frac{1}{1-\frac{1}{p^s}}\right) = \mathrm{Re}\left(\sum_{p\in\mathbb{P}}\left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots\right)\right) \\
&= \mathrm{Re}\left(\sum_{n\in\mathbb{N}_{>0}} \frac{a_n}{n^s}\right) \quad \text{mit } 0 \leq a_n \in \mathbb{R} \text{ („unbedingte Konvergenz“)}
\end{aligned}$$

Annahme: $\zeta(1 + iy) = 0$ für $0 \neq y \in \mathbb{R}$
Betrachte $h(s) = \zeta(s)^3 \cdot \zeta(s + iy)^4 \cdot \zeta(s + 2iy)$; $\mathrm{Re}(s) > 0$

$$\left.\begin{array}{r}\text{Nach 1.8}\\ \text{und Annahme}\end{array}\right\} \text{ ist } h(s) \text{ holomorph fortsetzbar für } \mathrm{Re}(s) > 0, s = 1, \text{ mit } h(1) = 0$$

Insbesondere ist $\lim\limits_{\substack{x\to 1\\(x\in\mathbb{R})}} \log|h(x)| = -\infty$

Andererseits:

$$\begin{aligned}(1 < x \in \mathbb{R}):\ \log|h(x)| &= 3\cdot\log|\zeta(x)| + 4\cdot\log|\zeta(x+iy)| + \log|\zeta(x+2iy)| \\ &= \mathrm{Re}\left(\sum_{n=1}^{\infty} a_n\left(\frac{3}{n^x} + \frac{4}{n^{x+iy}} + \frac{1}{n^{x+2iy}}\cdots\right)\right) \\ &= \sum_{n=1}^{\infty}\frac{a_n}{n^x}\left(\underbrace{3 + 4\cdot\cos(y\log n) + \cos(2y\log n)}_{\geq 0}\right) \\ &\geq 0 \text{ (für alle } x > 1) \text{ Widerspruch}\end{aligned}$$

■

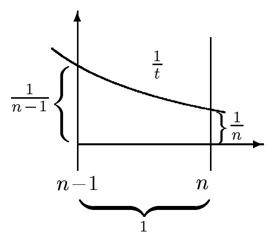
2 Die Gamma-Funktion

(2.1) Lemma. $\gamma := \lim\limits_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right)$ *existiert.*

(Euler Konstante; $\gamma \approx 0,577\ldots$*).*

Beweis. Für $2 \leq n \in \mathbb{N}$ gilt

$$\frac{1}{n-1} > \int_{n-1}^{n}\frac{dt}{t} > \frac{1}{n}, \text{ also } \frac{1}{n-1} - \frac{1}{n} > \frac{1}{n-1} - \int_{n-1}^{n}\frac{dt}{t} > 0$$



$$\sum_{n=2}^{\infty}\left[\frac{1}{n-1} - \frac{1}{n}\right] = \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 1 \text{ konvergiert (absolut)}$$

Folglich $\lim\limits_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n-1} - \underbrace{\sum_{k=2}^{n}\int_{k=1}^{k}\frac{dt}{t}}_{=\int_1^n \frac{dt}{t} = \log n}\right) = \gamma'$

existiert, $0 < \gamma' < 1$.
Wegen $\lim\limits_{n\to\infty}\frac{1}{n} = 0$ ist $\gamma' = \gamma$. ■

(2.2) Lemma.

$$G(s) = e^{\gamma s}\cdot s\cdot\prod_{n=1}^{\infty}\left[\left(1 + \frac{s}{n}\right)e^{-\frac{s}{n}}\right]$$

ist holomorph auf $\mathbb{C}$ *(„ganze Funktion“) mit genau den einfachen Nullstellen in* $s = -n, n \in \mathbb{N}$

Beweis. Sei $\mathrm{D} \subseteq \mathbb{C}$ kompakt (Kreisscheibe).
Finde $n_0 \in \mathbb{N}$ derart, dass $\frac{|s|}{n} \leq q < 1$ für alle $n \geq n_0$ und alle $s \in \mathrm{D}$.
Dann ist $(1 + \frac{s}{n})e^{-\frac{s}{n}} \neq 0$ für diese n und s.
Genügt zu zeigen: $\prod\limits_{n=n_0}^{\infty} (1 + \frac{s}{n})e^{-\frac{s}{n}}$ ist holomorph in $\mathring{\mathrm{D}}$ und konvergiert normal in D und ohne Nullstellen.
($\overset{(1.4)}{\Rightarrow}$ $G(s)$ ist holomorph auf $\mathring{\mathrm{D}}$ mit genau den Nullstellen in $\mathring{\mathrm{D}} \cap (-\mathbb{N})$.)
Genügt zu zeigen: 1.5 $\sum\limits_{n=n_0}^{\infty} \log[(1 + \frac{s}{n})e^{-\frac{s}{n}}]$ konvergiert normal auf D
Für $s \in \mathrm{D}$ und $n \geq n_0$ gilt:

$$\begin{aligned}
\left|\log\left[\left(1 + \frac{s}{n}\right)e^{-\frac{s}{n}}\right]\right| &= \left|\log\left(1 + \frac{s}{n}\right) - \frac{s}{n}\right| = \left|\left(\frac{s}{n}\right)^2 \cdot 2 - \frac{s^3}{3n^3} + \cdots\right| \\
&\leq \frac{|s|^2}{n^2} + \frac{|s|^3}{n^3} + \frac{|s|^4}{n^4} + \cdots \\
&\leq \frac{|s|^2}{n^2} \cdot \frac{1}{1-q} = \frac{c}{n^2} \text{ mit Konstanten } c = c(\mathrm{D})
\end{aligned}$$

Die Reihe $\sum\limits_{n=n_0}^{\infty} \frac{c}{n^2}$ konvergiert. ■

(2.3) Definition. Suche meromorphe Funktion Γ (auf $\mathbb{C}$) mit folgenden Eigenschaften (Legendre):

(i) $(s-1)! = \Gamma(s)$ für $s \in \mathbb{N}_{>0}$

(ii) $\Gamma(s+1) = s\Gamma(s)$ für $0 \neq s \in \mathbb{C}$ („Funktionalgleichung“)

Γ ist durch (i), (ii) noch nicht bestimmt (falls existent).
Heuristik: Für $s, n \in \mathbb{N}_{>0}$ gilt:

$$(s-1)! = \frac{(s+n)!}{s(s+1)\cdots(s+n)} = \frac{n! \cdot n^s}{s(s+1)\cdots(s+n)} \cdot \Bigg[\underbrace{\frac{n+1}{n} \cdot \frac{n+2}{n} \cdots \frac{n+s}{n}}_{\to 1 \text{ für } n \to \infty}\Bigg]$$

Ansatz(Gauß) $\Gamma(s) := \lim\limits_{n\to\infty} \dfrac{n! n^s}{s(s+1)\cdots(s+n)}, \quad (s \in \mathbb{C})$

(2.4) Satz. $\Gamma(s) = \frac{1}{G(s)}$ *ist meromorph auf* $\mathbb{C}$ *ohne Nullstellen und mit genau den (einfachen) Polstellen in* $s = n, n \in \mathbb{N}$ *und Residuum* $\frac{(-1)^n}{n!}$.
$\Gamma(s)$ *erfüllt (i), (ii).*

Beweis.

$$\begin{aligned}
\frac{1}{\Gamma(s)} &= \lim_{n\to\infty} \frac{s(s+1)\cdots(s+n)}{n!\cdot n^s} \\
&= \lim_{n\to\infty} \left[e^{-s\log n} \cdot s \cdot \prod_{k=1}^{n} \left[\left(1+\frac{s}{k}\right) e^{-\frac{s}{k}} \right] e^{s(1+\frac{1}{2}+\cdots+\frac{1}{n})} \right] \\
&\overset{(2.1),(2.2)}{=} e^{\gamma s} \cdot s \prod_{n=1}^{\infty} \left[\left(1+\frac{s}{n}\right) e^{-\frac{s}{n}} \right] = G(s)
\end{aligned}$$

$\Gamma(s) = \frac{1}{G(s)}$ hat keine Nullstellen und einfache Polstelle in $s=-n, n\in\mathbb{N}$.
Residuum in $s=-n$: Benütze Funktionalgleichung (ii) [später bewiesen]

$$\begin{aligned}
\lim_{s\to -n} (s+n)\Gamma(s) &\overset{(ii)}{=} \lim_{s\to -n} \frac{(s+n)\Gamma(s+1)}{s} = \lim_{s\to -n} \frac{(s+n)\Gamma(s+2)}{s(s+1)} = \cdots \\
&= \lim_{s\to -n} \frac{(s+n)\Gamma(s+n+1)}{s(s+1)\cdots(s+n)} = \frac{\Gamma(1)}{(-n)(-n+1)\cdots(-1)} = \frac{(-1)^n}{n!}
\end{aligned}$$

Eigenschaft (i): Folgt aus der Heuristik in 2.3.
Funktionalgleichung (ii):

$$\begin{aligned}
\Gamma(s+1) &= \lim_{n\to\infty} \frac{n! n^{s+1}\cdot s}{(s+1)(s+2)\cdots(s+n+1)\cdot s} \\
&= s\cdot \lim_{n\to\infty} \left[\frac{n!\cdot n^s}{s\cdot(s+1)\cdots(s+n+1)} \cdot \frac{n}{s+n+1} \right] \\
&= s\cdot\Gamma(s) \text{ weil } \lim_{n\to\infty} \frac{n}{s+n+1} = 1
\end{aligned}$$

■

(2.5) Satz.

$$\Gamma(s)\cdot\Gamma(1-s) = \frac{\pi}{\sin \pi s}$$

Beweis. „Bekanntlich“ gilt $\sin\pi s = \pi s \cdot \prod_{n=1}^{\infty} (1-\frac{s^2}{n^2})$, vergleiche Übung 7.
Rechne

$$\begin{aligned}
\frac{1}{\Gamma(s)} \cdot \frac{1}{\Gamma(1-s)} &\overset{(ii)}{=} \frac{1}{\Gamma(s)} \cdot \frac{1}{\Gamma(-s)} \cdot \frac{1}{-s} \overset{(2.4)}{=} -\frac{1}{s} G(s)G(-s) \\
&= s e^{\gamma s} \cdot e^{-\gamma s} \prod_{n=1}^{\infty} \left[\left(1+\frac{s}{n}\right) e^{-\frac{s}{n}} \left(1-\frac{s}{n}\right) e^{\frac{s}{n}} \right] \\
&= s\cdot \prod_{n=1}^{\infty} \left(1-\frac{s^2}{n^2}\right) = \frac{1}{\pi} \sin \pi s
\end{aligned}$$

■

Folgerung.

$$\Gamma(\frac{1}{2}) = \sqrt{\pi}$$

Beweis. $(s=\frac{1}{2})$: $\Gamma(\frac{1}{2})\cdot\Gamma(1-\frac{1}{2}) = \frac{\pi}{\sin\frac{\pi}{2}}$; $\Gamma(\frac{1}{2}) = \pm\sqrt{\pi}$

$\Gamma(\frac{1}{2}) = \lim\limits_{n\to\infty} \frac{n!\sqrt{n}}{\underbrace{\frac{1}{2}(\frac{1}{2}+1)\cdots(\frac{1}{2}+n)}_{\geq 0}} \geq 0$ ∎

(2.6) Satz.

$$\Gamma(\frac{s}{2})\cdot\Gamma(\frac{s+1}{2}) = 2^{1-s}\sqrt{\pi}\Gamma(s) \text{ \textit{(Legendre Verdopplung)}}$$

Beweis.

$$\begin{aligned}
2^s\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) &\overset{(ii)}{=} \frac{s-1}{2}\cdot 2^s\Gamma(\frac{s}{2})\Gamma(\frac{s-1}{2}) \\
&= \lim_{n\to\infty} \frac{(\frac{s-1}{2})\cdot 2^s(n!)^2\cdot n^{\frac{s}{2}}\cdot n^{\frac{s-1}{2}}}{\frac{s}{2}(\frac{s}{2}+1)\cdots(\frac{s}{2}+n)\frac{s-1}{2}(\frac{s-1}{2}+n)\cdots(\frac{s-1}{2}+n)} \\
&= \lim_{n\to\infty} \frac{2^{2n+1}(2n)^s\cdot n^{-\frac{1}{2}}(n!)^2}{s(s+2)\cdots(s+2n)(s+1)\cdots(s+2n-1)} \\
&= \underbrace{\lim_{n\to\infty} \frac{(2n)!(2n)^s}{s(s+1)\cdots(s+2n)}}_{=\Gamma(s)} \cdot \underbrace{\lim_{n\to\infty} \frac{(n!)^2 n^{-\frac{1}{2}}\cdot 2^{2n+1}}{(2n)!}}_{=:c}
\end{aligned}$$

Für $s=1$ *erhalte:* $2\cdot\underbrace{\Gamma(\frac{1}{2})}_{\sqrt{\pi}}\cdot\underbrace{\Gamma(1)}_{1} = c\cdot\underbrace{\Gamma(1)}_{=1}$; $\quad c = 2\cdot\sqrt{\pi}$

Behauptung folgt. ∎

(2.7) Satz. *(Euler)*

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\,dt \qquad (\mathrm{Re}(s)>0)$$

Beweis. Setze $\widetilde{\Gamma}(s) := \int\limits_0^\infty e^{-t}t^{s-1}\,dt \quad (\mathrm{Re}(s)>0)$

(a) *Euler-Integral*
$|e^{-t}t^{s-1}|$ majorisiert durch $t^{\mathrm{Re}(s)-1}$ bei 0 $\quad [\int_0^1 \frac{dt}{t^{1-a}}$ ex. für $a>0]$
und durch e^{-t} bei ∞ $\quad [\int_1^\infty e^{-t}\,dt$ ex.$]$
Also existiert $\widetilde{\Gamma}(s)$ für $\mathrm{Re}(s)>0$; $\widetilde{\Gamma}(s)$ holomorph.

(b) $\Gamma(s) = \widetilde{\Gamma}(s)$ für $\mathrm{Re}(s) > 0$.
Partielle Integration: $\widetilde{\Gamma}(s+1) = \int_0^\infty e^{-t} t^s \, dt$
Mit $u = t^s$; $u' = st^{s-1}$; $v = -e^{-t}$; $v' = e^{-t}$ folgt

$$\begin{aligned}\widetilde{\Gamma}(s+1) &= \int_0^\infty e^{-t} t^s \, dt \\ &= \underbrace{[-e^{-t}t^s]_0^\infty}_{=0} + \underbrace{s \int_0^\infty e^{-t} t^{s-1} \, dt}_{s\widetilde{\Gamma}(s);\ (ii)}\end{aligned}$$

Sei $n \in \mathbb{N}_{>0}$ fest. Betrachte für $\mathrm{Re}(s) > 0$;

$$\Gamma_n(s) := \frac{n^s n!}{s(s+1)\cdots(s+n)}; \quad \Gamma_n(s) \underset{(n\to\infty)}{\longrightarrow} \Gamma(s); \ (2.3)$$

$$\widetilde{\Gamma}_n(s) := \int_0^n (1 + \frac{-t}{n})^n t^{s-1} \, dt; \quad \widetilde{\Gamma}_n(s) \underset{(n\to\infty)}{\longrightarrow} \widetilde{\Gamma}(s) \ \ [\text{wegen } \lim_{n\to\infty} (1 - \frac{t}{n})^n = e^{-t}]$$

Behauptung: $\Gamma_n(s) = \widetilde{\Gamma}_n(s)$
Partialbruchzerlegung:

$$\Gamma_n(s) = n^s \sum_{k=0}^n \frac{(-1)^k \binom{n}{k}}{s+k}, \text{ denn für } 0 \le k \le n \text{ gilt}$$

$$\begin{aligned}\lim_{s\to k} (s+k) \frac{n!}{s(s+1)\cdots(s+k)\cdots(s+n)} &= \frac{n!}{(-k)(-k+1)\cdots(-1)1\cdots(n-k)} \\ &= \frac{(-1)^k n!}{k!(n-k)!} = (-1)^k \binom{n}{k}\end{aligned}$$

Binomischer Lehrsatz

$$\begin{aligned}\widetilde{\Gamma}_n(s) &= \int_0^n \sum_{k=0}^n \frac{(-1)^k t^k}{n^k} \binom{k}{n} t^{s-1} \, dt \\ &= \sum_{k=0}^n \binom{k}{n} \frac{(-1)^k}{n^k} \underbrace{\int_0^n t^{k+s-1} \, dt}_{=\left[\frac{t^{k+s}}{k+s}\right]_0^n = n^{k+s}} = n^s \sum_{k=0}^n \frac{(-1)^k \binom{k}{n}}{s+k}\end{aligned}$$

■

(2.8) Satz.

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}}{e^t - 1} \, dt \quad (\mathrm{Re}(s) > 1).$$

Beweis. Für $n \in \mathbb{N}_{>0}$ und $\mathrm{Re}(s) > 1$ gilt:

$$\text{(1)} \qquad \int_0^\infty e^{-tn} t^{s-1}\, dt = \int_0^\infty e^{-u} \left(\frac{u}{n}\right)^{s-1} \frac{du}{n} \quad [u = nt,\ du = n\, dt]$$

$$\text{(2)} \qquad = \frac{1}{n^2} \int_0^\infty e^{-u} u^{s-1}\, du \underset{2.7}{=} \frac{1}{n^s}\Gamma(s).$$

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \frac{1}{\Gamma(s)} \sum_{n=1}^\infty \int_0^\infty e^{-tn} t^{s-1}\, dt = \frac{1}{\Gamma(s)} \int_0^\infty (t^{s-1} \sum_{n=1}^\infty e^{-tn})\, dt$$
$$= \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} \frac{e^{-t}}{1 - e^{-t}} = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}}{e^t - 1}\, dt$$

■

(2.9) Anhang. (=Übung 7)

$$a \neq b\ , \quad \frac{c}{(s-a)(s-b)} = \frac{A}{s-a} + \frac{B}{s-b}$$

$$\sin \pi s = \pi s \cdot \prod_{n=1}^\infty (1 - \frac{s^2}{n^2}) \quad \text{(„Sinusprodukt“)}$$

$$\text{und } \pi \cot \pi s = \frac{1}{s} + \sum_{n=1}^\infty \frac{2s}{s^2 - n^2} = \frac{1}{s} \underbrace{\sum_{n=1}^\infty \left[\frac{1}{s-n} + \frac{1}{s+n}\right]}_{\text{(„Partialbruchzerlegung“)}}$$

Beweis. (Wielandt, ungefähr 1955)

$$f(s) = s \prod_{n=1}^\infty (1 - \frac{s^2}{n^2}) \underset{\substack{2.2,\\ 2.6}}{=} G(s) \cdot G(1-s)$$

holomorph auf $\mathbb{C}$ („ganz“) mit genau den (einfachen) Nullstellen für $s \in \mathbb{Z}$.
$\sin \pi s$ hat ebenfalls genau für $s \in \mathbb{Z}$ einfache Nullstellen.
Folglich: $\sin \pi s = e^{h(s)} f(s)$ für eine ganze Funktion (ohne Nullstellen) h.
Logarithmische Ableitung:

$$\frac{\pi \cdot \cos \pi s}{\sin \pi s} = \pi \cot \pi s = h'(s) + \frac{1}{s} + \sum_{n=1}^\infty \frac{\frac{-2s}{n^2}}{1 - \frac{s^2}{n^2}}$$
$$= h'(s) + \frac{1}{s} + \sum_{n=1}^\infty \frac{2s}{s^2 - n^2}$$

Ableitung:

$$\frac{-\pi^2}{\sin^2 \pi s} = h''(s) - \sum_{n=-\infty}^{\infty} \frac{1}{(s-n)^2}$$

Es gilt: $h''(s) + h''(s+\frac{1}{2}) = 4h''(2s)$, (*) denn

$$\frac{\pi^2}{\sin^2 \pi s} + \frac{\pi^2}{\sin^2 \pi(s+\frac{1}{2})} = \frac{\pi^2}{\sin^2 \pi s} + \frac{\pi^2}{\cos^2 \pi s} \cdots\cdots \quad \stackrel{!}{=} \frac{4\pi^2}{\sin^2(2\pi s)}$$

und

$$\sum_{n\in\mathbb{Z}} \frac{1}{(s-n)^2} + \sum_{n\in\mathbb{Z}} \frac{1}{(s+\frac{1}{2}-n)^2} = \sum_{n\in\mathbb{Z}} \frac{4}{(2s-2n)^2} + \sum_{n\in\mathbb{Z}} \frac{4}{(2s+1-2n)^2} \stackrel{!}{=} \sum_{n\in\mathbb{Z}} \frac{4}{(2s-n)^2}$$

Sei M_1 bzw. M_2 bzw. M_3 das Maximum von $|f_n''(s)|$ für $|s| = 1$ bzw. $|s| = \frac{3}{2}$ bzw. $|s| = 2$
Maximumprinzip: $M_1 \leq M_2 \leq M_3$
Aus (*) folgt: $M_1 + M_2 > 4M_3 \Rightarrow M_3 = 0;\ h'' = 0$
Also ist $h'(s) = c$ konstant. Damit

$$\left.\begin{array}{l} \pi \cot \pi s = c + \frac{1}{s} + \sum_{n=1}^{\infty} \frac{2s}{s^2-n^2} \\ -\pi \cot \pi s = \pi \cdot \cot(-\pi s) = c - \frac{1}{s} - \sum_{n=1}^{\infty} \frac{2s}{s^2-n^2} \end{array}\right\} \ 0 = 2c,\ c = 0$$

Also ist $h(s) = c_1$ konstant, oder $e^{h(s)} = c_2$ konstant. Damit

$$\sin \pi s = c_2 \cdot s \prod_{n=1}^{\infty} (1 - \frac{s^2}{n^2}); \quad \lim_{s\to 0} \frac{\sin \pi s}{s} = \pi = c_2$$

liefert die Behauptung. ■

3 Bernoulli-Zahlen

(3.1) Definition. Die Bernoulli-Zahlen[1] B_n ($n \in \mathbb{N}$) sind erklärt durch die erzeugende Funktion (formale Potenzreihe über $\mathbb{Q}$)

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$$

Bemerkung. Für $|s| < 2\pi$ ist $\frac{s}{e^s-1}$ holomorph, also dort als konvergente Potenzreihe darstellbar

$$\frac{s}{e^s - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} s^n.$$

[1] Jakob Bernoulli, 1654-1705

(3.2) Lemma. *$B_0 = 1$ und für $n \geq 1$ gilt: $\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0$ („Rekursionsformel“)*

Beweis.

$$\frac{t}{e^t - 1} = \frac{t}{1 + t + \frac{t^2}{2!} + \cdots - 1} = \frac{1}{1 + \frac{t}{2!} + \frac{t^2}{3!} + \cdots} = B_0 + B_1 t + \frac{B_2}{2!} t^2 + \cdots$$

Also

$$\left(1 + \frac{t}{2!} + \frac{t^2}{3!} + \cdots + \frac{t^n}{(n+1)!} + \cdots\right) \underset{\substack{\uparrow \\ \text{Cauchy-} \\ \text{Produkt}}}{\cdot} \left(B_0 + B_1 t + \cdots \frac{B_n}{n!} t^n + \cdots\right) = 1(+0t + 0t^2 + \cdots)$$

Daher ist $B_0 = 1$ und für $n \geq 1$ gilt

$$\frac{1}{(n+1)!} + \frac{1}{n!} B_1 + \frac{1}{(n-1)!} \frac{B_2}{2!} + \cdots + \frac{1}{(n-k+1)!} \frac{B_k}{k!} + \cdots + \frac{B_n}{n!} = 0 \quad \Big| \quad (n+1)!$$

$$\underset{(=B_0)}{1} + \binom{n+1}{1} B_1 + \cdots + \underbrace{\frac{(n+1)!}{(n+1-k)!k!}}_{\binom{n+1}{k}} B_k + \cdots + \binom{n+1}{n} B_n = 0$$

∎

Beispiel:

$$\underbrace{1}_{B_0} + 2B_1 = 0\ ; \quad B_1 = -\frac{1}{2}$$

$$B_0 + 3B_1 + 3B_2 = 0\ ; \quad B_2 = \frac{1}{6}$$

$$B_0 + 4B_1 + 6B_2 + 4B_3 = 0\ ; \quad B_3 = 0$$

$$B_0 + 5B_1 + 10B_2 + 10B_3 + 5B_4 = 0\ ; \quad B_4 = -\frac{1}{30}$$

(3.3) Lemma. *Für $n \geq 3$ ungerade ist $B_n = 0$.*

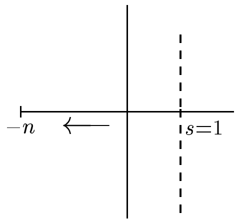
Beweis.

$$\underset{\substack{\| \\ \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n + t\right)}}{\frac{t}{e^t - 1} + t} = \frac{t + te^t - t}{e^t - 1} = \frac{t \cdot e^t}{e^t - 1} = \frac{t}{1 - e^{-t}} = \frac{-t}{e^{-t} - 1} \left(= \sum_{n=0}^{\infty} \frac{B_n}{n!} (-t)^n\right)$$

Für $n \geq 2$ gilt also $(-1)^n B_n = B_n$. (Koeffizientenvergleich) ∎

(3.4) Satz. *$\zeta(s)$ kann analytisch auf $\mathrm{Re}(s) \leq 0$ fortgesetzt werden. Zu jedem $n \in \mathbb{N}_{>0}$ gibt es eine (eindeutige) holomorphe Funktion $f_n(s)$ in $\mathrm{Re}(\mathbf{s}) > -\mathbf{n}$ mit*

$$\zeta(s) = \frac{f_n(s)}{\Gamma(s)} + \frac{1}{s-1} + \frac{1}{2} + \sum_{k=2}^{n} \frac{B_k}{k!} s(s+k)(s+k-2)$$



Beweis. Nach (2.8):

$$\zeta(s)\Gamma(s) = \int_0^\infty \frac{t^{s-1}}{e^t-1}\,dt = \int_0^\infty \left(\frac{te^t}{e^t-1}\right)\cdot e^{-t}t^{s-2}\,dt$$

Sei $n \in \mathbb{N}_{>0}$ fest. Für $|s| < 1$ ist

$$\frac{se^s}{e^s-1} = \underset{(=B_0)}{1} + \underset{(=B_1+1)}{\frac{1}{2}s} + \sum_{k=2}^{\infty} \frac{B_k}{k!} s^k$$

Setze

$$g_n(s) = 1 + \frac{1}{2}s + \sum_{k=2}^{n} \frac{B_k}{k!} s^k$$

dann

$$\begin{aligned} \frac{se^s}{e^s-1} - g_n(s) &= O(s^{n+1}) \text{ für } s \to 0 \\ \Bigg(&= s^{n+1} \sum_{k=n+1}^{\infty} \frac{B_k}{k!} s^{k-n-1} \Bigg) \end{aligned}$$

Also

$$\zeta(s)\Gamma(s) = \underbrace{\int_0^\infty \left(\frac{te^t}{e^t-1} - g_n(t)\right) e^{-t}t^{s-2}\,dt}_{=:f_n(s)} + \underbrace{\int_0^\infty g_n(t)e^{-t}t^{s-2}\,dt}_{=:\widetilde{g}_n(s)}$$

$f_n(s)$ holomorph für $\mathrm{Re}(s) > -n$ (wegen $\frac{te^t}{e^t-1} - g_n(t) = O(t^{n+1})$)
Es gilt (Existenz bei 0)

$$\begin{aligned} \widetilde{g}_n(s) &= \int_0^\infty e^{-t}t^{s-2}\,dt + \frac{1}{2}\int_0^\infty te^{-t}t^{s-2}\,dt + \sum_{k=2}^{n} \frac{B_k}{k!} \int_0^\infty e^{-t}t^{s-k-2}\,dt \\ &\underset{(2.7)}{=} \Gamma(s-1) + \frac{1}{2}\Gamma(s) + \sum_{k=2}^{n} \frac{B_k}{k!} \Gamma(s+k-1) \text{ meromorph (auf } \mathbb{C}) \end{aligned}$$

Also ist $\zeta(s)\Gamma(s)$ für $\mathrm{Re}(s) > -n$ erklärt, und dort gilt (mit Funktionalgleichung für Γ-Fkt)

$$\zeta(s) = \underbrace{\frac{f_n(s)}{\Gamma(s)}}_{\left(\substack{\text{holomorph} \\ \text{für } \mathrm{Re}(s)>-n}\right)} + \underbrace{\frac{\Gamma(s-1)}{\Gamma(s)}}_{=\frac{1}{s-1}} + \frac{1}{2} + \sum_{k=2}^{n} \frac{B_k}{k!} \underbrace{\frac{\Gamma(s+k-1)}{\Gamma(s)}}_{=s(s+1)\cdots(s+k-2)}$$

■

(3.5) Satz. $\zeta(0) = -\frac{1}{2}$ *und für* $n \in \mathbb{N} > 0$ *gilt:* $\zeta(-2n) = 0,\ \zeta(1-2n) = -\frac{B_{2n}}{2n}$

Beweis.

$n = 1$

$$\zeta(s) = \frac{f_1(s)}{\Gamma(s)} + \frac{1}{s-1} + \frac{1}{2} \quad (\mathrm{Re}(s) > -1); \quad (3.4)$$

Nach (2.3) gilt $\frac{1}{\Gamma(-m)} = 0$ für alle $m \in \mathbb{N}$.

$$\zeta(0) = \frac{1}{-1} + \frac{1}{2} = -\frac{1}{2}$$

$n = 2$

$$\zeta(s) = \frac{f_2(s)}{\Gamma(s)} + \frac{1}{s-1} + \frac{1}{2} + \frac{B_2}{2!}s \quad (\mathrm{Re}(s) > -2)$$

$$\zeta(-1) = \frac{1}{-2} + \frac{1}{2} - \frac{B_2}{2!} = -\frac{B_2}{2!} = -\frac{1}{12}$$

Sei $n > 2$. Dann für $\mathrm{Re}(s) > -n$ die Darstellung in (3.4), also

$$\begin{aligned}
\zeta(1-n) &= \frac{1}{1-n-1} + \underbrace{\frac{1}{2}}_{=-B_1} + \sum_{k=2}^{n} \frac{B_k}{k!}(1-n)(1-n+1)\cdots(1-n+k-2) \\
&= -\frac{1}{n}[B_0 + \underbrace{n}_{=\binom{n}{1}} B_1 + \sum_{k=1}^{n} \frac{B_k}{k!}(-1)^k(n-1)(n-2)\cdots(n-k+1)(+n)] \\
&\underset{3.3}{=} -\frac{1}{n} \sum_{k=0}^{n} \binom{n}{k} B_k \underset{3.2}{=} -\frac{B_n}{n}
\end{aligned}$$

■

Ist $1 - n = -2m$, *so* $\zeta(-2m) = -\frac{B_n}{n} = -\frac{B_{2m+1}}{2m+1} = 0$ *nach (3.2)*
Ist $1 - n = -2m + 1$, *so* $\zeta(1-2m) = -\frac{B_{2m}}{2m}$

(3.6) Lemma. *Für* $|s| < 1$ *gilt:*

$$\sum_{n=1}^{\infty} (-1)^{n-1} 2^{2n-1} \pi^{2n} \frac{B_{2n}}{(2n)!} s^{2n} = \frac{s}{2}(\frac{1}{s} - \pi \cot \pi s) = \sum_{n=1}^{\infty} \zeta(2n) s^{2n}$$

Beweis.

$$\begin{aligned}
\text{linke Seite} \quad &= \quad -\frac{1}{2}\sum_{n=1}^{\infty}\frac{B_{2n}}{(2n)!}(2\pi is)^{2n} \overset{(3.3)}{=} -\frac{1}{2}\sum_{n=0}^{\infty}\frac{B_n}{n!}(2\pi is)^n + \underbrace{\frac{1}{2}B_0}_{=\frac{1}{2}} + \underbrace{\frac{1}{2}B_1 2\pi is}_{=-\frac{1}{2}\pi is} \\
&= \quad +\frac{1}{2}(1 - \pi is - \sum_{n=0}^{\infty}\frac{B_n}{n!}(2\pi is)^n) = \frac{1}{2}(1 - \pi is - \frac{2\pi is}{e^{2\pi is}-1}) \\
&= \quad \frac{s}{2}(\frac{1}{s} - \frac{\pi i e^{2\pi is} + \pi i}{e^{2\pi is}-1}) = \frac{s}{2}(\frac{1}{s} - \pi i\frac{e^{\pi is}+e^{-\pi is}}{e^{\pi is}-e^{-\pi is}}) \\
&= \quad \frac{s}{2}(\frac{1}{s} - \pi\cot\pi s) \overset{(2.9)}{=} -\frac{s}{2}\sum_{n=1}^{\infty}\frac{2s}{s^2-n^2} = \sum_{n=1}^{\infty}\frac{\frac{s^2}{n^2}}{1-(\frac{s}{n})^2} \\
&\overset{|s|<1}{=} \quad \sum_{n=1}^{\infty}\frac{s^2}{n^2}(1 + (\frac{s}{n})^2 + (\frac{s}{n})^4 + (\frac{s}{n})^6 + \dots) \quad ; \quad |s| < 1 \\
&= \quad \sum_{n=1}^{\infty}(\frac{s^2}{n^2} + \frac{s^4}{n^4} + \frac{s^6}{n^6} + \frac{s^8}{n^8} + \dots) \\
&= \quad \sum_{n=1}^{\infty}(\zeta(2)s^2 + \zeta(4)s^4 + \dots) \quad \text{(Umordnung)} \\
&= \quad \sum_{n=1}^{\infty}\zeta(2n)s^{2n}.
\end{aligned}$$

■

(3.7) Satz. *Für $n \in \mathbb{N}_{>0}$ gilt*

$$\zeta(2n) = (-1)^{n-1}2^{2n-1}\pi^{2n}\frac{B_{2n}}{(2n)!}.$$

Insbesondere $(-1)^{n-1}B_{2n} > 0$.

Beweis. Koeffizientenvergleich in (3.6). Beachte $\zeta(2n) = \sum_{k=1}^{\infty}\frac{1}{k^{2n}} \geq 1$. ■

Spezialfälle:

$$\left.\begin{array}{l} n = 1: \quad \zeta(2) = \sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{\pi^2}{6} \\ n = 2: \quad \zeta(4) = \sum_{k=1}^{\infty}\frac{1}{k^4} = \frac{\pi^4}{90} \end{array}\right\} \textit{(Euler!!!)}$$

$$\textit{Analog: } \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450}, \dots$$

(3.8) Bemerkungen.

(a) $\zeta(1-2n)$ und $\zeta(2n)$ sind Funktionen von B_{2n}. Dies ist ein Spezialfall der Funktionalgleichung der Zeta-funktion. Aus dieser Funktionalgleichung folgt, zusammen mit (1.6), (1.10), dass in $\mathrm{Re}(s) \leq 0$ nur die (trivialen) Nullstellen von $\zeta(s)$ für $s = -2n, n \in \mathbb{N}_{>0}$, vorkommen.

