Generalized Number-Theoretic Functions

MAGA, Péter

1 Definitions, notations and basic properties

Let R be an integral domain, that is, a commutative ring with a unit element and without zero divisor. We call $x, y \in R$ *associates* ($x \sim y$) if there exists a unit element u in R such that $ux = y$. This equivalence relation partitions R into associate classes, we denote by $A : R \setminus \{0\} \to R'$ the function that maps every element to its associate class. We will assume that R is a unique factorization domain.
Let $\mathbb{F}$ be an arbitrary field. We denote the set of $R' \to \mathbb{F}$ functions by $R\mathbb{F}$ and call them the $\mathbb{F}$-valued number-theoretic functions. Informally, $R\mathbb{F}$ consists of those functions $R \to \mathbb{F}$, which are constant on the associate classes. We denote the unit element by 1 and the zero element by 0 in the case of the field and the ring, as well.
We introduce an algebraic structure on $R\mathbb{F}$ as follows. For $f, g \in R\mathbb{F}$ addition is defined as

$$(f + g)(r) = f(r) + g(r),$$

whereas the product of f and g is given by the convolution formula:

$$(f * g)(r) = \sum_{x|r} f(x)g(r/x).$$

Note the above sum is finite due to the unique factorization property of R.

Unit element, constant functions. Consider the function

$$u(r) = \begin{cases} 1, & \text{if } r \sim 1, \\ 0, & \text{if } r \nsim 1. \end{cases}$$

One can readily check that $R\mathbb{F}$ is a commutative ring in which u is a unit element. For any $c \in \mathbb{F}$, we denote by $\mathbf{c}$ the constant function $\mathbf{c}(r) = c$.

Function Ω, well-ordering, zero divisors. We define Ω as the number of prime divisors. Precisely, if $r = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$, then let $\Omega(r) = a_1 + \ldots + a_s$. Ω is constant on the associate classes, so we can consider it as a function on R', as well. Note that Ω is a totally additive number-theoretic function on R, that is, $\Omega(ab) = \Omega(a) + \Omega(b)$ for all $a, b \in R$.
Using Ω, we define a well-ordering $<$ on R'. We start with any well-ordering of the prime elements of R' and extend it as follows. Let $r_1 = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}, r_2 = p_1^{b_1} \cdot \ldots \cdot p_s^{b_s}$ $(p_1 < \ldots < p_s)$. We say that $r_1 < r_2$ if either $\Omega(r_1) < \Omega(r_2)$ or $\Omega(r_1) = \Omega(r_2)$ and $a_j > b_j$, $a_i = b_i$ $(i < j)$ holds for some index j. It is easy to check that $<$ is a well-ordering on R'.
For $f, g \neq \mathbf{0}$ choose $r, s \in R'$ that are minimal (with respect to $<$) and satisfy $f(r), g(s) \neq 0$. Then $(f * g)(rs) = f(r)g(s) \neq 0$, demonstrating that there are no zero divisors in $R\mathbb{F}$.

Units. Next we determine the units of $R\mathbb{F}$. We claim that $f \in R\mathbb{F}$ is unit if and only if $f(1) \neq 0$. Indeed, if $f(1) \neq 0$, we can define $f^{-1}(r)$ recursively by $\Omega(r)$. Let $f^{-1}(1) = 1/f(1)$ and if $\Omega(r) > 0$, then the only possibility for $f^{-1}(r)$:

$$0 = u(r) = (f * f^{-1})(r) = \sum_{x|r, \Omega(x)<\Omega(r)} f(r/x) f^{-1}(x) + f(1) f^{-1}(r),$$

which implies that $f^{-1}(r)$ exists and well-defined. It is easy to check that $f * f^{-1} = u$. On the other hand, if $f(1) = 0$, then $(f * g)(1) = 0$ for all $g \in R\mathbb{F}$.

This simple condition on the invertible elements shows that $M = \{f \in R\mathbb{F} \mid f(1) = 0\}$ is the only maximal ideal in $R\mathbb{F}$ that in fact contains all proper ideals. That is, $R\mathbb{F}$ is a *local ring.*

Support, norm. For $f \in R\mathbb{F}$ and let $\mathrm{supp}(f) = \{R' \mid f(r) \neq 0\}$ be the *support* of f. If $f \neq \mathbf{0}$, then let $N(f) = \min_< \mathrm{supp}(f)$ be the *norm* of f. One can check that $N(f * g) = N(f)N(g)$. If f and g differ only in a unit factor, then $N(f) = N(g)$. The converse is only true in the following sense. If $f \mid g$ and $N(f) = N(g)$, then $f \sim g$.

