7. Formal Power Series.

In Sections 4 through 6 we have been manipulating infinite power series in one or more indeterminates without concerning ourselves that such manipulations are justified. So far we have not run into any problems, but perhaps that was just a matter of good luck. In this section we will see which algebraic manipulations are valid for formal power series (and more generally for formal Laurent series), as well as seeing some manipulations which are invalid. Special attention should be paid to the concept of convergence of a sequence of formal power series. Many students consistently confuse this with the concept of convergence of a sequence of real numbers (familiar from calculus), but the two concepts are in fact quite different.

First we recall some basic concepts and terminology of abstract algebra. (These are covered in MATH 135, but some review is warranted.) A *ring* is a set R which has two special elements, a *zero* $0 \in R$ and a *one* $1 \in R$, and is equipped with two binary operations, *multiplication* $\cdot : R \times R \to R$ and *addition* $+ : R \times R \to R$. A long list of axioms completes the definition, but suffice it here to say that the axioms state that the usual rules of integer arithmetic hold for $(R; \cdot, +; 0, 1)$ with one exception. In general, the multiplication in a ring is not required to be commutative: that is, the rule $ab = ba$ for all $a, b \in R$ is **not** in general required. When multiplication in R **is** commutative we say that R is a *commutative ring*. (The ring of 2–by–2 matrices with real entries is an example of a ring that is not commutative.) Some noncommutative rings are in fact useful in combinatorial enumeration, but all of the rings of importance in these notes are commutative.

The point of the previous paragraph is that when we say "R is a commutative ring" we mean that the familiar rules of arithmetic continue to hold for R.

Let $(R; \cdot, +; 0, 1)$ be a commutative ring. An element $a \in R$ is a *zero–divisor* if $a \neq 0$ and there is an element $b \in R$ with $b \neq 0$ such that $ab = 0$. For example, in the ring $\mathbb{Z}_{15}$ of integers modulo 15, we have $[3][5] = [15] = [0]$, so that $[3]$ and $[5]$ are zero–divisors in $\mathbb{Z}_{15}$. If R has no zero–divisors then R is called an *integral domain*. An element $a \in R$ is *invertible* if there is an element $b \in R$ such that $ab = 1$. Such an element is unique if it exists, for if $ac = 1$ as well, then

$$b = b1 = b(ac) = (ba)c = (ab)c = 1c = c.$$

Here we have used several of the axioms, including associativity and commutativity of multiplication. If $a \in R$ is invertible, then the unique element $b \in R$ such that $ab = 1$ is denoted by a^{-1}, and is called the *multiplicative inverse* of a. Notice that

$(a^{-1})^{-1} = a$. Finally, a commutative ring R is called a *field* if every $a \in R$ with $a \neq 0$ is invertible.

Proposition 7.1. *Let R be a commutative ring. If R is a field then R is an integral domain.*

Proof. Arguing for a contradiction, suppose not – thus, assume that R is a field but that $a \in R$ is a zero–divisor. Then $a \neq 0$ so that a^{-1} exists, and there is a $0 \neq b \in R$ such that $ab = 0$. Now we calculate that

$$b = b1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} = 0a^{-1} = 0,$$

which is the desired contradiction. □

There are several ways to construct a new ring starting from a ring which is already known. We will just give the four constructions which are useful for our purposes, and only for commutative rings. So, for the next little while, let R be a commutative ring.

Definition 7.2 (The Polynomial Ring)**.** The *ring of polynomials in x with coefficients in R* is denoted by $R[x]$, and is defined as follows. Here x is an *indeterminate*, meaning a symbol which is not in the set R, and is not a solution of any algebraic equation with coefficients in R. The elements of $R[x]$ are expressions of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

for some $n \in \mathbb{N}$, in which $a_i \in R$ for all $0 \leq i \leq n$. Addition and multiplication are defined as you would expect, using the definitions of addition and multiplication in R for the coefficients, the distributive and associative laws, and the exponent rule for x – that is, $x^i \cdot x^j = x^{i+j}$. Since R is commutative, $R[x]$ is also commutative, but $R[x]$ is never a field. The invertible elements of $R[x]$ are just the constant polynomials a_0 with a_0 invertible in R. In particular, $x \in R[x]$ is not invertible. If R is an integral domain then so is $R[x]$ (this is Exercise 7.2(a)).