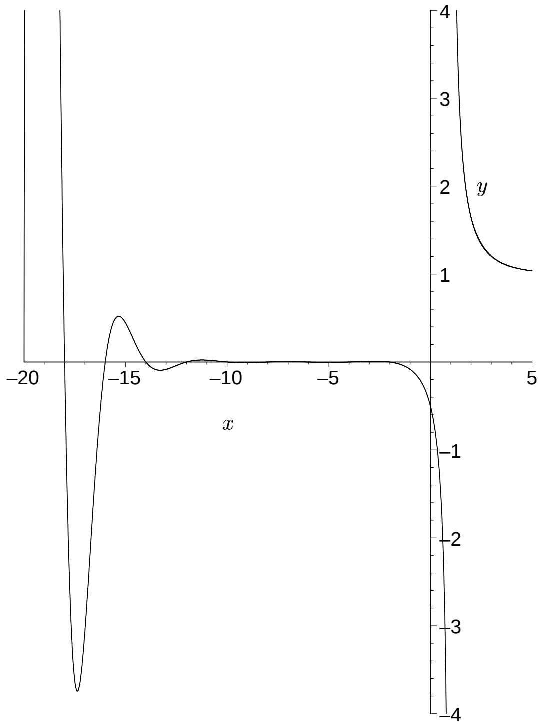
(b) Im kritischen Streifen $0 < \mathrm{Re}(s) < 1$ liegen unendlich viele Nullstellen von $\zeta(s)$, und zwar symmetrisch zu $\mathrm{Re}(s) = \frac{1}{2}$ und $\mathrm{Im}(s) = 0$.
Die „ersten" Nullstellen sind $\frac{1}{2} \pm i \cdot 14,134\ldots$, $\frac{1}{2} \pm i \cdot 21,022\ldots$, $\frac{1}{2} \pm i \cdot 25,010\ldots$

(c) Die Berechnung von $\zeta(2n+1), n \in \mathbb{N}_{>0}$ erfordert „neue Theorie" (Borel, Kato, Tamayawa,...).

(3.9) Die reelle Zeta-Funktion.

$$\zeta(x) \sim \frac{1}{x-1} \text{ für } x \to 1 \ (1.7)\ldots$$

$$\zeta(s) \geq 1 \text{ für } x > 1; \zeta(-2n) = 0; \zeta(1-2n) = -\frac{B_{2n}}{2n} \ (3.5)$$



$$B_{18} = \frac{43867}{798}; \quad \zeta(-17) = -\frac{B_{18}}{18} \approx -3$$

$$B_{20} = -\frac{174611}{230}; \quad \zeta(-19) = -\frac{B_{20}}{20} \approx 26$$

4 Dirichlet Reihen

Dirichlet, Gustav Peter Lejeune (1805-1859), frz. Mathematiker.

(4.1) Definition. Sei $(a_n)_{n\geq 1}$ eine Folge komplexer Zahlen, sei $(\lambda_n)_{n\geq 1}$ eine streng monoton wachsende Folge reeller Zahlen mit $\lim\limits_{n\to\infty} \lambda_n = +\infty$. Dann

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

die durch (a_n), (λ_n) bestimmte Dirichlet-Reihe.

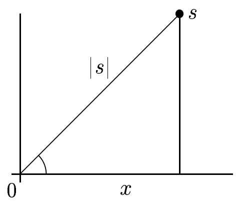
Spezialfälle.

- $\lambda_n = n$: $\sum_{n=1}^{\infty} a_n e^{-\lambda_n s} = \sum_{n=1}^{\infty} a_n (e^{-s})^n$ Potenzreihe in $z = e^{-s}$ $(|z| \leq a \Leftrightarrow \mathrm{Re}(s) \geq a)$
- $\lambda_n = \log n$: $\sum_{n=1}^{\infty} a_n e^{-\lambda_n s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ gewöhnliche Dirichlet Reihe

(4.2) Lemma. *Sei* $0 < a < b$ *reelle Zahlen; sei* $z \in \mathbb{C}$ *mit* $\mathrm{Re}(z) = x > 0$.
Behauptung: $|e^{-as} - e^{-bs}| \leq \frac{|s|}{x}(e^{-ax} - e^{-bx})$

Beweis.

$$\begin{aligned} |e^{-as} - e^{-bs}| &= |s| \cdot \left| \int_0^b e^{-ts}\, dt \right| \leq |s| \cdot \left| \int_a^b |e^{-ts}|\, dt \right| \\ &= |s| \cdot \left| \int_a^b e^{-tx}\, dt \right| = \frac{|s|}{x} \left[e^{-tx} \right]_a^b \end{aligned}$$



■

(4.3) Lemma (Abelsche Summation). *Seien* $(a_n), (b_n)$ *komplexe Folgen; schreibe (durchweg) für* $m \leq r$ *in* $\mathbb{N} > 0$

$$A_m = \sum_{n=1}^{m} a_n, \quad A_{m,r} = \sum_{n=m}^{r} a_n$$

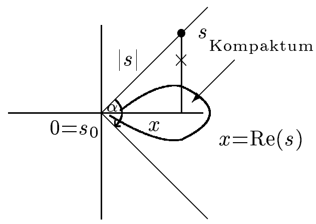
Behauptung: $S_{m,r} = \sum_{n=m}^{r} a_n b_n = A_{m,r} b_r + \sum_{n=m}^{r-1} A_{n,m}(b_n - b_{n+1})$

Beweis. Es ist $a_n = A_{m,n} - A_{m,n-1}$ $(m < n \leq r)$
Also

$$\begin{aligned} S_{m,r} &= (A_{m,r} - A_{m,r-1})b_r + (A_{m,r-1} - A_{m,r-2})b_{r-1} + \cdots + \\ &\quad +(A_{m,m+1} - A_{m,n})b_{m+1} + A_{m,n}b_n \\ &= A_{m,r}b_r + A_{m,r-1}(b_{r-1} - b_r) + \cdots + A_{m,m}(b_m - b_{m+1}) \end{aligned}$$

■

(4.4) Satz. *Die Dirichlet-Reihe* $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ *konvergiere für* $s = s_0$. *Dann konvergiert die Reihe gleichmäßig in jedem „Sektor“* $\mathrm{Re}(s - s_0) \geq 0, \mathrm{Arg}(s - s_0) \leq \alpha$ $(|\alpha| < \frac{\pi}{2})$. *Insbesondere stellt* $f(s)$ *für* $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ *eine holomorphe Funktion dar (und gliedweise Differentiation!)*



Beweis. o.B.b.A: $s_0 = 0$. [Ersetze s durch $t = s - s_0$ und a_n durch $a_n e^{-\lambda_n s_0}$.
$\sum_{n=1}^{\infty} (a_n e^{-\lambda_n s_0}) e^{-\lambda_n t}$ konvergiert für $t = 0$.]
Dann konvergiert nach Voraussetzung die Reihe $\sum_{n=1}^{\infty} a_n$.
Sektor: Sei $M > 0$, und betrachte $S_M = \{s \in \mathbb{C} | \mathrm{Re}(s) > 0, \ \frac{|s|}{\mathrm{Re}(s)} \leq M\} \big(\cup \{0\}\big)$
(Jeder „Sektor“ ist von dieser Form und jedes Kompaktum in $\mathrm{Re}(s) > 0$ liegt in einem solchen S_M.)
Sei $\varepsilon > 0$; $\ s \in S_M$, $\ x = \mathrm{Re}(s) > 0$; es gibt $N \in \mathbb{N}_{>0}$ derart, dass $\lambda_N > 0$ ($\lambda_n > 0$ für alle $n \geq N$) und $|A_{m,r}| = |\sum_{n=m}^{r} a_n| < \varepsilon$ für alle $r \geq m \geq N$.
Wir rechnen mit (4.3) [$b_n = e^{-\lambda_n s}$] und (4.2): [$r \geq m \geq N$]

$$\begin{aligned}
\left|\sum_{n=m}^{r} a_n e^{-\lambda_n s}\right| &= \left|A_{m,r} e^{-\lambda_r s} + \sum_{n=m}^{r-1} A_{m,r} \left(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right)\right| \\
&\leq \underbrace{|A_{m,r}|}_{<\varepsilon} \underbrace{|e^{-\lambda_r s}|}_{=e^{-\lambda_r x} < 1} + \sum_{n=m}^{r-1} \underbrace{|A_{m,n}|}_{<\varepsilon} \cdot \underbrace{|e^{-\lambda_n s} - e^{-\lambda_{n+1} x}|}_{\underset{(4.2)}{\leq} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) \cdot \frac{|s|}{x}} \\
&< \varepsilon \left(1 + \frac{|s|}{x} \sum_{n=m}^{r-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}\right) \\
&\leq \varepsilon(1 + M(e^{-\lambda_m x} - e^{-\lambda_r x})) < \varepsilon(1 + M).
\end{aligned}$$

Der Rest folgt aus (1.4). ■

(4.5) Folgerungen. Die Dirichlet-Reihe $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ konvergiere irgendwo

(a) Entweder ist $f(s)$ holomorph auf $\mathbb{C}$ (Konvrergenz überall; $\varrho_f = -\infty$) oder es gibt eine kleinste reelle Zahl $\varrho = \varrho_f$, so dass $f(s)$ holomorph in $\mathrm{Re}(s) > \varrho$.
ϱ_f heißt die **Konvergenzabszisse** von f

(b) Gilt $f(x) = 0$ für alle reellen $x > \varrho$ ($\varrho \in \mathbb{R}$ geeignet), so ist $a_n = 0$ für alle n.

Beweis. Sonst gibt es ein kleinstes $k \in \mathbb{N}_{>0}$ mit $a_k \neq 0$.
Für alle $x > \varrho$ gilt:

$$0 = f(x) \cdot e^{\lambda_k x} = a_k + \sum_{n=k+1}^{\infty} a_n e^{-(\lambda_n - \lambda_k)x}$$

Es gilt $\lim_{x\to+\infty} a_n e^{-\overbrace{(\lambda_n-\lambda_k)}^{>0}x} = 0$ Wegen der gleichmäßigen Konvergenz:

$$\lim_{x\to+\infty} \sum_{n=k+1}^{\infty} a_n e^{-(\lambda_n-\lambda_k)x} = 0$$

$\Longrightarrow a_k = 0$ Widerspruch ■

Konsequenz: Sei auch $g(s) = \sum_{n=1}^{\infty} b_n e^{-\lambda_n s}$ Dirichlet-Reihe (zu (λ_n)).
Gilt auch $g(s) = f(s)$ für alle $s = x > \varrho$ ($\varrho \in \mathbb{R}$), so gilt $\underbrace{b_n = a_n \text{ für alle } n}_{\text{„Identitätssatz“}}$

Beweis. Betrachte $g - f$. ■

(4.6) Satz. *Sei* $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *eine gewöhnliche Dirichlet-Reihe,*
$A_m = \sum_{n=1}^{m} a_n \quad (n \in \mathbb{N}_>)$.
Es gebe $a, c \in \mathbb{R}$ $(c > 0)$ *mit* $|A_m| \le cm^a$ *für alle* $m \in \mathbb{N}_{>0}$,
d.h (d.s.h)[2]***:*** $A_m = O(m^a)$.
Behauptung: $\varrho_f \le a$

Beweis. Sei $\delta > 0$ und $x = a + \delta$.
Nach (4.4) genügt es zu zeigen: $\sum_{n=1}^{\infty} \frac{a_n}{n^x}$ konvergiert.
Nach (4.3) gilt für jedes $m \in \mathbb{N}_{>0}$ (und $b_n = \frac{1}{n^x}$):

$$\sum_{n=1}^{m} \frac{a_n}{n^x} = A_m \cdot \frac{1}{m^x} + \sum_{n=1}^{m-1} A_n \left(\frac{1}{n^x} - \frac{1}{(n+1)^x} \right)$$

(i)

$$|A_m \frac{1}{n^x}| \le cm^a \frac{1}{m^x} = \frac{c}{m^\delta} \underset{(m\to\infty)}{\longrightarrow} 0$$

(ii)

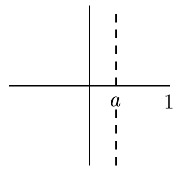
$$\begin{aligned}
\left| A_n \cdot \left(\frac{1}{n^x} - \frac{1}{(n+1)^x} \right) \right| &\le cn^a \cdot |x| \cdot \left| \int_n^{n+1} \frac{dt}{t^{x+1}} \right|, \quad (1 \le n \le m-1) \\
&\le c \cdot |x| \cdot \left| \int_n^{n+1} \frac{dt}{t^{\delta+1}} \right| \quad (n \le t \le n+1) \\
&\le c \cdot |x| \cdot \frac{1}{n^{\delta+1}}
\end{aligned}$$

Die Reihe $c|x| \sum_{n=1}^{\infty} \frac{1}{n^{\delta+1}}$ konvergiert (Majorante) ■

---

[2]=Das soll heißen

(4.7) Folgerung. Sei $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, es gelte: $A_m = mz_0 + O(m^a)$ für geeignete $z_0 \in \mathbb{C}^*$ und $0 \leq a < 1$.
Dann ist $f(s)$ holomorph für $\mathrm{Re}(s) > a$ bis auf die Stelle $s = 1$, wo $f(s)$ einen einfachen Pol mit Residuum z_0 hat.



Beweis. Betrachte

$$\widetilde{f}(s) = \sum_{n=1}^{\infty} \frac{a_n - z_0}{n^s};$$

$$\widetilde{A}_m = \sum_{n=1}^{m} (a_n - z_0) = A_m - mz_0 = O(m^a)$$

Nach (4.6) ist $\widetilde{f}(s)$ holomorph für $\mathrm{Re}(s) > a$. Es gilt für $\mathrm{Re}(s) > 1$

$$\widetilde{f}(s) = f(s) - z_0\zeta(s)$$

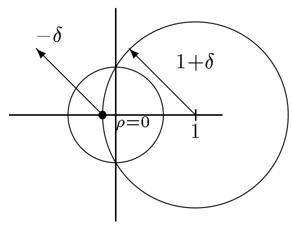
Wende (1.7) [oder (3.4)] an. ■

(4.8) Satz (Landau). *Sei*

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

Dirichlet-Reihe mit $\varrho = \varrho_f \in \mathbb{R}$ $(\varrho_f \neq -\infty)$
Gilt $0 \leq a_n \in \mathbb{R}$ *für alle* $n \in \mathbb{N}_{>0}$, *so hat* $f(s)$ *in* $s = \varrho$ *einen singulären Punkt.*

Beweis. o.B.d.A: $\varrho = 0$ [Translation! (4.4)]
o.B.d.A: $\lambda_n > 0$ für alle n.
Anmerkung: $f(s)$ hat in $s = 0$ einen regulären Punkt, d.h.:
$f(s)$ um $s = 0$ in Taylorreihe darstellbar,
d.h. es gibt $\delta > 0$ derart, dass die Taylorreihe



$$f(s) = \sum_{k=0}^{\infty} \frac{f^k(1)}{k!}(s-1)! \text{ für } |s-1| \leq \delta$$

konvergiert (und in $\mathrm{Re}(s) > 0$ die Funktion $f(s)$ darstellt)
Nach (4.4) und Definition von $\varrho = \varrho_f = 0$ ist die Reihe

$$\sum_{n=1}^{\infty} a_n e^{(-\lambda_n)(-\delta)} = \sum_{n=1}^{\infty} a_n e^{\lambda_n \delta}$$

nicht konvergent. Nach (4.4)

$$f^{(k)}(s) = \sum_{n=1}^{\infty} (-\lambda_n)^k a_n e^{-\lambda_n s} \quad (\mathrm{Re}(s) > 0)$$

also konvergiert

$$(-1)^k f^k(1) = \sum_{n=1}^{\infty} \lambda_n^k a_n e^{-\lambda_n} \quad (k = 0, 1, 2, \ldots).$$

Andererseits konvergiert („absolut“)

$$f(-\delta)_{„} = „ \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!}(-\delta - 1)^k = \sum_{k=0}^{\infty} \left(\sum_{n=1}^{\infty} \frac{\lambda_n^k a_n}{k!} (\delta + 1)^k \cdot e^{-\lambda_n} \right).$$

Alle Faktoren der Glieder dieser Doppelreihe sind nicht negative reelle Zahlen,
absolute Konvergenz
Umordnung

$$f(\delta) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n} \underbrace{\left(\sum_{k=0}^{\infty} \frac{\lambda_n^k (\delta + 1)^k}{k!} \right)}_{= e^{\lambda_n(\delta+1)}} = \sum_{n=1}^{\infty} a_n e^{\lambda_n \delta}$$

Dies ist ein Widerspruch. ■

5 Faktorisierungen und Faltungen

$\chi : \mathbb{N}_{>0} \to \mathbb{C}$ komplexe Folge ($\chi \in \mathbb{C}^{\mathbb{N}_{>0}}$); $\mathsf{X}(s) = \sum \frac{\chi(n)}{n^s}$ zugehörige gewöhnliche Dirichlet-Reihe. ($\chi \neq 0$)

(5.1) Definition. χ *multiplikativ* $\Leftrightarrow \chi(n \cdot m) = \chi(n) \cdot \chi(m)$ für alle teilerfremden n, m.
χ *stark multiplikativ* $:\Leftrightarrow \chi(n \cdot m) = \chi(n) \cdot \chi(m)$ für alle n, m.

Bemerkung. Gilt $\chi(n) = 1$ für alle $n \in \mathbb{N}$, so ist χ stark multiplikativ (und $\chi(s) = \zeta(s)$)
Sei χ multiplikativ; es gibt dann $n \in \mathbb{N}_{>0}$ mit $0 \neq \chi(n) = \chi(1 \cdot n) = \chi(1) \cdot \chi(n)$
Also dann $0 \neq \chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$ und $\chi(1) = 1$

(5.2) Beispiel. Sei χ multiplikativ.

(a) Für $b \in \mathbb{R}(\mathbb{C})$ ist $\widetilde{\chi} : n \mapsto \chi(n) n^b$ multiplikativ $[(nm)^b = n^b m^b]$
Es ist

$$\widetilde{\mathsf{X}}(s) = \sum_{n=1}^{\infty} \frac{\widetilde{\chi}(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{s-b}} = \mathsf{X}(s - b)$$

(b) Für $a \in \mathbb{N}_{>0}$ ist $\widetilde{\chi} : \mathbb{N}_{>0} \to \mathbb{C}$ multiplikativ, wo

$$\widetilde{\chi}(m) = \begin{cases} \chi(n), & \text{falls } m = n^a \\ 0 & \text{sonst} \end{cases}$$

[$m \cdot m' = n^a$ für $m, m' \in \mathbb{N}_>$ teilerfremd, $n \in \mathbb{N}_{>0}$, so ist $m = k^a, m' = \ell^a$ mit $k, \ell \in \mathbb{N}_{>0}$.]
Es gilt

$$\widetilde{\mathsf{X}}(s) = \sum_{n=1}^{\infty} \frac{\widetilde{\chi}(m)}{m^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{(n^a)^s} = \mathsf{X}(as)$$

(5.3) Satz. *χ ist genau dann multiplikativ, wenn das* ***Euler-Produkt*** *gilt.*

$$\mathsf{X}(s) = \prod_{p \in \mathbb{P}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \frac{\chi(p^3)}{p^{3s}} + \cdots\right) \tag{3}$$

[Das Produkt konvergiert in jeder Halbebene, in der $\mathsf{X}(s)$ konvergiert]

Beweis. Sei $2 \leq a \in \mathbb{R}$ (groß), $\mathbb{P}_a = \{p \in \mathbb{P} | p \leq a\}, \mathbb{N}_a := \{n \in \mathbb{N}_{>0} | n$ nur durch $p \in \mathbb{P}_a$ teilbar $\}$
Rechne (Cauchy-Produkt):

$$\begin{aligned}
\prod_{p \in \mathbb{P}} \left(\chi(1) + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) &= \sum_{n \in \mathbb{N}_a} \frac{\pi(n)}{n^s}; \text{ wobei } \pi(n) = \chi(1)\chi(p_1^{e_1}) \cdots \chi(p_r^{e_r}), \\
&\quad \text{falls } n = p_1^{e_1} \cdot \cdots \cdot p_r^{e_r} \text{ PFZ } (p_i \leq a) \\
&= \sum_{n \in \mathbb{N}_a} \frac{\chi(n)}{n^s} \Leftrightarrow (\chi(1) = 1) \\
&\quad \text{und } \chi \text{ multiplikativ auf } \mathbb{N}_a
\end{aligned}$$

Lasse $a \to \infty$

Zusatz. Ist χ *stark* multiplikativ, so [$\chi(p^k) = \chi(p)^k$ für $p \in \mathbb{P}, k \in \mathbb{N}$] **Euler-Produkt:**

$$\boxed{\mathsf{X}(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}} \qquad \text{(geometrische Reihe)}$$

■

(5.4) Definition. Seien $\chi,\ \widetilde{\chi} : \mathbb{N}_{>0} \to \mathbb{C}$ Folgen, dann Faltung $\chi \star \widetilde{\chi} : \mathbb{N}_{>0} \to \mathbb{C}$,

$$(\chi \star \widetilde{\chi})(n) = \sum_{\substack{(k,\ell \in \mathbb{N}_{>0}) \\ k\ell = n}} \chi(k) \cdot \chi(\ell) = \sum_{d|n} \chi(d) \cdot \widetilde{\chi}(\frac{n}{d})$$

Lemma. *Ist* $\overset{(\sim)}{\mathsf{X}}(s) = \sum_{n=1}^{\infty} \frac{\overset{(\sim)}{\chi}(n)}{n^s}$, *so ist* $\mathsf{X}(s) \cdot \widetilde{\mathsf{X}}(s) = \sum_{n=1}^{\infty} \frac{(\chi \star \widetilde{\chi})(n)}{n^s}$

Beweis.

$$\mathsf{X}(s) \cdot \widetilde{\mathsf{X}}(s) = \sum_{k,\ell \in \mathbb{N}_{>0}} \frac{\chi(k)}{k^s} \cdot \frac{\widetilde{\chi}(\ell)}{\ell^s} = \sum_{n=1}^{\infty} \frac{(\chi \star \widetilde{\chi})(s)}{n^s} \quad [k \cdot \ell = n]$$

■

(5.5) Folgerung. Sind χ und $\widetilde{\chi}$ multiplikativ, so auch $\chi \star \widetilde{\chi}$.

Beweis.

$$\begin{aligned} \mathsf{X}(s) \cdot \widetilde{\mathsf{X}}(s) &= \prod_{p \in \mathbb{P}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right)\left(1 + \frac{\widetilde{\chi}(p)}{p^s} + \frac{\widetilde{\chi}(p^2)}{p^{2s}} + \cdots\right) \\ &= \prod_{p \in \mathbb{P}} \left(1 + \frac{\chi(p) + \widetilde{\chi}(p)}{p^s} + \frac{\overbrace{\chi(p^2) + \widetilde{\chi}(p^2) + \chi(p)\widetilde{\chi}(p)}^{(\chi\star\widetilde{\chi})(p^2)}}{p^{2s}} + \cdots\right. \end{aligned}$$

Wende (5.3) an! ■

(5.6) Beispiele.

(a)

$$\zeta(s)^2 = \zeta(s) \cdot \zeta(s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}$$

für eine multiplikative Folge d. (5.5)
Es ist $d(n) = \sum_{d|n} 1 \cdot 1 =$ Anzahl der Teiler von n.

(b)

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

für eine multiplikative Folge τ (5.5) [$\mathrm{Re}(s) > 2$]
Es ist $\tau(n) = \sum_{d|n} d \cdot 1$ Summe der Teiler von s.

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

(c)

$$\zeta(s) \cdot \zeta(s-k) \underset{\left.\begin{subarray}{c}(5.2)(a)\\(5.5)\end{subarray}\right\}}{=} \sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} \text{ mit einer multiplikativen Funktion } \sigma_k \ (\mathrm{Re}(s) > k)$$

Es ist $\sigma_k(n) = \sum\limits_{d|n} d^k \cdot 1 \quad [\zeta(s-k) = \sum_{n=1}^{\infty} \frac{n^k}{n^s}]$
Summe der k-ten Potenzen der Teiler von m.

Bemerkung. $\sigma_0 = d, \sigma_1 = c$

(d)

$$\begin{aligned} \frac{1}{\zeta(s)} &\underset{(1.6)}{=} \prod_{p\in\mathbb{P}}(1-\frac{1}{p^s}) = \prod_{p\in\mathbb{P}}(1-\frac{1}{p^s}+\frac{0}{p^{2s}}+\cdots) \quad (\mathrm{Re}(s)>1) \\ &= \sum_{n=1}^{\infty}\frac{\mu(s)}{n^s} \text{ mit einer } \textbf{multiplikativen} \text{ Funktion } \mu. \quad (5.3) \end{aligned}$$

Es gilt: $\mu(p) = -1,\ \mu(p^2) = 0,\ \mu(p^k) = 0$ für $p \in \mathbb{P}$, $k \in \mathbb{N}_{\geq 2}$, also

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{, falls } n \text{ nicht quadratfrei} \\ (-1)^r & \text{, falls } n = p_1 \cdot \cdots \cdot p_r \text{ mit verschiedenen Primzahlen } p_i \end{cases}$$

Wegen

$$\frac{1}{\zeta(s)} \cdot \zeta(s) = 1 = \overbrace{1}^{\frac{1}{1^s}} + \frac{0}{2^s} + \frac{0}{3^s} + \cdots \text{ folgt nach (5.4)}$$

$$\boxed{\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{, falls } n = 1 \\ 0 & \text{sonst} \end{cases}}$$

Bemerkung. μ heißt **Möbius-Funktion**

(e)

$$\begin{aligned} \frac{\zeta(s-1)}{\zeta(s)} &= \sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} \\ &\quad \text{mit einer multiplikativen Funktion } \varphi \ \ (5.4) \text{ und (d); } \mathrm{Re}(s) > 2 \\ &= \prod_{p\in\mathbb{P}}\left(1+\frac{p}{p^s}+\frac{p^2}{p^{2s}}+\frac{p^3}{p^{3s}}+\cdots\right)\left(1-\frac{1}{p^s}\right) \\ &= \prod_{p\in\mathbb{P}}\left(1+\frac{p-1}{p^s}+\frac{p^2-p}{p^{2s}}+\cdots\cdots\frac{p^k-p^{k-1}}{p^{ks}}+\cdots\right) \end{aligned}$$

Also:

$$\varphi(p) = p-1,\ \varphi(p^2) = p^2-p = p(p-1), \ldots, \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Wegen

$$\frac{\zeta(s-1)}{\zeta(s)} \cdot \zeta(s) = \zeta(s-1) \quad \left[= \sum_{n=1}^{\infty} \frac{n}{n^s} \right] \text{ gilt nach (5.4) :}$$

$$\boxed{\sum_{d|n} \varphi(d) = n}$$

Bemerkung. φ heißt die **Eulersche φ-Funktion**. Es gilt:

$$\varphi(n) = |\{r \in \mathbb{N}_{>0} | r \leq n, \mathrm{ggT}(r,n) = 1\}|$$

Anmerkung: Für den Primzahlsatz wichtige Funktionen

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s} \quad (\mathrm{Re}(s) > 1)$$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \| \; e^{-s \log n}$$

(5.7) Satz (Möbius-Inversion). *Für $\chi, \widetilde{\chi} : \mathbb{N}_{>0} \to \mathbb{C}$ sind folgende Eigenschaften äquivalent:*

(i) $\chi(n) = \sum_{d|n} \widetilde{\chi}(d) \cdot 1$

(ii) $\widetilde{\chi}(n) = \sum_{d|n} \mu(d) \chi(\frac{n}{d})$,

Beweis. (Aus (i) kann $\widetilde{\chi}$ aus χ rekursiv berechnet werden.
Konvergenz der Dirichlet-Reihen sind nie ein Problem. Sei

$$\mathsf{X}(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \widetilde{\mathsf{X}}(s) = \sum_{n=1}^{1} \frac{\widetilde{\chi}(n)}{n^s}$$

$$\text{(i)} \underset{(5.4)}{\Leftrightarrow} \mathsf{X}(s) = \widetilde{\chi}(s) \cdot \zeta(s) \Leftrightarrow \widetilde{\mathsf{X}}(s) = \frac{1}{\zeta(s)} \chi(s) \underset{\substack{(5.6)(d) \\ (5.4)}}{\Longleftrightarrow} \text{(ii)}$$

■

Zusatz. gilt (i) oder (ii), so ist χ multiplikativ $\Leftrightarrow$ $\widetilde{\chi}$ multiplikativ.

Beweis. folgt aus (5.6)(d) und (5.4). ■

6 Das Dirichlet-Integral

(6.1) Definition. Sei $f : \mathbb{R}_{\geq 0} \to \mathbb{C}$ regel-integrierbar auf allen endlichen Teilintervallen. Dann

$$\boxed{F(s) = \int_0^\infty f(t)e^{-ts}\,dt} \qquad (s \text{ komplexe Variable})$$

das zu f gehörende Dirichlet-Integral.

Bemerkung. $F(s)$ heißt auch die **Laplace-Transformierte** von f.

(6.2) Lemma (Partielle Integration). *Sei $f : [a,b] \to \mathbb{C}$ Regelfunktion und $h : [a,b] \to \mathbb{C}$ stetig diffbar ($a < b$ reell). Dann:*

(a) $f_0(x) = \int_a^x f(t)\,dt$ ist differenzierbar auf $[a,b]$ mit Ausnahme von höchstens abzählbar vielen Ausnahmestellen, und dort

$$f_0' = f \quad \textit{(Stammfunktion)}$$

(b)

$$\int_a^b f \cdot h = [f_0 h]_a^b - \int_a^b f_0 h'$$

Beweis.

(a) Vergl. Königsberger 1, S. 197f.

(b)

$$(f_0 h') = f_0 h' + fh \quad (\text{„Produktregel“})$$

Also

$$[f_0 h]_a^b = \int_a^b f_0 h' + \int_a^b fh$$

■

(6.3) Satz (Das uneigentliche Integral). [3]

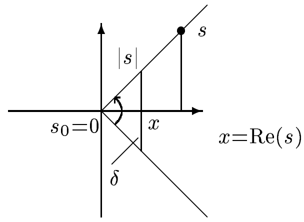
$$F(s) = \int_0^\infty f(t)e^{-ts}\,dt$$

existiere für $s = s_0$
Dann stellt $F(s)$ für $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ eine holomorphe Funktion dar (und Differentiation unter Integralzeichen).

[3] ($\triangleq$ (4.4))

Beweis. OBdA: $s_0 = 0$ [Ersetze s durch $s - s_0$; $t \mapsto f(t)e^{-ts_0}$ regel-integrierbar auf allen endlichen Teilintervallen $[0, \infty)$]
Dann nach Voraussetzung $\int_0^\infty f(t)\,dt$ konvergent. Betrachte

$$f_0(x) = \int_0^x f(t)\,dt \quad (x \geq 0)$$



Die Funktion $f_0 : [0, \infty \to \mathbb{C}$ ist eine „Stammfunktion" von f (nach (6.2) und beschränkt, etwa $|f_0(x)| \leq c$ für alle $x \geq 0$.
Seien $M > 0, \delta > 0$, betrachte

$$S = \underset{\text{(„Stumpfer Sektor")}}{S(M, \delta)} = \{s \in \mathbb{C} |\, \mathrm{Re}(s) \geq \delta, \frac{|s|}{\mathrm{Re}(s)} \leq M\}$$

[Jedes Kompaktum in $\mathrm{Re}(s) > 0$ liegt in einem solchen stumpfen Sektor!]
Sei $\varepsilon > 0$. Es gibt $N \in \mathbb{N}$ derart, dass $e^{-N\delta} < \varepsilon$ ist. Für $b > a \geq N$ gilt mit (6.2) für alle $s \in S(M, \delta)$

$$\begin{aligned}
\left| \int_a^b f(t)e^{-ts}\,dt \right| &= \left| \Big[f_0(t)e^{-ts} \Big]_a^b - s\int_a^b f_0(t)e^{-ts}\,dt \right| \\
&\leq \left| \big[f_0(t)e^{-ts}\big]_a^b \right| + |s| \int_a^b |f_0(t)||e^{-ts}|\,dt \\
&\leq c \cdot |e^{-b\,\mathrm{Re}(s)} - e^{-a\,\mathrm{Re}(s)}| + c \cdot |s| \int_a^b e^{-t\,\mathrm{Re}(s)}\,dt| \\
&\leq c\varepsilon + \frac{c|s|}{\mathrm{Re}(s)} \left| \big[e^{-t\,\mathrm{Re}(s)}\big]_a^b \right| \leq c\varepsilon(1 + M)
\end{aligned}$$

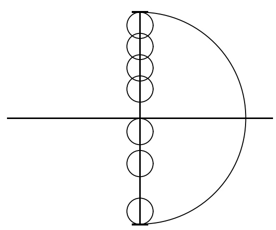
Wende (1.4) an. ■

(6.4) Hauptsatz (Tauber - Wiener - Ikehara). *Sei $f : [0, \infty) \to \mathbb{C}$* ***beschränkt*** *und regel-integrierbar auf allen endlichen Teilintervallen. Dann gilt*

(a) $F(s) = \int_0^\infty f(t)e^{-ts}\,dt$ ist holomorph (konvergent) für $\mathrm{Re}(s) > 0$.

(b) Ist $F(s)$ holomorph fortsetzbar über die Gerade $\mathrm{Re}(s) = 0$ *linear, so existiert das uneigentliche Integral*

$$\int_0^\infty f(t)\,dt.$$



Beweis. O.B.d.A: $|f(t)| \leq 1$ für alle $t > 0$.

