

## § 7. Arithmetische Funktionen. Möbiussche Umkehrformel

**7.1. Definition.** Unter einer *arithmetischen Funktion* versteht man eine Abbildung

$$\alpha : \mathbb{N}_1 \longrightarrow \mathbb{C}.$$

Die arithmetische Funktion  $\alpha$  heißt *multiplikativ*, falls  $\alpha(1) = 1$  und

$$\alpha(m_1 m_2) = \alpha(m_1) \alpha(m_2) \quad \text{für alle } m_1, m_2 \in \mathbb{N}_1 \text{ mit } \text{gcd}(m_1, m_2) = 1.$$

$\alpha$  heißt *vollkommen multiplikativ*, falls sogar

$$\alpha(m_1 m_2) = \alpha(m_1) \alpha(m_2) \quad \text{für alle } m_1, m_2 \in \mathbb{N}_1.$$

*Bemerkung.* Viele der zu betrachtenden arithmetischen Funktionen haben ihre Werte bereits in  $\mathbb{Z}$  oder  $\mathbb{R}$ .

**7.2.** Als erstes Beispiel betrachten wir die *Eulersche Phi-Funktion*

$$\varphi : \mathbb{N}_1 \longrightarrow \mathbb{Z}.$$

Sie wurde bereits im vorigen Paragraphen definiert, und zwar ist  $\varphi(m)$  die Anzahl der Elemente der multiplikativen Gruppe  $(\mathbb{Z}/m)^*$ , also gleich der Anzahl derjenigen unter den Zahlen

$$1, 2, \dots, m$$

die zu  $m$  teilerfremd sind.

**Satz.** Die Eulersche Phi-Funktion  $\varphi : \mathbb{N}_1 \rightarrow \mathbb{Z}$  ist multiplikativ.

Dies folgt unmittelbar aus dem Chinesischen Restsatz, da für teilerfremde  $m_1, m_2 \in \mathbb{N}_1$  gilt

$$(\mathbb{Z}/m_1 m_2)^* \cong (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*$$

Da jede natürliche Zahl  $n \in \mathbb{N}_1$  sich als Produkt von (zueinander teilerfremden) Primzahlpotenzen schreiben lässt, ist eine multiplikative arithmetische Funktion schon eindeutig bestimmt, wenn man sie für Primzahlpotenzen  $p^k$  kennt. Für die Eulersche Phi-Funktion ist

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right),$$

denn die nicht zu  $p^k$  teilerfremden unter den Zahlen  $1, 2, \dots, p^k$  sind genau die  $p^{k-1}$  Zahlen

$$\nu p, \quad 1 \leq \nu \leq p^{k-1}.$$

**Folgerung.** Ist  $n = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$  die Primfaktorzerlegung von  $n$ , so gilt

$$\varphi(n) = n \prod_{j=1}^r \left(1 - \frac{1}{p_j}\right).$$

*Beweis.* Wegen der Multiplikativität von  $\varphi$  ist

$$\varphi(n) = \prod_{j=1}^r \left\{ p_j^{k_j} \left(1 - \frac{1}{p_j}\right) \right\} = n \prod_{j=1}^r \left(1 - \frac{1}{p_j}\right), \quad \text{q.e.d.}$$

Z.B. ist

$$\begin{aligned} \varphi(2) &= 2 \left(1 - \frac{1}{2}\right) = 1, \\ \varphi(6) &= 6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 2, \\ \varphi(12) &= 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4. \end{aligned}$$

Dies zeigt auch, dass  $\varphi$  nicht vollkommen multiplikativ ist, denn  $\varphi(2)\varphi(6) \neq \varphi(12)$ .

**7.3.** Als nächstes betrachten wir die *Teileranzahl-Funktion*

$$\tau : \mathbb{N}_1 \longrightarrow \mathbb{Z}.$$

Nach Definition ist  $\tau(n)$  die Anzahl aller natürlichen Zahlen, die Teiler von  $n$  sind (einschließlich 1 und  $n$ ), d.h. die Anzahl der Elemente der Menge

$$T(n) := \{d \in \mathbb{N}_1 : d \mid n\}.$$

Für eine Primzahl  $p$  gilt also  $\tau(p) = 2$ , allgemeiner für eine Primzahlpotenz

$$\tau(p^k) = k + 1,$$

da die Teiler von  $p^k$  genau die Zahlen  $p^j$ ,  $j = 0, 1, \dots, k$ , sind.

**Satz.** Die Teileranzahl-Funktion  $\tau$  ist multiplikativ. Genauer gilt: Sind  $m_1, m_2 \in \mathbb{N}_1$  teilerfremd, so ist die Abbildung

$$T(m_1) \times T(m_2) \longrightarrow T(m_1 m_2), \quad (d_1, d_2) \mapsto d_1 d_2$$

bijektiv.

