A Combinatorial Construction used in Number Theory

Wim Ruitenburg

These are notes useful for our Number Theory class.

1 Power Series as an Example

We precede the intended topic by first making a comparison. Recall that we can compute with power series

$$f = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots = \sum_{n\geq 0} a_nX^n$$

over the real numbers in the expected way. We add or subtract power series coefficient by coefficient. So

$$\begin{aligned}&(a_0 + a_1X + a_2X^2 + \ldots) + (b_0 + b_1X + b_2X^2 + \ldots) =\\&= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \ldots =\\&= \textstyle\sum_{n\geq 0}(a_n + b_n)X^n,\end{aligned}$$

and

$$\begin{aligned}&-(a_0 + a_1X + a_2X^2 + \ldots) =\\&= (-a_0) + (-a_1)X + (-a_2)X^2 + \ldots =\\&= \textstyle\sum_{n\geq 0}(-a_n)X^n.\end{aligned}$$

We multiply power series by the usual 'convolution' product

$$\begin{aligned}&(a_0 + a_1X + a_2X^2 + \ldots)(b_0 + b_1X + b_2X^2 + \ldots) =\\&= (a_0b_0) + (a_1b_0 + a_0b_1)X + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + \ldots =\\&= \textstyle\sum_{n\geq 0}(\sum_{j+k=n} a_jb_k)X^n.\end{aligned}$$

We can also divide, finding the (multiplicative) inverse of a power series. Recall that the inverse of a number a is that number b for which both $ab = 1$ and $ba = 1$. We often write a^{-1} for this unique b. Recall that for real numbers $\mathbb{R}$ all nonzero numbers have a (multiplicative) inverse. For example, 0.5 is the inverse of 2, and therefore also written as $0.5 = 1/2$ or as $0.5 = \frac{1}{2}$ or as $0.5 = 2^{-1}$. However, the number 0 has no such inverse. Among power series over $\mathbb{R}$ we find that many have multiplicative inverses, though not all. For example, $1 - X$ is invertible with inverse $\sum_{n\geq 0} X^n$, since

$$(1 - X)(1 + X + X^2 + X^3 + \ldots) = 1,$$

while X has no inverse. In fact, more generally, a power series $a_0+a_1X+a_2X^2+a_3X^3+\ldots$ is invertible exactly when a_0 is invertible (try to prove this!). Thus $(1 - X)^{-1}$ exists, while X^{-1} does not exist, among the power series.

There is no relevant information lost when we write power series as infinite sequences of numbers, like

$$\begin{aligned}&f = (a_0, a_1, a_2, a_3, \ldots) = (a_n)_{n\geq 0} \quad \text{and}\\&g = (b_0, b_1, b_2, b_3, \ldots) = (b_n)_{n\geq 0}.\end{aligned}$$

So

$$\begin{aligned}&f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) = (a_n + b_n)_{n\geq 0} \quad \text{and}\\&fg = (a_0b_0, a_1b_0 + a_0b_1, a_2b_0 + a_1b_1 + a_0b_2, \ldots = (\textstyle\sum_{j+k=n} a_jb_k)_{n\geq 0}.\end{aligned}$$

We have all these familiar nice[1] properties like $(fg)h = f(gh)$ and $f(g+h) = fg + fh$. For those who remember 'Foundations of Mathematics', f and g are in essence functions from $\mathbb{Z}^{\geq 0}$ to $\mathbb{R}$ or, in other words, elements of $\mathbb{R}^{(\mathbb{Z}^{\geq 0})}$. Sum and product are also defined by

$$(f+g)(n) = f(n) + g(n) \text{ for all } n \geq 0, \quad \text{and}$$
$$(fg)(n) = \textstyle\sum_{j+k=n} f(j)g(k) \text{ for all } n \geq 0.$$

We also talk about f and g as sequence f or sequence g. In such cases we usually write

$$(f+g)_n = f_n + g_n \text{ for all } n \geq 0, \quad \text{and}$$
$$(fg)_n = \textstyle\sum_{j+k=n} f_j g_k \text{ for all } n \geq 0.$$

2 The Dirichlet Product

Given the *example* of power series in Section 1, we now consider a different but similar such nice structure. Let us consider functions from $\mathbb{N} = \mathbb{Z}^{>0}$ to $\mathbb{R}$ or, in other words, elements of $\mathbb{R}^{\mathbb{N}}$. Its elements are written as

$$s = (s_1, s_2, s_3, s_4, \ldots) = (s_n)_{n>0} \quad \text{or}$$
$$t = (t_1, t_2, t_3, t_4, \ldots) = (t_n)_{n>0}.$$

Note that we do not have an s_0 or a t_0. We define addition and subtraction as we did before in the power series case. So for example

$$s + t = (s_1 + t_1, s_2 + t_2, s_3 + t_3, \ldots) = (s_n + t_n)_{n>0}.$$

We define a *new* product, called Dirichlet product or Dirichlet convolution, by

$$s * t = (\textstyle\sum_{de=n} s_d t_e)_{n>0},$$

also written

$$s * t = (\sum_{d|n} s_d t_{\frac{n}{d}})_{n>0}.$$

This product has nice properties like

$$s * t = t * s,$$
$$s * (t + u) = s * t + s * u, \quad \text{and}$$
$$s * (t * u) = (s * t) * u.$$

For this last equation, observe that both sides are equal to

$$s * (t * u) = (\textstyle\sum_{def=n} s_d t_e u_f)_{n>0}.$$

Consider the following sequences

$$O = (0, 0, 0, 0, 0, \ldots),$$
$$I = (1, 0, 0, 0, 0, \ldots), \quad \text{and}$$
$$E = (1, 1, 1, 1, 1, \ldots).$$

We easily verify that for all s we have

$$s * O = O,$$
$$s * I = s, \quad \text{and}$$
$$s * E = (\textstyle\sum_{de=n} s_d)_{n>0} = (\sum_{d|n} s_d)_{n>0}.$$

[1] Commutative ring properties and more, from abstract algebra.

So O plays a role like the zero number 0 among $\mathbb{R}$ or $\mathbb{Z}$, and I plays a role like the unity number 1 among $\mathbb{R}$ or $\mathbb{Z}$. Multiplication by E is of special interest in number theory.

When does a sequence s have a multiplicative inverse, that is, have an element $x = (x_1, x_2, x_3, x_4, \ldots)$ such that $s * x = I$? Such x may be called $x = s^{-1}$. Given s, to compute x we have to find values $x_1, x_2, x_3, \ldots$ satisfying the system of equations

$$
\begin{aligned}
&s_1 x_1 = 1,\\
&s_2 x_1 + s_1 x_2 = 0,\\
&s_3 x_1 + s_1 x_3 = 0,\\
&s_4 x_1 + s_2 x_2 + s_1 x_4 = 0,\\
&s_5 x_1 + s_1 x_5 = 0,\\
&s_6 x_1 + s_3 x_2 + s_2 x_3 + s_1 x_6 = 0,\\
&\ldots,\\
&\textstyle\sum_{de=n} s_d x_e = 0,\\
&\ldots.
\end{aligned}
$$

So x_1 exists exactly when s_1 is invertible. Observe that if $x_1, x_2, \ldots, x_{n-1}$ can be found for some $n > 1$ (so s_1 is invertible), then x_n can also be computed by moving all but the last term to the right of the equation, and divide by s_1. Thus sequence s is invertible exactly when its term s_1 is invertible.