3. Arithmetical Functions. Möbius Inversion Theorem

3.1. Definition. a) An arithmetical function is a map 
\[ f : \mathbb{N}_1 \rightarrow \mathbb{C}. \]
b) The function \( f \) is called multiplicative if it is not identically zero and 
\[ f(nm) = f(n)f(m) \quad \text{for all } n, m \in \mathbb{N}_1 \text{ with } \gcd(n, m) = 1. \]
c) The function \( f \) is called completely multiplicative or strictly multiplicative if it is not identically zero and 
\[ f(nm) = f(n)f(m) \quad \text{for all } n, m \in \mathbb{N}_1 \text{ (without restriction)}. \]

Remark. A multiplicative arithmetical function \( a : \mathbb{N}_1 \rightarrow \mathbb{C} \) satisfies \( a(1) = 1 \). This can be seen as follows: Since \( \gcd(1, n) = 1 \), we have \( a(n) = a(1)a(n) \) for all \( n \). Therefore \( a(1) \neq 0 \), (otherwise \( a \) would be identically zero), and \( a(1) = a(1)a(1) \) implies \( a(1) = 1 \).

3.2. Examples
i) The Euler phi function \( \varphi : \mathbb{N}_1 \rightarrow \mathbb{N}_1 \subset \mathbb{C} \), which was defined in (2.9), is a multiplicative arithmetical function. It is not completely multiplicative, since for a prime \( p \) we have 
\[ \varphi(p^2) = p^2 - p = (p - 1)p \neq \varphi(p)^2 = (p - 1)^2. \]

ii) Let \( \alpha \in \mathbb{C} \) be an arbitrary complex number. We define a function 
\[ p_\alpha : \mathbb{N}_1 \rightarrow \mathbb{C}, \quad n \mapsto p_\alpha(n) := n^\alpha = e^{\alpha \log(n)}. \]
Then \( p_\alpha \) is a completely multiplicative arithmetical function.

iii) Let \( f : \mathbb{N}_1 \rightarrow \mathbb{Z} \subset \mathbb{C} \) be defined by \( f(p) := 1 \) for primes \( p \) and \( f(n) = 0 \) if \( n \) is not prime. This is an example of an arithmetical function which is not multiplicative.

Remark. A multiplicative arithmetical function \( f : \mathbb{N}_1 \rightarrow \mathbb{C} \) is completely determined by its values at the prime powers: If \( n = \prod_{i=1}^r p_i^{e_i} \) is the canonical prime decomposition of \( n \), then 
\[ f(n) = \prod_{i=1}^r f(p_i^{e_i}). \]

3.3. Divisor function \( \tau : \mathbb{N}_1 \rightarrow \mathbb{N}_1 \). This function is defined by 
\[ \tau(n) := \text{number of positive divisors of } n. \]
Thus \( \tau(p) = 2 \) and \( \tau(p^k) = 1 + k \) for primes \( p \). (The divisors of \( p^k \) are \( 1, p, p^2, \ldots, p^k \)).
The divisor function is multiplicative. This can be seen as follows: Let \( m_1, m_2 \in \mathbb{N}_1 \) be a pair of coprime numbers and \( m := m_1 m_2 \). Looking at the prime decompositions one sees that the product \( d := d_1 d_2 \) of divisors \( d_1 \mid m_1 \) and \( d_2 \mid m_2 \) is a divisor of \( m \) and conversely every divisor \( d \mid m \) can be uniquely decomposed in this way. This can be also expressed by saying that the map
\[
\text{Div}(m_1) \times \text{Div}(m_2) \longrightarrow \text{Div}(m_1 m_2), \quad (d_1, d_2) \mapsto d_1 d_2
\]
is bijective, where \( \text{Div}(n) \) denotes the set of positive divisors of \( n \). This implies immediately the multiplicativity of \( \tau \).

### 3.4. Divisor sum function \( \sigma : \mathbb{N}_1 \to \mathbb{N}_1 \)
This function is defined by
\[
\sigma(n) := \text{sum of all positive divisors of } n.
\]
Thus for a prime \( p \) we have \( \sigma(p) = 1 + p \) and
\[
\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}.
\]
The divisor sum function is also multiplicative.