Definition 7.3 (The Ring of Rational Functions)**.** The *ring of rational functions in x with coefficients in R* is denoted by $R(x)$, and is defined as follows. There is some subtlety if R contains zero–divisors, so we will only consider the case in which R is an integral domain. The elements of $R(x)$ are of the form $f(x)/g(x)$ with $f(x), g(x) \in R[x]$ and $g(x) \neq 0$. Addition and multiplication are bootstrapped up from $R[x]$ by using the familiar means of manipulating fractions, and $R(x)$ is commutative because R is. Every nonzero element $f(x)/g(x)$ has a multiplicative inverse $g(x)/f(x)$, so that $R(x)$ is a field. In the expression $f(x)/g(x)$ we may take $g(x) = 1$, which shows that $R[x]$ is a subset of $R(x)$. The algebraic operations of these two rings agree on this subset $R[x]$, as is easily verified.

Definition 7.4 (The Ring of Formal Power Series)**.** The *ring of formal power series in x with coefficients in R* is denoted by $R[[x]]$, and is defined as follows. The elements of $R[[x]]$ are infinite expressions of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

in which $a_n \in R$ for all $n \in \mathbb{N}$. Addition and multiplication are defined just as for the ring of polynomials $R[x]$, and $R[[x]]$ is commutative because R is. It is clear that $R[x]$ is a subset of $R[[x]]$, and that the algebraic operations of these two rings agree on this subset. The ring $R[[x]]$ is not a field because, for example, x is not invertible in $R[[x]]$. However, as the following proposition shows, there are quite a few invertible elements in $R[[x]]$.

Proposition 7.5. *Let R be a commutative ring, and let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ be a formal power series in $R[[x]]$. Then $f(x)$ is invertible in $R[[x]]$ if and only if a_0 is invertible in R.*

Proof. We need to determine whether or not there exists a formal power series $g(x) = \sum_{j=0}^{\infty} b_j x^j$ in $R[[x]]$ such that $f(x)g(x) = 1$. Expanding the product, we have

$$\begin{aligned} f(x)g(x) &= \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) \\ &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_i b_j x^{i+j} = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k. \end{aligned}$$

Comparing the coefficient of x^k on both sides of $f(x)g(x) = 1$, we see that $g(x)$ satisfies the equation if and only if $a_0 b_0 = 1$ and $\sum_{i=0}^{k} a_i b_{k-i} = 0$ for all $k \geq 1$. If a_0 is not invertible in R then the equation $a_0 b_0 = 1$ can not be solved for b_0, so that $g(x)$ does not exist and $f(x)$ is not invertible in $R[[x]]$. If a_0 is invertible in R then $b_0 := a_0^{-1}$ exists. Each of the remaining equations (for $k \geq 1$) can be rewritten as $a_0 b_k = -\sum_{i=1}^{k} a_i b_{k-i}$, or, upon multiplying by b_0,

$$b_k = -b_0 \sum_{i=1}^{k} a_i b_{k-i}.$$

These equations can be solved by induction on $k \geq 1$, yielding a solution for $g(x)$ which gives the multiplicative inverse of $f(x)$. Therefore, $f(x)$ is invertible in $R[[x]]$. □

Definition 7.6 (The Ring of Formal Laurent Series)**.** The *ring of formal Laurent series in x with coefficients in R* is denoted by $R((x))$, and is defined as follows. The elements of $R((x))$ are infinite expressions of the form

$$f(x) = a_r x^r + a_{r+1} x^{r+1} + a_{r+2} x^{r+2} + \cdots$$

in which $r \in \mathbb{Z}$ and $a_n \in R$ for all $n \geq r$. That is, a formal Laurent series is a generalization of a formal power series in which finitely many negative exponents are permitted. Addition and multiplication are defined just as for the ring $R[[x]]$ of formal power series, and $R((x))$ is commutative because R is. (I encourage you to check that when multiplying two formal Laurent series the coefficients of the product really are polynomial functions of the coefficients of the factors, and hence are in the ring R. This ensures that the multiplication in $R((x))$ is well–defined.) Note that the ring $R[[x]]$ is a subset of the ring $R((x))$, and that the algebraic operations of these rings agree on the subset $R[[x]]$. If $f(x) \in R((x))$ and $f(x) \neq 0$, then there is a smallest integer n such that $[x^n]f(x) \neq 0$; this is called the *index of* $f(x)$ and is denoted by $I(f)$. By convention, the index of 0 is $I(0) := +\infty$. Concerning the existence of multiplicative inverses in $R((x))$, we have the following proposition.

