



universität
wien

BACHELORARBEIT

Titel der Bachelorarbeit
The ring of number-theoretic functions

Verfasser
Jakob Preininger

angestrebter akademischer Grad
Bachelor of Science

Wien, im März 2010

Studienkennzahl lt. Studienblatt: A 033 621
Studienrichtung lt. Studienblatt: Mathematik
Betreuer: Dr. Leonhard Summerer

CONTENTS

Acknowledgement	1
1. Introduction	1
2. Definition and Examples	2
3. The Isomorphism with \mathbb{C}_ω	3
4. Norm, Degree and Units	6
5. The Group of Multiplicative Functions	7
6. Primes and Factorisation	9
References	12

ACKNOWLEDGEMENT

I would like to thank my supervisor Professor Leonhard Summerer for his valuable comments, corrections and his indestructible optimism. I also thank my colleague Christian Schmid and my father Helmut Preininger for proof-reading.

1. INTRODUCTION

The main issue of this paper is to introduce the arithmetic product, the most important product on the set $\mathbb{C}^{\mathbb{N}}$ of number-theoretic functions. This set forms an integral domain under ordinary addition and the arithmetic product. In opposition to the set of formal power series in one variable the domain $\mathbb{C}^{\mathbb{N}}$ is not a principal ideal domain. But we will see that it is isomorphic to the ring \mathbb{C}_ω of formal power series in countably infinitely many variables. This fact will make it a lot easier for us to understand the ring $\mathbb{C}^{\mathbb{N}}$ in more detail. We will conclude that the units in our ring are all number-theoretic functions f with $f(1) \neq 0$ and that we can transfer the concept of the degree from \mathbb{C}_ω to $\mathbb{C}^{\mathbb{N}}$. Furthermore we will see that the set of multiplicative number-theoretic functions forms a subgroup of the group of units. Finally we will be able to show that $\mathbb{C}^{\mathbb{N}}$ is a factorial ring. This has been an unsolved problem until 1959 when Cashwell and Everett proved it for the first time in [2].

2. DEFINITION AND EXAMPLES

In the following n will always stand for a natural number that has the special prime factorisation $n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ where p_i are the prime numbers (w.l.o.g. we may assume $p_1 = 2, p_2 = 3$ etc.), $\alpha_i \in \mathbb{N}_0$ and $\alpha_i = 0$ for almost all i .

Any map f from the natural numbers \mathbb{N} into the complex field \mathbb{C} is called a number-theoretic (or arithmetic) function. In analysis f would simply be some complex-valued sequence but we will look at it from a different point of view.

Some examples are known from elementary number theory. Probably the most famous is Euler's totient function φ , which counts the number of natural numbers smaller or equal to n that are relative prime to n .

Other examples are the number-of-divisors function

$$\tau(n) = \sum_{d|n} 1 = \prod_{i=1}^k (\alpha_i + 1),$$

the sum-of-divisors function

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^k (1 + p_i + \cdots + p_i^{\alpha_i})$$

or the function v_p that counts the number of factors p in n given by

$$v_p(n) = \max \{ \alpha \in \mathbb{N} : p^\alpha \mid n \}.$$

But we will also need quite elementary functions like the function e_0 , which is zero except for $n = 1$ where it has the value one

$$e_0(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}.$$

Other elementary functions we will use are the constant function $e(n) = 1$ and the identity $I(n) = n$.

Finally there is a quite important function in number theory, the so called Möbius function μ given by

$$\mu(n) = \begin{cases} (-1)^r & n = p_1 \cdots p_r \\ 0 & n \text{ not square free} \end{cases}$$

where $r \geq 0$ and p_1, \dots, p_r are distinct primes.

We want to give the set of these functions some algebraic structure that respects their number-theoretical properties.

So we define a componentwise addition on the set $\mathbb{C}^{\mathbb{N}}$ of number-theoretic functions by

$$(f + g)(n) = f(n) + g(n)$$

and a multiplication by the following arithmetic product

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

With this product we have

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

and

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

Thus the functions τ and σ can be written as products of the elementary functions e and I .