(a) Sei $\delta > 0$; ist $\mathrm{Re}(s) = \delta$, so konvergiert

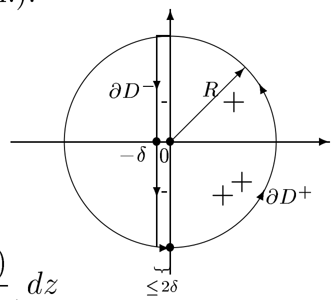
$$\int_0^\infty f(t)e^{-ts_0}\,dt$$

Nach (6.3) ist $F(s)$ holomorph für $\mathrm{Re}(s) > \delta$. Beh. folgr (δ klein)

(b) Sei $F(s)$ holomorph (erklärt) in jedem Punkt von $\mathrm{Re}(s) = 0$. Sei $b > 0$ (groß) und

$$F_b(s) = \int_0^b f(t)e^{-ts}\,dt;$$

F_b ganze Funktion (Differentiation unter Integralzeichen!).
Zeige: $\lim_{b\to\infty} F_b(0) = F(0)$ existiert.
Sei $\varepsilon > 0$ vorgegeben (ε klein; $\varepsilon < 1$). Setze $R = \frac{1}{\varepsilon}$.
Es gibt $\delta > 0$ derart, dass $F(s)$ holomorph (erklärt) in $D = \underbrace{S(\delta) = \{S \in \mathbb{C} \big| |s| \le R, \mathrm{Re}(s) \ge -\delta\}}_{\text{(Kompaktheitsargument!)}}$



Cauchy Integralformel:

$$F(0) - F_b(0) = \frac{1}{2\pi i}\int_{\partial D} \frac{F(z) - F_b(z)}{z}\underset{\uparrow(\cdot e^{bz})}{dz}$$

Positivbereich ($x = \mathrm{Re}(s) > 0$):

$$|F(s) - F_b(s)| = \left|\int_b^\infty f(t)e^{-ts}\,dt\right| \le |\int_b^\infty e^{-tx}\,dt| = \frac{e^{-bx}}{x}$$

Negativbereich ($x = \mathrm{Re}(s) < 0$):

$$|F_b(s)| = \left|\int_0^b f(t)e^{-ts}\,dt\right| \le \frac{e^{-bx} - 1}{|x|} \le \frac{e^{-bx}}{|x|}$$

Für $\underset{(\sqrt{z\bar{z}})}{|z|} = R$ gilt

$$\frac{1}{z} + \frac{z}{R^2} = \frac{\bar{z} + z}{R^2} = \frac{2\,\mathrm{Re}(z)}{R^2}$$

Cauchy Integralsatz:

$$\frac{1}{2\pi i}\int_{\partial D}(F(z) - F_b(z)) \cdot \frac{z}{R^2}\,dz = 0$$

Da $z \mapsto e^{bz}$ holomorph (und $e^{b0} = 1$) ist, gilt also:

$$\boxed{F(0) - F_b(0) = \frac{1}{2\pi i}\int_{\partial D}(F(z) - F_b(z))e^{bz}\big(\frac{1}{z} + \frac{z}{R^2}\big)\,dz}$$

Zerlege ∂D in den positiven Anteil ∂D^+ und den negativen ∂D^-. Es gilt

$$|F(0) - F_b(0)| \le I_1 + I_2,$$

wobei

$$\begin{aligned} I_1 = I_1(b,\delta) &= \left|\frac{1}{2\pi i}\int_{\partial D^+}(F(z) - F_b(z))e^{bz}\big(\frac{1}{z} + \frac{z}{R^2}\big)\,dz\right| \\ &\le \frac{1}{2\pi}\pi R \sup_{\substack{|z|=R \\ x=\mathrm{Re}(z)>0}} \underbrace{|F(z) - F_b(z)|}_{\le \frac{e^{-bz}}{x}} e^{bx} \underbrace{\left|\frac{1}{z} + \frac{z}{R^2}\right|}_{=\frac{2x}{R^2}} = \frac{1}{R} = \varepsilon \end{aligned}$$

(unabhängig von b und δ)

$$\begin{aligned}
|F(0)-F_b(0)| &\leq \varepsilon + \left|\frac{1}{2\pi i}\int_{\partial D}(F(z)-F_b(z))e^{bz}\big(\frac{1}{z}+\frac{z}{R^2}\big)\,dz\right| \\
&\leq \varepsilon + \left|\frac{1}{2\pi i}\int_{\partial D^-} F_b(z)e^{bz}\big(\frac{1}{z}+\frac{z}{R^2}\big)\,dz\right| \\
&\quad + \left|\frac{1}{2\pi i}\int_{\partial D^-} F(z)e^{bz}\big(\frac{1}{z}+\frac{z}{R^2}\big)\,dz\right|
\end{aligned}$$

Da der Integrand des „ersten“ Integrals holomorph im $\mathrm{Re}(z) < 0$ ist, gilt mit Cauchy:

$$\begin{aligned}
\left|\frac{1}{2\pi i}\int_{\partial D^-} F_b(z)e^{bz}\big(\frac{1}{z}+\frac{z}{R^2}\big)\,dz\right| &= \left|\frac{1}{2\pi i}\int\limits_{|z|=R,\mathrm{Re}(z)=x<0} F_b(z)e^{bz}\big(\frac{1}{z}+\frac{z}{R^2}\big)\,dz\right| \\
&\leq \frac{1}{2\pi i}\pi R \sup_{\substack{|z|=R\\ x=\mathrm{Re}(z)<0}} \underbrace{|F_b(z)|}_{\leq\frac{e^{-bx}}{|x|}}\underbrace{|e^{bz}|}_{e^{bx}}\cdot\underbrace{\big|\frac{1}{z}+\frac{z}{R^2}\big|}_{=\frac{2|x|}{R^2}} \\
&\leq \frac{1}{R}=\varepsilon
\end{aligned}$$

Zerlege ∂D^- in die beiden Kreisbögen $|z| = R, \delta \leq \mathrm{Re}(z) \leq 0$ und die Strecke $\mathrm{Re}(z) = -\delta, |z| \leq R$.
Sei

$$M_1 = \sup_{\substack{|z|=R\\ -\delta\leq\mathrm{Re}(z)\leq 0}} |F(z)|\cdot|e^{bz}|$$

(existenz, da F $\underset{\text{Kompaktheit}}{\text{holomorph}}$ / stetig auf D)

$$M_2 = \sup_{\substack{\mathrm{Re}(z)=-\delta\\ |z|\leq R}} |F(z)|\cdot\big|\frac{1}{z}+\frac{z}{R^2}\big|$$

(existenz, da F $\underset{\text{Kompaktheit}}{\text{holomorph}}$ / stetig auf D)

Damit:

$$\begin{aligned}
|F(0)-F_b(0)| &\leq 2\varepsilon + \frac{1}{2\pi}\mathbf{4\boldsymbol{\delta}}M_1\cdot \sup_{\substack{|z|=R\\ -\delta\leq\mathrm{Re}(z)=x\underset{(-)}{<}0}} \underbrace{\big|\frac{1}{z}+\frac{z}{R^2}\big|}_{=\frac{2|x|}{R^2}} \\
&\quad + \frac{1}{2\pi}\cdot\mathbf{2R}M_2 \sup_{\substack{x=\mathrm{Re}(z)=-\delta\\ (|z|\leq R)}} \underbrace{|e^{bx}|}_{=e^{bx}} \\
&\leq 2\varepsilon + \frac{4\delta^2 M_1}{\pi\cdot R^2} + \frac{M_2}{\pi}Re^{-b\delta}
\end{aligned}$$

Wähle $\delta > 0$ *so klein*, dass $\frac{4\delta^2 M_1}{\pi} < 1$ ist.
Dann $\frac{4\delta^2 M_1}{\pi R^2} < \frac{1}{R^2} = \varepsilon^2 < \varepsilon \quad (\varepsilon < 1)$
Wähle $b > 0$ *so groß* $[|e^{bz}|$ monoton fallend für $\mathrm{Re}(z) < 0, \mathrm{Re}(z) \to \infty]$, dass

$$\frac{M_2 e^{-b\delta}}{\pi} \leq \varepsilon^2$$

ist. Dann

$$\frac{M_2 e^{-b\delta}}{\pi} R \leq \frac{\varepsilon^2}{\varepsilon} = \varepsilon$$

Damit:

$$|F(0) - F_b(0)| \leq 4\varepsilon$$

■

7 Der Primzahlsatz

(7.1) Titelsatz (Hadamard, de la Vallée-Poussin,1896). [4]

$$\pi(x) \sim \frac{x}{\log(x)} \text{ \textit{für} } x \to \infty, \text{ \textit{d.h.} } \lim_{x\to\infty} \frac{\pi(x)\cdot\log(x)}{x} = 1$$

$$(\pi(x) = \sum_{\substack{p \leq x \\ (p \leq \mathbb{P})}} 1)$$

(7.2) Definition. Mangoldt-Funktion

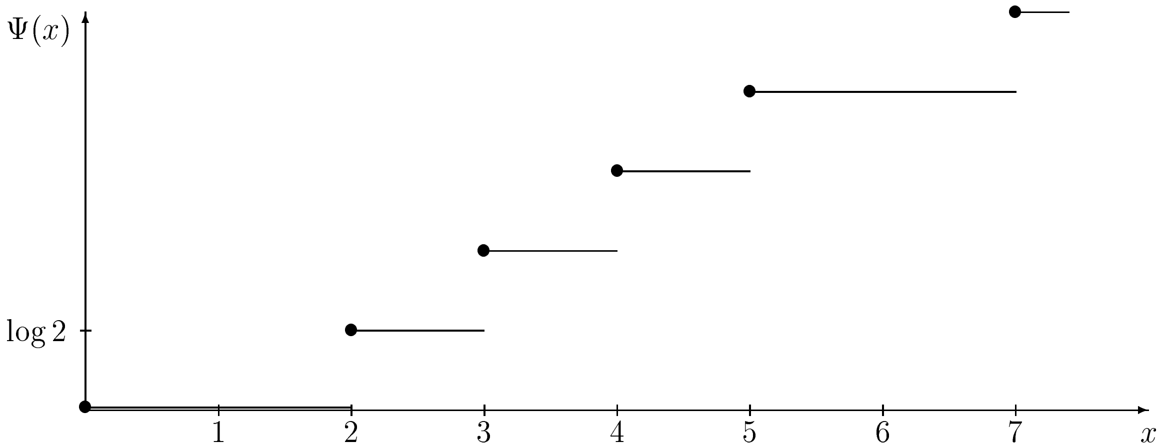
$$\Lambda : \mathbb{N}_{>0} \to \mathbb{C}, \Lambda(n) = \begin{cases} \log p & \text{, falls } n = p^k \text{ für } p \in \mathbb{P}, k \in \mathbb{N}_{>0} \\ 0 & \text{sonst} \end{cases}$$

Chebyshev[5]-Funktion

$$\Psi : [0, \infty) \to \mathbb{C}, \Psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{\substack{p^k \leq x \\ (p \in \mathbb{P}, k \in \mathbb{N}_{>0}}} \log p$$

[4] Hadamard: 1865-1963
de la Vallée-Poussin: ??
[5] (Tschebyscheff)

Diskussion.



$$\begin{aligned}
\Psi(x) &= 0 \text{ für } 0 \le x < 2 \\
\Psi(x) &= \log 2 \text{ für } 2 \le x < 3 \\
\Psi(x) &= \log 2 + \log 3 \text{ für } 3 \le x < 4 \\
\Psi(x) &= \underbrace{\log 2 + \log 3}_{\Psi(3)} + \log 2 \text{ für } 4 \le x < 5 \\
\Psi(x) &= \Psi(4) + \underbrace{\log 5}_{\Lambda(5)} \text{ für } 5 \le x < 7
\end{aligned}$$

Ergebnis. Ψ ist eine monoton wachsende Treppenfunktion
Ψ ist konstant auf allen Intervallen $(n, n-1], n \in \mathbb{N}_{>0}$
Es ist $\Psi(n) = \Psi(m-1) + \Lambda(n)$ für alle $n \in \mathbb{N}_{>0}$.

(7.3) Satz. *Für* $\mathrm{Re}(s) > 1$ *gilt:*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \cdot \int_1^{\infty} \Psi(t) t^{-s-1}\, dt$$

Beweis. Nach (1.6):

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} \quad (\mathrm{Re}(s) > 1)$$

logarithmieren:

$$\log \zeta(s) = \sum_{p \in \mathbb{P}} \log \left(\frac{1}{1 - \frac{1}{p^s}} \right) = \sum_{p \in \mathbb{P}} \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots \right)$$

Gliedweise Differentiation:

$$
\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds}\log\zeta(s) &= \sum_{p\in\mathbb{P}}\left(\frac{\log p}{p^s}+\frac{\log p}{p^{2s}}+\frac{\log p}{p^{3s}}+\cdots\right)\\
&= \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} \underset{(7.2)}{=} \sum_{n=1}^{\infty}\frac{\Psi(n)-\Psi(n-1)}{n^s}\\
&\underset{(7.2)}{=} \sum_{n=1}^{\infty}\left[\frac{\Psi(n)}{n^s}-\frac{\Psi(n)}{(n+1)^s}\right] = \sum_{n=1}^{\infty}\Psi(n)(+s)\int_n^{n+1}\frac{dt}{t^{s+1}}\\
&\underset{(7.2)}{=} \sum_{n=1}^{\infty}s\int_n^{n+1}\frac{\Psi(t)}{t^{s+1}}\,dt = s\int_1^{\infty}\Psi(t)t^{-s-1}\,dt
\end{aligned}
$$

■

Notation. Für $x\in\mathbb{R}$ sei
$[x]=\lfloor x\rfloor :=$ größte ganze Zahl $\leq x$ (Gauß-Klammer), (Abrundung)
$\lceil x\rceil :=$ kleinste ganze Zahl $\geq x$ (Aufrundung)
($\{x\}:=x-[x]\in[0,1)$ „fractional part“ von x)

(7.4) Lemma. *Für $x>e$ gilt*

$$
\frac{\Psi(x)}{x}\leq\frac{\pi(x)\cdot\log x}{x}\leq\frac{1}{\log x}+\frac{\Psi(x)}{x}\cdot\frac{\log x}{\log x-2\log\log x}
$$

Beweis.

(a)

$$
\Psi(x)=\sum_{p^k\leq n}\log p=\sum_{p\leq x}\left[\frac{\log x}{\log p}\right]\log p\leq\sum_{p\leq x}\frac{\log x}{\log p}\cdot\log p=\log x\cdot\underbrace{\sum_{p\leq x}1}_{=\pi(x)}
$$

(b) Für $1<y<x$ gilt:

$$
\begin{aligned}
\pi(x)=\pi(y)+\sum_{y<p\leq x}1 &\leq y+\sum_{y<p\leq x}\frac{\log p}{\log y}\leq y+\frac{1}{\log y}\sum_{p\leq x}\log p\\
&\leq y+\frac{\Psi(x)}{\log y}
\end{aligned}
$$

Setze

$$
y=\frac{x}{\log^2 x}=\frac{x}{(\log x)^2};\quad 1<y<x.
$$

Dann

$$
\pi(x)\leq\frac{x}{\log^2 x}+\frac{\Psi(x)}{\log x-2\log\log x}\qquad\Big|\cdot\frac{\log x}{x}
$$

■

(7.5) Folgerung. Folgende Eigenschaften sind äquivalent:

(i) $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ („Primzahlsatz")

(ii) $\lim_{x\to\infty} \frac{\Psi(x)}{x} = 1$ $[\Psi(x) \sim x$ für $x \to \infty]$

Beweis. $\lim_{x\to\infty} \frac{\log x}{\log x - 2\log\log x} = 1 \quad [\lim_{x\to\infty} \frac{1}{\log x} = 0]$ ■

(7.6) Lemma.

$$\prod_{p\leq x} p \leq 4^{[x]-1} \quad \textit{für } x \geq 1$$

Beweis. $x = 1$ und $x = 2$ in Ordnung. o.B.d.A.: $x = [x] = 2m+1$ ungerade (Primzahl); $m \in \mathbb{N}_{>0}$
Induktion:

$$\prod_{p\leq m+1} p \leq 4^m.$$

Damit

$$\prod_{p\leq x} p = \prod_{p\leq m+1} p \cdot \prod_{m+1<p\leq 2m+1} p \leq 4^m \cdot \underbrace{\binom{2m+1}{m+1}}_{=\frac{(2m+1)!}{(m+1)!m!} \overset{(!)}{\leq} \frac{2^{2m+1}}{2} = 2^{2m} = 4^m}$$

denn

$$\binom{2m+1}{m+1} = \binom{2m+1}{m} \text{ sind Summanden in } 2^{2m+1} = (1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k}$$

Also

$$\prod_{p\leq 2m+1} p \leq 4^m \cdot 4^m = 4^{2m}$$

■

(7.7) Lemma. *Es ist* $\Psi(x) = O(x)$*; twas genauer* $(0 \leq)\Psi(x) \leq (8\log 2)x, (x \in \mathbb{R}_{\geq 0})$

Beweis. o.B.d.A.: $x \geq 4$; (7.2).
Nach (7.6)

$$\prod_{p\leq x} p \leq 4^{[x]-1} \leq 4^x, \text{ also } \sum_{p\leq x} \log p \leq x \log 4$$

Entsprechend

$$\begin{aligned}
\sum_{p^2 \leq x} \log p &= \sum_{p \leq \sqrt{x}} \log p \leq \sqrt{x} \cdot \log 4, \\
\sum_{p^3 \leq x} \log p &= \sum_{p \leq x^{\frac{1}{3}}} \log p \leq x^{\frac{1}{3}} \log 4 \\
\Rightarrow \Psi(x) &\leq (x + x^{\frac{1}{2}} + x^{\frac{1}{3}} + \cdots + \quad) \log 4
\end{aligned}$$

Sei $n \in \mathbb{N}_{>0}$ mit $x \in (2^{n-1}, 2^n]$
Zeige:

$$\Psi(2^n) \leq 2^n (4 \cdot \log 2) \qquad \left[\Rightarrow \quad \frac{\Psi(x)}{x} \underset{7.2}{\leq} \frac{\Psi(2^n)}{2^{n-1}} \leq 8 \log 2 \right]$$

Es ist also nach oben:

$$\begin{aligned}
\Psi(2^n) &\leq (2^n + 2^{\frac{n}{2}} + 2^{\frac{n}{3}} + \cdots + +2^{\frac{n}{n}}) \log 4 \\
&\leq (2^n + \underbrace{(n-1) 2^{\frac{n}{2}}}_{\leq 2^n}) \underset{\text{(Induktion)}}{\log 4} \leq 2^{n+1} \log 4 = 2^n (4 \log 2)
\end{aligned}$$

■

(7.8) Lemma. *Existiert (konvergiert)*

$$\int_1^\infty \frac{\Psi(x) - x}{x^2} \, dx, \quad \textit{so gilt} \ \lim_{x \to \infty} \frac{\Psi(x)}{x} = 1$$

Beweis. Nach (7.7) existieren

$$\left.\begin{aligned}
c_1 &= \limsup_{x \to \infty} \tfrac{\Psi(x)}{x} = \lim_{n \to \infty} \left(\sup_{x \geq n} \tfrac{\Psi(x)}{x} \right) \\
c_2 &= \liminf_{x \to \infty} \tfrac{\Psi(x)}{x} = \lim_{n \to \infty} \left(\inf_{x \geq n} \tfrac{\Psi(x)}{x} \right)
\end{aligned}\right\} \begin{matrix} (!!) \\ \text{Analysis I} \end{matrix}$$

Es gilt $0 \underset{\neq 0}{<} c_2 \leq c_1$, und es gilt

$$\lim_{x \to \infty} \frac{\Psi(x)}{x} = 1 \text{ (existiert)} \ \Leftrightarrow c_1 = 1 = c_2$$

Annahme: $c_1 > 1$; etwa $c_1 = 1 + 2\delta, \delta > 0$.
Setze $a = \frac{1+2\delta}{1+\delta}$ (> 1) und $\varepsilon = \delta \log a$
Nach Voraussetzung gibt es $N \in \mathbb{N}$ derart, dass

$$\left| \int_y^{y'} \frac{\Psi(x) - x}{x^2} \, dx \right| < \varepsilon \text{ für alle } y' \geq y \geq N$$

Andererseits gibt es $y > N$ mit $\Psi(y) \geq c, y = (1+2\delta)y$.
Für

$$y \leq x \leq ay \text{ gilt } \Psi(x) \geq \Psi(y) \geq ay(1+\delta) \geq x(1+\delta).$$

Damit

$$(0 \leq) \int_y^{ay} \frac{\Psi(x)-x}{x^2}\,dx \geq \int_y^{ay} \frac{\delta}{x}\,dx = \delta(\log ay - \log y) = \varepsilon$$

Widerspruch.
Annahme: $c_2 < 1$; etwa $c_2 = 1-2\delta, 0 < \delta < \frac{1}{2}$.
Setze $a = \frac{1-2\delta}{1-\delta} \quad (0 < a < 1); \quad \varepsilon = -\delta \log a \quad (> 0)$
Nach Voraussetzung gibt es $N \in \mathbb{N}$ derart, dass

$$\left| \int_y^{\prime y} \frac{\Psi(x)-x}{x^2}\,dx \right| < \varepsilon \text{ für alle } y' \geq y \geq N$$

Andererseits gibt es $y \in \mathbb{R}$ mit $ay \geq N$ und $\Psi(y) \leq (1-2\delta)y$ ist.
Für

$$ay \leq x \leq y \text{ gilt } \Psi(x) \leq \Psi(y) \geq ay(1-\delta) \leq x(1-\delta),$$

somit

$$\int_{ay}^{y} \frac{\Psi(x)-x}{x^2}\,dx \leq -\int_{ay}^{y} \frac{\delta}{x}\,dx = \delta \log a = -\varepsilon < 0$$

■

(7.9) Beweis des Primzahlsatzes. Nach (7.8) und (7.5) genügt es zu zeigen:

$$\int_1^\infty \frac{\Psi(x)-x}{x^2}\,dx$$

konvergiert.
Betrachte

$$f : [0,\infty) \to \mathbb{C}, \quad f(t) = \frac{\Psi(e^t)}{e^t} - 1.$$

Nach (7.7) ist f beschränkt $(-1 \leq f(t) \leq 8\log 2 - 1)$ und f ist regel-integrierbar auf allen endlichen Teilintervallen von $[0,\infty)$. Nach (6.4)(a) ist

$$F(s) = \int_0^\infty f(t) e^{-ts}\,dt$$

holomorph für $ReT(s) > 0$.
Substitution:

$$x = e^t; \quad dx = e^t\,dt = x\,dt \quad [t = 0 \Rightarrow x = 1]$$

$$\begin{aligned}
F(s) &= \int_1^\infty \left(\frac{\Psi(x)}{x}-1\right)x^{-s}\frac{dx}{x} = \int_1^\infty \left(\frac{\Psi(x)-x}{x^2}\right)x^{-s}\,dx \;(\mathrm{Re}(s)>0)\\
&= \int_1^\infty \Psi(x)\cdot x^{-s-2}\,dx - \int_1^\infty x^{-s-1}\,dx\\
&= \frac{1}{s+1}(s+1)\int_1^\infty \Psi(x)x^{-(s+1)-1}\,dx + \frac{1}{s}[x^{-s}]_1^\infty\\
&\underset{7.3}{=} \frac{1}{s+1}\,\frac{-\zeta'(s+1)}{\zeta(s+1)} - \frac{1}{s}\\
&= \frac{-1}{s+1}\left[\frac{\zeta'(s+1)}{\zeta(s+1)} + \frac{s+1}{s}\right]
\end{aligned}$$

Verhalten von $F(s)$ für $\mathrm{Re}(s) = 0$:
s=0: $\zeta(s+1)$ hat in $s = 0$ nach (1.7) ein einfachen Pol mit Residuum 1.
Also hat

$$\frac{\zeta'(s+1)}{\zeta(s+1)}$$

in $s = 0$ einen einfachen Pol mit Residuum 1 (Übung 11), also

$$\frac{\zeta'(s+1)}{\zeta(s+1)} \sim \frac{-1}{s}$$

für $s \to 0$; somit ist $F(s)$ holomorph (fortsetzbar) in $s = 0$.
$\mathrm{Re}(s) = 0, s \neq 0$: Nach (1.10) gilt dort

$$\zeta(s+1) \neq 0$$

Also $F(s)$ holomorph (fortsetzbar) auf die Gerade

$$\underset{(6.4)(b)}{\Longrightarrow} \quad F(0) = \int_0^\infty f(t)\,dt = \int_1 \infty \frac{\Psi(x)-x}{x^2}\,dx$$

existiert.

8 Bertrands Postulat

(8.1) „Satz“. *Für die Anzahl der Primzahlen zwischen $n \in \mathbb{N}_{>0}$ (echt) und $2n$ gilt näherungsweise*

$$|\mathbb{P} \cap (n, 2n]| \approx \frac{n}{\log n}$$

Beweis.

$$\begin{aligned}
|\mathbb{P} \cap (n, 2n]| = \pi(2n) - \pi(n) \underset{(7.1)}{\sim} \frac{2n}{\log 2n} - \frac{n}{\log n} &= \frac{2n\log n - n\log n - n\log 2}{\log n(\log n + \log 2)}\\
&= \frac{n(\log n - \log 2)}{\log n(\log n + \log 2)} \approx \frac{n}{\log n}
\end{aligned}$$

■

(8.2) Bertrands Postulat (Bertrand, 1845).

$$\mathbb{P} \cap (n, 2n] \neq \emptyset \text{ für alle } n \leq 3\,000\,000$$

(richtig); gilt immer ?!
Chebyshev (1850) $\mathbb{P} \cap (n, 2n] \neq \emptyset$ *für alle* $n \in \mathbb{N}_{>0}$

Beweis. (Erdös, 1932)
1. Schritt: Primzahlen

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

Für diese 14 Primzahlen p_i gilt

$$p_{i+1} < 2p_i$$

Daher gilt der Satz für $n \leq 4000$
2. Schritt: Betrachte die Primfaktorzerlegung von

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

■

(8.3) Lemma.

$$\binom{2n}{n} \geq \frac{4^n}{2n} \quad (n \in \mathbb{N}_{>0})$$

Beweis. Für $1 \leq k \leq 2n$ gilt

$$\binom{2n}{k} = \binom{2n}{k-1} \cdot \frac{2n-k+1}{k}.$$

Also

$$\binom{2n}{0} = 1 < \binom{2n}{1} < \cdots < \binom{2n}{n-1} < \binom{2n}{n} > \binom{2n}{n+1} > \cdots > \binom{2n}{2n} = 1$$

Folglich

$$\begin{aligned} \binom{2n}{n} &\geq \frac{1}{2n}\left[\left(\binom{2n}{0} + \binom{2n}{2n}\right) + \binom{2n}{1} + \cdots + \binom{2n}{2n-1}\right] \\ &= \frac{1}{2n}(1+1)^{2n} = \frac{2^{2n}}{2n} \end{aligned}$$

■

Notation. Für $n \in \mathbb{N}_{>0}, p \in \mathbb{P}$ in

$$\Psi_p(a) := \max\{r \in \mathbb{N} \big| p^r \big| n\}$$

$(v_p(nm) = v_p(n) + v_p(m))$

(8.4) Lemma. *Legendre*

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \quad (n \in \mathbb{N}_{>0}, p \in \mathbb{P})$$

(Summation über alle $k \in \mathbb{N}_{>0}$ mit $p^k \leq n$)

Beweis. Genau $\lfloor \frac{n}{p} \rfloor$ viele Faktoren $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ von $n!$ sind durch p teilbar.
Genau $\lfloor \frac{n}{p^2} \rfloor$ viele Faktoren $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ von $n!$ sind durch p^2 teilbar.

$$\Rightarrow v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

■

(8.5) Lemma.

$$v_p\left(\binom{2n}{n}\right) \leq \log_p 2n \quad (n \in \mathbb{N}_{>0}, p \in \mathbb{P});$$

Mit anderen Worten:

$$\text{Ist } p^r \Big| \binom{2n}{n}, \text{ so ist } p^r \leq 2m.$$

Beweis. Nach (8.4) gilt:

$$\begin{aligned} v_p\left(\binom{2n}{n}\right) &= v_p\big((2n)!\big) - 2v_p(n!) \\ &= \sum_{k \geq 1} \left([\frac{2n}{p^k}] - 2[\frac{n}{p^k}] \right) \leq \sum_{\substack{k \geq 1 \\ p^k \leq 2n}} 1 \leq [log_p 2n] \end{aligned}$$

$$\text{Es ist } \mathbb{N} \ni [\frac{2n}{p^k}] - 2[\frac{n}{p^k}] \quad < \quad \frac{2n}{p^k} - 2\big(\frac{n}{p^k} - 1\big) = 2 \text{ für alle } k \in \mathbb{N}_{>0}$$

■

Zusätze. *(a) Ist $p > \sqrt{2n}$, so ist $p^2 \nmid \binom{2n}{n}$*

(b) Ist $\frac{2n}{3} < p \leq n$ und $n \geq 3$, so ist $p \nmid \binom{2n}{n}$

Beweis. Wegen $3p > 2n \geq 6$ ist $p > 2$, also p und $2p$ einzige natürliche Zahlen $\leq 2n$, die durch p teilbar sind, d.h.

$$\left.\begin{array}{r} v_p\Big((2n)!\Big) \leq 2 \\ \text{wegen } p \leq n \text{ gilt andererseits } v_p\Big((n!)^2\Big) \geq 2. \end{array}\right\} \Rightarrow v_p\left(\binom{2n}{n}\right) = 0$$

■

(8.6) Beweis des Postulats.
Annahme: $\mathbb{P} \cap (n, 2n] = \emptyset$ für ein $n \in \mathbb{N}_{>0}$
Dann nach (8.2) [Schritt 1] $n > 4\,000$. Mit (8.3),(8.5) erhalten wir:

$$\frac{4^n}{2n} \leq \binom{2n}{n} = \prod_{p\in\mathbb{P}} p^{v_p\left(\binom{2n}{n}\right)} \leq \underbrace{\prod_{p\leq\sqrt{2n}} 2n}_{\leq(2n)^{\sqrt{2n}}} \cdot \underbrace{\prod_{\sqrt{2n}<p\leq\frac{2n}{3}} p^1}_{\leq\prod_{p\leq\frac{2n}{3}} p} \cdot \underbrace{\prod_{\frac{2n}{3}<p\leq n} p^{v_p\left(\binom{2n}{n}\right)}}_{=1 \text{ nach Zusatz (b)}} \cdot \underbrace{\prod_{n<p\leq 2n} p^{v_p\left(\binom{2n}{n}\right)}}_{=1 \text{ nach Annahme}}$$

Nach (7.6)

$$\prod_{p\leq\frac{2n}{3}} p \leq 4^{\frac{2n}{3}}.$$

Damit

$$4^n \leq (2n)^{\sqrt{2n}+1} \cdot 4^{\frac{2n}{3}}, \text{ oder } 2^{\frac{2n}{3}} = 4^{\frac{n}{3}} \leq (2n)^{1+\sqrt{2n}}$$

Für $m \geq 2$ gilt $1 + m \leq 2^m$, also

$$(2n \leq)\big([\sqrt[6]{2n}] + 1\big)^6 \leq \big(2^{[\sqrt[6]{2n}]}\big)^6 \leq 2^{6\sqrt[6]{2n}}.$$

Damit

$$2^{\frac{2n}{3}} \leq 2^{6\cdot\sqrt[6]{2n}(1+\sqrt{2n})}, \text{ oder } 2^{2n} \leq 2^{\sqrt[6]{2n}(18+18\sqrt{2n})}$$

Wegen $18 \leq 2 \cdot \sqrt{2n}$ (für $n \geq 50$) folgt

$$2^{2n} \leq 2^{20(2n)^{\frac{2}{3}}}, \text{ oder } 2n \leq 20(2n)^{\frac{2}{3}}, \quad (2n)^{\frac{1}{3}} \leq 20$$

$2n \leq 8\,000$, $n \leq 4\,000$ (Widerspruch)

9 Fourier - Analyse

Jean-Baptiste-Joseph de Fourier (1768-1830)
Laurent Schwartz (1915-2002)

(9.1) Definition. Sei $S = S(\mathbb{R}, \mathbb{C})$ die Menge (Raum) aller C^∞-Funktionen $f : \mathbb{R} \to \mathbb{C}$, die **stark abfallend** sind im folgenden Sinne

$$\lim_{x\to\infty} |x|^n |f^{(k)}(x)| = 0 \text{ für alle } n, k \in \mathbb{N}.$$

S heißt der Schwartz-Raum.

Beispiel:.

$$f(x) = e^{-x^2} \quad (x \in \mathbb{R})$$

Für $f \in S$ definiere die **Fourier-Transformierte** $\widehat{f} : \mathbb{R} \to \mathbb{C}$ mit

$$\boxed{\widehat{f}(x) = \int_{-\infty}^{\infty} f(t) e^{-2\pi i x t}\, dt}$$

(9.2) Satz. *Ist $f \in S = S(\mathbb{R}, \mathbb{C})$, so auch f' $(f'', \dots f^{(k)})$ und $\widehat{f}$, und es gilt*

(a) $$\widehat{f}'(x) = -2\pi i \int_{-\infty}^{\infty} t \cdot f(t) e^{-2\pi i x t}\, dt \text{ („Differentiation unter Integralzeichen“)}$$

(b) $$\widehat{f'}(x) = 2\pi i x \cdot \widehat{f}(x), \quad x \in \mathbb{R}$$

Beweis. Klar: $f' \in S$. Es ist

$$\lim_{|x|\to\infty} (1 + x^2)|f(x)| = 0, \text{ also } |f(x)| \leq \frac{c}{1 + x^2}$$

für konstante c und

$$|\widehat{f}(x)| \leq \int_{-\infty}^{\infty} |f(t)| \underbrace{|e^{-2\pi i x t}|}_{=1}\, dt \leq \int_{-\infty}^{\infty} \frac{c}{1 + t^2}\, dt = c \cdot \pi$$

Wir haben absolute (kompakte) konvergenz für das uneigentliche Integral, es gilt (a).
Ad(b)

$$\widehat{f'}(x) = \int_{-\infty}^{\infty} f'(t) e^{-2\pi i x t}\, dt \underset{\substack{\text{Partielle}\\\text{Integration}}}{=} \underbrace{\left[f(t) \cdot e^{-2\pi i x t}\right]_{t=-\infty}^{\infty}}_{=0} + \underbrace{2\pi i x \int_{-\infty}^{\infty} f(t) e^{-2\pi i x t}\, dt}_{=2\pi i x \cdot \widehat{f}(x)}$$

Analog: $\widehat{f''}(x) = 2\pi i x \cdot \widehat{f'}(x) = 2\pi i x^2 \widehat{f}(x)$
$\widehat{f^{(n)}}(x) = (2\pi i x)^n \widehat{f}(x), \quad n \in \mathbb{N}$
Also: $|\widehat{f}(x)| = \frac{1}{(2\pi x)^n} |\widehat{f^{(n)}}(x)|$ für alle $n \in \mathbb{N}, x \in \mathbb{R}, x \neq 0$
Wegen $f^{(n)} \in S$ ist $\widehat{f^{(n)}}$ beschränkt (auf $\mathbb{R}$), somit

$$\lim_{|x|\to\infty} |x|^m |\widehat{f}(x)| = 0 \text{ für alle } m \in \mathbb{N}$$

Erhalte: $\widehat{f} \in S$ ∎

Anmerkung. $S(\mathbb{R},\mathbb{C})$ ist ein komplexer Vektorraum (Algebra (Ring)) bezüglich punktweiser Verknüpfungen, und $f \mapsto \widehat{f}$ ist ein linearer Operator auf diesem Schwartzraum auf $S(\mathbb{R},\mathbb{C})$. Es gilt für $f, g \in S(\mathbb{R},\mathbb{C})$

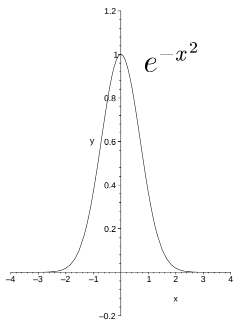
$$\widehat{f} \cdot \widehat{g} = \widehat{f \star g},$$

wobei die **Faltung**

$$(f \star g)(x) = \int_{-\infty}^{\infty} f(x-t) \cdot g(t)\, dt \quad \text{(ohne Beweis)}$$

(9.3) Beispiel. Sei $a > 0$ reell und

$$f(x) = f_a(x) = e^{-\frac{\pi}{a}x^2} \quad (x \in \mathbb{R})$$



Behauptung: $f \in S(\mathbb{R},\mathbb{C})$ und $\widehat{f}(x) = \sqrt{a} \cdot e^{-\pi a x^2}$
(Insbesondere: $\widehat{f_1} = f_1$)

Beweis. Klar: $f \in S(\mathbb{R},\mathbb{C})$
Es gilt

$$\widehat{f}'(x) \underset{(9.2)}{=} -2\pi i \int_{-\infty}^{\infty} t e^{-\frac{\pi}{a}t^2} e^{-2\pi i x t}\, dt$$

Partielle Integration:

$$u(t) = e^{-2\pi i x t};\quad u'(t) = -2\pi i x e^{-2\pi i x t};\quad v'(t) = -2\pi i t e^{-\frac{\pi}{a}t^2};\quad v(t) = i \cdot a e^{-\frac{\pi}{a}t^2}$$

$$\begin{aligned}
\widehat{f}'(x) \quad & \underset{(9.2)}{=} \quad -2\pi i \int_{-\infty}^{\infty} t e^{-\frac{\pi}{a}t^2} e^{-2\pi i x t}\, dt \\
& \underset{\text{(Part. Int.)}}{=} \quad \left[i \cdot a e^{-\frac{\pi}{a}t^2} e^{-2\pi i x t}\right]_t^{\infty} \\
& \qquad +2\pi i x t i \cdot a) \int_{-\infty}^{\infty} e^{-\frac{\pi}{a}t^2} \cdot e^{-2\pi i x t}\, dt \\
& = \quad -2\pi a x \widehat{f}(x)
\end{aligned}$$

Also

$$\frac{d}{dx} \log \widehat{f}(x) = -2\pi a, \quad \log \widehat{f}(x) = -\pi^a x^2 + c_0 \text{ mit Konstanten } c_0$$

Damit

$$\widehat{f}(x) = c \cdot e^{-\pi a x^2} \quad , \quad c = e^{c_0}$$

Es gilt

$$c = \widehat{f}(0) = \int_{-\infty}^{\infty} e^{-\frac{\pi}{a}t^2}\, dt = \frac{\sqrt{a}}{\sqrt{\pi}} \underbrace{\int_{-\infty}^{\infty} e^{-u^2}\, du}_{(2)=\Gamma(\frac{1}{2})=\sqrt{\pi}} = \sqrt{a}$$

mit

$$\boxed{u = \sqrt{\frac{\pi}{a}}t} \quad \boxed{u^2 = \frac{\pi}{a}t^2}$$

■

(9.4) Definition. Sei $f : \mathbb{R} \to \mathbb{C}$ stetig und 1-periodisch ($\mathbb{Z}$-periodisch), d.h.