**Proof.** Let \( m_1, m_2 \in \mathbb{N}_1 \) be coprime numbers. Then
\[
\sigma(m_1 m_2) = \sum_{d \mid m_1 m_2} d = \sum_{d_1 \mid m_1, d_2 \mid m_2} d_1 d_2 = \left( \sum_{d_1 \mid m_1} d_1 \right) \left( \sum_{d_2 \mid m_2} d_2 \right) = \sigma(m_1) \sigma(m_2).
\]

### 3.5. Definition
A perfect number (G. vollkommene Zahl) is a number \( n \in \mathbb{N}_1 \) such that \( \sigma(n) = 2n \).

The condition \( \sigma(n) = 2n \) can also be expressed as
\[
\sum_{d \mid n, d < n} d = n,
\]
i.e. a number \( n \) is perfect if the sum of its proper divisors equals \( n \). The smallest perfect numbers are
\[
6 = 1 + 2 + 3, \\
28 = 1 + 2 + 4 + 7 + 14.
\]
The next perfect numbers are 496, 8128. The even perfect numbers are characterized by the following theorem.

**Theorem.** a) (Euclid) If \( q \) is a prime such that \( 2^q - 1 \) is prime, then \( n := 2^{q-1}(2^q - 1) \) is a perfect number.
b) (Euler) \textit{Conversely, every even perfect number }\( n \)\textit{ may be obtained by the construction in a).}

The prove is left as an exercise.

The above examples correspond to \( q = 2, 3, 5, 7 \). For \( q = 11 \), \( 2^{11} - 1 = 2047 = 23 \cdot 89 \) is not prime.

It is not known whether there exist odd perfect numbers.

### 3.6. Möbius function \( \mu : \mathbb{N}_1 \rightarrow \mathbb{Z} \).

This rather strange looking, but important function is defined by

\[
\mu(n) := \begin{cases} 
1, & \text{for } n = 1, \\
0, & \text{if there exists a prime } p \text{ with } p^2 \mid n, \\
(-1)^r, & \text{if } n \text{ is a product of } r \text{ different primes.}
\end{cases}
\]

This leads to the following table

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \mu(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>-1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>-1</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

It follows directly from the definition that \( \mu \) is multiplicative.

### 3.7. Definition.

Let \( f : \mathbb{N}_1 \rightarrow \mathbb{C} \) be an arithmetical function. The \textit{summatory function} of \( f \) is the function \( F : \mathbb{N}_1 \rightarrow \mathbb{C} \) defined by

\[
F(n) := \sum_{d \mid n} f(d),
\]

where the sum is extended over all positive divisors \( d \) of \( n \).

### 3.8. Examples.

i) The divisor sum function

\[
\sigma(n) = \sum_{d \mid n} d
\]

is the summatory function of the identity map

\[
\iota : \mathbb{N}_1 \rightarrow \mathbb{N}_1, \quad \iota(n) := n.
\]

ii) The divisor function \( \tau : \mathbb{N}_1 \rightarrow \mathbb{N}_1 \) can be written as

\[
\tau(n) = \sum_{d \mid n} 1.
\]

Therefore \( \tau \) is the summatory function of the constant function

\[
u : \mathbb{N}_1 \rightarrow \mathbb{N}_1, \quad u(n) := 1 \text{ for all } n.
\]
3.9. **Theorem** (Summatory function of the Euler phi function). For all \( n \in \mathbb{N}_1 \)

\[
\sum_{d \mid n} \varphi(d) = n.
\]

This means that the summatory function of the Euler phi function is the identity map \( \iota : \mathbb{N}_1 \to \mathbb{N}_1 \).