Dies sieht man unmittelbar durch Betrachtung der Primfaktor-Zerlegungen von  $m_1$  und  $m_2$  sowie der Teiler.

**Folgerung.** Ist  $n = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$  die Primfaktorzerlegung von  $n$ , so gilt

$$\tau(n) = \prod_{j=1}^r (k_j + 1).$$

*Bemerkung.* Die  $\tau$ -Funktion ist nicht vollkommen multiplikativ, da z.B. für eine Primzahl  $\tau(p) = 2$ , aber  $\tau(p^2) = 3 \neq \tau(p)^2$ .

**7.4.** Wir geben jetzt einige Beispiele von vollkommen multiplikativen arithmetischen Funktionen an, die wir später noch brauchen werden.

$$(1) \quad u : \mathbb{N}_1 \rightarrow \mathbb{Z}, \quad u(n) := 1 \text{ für alle } n \in \mathbb{N}_1.$$

$$(2) \quad \iota : \mathbb{N}_1 \rightarrow \mathbb{Z}, \quad \iota(n) := n \text{ für alle } n \in \mathbb{N}_1.$$

$$(3) \quad \varepsilon : \mathbb{N}_1 \rightarrow \mathbb{Z}, \quad \varepsilon(n) := \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

Es ist klar, dass diese Funktionen vollkommen multiplikativ sind.

**7.5. Definition.** Sei  $f : \mathbb{N}_1 \rightarrow \mathbb{C}$  eine arithmetische Funktion. Unter der *summatorischen Funktion* von  $f$  versteht man die Funktion  $F : \mathbb{N}_1 \rightarrow \mathbb{C}$ , die durch

$$F(n) = \sum_{d|n} f(d)$$

definiert ist.

Dabei wird über alle positiven Teiler  $d$  von  $n$  summiert, z.B. ist

$$F(6) = f(1) + f(2) + f(3) + f(6).$$

*Beispiele.* a) Die Teileranzahl-Funktion  $\tau$  ist die summatorische Funktion von der in 7.4 definierten Funktion  $u$ , denn

$$\tau(n) = \sum_{d|n} 1.$$

b) Die summatorische Funktion der Funktion  $\iota$  ist die sog. *Teilersummen-Funktion*

$$\sigma(n) = \sum_{d|n} d.$$

**7.6. Satz** (Summatorische Funktion der Eulerschen Phi-Funktion).

$$\sum_{d|n} \varphi(d) = n \quad \text{für alle } n \in \mathbb{N}_1.$$

*Beweis.* Für jeden Teiler  $d \mid n$  sei

$$A(n, d) := \{k \in \mathbb{N}_1 : k \leq n \text{ und } \gcd(k, n) = d\}.$$

Da  $\bigcup_{d|n} A(n, d) = \{1, 2, \dots, n\}$ , gilt

$$\sum_{d|n} \#A(n, d) = n.$$

Die Elemente  $k \in A(n, d)$  sind alle durch  $d$  teilbar. Da

$$\gcd(k, n) = d \iff \gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1,$$

steht  $A(n, d)$  in bijektiver Beziehung zu  $A(n/d, 1)$ . Es folgt  $\#A(n, d) = \#A(n/d, 1) = \varphi(n/d)$ , also

$$n = \sum_{d|n} \#A(n, d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d), \quad \text{q.e.d.}$$

**7.7. Satz.** Sei  $f : \mathbb{N}_1 \rightarrow \mathbb{C}$  eine multiplikative arithmetische Funktion und  $F : \mathbb{N}_1 \rightarrow \mathbb{C}$  die summatorische Funktion von  $f$ . Dann ist auch  $F$  multiplikativ.

*Beweis.* Seien  $m_1, m_2 \in \mathbb{N}_1$  teilerfremd. Dann erhalten wir unter Benutzung von Satz 7.3

$$\begin{aligned} F(m_1 m_2) &= \sum_{d|m_1 m_2} f(m_1 m_2) \\ &= \sum_{d_1|m_1} \sum_{d_2|m_2} f(m_1 m_2) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(m_1) f(m_2) \\ &= \sum_{d_1|m_1} f(m_1) \sum_{d_2|m_2} f(m_2) = F(m_1) F(m_2). \end{aligned}$$

*Beispiel.* Da die in 7.4 definierte Funktion  $\iota$  multiplikativ ist, ist auch die Teilersummenfunktion