Note that the arithmetic product looks similar to the more elementary Cauchy product

$$(f \cdot g)(n) = \sum_{m \in \mathbb{N}_0} f(m) g(n - m)$$

which is used in the ring of complex formal power series in one variable. We will show that the arithmetic product and the componentwise addition give the set of number theoretic functions a ring structure that is isomorphic to the ring of formal power series in countably infinitely many variables \mathbb{C}_ω and hence an integral domain. Moreover it will turn out to be a factorial ring like formal power series are in finitely many variables.

3. THE ISOMORPHISM WITH \mathbb{C}_ω

We define \mathbb{C}_ω to be the set of complex formal power series in countably infinitely many indeterminates x_1, x_2, \dots i.e. for $A \in \mathbb{C}_\omega$ we have

$$A = \sum A_i x_1^{i_1} x_2^{i_2} \cdots,$$

where the summation extends over all infinite sequences $i = (i_1, i_2, \dots) \in \mathbb{N}^{\mathbb{N}}$ with finite support. So every term involves only finitely many variables x_i , but the sum may have infinitely many terms. Like power series in finitely many variables the set \mathbb{C}_ω forms a commutative ring with unity under ordinary addition and multiplication.

Consider the map

$$\begin{aligned} \Phi : \mathbb{C}^{\mathbb{N}} &\rightarrow \mathbb{C}_\omega \\ f &\mapsto \Phi(f) := \sum_{n \in \mathbb{N}} f(n) x_1^{\alpha_1} x_2^{\alpha_2} \dots \end{aligned}$$

The map Φ is injective because if $\Phi(f) = \Phi(g)$ then for every $n \in \mathbb{N}$ we get $f(n) = g(n)$ and so $f = g$. Moreover, for $A = \sum A_i x_1^{i_1} x_2^{i_2} \dots \in \mathbb{C}_\omega$ the number-theoretic function $f_A(n) = A_i$ for $i = (\alpha_1, \alpha_2, \dots)$ is the inverse image of A under Φ . So Φ is bijective.

We note that for all $f, g \in \mathbb{C}^{\mathbb{N}}$ we have

$$\Phi(f + g) = \sum_{n \in \mathbb{N}} (f + g)(n) x_1^{\alpha_1} x_2^{\alpha_2} \dots = \Phi(f) + \Phi(g)$$

and

$$\begin{aligned} \Phi(f \star g) &= \sum_{n \in \mathbb{N}} (f \star g)(n) x_1^{\alpha_1} x_2^{\alpha_2} \dots \\ &= \sum_{n \in \mathbb{N}} \sum_{d_1 d_2 = n} f(d_1) g(d_2) x_1^{\beta_1 + \gamma_1} x_2^{\beta_2 + \gamma_2} \dots \\ &= \left(\sum_{d_1 \in \mathbb{N}} f(d_1) x_1^{\beta_1} x_2^{\beta_2} \dots \right) \left(\sum_{d_2 \in \mathbb{N}} g(d_2) x_1^{\gamma_1} x_2^{\gamma_2} \dots \right) \\ &= \Phi(f) \Phi(g) \end{aligned}$$

where $d_1 = p_1^{\beta_1} p_2^{\beta_2} \dots$ and $d_2 = p_1^{\gamma_1} p_2^{\gamma_2} \dots$. Hence $\mathbb{C}^{\mathbb{N}}$ is also a commutative ring with unity and Φ is an isomorphism of rings.

With this isomorphism we can show some easy relations between number-theoretic functions. First note that the unity in $\mathbb{C}^{\mathbb{N}}$ is $\Phi^{-1}(1) = e_0$.