**Proof.** The set \( M_n := \{1, 2, \ldots, n\} \) is the disjoint union of the sets

\[
A_d := \{m \in M_n : \gcd(m, n) = d\}, \quad d \mid n.
\]

Therefore \( n = \sum_{d \mid n} \#A_d \). We have \( \gcd(m, n) = d \iff d \mid m, d \mid n \) and \( \gcd(m/d, n/d) = 1 \). It follows that \( \#A_d = \varphi(n/d) \), hence

\[
n = \sum_{d \mid n} \#A_d = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d), \quad \text{q.e.d.}
\]

3.10. **Theorem** (Summatory function of the Möbius function).

\[
\sum_{d \mid n} \mu(d) = \begin{cases} 
1 & \text{for } n = 1, \\
0 & \text{for all } n > 1.
\end{cases}
\]

Therefore the summatory function of the Möbius function is the function

\[
\delta_1 : \mathbb{N}_1 \to \mathbb{Z}, \quad \delta_1(n) := \begin{cases} 
1 & \text{for } n = 1, \\
0 & \text{for all } n > 1.
\end{cases}
\]

**Proof.** The case \( n = 1 \) is trivial.

Now suppose \( n \geq 2 \) and let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be the canonical prime factorization of \( n \). For \( 0 \leq s \leq r \) we denote by \( D_s \) the set of all divisors \( d \mid n \) which are the product of \( s \) different primes \( \in \{p_1, \ldots, p_r\} \), \( (D_0 = \{1\}) \). For all \( d \in D_s \) we have \( \mu(d) = (-1)^s \); but \( \mu(d) = 0 \) for all divisors of \( n \) that do not belong to any of the \( D_s \). Therefore

\[
\sum_{d \mid n} \mu(d) = \sum_{s=0}^{r} \sum_{d \in D_s} \mu(d) = \sum_{s=0}^{r} (-1)^s \#D_s = \sum_{s=0}^{r} (-1)^s \binom{r}{s}
\]

\[
= (1 + (-1))^r = 0,
\]

where we have used the binomial theorem. This proves our theorem.

3.11. **Definition** (Dirichlet product). For two arithmetical functions \( f, g : \mathbb{N}_1 \to \mathbb{C} \) one defines their Dirichlet product (or Dirichlet convolution) \( f \ast g : \mathbb{N}_1 \to \mathbb{C} \) by

\[
(f \ast g)(n) := \sum_{d \mid n} f(d)g(n/d).
\]
This can be written in a symmetric way as
\[(f * g)(n) = \sum_{k\ell = n} f(k)g(\ell),\]
where the sum extends over all pairs \(k, \ell \in \mathbb{N}_1\) with \(k\ell = n\). This shows that \(f * g = g * f\) and \((f * g)(n) = \sum_{d|n} f(n/d)g(d)\).

**Example.** \((f * g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1)\).

**Remark.** Let \(f\) be an arbitrary arithmetical function and \(u\) the constant function \(u(n) = 1\) for all \(n \in \mathbb{N}_1\). Then
\[(u * f)(n) = \sum_{d|n} u(n/d)f(d) = \sum_{d|n} f(d).\]
Thus the summatory function of an arithmetical function \(f\) is nothing else than the Dirichlet product \(u * f\).

**3.12. Theorem.** If the arithmetical functions \(f, g : \mathbb{N}_1 \to \mathbb{C}\) are multiplicative, their Dirichlet product \(f * g\) is again multiplicative.

**Example.** Since the constant function \(u(n) = 1\) is clearly multiplicative, the summatory function of every multiplicative arithmetical function is multiplicative.

**Proof.** Let \(m_1, m_2 \in \mathbb{N}_1\) be two coprime numbers. Then
\[
(f * g)(m_1m_2) = \sum_{d|m_1m_2} f(d)g\left(\frac{m_1m_2}{d}\right) = \sum_{d_1|m_1, d_2|m_2} f(d_1d_2)g\left(\frac{m_1m_2}{d_1d_2}\right)
= \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1)f(d_2)g\left(\frac{m_1}{d_1}\right)g\left(\frac{m_2}{d_2}\right)
= \sum_{d_1|m_1} f(d_1)g\left(\frac{m_1}{d_1}\right) \sum_{d_2|m_2} f(d_2)g\left(\frac{m_2}{d_2}\right)
= (f * g)(m_1)(f * g)(m_2), \quad \text{q.e.d.}
\]