Proposition 7.7. *Let R be a commutative ring. If R is a field then $R((x))$ is a field.*

Proof. Consider a nonzero $f(x) = \sum_{n=I(f)}^{\infty} a_n x^n$ in $R((x))$. Then $a_{I(f)} \neq 0$ so that it is invertible in R, since R is a field. We may write $f(x) = x^{I(f)} g(x)$ with $g(x) = \sum_{n=0}^{\infty} a_{n+I(f)} x^n$, so that $g(x)$ is a formal power series in $R[[x]]$. The coefficient of x^0 in $g(x)$ is $a_{I(f)}$ and, by Proposition 7.5, it follows that $g(x)$ is invertible in $R[[x]]$, and hence in $R((x))$. Let $h(x) := x^{-I(f)} g^{-1}(x)$. Then

$$f(x)h(x) = x^{I(f)} g(x) x^{-I(f)} g^{-1}(x) = 1,$$

so that $h(x) = f^{-1}(x)$ and $f(x)$ is invertible in $R((x))$. Therefore, $R((x))$ is a field. □

The inclusions $R[x] \subset R[[x]] \subset R((x))$ and $R[x] \subset R(x)$ have been remarked upon already. In fact, if R is a field then $R(x) \subset R((x))$ as well. Also, the rings $R[[x]]$ and $R(x)$ have a nontrivial intersection, but neither one contains the other. Since we have no pressing need for these facts we will not pause to prove them, but instead relegate them to Exercise 7.2.

The constructions above may be combined and iterated, since the commutative ring R was quite general. For example, $R[x, y, z]$ denotes the ring of polynomials in three indeterminates x, y, and z. Similarly, $R[y][[x]]$ denotes the ring of formal power series in the indeterminate x with coefficients which are polynomials in the indeterminate y.

Example 7.8 (The Binomial Series)**.** In the polynomial ring $\mathbb{Q}[y]$, we define the polynomials $\binom{y}{n}$ for every $n \in \mathbb{N}$ by

$$\binom{y}{n} := \frac{y(y-1)\cdots(y-n+1)}{n!}.$$

The *binomial series* is then defined in $\mathbb{Q}[y][[x]]$ to be

$$(1+x)^y := \sum_{n=0}^{\infty} \binom{y}{n} x^n.$$

Notice that in the ring $\mathbb{Q}[y,z][[x]]$ we have the following identity:

$$\begin{aligned}
(1+x)^{y+z} &= \sum_{n=0}^{\infty} \binom{y+z}{n} x^n \\
&= \sum_{n=0}^{\infty} \sum_{j=0}^{n} \binom{y}{j} \binom{z}{n-j} x^n \\
&= \left(\sum_{j=0}^{\infty} \binom{y}{j} x^j \right) \left(\sum_{k=0}^{\infty} \binom{z}{k} x^k \right) \\
&= (1+x)^y \cdot (1+x)^z.
\end{aligned}$$

In this calculation we have used the Vandermonde Convolution Formula (Exercise 3.5). Notice that y and z, as well as x, are also indeterminates. Any complex number $\alpha \in \mathbb{C}$ may be substituted for y in $(1+x)^y$, and the resulting $(1+x)^\alpha$ is a formal power series in $\mathbb{C}[[x]]$.

The usual rules of arithmetic hold for all of the rings constructed above, but there are other operations on these rings that have no analogues in $\mathbb{Z}$. Care must be taken with these operations to ensure that they produce well–defined power series. In other words, these operations are not universally defined.

The first of the new operations are *formal differentiation* and *formal integration*. Since $R((x))$ contains all the other rings above (if R is a field) we will just define these operations on a typical formal Laurent series $f(x) = \sum_{n=I(f)}^{\infty} a_n x^n$. The formal derivative is always defined as

$$f'(x) := \frac{d}{dx} f(x) := \sum_{n=I(f)}^{\infty} n a_n x^{n-1}.$$

The formal integral is defined only if $\mathbb{Q} \subseteq R$ and $a_{-1} = 0$, in which case

$$\int f(x) dx := \sum_{n \geq I(f),\ n \neq -1} a_n \frac{x^{n+1}}{n+1}.$$

In particular, the formal integral is defined on all of $R[[x]]$ when $\mathbb{Q} \subseteq R$. One can show algebraically from the definitions that the familiar rules of calculus (the Product Rule, Quotient Rule, Chain Rule, Integration by Parts, and so on) continue to hold when all the integrals involved are defined.

Example 7.9 (The Logarithmic and Exponential Series). (a) From calculus, we know that as functions of a real variable t,

$$\frac{d}{dt}\log(t) = \frac{1}{t}.$$

Now let $x := 1 - t$, so that $dx = -dt$. Then

$$\frac{d}{dx}\log\left(\frac{1}{1-x}\right) = \frac{d}{dt}\log(t) = \frac{1}{t} = \frac{1}{1-x}.$$