For the constant function $e(n) = 1$ we have

$$\begin{aligned}\Phi(e) &= \sum_{n \in \mathbb{N}} e(n) x_1^{\alpha_1} x_2^{\alpha_2} \cdots = \sum_{n \in \mathbb{N}} x_1^{\alpha_1} x_2^{\alpha_2} \cdots \\ &= \left(\sum_{\alpha_1 \in \mathbb{N}_0} x_1^{\alpha_1} \right) \left(\sum_{\alpha_2 \in \mathbb{N}_0} x_1^{\alpha_2} \right) \cdots \\ &= \prod_{i=1}^{\infty} (1 - x_i)^{-1}.\end{aligned}$$

Similarly for τ we can compute

$$\begin{aligned}\Phi(\tau) &= \sum_{n \in \mathbb{N}} \tau(n) x_1^{\alpha_1} x_2^{\alpha_2} \cdots = \sum_{n \in \mathbb{N}} \prod_{i \in \mathbb{N}} ((\alpha_i + 1) x_i^{\alpha_i}) \\ &= \prod_{i \in \mathbb{N}} \left(\sum_{\alpha_i \in \mathbb{N}_0} (\alpha_i + 1) x_i^{\alpha_i} \right) = \prod_{i \in \mathbb{N}} (1 + 2x_i + 3x_i^2 + \cdots) \\ &= \prod_{i \in \mathbb{N}} ((1 + x_i + x_i^2 + \cdots) + x_i(1 + x_i + x_i^2 + \cdots) + \cdots) \\ &= \prod_{i \in \mathbb{N}} (1 + x_i + x_i^2 + \cdots)^2 = \prod_{i \in \mathbb{N}} (1 - x_i)^{-2}.\end{aligned}$$

Not surprisingly we again conclude $\tau = e \star e$.

Finally for the Möbius function μ we get

$$\begin{aligned}\Phi(\mu) &= \sum_{n \in \mathbb{N}} \mu(n) x_1^{\alpha_1} x_2^{\alpha_2} \cdots \\ &= \prod_{i \in \mathbb{N}} \sum_{\alpha_i \in \{0,1\}} (-1)^{\alpha_i} x_i^{\alpha_i} = \prod_{i \in \mathbb{N}} (1 - x_i) \\ &= \Phi(e)^{-1},\end{aligned}$$

hence the Möbius function is the multiplicative inverse to e .

With this in hand, we easily deduce the so called Möbius inversion formula. If f is a number theoretic function and F is its summatorial function given by

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

then f can be expressed by F as

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

We deduce another interesting relation between the Möbius function and the floor function $\lfloor \cdot \rfloor$ by the following equalities:

$$\begin{aligned} 1 &= \sum_{m=1}^n e_0(m) = \sum_{m=1}^n \sum_{d|m} \mu(d) e\left(\frac{m}{d}\right) = \\ &= \sum_{d=1}^n \sum_{l=1}^{\lfloor \frac{n}{d} \rfloor} \mu(d) \\ &= \sum_{d=1}^n \mu(d) \left\lfloor \frac{n}{d} \right\rfloor. \end{aligned}$$

4. NORM, DEGREE AND UNITS

In order to determine which functions in $\mathbb{C}^{\mathbb{N}}$ do have an inverse we have to define a norm N as follows. For any nonzero number-theoretic function $f \in \mathbb{C}^{\mathbb{N}}$ we define $N(f)$ to be the smallest natural number n such that $f(n)$ is nonzero. For $f = 0$ we additionally define $N(f) = 0$.

If f and g are nonzero functions in $\mathbb{C}^{\mathbb{N}}$ with $N(f) = a$ and $N(g) = b$ then for every $n < ab$ we get $(f \star g)(n) = 0$ and for $n = ab$ we have $(f \star g)(n) = f(a)g(b) \neq 0$. So $N(f \star g) = N(f)N(g)$ i.e. the norm N is a multiplicative function. An immediate consequence is that $\mathbb{C}^{\mathbb{N}}$ has no proper divisors of zero i.e. $\mathbb{C}^{\mathbb{N}}$ is an integral domain.