**3.13. Theorem.** The set \(\mathcal{F}(\mathbb{N}_1, \mathbb{C})\) of all arithmetical functions \(f : \mathbb{N}_1 \to \mathbb{C}\) is a commutative ring with unit element when addition is defined by
\[(f + g)(n) := f(n) + g(n) \quad \text{for all } n \in \mathbb{N}_1\]
and multiplication is the Dirichlet product. The unit element is the function \(\delta_1 : \mathbb{N}_1 \to \mathbb{C}\) defined by
\[\delta_1(1) := 1, \quad \delta_1(n) = 0 \quad \text{for all } n > 1.\]
Remark. The notation $\delta_1$ is motivated by the Kronecker $\delta$-symbol

$$
\delta_{ij} = \begin{cases}
1 & \text{for } i = j, \\
0 & \text{otherwise}.
\end{cases}
$$

Using this, one can write $\delta_1(n) = \delta_{1n}$.

Proof. That $\delta_1$ is the unit element is seen as follows

$$(\delta_1 * f)(n) = \sum_{d|n} \delta_1(d) f\left(\frac{n}{d}\right) = \delta_1(1) f\left(\frac{n}{1}\right) = f(n).$$

All ring axioms with exception of the associative law for multiplication are easily verified. Proof of associativity:

$$(f * (g * h))(n) = \sum_{k,\ell} f(k) g(\ell) h(n) = \sum_{i,j} \sum_{k|n} f(i) g(j) h(\ell) = \sum_{i,j} f(i) g(j) h(\ell) = (f * (g * h))(n), \quad \text{q.e.d.}$$

3.14. Theorem (Möbius inversion formula). Let $f : \mathbb{N}_1 \to \mathbb{C}$ be an arithmetical function and $F : \mathbb{N}_1 \to \mathbb{C}$ its summatory function,

$$F(n) = \sum_{d|n} f(d) \quad \text{for all } n \in \mathbb{N}_1. \quad (\ast)$$

Then $f$ can be reconstructed from $F$ by the formula

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) \quad \text{for all } n \in \mathbb{N}_1. \quad (\ast\ast)$$

Conversely, $(\ast\ast)$ implies $(\ast)$.

Proof. The formula $(\ast)$ can be written as

$$F = u * f,$$

where $u$ is the constant function $u(n) = 1$ for all $n$. Theorem 3.10 says that $u$ is the Dirichlet inverse of the Möbius function:

$$u * \mu = \mu * u = \delta_1.$$

Therefore

$$\mu * F = \mu * (u * f) = (\mu * u) * f = \delta_1 * f = f,$$

3.6
which is formula (**) Conversely, from \( f = \mu * F \) one obtains
\[
u \ast f = \nu \ast (\mu \ast F) = (\nu \ast \mu) \ast F = \delta_1 \ast F = F,\]
that is formula (*), q.e.d.

3.15. Examples. i) Applying the M"obius inversion formula to the summatory function of the Euler phi function (theorem 3.9)
\[
n = \iota(n) = \sum_{d \mid n} \varphi(d)
\]
yields \( \varphi = \mu \ast \iota \), i.e.
\[
\varphi(n) = \sum_{d \mid n} \mu(d) \iota\left(\frac{n}{d}\right) = \sum_{d \mid n} \frac{n}{d} \mu(d).
\]
This can also be written as
\[
\frac{\varphi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{d}.
\]
ii) Example 3.8.i) says \( u \ast \iota = \sigma \) which implies \( \iota = \mu \ast \sigma \), i.e.
\[
\sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d) = n.
\]
iii) Example 3.8.ii) says \( u \ast u = \tau \), hence \( u = \mu \ast \tau \), i.e.
\[
\sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) = 1 \quad \text{for all } n \geq 1.
\]
We now state a second M"obius inversion formula for functions defined on the real interval
\[
I_1 := \{ x \in \mathbb{R} : x \geq 1 \}.
\]
3.16. Theorem. For a function \( f : I_1 \to \mathbb{C} \) define \( F : I_1 \to \mathbb{C} \) by
\[
F(x) = \sum_{k \leq x} f\left(\frac{x}{k}\right) \quad \text{for all } x \geq 1, \quad (\diamond)
\]
where the sum extends over all positive integers \( k \leq x \). Then
\[
f(x) = \sum_{k \leq x} \mu(k) F\left(\frac{x}{k}\right) \quad \text{for all } x \geq 1. \quad (\diamond\diamond)
\]
Conversely, \((\diamond\diamond)\) implies \((\diamond)\).
Example. If \( f \) is the constant function \( f(x) = 1 \) for all \( x \geq 1 \), then \( F(x) = \lfloor \frac{x}{k} \rfloor = \text{greatest integer } \leq x \). The theorem implies the remarkable formula
\[
\sum_{k \leq x} \mu(k) \lfloor \frac{x}{k} \rfloor = 1 \quad \text{for all } x \geq 1.
\]
E.g. for \( x = 5 \) this reads
\[
5\mu(1) + 2\mu(2) + \mu(3) + \mu(4) + \mu(5) = 1.
\]
To prove theorem 3.16, we put it first into an abstract context.