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \iota(d)$$

multiplikativ. Wir benützen dies zur Herleitung einer Formel für  $\sigma(n)$ . Für eine Primzahlpotenz gilt

$$\sigma(p^k) = \sum_{j=0}^k p^j = \frac{p^{k+1} - 1}{p - 1},$$

deshalb folgt für  $n = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$

$$\sigma(n) = \prod_{j=0}^r \frac{p_j^{k_j} - 1}{p_j - 1}.$$

**7.8. Vollkommene Zahlen.** Eine Zahl  $n \in \mathbb{N}_1$  heißt *vollkommen*, falls  $\sigma(n) = 2n$ . Dies lässt sich auch so ausdrücken: Bezeichnet

$$\sigma'(n) := \sum_{\substack{d|n \\ d < n}} d = \sigma(n) - n$$

die Summe der *echten* Teiler von  $n$ , so ist eine vollkommene Zahl  $n$  dadurch charakterisiert, dass  $\sigma'(n) = n$ . Die kleinsten vollkommenen Zahlen sind

$$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 4 + 7 + 14. \end{aligned}$$

Die vollkommenen Zahlen hängen eng mit den Mersenneschen Primzahlen zusammen, wie folgender Satz zeigt:

**Satz.** a) (Euklid) *Ist  $M_p = 2^p - 1$  eine Primzahl, so ist*

$$N := 2^{p-1}(2^p - 1)$$

*eine vollkommene Zahl.*

b) (Euler) *Umgekehrt lässt sich jede gerade vollkommene Zahl als  $2^{p-1}(2^p - 1)$  mit einer Mersenneschen Primzahl  $2^p - 1$  schreiben.*

*Beweis.* a) Wegen der Multiplikativität von  $\sigma$  gilt

$$\sigma(N) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Nun ist  $\sigma(2^{p-1}) = 2^p - 1$  und, da  $2^p - 1$  nach Voraussetzung prim ist,  $\sigma(2^p - 1) = 2$ , also insgesamt  $\sigma(N) = 2N$ .

b) Sei  $N$  eine gerade vollkommene Zahl. Sie lässt sich schreiben als

$$N = 2^s n \quad \text{mit } s \geq 1 \text{ und } n \text{ ungerade.}$$

Nun ist

$$2N = \sigma(N) = \sigma(2^s)\sigma(n) = (2^{s+1} - 1)\sigma(n).$$

Da  $2N = 2^{s+1}n$ , folgt daraus

$$\sigma(n) = \frac{2^{s+1}}{2^{s+1} - 1} n = n + \frac{n}{2^{s+1} - 1} = n + d$$

mit  $d := n/(2^{s+1} - 1) \in \mathbb{N}_1$ . Da  $d$  ein Teiler von  $n$  ist, folgt aus der Gleichung  $\sigma(n) = n + d$ , dass  $n$  und  $d$  die einzigen Teiler von  $n$  sind; also muss  $d = 1$  und  $n$  eine Primzahl sein. Aus  $d = 1$  folgt weiter  $n = 2^{s+1} - 1$ , also ist  $n$  eine Mersennesche Primzahl, insbesondere ist  $p := s + 1$  prim (vgl. 4.2). Daraus folgt Teil b) des Satzes.

*Bemerkung.* Die vollkommenen Zahlen 6 und 28 gehören zu den Mersenneschen Primzahlen  $M_2 = 3$  und  $M_3 = 7$ , die nächsten Beispiele vollkommener Zahlen sind also  $2^4(2^5 - 1) = 496$  und  $2^6(2^7 - 1) = 8128$ . Es ist unbekannt, ob es ungerade vollkommene Zahlen gibt.

**7.9. Möbius-Funktion.** Eine Zahl  $n \in \mathbb{N}_1$  heißt *quadratzfrei*, wenn  $n$  von keiner Quadratzahl  $> 1$  geteilt wird, d.h. wenn es keine Primzahl  $p$  mit  $p^2 \mid n$  gibt. Die Möbius-Funktion  $\mu : \mathbb{N}_1 \rightarrow \mathbb{Z}$  wird nun definiert durch

$$\mu(n) := \begin{cases} 0, & \text{falls } n \text{ nicht quadratzfrei,} \\ (-1)^r, & \text{falls } n \text{ quadratzfrei und } r \text{ verschiedene Primteiler hat.} \end{cases}$$

Für  $n \leq 14$  ergeben sich folgende Werte

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

Es folgt unmittelbar aus der Definition, dass  $\mu$  multiplikativ ist.