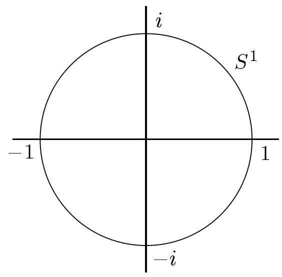
$$f(x+1) = f(x) \quad \text{für alle} x \in \mathbb{R}$$

Dann sind die Fourier-Koeffizienten von f für jedes $n \in \mathbb{Z}$

$$a_n = \int_0^1 f(t)e^{2\pi int}\,dt \quad (x \in \mathbb{R})$$

Fourier-Reihe von f:

$$\sum_{n\in\mathbb{Z}} a_n e^{2\pi inx} \quad (x \in \mathbb{R})$$



Bemerkungen.

(a) f induziert (stetige) Abbildung $\mathbb{R}/\mathbb{Z} \to \mathcal{P}$
Es ist $\mathbb{R}/\mathbb{Z} = S^1 = \{z \in \mathbb{C} \big| |z| = 1\}$ via $t \mapsto e^{2\pi it}$

(b) Für $k, l \in \mathbb{Z}$ gilt:

$$\int_0^1 e^{2\pi ikt} \cdot e^{-2\pi ilt}\,dt = \begin{cases} 1 & , k = l \\ 0 & \text{sonst} \end{cases}$$

(9.5) Satz (Weierstraß). *Jede 1-periodische stetige Funktion $f : \mathbb{R} \to \mathbb{C}$ ist gleichmäßiger Limes von trigonometrischen Polynom*

$$T(x) = \sum_{k=-n}^{n} c_k e^{2\pi ikt} \quad (c_k \in \mathbb{C}, n \in \mathbb{N})$$

Beweis. Es ist $f(x) = f_0(e^{2\pi ix})$ mit (eindeutig bestimmter) stetiger Funktion
$f_0 : S^1 \to \mathbb{C}$.
f_0 ist gleichmäßiger Limes komplexer Polynome

$$p(x) = \sum_{k=0}^{n} a_k z^b$$

und der konjugierten.

$$(\text{Es gilt } \overline{p(e^{2\pi ix})} = \sum_{k=0}^{n} \overline{a_k} e^{-2\pi ikx}.)$$

■

(9.6) Satz. *Ist f eine 1-periodische C^∞-Funktion, so konvergiert die Fourierreihe von f $\underset{(kompakt)}{\text{normal}}$ gegen f (und Entsprechendes für die Ableitungen; gleidweise Differentiation)*

Beweis. (a) **Konvergenz der Fourier-Reihe** (plus Ableitungen)

$$\begin{aligned}
\text{Fourier-Koeffizient von } f\text{: } a_n &= \int_0^1 f(f)e^{-2\pi int}\,dt \quad (n \in \mathbb{Z}) \\
\text{Fourier-Koeffizient von } f'\text{: } b_n &= \int_0^1 f'(t)e^{-2\pi int}\,dt \quad (n \in \mathbb{Z}) \\
&= \underbrace{\left[f(t)e^{-2\pi int}\right]_{t=0}^1}_{=0} + 2\pi in \underbrace{\int_0^1 f(f)e^{-2\pi int}\,dt}_{=a_n} \\
&= 2\pi ina_n \\
\text{Fourier-Koeffizient von } f''\text{: } c_n &= \int_0^1 f''(t)e^{-2\pi int}\,dt \quad (n \in \mathbb{Z}) \\
&\underset{(\text{analog})}{=} 2\pi inb_n = (2\pi in)^2 \cdot a_n \\
\cdots\cdots &
\end{aligned}$$

Folglich

$$|a_n| = \frac{|c_n|}{4\pi^2 n^2}, \text{ und } |c_n| \leq \int_0^1 |f''(t)|\,dt = \text{ Konstante}$$

Also konvergiert die Fourierrreihe

$$\sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}$$

von f normal (Analoges für die Anleitungen !)

(b) **Gleichheit:**
Setze

$$\widetilde{f}(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx} \quad (x \in \mathbb{R};\ \text{Forurierreihe von } f)$$

$\widetilde{f}$ 1-periodische C^∞ - Funktion (gleidweise Differentiation)
Fourier-Koeffizienten von $\widetilde{f}$:

$$\begin{aligned}
\widetilde{a}_k &= \int_0^1 \widetilde{f}(t)e^{-2\pi ikt}\,dt \quad (k \in \mathbb{Z}) \\
&= \sum_{n\in\mathbb{Z}} a_n \left(\int_0^1 e^{2\pi int}e^{-2\pi ikt}\,dt \right) = a_k
\end{aligned}$$

Betrachte $g = f - \widetilde{f}$; g ist 1-periodische C^∞-Funktion, der Fourier-Koeffizienten alle gleich Null sind.

Let $\varepsilon > 0$. Nach (9.5) gibt es

$$T(x) = \sum_{k=-n}^{n} c_k e^{2\pi ikx} \quad (c_k \in \mathbb{C}, n \in \mathbb{N})$$

mit

$$|g(x) - T(x)| < \varepsilon \text{ für alle } x \in \mathbb{R}$$

Es gilt

$$\int_0^1 g(t)\overline{T(t)}\,dt = \sum_{k=-n}^{n} \overline{c_k} \int_0^1 g(t) e^{-2\pi ikt}\,dt = 0.$$

Damit

$$\int_0^1 |g(t)|^2\,dt = \int_0^1 |g(t)| \cdot \big|\big(\underbrace{\overline{g(t)} - \overline{T(t)}}_{<\varepsilon}\big)\big|\,dt < \varepsilon \cdot \underbrace{\int_0^1 |g(t)|\,dt}_{=\text{ Konstante}}$$

$$\underset{g \text{ stetig}}{\Longrightarrow} \quad g = 0, \quad \widetilde{f} = f$$

■

(9.7) Poisson - Summation[6]. *Für* $f \in S(\mathbb{R}, \mathbb{C})$ *gilt*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)$$

Beweis. Setze

$$g(x) = \sum_{n\in\mathbb{Z}} f(x+n) \ : \quad x \in \mathbb{R}$$

Offenbar g eine 1-periodische C^∞-Funktion (gliedweise Differentiation; $f, \widehat{f} \in S(\mathbb{R}, \mathbb{C})$)
Nach (9.6) gilt

$$g(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx} \quad \text{(Fourierreihe von } g\text{)}$$

Also

$$g(0) = \sum_{n\in\mathbb{Z}} a_n = \sum_{n\in\mathbb{Z}} f(n)$$

andererseits: $(n \in \mathbb{Z})$

$$\begin{aligned} a_n = \int_0^1 g(x) e^{-2\pi inx}\,dx &= \sum_{k\in\mathbb{Z}} \int_0^1 f(x+k) e^{-2\pi in(x+k)}\,dx \\ &= \int_{-\infty}^{\infty} f(t) e^{-2\pi int}\,dt = \widehat{f}(n) \end{aligned}$$

■

[6] oder Summierung

10 Funktionalgleichung der Zeta - Funktion

(10.1) Definition. Reelle Jakobische Theta - Funktion Θ $\Theta : (0, \infty) \to \mathbb{R}$

$$\Theta(x) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x}$$

Behauptung. Θ *ist* C^∞*-Funktion*

Beweis. Sei $\delta > 0$. Dann

$$|e^{-\pi n^2 x}| \le e^{-\pi n^2 \delta}$$

für alle $x \ge \delta$. Für alle $k \in \mathbb{N}$ konvergiert die Reihe
(absolut)

$$\sum_{n \in \mathbb{Z}} (\pi n^2)^k e^{-\pi n^2 \delta}$$

[$\Rightarrow$ Behauptung]
$\Big[\sum_{n \in \mathbb{Z}} e^{(\log \pi n^2)k - \pi n^2 \delta} = \sum_{n \in \mathbb{Z}} e^{k \log \pi + 2k \log n - \pi n^2 \delta}$; Es gibt $N \in \mathbb{N}$, so dass $2k \log n - \pi n^2 \delta \le -1$ ist für alle $n \ge N$. Quotientenkriterium! ($q = e^{-1} < 1$).$\Big]$ ∎

(10.2) Satz. *Die Funktion* Θ *erfüllt die Funktionalgleichung*

$$\boxed{\Theta(\frac{1}{x}) = \sqrt{x} \cdot \Theta(x)}$$

Beweis. Sei $a > 0$ fest; sei $f(x) = f_a(x) = e^{-\frac{\pi}{a} x^2}$.
Nach (9.3) ist $f \in S(\mathbb{R}, \mathbb{C})$ mit $\widehat{f}(x) = \sqrt{a}\, e^{-\pi a x^2}$. Folglich mit Poisson (9.7):

$$\Theta(\frac{1}{a}) = \sum_{n \in \mathbb{Z}} e^{-\frac{\pi}{a} n^2} = \sum_{n \in \mathbb{Z}} f(n) \underset{\uparrow}{=} \sum_{n \in \mathbb{Z}} \widehat{f}(n) = \sqrt{a} \sum_{n \in \mathbb{Z}} e^{-\pi a n^2} = \sqrt{a}\, \Theta(a)$$

∎

(10.3) Definition. „Vollständige Riemannsche Zeta - Funktion“:

$$Z(s) := \pi^{-\frac{s}{2}} \Gamma\Big(\frac{s}{2}\Big) \zeta(s) \quad (s \in \mathbb{C})$$

Diskussion. $\Gamma({}^s/_2)$ hat (nur einfache) Polstellen für $s = -2n, n \in \mathbb{N}$ (2.4)
$\zeta(s)$ hat (einfache) Nullstellen für $s = -2n, n \in \mathbb{N}_{>0}$ (3.5)
$\zeta(s)$ hat nur (einfache) Polstelle für $s = 1$ (1.7)

Folglich. $Z(s)$ ist holomorph bis auf die Stellen $s = 1, s = 0$ wo einfache Pole vorliegen. (Residuen?)

Bemerkung. Man betrachtet auch oft die sogenannte **Xi-Funktion**

$$\boxed{\xi(s) = \frac{s}{2}(s-1)Z(s)}$$

ξ ist eine ganze Funktion (Übung 34)

(10.4) Hauptsatz (B. Riemann).

$$Z(s) = Z(1-s)$$

Beweis. Wir zeigen (direkt) die Existenz einer ganzen Funktion $I(s)$ mit $I(s) = I(1-s)$, so dass

$$Z(s) = \frac{1}{s-1} - \frac{1}{s} + I(s)$$

Setze

$$\Theta_0(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t} \quad (t > 0) \quad \text{also } \Theta_0(t) = \frac{1}{2}(\Theta(t) - 1)$$

Es gilt nach (10.2)

$$\Theta_0\big(\frac{1}{t}\big) = \frac{1}{2}(\Theta\big(\frac{1}{t}\big) - 1) = \frac{1}{2}(\sqrt{t}\,\Theta(t) - 1) = \frac{1}{2}(2\sqrt{t}\,\Theta_0(t) + \sqrt{t} - 1) = \sqrt{t}\,\Theta_0(t) + \frac{\sqrt{t}}{2} - \frac{1}{2}$$

Für $\mathrm{Re}(s) > 0$ und $n \in \mathbb{N}_{>0}$ gilt nach (2.7):

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\big(\frac{s}{2}\big)\frac{1}{n^2} &= \int_0^{\infty} \frac{e^{-t}t^{\frac{s}{2}-1}}{(\pi n^2)^{\frac{s}{2}}}\,dt = \int_0^{\infty} \frac{e^{-\pi n^2 u}(\pi n^2 u)^{\frac{s}{2}-1}}{(\pi n^2)^{\frac{s}{2}}} \cdot \pi n^2\,du \qquad u = \tfrac{t}{\pi n^2} \\
&= \int_0^{\infty} e^{-\pi n^2 u} u^{\frac{s}{2}-1}\,du
\end{aligned}$$

Für $\mathrm{Re}(s) > 1$ gilt also:

$$Z(s) = \pi^{-\frac{s}{2}}\Gamma\big(\frac{s}{2}\big)\sum_{n=1}^{\infty}\frac{1}{n^2} = \int_0^{\infty} \Theta_0(t)t^{\frac{s}{2}-1}\,dt$$

Es gilt:

$$\begin{aligned}
\int_0^1 \Theta_0(t)t^{\frac{s}{2}-1}\,dt &= -\int_{\infty}^1 \Theta_0\big(\frac{1}{u}\big)u^{-\frac{s}{2}+1}\frac{du}{u^2} \qquad t=\tfrac{1}{u} \quad dt=-\tfrac{du}{u^2} \\
&= \int_1^{\infty}\left(u^{\frac{1}{2}}\Theta_0(u) + \frac{u^{\frac{1}{2}}}{2} - \frac{1}{2}\right)u^{-\frac{s}{2}+1}\frac{du}{u^2} \\
&= \int_1^{\infty} \Theta_0(t)t^{-\frac{s}{2}-\frac{1}{2}}\,dt + \frac{1}{2}\int_1^{\infty}\left[t^{-\frac{s}{2}-\frac{1}{2}} - t^{-\frac{2}{2}-1}\right]dt.
\end{aligned}$$

Setze:

$$\begin{aligned} I(s) &= \int_1^\infty \Theta_0(t)\big[t^{\frac{s}{2}-1} + t^{-\frac{s}{2}-\frac{1}{2}}\big]\,dt \quad \text{und} \\ I_0(s) &= \frac{1}{2}\int_1^\infty \big[-t^{-\frac{s}{2}-\frac{1}{2}} + t^{-\frac{s}{2}-1}\big]\,dt \\ &= +\big[\frac{1}{-s+1}\big]_{t=1}^\infty - \big[-\frac{1}{s}t^{-\frac{s}{2}}\big]_{t=1}^\infty = -\frac{1}{s} + \frac{1}{s-1} \end{aligned}$$

Zwischenergebnis:

$$Z(s) = \frac{1}{s-1} - \frac{1}{s} + I(s) \quad (\mathrm{Re}(s) > 1)$$

Zu zeigen:

$$I(s) = \int_0^1 \Theta_0(t)\big[t^{\frac{s}{2}} + t^{\frac{1-s}{2}}\big]\frac{dt}{t}$$

konvergiert kompakt (auf $\mathbb{C}$), also $I(s)$ ganz (1.4)
Sei $a \geq 2$ und $-a \leq \mathrm{Re}(s) \leq a$. Für $t \geq 1$ gilt:

$$\sup_{-a\leq \mathrm{Re}(s)\leq a} \left|t^{\frac{s}{2}-1} + t^{\frac{-1+a}{2}}\right| \leq t^{\frac{a}{2}-1} + t^{\frac{-1+a}{2}} \leq 2t^a$$

$$\left.\begin{array}{r}\text{Also:}\\ \text{für } \mathrm{Re}(s) \leq a\end{array}\right\} \quad |\Theta_0(t)|\cdot\left|t^{\frac{s}{2}-1} + t^{\frac{-1-s}{2}}\right| \leq 2t^a \sum_{n=1}^\infty e^{-\pi n^2 t} \qquad (\underset{t\to\infty}{\longrightarrow} 0)$$

Offenbar konvergiert $I(s)$ kompakt. Wende (1.4) an. ■

(10.5) Hauptsatz (Riemann).

$$\boxed{\frac{\zeta(1-s)}{2^{1-s}} = \frac{\cos\frac{\pi s}{2}}{\pi^s}\cdot\Gamma(s)\cdot\zeta(s)}$$

Beweis. Mit (10.4):

(A) $$\pi^{-\frac{s}{2}}\Gamma\big(\frac{s}{2}\big)\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma\big(\frac{1-2}{2}\big)\zeta(1-s)$$

Nach (2.5):

$$\Gamma(s)\cdot\Gamma(1-s) = \frac{\pi}{\sin\pi s},\ \text{also}\ \Gamma\big(\frac{1-s}{2}\big)\Gamma\big(\underbrace{1-\frac{1-s}{2}}_{=\frac{s+1}{2}}\big) = \frac{\pi}{\sin\frac{\pi(1-s)}{2}} = \frac{\pi}{\cos\frac{\pi s}{2}}$$

Nach (2.6) gilt:

$$\Gamma\big(\frac{s}{2}\big)\cdot\Gamma\big(\frac{s+1}{2}\big) = 2^{1-s}\pi^{\frac{1}{2}}\Gamma(s),$$

also

$$\text{(B)} \qquad \Gamma\Big(\frac{1-s}{2}\Big) = \frac{\pi}{\cos\frac{\pi s}{2}} \cdot \frac{1}{\Gamma\big(\frac{s+1}{2}\big)} = \frac{\pi}{\cos\frac{\pi s}{2}} \cdot \frac{\Gamma\big(\frac{s}{2}\big)2^{s-1}}{\Gamma(s)\pi^{\frac{1}{2}}}$$

$$\underset{(A),(B)}{\Longrightarrow} \pi^{-\frac{s}{2}}\zeta(s) = \pi^{\frac{s-1}{2}} \cdot \frac{\pi}{\cos\frac{\pi s}{2}} \cdot \frac{1}{\Gamma(s)} \cdot \frac{2^{s-1}}{\pi^{\frac{1}{2}}}\zeta(1-s) \Rightarrow \text{ Beh.}$$

■

(10.6) Nullstellen der Zeta - Funktion (nochmals).
$\zeta(s)$ hat für $\mathrm{Re}(s) \geq 1$ keine Nullstellen (1.6),(1.10)
$\Gamma(s)$ hat (für $\mathrm{Re}(s) \geq 1$) keine Nullstellen (2.4)
$\cos\frac{\pi s}{2}$ hat für $\mathrm{Re}(s) \geq 1$ nur die (einfachen) Nullstellen in $s = 2n+1, n \in \mathbb{N}$
$\zeta(s)$ hat in $s = 1$ einen einfachen Pol (1.7)
$\underset{(10.5)}{\Longrightarrow} \zeta(1-s)$ hat nur Nullstellen in $s = 2n+1, n \in \mathbb{N}_{>0}$ (in $\mathrm{Re}(s) \geq 1$)
M.a.W: $\zeta(s)$ hat in $\mathrm{Re}(s) \leq 0$ unendlich viele Nullstellen auf $\mathrm{Re}(s) = \frac{1}{2}$
(vgl. Edwards, p. 226-229)

(10.7) Spezielle Werte der Zeta-Funktion (nochmals). Sei $n \in \mathbb{N}_{>0}$. Nach (3.5) gilt:

$$\zeta(1-2n) = -\frac{B_{2n}}{2n}$$

Also nach (10.5):

$$\zeta(2n) = \frac{\zeta(1-2n)}{2^{1-2n}} \underbrace{\frac{\pi^{2n}}{\cos\frac{\pi 2n}{2}}}_{=(-1)^n} \cdot \underbrace{\frac{1}{\Gamma(2n)}}_{=(2n-1)!} = (-1)^{n-1}2^{2n-1}\pi^{2n}\frac{B_{2n}}{(2n)!}$$

Dies ist (3.7)!!

(10.8) Satz. *Für $n \in \mathbb{N}_{>0}$ gilt*

$$\zeta(2n+1) = (-1)^n\pi^{2n}2^{n+1}\frac{\zeta'(-2n)}{(2n)!}$$

Beweis. Es ist nach (10.5)

$$\boxed{\zeta(s) = \frac{\zeta(1-s)}{2^{1-s}}\frac{\pi^2}{\cos\frac{\pi s}{2}} \cdot \frac{1}{\Gamma(s)}}$$

$\zeta(s)$ ist holomorph in $s = 2n+1$, ebenso $\frac{1}{\Gamma(s)}$; also ist

$$\frac{\zeta(1-s)}{\cos\frac{\pi s}{2}}$$

holomorph in $s = 2n+1$, also

$$\zeta(1-(2n+1)) = \zeta(-2n) = 0 \quad \text{(vergl. (3.5!)}$$

[$\zeta(s)$ hat in $s = -2n$ **einfache** Nullstellen!]
[$\cos\frac{\pi s}{2}$ hat in $s = 2n+1$ **einfache** Nullstellen!] Also nach l'Hospital:

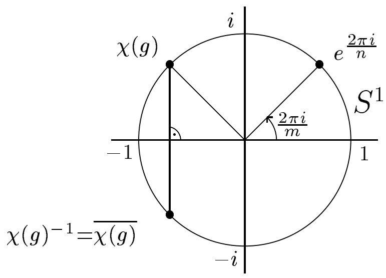
$$\begin{aligned}
\zeta(2n+1) &= \frac{\pi^{2n+1}2^{2n}}{(2n)!}\lim_{x\to 2n+1}\frac{\zeta(1-x)}{\cos\frac{\pi x}{2}} \\
&= \frac{\pi^{2n+1}2^{2n}}{(2n)!}\lim_{x\to 2n+1}\frac{-\zeta'(1-x)}{-\frac{\pi}{2}\cdot\sin\frac{\pi x}{2}} \\
&= \frac{\pi^{2n}2^{2n+1}}{(2n)!}\,\underbrace{\frac{\zeta'(-2n)}{\sin\frac{\pi(2n+1)}{2}}}_{(-1)^n} = \frac{(-1)^n\pi^{2n}2^{2n+2}}{(2n)!}\zeta(-2n)
\end{aligned}$$

■

Literatur zur Zeta-Funktion. Pracher; Edwards; Titchmash

11 Charaktere endlicher abelscher Gruppen

$G = (G,\cdot)$ endliche abelsche Gruppe; $m \in \mathbb{N}_{\geq 2}$
$\mu_m = \{z \in \mathbb{C}^* \,|\, z^m = 1\}$ Gruppe der m-ten Einheitswurzeln.
($\mu_m = \langle e^{\frac{2\pi i}{n}}\rangle$ zyklisch der Ordnung m;
$\mu_m \leq S^1$.)



(11.1) Definition. Ein (komplexer, irreduzibler) Charakter von G ist ein Gruppenhomomorphismus

$$\chi : G \to G^*$$

Diese Charaktere bilden bezüglich Punktweiser Multiplikation eine abelsche Gruppe $\widehat{G}$ („Charaktergruppe"; „duale Gruppe").

Diskussion. Neutralelement in $\widehat{G}$: $\mathbb{1}_G : G \to \mathbb{C}^*, g \mapsto 1$.
Ist $\chi \in \widehat{G}, g \in G$, so $g^n = 1$ für ein $n \in \mathbb{N}$ und

$$1 = \chi(1_G) = \chi(g^n) = \chi(g)^n, \quad \chi(g) \in \mu_n \subseteq S^1.$$

Dann $\chi(g)^{-1} = \overline{\chi(g)}$, also Inverses: $\chi^{-1} = \overline{\chi}$ konjugiert komplexer Charakter

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

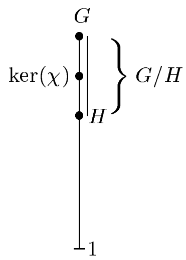
(11.2) Beispiel. Sei $G = \langle g \rangle$ zyklisch, $|G| = o(g) = n$ $G \cong Z_n = \mathbb{Z}/n\mathbb{Z}$ die zyklische Gruppe der Ordnung n).
Jedes $\chi \in \widehat{G}$ ist festgelegt durch den Wert $\chi(g) = \mu \in \mu_n$ (n-te Einheitswurzel)
Umgekehrt: $\mu \in \mu_n; g^r \mapsto \mu^r (r \in \mathbb{Z})$ definiert $\chi \in \widehat{G}$
Folglich: $\widehat{G} \cong \mu_n \cong Z_m$ zyklisch der Ordnung n ($\widehat{G} \cong G$)

(11.3) Satz. *Sei H Untergruppe von G.*

*(a) Die Einschränkung $\chi \mapsto \chi\big|_H$ ist ein Gruppen**epi**morphismus*

$$\mathrm{Res} : \widehat{G} \mapsto\!\!\!\!\rightarrow \widehat{H}$$

d.h. jeder Charakter von H lässt sich zu Charakter von G fortsetzen.

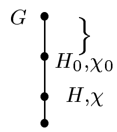


(b) Kern $\ker(\mathrm{Res}) \cong \widehat{G/H}$ *(in natürlicher Weise).*

Beweis. (a) Nur zu zeigen: Zu $\chi \in \widehat{H}$ existiert $\chi_0 \in \widehat{G}$ mit

$$\chi_0\big|_H = \chi$$

Induktion nach dem Index $|G : H| = |G/H|$
$|G : H| = 1 :$ $H = G$ in Ordnung. Sei $H \neq G$



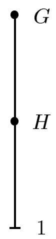
Wähle $x \in G \setminus H$: betrachte $H_0 = \langle H, x \rangle$ (Erzeugnis)
Es genügt zu zeigen: $\chi \in \widehat{H}$ kann zu $\chi_0 \in \widehat{H}_0$ fortgesetzt werden.
[$|G : H_0| < |G : H| \underset{\text{I.V.}}{\Longrightarrow} \chi_0$ kann nach G fortgesetzt werden]
Sei $|H_0/H| = n$ $\quad [H_0/H = \langle H_x \rangle, n =$ kleinste nat. Zahl mit $x^n \in H]$
Jedes Element von H_0 eindeutige Darstellung hx^r ($h \in H, r \in \mathbb{N}, r < n$).
Sei $\chi(x^n) = \varepsilon$ (Einheitswurzel); $\mathbb{C}$ ist algebraisch abgeschlossen, somit existieren $\omega \in \mathbb{C}^*$ mit $\boxed{\omega^n = \varepsilon}$ (ω Einheitswurzel)
Definiere $\chi_0 : H_0 \to \mathbb{C}^*$ durch $\underset{(h \in H, 0 \leq r < n)}{\chi_0(hx^r)} = \chi(h)\omega^r$
Dann $\chi_0\big|_H = \chi$; sei auch $h'x^s \in H_0$ ($h' \in H, 0 \leq s < n$)

$$\chi_0(hx^r h'x^s) = \chi_0(hh')x^{r+s} = \begin{cases} \chi(hh')\omega^{r+s}, & r+s < n \\ \underbrace{\chi_0\big((hh'x^n)x^{r+s-n}\big)}, & \underset{(0 \leq r+s-n < n)}{r+s \geq n} \end{cases}$$
$$= \chi(hh'x^n)\omega^{r+s-n}$$
$$= \chi(h)\chi(h')\chi(x^n)\omega^{r+s-n}$$
$$= \chi(h) \cdot \chi(h')\omega^{r+s}$$
$$= \chi(h)\omega^r \chi(h')\omega^s$$
$$= \chi_0(hx^r) \cdot \chi_0(h'x^s)$$

(b) Jeder Charakter χ von G mit $\chi\big|_H = \mathbb{1}_H$ "ist" ein Charakter von G/H. Jeder Charakter von G/H ist (in natürlicher Weise) ein Charakter von G (Inflation)

■

(11.4) Folgerungen. (a) $|\widehat{G}| = |G|$.



Beweis. Ist G zyklisch, so richtig (11.2)
Sei also $H \neq \{1\}$ eine echte Untergruppe von G.
Induktiv

$$\begin{array}{rcl} & |\widehat{H}| &=& |H|; \\ \underset{\substack{(11.3)\\ \text{[plus Homomorphisatz]}}}{\Longrightarrow} & |\widehat{G}| &=& |\widehat{H}| \cdot |\widehat{g/H}| = |H| \cdot |G/H| = |G| \end{array}$$

■

Bemerkung: es gilt sogar:

$$\widehat{G} \cong G \quad \text{(nichtnatürlich)}$$

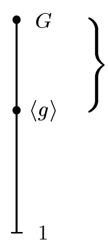
[G = direktes Produkt zyklischer Gruppen]

(b) $G \cong \widehat{\widehat{G}}$ (natürlich isomorph) via „Auswertung".

Beweis. Ordne jedem Element $g \in G$ die Auswertung

$$\widehat{g} : \widehat{G} \to \mathbb{C}^* \text{ zu } \boxed{\widehat{g} = \chi(g)}$$

$\widehat{g} \in \widehat{\widehat{G}}$ $[\widehat{g}(\chi\chi') = (\chi\chi')(g) = \chi(g)\chi'(g) = \widehat{g}(\chi)\widehat{g}(\chi')]$
$g \mapsto \widehat{g} : G \to \widehat{\widehat{G}}$ ist ein Gruppenhomomorphismus



$$\begin{array}{rcl} \widehat{gg'}(\chi) &=& \chi(gg') = \chi(g)\chi(g') \\ &=& \widehat{g}(\chi)\widehat{g}\,'(\chi) = (\widehat{g}\widehat{g}\,')(x) \end{array}$$

Es genügt zu zeigen: $g \mapsto \widehat{g}$ injektiv $(|G| \underset{(a)}{=} |\widehat{G}| \underset{(b)}{=} |\widehat{\widehat{G}}|)$

Sei $g \in G$ mit $\widehat{g} = 1$, d.h. $\chi(g) = 1$ für alle $\chi \in \widehat{G}$
$\underset{(a)}{\Longrightarrow} g = 1$

■

(11.5) Orthogonalitätsrelation.

(a) $$\textit{Für } \chi \in \widehat{G} \textit{ gilt } \sum_{g\in G} \chi(g) = \begin{cases} |G|, & \chi = \mathbb{1}_{(G)} \\ 0 & \textit{sonst} \end{cases}$$

(b) $$\textit{Für } g \in G \textit{ gilt } \sum_{\chi\in\widehat{G}} = \begin{cases} |G| & , g = 1 \\ 0 & \textit{sonst} \end{cases}$$

Beweis. (a) $\chi = 1$ O.K. Sei $\chi \neq 1$; etwa $\chi(x) \neq 1$ $(x \in G)$

$$\chi(x) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(xg) = \sum_{g\in G} \chi(g) = \underbrace{(\chi(x) - 1)}_{\neq 0} \sum_{g\in G} \chi(g) = 0 \Rightarrow \sum_{g\in G} \chi(g) = 0$$

(b)

$$\sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} \widehat{g}(\chi); \quad \widehat{g} \in \widehat{\widehat{G}}.$$

Wende (a) und (11.4)(b) an.

Charaktertafel

$$\begin{array}{c|ccccccc|c}
\widehat{G} \diagdown G & 1 & \cdots & g & \cdots & g' & \cdots & & \\
\hline
1 & & & \vdots & & & & & \\
\vdots & & & \vdots & & & & & \\
\chi & \cdots & \cdots & \chi(g) & & & & & |G| \\
\vdots & & & \vdots & & & & & \\
\chi' & \cdots & \cdots & \vdots & \cdots & \chi'(g') & & & \\
\vdots & & & & & & & & \\
\hline
 & & & |G| & & & & &
\end{array}$$

Zeilen:

$$\chi, \chi' \in \widehat{G} : \sum_{g\in G} \underbrace{\chi(g) \cdot \overline{\chi'(g)}}_{=(\chi\chi'^{-1})(g)} = \begin{cases} |G|, & \chi = \chi' \\ 0 & , \chi \neq \chi' \end{cases}$$

Spalten:

$$g, g' \in G : \sum_{\chi\in\widehat{G}} \underbrace{\chi(g) \cdot \overline{\chi(g')}}_{=\chi(gg'^{-1})} = \begin{cases} |G|, & g = g' \\ 0 & , g \neq g' \end{cases}$$

■

(11.6) Prime Restklassengruppe. $G(m) := (\mathbb{Z}/m\mathbb{Z})^*$; $2 < m \in \mathbb{N}$
$G(m)$ abelsch, $|G(m)| = \varphi(m)$ $[= |\{r \in \mathbb{N} \big| r \leq m, \mathrm{ggT}(r,m) = 1\}]$
Es ist $G(m) \cong \mathrm{Aut}(Z_m)$, (via $r + m\mathbb{Z} \mapsto g^r$ für $Z_m = \langle g \rangle$)
Satz (Gauß). Galoisgruppe des m-ten Kreisteilungskörpers $\mathbb{Q}(\mu_m)$ ist isomorph zu $G(m)$:

$$\boxed{\mathrm{Gal}(\mathbb{Q}(\mu_m) \big| \mathbb{Q}) \cong G(m)}$$

Beweis. m-tes Kreisteilungspolynom

$$\Phi_m(X) = \prod_{\substack{\mu \in \mu_m \\ o(\mu) = m}} (X - \mu) \in \mathbb{Z}[X]$$

Zeige Φ_m irreduzibel über $\mathbb{Q}$ ■

Zusätze. (a) Ist $m_0 \big| m$ ($m_0 \in \mathbb{N}_{>0}$), so natürlicher Homomorphismus

$$G(m) \to G(m_0),\ a + m\mathbb{Z} \mapsto a + m_0\mathbb{Z} \quad (\mathrm{ggT}(a,n) = 1)$$

Dies ist surjektiv (!)

(b) Chinesischer Restesatz: Sind m, m' teilerfremd, so natürlicher Isomorphismus

$$G(m \cdot m') \cong G(m) \times G(m')$$

(11.7) Dirichlet - Charaktere. $\widehat{G(m)}$ = Gruppe der Dirichlet - Charaktere mod m.
Ist $\chi \in \widehat{G(m)}$, so definiert $\chi : \mathbb{Z} \to \mathbb{C}$ durch die Vorschrift

$$\chi(a) = 0 \text{ ,falls } (a = 0 \text{ oder}) \ \mathrm{ggT}(a,m) \neq 1$$

(sonst $\chi(a) = \chi(a + m\mathbb{Z})$)
M.a.W. Ein Dirichlet-Charakter mod m ist eine Abbildung Abbildung $\chi : \mathbb{Z} \to \mathbb{C}$ mit ($a \in \mathbb{Z}$)

(i) $\chi(a + m) = \chi(a)$ [Periode m]

(ii) χ ist stark multiplikativ

(iii) $\chi(a) = 0$, falls $\mathrm{ggT}(a,m) \neq 1$

Eigenschaften. Sei χ Dirichlet-Charakter mod m

(a) χ ist quadratisch (reell) $:\Longleftrightarrow$ Ordnung $o(\chi)$ in $\widehat{G(m)}$ ist 2 [Werte $\pm 1, 0$]

(b) χ ungerade [gerade] $:\Longleftrightarrow$ $\chi(-1) = -1$ $[\chi(-1) = 1]$

(c) χ imprimitiv $:\Longleftrightarrow$ Es gibt echten Teiler $m_0 \big| m$ und $\chi_0 \in \widehat{G(m_0)}$ mit??
Sonst heißt χ primitiv mod m
Es gibt immer einen kleinsten Modulus $m_0 = f(\chi)$, so dass χ induziert von geeignetem $\chi_0 \in \widehat{G(m_0)}$
$f(\chi)$ heißt der Führer von χ („Konduktor")

$$\begin{tikzcd} G(m) \arrow[rr, "\chi"] \arrow[dr] & & \mathbb{C}^* \\ & G(m_0) \arrow[ur, dotted, "\chi_0"'] & \end{tikzcd} \quad (\chi \textit{ von } \chi_0 \textit{ induziert})$$

(11.8) Beispiele.