Special functions. The definition of Ω was motivated by the $R = \mathbb{Z}$ case. Let us examine the most important number-theoretic functions: which of them make sense over a general unique factorization domain?

The constant functions obviously make sense. $\mathbf{0}$ and $\mathbf{1}$ play special rôle: $\mathbf{0}$ is the null element of $R\mathbb{F}$; convolution of $\mathbf{1}$ and an arbitrary f gives the *summation function* of f.

We can define ω as the number of the different prime divisors, that is, if $r = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$, then $\omega(r) = s$. This function is additive, but not totally: $\omega(ab) = \omega(a) + \omega(b)$ holds if and only if a and b have no common prime divisor.

Let us consider the Möbius function. If r is not square-free, then let $\mu(r) = 0$, and if r is square-free, then let $\mu(r) = (-1)^{\Omega(r)}$. Note that if the characteristic of $\mathbb{F}$ is 2, then the range of μ is $\{0, 1\}$. This function is in fact the inverse of $\mathbf{1}$.

Using the associativity of the convolution, one can prove the following theorems. Duality: if F, G are the summation functions of f, g, respectively, then $F * g = f * G$. Möbius Inversion Formula: if F is the summation function of f, then $f = F * \mu$.

2 Prime factorization in $R\mathbb{F}$

Our next aim is to show that $R\mathbb{F}$ is a unique factorization domain, that is, every $f \in R\mathbb{F}$ number-theoretic function can be written as a product of irreducible number-theoretic functions and this representation is unique up to the order and some unit factors. We call a function *irreducible* if its only divisors are the units and its associates. We call a function f *prime* if $f \mid ab$ implies that $f \mid a$ or $f \mid b$. Of course, we do not call $\mathbf{0}$ and the units irreducible or prime.

It is well-known that unique factorization is equivalent to the following two conditions:

(1) (*chain condition*) if (f_n) is an infinite chain of functions such that $f_{n+1} \mid f_n$ for all n, then there is an n_0 such that $f_n \sim f_{n_0}$ for all $n > n_0$;

(2) all irreducible elements are primes (note that it is easy to check that primes are irreducibles in every case).

Indeed, the existence of factorization is provided by (1) and the uniqueness is provided by (2). In the following, we indicate (1), and instead of proving (2), we prove the uniqueness directly.

Before starting our proof, we make a few remarks. In 1959, E. D. Cashwell and C. J.

Everett [1] showed that unique factorization holds if $R = \mathbb{Z}$. Our proof is based on theirs and combined with some transfinite tools. One can read other but similar methods in [4] and [5] where the authors prove a more general (and more complicated) statement.
We will introduce an isomorphism between $R\mathbb{F}$ and the corresponding ring of formal power series.
Depending on the number of prime elements of R (or equivalently, the number of formal variables), we talk about the *finite* and the *infinite* case. In this paper, we examine the infinite one. In the finite case, other, but very interesting algebraic methods work. One can define the so-called *Weierstrass Polynomials.* A Weierstrass Polynomial of the power series ring $\mathbb{F}(x_1, \ldots, x_n, w)$ is a polynomial of the form

$$a_m w^m + \ldots + a_1 w + a_0,$$

where $a_j \in \mathbb{F}(x_1, \ldots, x_n)$. Using Weierstrass Polynomials and the fact that every ring of polynomials over a unique factorization domain is a unique factorization domain, we can prove our theorem. For details, see [2], [3] and [6].

Proof of (1). Let us suppose that $f_{n+1} \mid f_n$ $(n \in \mathbb{N})$ is an infinite chain. Consider the following sequence: $N(f_1), N(f_2), \ldots$. This is decreasing (with respect to $<$) and because of the well-ordering of $<$, is constant from a certain point on. Accordingly, all functions f_n are associates if n is large enough. □

Proof of the uniqueness. Our proof depends on the following reduction lemma due to Lindemann and Davenport. For the sake of completeness, we include the short proof.
Reduction Lemma. *Let us suppose that the unique factorization falls in $R\mathbb{F}$. Then there exists a function f with essentially different factorizations $f = s_1 s_2 = t_1 t_2$ such that the irreducibles s_1, s_2, t_1, t_2 are of the same norm.*
Proof. Let us suppose that uniqueness falls. Let f be an element of minimal norm and of the property that there are at least two different factorization into irreducibles: $f = s_1 \cdot \ldots \cdot s_m = t_1 \cdot \ldots \cdot t_n$. It is clear that $m, n > 1$ and $s_i \not\sim t_j$. We can suppose that $N(s_1) \leq \ldots \leq N(s_m), N(t_1) \leq \ldots \leq N(t_n), N(s_1) \leq N(t_1)$. Hence