Obviously every unit u must have $N(u) = 1$. To see that the converse is also true let u be in $\mathbb{C}^{\mathbb{N}}$ with $u(1) = c \neq 0$. We have to find u' such that $u \cdot u' = e_0$. For $n = 1$ this implies $u'(1) = \frac{1}{c}$ and for $n \neq 1$ we get

$$\sum_{d|n} u(d) u'\left(\frac{n}{d}\right) = e_0(n) = 0.$$

Consequently for $u'(n)$ we get

$$u'(n) = -\frac{1}{c} \sum_{1 < d|n} u(d) u'\left(\frac{n}{d}\right).$$

Since $\frac{n}{d} < n$ for $d > 1$, $u'(n)$ can be constructed inductively using the above equation. This shows that all $u \in \mathbb{C}^{\mathbb{N}}$ with $u(1) \neq 0$ are units. In view of the isomorphism onto \mathbb{C}_ω , we conclude that all formal power series with a nonzero constant term are invertible just as in the case of formal power series in one variable.

For formal power series one can define its degree as the smallest degree of its nonzero monomials. To carry over this notion to our

number-theoretic functions we will at first define $\lambda(n)$ as the number of prime factors in n (i.e. $\lambda(n) = \alpha_1 + \dots + \alpha_k$). Then for any nonzero number-theoretic function we define its degree as

$$D(f) = \min \{ \lambda(n) : f(n) \neq 0 \},$$

which corresponds to the given definition on \mathbb{C}_ω . Hence for nonzero $f, g \in \mathbb{C}^\mathbb{N}$ the equation

$$D(f \star g) = D(f) + D(g)$$

holds. Furthermore f is a unit if and only if $D(f) = 0$.

5. THE GROUP OF MULTIPLICATIVE FUNCTIONS

We call a nonzero number-theoretic function f multiplicative if for any relatively prime natural numbers m and n we have

$$f(m \star n) = f(m) f(n).$$

For $n = 1$ this yields $f(m) = f(m) f(1)$ and since f is nonzero ($f(m) \neq 0$ for some m) we get $f(1) = 1$. So in particular all multiplicative functions are units.

For $n > 1$ we get

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$$

and we can conclude that f is uniquely determined by its values at the powers of primes.

The set M of multiplicative functions play an important role in number theory since most of the important number theoretic functions are multiplicative (e.g. φ , τ , σ and μ). We will see that M is a subgroup of the group of units in $\mathbb{C}^\mathbb{N}$, which underlines again the importance of the introduced arithmetic product.

If $f, g \in M$ and $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ then

$$\begin{aligned}
(f \star g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) \\
&= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right) \right) \left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right) \right) \\
&= (f \star g)(m) (f \star g)(n).
\end{aligned}$$

Hence $M \star M \subseteq M$.

It remains to show that for f multiplicative its inverse f^{-1} is also multiplicative. Given f in M define f' in M as follows. For each prime p and each natural number $\alpha \geq 1$ let $f'(p^\alpha)$ be defined by the relation

$$\sum_{d|p^\alpha} f(d) f'\left(\frac{p^\alpha}{d}\right) = 0.$$

Since f' should be in M it is uniquely determined by those values. Now both f and f' are in M and we can conclude that $f \cdot f'$ is in M . But by definition $(f \cdot f')(p^\alpha) = 0$. So $f \cdot f' = e_0$ and f' is inverse to f . Hence M is indeed a subgroup of the group of units in $\mathbb{C}^{\mathbb{N}}$.

Another way to see this is by using the power series notation. For a multiplicative f we have

$$\begin{aligned}
\Phi(f) &= \sum_{n \in \mathbb{N}} f(n) x_1^{\alpha_1} x_2^{\alpha_2} \cdots = \sum_{n \in \mathbb{N}} \prod_{i \in \mathbb{N}} f(p_i^{\alpha_i}) x_i^{\alpha_i} \\
&= \prod_{i \in \mathbb{N}} \sum_{\alpha_i \in \mathbb{N}_0} f(p_i^{\alpha_i}) x_i^{\alpha_i} = \prod_{i \in \mathbb{N}} s_i(x_i)
\end{aligned}$$