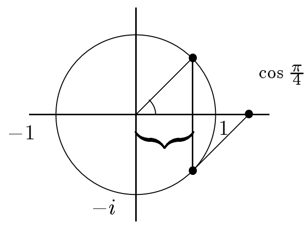
(a) $m = 4$: $G(4) = \langle 3 \bmod 4\rangle$ zyklisch der Ordnung 2 $[= \varphi(4)]$
Für ungerades $a \in \mathbb{Z}$ definiere

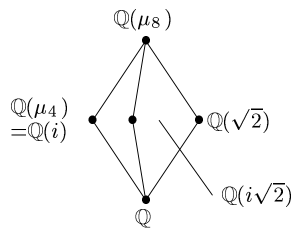
$$\varepsilon(a) = \frac{a-1}{2} \bmod 2 = \begin{cases} 0 & \text{falls } a \equiv 1 \pmod 4 \\ 1 & \textit{sonst} \end{cases}$$

Dirichlet-Charakter

$$(-1)^{\varepsilon} : G(4) \to \mathbb{C}^* \qquad \left[(-1)^{\varepsilon(a)} = \begin{cases} 1 & a \equiv 1 \pmod 4 \\ -1 & \text{sonst} \end{cases} \right]$$

(b) $m = 8$: $G(8) \cong Z_2 \times Z_2$ Vierergruppe





Für ungerades $a \in \mathbb{Z}$ definiere

$$\omega(a) = \frac{a^2-1}{8} \quad \bmod 2 = \begin{cases} 0, & \text{falls } a \equiv \pm 1 \pmod 8 \\ 1, & \text{falls } a \equiv \pm 3 \pmod 8 \end{cases}$$

Dirichlet-Charakter mod 8:

$$(-1)^{\omega} : G(8) \to \mathbb{C}^*,$$

$$(-1)^{\omega(a)} = \begin{cases} 1, & \text{falls } a \equiv \pm 1 \pmod 8 \\ -1 & \text{sonst} \end{cases}$$

$(-1)^\omega$ ist primitiv $\mod 8$

$$\begin{tikzcd} G(8) \arrow[r, two heads] \arrow[rr, bend right] & G(4) \arrow[r, "(-1)^\varepsilon"] & \mathbb{C}^* \end{tikzcd}$$

Fasse $(-1)^\varepsilon$ als imprimitiven Charakter $\mod 8$ auf via

$$G(8) \twoheadrightarrow G(4) \xrightarrow{(-1)^\varepsilon} \mathbb{C}^*$$

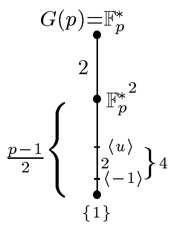
Charaktertafel

		1	3	5	7	
	1	1	1	1	1	
primitiv(8) $\rightarrow$	$(-1)^\omega$	1	-1	-1	1	0
	$(-1)^\varepsilon$	1	-1	1	-1	0
primitiv(8) $\rightarrow$	$(-1)^{\omega+\varepsilon}$	1	1	-1	-1	0
			0	0	0	

Bemerkung: Ist $r \geq 3$, so ist

$$\begin{aligned} G(2^r) &= \langle -1 \mod 2^r \rangle \times \langle 5 \mod 2^r \rangle \\ &\cong Z_2 \times Z_{2^{r-2}}. \end{aligned}$$

(c) $p \in \mathbb{P}, p \neq 2$: $G(p) = \mathbb{F}_p^* = \langle g \mod p \rangle$ zyklisch der Ordnung $p-1$ (g heißt primitive Kongruenzwurzel $\mod p$).
Also $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$. Es gibt genau einen quadratischen Dirichlet-Charakter $\mod p$, nämlich den Legendre-Charakter $(\frac{\bullet}{p})$. Es gilt ($a \in \mathbb{F}_p^*$):



$$\left(\frac{a}{p}\right) = 1 \iff a \in \mathbb{F}_p^{*2} \quad [\iff a \text{ Quadrat} \mod p]$$

$[(\frac{a}{p}) = -1$ sonst $]$

(11.9) Das Quadratische Reziprozitätzgesetz. *(=Übungsblatt 10)*
Sind $p \neq q$ ungerade Primzahlen, so gilt

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

Ergänzungsgesetze.

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

Beweis.
$$\left(\frac{-1}{p}\right) = 1 \iff -1 \in \mathbb{F}_p^{*^2} \iff \exists u \in \mathbb{F}_p^* : u^2 = -1 \iff 4\big|p-1$$

■

(b)
$$\left(\frac{2}{p}\right) = (-1)^{\omega(p)} = (-1)^{\frac{p^2-1}{8}} \quad [= 1 \iff p \equiv \pm 1 \pmod 8]$$

Beweis. Sei ε primitive 8-te Einheitswurzel über $\mathbb{F}_p$: dann

$$\varepsilon^2 + \varepsilon^{-2} = 0 \text{ und } (\varepsilon + \varepsilon^{-1})^2 = 2$$

$$\begin{aligned}
(\frac{2}{p}) = 1 \quad &\iff \quad 2 \in \mathbb{F}_p^{*^2} \iff \varepsilon + \varepsilon^{-1} \in \mathbb{F}_p \iff \varepsilon^p + \varepsilon^{-p} = (\varepsilon + \varepsilon^{-1})^p = \varepsilon + \varepsilon^{-1} \\
&\iff \quad \begin{cases} \varepsilon^p = \varepsilon, & \text{d.h. } 8\big|p-1 \\ \text{oder } \varepsilon^p = \varepsilon^{-1}, & \text{d.h. } 8\big|p+1 \end{cases}
\end{aligned}$$

■

Beispiel.

$$\begin{aligned}
\left(\frac{115}{43}\right) &= \left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{7}{29}\right) \\
&= -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1
\end{aligned}$$

12 Dirichletsche L-Funktionen

$m \in \mathbb{N}_{\geq 3}$; $\chi \in \widehat{G(m)}$ Dirichlet - Charakter mod m ($\chi : \mathbb{Z} \to \mathbb{C}$)

(12.1) Definition.

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

heißt die zu χ gehörige L-Reihe („L-Funktion“). Ferner:

$$\zeta_m(s) = \prod_{\chi \in \widehat{G(m)}} L(s, \chi)$$

Bemerkung. Es gilt:

$$|\chi|(n) := |\chi(n)| = \begin{cases} 1, & \text{falls } \operatorname{ggT}(n,m) = 1 \\ 0 & \text{sonst} \end{cases}$$

Also $|\chi| = \mathbb{1}$ der Dirichlet 1-Charakter $\mod m$
$\zeta_m(s)$ ist „im Wesentlichen“ die (Dedekindsche) Zeta-Funktion von $\mathbb{Q}(\mu_m)$

(12.2) Satz. *Für* $\operatorname{Re}(s) > 1$ *gilt das Euler-Produkt*

$$L(s,\chi) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

(a) Für $\chi = \mathbb{1}$ *gilt*

$$L(s,\mathbb{1}) = \zeta(s) \cdot \prod_{p|m} (1 - \frac{1}{p^s})$$

Also ist $L(s,\mathbb{1})$ *holomorph überall bis auf die Stelle* $s = 1$, *wo ein einfaher Pol vorliegt mit Residuum* $\frac{\varphi(m)}{m}$

(b) Für $\chi \neq \mathbb{1}$ *ist* $L(s,\chi)$ *konvergent*[7] *(und damit holomorph) für* $\operatorname{Re}(s) > 0$

Beweis. Wir haben (wegen $|\chi(m)| \le 1$) absolute Konvergenz für $L(s,\chi)$ für $\operatorname{Re}(s) > 1$. Wende (5.3) an!
Beachte: $L(s,\chi) \neq 0$ für $\operatorname{Re}(s) > 1$ (Euler Produkt)

(a) Für $\operatorname{Re}(s) > 1$ gilt (nach obigem):

$$L(s,\mathbb{1}) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{\mathbb{1}(p)}{p^s}} = \prod_{p\nmid m} \frac{1}{1 - \frac{1}{p^s}} = \underbrace{\prod_{p} \frac{1}{1 - \frac{1}{p^s}}}_{=\zeta(s)} \cdot \prod_{p|m} (1 - \frac{1}{p^s})$$

Nach (3.4) ist also $L(s,\mathbb{1})$ erklärt (erklärbar!) auf $\mathbb{C}$, und ist dort holomorph (wie $\zeta(s)$) mit Ausnahme der Stelle $s = 1$, wo $L(s,\mathbb{1})$ einen einfachen Pol mit Residuum

$$1 \cdot \prod_{p|m} (1 - \frac{1}{p}) = \frac{\varphi(m)}{m}$$

hat.
$[m = \prod_{p|m} p^{e_p}$ PFZ: $\varphi(m) = \prod_{p|m} p^{e_p - 1}(p-1) = m \prod_{p|m}(1 - \frac{1}{p})]$

(b) Sei $N \in \mathbb{N}_{>0}$; $A_N = \sum_{n=1}^{m} \chi(m)$ (schaue auf (4.6)!)
Für $N = m$ gilt nach (11.5):

$$\sum_{n=1}^{m} \chi(n) = \sum_{\substack{n=1 \\ (n,m)=1}} \chi(n) = \sum_{\bar{n}\in G(m)} \chi(\bar{n}) = 0 \quad (!)$$

[7] kompakt konvergent

Im Allgemeinen: Es gibt $k \in \mathbb{N}$ mit $km \leq N < (k+1)m$. Dann (Periode m)

$$|A_N| = \left| \sum_{n=km+1}^{N} \chi(n) \right| = \left| \sum_{n=1}^{n-km} \chi(n) \right| \leq \sum_{n=1}^{N-kn} |\chi(n)| \leq |G(m)| = \varphi(m)$$

Also $A_N = O(1)$ beschränkt. Wende (4.6) an.

$\blacksquare$

Bemerkung.

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0 \quad (\chi \neq 1)$$

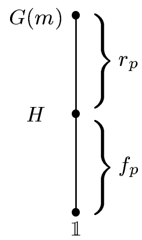
lässt sich holomorph fortsetzen.

(12.3) Lemma. *Sei* $p \nmid m \quad (p \in \mathbb{P})$*; sei* $f_p = 0(p \mod m)$ *Ordnung von* $p + m\mathbb{Z}$ *in* $G(m)$ *und* $r_p = \frac{\varphi(m)}{f_p}$ *(„Zerlegungszahl“)*

Behauptung:

$$\prod_{\chi \in \widehat{G(m)}} \big(1 - \chi(p)X\big) = (1 - x^{f_p})^{r_p}$$

im Polynomring $\mathbb{Z}[X]$.



Beweis. Sei $H = \langle p + m\mathbb{Z} \rangle$ (Untergruppe von $G(m)$); $|H| = f_p$
Nach (11.3), (11.4) hat jedes $\chi' \in \widehat{H}$ genau $r_p = \frac{|G(m)|}{|H|}$
viele $\chi \in \widehat{G(m)}$ mit $\chi\big|_H = \chi'$.
Also

$$\prod_{\chi \in \widehat{G(m)}} (1 - \chi(p)X) = \prod_{\chi' \in \widehat{H}} (1 - \chi'(p)X)^{r_p} = (1 - \chi^{f_p})^{r_p}$$

[$\chi'(p) = \chi'(p + m\mathbb{Z})$ f_p-te Einheitswurzel] $\blacksquare$

(12.4) Lemma. *Für* $\mathrm{Re}(s) > 1$ *(mindestens) gilt* $\zeta_m(s) \neq 0$ *(Euler-Produkt), und:*

(a)
$$\zeta_m(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ mit } \underset{(a_n \in \mathbb{N}_{>0})}{\text{multiplikativen}} \ (a_n) \in \mathbb{N}(\mathbb{N}_{>0})$$

(b)
$$\log \zeta_m(s) = \varphi(m) \sum_{\substack{p \in \mathbb{P} \\ p^r \equiv 1 (\mathrm{mod}\ m)}} \sum_{r \in \mathbb{N}_{>0}} \frac{1}{r p^{rs}}$$

Beweis. (a) Nach (12.2):

$$\begin{aligned}\zeta_m(s) &= \prod_{\chi\in\widehat{G(m)}} L(s,\chi) = \prod_{\substack{p\in\mathbb{P}\\(p\nmid m)}}\left(\prod_{\chi\in\widehat{G(m)}}\frac{1}{1-\frac{\chi(p)}{p^s}}\right)\\ &\underset{(12.3)}{=} \prod_{p\nmid m}\frac{1}{\left(1-\frac{1}{p^{sf_p}}\right)^{r_p}} = \prod_{p\nmid m}\left(1+\left(\frac{1}{p^s}\right)^{f_p}+\left(\frac{1}{p^{2s}}\right)^{f_p}+\cdots\right)^{r_p}\end{aligned}$$

Ausmultiplizieren! (Rest §5)

(b)

$$\zeta_m(s) = \prod_{\chi\in\widehat{G(m)}}\prod_{p\in\mathbb{P}}\frac{1}{1-\frac{\chi(p)}{p^s}} \quad (\neq 0) \quad \Big(\mathrm{Re}(s)>1;\ (12.2)\Big)$$

$$\log\zeta_m(s) = \sum_{\chi\in\widehat{G(m)}}\sum_{p\in\mathbb{P}}\log\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right) = \sum_{p\in\mathbb{P}}\sum_{\chi\in\widehat{G(m)}}\left(\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{2p^{2s}}+\frac{\chi(p^3)}{3p^{3s}}+\cdots\right)$$

Nach (11.5) gilt:

$$\sum_{\chi\in\widehat{G(m)}}\chi(p^r) = \begin{cases}\varphi(m), & p^r\equiv 1 \pmod m\\ 0 & \text{sonst}\end{cases}$$

Damit:

$$\log\zeta_m(s) = \varphi(m)\sum_{\substack{p\in\mathbb{P}\\p^r\equiv 1(\mathrm{mod}\ m)}}\sum_{r\in\mathbb{N}_{>0}}\frac{1}{rp^{rs}}$$

■

(12.5) Hauptsatz. *Für* $\chi\neq\mathbb{1}$ *gilt* $L(1,\chi)\neq 0$

Beweis. Wir wissen:

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

konvergiert (12.2)
Annahme: $L(1,\chi)=0$ (für ein $\mathbb{1}\neq\chi\in\widehat{G(m)}$)
Dann ist nach (12.2) $\zeta_m(s)$ holomorph für $\mathrm{Re}(s)>0$
Damit nach (12.4)(a) und (4.8) [Landau]

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

konvergent für $\mathrm{Re}(s) > 0$ $(0 \leq a_n \in \mathbb{R})$
Damit hat $\zeta_m(s)$ in $\mathrm{Re}(s) > 0$ ein Eulerprodukt ((a_n) multiplikativ; absolute konvergenz)
Also $\zeta_m(s) \neq 0$ für $\mathrm{Re}(s) > 0$ und damit $\log \zeta_m(s)$ konvergent $(\mathrm{Re}(s) > 0)$
Nach (12.4)(b)

$$\log \zeta_m(s) = \varphi(m) \sum_{\substack{p \in \mathbb{P} \\ p^r \equiv 1 (\mathrm{mod}\ m)}} \sum_{r \in \mathbb{N}_{>0}} \frac{1}{rp^{rs}}$$

konvergent für $\mathrm{Re}(s) > 0$.
Sei $0 < x < 1$ (reell). Nach dem kleinen Satz von Fermat[8] gilt

$$\sum_{\substack{p \in \mathbb{P} \\ p^r \equiv 1 (\mathrm{mod}\ m)}} \sum_{r \in \mathbb{N}_{>0}} \frac{1}{rp^{rs}} \geq \sum_{p \nmid m} \sum_{\varphi(m) | r} \frac{1}{rp^{rx}} = \frac{1}{\varphi(m)} \sum_{p \nmid m} \sum_{k=1}^{\infty} \frac{1}{kp^{k\varphi(m)x}} \qquad [r = k\varphi(m)]$$

Daher konvergiert

$$\sum_{p \nmid m} \sum_{k=1}^{\infty} \frac{1}{kp^{k\varphi(m)x}} \qquad (\text{für alle } 0 < x < 1)$$

$$= \log L(\varphi(m)x, \mathbb{1})$$

Wähle $x = \frac{1}{\varphi(m)}$ (Widerspruch. $L(s, \mathbb{1})$ hat in $s = 1$ nach (12.2) einen Pol!) ■

Aufgabenstellung. Berechne $L(1, \chi)$ für $\chi \neq 1$
Etwa: $m = 4,\ \chi = (-1)^{\varepsilon}:\quad L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - + (= \frac{\pi}{4})$

(12.6) Folgerung. $\zeta_m(s)$ hat in $s = 1$ einen einfachen Pol mit Residuum

$$\frac{\varphi(m)}{m} \prod_{\mathbb{1} \neq \chi \in \widehat{G(m)}} L(1, \chi)$$

Beweis. Folgt aus dem Hauptsatz (12.5) und (12.2). ■

(12.7) Folgerung. Die Reihe

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv 1 (m)}} \frac{1}{p}$$

ist divergent.

[8]Pierre de Fermat (1601-1665)

Beweis. Nach (12.6):

$$\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv 1 (\mathrm{mod}\ m)}}\sum_{r\in\mathbb{N}_{>0}} \frac{1}{rp^r} = \sum_{\substack{p\in\mathbb{P} \\ p\equiv 1(m)}} \frac{1}{p} + \sum_{\substack{p\in\mathbb{P} \\ p^r\equiv 1 (\mathrm{mod}\ m)}}\sum_{r\geq 2} \frac{1}{rp^r}$$

divergiert. **Zeige:**

$$\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv 1 (\mathrm{mod}\ m)}}\sum_{r\geq 2} \frac{1}{rp^r} \leq \frac{1}{2}\sum_{\substack{p\nmid m \\ p\in\mathbb{P}}}\sum_{r=2}^{\infty}\frac{1}{p^r} = \frac{1}{2}\sum_{p\in\mathbb{P}}\frac{1}{p^2(1-\frac{1}{p})} \leq \frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{n(n-1)} = \frac{1}{2}$$

ist konvergent. Majorantenkriterium! ■

13 Primzahlen in arithmetischer Progression

$m \in \mathbb{N}_{\geq 3}$, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m)$. Dann

$$\mathbb{P}_a = \mathbb{P}_{a,m} := \mathbb{P} \cap (a + m\mathbb{Z}) = \{p \in \mathbb{P} \big| p \equiv a \pmod m\}$$

(Ist $\mathrm{ggT}(a, m) \neq 1$, so ist $\mathbb{P}\cap(a+m\mathbb{Z}) = \emptyset$ oder $\mathrm{ggT}(a, m) = p$ ist die einzige Primzahl in $a + m\mathbb{Z}$)

(13.1) Hauptsatz (Dirichlet).

$$\mathbb{P}_a \textit{ ist unendlich; genauer: } \sum_{p\in\mathbb{P}} \frac{1}{p} \textit{ ist divergent}$$

Beweis. Für $p \in \mathbb{P}, r \in \mathbb{N}_{>0}$ gilt nach (11.5):

$$\sum_{\chi\in\widehat{G(m)}} \chi(p^r)\chi(a) = \begin{cases} \varphi(m), & p^r \equiv a \pmod m \\ 0 & \text{sonst} \end{cases}$$

Damit für $\mathrm{Re}(s) > 1$:

$$\begin{aligned}
\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv 1 (\mathrm{mod}\ m)}}\sum_{r\in\mathbb{N}_{>0}} \frac{1}{rp^{rs}} &= \frac{1}{\varphi(m)}\sum_{p\in\mathbb{P}}\sum_{r\in\mathbb{N}_{>0}}\sum_{\chi\in\widehat{G(m)}} \widehat{\chi}(a)\frac{\chi(p^r)}{rp^{rs}} \\
&= \frac{1}{\varphi(m)}\left[\log L(s,\mathbb{1}) + \sum_{\mathbb{1}\neq\chi\in\widehat{G(m)}} \widehat{\chi}(a)\log L(s,\chi)\right]
\end{aligned}$$

Nach (12.5) konvergiert

$$\sum_{1\neq\chi\in G(m)} \widehat{\chi}(a)\log L(s,\chi) \quad \text{für } s = 1$$

Nach (12.2) konvergiert $\log L(s, \mathbb{1})$ für $s = 1$ nicht. Also

$$\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv 1 (\mathrm{mod}\ m)}} \sum_{r\in\mathbb{N}_{>0}} \frac{1}{rp^r} = \sum_{p\in\mathbb{P}_a} \frac{1}{p} + \sum_{\substack{p\in\mathbb{P} \\ p^r\equiv a (\mathrm{mod}\ m)}} \sum_{r\geq 2} \frac{1}{rp^r}$$

divergiert.
Wie im Beweis von (12.7) ist die Reihe

$$\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv a (\mathrm{mod}\ m)}} \sum_{r\geq 2} \frac{1}{rp^r} \quad \left(\leq \frac{1}{2}\right)$$

konvergent. $\Rightarrow$ Behauptung. ■

(13.2) Definition. Sei $Q \subseteq \mathbb{P}$; Q hat eine (die) **Dirichlet-Dichte** (oder **analytische Dichte**) $\delta(Q)$, falls der Limes

$$\lim_{x\searrow 1} \frac{\sum_{p\in Q} \frac{1}{p^x}}{\sum_{p\in\mathbb{P}} \frac{1}{p^x}} =: \delta(Q)$$

existiert.

Bemerkungen:. Es ist $\delta(\mathbb{P}) = 1$ und $\delta(Q) \leq 1$ (falls existent).
Ist Q eine endliche Menge, so ist $\delta(Q) = 0$.

Beispiel (Bombieri). $\mathbb{P}(1)$ = Menge der Primzahlen mit erster Dezimale 1

$$(11, 13, 17, 19, 101, \ldots$$

$$\delta(\mathbb{P}(1)) = \log_{10} 2$$

(13.3) Lemma.

$$Q \subseteq \mathbb{P}; \quad \delta(Q) = \lim_{x\searrow 1} \frac{\sum_{p\in Q} \frac{1}{p^x}}{\log \frac{1}{x-1}} \quad \textit{(falls existent)}$$

Beweis. Nach (1.8) gilt

$$\sum_{p\in\mathbb{P}} \frac{1}{p^x} \sim \frac{1}{x-1} \text{ für } x \searrow 1$$

■

$\Big[\lim_{s\to 1}(s-1)\zeta(s) = 1;\quad \log\zeta(s) \sim \log\frac{1}{s-1}$ *für* $s \to 1; \zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}\quad (\mathrm{Re}(s) > 1)$

$\log\zeta(s) = \sum_p \sum_{r\geq 1} \frac{1}{rp^{rs}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{r\geq 2} \frac{1}{rp^{rs}}.\Big]$

(13.4) Hauptsatz' (Dirichlet). $\delta(\mathbb{P}_a) = \frac{1}{\varphi(m)}$ *(existiert).*
Die Primzahlen sind also ***gleichverteilt*** *auf die verschiedenen primen Restklassen* mod m[9]

Beweis. Die Reihe

$$\sum_{p\in\mathbb{P}} \frac{1}{p^x}$$

ist für $x \searrow 1$ monoton wachsend und divergent (1.2).
Nach (13.1) [inklusive Beweis] gilt für $\mathrm{Re}(s) > 1$:

$$\sum_{\substack{p\in\mathbb{P} \\ p^r\equiv a (\mathrm{mod}\ m)}} \sum_{r\geq 1} \frac{1}{rp^{rs}} = \frac{1}{\varphi(m)}\left[\log L(s,\mathbb{1}) + \sum_{\chi\neq 1} \widehat{\chi}(a)\log L(s,\chi)\right]$$

Es ist für $x > 1$*:

$$\sum_{\substack{p \\ p^r\equiv a(m)}} \sum_{r} \frac{1}{rp^{rx}} = \sum_{p\in\mathbb{P}_a} \frac{1}{p^x} + \sum_{\substack{p \\ p^r\equiv a(m)}} \sum_{r\geq 2} \frac{1}{rp^{rx}}$$

und

$$\lim_{x\searrow 1} \sum_{\substack{p \\ p^r\equiv a(m)}} \sum_{r\geq 2} \frac{1}{rp^{rx}}$$

existiert (Grenzwert $\leq \frac{1}{2}$, vergl. (13.1))

Es ist für $x > 1$:

$$\begin{aligned} \log L(x,\mathbb{1}) &= \sum_{p\nmid m} \sum_{r\geq 1} \frac{1}{rp^{rx}} \qquad \left[L(x,\mathbb{1}) = \prod_{p\nmid m} \frac{1}{1-\frac{1}{p^x}}\right] \\ &= \sum_{p} \frac{1}{p^x} - \sum_{p\mid m} \frac{1}{p^x} + \sum_{p\nmid m} \sum_{r\geq 2} \frac{1}{rp^{rx}} \end{aligned}$$

Es ist für $x > 1$*:

$$\lim_{x\searrow 1} \sum_{\chi\neq 1} \widehat{\chi}(a)\log L(x,\chi) \text{ existiert, denn}$$

$$L(1,\chi) \neq 0 \text{ für } \chi \neq \mathbb{1} \quad (12.5)$$

$\big[$ und $L(s,\chi)$ holomorph für $\mathrm{Re}(s) > 0$; (12.2) $\big]$

Konsequenz:

$$\sum_{p\in\mathbb{P}_a} \frac{1}{p^x} - \frac{1}{\varphi(m)} \sum p \in \mathbb{P} \frac{1}{p^x} = f(x) \text{ mit } \lim_{x\nearrow 1} \frac{f(x)}{\sum_{p\in\mathbb{P}} \frac{1}{p^x}} = 0$$

[9] wird falsch, falls m eine Primzahl ist

■

(13.5) Definition. $Q \subseteq \mathbb{P}$; Q hat die **natürliche (statistische) Dichte** $\delta_0(Q)$, falls

$$\lim_{N\to\infty} \frac{\big|Q \cap [1,N]\big|}{\pi(N)} = \delta_o(Q)$$

existiert.

Bemerkung. Existiert $\delta_0(Q)$, so auch $\delta(Q)$ und $\delta(Q) = \delta_0(Q)$ [Übung 51]. (Umkehrung gilt nicht!)

(13.6) Hauptsatz''' (Pracher).

$$\delta_0(\mathbb{P}_a) = \frac{1}{\varphi(m)} \qquad \textit{(existiert)}$$

Beweis.

(a) Setze $\pi(N) = \big|\{p \in \mathbb{Q} \big| p \leq N\}\big|$
Zu zeigen:

$$\lim_{N\to\infty} \frac{\pi_a(N)}{\pi(n)} = \frac{1}{\varphi(m)}$$

Setze

$$\begin{aligned} f(s) &= \sum_{p\in\mathbb{P}_a} \frac{1}{p^s} - \frac{1}{\varphi(m)} \sum_{p\in\mathbb{P}} \frac{1}{p^s} \quad (\mathrm{Re}(s) > 1) \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ mit } a_n = \begin{cases} 1 - \frac{1}{\varphi(m)}, & n \in \mathbb{P}_a \\ -\frac{1}{\varphi(m)}, & n \in \mathbb{P} \setminus \mathbb{P}_a \text{ sonst} \end{cases} \end{aligned}$$

Zeige (in (b)): f hat Konvergenzabszisse $\rho_f < 1$
Dann ist

$$A_N = \sum_{n=1}^{N} a_n = O(N^{1-\varepsilon}),\ \varepsilon > 0$$

Vergl. Übung 19
[Es existiert $0 < a < 1$, wo

$$\sum_{n=1}^{\infty} \frac{a_n}{n^a} = f(a)$$

konvergiert. ($\varepsilon = 1 - a > 0$)

$$|B_N| = \left| \sum_{n=1}^{N} \frac{a_n}{n^a} \right| \leq c$$

beschränkt für alle $N \in \mathbb{N}$.
Partielle Summation (4.3):

$$\begin{aligned} |A_N| &= \left|\sum_{n=1}^{N} \frac{a_n}{n^a} \cdot n^a\right| = \left|B_N N^a + \sum_{n=1}^{N-1} B_n(n^a - (n+1)^a)\right| \\ &\le cN^a + c\sum_{n=1}^{N-1}((n+1)^a - n^a) < 2cN^a.\Big] \end{aligned}$$

Aber nun ist

$$A_N = \pi(N) - \frac{1}{\varphi(m)}\pi(N) = O(N^{1-\varepsilon})$$

Primzahlsatz (7.1)[10]:

$$\frac{\pi_a(N)}{\pi(N)} = \frac{1}{\varphi(m)} + O\left(\frac{N^{1-\varepsilon}}{\pi(N)}\right) \underset{\substack{\uparrow\\ \text{PZS}}}{=} \frac{1}{\varphi(m)} + O\left(\frac{\log N}{N^\varepsilon}\right)$$

Es gilt

$$\lim_{N\to\infty} \frac{\log N}{N^\varepsilon} = 0$$

(b) Nach (13.1) [inklusive Beweis] gilt für $\mathrm{Re}(s) > 1$:

$$\sum_{\substack{p \\ p^r \equiv a(m)}} \sum_{r\ge 1} \frac{1}{rp^{rs}} = \frac{1}{\varphi(m)}\left[\log L(s, \mathbb{1}) + \sum_{\chi\ne 1} \widehat{\chi}(a) \log L(s,\chi)\right]$$

- $$\sum_{\substack{p \\ p^r \equiv a(m)}} \sum_{r\ge 1} \frac{1}{rp^{rs}} = \sum_{p\in\mathbb{P}_a} \frac{1}{p^s} + \sum_{\substack{p \\ p^r \equiv a(m)}} \sum_{r\ge 2} \frac{1}{rp^{rs}},$$

  wo der zweite Summand konvergent ist für $\mathrm{Re}(s) > \frac{1}{2}$

- $$\log L(s,\mathbb{1}) = \sum_{p\nmid m} \sum_{r\ge 1} \frac{1}{rp^{rs}} = \sum_{p} \frac{1}{p^s} + \left(-\sum_{p\mid m} \frac{1}{p^s} + \sum_{p\mid m} \sum_{r\ge 2} \frac{1}{rp^{rs}}\right),$$

  wo der zweite Summand konvergent ist für $\mathrm{Re}(s) > \frac{1}{2}$

- $$F(s) = \sum_{\chi\ne 1} \widehat{\chi}(a) \log L(s,\chi) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} \text{ Dirichlet Reihe (siehe oben)}$$

[10][$\pi(N) \sim \frac{N}{\log N}, N \to \infty$]

Nach (12.5) ist $L(s,\chi) \neq 0$ für s in Umgebung von $s = 1, \chi \neq 1$. Also ist $F(s)$ holomorph in Umgebung von $s = 1$; F hat Konvergenzabszisse $\rho_F < 1$ (Argument wie in Landau (4.8)!)

$$\Rightarrow \quad f(s) = \sum_{p \in \mathbb{P}_a} \frac{1}{p^s} - \frac{1}{\varphi(m)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} \text{ holomorph}$$

■

(13.7) Anhang (Chebotarevs Dichtesatz). Sei $f \in \mathbb{Z}[X]$ ein separables Polynom vom Grade $n \geq 2$ über $\mathbb{C}$: $f(X) = a_n \prod_{i=1}^n (X - \alpha_i)$ (mit Diskriminante $d(f) \neq 0$), $W_f = \{\alpha_1, \ldots, \alpha_n\}$; $|W_f| = n$.
Sei $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$; $G = \mathrm{Gal}(K(\mathbb{Q})) = \mathrm{Aut}(K)$, G Untergruppe von $\mathrm{Sym}(W_f)$; $|G| = [K : \mathbb{Q}]$.
Sei p eine „gute Primzahl für f", d.h. $p \nmid a_n$, $p \nmid$ Diskriminante von f, d.h. Reduktion $\bar{f} = f \mod p$ ist separabel über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ vom Grade n. (Es gibt nur endlich viele schlechte Primzahlen).
Sei $\mathfrak{p} \supseteq pR$ ein maximales Ideal von R (R ist G-invariant und $\mathfrak{p}$ bis auf G-Konjugation bestimmt.)
Dann $\bar{K} = R/\mathfrak{p}$ endlicher Körper der Charakteristik p; $\mathrm{Gal}(\bar{K}|\mathbb{F}_p)$ wird erzeugt durch $\bar{x} \mapsto \bar{x}^p$ (Frobenius)
$W_{\bar{f}} = \{\bar{\alpha}_i = \alpha_i + \mathfrak{p} \big| 1 \leq i \leq n\}$; $\bar{f} = \bar{a}_n \prod_{i=1}^n (X - \bar{\alpha}_i)$.
Sei $p \in \mathbb{P}$ mit $p \nmid a_n d(f)$; $\bar{f} = f \mod p \in \mathbb{F}_p[X]$, $\mathrm{grd}(\bar{f}) = n$, $d(\bar{f}) \neq 0$.

Lemma 1. *G operiert transitiv auf den maximalen Idealen $\mathfrak{p}$ von R mit $\mathfrak{p} \supseteq pR$.*

Beweis. O.B.d.A. $a_n = 1$. [Sonst ersetze $\mathbb{Z}$ durch $\mathbb{Z}_{(p)} = \{\frac{a}{b} \big| a, b \in \mathbb{Z}, p \nmid b\}$]
Dann (!) $R \cap \mathbb{Q} = \mathbb{Z}$ und $\mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z} \subseteq pR$.
Annahme: Es gibt ein maximales Ideal $\mathfrak{q}$ von R mit $\mathfrak{q} \supseteq pR$ und $\mathfrak{p} \notin \{\mathfrak{q}^\sigma = \sigma(\mathfrak{q}) \big| \sigma \in G\}$.
Chinesischer Restesatz: Es existiert $x \in R$ mit $x \equiv 0(\mod \mathfrak{p}), x \equiv 1(\mod \mathfrak{q}^\sigma), \sigma \in G$

$$\left.\begin{array}{rc} \text{Norm:} & N_{K|\mathbb{Q}}(x) := \prod_{\sigma \in G} x^\sigma = x \cdot \prod_{1 \neq \sigma \in G} x^\sigma \in \mathfrak{p} \cap \mathbb{Q} \subseteq pR \\ \text{Andererseits:} & N_{K|\mathbb{Q}}(x) \equiv 1 \ (\mod \mathfrak{q}), \notin \mathfrak{q}, \mathfrak{q} \supseteq pR \end{array}\right\}$$

■

Lemma 2 (Dedekind-Bauer). *Sei $\mathfrak{p} \supseteq pR$ maximales Ideal von R, $\bar{K} = {}^R/_{\mathfrak{p}} = \mathbb{F}_p(W_{\bar{f}}$, $\bar{f} = \widehat{a_n} \prod_{i=1}^n (X - \bar{\alpha}_i)$, $\bar{\alpha}_i = \alpha_i + \mathfrak{p}$*
$[\bar{f}(\bar{\alpha}_i) = f(\alpha_i) + \mathfrak{p}]$. ($\bar{K}$ endlicher Körper der Charakteristik p)
Behauptung: $\bar{G} = \mathrm{Gal}(\bar{K}|\mathbb{F}_p)$ ist isomorph zu $G_\mathfrak{p} := \{\sigma \in G \big| \mathfrak{p}^\sigma = \mathfrak{p}\}$. („Zerlegungsgruppe") als Permutationsgruppe von $W_{\bar{f}}$ bzw. W_f.