$$N(s_1 t_1) = N(s_1)N(t_1) \leq N(t_1)N(t_2) = N(t_1 t_2) \leq N(f).$$

Assume that $N(s_1 t_1) < N(f)$. Consider $g = f - s_1 t_1$, $g \neq \mathbf{0}$. Hence $s_1 \mid g, t_1 \mid g$ and $N(g) < N(f)$ (property of the norm). Because of this strict inequality, g has unique factorization into irreducibles, which implies that $s_1 t_1 \mid g$. Hence $s_1 t_1 \mid f$, $h s_1 t_1 = s_1 \cdot \ldots \cdot s_m$, $f/s_1 = h t_1 = s_2 \cdot \ldots \cdot s_m$. The fact that f/s_1 has at least two different factorization into irreducibles is a contradiction.
In the inequality above, equality must hold. This implies $n = 2, m = 2$ and the fact that s_1, s_2, t_1, t_2 are of the same norm. □

Let $(p_i)_{i \in I}$ be the well-ordered set of primes of R. Accordingly, let $(x_i)_{i \in I}$ be a well-ordered set of formal variables. With every element $f \in R\mathbb{F}$, we associate a formal power series as follows. If $r = p_{i_1}^{a_1} \cdot \ldots \cdot p_{i_s}^{a_s}$, then let $m(r) = x_{i_1}^{a_1} \cdot \ldots \cdot x_{i_s}^{a_s}$ and let

$$\mathcal{P}(f) = \sum_{r \in R'} f(r) m(r).$$

One can check that we gave an isomorphism between the ring of number-theoretic functions and the ring of the formal power series. It is sufficient to show that the ring of formal power series is a unique factorization domain.

We denote the ring of formal series by F_I. If $\alpha < \beta < I$ are ordinals, then we consider the corresponding rings as $F_\alpha \subset F_\beta \subset F_I$ and we think about them as the ring of the "first α" or "first β" variables. If $A \in F_I$ and $\alpha < I$, then $(A)_\alpha$ is the element of F_α that we get by dropping the variables of greater index. It is easy to check that $(AB)_\alpha = (A)_\alpha(B)_\alpha$.

Applying a standard trick, we can change the well-ordering of the variables such that I is not just an ordinal, but a cardinal, as well, that is, if $\alpha < I$, then $|\alpha| < |I|$. We proceed by transfinite induction, so let us suppose that unique factorization holds in F_α for every $\alpha < I$.
Let $\mathbf{0} \neq A \in F_I$. There exist some minimal $L(A)$ such that $\beta \geq L(A)$ implies that $(A)_\beta \neq \mathbf{0}$.
It is clear that if $(A)_\alpha$ is irreducible for some $\alpha < I$, then A is irreducible. We call an irreducible element A *finitely irreducible* if there is some $\alpha < I$ such that $(A)_\alpha$ is irreducible. Note that this is the right generalization of the notion introduced by Cashwell and Everett.

Lemma. *Every irreducible of F_I is finitely irreducible.*
Proof. Let $A \neq \mathbf{0}$ that is not a unit. Let us suppose that $(A)_\alpha$ has a factorization $(A)_\alpha = S_\alpha T_\alpha$ for all $I > \alpha \geq L(A) = L$ such that none of S_α and T_α is a unit. Our goal is to construct a factorization $A = ST$ such that none of S and T is a unit.
We say that S_β dominates S_α ($\alpha < \beta$), if $(S_\beta)_\alpha = S_\alpha$. Generally, a divisor of $(A)_\alpha$ is not dominated by $(A)_\beta$, but sometimes it can happen. Indeed, if $L(A) \leq \alpha < \beta < I$, every divisor of $(A)_\beta$ dominates at least one divisor of $(A)_\alpha$, namely, its restriction.
We construct an unbounded chain S^*_α ($L(A) \leq \alpha < I$), that is, $S^*_\alpha = (S^*_\beta)_\alpha$ for all $L(A) \leq \alpha < \beta < I$. The corresponding elements $T^*_\alpha = (A)_\alpha / S^*_\alpha$ form also a chain: $T^*_\alpha = (T^*_\beta)_\alpha$ for all $L(A) \leq \alpha < \beta < I$, because

$$S^*_\alpha T^*_\alpha = (S^*_\beta T^*_\beta)_\alpha = S^*_\alpha (T^*_\beta)_\alpha$$