where $s_i(x_i) = \sum_{\alpha_i \in \mathbb{N}_0} f(p_i^{\alpha_i}) x_i^{\alpha_i}$ are formal power series in one variable. Note that since $f(1) = 1$ the constant term in s_i is always equal to one. Conversely if s_i are power series of the form

$$s_i(x_i) = \sum_{k \in \mathbb{N}_0} s_{i,k} x_i^k$$

with $s_{i,0} = 1$ its formal product s corresponds to a multiplicative function f given by

$$f(n) = \prod_{i \in \mathbb{N}} s_{i, \alpha_i}.$$

Since formal power series of the form $s = \prod_{i \in \mathbb{N}} s_i(x_i)$ form a subgroup of the group of units in \mathbb{C}_ω , so do the multiplicative functions.

6. PRIMES AND FACTORISATION

In this chapter we will show that any number-theoretic function can be written as a finite product of irreducible elements and that this factorisation is unique up to order and units i.e. that $\mathbb{C}^{\mathbb{N}}$ is a factorial ring.

Since $D(f \cdot \star g) = D(f) + D(g)$ and $D(f) = 0$ only for units, we can conclude that every f with $D(f) = 1$ is irreducible. Moreover for any given f with $D(f) = n$ we know that f can be written as a product of not more than n irreducible elements. Hence every f can be written as a finite product of irreducible elements.

To show that this factorisation is unique is far more difficult. In fact, we will prove that if factorisation fails, then it fails already in a rather simple way.

First divide the nonzero and non unit number-theoretic functions into two sets: The normal elements whose factorisation is unique and abnormal elements which can be factored in two essentially different ways. Then all irreducible elements are normal.

Now let f be an abnormal element with minimal norm $N(f)$. Such f can be written in two essentially different ways as a product of irreducible elements:

$$f = f_1 \star \cdots \star f_k = g_1 \star \cdots \star g_r.$$

Here no f_i is associated to any g_j because otherwise one could cancel these elements and obtain an abnormal element of smaller norm. Moreover without loss of generality we may assume $N(f_1) \leq \cdots \leq N(f_k)$, $N(g_1) \leq \cdots \leq N(g_r)$ and $N(f_1) \leq N(g_1)$. Then the following inequality chain holds

$$N(f_1)N(g_1) \leq N(g_1)N(g_2) \leq N(f).$$

Suppose now that $N(f_1)N(g_1) < N(f)$ i.e. the outer inequality is strict, and define $h = f - f_1g_1$. Then $h \neq 0$ and $N(h) = N(f_1g_1) < N(f)$. So h is normal and with $f_1 \mid h$ and $g_1 \mid h$ we get $f_1g_1 \mid h$. This shows that $f_1g_1 \mid f = f_1 \star \cdots \star f_k$ and thus $g_1 \mid f_2 \star \cdots \star f_k$. Since

$f_2 \star \cdots \star f_k$ is normal it follows that g_1 is associated to some f_i which contradicts our assumptions.

So we now know that

$$N(f_1)N(g_1) = N(f)$$

and therefore $k = r = 2$ and $N(f_1) = N(f_2) = N(g_1) = N(g_2)$.

Hence we are reduced to a situation involving only products of two functions $f_1 \star f_2$ and $g_1 \star g_2$. In this case let $A = \Phi(f_1)$, $B = \Phi(f_2)$, $C = \Phi(g_1)$ and $D = \Phi(g_2)$ be the power series representations of the above factors. Now we have

$$AB = CD$$

with irreducible $A, B, C, D \in \mathbb{C}_\omega$. If A, B, C, D were irreducible formal power series in finitely many indeterminates (i.e. elements of a factorial ring!) we would know that A is associated to either C or D and we would be done.

For $A = A(x_1, x_2, \dots) \in \mathbb{C}_\omega$ we define

$$(A)_l = A(x_1, \dots, x_l, 0, 0, \dots)$$

to be the series we get from A by deleting all terms of A having at least one factor x_i with $i > l$. The map $A \mapsto (A)_l$ is then an endomorphism of rings in \mathbb{C}_ω and its image set \mathbb{C}_l is the set of formal power series in l indeterminates. These are as already mentioned factorial rings and we have $\mathbb{C}_1 \subset \mathbb{C}_2 \subset \cdots \subset \mathbb{C}_\omega$. Moreover if $(A)_l$ is irreducible for some l then $(A)_k$ is irreducible as well for all $k > l$.