Beweis. O.B.d.A. $a_n = 1$ [sonst ersetze $\mathbb{Z}$ durch $\mathbb{Z}_p$].
$G_\mathfrak{p}$ operiert auf $W_{\bar{f}}$ durch $\bar{\alpha}_i^\sigma = (\alpha_i + \mathfrak{q})^\sigma = \alpha_i^\sigma + \mathfrak{p}$ $(\sigma \in G_\mathfrak{p})$.
Sei $\bar{K} = \mathbb{F}_p(\bar{\beta})$ ($\bar{\beta}$ existiert; $\bar{K}^*$ zyklisch). Finde $\beta \in R$ mit

$$\beta + \mathfrak{p} = \bar{\beta}, \quad \beta \equiv 0(\mod \mathfrak{p}^\sigma), \quad \sigma \in G \setminus G_\mathfrak{p} \quad \text{(Chinesischer Restesatz)}.$$

Betrachte: $h = \prod_{\sigma \in G}(X - \beta^\sigma) \in \mathbb{Z}[X]$ (Vietá + ganz Algebraischhut).

$$\hat{h} = h \mod p [= h \mod \mathfrak{p}] = X^{|G|-|G_\mathfrak{p}|} \cdot \prod_{\sigma \in G_\mathfrak{p}} (X - \hat{\beta}^\sigma); \quad \hat{\beta}^\sigma = \beta^\sigma + \mathfrak{p} \ (\sigma \in G_\mathfrak{p}) \in \mathbb{F}_p[X].$$

G operiert transitiv auf den Wurzeln $\neq 0$ von $\bar{h}$ und $\bar{h}(\bar{\beta}) = 0$.
Die Zuordnung $G_\mathfrak{p} \to \bar{G}$ auf W_f bzw. $W_{\hat{f}}$ ist injektiv. ■

Definition. Sei $p \in \mathbb{P}, p \nmid a_n d(f)$; dann gibt es $\sigma_p \in G$ mit $\mathfrak{p}^\sigma = \mathfrak{p}$ für $\mathfrak{p}$ maximal in R mit $\mathfrak{p} \supseteq pR$, so dass σ_p den „Frobenius" $\bar{\beta} \mapsto \bar{\beta}^p$ in $R/\mathfrak{p} (= \bar{K})$ erzeugt (Lemma 2). Nach Lemma 1 ist σ_p bestimmt bis auf G-Konjugiertheit, und die Klasse heißt der „Frobenius" zu p in G.

Satz. *Sei $C \subseteq G$ eine normale Teilmenge (=Vereinigung von Konjugiertenklassen von G).*
Sei

$$\mathbb{P}_C = \{p \in \mathbb{P} \mid p \nmid a_n d(f), \sigma_p \in C\}$$

Dann

$$\delta_0(\mathbb{P}_C) = \frac{|C|}{|G|} = \frac{|C|}{[K : \mathbb{Q}]} \text{ existiert.}$$

Literatur: Neukirch (Algebrische Zahlentheorie): S. 569. (für δ statt δ_0)

Beispiel 1. (vgl. Übung 52): Sei $f = \Phi_m$; $\varepsilon = e^{\frac{2\pi i}{m}}, K = \mathbb{Q}(\varepsilon), R = \mathbb{Z}[\varepsilon]$ $(a_n = 1)$.
$p \in \mathbb{P}$ $p \nmid d(\Phi) \iff p \nmid m$.
$[\Phi_m \big| X^m - 1,\ (X^m-1)' = mX^{m-1}]$ $G = \mathrm{Gal}(K|\mathbb{Q}) \cong G(m)$ (abelsch); $\sigma_p : \varepsilon \mapsto \varepsilon^p$ $(p \nmid m)$.
Ordne a das Element $a + m\mathbb{Z} \in G(m)$ bzw. $\hat{a} : \varepsilon \mapsto \varepsilon^a$ in G zu $(C = \{\hat{a}\})$

$$\mathbb{P}_{\hat{a}} = \{p \in \mathbb{P} \big| p \nmid m,\ \varepsilon^p = \varepsilon^a = \varepsilon^{a+m\mathbb{Z}}\} = \mathbb{P}_a.$$

D.h.: Chebotarev $\Rightarrow$ Dirichlet.

Beispiel 2. Sei $C = \{1\} \subseteq G$; dann $P_{\{1\}} = \{p \in \mathbb{P} \big| p \nmid a_n d(f),\ f \mod p$ zerfällt über $\mathbb{F}_p$ in Linearfaktoren$\}$.
Also hat $\mathbb{P}_f = \{p \in \mathbb{P} \big| f \mod p$ zerfällt $\}$ die Dichte $\delta_0(\mathbb{P}_f) = \frac{1}{[K:\mathbb{Q}]}$.
Konkret: (vgl. (14.6): $f = X^2 - a,\ a \in \mathbb{Z}$ kein Quadrat in $\mathbb{Z}$. Dann $K = \mathbb{Q}(\sqrt{a})$ quadratisch,

$$\mathbb{P}_f \setminus \{2;\ \text{Primteiler von } a\} = \{2 \neq p \in \mathbb{P} \big| \left(\frac{a}{p}\right) = 1\}$$

hat Dichte $\frac{1}{2}$.

14 Quadratische Zahlkörper

Für $0 \neq a \in \mathbb{R}$ sei

$$\sqrt{a} = e^{\frac{1}{2}\log a} = \begin{cases} +\sqrt{a}, & a > 0 \\ i_+\sqrt{|a|}, & a < 0 \end{cases}$$

(log = Hauptzweig von log. Argumente $(-\pi, \pi]$) $[\log(-1) = \pi i]$

(14.1) Lemma. *Sei $K (\subseteq \mathbb{C})$ ein quadratischer Zahlkörper, d.h. $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K = 2$.*
Dann gibt es genau ein eindeutig bestimmtes quadratfreies $d \in \mathbb{Z} \setminus \{0, 1\}$ mit $K = \mathbb{Q}(\sqrt{d})$.

Beweis. **Existenz**
Wähle $d \in K \setminus \mathbb{Q}$; dann $\{1, \alpha\}$ $\mathbb{Q}$-Basis von $K\big([K : \mathbb{Q}] = \dim_{\mathbb{Q}} K = 2\big)$.
Also $1, \alpha, \alpha^2$ $\mathbb{Q}$-linear-Abhängig, damit $\alpha^2 = a \cdot \alpha - b \cdot 1$ mit $a, b \in \mathbb{Q}$. $(\alpha^2 - a \cdot \alpha + b = 0)$
D.h.: α Wurzel von $f = X^2 - aX + b \in \mathbb{Q}[X]$.
Über K:

$$f = (X - \alpha)(X - \alpha') \quad [= X^2 - (\alpha + \alpha')X + \alpha\alpha' \;]$$

wobei α' die „Konjugierte“ von α ist. ($K = \mathbb{Q}(\alpha); \alpha \mapsto \alpha'$ erzeugt $\mathrm{Gal}(K|\mathbb{Q})$)

$$\left.\begin{array}{ll} \text{Norm:} & \alpha\alpha' = b \\ \text{Spur:} & \alpha + \alpha' = a \end{array}\right\} \text{(Vieta)}$$

Diskrimiante

$$d(f) := (\alpha - \alpha')^2 = (\alpha + \alpha')^2 - 4\alpha\alpha' = a^2 - 4b$$

Es ist $K = \mathbb{Q}(\alpha - \alpha') = \mathbb{Q}(\sqrt{a^2 - 4b})$, denn wäre $\underset{+\alpha+\alpha'}{\alpha - \alpha'} \in \mathbb{Q}$, so wäre $2\alpha \in \mathbb{Q}, \alpha \in \mathbb{Q}$
Schreibe $a^2 - 4b = \frac{r}{s} = \frac{r \cdot s}{s^2}$ mit $r, s \in \mathbb{Z}$; nenne d den quadratfreien Anteil von rs.
Eindeutigkeit:
Sei auch $K = \mathbb{Q}(\sqrt{d'})$ mit $d' \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Dann

$$\begin{aligned} \sqrt{d'} &= x + y\sqrt{d} \text{ mit } x, y \in \mathbb{Q} \text{ (eindeutig)} \\ d' &= x^2 + dy^2 + 2xy\sqrt{d} \Longrightarrow \underset{(2\neq 0)}{2xy} = 0; \end{aligned}$$

$$\begin{aligned} x = 0 &\Rightarrow d' = dy^2, d' = d \\ y = 0 &\Rightarrow d' = x^2 \text{ (Widerspruch)} \end{aligned}$$

∎

(14.2) Lemma. *Sei $2 \neq p \in \mathbb{P}$; sei ε eine primitive p-te Einheitswurzel, sei*

$$\tau = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \varepsilon^a \text{ („Gaußsche Summe“)}$$

(a) $\tau^2 = (\frac{-1}{p})p = (-1)^{\frac{p-1}{2}}p =: p^*$ *(„Primdiskriminante“)*

(b) $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p^*})$ *ist der einzige quadratische Zahlkörper in* $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\mu_p)$

Beweis. (a) Es gilt

$$1 + \varepsilon + \cdots + \varepsilon^{p-1} = \frac{\varepsilon^p - 1}{\varepsilon - 1} = 0; \quad \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0 \quad (\mathbb{F}_p^* : \mathbb{F}_p^{*^2} \mid = 2)$$

Ferner für jedes $b \in \{1, \ldots, p-1\}$ $(b \in G(p))$:

$$\tau = \sum_{\substack{a \in G(p) \\ [=\mathbb{F}_p^*]}} \left(\frac{a}{p}\right) \varepsilon^a = \sum_{a \in G(p)} \left(\frac{ab}{p}\right) \varepsilon^{ab}$$

Damit:

$$\begin{aligned}
\tau^2 &= \sum_{b \in G(p)} \sum_{a \in G(p)} \left(\frac{a}{b}\right) \left(\frac{a \cdot b}{p}\right) \varepsilon^b \varepsilon^{ab} = \sum_{a,b} \underbrace{\left(\frac{ab^2}{p}\right)}_{=(\frac{a}{b})} \varepsilon^{(a+1)b} \\
&= \sum_{b=1}^{p-1} \left(\frac{-1}{p}\right) \varepsilon^0 + \sum_{a \neq -1} \left(\frac{a}{p}\right) \underbrace{\sum_{b=1}^{p-1} \varepsilon^{(a+1)b}}_{=-1} \\
&= \left(\frac{-1}{p}\right) p - \underbrace{\sum_{a=1}^{p-1} \left(\frac{a}{b}\right)}_{=0}
\end{aligned}$$

(b) Folgt aus (a) und der zyklizität von $G(p) \cong \mathbb{F}_p^*$ [plus Galoistheorie]

$\blacksquare$

Bemerkung. Sei $\varepsilon = e^{\frac{2\pi i}{p}}$; was ist τ $(\tau = \underset{(-)}{+}\sqrt{p^*}!)$
Vorzeichen? [Gauß hat sich mit dieser Frage 4 Jahre lang beschäftigt (1801-1805)]

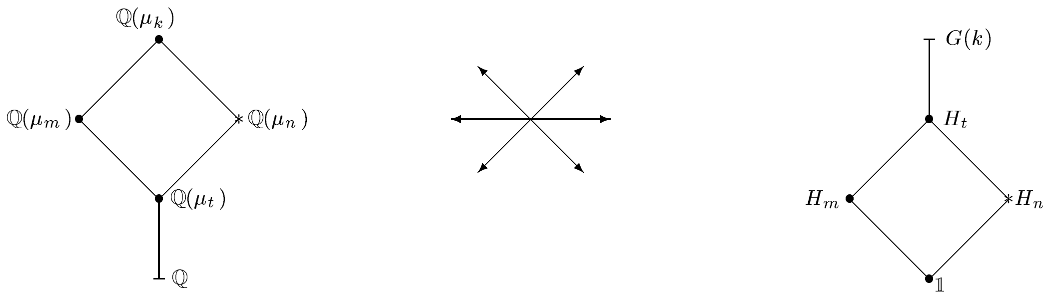
Beispiel.

$$\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{3^*}) = \mathbb{Q}(\mu_3); \quad \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\mu_3)(i)$$
$$\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\mu_5); \quad \mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(\mu_{17})$$

(14.3) Lemma. *Für* $m, n \in \mathbb{N}_{\geq 3}$ *gilt*

$$\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{(m,n)})$$

Beweis. (Galoistheorie) Klar: „$\supseteq$"
Setze $t = (m,n) = \mathrm{ggT}(m,n),\ k = \mathrm{kgV}(m,n)$



Sei $H_m = \ker\big(G(k) \twoheadrightarrow G(m)\big)$, analog H_n, H_f
Klar: $H_m H_n \subseteq H_t$
Es existieren $y, z \in \mathbb{Z}$ mit $t = ym + zm$. Also

$$s = 1 + xym + xzn$$

Setze $a = 1 + xym,\ b = 1 + xzn$, dann $a \cdot b = s + x^2 yzmn$
Damit (Restklassen):

$$a \in H_m, b \in H_n \text{ und } ab „=" s.$$

■

(14.4) Satz. *Zu jedem quadratischen Zahlkörper K gibt es eine kleinste Nummer $m = f(K)$ mit der Eigenschaft $K \subseteq \mathbb{Q}(\mu_m)$.*
Ist $\mathbf{K} = \mathbb{Q}(\sqrt{\mathbf{d}})$ mit $d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei, so ist der „Führer":

$$f(K) = \begin{cases} |d|, & \textit{falls } d \equiv 1 \pmod 4 \\ 4|d| & \textit{sonst} \end{cases}$$

Beweis. (a) Ordne $2 \neq p \in \mathbb{P}$ die Primdiskriminante $p^* = (-1)^{\frac{p-1}{2}} p$ zu (14.2); $p^* \equiv 1 \pmod 4$
Ferner $2^* \in \{-4, 8, -8\}$ (Primdiskriminante zu 2).
Sei $|d| = p_1 \cdot p_r$ PFZ.
1.Fall: $d \equiv 1 \pmod 4$
Dann $d = p_1^* \cdots p_r^*$ (eindeutig). Nach Lemma (14.2) ist

$$\mathbb{Q}(p_i^*) \subseteq \mathbb{Q}(\mu_{p_i}),\ i = 1, \ldots, r$$

Also

$$K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\mu_{|d|}).$$

2. Fall: $d \equiv 3 \pmod 4$
Dann ist $d = -p_1^* \cdots p_r^*$;

$$K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{4d}) = \mathbb{Q}(i\sqrt{p_1^* \cdots p_r^*}) \subseteq \mathbb{Q}(\mu_{4|d|})$$

($4d = 2^* p_1^* \cdots p_r^*$ mit $2^* = -4$.)
3. Fall: $d \equiv 2 \pmod 4$
Sei etwa $p_1 = 2$. Ist $\frac{d}{2} \equiv 1 \pmod 4$, so ist $\frac{d}{2} = p_2^* \cdots p_r^*$ und

$$K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}\left(\sqrt{\frac{d}{4}}\right) \subseteq \mathbb{Q}(\mu_{8 \cdot |\frac{d}{2}|}) \subseteq \mathbb{Q}(\mu_{4|d|})$$

Ist $\frac{d}{2} \equiv 3 \pmod 4$, so ist $\frac{d}{2} = -p_2^* \cdots p_r^*$ und

$$K = \mathbb{Q}\left(\sqrt{\frac{d}{4}}\right) = \mathbb{Q}(\mu_8, \mu_{\frac{|d|}{4}}) = \mathbb{Q}(\mu_{4|d|})$$

(b) **Minimalität:**
Setze

$$D = \begin{cases} |d|, & d \equiv 1 \pmod 4 \\ 4|d| & \text{sonst} \end{cases}$$

D hat eine eindutige Prim*-Zerlegung:

$$D = p_1^* \cdot \dots \cdot p_r^*$$

mit Primzahlen $p_1 < p_2 < \dots < p_r$ (anders als in (a)). Dabei ist für

$$\begin{aligned} d &\equiv 3 \pmod 4 : p_1 \text{ und } p_1^* = -4 \\ d &\equiv 2 \pmod 4 : p_1 = 2 \text{ und } p_1^* = \begin{cases} +8, & \frac{d}{2} \equiv 1 \pmod 4 \\ -8, & \frac{d}{2} \equiv 3 \pmod 4 \end{cases} \end{aligned}$$

Nach (14.3) und a)

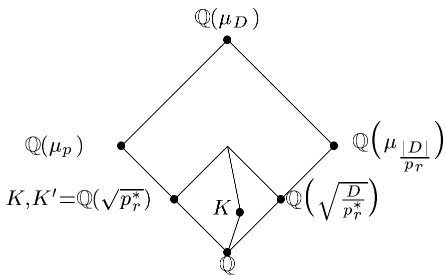
$$f(K) \big| |D|$$

Zeige: $f(K) = |D|$
Induktion nach r: $r = 1$: Wende (14.2) bzw. (11.8) [für $p_1 = 2$] an.
Sei $r > 1$.
Annahme:

$$K \subseteq \mathbb{Q}(\mu_{\frac{|D|}{p_r}}).$$

Sei $K' = \mathbb{Q}(\sqrt{\frac{D}{p_1^*}})$; nach Induktionsvoraussetzung

$$f(K') = \mathbb{Q}(\frac{\mu_{|D|}}{p_r})$$



Es gilt

$$\sqrt{\frac{D}{p_r^*}} \cdot \sqrt{p_r^*} = \pm\sqrt{D};$$

also

$$K' \cdot \mathbb{Q}(\sqrt{p_r^*}) = \mathbb{Q}(\sqrt{D}) = K$$

Also liegt

$$K \not\subseteq \mathbb{Q}(\mu_{\frac{|D|}{p_r}}) \qquad \text{(Widerspruch)}$$

■

(14.5) Definition. Sei $d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei. Ordne $K = \mathbb{Q}(\sqrt{d})$ zu.

(i) Diskriminante

$$D_K = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d, & \text{sonst} \end{cases}$$

Bemerkung: $K = \mathbb{Q}(\sqrt{D})$ und $f(K) = |D_K|$ (14.4).

(ii) Polynom

$$f_K = \begin{cases} X^2 - X + \frac{1-d}{4}, & d \equiv 1 \pmod 4 \\ X^2 - d & \text{sonst.} \end{cases}$$

Bemerkung: $d(f_K) = D_K$ (und $K = \mathbb{Q}(\sqrt{D_K})$)

(iii) Ring

$$R_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{sonst} \end{cases}$$

Bemerkung: R_K heißt (ist) der Ring aller ganzen algebraischen Zahlen in K.

Beispiele:. $d = -1$, $K = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[e^{\frac{2\pi i}{4}}] = \mathbb{Z}[i]$ Ring der ganzen Gaußschen Zahlen (Hauptidealring).
$d = -3 : R_K = \mathbb{Z}[\frac{1+\sqrt{-2}}{2}] = \mathbb{Z}[e^{\frac{2\pi i}{3}}]$ (Hauptidealring)
$d = 2 : R_K = \mathbb{Z}[\sqrt{2}]$ (Hauptidealring)
$d = -5 : R_K = \mathbb{Z}[\sqrt{-5}]$ **kein** Hauptidealring, denn $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ Produkte von unzerlegbaren Elementen in R_K.

(14.6) Satz. *Sei $K = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei; $D = D_K$*
Es gibt genau einen Dirichlet-Charakter $\chi = \chi_0 = \chi_K \mod |D|$ mit

$$\chi(p) = (\frac{d}{p}) = (\frac{D}{p})$$

für alle ungeraden $p \in \mathbb{P}$ $(p \nmid d)$. Es ist χ primitiv ($\bmod |D|$) und quadratisch (reell) und es gilt:

(a)
$$\chi \textit{ gerade } [\chi(-1) = 1] \iff d > 0 \quad [K \textit{ reell }]$$

(b)
$$\chi(2) = \begin{cases} 1, & d \equiv 1 \pmod 8 \\ -1, & d \equiv 5 \pmod 8 \\ 0 & \textit{sonst} \end{cases}$$

Beweis. **(Eindeutigkeit):**

$$G(|D|) = \langle p \mod |D| \big| p \in \mathbb{P}, p \neq 2, p \nmid |d| \rangle$$

Damit ist χ durch die genannte Forderung bestimmt.
(Existenz): Prim*-Zerlegung:

$$D = p_1^* \cdot \ldots \cdot p_r^* \quad (p_1 < \cdots < p_r \text{ Primzahlen})$$

Seien ε, ω auf ungeraden ganzen Zahlen erklärt ($\bmod 2\mathbb{Z}$) wie in (11.8).
$[\varepsilon(n) = \frac{n-1}{2} \mod 2;\ \omega(n) = \frac{n^2-1}{8} \mod 2]$

1. Fall: $D = d$ $(d \equiv 1 \pmod 4)$
Definiere
$$\chi = (\frac{\cdot}{p_1}) \cdot \ldots \cdot (\frac{\cdot}{p_r}).$$
χ ist quadratisch und primitiv $\bmod |D|$ (Chinesischer Restesatz)
Für $p \in \mathbb{P}, p \neq 2, p \nmid D$ gilt nach dem Quadratischen Reziprozitätzgesetz:

$$\begin{aligned} \chi(p) &= (\frac{p}{p_1}) \cdot \ldots \cdot (\frac{p}{p_r}) = (-1)^{\varepsilon(p)\cdot\varepsilon(p_1)}(\frac{p_1}{p}) \cdot \cdots \cdot (-1)^{\varepsilon(p)\varepsilon(p_r)}(\frac{p_r}{p}) \\ &= (-1)^{\varepsilon(p)\varepsilon(|D|)}(\frac{|D|}{p}) = (\frac{D}{p}) \quad [D > 0; D < 0: \text{ 1. Ergänzungsgesetz}] \end{aligned}$$

Ferner:

$$\chi(-1) = (\frac{-1}{p_1}) \cdot \ldots \cdot (\frac{-1}{p_r}) = (-1)^{\varepsilon(p_1)+\cdots+\varepsilon(p_r)} = (-1)^{\varepsilon(|D|)} = \begin{cases} 1, & |D| = D \\ -1, & |D| = -D \end{cases}$$

$$\chi(2) = (\frac{2}{p_1}) \cdot \ldots \cdot (\frac{2}{p_r}) = (-1)^{\omega(p_1)+\cdots+\omega(p_r)} = (-1)^{\omega(|D|)} = \begin{cases} 1 & d \equiv 1 \pmod 8 \\ -1 & d \equiv 5 \pmod 8 \end{cases}$$

2. Ergänzungsgesetz.

2. Fall: $d \equiv 3 \pmod 4$; $p_1^* = -4$
Definiere:
$$\chi = (-1)^{\varepsilon}(\frac{\cdot}{p_2}) \cdot \ldots \cdot (\frac{\cdot}{p_r})$$

χ quadratisch, primitiv $\mod 4|d| = |D|$.
Für $p \in \mathbb{P}, p \nmid D$ gilt mit dem Quadratischen Reziprozitätsgesetz [plus Ergänzungsgesetz]

$$\begin{aligned}\chi(p) &= (-1)^{\varepsilon(p)}\big(\frac{p}{p_2}\big)\cdot\ldots\cdot\big(\frac{p}{p_r}\big) \\ &= (-1)^{\varepsilon(p)}\cdot(-1)^{\varepsilon(p)\varepsilon(p_2\cdot\ldots\cdot p_r)}\cdot\big(\frac{p_2\cdot\ldots\cdot p_r}{p}\big) \overset{!}{=} \big(\frac{D}{p}\big) \quad [p_2\cdot\ldots\cdot p_r = |d|]\end{aligned}$$

Es gilt:

$$\begin{aligned}\chi(-1) &= (-1)^{\varepsilon(-1)}(-1)^{\varepsilon(p_2\cdot\ldots\cdot p_r)} = (-1)\cdot(-1)^{\varepsilon(|d|)} = \begin{cases}1, & d>0\\ -1, & d<0\end{cases} \\ \chi(2) &= (-1)^{\varepsilon(2)}\big(\frac{2}{p_2}\big)\cdot\ldots\cdot\big(\frac{2}{p_r}\big) = 0\end{aligned}$$

3. Fall: $d \equiv 2 \pmod 4$
Hier ist $p_1 = 2$ und $p_1^* = \pm 8$, $|D| = 4|d| = 8\cdot p_2\cdot\ldots\cdot p_r$. Nach dem Chinesischen Restesatz gilt:

$$G(|D|) \cong G(8)\times G(p_2)\times\cdots\times G(p_r)$$

Ist $p_1 = 8$ $[\frac{d}{2} \equiv 1 \pmod 4]$, so definiere $\chi = \chi_0$ durch

$$\chi = (-1)^{\omega}\cdot\big(\frac{\cdot}{p_2}\big)\cdot\ldots\cdot\big(\frac{\cdot}{p_r}\big)$$

χ ist primitiv $\mod |D|$ und quadratisch. Für $p \nmid D$ gilt mit (QR)[11]:

$$\begin{aligned}\chi(p) &= (-1)^{\omega(p)}\big(\frac{p}{p_2}\big)\cdot\ldots\cdot\big(\frac{p}{p_r}\big) \\ &= (-1)^{\omega(p)}(-1)^{\varepsilon(p)(\varepsilon(p_2)+\cdots+\varepsilon(p_r))}\big(\frac{p_2}{p}\big)\cdot\ldots\cdot\big(\frac{p_r}{p}\big) \\ &= (-1)^{\omega(p)}(-1)^{\varepsilon(p)\varepsilon(\frac{|d|}{2})}\underbrace{\underbrace{\left(\frac{\frac{|d|}{2}}{p}\right)}_{=\left(\frac{2|d|}{p}\right)}}_{=(-1)^{\omega(p)}\left(\frac{|d|}{p}\right)} \\ &= (-1)^{\varepsilon(p)\varepsilon\left(\frac{|d|}{2}\right)}\big(\frac{|d|}{p}\big) = \big(\frac{d}{p}\big) \qquad [d>0; d<0]\end{aligned}$$

Es ist $\chi(2) = 0$ [wegen $2|d$] und

$$\begin{aligned}\chi(-1) &= \underbrace{(-1)^{\omega(-1)}}_{=1}\big(\frac{-1}{p_2}\big)\cdots\big(\frac{-1}{p_r}\big) \\ &= (-1)^{\varepsilon\left(\frac{|d|}{2}\right)} = \begin{cases}1, & d>0\\ -1, & d<0\end{cases}\end{aligned}$$

[11] Quadratisches Reziprozitätzgesetz, (11.9)

Ist $p_1 = -8$ [$\frac{d}{2} \equiv 3 \pmod 4$], so definiere

$$\chi = (-1)^{\omega+\varepsilon}\Big(\frac{\cdot}{p_2}\Big)\cdots\Big(\frac{\cdot}{p_r}\Big)$$

■

(14.7) Anwendung (vergl. 13.7). Sei $d \in \mathbb{Z}$ kein Quadrat in $\mathbb{Z}$ und

$$Q = \{p \in \mathbb{P} \,\big|\, p \neq 2, \Big(\frac{d}{p}\Big) = 1\}$$

Behauptung: $\delta_0(Q) = \frac{1}{2}$ (existiert).

Beweis. o.B.d.A.: d quadratfrei; $d \neq 0,\ 1$. Sei

$$D = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d & \text{sonst.} \end{cases}$$

und $\chi = \chi_0$ wie in (14.6). Sei $H = \ker(\chi)$,

$$\chi : G(|D|) \twoheadrightarrow \{\pm 1\}$$

Also

$$|G(|D|) : H| = 2.$$

Ferner:

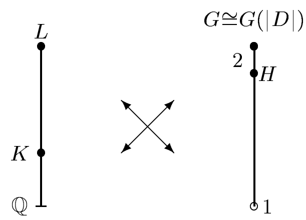
$$Q = \bigcup_{a \in \ker(\chi) = H} \mathbb{P}_{a,|d|}$$

Wende (13.7) an. [$|H| \cdot \frac{1}{\varphi(|D|)} = \frac{1}{2}$] ■

(14.8) Satz. *Sei K quadratischer Zahlkörper, $D = D_K$ [also $K = \mathbb{Q}(\sqrt{D})$] und $\chi = \chi_K$ der „K zugeordnete Dirichlet-Charakter“ [Kronecker-Charakter]*
Sei $L = \mathbb{Q}(\mu_{|D|})$ und identifiziere $G = \mathrm{Gal}(L|\mathbb{Q}) = G(|D|)$.
Behauptung: *K ist der durch $H = \ker(\chi)$ bestimmte Teilkörper von L.*
[Galoiskorrespondenz]

Beweis. Sei $p \in \mathbb{P}, p \nmid D$; $\sigma_p =$ Frobenius zu p;
d.h. $\sigma_p : \varepsilon \mapsto \varepsilon^p$ für primitive $|D|$-te EHW[12].
($\sigma_p \leftrightarrow p \mod |D|$)
Wir wissen:

$$\begin{cases} |G : H| = 2;\ \text{zu zeigen: } K \subseteq \mathrm{Fix}_H(L) \\ K \subseteq L \end{cases}$$



[12] Einheitswurzel

$$
\begin{aligned}
K \text{ elementweise fest unter } \sigma_p &\iff \sqrt{D}^{\sigma_p} = \sqrt{D} \\
&\underset{(13.7)}{\iff} X^2 - D \text{ zerfällt über } \mathbb{F}_p \text{ in Linearfaktoren} \\
&\iff \left(\frac{D}{p}\right) = 1 \iff p \mod |D| \in \ker(\chi)
\end{aligned}
$$

■

(14.9) Anhang (Quadratisches Reziprozitätsgesetz). *Für ungerade Primzahlen $p \neq q$ gilt*

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

Beweis. Sei ε eine primitive p-te EHW $\underset{(q\neq p)}{\text{über}}$ $\mathbb{F}_q$,

$$\tau = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\varepsilon^a \quad \text{(Gaußsche Summe)}$$

Nach (14.2)

$$\tau^2 = (-1)^{\frac{p-1}{2}}p \quad (\in \mathbb{F}_q)$$

Andererseits

$$
\begin{aligned}
\tau^q &= \sum_{a=1}^{p-1}\underbrace{\left(\frac{a}{p}\right)^q}_{\substack{=(\frac{a}{p}) \\ [q\neq 2]}}\varepsilon^{aq} = \sum_{a=1}^{p-1}\underbrace{\left(\frac{a\cdot q^{-1}}{p}\right)}_{=(\frac{a}{p})\cdot(\frac{q}{p})}\varepsilon^a \\
&= \left(\frac{q}{p}\right)\tau.
\end{aligned}
$$

Euler - Kriterium:

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

■

15 Zeta - Funktionen quadratischer Zahlkörper

K quadratischer Zahlkörper, $D = D_K$ [also $K = \mathbb{Q}(\sqrt{D})$], $\boldsymbol{\chi = \chi_K}$; $f = f_K$, $R = R_K$

(15.1) Stellen („Bewertungen“). (a)

$$
\begin{aligned}
K \text{ reell } &:\iff D > 0 \;\; [2 \text{ Einbettungen } K \hookrightarrow \mathbb{R}] \\
K \text{ imaginär } &:\iff D < 0 \;\; [1 \text{ Einbettung } K \hookrightarrow \mathbb{C}]
\end{aligned}
$$

(b) Sei $\mathbb{P}_K$ die Menge aller maximalen Ideale [Primideale $\neq 0$] von R
(Jedes $\mathfrak{p} \in R_K$ bestimmt eine $\mathfrak{p}$-adische Stelle in K)

Bemerkung. (ohne Beweis). $R = R_K$ ist ein sogenannter Dedekindring [ZPI - Ring]; d.h.
Jedes Ideal $\mathfrak{A} \neq 0$ von R hat eindeutige Darstellung

$$\mathfrak{A} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}, \quad n_\mathfrak{p} \in \mathbb{N},$$

fest unter $n_\mathfrak{p} = 0$.

(15.2) Norm. Für ein Ideal $\mathfrak{A} \neq 0$ von R definiere $N(\mathfrak{A}) := |R/\mathfrak{A}|$
Wohldefiniert:

$$N(\mathfrak{A}) \in \mathbb{N}_{>0}.$$

Es gibt $0 \neq \alpha \in \mathfrak{A}$; es ist $R \cap \mathbb{Q} = \mathbb{Z}$.
Ist $\alpha = \pm n,\ n \in \mathbb{N}_{>0}$, so ist $n \in \mathfrak{A}\ nR \subseteq \mathfrak{A}$
Wegen $R^+ \cong \mathbb{Z} \oplus \mathbb{Z}$ ist $|R/nR| = n^2$, also $|R/\mathfrak{A}| \leq n^2$.
Sei $\alpha \notin \mathbb{Z}$, $(0 \neq \alpha \in \mathfrak{A})$

$$\alpha = \begin{cases} a + b\frac{1+\sqrt{d}}{2} & ,d = D \equiv 1(4) \\ a + b\sqrt{d} & ,d = \frac{D}{4} \not\equiv 1(4) \end{cases} \quad (a, b \in \mathbb{Z})$$

Dann ist

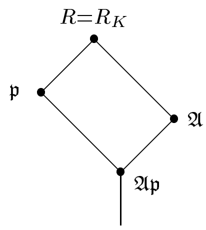
$$\alpha' = \begin{cases} a + b\frac{1-\sqrt{d}}{2} \\ a - d\sqrt{d} \end{cases} \qquad \text{(konjugiert)}\ ; \quad 0 \neq \alpha' \in R$$

„Norm“

$$N(\alpha) := \alpha\alpha' \in \mathbb{Z} \setminus \{0\}; \quad \alpha\alpha' \in \alpha R \subseteq \mathfrak{A}.$$

(15.3) Lemma. *Für Ideale* $\mathfrak{A},\ \mathfrak{b}\ (\neq 0)$ *von* R *gilt*

$$N(\mathfrak{A}\mathfrak{b}) = N(\mathfrak{A}) \cdot N(\mathfrak{b}).$$



Beweis. O.B.d.A.: $\mathfrak{b} = \mathfrak{p} \in \mathbb{R}_K$ (wegen ZPI).
$\mathfrak{A}/\mathfrak{A}\mathfrak{p}$ ist ein einfacher R-Modul via Rechtsmultiplikation (wegen ZPI), der von $\mathfrak{p}$ annuliert wird, d.h. $\mathfrak{A}/\mathfrak{A}\mathfrak{p}$ ist $R/\mathfrak{p}$-Modul ($R/\mathfrak{p}$ Körper; $R/\mathfrak{p}$-Vektorraum).

$$(a + \mathfrak{A}\mathfrak{p})(x + \mathfrak{p}) = ax + \mathfrak{A}\mathfrak{p}.$$

Also

$$\dim_{R/\mathfrak{p}} \mathfrak{A}/\mathfrak{A}\mathfrak{p} = 1, \text{ also } |\mathfrak{A}/\mathfrak{A}\mathfrak{p}| = |R/\mathfrak{p}| = N(\mathfrak{p})$$

Damit

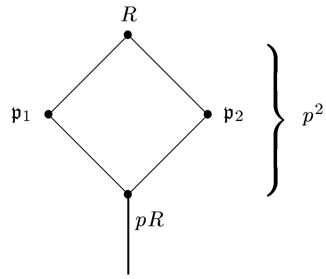
$$N(\mathfrak{A}\mathfrak{p}) = |R/\mathfrak{A}\mathfrak{p}| = |R/\mathfrak{A}| \cdot |\mathfrak{A}/\mathfrak{A}\mathfrak{p}| = N(\mathfrak{A}) \cdot N(\mathfrak{p}).$$

■

(15.4) Lemma. *(a) Ist $\mathfrak{p} \in \mathbb{P}_K$, so ist $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für (genau) ein $p \in \mathbb{P}$* $(\mathfrak{p}/p)$[13]

(b) Ist $p \in \mathbb{P}$, so ist $N(pR) = |R/pR| = p^2$, also

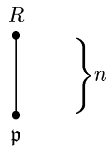
$$pR = \begin{cases} \mathfrak{p} \in \mathbb{P}_K & (\text{„Zerfällung“}) \\ \mathfrak{p}_1\mathfrak{p}_2 \text{ mit } \mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ in } \mathbb{P}_K & (\text{„Zerfällung“}) \\ \mathfrak{p}^2 \text{ mit } \mathfrak{p} \in \mathbb{P}_K & (\text{„Verzweigung“}) \end{cases}$$



Beweis.