**Satz.** Die summatorische Funktion der Möbius-Funktion ist die in 7.4 definierte Funktion  $\varepsilon$ , d.h.

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

*Beweis.* Wir bezeichnen für den Augenblick mit  $M$  die summatorische Funktion von  $\mu$ , d.h.  $M(n) = \sum_{d|n} \mu(d)$ . Die Funktion  $M$  ist nach Satz 7.7 multiplikativ, ebenso die Funktion  $\varepsilon$ . Um also  $M = \varepsilon$  zu beweisen, genügt es  $M(p^k) = \varepsilon(p^k)$  für alle Primzahlpotenzen  $p^k$  zu zeigen. Der Fall  $k = 0$  ist trivial. Für  $k \geq 1$  ist

$$M(p^k) = \sum_{j=0}^k \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0 = \varepsilon(p^k), \quad \text{q.e.d.}$$

**7.10. Dirichlet-Faltung.** Sind  $f, g : \mathbb{N}_1 \rightarrow \mathbb{C}$  zwei arithmetische Funktionen, so ordnet man ihnen eine neue arithmetische Funktion  $f * g : \mathbb{N}_1 \rightarrow \mathbb{C}$ , die sog. Dirichlet-Faltung von  $f$  und  $g$  zu, die durch

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d)$$

definiert ist. Die letzte Gleichung ist so zu begründen: Durchläuft  $d$  alle Teiler von  $n$ , so durchläuft auch  $n/d$  alle Teiler von  $n$ . Die Dirichlet-Faltung lässt sich in symmetrischer Form auch als

$$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

schreiben. Die Summe ist über alle Paare  $d_1, d_2 \in \mathbb{N}_1$  mit  $d_1 d_2 = n$  zu erstrecken.

**Satz.** Die Dirichlet-Faltung arithmetischer Funktionen ist kommutativ und assoziativ. Die Funktion

$$\varepsilon : \mathbb{N}_1 \rightarrow \mathbb{Z}, \quad \varepsilon(n) := \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst,} \end{cases}$$

ist neutrales Element für die Dirichlet-Faltung.

Beweis. i) Die Kommutativität  $f * g = g * f$  ist trivial.

ii) Zur Assoziativität. Seien  $f, g, h : \mathbb{N}_1 \rightarrow \mathbb{C}$  drei arithmetische Funktionen. Dann ist

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{\substack{k, \ell \\ k\ell=n}} (f * g)(k)h(\ell) = \sum_{\substack{k, \ell \\ k\ell=n}} \sum_{\substack{i, j \\ ij=k}} f(i)g(j)h(\ell) \\ &= \sum_{\substack{i, j, \ell \\ ij\ell=n}} f(i)g(j)h(\ell). \end{aligned}$$

Ebenso gilt

$$\begin{aligned} (f * (g * h))(n) &= \sum_{\substack{i, m \\ im=n}} f(i)(g * h)(m) = \sum_{\substack{i, m \\ im=n}} \sum_{\substack{j, \ell \\ j\ell=m}} f(i)g(j)h(\ell) \\ &= \sum_{\substack{i, j, \ell \\ ij\ell=n}} f(i)g(j)h(\ell), \end{aligned}$$

also  $(f * g) * h = f * (g * h)$ .

iii) Neutrales Element:

$$(f * \varepsilon)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) \varepsilon(d) = f(n) \varepsilon(1) = f(n), \quad \text{q.e.d.}$$

*Bemerkung.* Mithilfe der Dirichlet-Faltung lässt sich die summatorische Funktion

$$F(n) = \sum_{d|n} f(d)$$

einer arithmetischen Funktion  $f : \mathbb{N}_1 \rightarrow \mathbb{C}$  auch einfach ausdrücken als  $F = f * u$ , wobei  $u : \mathbb{N}_1 \rightarrow \mathbb{Z}$  die schon in 7.4 betrachtete Funktion mit  $u(n) = 1$  für alle  $n \in \mathbb{N}_1$  ist, denn

$$(f * u)(n) = \sum_{d|n} f(d)u\left(\frac{n}{d}\right) = \sum_{d|n} f(d).$$

**7.11. Satz** (Möbiussche Umkehrformel). *Sei  $f : \mathbb{N}_1 \rightarrow \mathbb{C}$  eine arithmetische Funktion und*

$$F(n) = \sum_{d|n} f(d)$$

*ihre summatorische Funktion. Dann gilt für alle  $n \in \mathbb{N}_1$*

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right)F(d).$$

*Beweis.* Da  $F$  die summatorische Funktion von  $f$  ist, gilt  $F = f * u$ . Multiplikation (bzgl. Dirichlet-Faltung) dieser Gleichung mit  $\mu$  ergibt

$$F * \mu = (f * u) * \mu = f * (u * \mu) = f * \varepsilon = f.$$

Dies ist aber die Behauptung.

**7.12. Beispiele.** Wir geben einige Anwendungen der Möbiusschen Umkehrformel.

a) Wir hatten für die Eulersche Phi-Funktion abgeleitet (Satz 7.6), dass

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

Daraus folgt

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

Dies lässt sich auch in der Form

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

schreiben.

b) Für die Teileranzahl-Funktion  $\tau(n) = \sum_{d|n} 1$  erhält man

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d) = 1.$$

c) Für die Teilersummen-Funktion  $\sigma(n) = \sum_{d|n} d$  ergibt sich

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n.$$