and F_α has no zero divisor.
Define the following partially ordered set that represents domination. On every $L(A) \leq \alpha < I$ level, consider the divisors of $(A)_\alpha$ (only 1 from each associate class). Every level is finite, since unique factorization holds in every F_α for all $L(A) \leq \alpha < I$. Furthermore, let $S_\alpha < S_\beta$, if $\alpha < \beta$ and $S_\alpha = (S_\beta)_\alpha$. This way, we obtain a *set-theoretic tree* $\mathcal{T}$, that is, $\{T \mid T < S\}$ is a well-ordered set for each element S of the partially ordered set. Let us denote by L_α the number of elements on the α-level.
Our aim is to construct an *unbounded branch*, that is, a well-ordered set that has no upper bound. We claim that such an unbounded branch exists.
If I is countably infinite, then Kőnig's Infinity Lemma shows that unbounded branch exists. If $\operatorname{cof}(I) = \omega$, then we consider an unbounded subset of I of ordinal ω. In this subset, Kőnig's Lemma provides an unbounded branch, which can be extended into $\mathcal{T}$. (Note that in a well-odering X, there exist some $Y \subseteq X$ such that Y is unbounded in X and Y is of ordinal $\operatorname{cof}(X)$; $\operatorname{cof}(X)$ is the minimal ordinal with this property.)

Let us suppose that $\operatorname{cof}(I) > \omega$. Remind the Bernstein-Hausdorff-Tarski Theorem:
Let κ be an ordinal and cardinal, as well. Then the cardinal of $\operatorname{cof}(\kappa)$ is the least cardinal λ, for which there exist subsets $C_\alpha \subset \kappa$ ($\alpha < \lambda$), $|C_\alpha| < \kappa$ such that $\kappa = \cup_{\alpha<\lambda} C_\alpha$.

This theorem provides that if $\cup_{n=1}^{\infty} B_n = I$ is a countable union, then at least one of the sets B_n is of cardinal I, implying also that such a B_n is unbounded in I. Let $B_n = \{\alpha \mid L(A) \leq \alpha < I : L_\alpha = n\}$. Because of the mentioned theorem, there exist some n such that B_n is unbounded in I. We show that there exist some unbounded branch in this B_n by mathematical induction on n.
If $n = 1$, then the statement is trivial.
Let us suppose that the statement holds for n, we prove that it holds for $n + 1$. Let us consider a certain level of B_{n+1} and erase that element along with its branch, whose branch is the shortest (in the case of ambiguity, we only erase one arbitrary branch). In case it cannot be done, i.e. there is no such a shortest branch, then all branches are unbounded, so we are done. Otherwise, after the end of shortest branch, there exist $n+1$ branch again, so we can repeat the erasing operation. Execute this along the whole tree. If we erase unboundedly many times, we are ready by induction. If we do not erase unboundedly many times, there are $n+1$ unbounded branches from a certain point on. $\square$

Let us suppose that there are irreducible power series A, B, C, D such that $AB = CD$ and $A \nsim C$, $A \nsim D$. Since for all $\alpha < I$ $(A)_\alpha(B)_\alpha = (C)_\alpha(D)_\alpha$ and unique factorization holds in F_α, we can suppose that $(A)_\alpha \sim (C)_\alpha$ for unboundedly many α ($(A)_\alpha, (B)_\alpha, (C)_\alpha, (D)_\alpha$ are all irreducibles from a certain point on). Hence $(A)_\alpha = U_\alpha(C)_\alpha$ holds with the suitable units U_α. Since $(C)_\alpha$ form a chain, so do the elements U_α. Their limit U is unit in F_I. Hence $A \sim C$ and this is a contradiction. $\square$

References

[1] E. D. Cashwell, C. J. Everett: *The Ring of Number-Theoretic Functions*, Pacific J. Math. **9** (1959), 975-985.

[2] W. Rückert: *Zum Eliminationsproblem der Potenzreihenideale*, Math. Ann. **107** (1933), 259-281.

[3] Szőke R.: *Többváltozós komplex függvénytan*, egyetemi jegyzet, ELTE, Budapest (2003), 16-20.

[4] D. Deckard, L. K. Durst: *Unique Factorization in Power Series Rings and Semigroups*, Pacific J. Math. (2) **16** (1966), 239-244.

[5] E. D. Cashwell, C. J. Everett: *Formal Power Series*, Pacific J. Math. **13** (1963), 45-64.

[6] W. Krull: *Beiträge zur Arithmetik kommutativer Integritätsbereiche, III. zum Dimensionsbegriff der Idealtheorie*, Math Zeit. **42** (1937) 745-766.