(a) $N(\mathfrak{p}) = n \in \mathbb{N}_{>0}$, also $n = n \cdot 1 \in \mathfrak{p} \cap \mathbb{Z} \neq \{0\}$
Ferner ist $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$ Primideal von $\mathbb{Z}$.
$[x, y \in \mathbb{Z} \setminus (\mathfrak{p} \cap \mathbb{Z}) \subseteq R\mathfrak{p} \Rightarrow xy \in R/\mathfrak{p}]$
Noch: $\mathbb{Z}$ ist Hauptidealring.

(b) Folgt wegen (ZPI).



■

(15.5) Lemma. *Sei $p \in \mathbb{P}$*

(a) p ist prim („träge“) in R (oder K) $:\Longleftrightarrow pR = \mathfrak{p} \in \mathbb{P}_K \Longleftrightarrow \chi(p) = -1$
In diesem Fall ist $N(\mathfrak{p}) = p^2$.

(b) p zerfällt in $R \Longleftrightarrow pR = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathbb{P}_K \Longleftrightarrow \chi(p) = 1$
In diesem Fall ist $N(\mathfrak{p}_i) = p,\ i = 1, 2, \ldots$

(c) p verzweigt in $R :\Longleftrightarrow pR = \mathfrak{p}^2 \Longleftrightarrow \chi(p) = 0 \quad [\Longleftrightarrow \quad p | D_K = D]$
In diesem Fall ist $N(\mathfrak{p}) = p$.

Beweis. Es ist

$$\mathbb{Z}[X]/(f_K) \cong R \ \ (\text{via} \quad X \mapsto \begin{cases} \frac{1+\sqrt{d}}{2} & D = d \\ \sqrt{d} & D = 4d \end{cases})$$

Also

$$\boxed{R/\mathfrak{p}R \cong \mathbb{F}_p[X]/(\bar{f}_K)}\,, \quad \bar{f}_K = f_K \mod p$$

[13] endliche Integritätsbereiche sind Körper

1. Fall: $D = d \equiv 1 \pmod 4$
Dann
$$f = f_K = X^2 - X + \frac{1-d}{4}.$$

$\mathbf{p = 2}$:

$$\bar{f} = f \mod 2 = \begin{cases} X^2 + X + 1, & d \equiv 5 \pmod 8 \leftrightarrow \chi(2) = -1 \\ \underbrace{X^2 + X}_{X(X+1)}, & d \equiv 1 \pmod 8 \leftrightarrow \chi(2) = 1 \end{cases}$$

Wende (14.6) an.
$\mathbf{p \neq 2}$:

$$\bar{f} = f \mod p = (X - \frac{1}{2})^2 = \frac{\bar{d}}{4} = \begin{cases} \text{irreduzibel über } \mathbb{F}_p, \text{ falls } \chi(p) = \left(\frac{d}{p}\right) = -1 \text{ zerfallend} \\ \text{über } \mathbb{F}_p \text{ (verschiedene Linearfaktoren), falls} \\ \chi(p) = \left(\frac{d}{p}\right) = 1 \quad (p \nmid d) \\ \\ (X - \frac{1}{2})^2 \quad \text{falls } p|d \end{cases}$$

2. Fall: $D = 4d \quad (d \equiv 2, 3 \pmod 4)$. Hier $f = X^2 - d$.
$\mathbf{p = 2}$:

$$\bar{f} = f \mod 2 = \left\{ \begin{array}{ll} X^2 + 1 = (X+1)^2 & , d \equiv 3 \pmod 4 \\ X^2 & , d \equiv 2 \pmod 4 \end{array} \right\} \text{Verzweigung!}$$

$\mathbf{p \neq 2}$:

$$\bar{f} = X^2 - \bar{d} = \begin{cases} (X - \bar{a})(X + \bar{a}), & \bar{a} \neq -\bar{a}, \text{ falls } \chi(p) = (\frac{d}{p}) = 1 \quad \text{„Zerfällung“)} \\ \text{irred. über } \mathbb{F}_p, & \text{falls } \chi(p) = (\frac{d}{p}) = -1 \text{ („Trägheit“)} \\ X^2, & \text{falls } p|d \quad \chi(p) = 0 \text{ („Verzweigung“)} \end{cases}$$

■

(15.6) Definition.
$$\zeta_K(s) = \sum_{\substack{\mathfrak{A} \neq 0 \\ \text{(Ideals von } R)}} \frac{1}{N(\mathfrak{A})}$$

(Dedekindsche) Zeta - Funktion von K.

Bemerkung. (a) Setze
$$j(n) := |\{\mathfrak{A} | N(\mathfrak{A}) = n\}| \quad (n \in \mathbb{N}_{>0}).$$

Dann

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j(n)}{n^s} \qquad \text{(Konvergenz!)}$$

Setze:

$$J(n) = \sum_{n=1}^{N} j(n) = |\{\mathfrak{A} | N(\mathfrak{A}) \leq N\}|$$

(b) Für $\mathrm{Re}(s) > 1$ gilt das **Euler - Produkt** (absolute Konvergenz).

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathbb{P}_K} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^2}} \qquad (\mathrm{Re}(s) > 1)$$

(Richtig, auch angesichts der Tatsache, dass $j(\cdot)$ nicht multiplikativ ist. Argumentiere wie in §§1, 5: Sei $N \in \mathbb{N}$, und betrachte $(\mathrm{Re}(s) > 1)$

$$\begin{aligned} \prod_{\substack{\mathfrak{p} \in \mathbb{P}_K \\ N(\mathfrak{p}) \leq N}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} &= \prod_{\substack{N(\mathfrak{p}) \leq N \\ \text{(endl. Prod.)}}} \left(1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \dots \right) \\ &\overset{(15.3)}{=} \sum_{\mathfrak{A}} \frac{1}{N(\mathfrak{A})^s}, \end{aligned}$$

wobei die Summation über die Ideale $\mathfrak{A} \neq 0$ von R erfolgen, die nur durch $\mathfrak{p} \in \mathbb{P}_K$ mit Norm $N(\mathfrak{A}) \leq N$ teilbar sind.
Lasse $N \to \infty$.

(15.7) Hauptsatz.

$$\zeta_K(s) = \zeta(s) \cdot (s, \chi) \quad (\mathrm{Re}(s) > 0)$$

Also $\zeta_K(s)$ *holomorph (fortsetzbar) auf* $\mathrm{Re}(s) > 0$ *(mindestens) wobei (nur) in* $s = 1$ *ein einfacher Pol mit Residuum* $L(1, \chi)$.

Beweis. Sei $\mathrm{Re}(s) > 1$. Dann gilt nach (15.6), (15.4), (15.5):

$$\begin{aligned} \zeta_K(s) &= \prod_{\mathfrak{p} \in \mathbb{P}_K} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \prod_{\substack{p \in \mathbb{P} \\ \chi(p) = -1}} \frac{1}{1 - \frac{1}{p^{2s}}} \cdot \prod_{\substack{p \in \mathbb{P} \\ \chi(p) = 1 \\ [N(\mathfrak{p}) = p = N(\mathfrak{p}')]}} \frac{1}{(1 - \frac{1}{p^s})^2} \cdot \prod_{\substack{p \in \mathbb{P} \\ \chi(p) = 0 \\ [N(\mathfrak{p}) = p | D_K]}} \frac{1}{1 - \frac{1}{p^s}} \\ &= \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} \cdot \prod_{\substack{p \\ \chi(p) = -1}} \frac{1}{1 + \frac{1}{p^s}} \cdot \prod_{\substack{p \\ \chi(p) = -1}} \frac{1}{1 - \frac{1}{p^s}} \cdot 1 \\ &= \zeta(s) \cdot \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \zeta(s) \cdot L(s, \chi) \end{aligned}$$

Wende (1.8), (12.3) an! ∎

(15.8) Folgerung. Es gilt:

$$j(n) = \sum_{r|n} \chi(r)$$

und ferner

$$L(1,\chi) = \lim_{N\to\infty} \frac{J(N)}{N}$$

Beweis. Die erste Aussage folgt aus §5 („Faltung“). Rechne:

$$\begin{aligned} j(N) = \sum_{n=1}^{N} j(n) = \sum_{n=r}^{N} \sum_{r|n} \chi(r) &= \sum_{\substack{n,r\\ nr\le N}} \chi(n) = \sum_{n=1}^{N} \chi(n) \underbrace{\sum_{r\le \frac{N}{n}} 1}_{=\left[\frac{N}{n}\right]} \\ &= \sum_{n<\sqrt{N}} \chi(n) \sum_{r\le\frac{N}{n}} 1 + \sum_{r\le\frac{N}{n}} 1 \Bigg(\sum_{\sqrt{N}\le n\le N} \chi(n) \Bigg) \end{aligned}$$

Für $n \geq \sqrt{N}$ und $r \leq \frac{N}{n}$ gilt $r \leq \frac{N}{\sqrt{N}} = \sqrt{N}$.
Ferner

$$\sum_{r\le\frac{N}{n}} 1 = \left[\frac{N}{n}\right] = \frac{N}{n} + O(1)$$

und nach (11.5) gilt

$$\sum_{k\le n<k+|D|} \chi(n) = 0 \qquad (k\in\mathbb{N}); \quad |\chi(n)| = 1 \text{ oder } 0$$

Also

$$\begin{aligned} J(n) &= \sum_{n<\sqrt{N}} \chi(n)\left(\frac{N}{n} + O(1)\right) + \sqrt{N}\cdot O(1) \\ &= N \sum_{n<\sqrt{N}} \frac{\chi(n)}{n} + O(\sqrt{N}) \end{aligned}$$

Damit

$$\lim_{N\to\infty} \frac{J(N)}{N} = \lim_{N\to\infty} \sum_{n<\sqrt{N}} \frac{\chi(n)}{n} = L(1,\chi)$$

∎

(15.9) Anhang (Klassenzahlformel). (a) Zwei Ideale $\mathfrak{A}, \mathfrak{b}$ von $R = R_K$ (Ideale $\neq 0$) heißen äquivalent ($\mathfrak{A} \sim \mathfrak{b}$), falls es $x, y \in R \setminus \{0\}$ ist. $x\mathfrak{A} = y\mathfrak{b}$. Schreibe

$$[\mathfrak{A}] = \{\mathfrak{b} | \mathfrak{b} \sim \mathfrak{A}\}$$

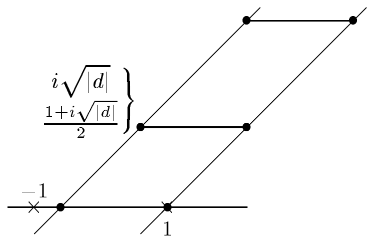
für die Ideale von $\mathfrak{A}$
$h_K :=$ Anzahl der verschiedenen Idealklassen von R („Klassenzahl")
Also: $h_K = 1 \iff R$ Hauptidealring.
$[\mathfrak{A} \sim R = (1);\ x\mathfrak{A} = yR;\ \mathfrak{A} = \frac{y}{x}R,\ \frac{y}{x} \in \mathfrak{A} = \left(\frac{y}{x}\right)]$

(b) Die Ideale von R sind gleichverteilt auf die verschiedenen Idealklassen c (ohne Beweis)
Sei

$$J_c(N) = |\{\mathfrak{A} | \mathfrak{A} \in c, N(\mathfrak{A}) \leq N\}|.$$

Ist K imaginär ($D < 0$), so gilt

$$\lim_{N \to 0} \frac{J_c(N)}{N} = \frac{1}{|R^*|} \cdot \frac{2\pi}{\sqrt{|D|}}.$$



Ist $D < -4$, so ist $R^* = \{\pm 1\}$. Dann mit (15.8)

$$\boxed{h_K = \frac{\sqrt{|D|}}{\pi} \cdot L(1, \chi)} \quad (D < -4)$$

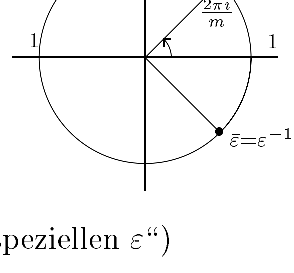
Ist K reell ($D > 0$), so gibt es eine kleinste Einheit $u_0 \in R^*$ mit $u_0 > 1$ („Fundamentaleinheit"), und dann

$$R^* = \{\pm {u_0}^n \mid n \in \mathbb{Z}\} = \{\pm 1\} \times \langle u_0 \rangle \text{ („Dirichlet")}$$

$$\boxed{h_k = \frac{\sqrt{D}}{2 \log u_0} L(1, \chi)} \quad (D > 0)$$

16 Gaußsche Summen

$m \in \mathbb{N}_{\geq 3}$, $\chi \in \widehat{G(m)}$ primitiver Dirichlet - Charakter mod m
($\Rightarrow$ $m \not\equiv 2 \pmod 4$)



(16.1) Definition. Sei

$$\varepsilon = e^{\frac{2\pi i}{m}}$$

$$\tau(\chi) := \sum_{\substack{n=1 \\ n \in G(m)}} \chi(n) \varepsilon^n$$

die zu χ gehörige „normierte" Gaußsche Summe („zum speziellen ε")

Bemerkung. $\chi \neq \mathbb{1}$ (χ prim; $m \geq 3$); $\bar{\chi} = \chi^{-1}$. Es gilt:

$$\begin{aligned}
\overline{\tau(\chi)} &= \sum_{n=1}^{m} \bar{\chi}(n)\varepsilon^{-n} = \sum_{n=1}^{m} \underbrace{\bar{\chi}(-n)\varepsilon^{n}}_{\bar{\chi}(-1)\bar{\chi}(n)} \quad [-n = n'] \\
&= \bar{\chi}(-1) \sum_{n=1}^{m} \bar{\chi}(n)\varepsilon^{n} \\
&= \chi(-1)\tau(\bar{\chi}) = \begin{cases} \tau(\bar{\chi}), & \chi \text{ gerade} \\ -\tau(\bar{\chi}), & \chi \text{ ungerade} \end{cases}
\end{aligned}$$

$\boxed{\text{Übung}}$ Ist $c \in \mathbb{Z}$, teilerfremd zu m, so ist

$$\sum_{n=1}^{m} \chi(n)(\varepsilon^{c})^{n} = \bar{\chi}(c)\tau(\chi)$$

(16.2) Lemma. *Für $k \in \mathbb{Z}$ gilt*

$$\bar{\chi}(k)\tau(\chi) = \sum_{n=1}^{m} \chi(n)\varepsilon^{kn}, \quad \varepsilon = e^{\frac{2\pi i}{m}}$$

Beweis. **1. Fall:** $\operatorname{ggT}(k,m) = 1$. Dann ist

$$\begin{aligned}
\sum_{n=1}^{m} \chi(n)(\varepsilon^{k})^{n} &= \sum_{n=1}^{m} \underbrace{\chi(k'n)}_{\chi(k')\chi(n)} \varepsilon^{n} \\
&= \underbrace{\chi(k')}_{=\bar{\chi}(k)} \tau(\chi)
\end{aligned}$$

2. Fall: $t = \operatorname{ggT}(k,m) \neq 1$ ($\Rightarrow \mathrm{LS}^{14} = 0$)
Setze $m' = \frac{m}{t}$. Da χ primitiv mod m ist, gibt es $c \in \mathbb{Z}$ mit $\operatorname{ggT}(c,m)$ $c \equiv 1 \pmod{m'}$ und $\chi(c) \neq 1$ (Übung 47). Dann $m' | c-1$, $m = tm' | t(c-1) | k(c-1)$, d.h. $kc \equiv k \pmod{m}$.
Damit

$$\mathrm{RS}^{15} = \sum_{n=1}^{m} \chi(n)\varepsilon^{kcn} = \sum_{n \in G(m)} \chi(c^{-1}n)\varepsilon^{kn} = \underbrace{\bar{\chi}(c)}_{\neq 1} \cdot (\mathrm{RS}) = 0 \quad [n' = cn]$$

■

(16.3) Lemma.

$$|\tau(\chi)| = \sqrt{m}$$

Beweis. Für $1 < n \leq m$ und $\alpha = \varepsilon^{n-1}$ $[\alpha \neq 1 = \alpha^m]$ gilt

$$\alpha + \alpha^2 + \alpha^m = \alpha \frac{\alpha^m - 1}{\alpha - 1} = 0$$

Damit

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \sum_{k=1}^{m} \underbrace{\tau(\chi)\overline{\chi(k)}}_{\underset{(16.2)}{=}\sum_{n=1}^{m}\chi(n)\varepsilon^{kn}} \varepsilon^{-k} = \sum_{n=1}^{m}\chi(n)\sum_{k=1}^{m}\varepsilon^{(n-1)k} = \chi(1)\sum_{k=1}^{m}\varepsilon^0 = m$$

■

(16.4) Folgerung. Sei $\chi = \chi_D = \chi_K$ der Kronecker - Charakter eines quadratischen Zahlkörpers K, $D = D_K$, $|D| = m$.
Behauptung: $\tau(\chi)^2 = D$ [vergl. (14.2) für $D = p^*$, $2 \neq p \in \mathbb{P}$]

Beweis. Hier ist $\bar{\chi} = \chi$ und

$$\overline{\tau(\chi)} = \left\{ \begin{array}{ll} \tau(\chi), & \chi \text{ gerade } (D > 0) \\ -\tau(\chi), & \chi \text{ ungerade } (D < 0) \end{array} \right\} \quad (16.1)$$

Nach (16.3):

$$\tau(\chi)^2 = \begin{cases} m = D, & D > 0 \\ -m = D, & D < 0 \end{cases}$$

■

Anmerkung (Gauß). Es gilt

$$\tau(\chi) = +\sqrt{D} = \begin{cases} +_+\sqrt{D}, & D > 0 \\ +i_+\sqrt{D}, & D < 0 \end{cases} \quad (vergl. (17.1))$$

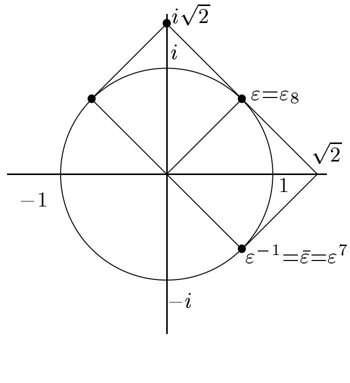
Beispiel.

$\chi = \chi_{-4}$ $(D = -4; \varepsilon = i) : \tau(\chi) = i - i^3 = 2i$

$$\chi = \chi_8 \ (D = 8; \varepsilon = e^{\frac{2\pi i}{8}}) : \tau(\chi) \ = \ \varepsilon - \varepsilon^3 - \varepsilon^5 + \varepsilon^7 \ = \ 2(\varepsilon + \bar{\varepsilon}) = 2\sqrt{2}$$

$\chi = \chi_{-8}$ $(D = -8; \varepsilon = e^{\frac{2\pi i}{8}})$:

$$\tau(\chi) = \varepsilon + \varepsilon^3 - \varepsilon^5 - \varepsilon^7 = (\varepsilon - \bar{\varepsilon}) = 2i\sqrt{2}$$



(16.5) Lemma. *Für* $0 < t < 2\pi$ *gilt:*

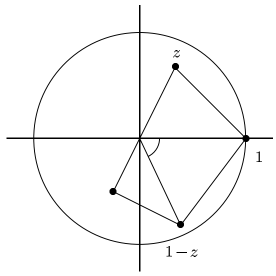
$$\sum_{n=1}^{\infty} \frac{e^{i\pi t}}{n} = -\log(2\sin\frac{t}{2}) + i(\frac{\pi}{2} - \frac{t}{2})$$

Beweis. Für $|z| \leq 1, z \neq 1$ gilt

$$\sum_{n=1}^{\infty} \frac{z^n}{n} = \log\frac{1}{1-z} = -\log(1-z) \qquad \text{[„Hauptzweig"; vergl. Übung 57]}$$

Dann:

$$\begin{aligned} -\frac{\pi}{2} &< \arg(1-z) < \frac{\pi}{2}, \text{ also} \\ -\frac{\pi}{2} &< \operatorname{Im}(\log(1-z)) < \frac{\pi}{2}. \end{aligned}$$



Damit

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{e^{int}}{n} &= -\log(1-e^{it}) = -\log(e^{\frac{it}{2}}(\underbrace{e^{-\frac{it}{2}} - e^{\frac{it}{2}}}_{=2i\sin\frac{t}{2}})) \\ &= -\log(2\sin\frac{t}{2}) - \underbrace{\log(e^{\frac{it}{2}-\frac{\pi i}{2}})}_{=+i(\frac{t}{2}-\frac{\pi}{2})}. \quad [\sin\frac{t}{2} > 0; -i = e^{-\frac{\pi i}{2}}] \end{aligned}$$

■

(16.6) Satz.

$$L(1,\chi) = \frac{\tau(\chi)}{m}\sum_{n=1}^{m-1} \bar{\chi}(n) L_n, \quad L_n = \begin{cases} \frac{\pi i n}{m}, & \chi \textit{ ungerade} \\ -\log(\sin\frac{\pi n}{m}), & \chi \textit{ gerade} \end{cases}$$

Beweis.

$$\begin{aligned} L(1,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k} &\underset{(16.2)}{=} \sum_{k=1}^{\infty} \frac{1}{\overline{\tau(\chi)}} \sum_{n=1}^{m-1} \frac{\bar{\chi}(n)}{k} \varepsilon^{-kn} \\ &= \frac{\tau(\chi)}{m} \sum_{n=1}^{m-1} \bar{\chi}(n) \overline{\sum_{k=1}^{\infty} \frac{e^{\frac{2\pi i k n}{m}}}{k}} \quad [t = t_n = \tfrac{2\pi n}{m} \text{ für } n = 1, \cdots, m-1] \\ &\underset{(16.5)}{=} \frac{\tau(\chi)}{m} \sum_{n=1}^{m-1} \bar{\chi}(n) \left[\cancel{-\log 2} - \log(\sin\frac{\pi n}{m}) - i(\cancel{\frac{\pi}{2}} - \frac{\pi n}{m})\right] \end{aligned}$$

Orthogonalitätsrelation (11.5):
1. Fall: χ ungerade:

$$\begin{aligned}\sum_{n=1}^{m-1}\bar\chi(n)\log(\sin\frac{\pi n}{m}) &= -\sum_{n=1}^{m-1}\underbrace{\bar\chi(-n)}_{\bar\chi(m-n)}\log(\sin\frac{\pi n}{m})\\ &= -\sum_{n=1}^{m-1}\bar\chi(n)\cdot\log(\underbrace{\sin\frac{\pi(m-n)}{m}}_{=\sin\frac{\pi n}{m}})\quad [n'=m-n]\\ &= 0\end{aligned}$$

2. Fall: χ gerade:

$$\sum_{n=1}^{m-1}\bar\chi(n)n=\sum_{n=1}^{m-1}\bar\chi(m-n)n=\sum_{n=1}^{m-1}\bar\chi(n)[m-n]\underset{(11.5)}{=}-\sum\bar\chi(n)n=0\qquad [n'=m-n]$$

■

(16.7) Hauptsatz. *Sei $\chi=\chi_D=\chi_K$ für einen imaginären quadratischen Zahlkörper $K, m=|D|=|D_K|$*
Behauptung:

$$L(1,\chi)=\frac{\pi}{\sqrt{m}(2-\chi(2))}\sum_{1\le n<\frac{m}{2}}\chi(n)$$

Beweis. [16] Hier ist $\chi=\bar\chi$ ungerade. Also nach (16.6) **und** (17.1) $[\tau(\chi)=i\sqrt{m}]$:

$$L(1,\chi)=-\frac{\pi}{m\sqrt{m}}\sum_{n=1}^{m-1}\chi(n)n$$

Setze

$$Q=\sum_{n=1}^{m-1}\chi(n)n$$

zu zeigen:

$$Q=-\frac{m}{2-\chi(2)}\sum_{1\le n<\frac{m}{2}}\chi(n)$$

1. Fall: m ungerade $[D\equiv 1 \pmod 4, m\equiv 3 \pmod 4]$

$$\text{Sei } 1\le n\le m-1;\quad \left.\begin{array}{ll} n \text{ gerade} & \Rightarrow n=2k, 1\le k\le\frac{m-1}{2}\\ n \text{ ungerade} & \Rightarrow n=2k-m, \frac{m+1}{2}\le k\le m-1\end{array}\right\}$$

[16] $(D<0)$

$$\begin{aligned} Q &= \sum_{k=1}^{\frac{m-1}{2}} \chi(2k)2k + \sum_{k=\frac{m+1}{2}}^{m-1} \underbrace{\chi(2k-m)}_{=\chi(2k)}(2k-m) \\ &= 2\chi(2)\cdot Q - m\chi(2) \sum_{k=\frac{m+1}{2}}^{m-1} \chi(k) \underset{(11.5)}{=} 2\chi(2)\cdot Q + m\chi(2)\cdot \sum_{k=1}^{\frac{m-1}{2}} \chi(k) \end{aligned}$$

$$\Rightarrow Q = \frac{m\cdot\chi(2)}{1-2\chi(2)} \sum_{k=1}^{\frac{m-1}{2}} \chi(k) \quad \left[\frac{\chi(2)}{1-2\chi(2)} = -\frac{1}{2-\chi(2)}; \quad \chi(2) = \pm 1\right]$$

2. Fall: m gerade $[m = |D| \equiv 0 \pmod 4]$
Zeige:

$$\boxed{\chi(n+\frac{m}{2}) = -\chi(n)} \quad \text{für} \quad n = 1, \dots, \frac{m}{2} - 1.$$

$$\left[\quad \Rightarrow Q = \sum_{n=1}^{\frac{m}{2}-1} \chi(n)n + \sum_{n=1}^{\frac{m}{2}-1} \underbrace{\chi(n+\frac{m}{2})}_{=-\chi(n)} [n + \frac{m}{2}] = -\frac{m}{2} \sum_{n=1}^{\frac{m}{2}-1} \chi(n); \ \chi(2) = 0 \quad \right]$$

Ist n gerade, so beide Seiten $= 0$
Sei n ungerade:

$$1 + \frac{m}{2} \not\equiv 1 \pmod m, \text{ aber } (1+\frac{m}{2})^2 = 1 + m + \frac{m}{4}\cdot m \equiv 1 \pmod m$$

Da χ primitiv $\mod m$ ist, gilt $\chi(1+\frac{m}{2}) = -1$. Ferner

$$n(1+\frac{m}{2}) = n + \frac{nm}{2} = n + \frac{m}{2} \pmod m \quad [n \text{ ungerade }],$$

also

$$\chi(n+\frac{m}{2}) = \chi(n)\cdot\chi(1+\frac{m}{2}) = -\chi(n)$$

■

Anmerkung. Aus (15.9) folgt die Klassenzahlformel:

$$\boxed{h_K = \frac{1}{2-\chi(2)} \sum_{1\le n<\frac{|D|}{2}} \chi_K(n)} \quad D = D_K < -4$$

Da $h_K \geq 1$ [und endlich] ist für $1 \leq n < \frac{|D|}{2}$ der Wert $\chi_K(n) = +1$ öfter als $\chi_K(n) = -1$, und der Überschuss ist 1-mal h_K für $D_K \equiv 1 \pmod 8$, $2h_K$ für $D_K \equiv 0 \pmod 4), 3h_K$ für $D_K \equiv 5 \pmod 8$

(16.8) Hauptsatz'. *Ist $\chi = \chi_D = \chi_K$ für einen reellen quadratischen Zahlkörper K, $m = D = D_K > 0$, so*

$$L(1,\chi) = -\frac{2}{\sqrt{D}} \sum_{1 \le n < \frac{D}{2}} \chi(n) \log(\sin \frac{\pi n}{m})$$

Beweis. Hier $\chi = \bar{\chi}$ gerade, also nach (16.6) und (17.1) [$\tau(\chi) = +\sqrt{m}$]:

$$L(1,\chi) = -\frac{1}{\sqrt{m}} \sum_{n=1}^{m-1} \chi(n) \log(\sin \frac{\pi n}{m})$$

Für $1 \le n < \frac{m}{2}$ ist $\chi(m-n) = \chi(n)$ und $\sin \frac{\pi(m-n)}{m} = \sin \frac{\pi n}{m}$
$\Rightarrow$ **Beh.** ■

17 Das Gaußsche Vorzeichen

$\chi = \chi_D = \chi_K$ für quadratischen Zahlkörper K, $D = D_K$, $m = |D|$,
$\tau(\chi) = \sum_{n=1}^{m-1} \chi(n) e^{\frac{2\pi i n}{m}}$

(17.1) Hauptsatz (Gauß; 1801 - 1805).

$$\tau(\chi) = +\sqrt{D} = \begin{cases} +_+\sqrt{m}, & D = m > 0 \\ +i_+\sqrt{m}, & D = -m < 0. \end{cases}$$

(Nach (16.4) ist $\tau(\chi)^2 = D$. Nur das Vorzeichen!?)