3.17. Let \( \mathcal{F}(I_1, \mathbb{C}) \) denote the vector space of all functions \( f : I_1 = [1, \infty[ \to \mathbb{C} \). We define an operation of the ring of all arithmetical functions on this vector space
\[
\mathcal{F}(N_1, \mathbb{C}) \times \mathcal{F}(I_1, \mathbb{C}) \to \mathcal{F}(I_1, \mathbb{C}) \quad (\alpha, f) \mapsto \alpha \triangleright f,
\]
where
\[
(\alpha \triangleright f)(x) := \sum_{k \leq x} \alpha(k) f\left(\frac{x}{k}\right).
\]

3.18. Theorem. With the above operation, \( \mathcal{F}(I_1, \mathbb{C}) \) becomes a module over the ring \( \mathcal{F}(N_1, \mathbb{C}) \).

Proof. It is clear that \( \mathcal{F}(I_1, \mathbb{C}) \) is an abelian group with respect to pointwise addition \((f + g)(x) = f(x) + g(x)\). So it remains to verify the following laws (for \( \alpha, \beta \in \mathcal{F}(N_1, \mathbb{C}) \) and \( f, g \in \mathcal{F}(I_1, \mathbb{C}) \)).

i) \( \alpha \triangleright (f + g) = \alpha \triangleright f + \alpha \triangleright g \),
ii) \( (\alpha + \beta) \triangleright f = \alpha \triangleright f + \beta \triangleright f \),
iii) \( \alpha \triangleright (\beta \triangleright f) = (\alpha * \beta) \triangleright f \),
iv) \( \delta_1 \triangleright f = f \).

The assertions i) and ii) are trivial. The associative law iii) can be seen as follows
\[
(\alpha \triangleright (\beta \triangleright f))(x) = \sum_{k \leq x} \alpha(k)(\beta \triangleright f)\left(\frac{x}{k}\right) = \sum_{k \leq x} \alpha(k) \sum_{\ell \leq x/k} \beta(\ell) f\left(\frac{x}{k\ell}\right)
\]
\[
= \sum_{k\ell \leq x} \alpha(k)\beta(\ell) f\left(\frac{x}{k\ell}\right)
\]
\[
= \sum_{n \leq x} \sum_{k\ell = n} \alpha(k)\beta(\ell) f\left(\frac{x}{n}\right)
\]
\[
= \sum_{n \leq x} (\alpha * \beta)(n) f\left(\frac{x}{n}\right) = ((\alpha * \beta) \triangleright f)(x).
\]
Proof of iv):

\[
(\delta_1 \triangleright f)(x) = \sum_{k \leq x} \delta_1(k) f\left(\frac{x}{k}\right) = \delta_1(1) f\left(\frac{x}{1}\right) = f(x), \quad \text{q.e.d.}
\]

3.19. Now we take up the proof of theorem 3.16. Equation (\bigtriangledown) can be written as

\[F = u \triangleright f\]

with the constant function \(u(n) = 1\). Multiplying this equation by the Möbius function yields

\[\mu \triangleright F = \mu \triangleright (u \triangleright F) = (\mu \ast u) \triangleright f = \delta_1 \triangleright f = f,
\]

which is equation (\bigtriangledown\bigtriangledown). Conversely, from \(f = \mu \triangleright F\) it follows

\[u \triangleright f = u \triangleright (\mu \triangleright F) = (u \ast \mu) \triangleright F = \delta_1 \triangleright F = F,
\]

which is equation (\bigtriangledown), q.e.d.