We say that a sequence S_n in \mathbb{C}_ω is telescopic if for arbitrary natural n, m with $n > m$ we have that $(S_n)_m = S_m$. Every formal power series in \mathbb{C}_ω is defined by its monomials and every monomial contains only finitely many indeterminates x_j . So for any infinite telescopic sequence S_n there is a uniquely determined element S with $(S)_m = S_m$ for all $m \in \mathbb{N}$.

If we could find l_A, l_B, l_C, l_D such that $(A)_{l_A}, (B)_{l_B}, (C)_{l_C}, (D)_{l_D}$ are irreducible we would be able to define $l = \max\{l_A, l_B, l_C, l_D\}$ and for every $k \geq l$

$$(A)_k (B)_k = (C)_k (D)_k$$

would imply that $(A)_k$ is associated to $(C)_k$ or $(D)_k$. The pigeonhole principle would guarantee the existence of an infinite increasing natural sequence (k_m) such that either $(A)_{k_m}$ is associated to $(C)_{k_m}$ or $(A)_{k_m}$ is associated to $(D)_{k_m}$. Without loss of generality we may assume the former case and that $k_m = m$. So there is a sequence U_m of units in $\mathbb{C}_m \subset \mathbb{C}_\omega$ with $(A)_m U_m = (C)_m$. Moreover U_m is telescopic and we get a unit U in \mathbb{C}_ω with $(U)_m = U_m$ for every m . Now if $AU \neq C$ we would get that the power series $AU - C$ has some nonzero monomial. Again this monomial has finitely many variables and hence there is some m such that $(AU - C)_m \neq 0$ which is a contradiction to $(A)_m (U)_m = (C)_m$. So $AU = C$ and hence A is associated to C .

It thus only remains to show that for every irreducible A there is some l_A such that $(A)_{l_A}$ is irreducible. Assume we have $A \in \mathbb{C}_\omega$ with $(A)_m$ reducible for every natural m . Let L be the smallest natural number such that $(A)_L$ is nonzero. Then by assumption for every $l \geq L$ there is some proper divisor R_l of $(A)_l$. So we have a sequence

$$\begin{aligned} \kappa_L &= \{R_L\} \\ \kappa_{L+1} &= \{(R_{L+1})_L, R_{L+1}\} \\ \kappa_{L+2} &= \{(R_{L+2})_L, (R_{L+2})_{L+1}, R_{L+2}\} \\ &\vdots \end{aligned}$$

of finite telescopic sequences κ_i of proper divisors of $(A)_L, (A)_{L+1}$ etc.

For any fixed $l \geq L$ unique factorisation holds in \mathbb{C}_l and hence there are only finitely many non associated factors of $(A)_l$. So infinitely many κ_{i_L} have their first entry associated to one proper divisor R_L^* . Of those κ_{i_L} there are again infinitely many $\kappa_{i_{L+1}}$ with their second entry associated to some R_{L+1}^* for which $(R_{L+1}^*)_L = R_L^*$ holds etc. By this diagonal argument we get an infinite telescopic sequence

$$\kappa^* = \{R_L^*, R_{L+1}^*, \dots\}$$

which then defines a proper divisor R^* of A . Hence A is reducible and the proof is complete.

REFERENCES

- [1] BUNDSCHUH, P., Einführung in die Zahlentheorie, Springer, Berlin-Heidelberg-New York, 1988 (5. Aufl. 2002).
- [2] CASHWELL, E.D., EVERETT, C.J., The ring of number-theoretic functions, Pacific J. Math. 9 (1959), 975-985.
- [3] SIVARAMAKRISHNAN, R., Classical Theory of Arithmetic Functions, Marcel Dekker Inc., New York, 1989