(17.2) Reduktion. *Es gelte $\tau(\chi_{p^*}) = \sqrt{p^*}$ für alle $2 \ne p \in \mathbb{P}$ [$\chi_{p^*} = (\frac{\cdot}{p})$ $\quad p^* = (-1)^{\frac{p-1}{2}} \cdot p$]*
Dann folgt der Hauptsatz

Beweis. Prim*-Zerlegung $D = p_1^* \cdots p_r^*$ mit Primzahlen $p_1 < p_2 < \cdots < p_r$ (eindeutig)
Induktion nach r:
Sei $r = 1$: Ist $p_1 = 2$, so folgt die Behauptung nach (16.4) [$2^* \in \{-4, \pm 8\}$]
$p_1 \ne 2$, so folgt die Behauptung nach Voraussetzung.
Sei $r > 1$; sei $D' = p_1^* \cdots p_{r-1}^*$, $p = p_r$ (> 2); $D = D' \cdot p^*$; $m' = |D|$ $\;(m = m' \cdot p)$

$$G(m) \cong G(m') \times G(p)$$

Schreibe $\chi' = \chi_{D'}, \chi^* = \chi_{p^*} = (\frac{\cdot}{p})$.
Sei $\varepsilon = e^{\frac{2\pi i}{m}}$; dann

$$\varepsilon^p = e^{\frac{2\pi i}{m'}}, \quad \varepsilon^{m'} = e^{\frac{2\pi i}{p}}$$

Es gibt $a, b \in \mathbb{Z}$ mit $1 = ap + bm'$ ($\varepsilon = \varepsilon^1 = \varepsilon^{ap} \cdot \varepsilon^{bm'}$); $\chi'(a) = \chi'(p)$; $\chi^*(b) = \chi^*(m')$

$$\begin{aligned} \tau(\chi) &= \sum_{n \in G(m')} \chi'(n) \cdot (\varepsilon^{ap})^n \cdot \sum_{n \in G(p)} \chi^*(n)(\varepsilon^{bp})^n \\ &\underset{(16.2)}{=} \chi'(p)\tau(\chi') \cdot \chi^*(m')\tau(\chi^*) = \sqrt{D} \end{aligned}$$

Nach Induktionsvoraussetzung ist $\tau(\chi') = \sqrt{D}$, nach Voraussetzung $\tau(\chi^*) = \sqrt{p^*}$
Ferner:

$$\chi'(p) = \left(\frac{D'}{p}\right), \quad \chi^*(m') = \left(\frac{m'}{p}\right).$$

Es gilt ($\chi' = \chi_{D'}$)

$$\left(\frac{D'}{p}\right) \cdot \left(\frac{|D'|}{p}\right) = \begin{cases} -1, & \text{falls } D' < 0 \text{ und } p = -p^* \ (\equiv 3 \pmod 4) \\ 1 & \text{sonst;} \quad \sqrt{D'} \cdot \sqrt{p^*} = \begin{cases} \sqrt{D}, & \substack{1>0, p^*>0 \text{ oder} \\ D<0, p^*>0 \text{ oder} \\ D'>0, p^*<0} \\ -\sqrt{D} & \text{sonst.} \end{cases} \end{cases}$$

■

(17.3) Lemma. *(Dirichlet). Sei* $f : \mathbb{R} \to \mathbb{C}$ *1-periodisch, regelintegrierbar auf* $[0, 1]$. *Sei* $x \in \mathbb{R}$*; es existiere die links- und rechtsseitige Ableitung von* f *in* x *sowie*

$$f(x + D) \lim_{h \searrow 0} f(x + h), \quad f(x-) = \lim_{h \searrow 0} f(x - h).$$

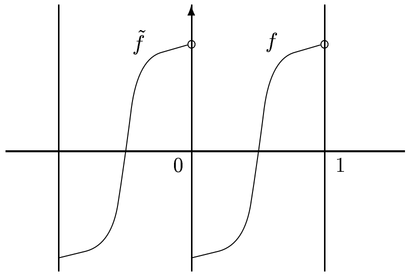
Dann konvergiert die Fourier - Reihe von f *in* x *gegen*

$$\frac{f(x+) + f(x-)}{2}$$

Beweis. Siehe KÖNIGSBERGER, *Analysis I*, Seite 314ff. ■

Folgerung. Sei $f : [0, 1] \to \mathbb{C}$ diffbar (einseitig am Rande). Dann

$$\frac{f(0) + f(1)}{2} = \sum_{n \in \mathbb{Z}} c_n(f), \quad c_n(f) = \int_0^1 f(t) e^{-2\pi i n t} \, dt$$



Beweis. Setze f 1-periodisch auf $\mathbb{R}$ fort $\left[\tilde{f}(x) = f(x - [x])\right]$
Betrachte $x = 0$ ■

(17.4) Beweis des Hauptsatzes. O.B.d.A. $D = p^*$ für $2 \neq p \in \mathbb{P}$ (17.2);
$\chi = \chi_{p^*} = \left(\frac{\cdot}{p}\right)$
Setze

$$Q(b) = \sum_{n=0}^{b-1} e^{\frac{2\pi i n^2}{b}}$$

für $b \in \mathbb{N}_{>0}$; $Q(1) = 1$. Ferner

$$\begin{aligned}\tau(\chi) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{\frac{2\pi i n}{p}} = \sum_{(\frac{n}{p})=1} e^{\frac{2\pi i n}{p}} - \sum_{(\frac{n}{p})=-1} e^{\frac{2\pi i n}{p}} + \underbrace{\sum_{n=0}^{p-1} e^{\frac{2\pi i n}{p}}}_{=0} &= 1 + 2\sum_{(\frac{n}{p})=1} e^{\frac{2\pi i n}{p}} \\ &= G(p) = Q(p)\end{aligned}$$

Sei

$$f(x) = f_p(x) = e^{\frac{2\pi i x^2}{p}}$$

und

$$f_k(x) = f(x+k) \text{ für } k = 0, \ldots, p-1 \text{ und } x \in [0,1]$$

Nach (17.3)[17]:

$$\begin{aligned} Q(p) &= \sum_{k=0}^{p-1} \frac{f_k(0) + f_k(1)}{2} \underset{(17.3)}{=} \sum_{k=0}^{p-1} \sum_{n\in\mathbb{Z}} \int_0^1 f_k(t) e^{-2\pi i n t}\, dt \\ &= \sum_{n\in\mathbb{Z}} \int_0^p \underbrace{e^{\frac{2\pi i t^2}{p}} e^{-2\pi i t}}_{=e^{\frac{2\pi i}{p}(t^2 - pnt)}}\, dt \\ &= \sum_{n\in\mathbb{Z}} e^{-\frac{\pi i p^2 n}{2}} \int_0^p e^{\frac{2\pi i}{p}(t-\frac{pn}{2})^2}\, dt \end{aligned}$$

Es gilt

$$e^{\frac{-\pi i p n^2}{2}} = \begin{cases} 1, & n \text{ gerade} \\ i^{-p}, & n \text{ ungerade} \end{cases}$$

Setze

$$I_p = \int_{-\infty}^{\infty} e^{\frac{2\pi i t^2}{p}}\, dt$$

„Offenbar“ gilt:

$$I_p = \sum_{n\in 2\mathbb{Z}} \int_0^p e^{\frac{2\pi i}{p}(t-\frac{pn}{2})^2}\, dt = \sum_{n\in 1+2\mathbb{Z}} \int_0^p e^{\frac{2\pi i}{p}(1-\frac{pn}{2})^2}\, dt$$

Also

$$Q(p) = (1 + i^{-p}) I_p.$$

[17] mit $[t^2 - pnt = (t - \frac{pn}{2})^2 - \frac{p^2 n^2}{4}]$ (quadr. Ergänzung)

Es ist

$$I_p = \sqrt{p} \cdot \int_{-\infty}^{\infty} e^{2\pi i t^2}\, dt = \sqrt{p} I_1 \qquad [u = \frac{t}{\sqrt{p}}]$$

Ersetzen von $b = p$ durch $b = 1$ liefert analog: $1 = Q(1) = (1 + i^{-1}) I_1$

$$\Rightarrow \tau(\chi) = Q(p) = \sqrt{p} \cdot \frac{1 + i^{-p}}{1 + i^{-1}} = \begin{cases} +\sqrt{p}, & p \equiv 1 \pmod 4 \;\; [p = p^*] \\ +i\sqrt{p}, & p \equiv 3 \pmod 4 \;\; [p = -p^*] \end{cases}$$

A Übungsaufgaben

Aufgaben

1. Sei (a_n) eine Folge komplexer Zahlen $\neq 0$ ($a_n \in \mathbb{C}^*$). Das unendliche Produkt $\prod_{n=1}^\infty a_n$ heißt konvergent, falls die Folge der *Partialprodukte* $p_n = a_1 \cdots a_n$ in $\mathbb{C}^*$ konvergiert ($\lim_{n\to\infty} p_n = p$ existiert und $p \neq 0$).
(a) Genau dann konvergiert $\prod_{n=1}^\infty a_n$, wenn es zu jedem $\varepsilon > 0$ eine Nummer N gibt, so dass $|a_n a_{n+1} \cdots a_{n+r} - 1| < \varepsilon$ ist für alle $n \geq N$ und alle $r \geq 0$.
(b) Konvergiert $\prod_{n=1}^\infty a_n$, so gilt $a_n = 1 + b_n$ mit einer Nullfolge (b_n).
2. $\prod_{n=1}^\infty (1 + \frac{1}{n})$ und $\prod_{n=1}^\infty (1 - \frac{1}{n+1})$ sind divergente Produkte.
3. Das unendliche Produkt $\prod_{n=1}^\infty (1 + b_n)$ heißt *absolut* konvergent, falls $\prod_{n=1}^\infty (1 + |b_n|)$ konvergiert.
(a) Absolute Konvergenz impliziert Konvergenz.
(b) Genau dann konvergiert $\prod_{n=1} \infty(1 + b_n)$ absolut, wenn die Reihe $\sum_{n=1}^\infty b_n$ absolut konvergiert.
Hinweis. $p_n = (1 + |b_1|) \cdots (1 + |b_n|)$ und $s_n = |b_1| + \cdots + |b_n|$ beschreiben monoton wachsende reelle Folgen mit $s_n \leq p_n$ und $p_n \leq e^{s_n}$.
4. Man zeige die absolute Konvergenz der folgenden unendlichen Produkte und berechne ihren Grenzwerte:
(a) $\prod_{n=1}^\infty (1 + \frac{1}{n(n+2)})$.
(b) $\prod_{n=2}^\infty \frac{n^3-1}{n^3+1}$.
Hinweis. Bei absolut konvergenten Produkten darf man (unbeschadet) beliebige Faktoren vertauschen oder auch Klammern setzen oder weglassen. In (b) schreibe man $n^3 - 1 = (n-1) \cdot f(n+1)$ und $n^3 + 1 = (n+1) \cdot f(n)$ mit einer gewissen Funktion f.
5. Sei $D = [a, b]$ ein kompaktes Intervall und $f : D \to \mathbb{C}$ stetig differenzierbar. Dann gilt $|f(s) - f(t)| \leq |s - t| \cdot \|f'\|_D$ (Schrankensatz). -Zum Beweis genügt es $s \in [a, b)$ zu finden mit $|f(b) - f(a)| \leq (b - a) \cdot |f'(s)|$. Dazu wähle man $c \in \mathbb{C}$ mit $|c| = 1$ und $|f(b) - f(a)| = c(f(b) - f(a))$ und wende den Mittelwertsatz auf die (reelle) differenzierbare Funktion $\mathrm{Re}(cf)$ an.
6. Sei $D = [a, b]$ ein kompaktes Intervall und $f : D \times \mathbb{C} \to \mathbb{C}$ stetig differenzierbar, als Funktion der zweiten, komplexen Variablen sogar holomorph. Dann ist $z \mapsto g(z) = \int_a^b f(t, z)dt$ holomorph und $g'(z) = \int_a^b \frac{d}{dz} f(t, z)dt$.
7. Man beweise die Eulersche Produktdarstellung ($z \in \mathbb{C}$):
$$\sin \pi z = \pi z \cdot \prod_{n=1}^\infty (1 - \frac{z^2}{n^2}).$$
(Die rechte Seite stellt eine auf $\mathbb{C}$ holomorphe Funktion dar mit genau den ganzen Zahlen als einfachen Nullstellen, ebenso wie $\sin \pi z$. Die beiden ganzen Funktionen links und rechts sind daher identisch, wenn sie auf dem Intervall $(0, 1)$ übereinstimmen. Für $0 < x < 1$ gilt $\pi \cot \pi x - \frac{1}{x} = \sum_{n=1}^\infty \frac{2x}{x^2 - n^2} = f(x)$ (normale Konvergenz), und eine Stammfunktion von f ist gegeben einerseits durch $F(x) = \log \frac{\sin \pi x}{\pi x}$, andererseits durch $F(x) = \int_0^x \sum_{n=1}^\infty \frac{2t}{t^2 - n^2} dt = \sum_{n=1}^\infty \log(1 - \frac{x^2}{n^2})$.)
8. Sei D die abgeschlossene (kompakte) Einheitskreisscheibe in $\mathbb{C}$. Bekanntlich bilden die auf D stetigen komplexen Funktionen bzgl. punktweisen Verknüpfungen und Sup-Norm eine komplexe Banachalgebra $C(D, \mathbb{C})$. Man zeige, dass die im Innern von D holomorphen Funktionen eine *echte, abgeschlossene* Teilalgebra $H(D)$ von $C(D, \mathbb{C})$ bilden. (Für den komplexen Weierstraß muss man zu $H(D)$ noch die komplexe Konjugation $z \mapsto \bar{z}$ hinzunehmen.)

9. Die Reihe $\sum_{n=1}^{\infty} b_n$ komplexer Zahlen sei absolut konvergent. Dann wird durch $f(s) = \prod_{n=1}^{\infty}(1+b_n s)$ eine auf $\mathbb{C}$ holomorphe Funktion erklärt.

10. Das unendliche Produkt $\prod_{n=0}^{\infty}(1+s^{2^n})$ stellt im Einheitskreis $|s| < 1$ eine holomorphe Funktion h dar. Man zeige, dass dort $h(s) = \frac{1}{1-s}$ ist.

11. Die meromorphe Funktion f habe im Punkte $s = s_0$ einen einfachen Pol mit Residuum a. Warum gilt dann $f(s) \sim \frac{a}{s-s_0}$ für $s \to s_0$? Man zeige, dass die *logarithmische Ableitung* $s \mapsto \frac{f'(s)}{f(s)}$ in s_0 einen einfachen Pol mit Residuum -1 hat.

12. Unter Benutzung von $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ und der Eulerschen Darstellung der Gammafunktion zeige man $\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}$.

Die *Bernoulli-Polynome* $B_n(X)$ sind definiert durch die erzeugende Funktion (formale Potenzreihe)

$$\frac{t}{e^t - 1} \cdot e^{tX} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}.$$

Es ist also $B_n(0) = B_n$ die n-te Bernoulli-Zahl. Man zeige:

13. $B_n(X) = \sum_{k=0}^{n} \binom{n}{k} B_k X^{n-k}$ ist ein rationales Polynom vom Grade n. (Also $B_1(X) = X - \frac{1}{2}, B_2(X) = X^2 - X + \frac{1}{6}, B_3(X) = X^3 - \frac{3}{2}X^2 + \frac{1}{2}X$ etc..) Es gilt ferner $B_n(1-X) = (-1)^n B_n(X)$.

14. $B_n(X+1) - B_n(x) = nX^{n-1}$.
Man folgere, dass für natürliche Zahlen $n, k \geq 2$ gilt:

$$1^{n-1} + 2^{n-1} + \cdots + k^{n-1} = \frac{1}{n}(B_n(k+1) - B_n).$$

15. Für natürliche Zahlen $n \geq 2, r \geq 1$ gilt

$$B_n = r^{n-1} \sum_{k=1}^{r} B_n(\frac{k}{r}).$$

(Man studiere die erzeugende Funktion $\sum_{n=0}^{\infty} r^{n-1} \sum_{k=1}^{r} B_n(\frac{k}{r})\frac{t^n}{n!}$ in der Unbeszimmten rt und eliminiere r.)

16. Für eine Primzahl p bezeichne $\mathbb{Z}_{(p)}$ die Menge der rationalen Brüche, deren Nenner nicht durch p teilbar ist. (Warum ist dies ein Teilring von $\mathbb{Q}$?) Sei $n \geq 2$ eine feste gerade natürliche Zahl.
(a) Sei p eine Primzahl. Geht $p-1$ nicht auf in n, so ist $B_n \in \mathbb{Z}_{(p)}$. Geht $p-1$ in n auf, so ist $B_n + \frac{1}{p} \in \mathbb{Z}_{(p)}$. (Man argumentiere per induktion nach n unter Verwendung der Aufgaben 15 und 13. Es ist $\sum_{k=1}^{p} k^n \equiv -1$ oder $0 \bmod p$, je nachdem ob n durch $p-1$ teilbar ist oder nicht. Warum?)
(b) $B_n + \sum_{p-1|n} \frac{1}{p}$ ist eine ganze Zahl (p prim).
(c) Schreibe $(-1)^{\frac{n}{2}+1} B_n = \frac{a}{b}$ als gekürzten Bruch natürlicher Zahlen. Man zeige, dass b durch 6 teilbar und quadratfrei ist.

Es sei $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ eine (gewöhnliche) dirichlet-Reihe mit Konvergenzabszisse ϱ_f ($\varrho_f \in \mathbb{R}$). Die Konvergenzabszisse der Reihe $\sum_{n=1}^{\infty} \frac{|a_n|}{n^s}$ sei ϱ_f^+ (absolute Konvergenz).

17. Ist die Folge (a_n) absolut beschränkt, so ist $\varrho_f^+ \leq 1$.

18. Sei (wie üblich) $A_m = \sum_{n=1}^{m} a_n$. Ist die Folge (A_m) beschränkt, so ist $\varrho_f \leq 0$. Man gebe ein Beispiel dafür an, dass in diesem Falle $\varrho_f^+ > 0$ sein kann.

19. Man zeige $\varrho_f = \inf\{a \in \mathbb{R} |\, A_m = O(m^a)\}$ und

$$\varrho_f \leq \varrho_f^+ \leq \varrho_f + 1$$

20. (a) Sei $a_n = (-1)^{n+1}$. Dann ist $\varrho_f = 0$ und $f(s) = (1 - 2^{1-s})\zeta(s)$ für $\mathrm{Re}(s) > 1$.
(b) Sei $a_n = 1$ für $n \equiv 1, 2 \pmod 3$ und $a_n = -2$ sonst. Dann ist $\varrho_f = 0$ und $f(s) = (1 - 3^{s-1})\zeta(s)$ für $\mathrm{Re}(s) > 1$.

21. Für die Wahrscheinlichkeit W dafür, dass zwei (willkürlich herausgegriffene) positive natürliche Zahlen teilerfremd sind, gilt $W = \frac{6}{\pi^2}$. (Die Wahrscheinlichkeit, dass eine Primzahl p in einer (bzw. zwei) natürliche Zahl(en) aufgeht, ist $\frac{1}{p}$ (bzw. $\frac{1}{p^2}$).)

22. Für eine natürliche Zahl n mit Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{e_i}$ sei $\nu(n) = \sum_{i=1}^{r} e_i$ und $\lambda(n) = (-1)^{\nu(n)}$. Man zeige, dass λ eine multiplikative Funktion und $\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \zeta(2s)/\zeta(s)$ für $\mathrm{Re}(s) > 1$ ist.

23. Sei $\omega(n)$ die Anzahl der verschiedenen Primteiler der (positiven) natürlichen Zahl n. Man zeige, dass $n \mapsto 2^{\omega(n)}$ multiplikativ und $\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \zeta(s)^2/\zeta(2s)$ für $\mathrm{Re}(s) > 1$ ist.

24. Sei $f : [a, b] \to \mathbb{C}$ stetig auf dem kompakten Intervall. Es existiere eine abzählbare Teilmenge A in $[a, b]$ derart, dass f auf $[a, b] \setminus A$ differenzierbar und dort $f' = 0$ ist. Man zeige, dass f konstant ist. (Man nehme etwa $f(x) \neq f(y)$ für $x < y$ an. Dann gibt es $\delta > 0$, so dass $F_\delta(y) > 0$ ist für die reelle stetige Funktion $F_\delta(t) = |f(t) - f(x)| - \delta(t - x)$. Man wende den Zwischenwertsatz auf F_δ geeignet an.)

25. Man zeige, dass das Faltungsprodukt $\star$ auf der Menge $\mathbb{C}^{\mathbb{N}_{>0}}$ aller komplexen Folgen kommutativ und assoziativ ist:

$$(\chi \star \widetilde{\chi})(n) = \sum_{d|n} \chi(d) \cdot \widetilde{\chi}(n/d).$$

26. Für jede Teilmenge $S \subseteq \mathbb{N}_{>0}$ sei $\varepsilon_S : \mathbb{N}_{>0} \to \mathbb{C}$ erklärt durch $\varepsilon_S(n) = 1$ für $n \in S$ und $= 0$ sonst; schreibe noch ε_n statt $\varepsilon_{\{n\}}$. Man zeige:
(a) $\varepsilon_n \star \varepsilon_m = \varepsilon_{nm}$ für alle n, m.
(b) ε_1 ist das Neutralelement in $(\mathbb{C}^{\mathbb{N}_{>0}}, \star)$.
(c) Für die Möbius-Funktion μ gilt $\mu \star \varepsilon_{\mathbb{N}_{>0}} = \varepsilon_1$.
(d) Für die Eulersche φ-Funktion φ ist $\varphi \star \varepsilon_{\mathbb{N}_{>0}}$ die Inklusion von $\mathbb{N}_{>0}$ in $\mathbb{C}$.

27. Genau dann ist eine Folge χ invertierbar in $(\mathbb{C}^{\mathbb{N}_{>0}}, \star)$, wenn $\chi(1) \neq 0$ ist. (Man konstruiere die Inverse rekursiv.)

28. Sei $\chi(n) = \log n$ für alle $n \in \mathbb{N}_{>0}$. Ist χ multiplikativ ? Man beschreibe die Faltung $\chi \star \mu$ im Detail. Insbesondere zeige man, dass $(\chi \star \mu)(n) = 0$ ist, wenn n keine Primzahlpotenz ist.

29. Sei $\delta > 0$ (klein). Für $\mathrm{Re}(s) \geq 1 + \delta$ ist $|\zeta(s)| \leq \zeta(1 + \delta)$ beschränkt. Für $\mathrm{Re}(s) \geq \delta$ gilt $|\zeta(s)| = O(|s|)$ für $|s| \to \infty$. (Man betrachte die in (1.7) der Vorlesung gegebene analytische Fortsetzung der Zeta-Funktion auf $\mathrm{Re}(s) > 0$.)
Zusatz. Es ist $\lim_{x \to \infty} \zeta(x) = 1$.

30. Die Zeta-Funktion $\zeta(s)$ hat keine Nullstellen für reelle $s > 0, s \neq 1$. Genauer: Für $0 < x < 1$ gilt $\zeta(x) < 0$. (Man studiere nochmals (1.7) der Vorlesung.) .

31. Es gelte $\psi(x) = x + O(x^a)$ für $x \to \infty$ mit einer reellen Zahl $a, \frac{1}{2} < a < 1$ (ψ = Chebyshev-Funktion). Warum ist diese Aussage stärker als der Primzahlsatz der Vorlesung ? Man zeige:
(a) $\frac{\zeta'(s)}{\zeta(s)}$ ist holomorph für $\mathrm{Re}(s) > a$ mit Ausnahme der Stelle $s = 1$, wo ein einfacher Pol mit Residuum -1 vorliegt.
(b) $\zeta(s)$ hat keine Nullstelle in $a < \mathrm{Re}(s) < 1$.

32. Es gilt $\overline{\zeta(s)} = \zeta(\overline{s})$ für alle $s \in \mathbb{C}, s \neq 1$. (Man studiere zunächst die komplexe Konjugation im Falle der Gamma-Funktion $\Gamma(s)$, dann die in (3.4) der Vorlesung beschriebene analytische Fortsetzung der Zeta-Funktion.)
Zusatz. Warum liegen die Nullstellen von $\zeta(s)$ (im kritischen Streifen) symmetisch zur imaginären Achse ?

33. Man nehme zu den folgenden (absurden) Aussagen Stellung:
Für $1 \neq s \in \mathbb{C}$ gilt $\int_0^1 t^{-s} dt = \frac{1}{1-s}$ sowie $\int_1^\infty t^{-s} dt = -\frac{1}{1-s}$, folglich $\int_0^\infty t^{-s} dt = 0$.

34. Man berechne die Residuen der vollständigen Riemannschen Zeta-Funktion
$Z(s) = \pi^{-s/2} \cdot \Gamma(s/2) \cdot \zeta(s)$ in den beiden einzigen (einfachen) Polstellen $s = 0$ und $s = 1$. Man folgere, dass die Funktionen $\xi(s) = \frac{1}{2}s(s-1) \cdot Z(s)$ eine ganze Funktion ist. Diese ganze Funktion genügt (ebenfalls) der Funktionalgleichung

$$\xi(s) = \xi(1-s),$$

und ihre Nullstellen sind gerade die Nullstellen von $\zeta(s)$ im kritischen Streifen. Man folgere, dass die Nullstellen von $\zeta(s)$ im kritischen Streifen symmetrisch zur Geraden $\mathrm{Re}(s) = \frac{1}{2}$ liegen.

35. Die komplexe Jacobische Theta-Funktion $\theta(s) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 s}$ ist holomorph (kompakt konvergent) in der oberen Halbebene von $\mathrm{Im}(s) > 0$ und genügt dort der Funktionalgleichung

$$\theta(-1/s) = \sqrt{s/i} \cdot \theta(s).$$

(Wie üblich meint $\sqrt{s} = e^{\frac{1}{2}\log s}$, wobei log der Hauptzweig des Logarithmus ist.)

36. Die Fouriersche Theta-Funktion ist erklärt als die Funktion

$$\theta(t, x) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t} \cdot e^{2\pi i n x}$$

in den reellen Variablen $t, x \in \mathbb{R}, t > 0$. Man zeige, dass $\frac{\partial^2}{\partial x^2}\theta(t,x) = 4\pi \frac{\partial}{\partial t}\theta(t,x)$ gilt, also $\theta(t,x)$ Lösung einer sog. Wärmeleitungsgleichung ist.

Sei p eine ungerade Primzahl. Für eine ganze zu p teilerfremde Zahl a ist das *Legendre-Symbol* $(\frac{a}{p}) = 1$ bzw. -1, je nachdem ob es $x \in \mathbb{Z}$ gibt mit $x^2 \equiv a \pmod p$ oder nicht.
(Man setzt meist noch $(\frac{a}{p}) = 0$ für $p \mid a$.)

37. Das Legendre-Symbol induziert einen (surjektiven) Homomorphismus (Charakter) $(\frac{-}{p}) : \mathbb{F}_p^* \to \{\pm 1\}$. Es gilt die *Euler-Identität* ($\frac{a}{p} = a^{\frac{p-1}{2}}$, wobei a und ± 1 mit Elementen von $\mathbb{F}_p^*$ identifiziert werden. Es gilt $(\frac{-1}{p}) = 1$ genau dann, wenn $p \equiv 1 \pmod 4$ ist. (Man verwende, dass die multiplikative Gruppe von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *zyklisch* der Ordnung $p-1$ ist, also $|\mathbb{F}_p^{*^2}| = \frac{p-1}{2}$.)

38. Sei $S = \{1, \ldots, \frac{p-1}{2}\} \subseteq \mathbb{F}_p^*$. Dann gilt $\mathbb{F}_p^* = S \dot{\cup} (-S)$. Zu jedem $a \in \mathbb{F}_p^*$ und $s \in S$ gibt es also genau ein $s_a \in S$ und $\varepsilon_s(a) = \pm 1$ mit $a \cdot s = \varepsilon_s(a) \cdot s_a$. Es gilt $\prod_{s \in S} s = \prod_{s \in S} s_a$ für jedes a und daher $(\frac{a}{p}) = \prod_{s \in S} \varepsilon_s(a)$ nach der Euler-Identität. Man zeige, dass $(\frac{2}{p}) = (-1)^r$ ist, wobei r die Anzahl der natürlichen Zahlen im Intervall $(\frac{p-1}{4}, \frac{p-1}{2}]$ ist. Es gilt daher $(\frac{2}{p}) = 1$ genau dann, wenn $p \equiv \pm 1 \pmod 8$ ist.

39. Für jede ungerade natürliche Zahl q (und $x \in \mathbb{R}$) ist $\frac{\sin qx}{\sin x} = \frac{e^{iqx} - e^{-iqx}}{e^{ix} - e^{-ix}}$ ein (reelles) Polynom in $\sin^2 x$ vom Grade $\frac{q-1}{2}$. Man folgere

$$\frac{\sin qx}{\sin x} = (-4)^{\frac{q-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} (\sin^2 x - \sin^2 \frac{2\pi k}{q})$$

durch Berechnung der Wurzeln dieses Polynoms und Vergleich der Koeffizienten von $e^{i(q-1)x}$ auf beiden Seiten.

40. Man beweise das *Quadratische Reziprozitätsgesetz:* Ist $q \neq p$ eine weitere ungerade Primzahl, so gilt

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

Anleitung (Gauß). Nach (38) gilt $qs = \varepsilon_s(q) \cdot s_q$, daher $\sin(\frac{2\pi}{p} qs) = \varepsilon_s(q) \sin(\frac{2\pi p}{q} s_q)$ und $(\frac{q}{p}) = \prod_{s \in S} \varepsilon_s(q) = \prod_{k=1}^{\frac{p-1}{2}} \sin \frac{2\pi qk}{p} / \sin \frac{2\pi k}{p}$. Man wende (39) an (auch bei Vertauschung von p und q).

41. Unter dem logarithmischen Integral versteht man die für positive reelle x erklärte Funktion $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. Gauß vermutete, dass $\pi(x) \cong \mathrm{Li}(x)$ für $x \to \infty$ gilt (konnte es aber nicht beweisen). Lag Gauß mit dieser Vermutung nahe bei der Wahrheit ?

42. Es gibt unendlich viele Primzahlen der Form $3n + 2$ bzw. $4n + 3$ bzw. $6n + 5$ ($n \in \mathbb{N}$). (Man modifiziere den Euklidischen Ansatz (1.1) der Vorlesung geeignet. Ist $p_1 = 2, p_2 = 3.p_4, \ldots p_r \cdots$ die Folge der Primzahlen, so betrachte man etwa $3p_1 \cdots p_r + 2$ bzw. $4p_1 \cdots p_r + 3$ bzw. $6p_1 \cdots p_r + 5$.)

43. Man zeige ähnlich elementar, dass es unendlich viele Primzahlen der Form $4n + 1$ gibt (etwa durch Betrachten von $(p_1 \cdots p_r)^2 + 1$).

44. Zu jedem $n \in \mathbb{N}_{>0}$ und jedem $x \in \mathbb{R}_{>0}$ gibt es $y > x$, so dass $\pi(y) = \pi(y + n)$ ist (Primzahllücken!).

45. Es sei χ ein Dirichlet-Charakter mod $m = 12$.
(a) Es gelte $\chi(5) = -1, \chi(7) = 1$ und $\chi(11) = 1$. Warum ist χ durch diese Forderungen bestimmt (und bestimmbar)? Man zeige, dass der Führer $f(\chi) = 3$ ist aber χ nicht 3-periodisch ist. Der dazugehörige primitive Charakter mod 3 ist $(\frac{\cdot}{3})$.
(b) Sei $\chi(5) = -1, \chi(7) = -1$ und $\chi(11) = 1$. Man zeige, dass nun χ primitiv mod 12 ist und $\chi = (-1)^{\varepsilon} \cdot (\frac{\cdot}{3})$.

46. Seien $d, m \in \mathbb{N}_{\geq 2}$ mit $d | m$. Man zeige:
(a) Der natürliche Homomorphismus $G(m) \to G(d)$ ist surjektiv.
(b) Aus $\varphi(m) = \varphi(d)$ folgt $G(m) \cong G(d)$ und $m = d$ oder $m = 2d, d$ ungerade.

47. Sei $\chi \neq 1$ ein Dirichlet-Charakter mod m. Genau dann ist χ primitiv (mod m), wenn es für jeden echten Teiler d von m eine zu m teilerfremde ganze Zahl a gibt mit $a \equiv 1 \pmod d$ und $\chi(a) \neq 1$.

48. Sei $\chi \neq 1$ ein Dirichlet-Charakter $\mod m$ und $d = f(\chi)$ der Führer von χ. Sei χ' der (einzige, primitive) Dirichlet-Charakter mod d, der χ induziert. Man Zeige
$$L(s,\chi) = L(s,\chi')\prod_{p|m}(1 - \frac{\chi'(p)}{p^s}).$$

49. Sei (n_k) eine monoton wachsende Folge positiver natürlicher Zahlen.
(a) Ist $\frac{n_{k+1}-n_k}{n_k} \geq \delta$ für festes $\delta > 0 (k \in \mathbb{N}_{>0})$, so ist die *Lückenreihe* $\sum_{k=1}^{\infty} \frac{1}{n_k}$ konvergent.
(b) Gilt $n_{k+1} - n_k \geq m$ für alle k und noch so großes $m \in \mathbb{N}$, so braucht die Reihe $\sum_{k=1}^{\infty} \frac{1}{n_k}$ dennoch nicht konvergent zu sein.

50. Seien Q, Q' disjunkte Mengen von Primzahlen. Haben zwei der drei Mengen Q, Q' und $Q \cup Q'$ Dirichlet-Dichten, so auch die dritte, und es gilt
$$\delta(Q \cup Q') = \delta(Q) + \delta(Q').$$

51. Existiert für die Primzahlmenge Q die natürliche (statistische) Dichte $\delta_0(Q)$, so existiert auch die Dirichlet-Dichte $\delta(Q)$, und es gilt $\delta(Q) = \delta_0(Q)$.

52. Sei $m \in \mathbb{N}_{\geq 3}, m \not\equiv 2(\mod 4)$ und sei ϕ_m das m-te Kreisteilungspolynom. Warum wird $G(m)$ durch die Bilder $\mod m$ der Primzahlen p mit $p \nmid m$ erzeugt? - Sei p eine solche Primzahl.
(a) Die Reduktion $\Phi_m \mod p$ ist separabel und ein Produkt von r_p Primpolynomen über $\mathbb{F}_p$ vom Grade f_p, wobei $f_p = o(p \mod m)$ und $r_p = \varphi(m)/f_p$ ist.
(b) Sei $R = \mathbb{Z}[\varepsilon]$ für $\varepsilon = e^{2\pi i/m}$. Ist $\mathfrak{p} \supseteq pR$ ein maximales Ideal von R, so ist $R/\mathfrak{p}$ ein Körper der Ordnung f_p.
(c) $\sigma_p : \varepsilon \mapsto \varepsilon^p$ ist ein Element der Ordnung f_p in $G = \mathrm{Gal}(\mathbb{Q}(\mu_m)|\mathbb{Q})$ (Frobeniusautomorphismus zu p).
Man folgere, dass die Galoisgruppe $G \cong G(m)$ und Φ_m irreduzibel über $\mathbb{Q}$ ist.

53. Sei $a \in \mathbb{Z}$. Ist die Kongruenz $X^2 \equiv a \pmod p$ lösbar in $\mathbb{Z}$ für fast alle Primzahlen p, so ist a ein Quadrat in $\mathbb{Z}$.

54. Sei Q die Menge der Primzahlen p, für welche die Kongruenz $X^3 \equiv 2 \pmod p$ lösbar ist. Unter Verwendung von Chebotarev zeige man, dass die natürliche Dichte $\delta_0(Q) = \frac{2}{3}$ existiert.

55. Sei Q' die Menge der Primzahlen p, für welche die Kongruenz $X^4 \equiv 2 \pmod p$ lösbar ist. Unter Verwendung von Chebotarev zeige man, dass $\delta_0(Q') = \frac{3}{8}$ existiert.

56. Sei Q'' die Menge der Primzahlen, deren erste Dezimalziffer gleich 1 ist (wie $11, 13, 17, 19, 101, 103, \ldots$). Durch Anwendung des Primzahlsatzes zeige man, dass $\delta_0(Q'')$ nicht existiert.

57. Die Potenzreihe $\sum_{n=1}^{\infty} \frac{s^n}{n}$ konvergiert für $|s| \leq 1, s \neq 1$ gegen den Hauptzweig des komplexen Logarithmus $\log \frac{1}{1-s}$. (Man verwende Abelsche partielle Summation. Ist $|s| = 1, s \neq 1$, so gilt $\lim_{t \nearrow 1} \sum_{n=1}^{\infty} \frac{(ts)^n}{n} = \log \frac{1}{1-s}$.)

58. Man berechne die L-Reihe $L(s,\chi)$ an der Stelle $s = 1$ für den primitiven Dirichlet-Charakter $\chi = (-1)^{\varepsilon} \mod 4$, d.h. $L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + - \cdots$.
(Hinweis: Es ist $\sum_{n=1}^{\infty} \frac{i^n}{n} - \sum_{n=1}^{\infty} \frac{(-i)^n}{n} = 2i \cdot L(1,\chi)$.)

59. Man berechne die L-Reihe $L(1,\chi)$ an der Stelle $s = 1$ für den primitiven Dirichlet-Charakter $\chi = (\frac{\cdot}{3}) \mod 3$, d.h. $L(1,\chi) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + - \cdots$.
(Hinweis: Ist $\varepsilon = \frac{-1+i\sqrt{3}}{2}$ eine primitive 3-te Einheitswurzel, so ist $\sum_{n=1}^{\infty} \frac{\varepsilon^n}{n} + \sum_{n=1}^{\infty} \frac{\varepsilon^{-n}}{n} = i\sqrt{3} \cdot L(1,\chi)$.)

60. Der Ring der ganzen Zahlen in $K = \mathbb{Q}(i\sqrt{5})$ ist $R_K = \mathbb{Z}[\frac{1+i\sqrt{5}}{2}]$. Man zeige, dass R_K kein Hauptidealring ist, d.h. die Klassenzahl $h_K \neq 1$, durch geeignete Zerlegung der Zahl 6 in unzerlegbare Elemente in R_K. Wie sieht in diesem Fall der Kronecker-Charakter χ_K aus sowie die Diskriminante D_K ? Man berechne die Klassenzahl durch Verwendung der *Klassenzahlformel*

$$h_K = \frac{1}{2 - \chi_K(2)} \sum_{1 \leq n < \frac{|D_K|}{2}} \chi_K(n),$$

die so für jeden imaginären quadratischen Zahlkörper $K \neq \mathbb{Q}(i), \mathbb{Q}(i\sqrt{3})$ gilt.
Zusatz. Als Übung zur Berechnung von Legendre-Symbolen bestimme man die Klassenzahl von $\mathbb{Q}(i\sqrt{47})$ mit dieser Formel.

Literatur

[1] D. B. Zagier, *Zetafunktionen und quadratische Zahlkörper*, Springer (1981).

[2] J. P. Serre, *A Course in Arithmetic*, Springer Graduate Texts (1973).

[3] A. A. Karatsuba, *Basic Analytic Number Theory*, Springer (1993).

[4] Lang; Narkiwics .

[5] Washington; Borevich-Shafarevich; Aigner-Ziegler; Ribenboim .

[6] Neukirch, Landau, Pracher .

[7] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer (1995)

[8] R. Remmert, G. Schumacher *Funktionentheorie 1*, Springer (2001).

[9] R. Remmert *Funktionentheorie 2*, Springer (1995).

[10] O. Forster *Analysis 1*, Vieweg (1999).

[11] K. Königsberger *Analysis 1*, Springer (2000).

[12] K. Königsberger *Analysis 2*, Springer (2000).

[13] S. Bosch *Algebra*, Springer (2003).

[14] Neukirch *Algebraische Zahlentheorie*, Springer (1986).

[15] H. Scheid *Zahlentheorie*, BI-Wiss.-Verlag (1991).

[16] H. Hardy, E.M. Wright *An introduction to the theory of numbers*, Oxford University Press (1978).

[17] E. Freitag, R. Busam *Funktionentheorie*, Springer (2000).

Index