Assuming that $\log(1-x)^{-1} = \sum_{n=I}^{\infty} c_n x^n$ has a Laurent series expansion, we obtain the equation

$$\sum_{n=I}^{\infty} n c_n x^{n-1} = \sum_{k=0}^{\infty} x^k.$$

This implies that $c_n = 1/n$ for all $n \geq 1$, and that $c_n = 0$ for all $n \leq -1$, but gives no information about c_0. However, substituting $x = 0$ we see that $c_0 = \log(1) = 0$. In summary, we have the expansion

$$\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

(b) As another example, the defining properties of the exponential function $\exp(x)$ are that $\exp(0) = 1$ and $\exp'(x) = \exp(x)$. Expanding this as a formal Laurent series $\exp(x) = \sum_{n=I}^{\infty} a_n x^n$ we get the equation

$$\frac{d}{dx}\exp(x) = \sum_{n=I}^{\infty} n a_n x^{n-1} = \sum_{m=I}^{\infty} a_m x^m = \exp(x).$$

Comparing the coefficients of x^{n-1} we see that $n a_n = a_{n-1}$ for all $n \geq I$. By induction, this implies that $a_n = 0$ for all $I \leq n < 0$, so that in fact $I \geq 0$. From $\exp(0) = 1$ we see that $a_0 = 1$, and it then follows that $a_n = 1/n!$ for all $n \in \mathbb{N}$, so that

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

The Chain Rule for differentiation involves "composition" of formal Laurent series, which has not yet been defined (and is not universally defined). In order to discuss the operation of composition we must introduce the concept of convergence of a sequence of formal Laurent series. This must not be confused with the concept of convergence of the single series $f(x) \in \mathbb{R}((x))$ if x is assigned a particular real value! In our applications the case of formal power series is most important, and we will restrict attention to this case for some points.

Definition 7.10 (Convergence of a Sequence of Formal Laurent Series)**.** Let $f_1(x)$, $f_2(x)$, $f_3(x)$,... be a sequence of formal Laurent series in $R((x))$. This sequence is *convergent* in $R((x))$ provided that the following two conditions hold:
• there is an integer J such that $J \leq I(f_k)$ for all $k \in \mathbb{N}$, and
• for every $n \in \mathbb{N}$ there exists a $K_n \in \mathbb{N}$ and $A_n \in R$ such that if $k \geq K_n$ then $[x^n]f_k(x) = A_n$.

The first condition says that there is a uniform lower bound for the indices of all of the entries $f_k(x)$ of the sequence. The second condition says that if we focus attention on only the n–th power of x, and consider the sequence $[x^n]f_k(x)$ of coefficients of x^n in $f_k(x)$ as $k \to \infty$, then this sequence (of elements of R) is *eventally constant*, with the ultimate value A_n.

If $(f_1(x), f_2(x), f_3(x), \ldots)$ is a convergent sequence of formal Laurent series then, with the above notations,

$$f(x) := \sum_{n=J}^{\infty} A_n x^n$$

is a well–defined formal Laurent series, called the *limit* of the convergent sequence. We use the notation

$$\lim_{k\to\infty} f_k(x) = f(x)$$

to denote this relationship.

Example 7.11. Here are a few simple examples for which you can check the definition easily.

(a) $\lim_{k\to\infty} x^k = 0.$

(b) $\lim_{k\to\infty} x^{-k}$ does not exist.

(c) $\lim_{k\to\infty} (1 + x + \cdots + x^k) = \dfrac{1}{1-x}.$

(d) $\lim_{k\to\infty} \dfrac{1}{1-x/k}$ does not exist.

This last example is particularly instructive. You might think that the limit should exist and equal 1. However, the coefficient of x^1 in $(1 - x/k)^{-1}$ is $1/k$, and we see that the sequence $(1/k : k \geq 1)$ is not eventually constant. Therefore, this sequence of formal power series does not converge according to Definition 7.10.

Two important special cases of this concept of limits are the interpretations of infinite sums and infinite products of formal Laurent series. For an infinite sequence $(f_k(x) : k \in \mathbb{N})$ of formal Laurent series, we define

$$\sum_{k=0}^{\infty} f_k(x) := \lim_{K\to\infty} \sum_{k=0}^{K} f_k(x)$$

and

$$\prod_{k=0}^{\infty} f_k(x) := \lim_{K\to\infty} \prod_{k=0}^{K} f_k(x),$$

provided that these limits exist.

Example 7.12. Consider the infinite summation

$$\sum_{k=1}^{\infty} \frac{x^k}{1-x^k}.$$

Does this converge? To check the definition, for each $K \in \mathbb{N}$ consider the partial sum

$$f_K(x) := \sum_{k=1}^{K} \frac{x^k}{1-x^k} = \sum_{k=1}^{K} \left(x^k + x^{2k} + x^{3k} + \cdots\right).$$

To show that $\lim_{K\to\infty} f_K(x)$ exists, we fix an $n \in \mathbb{N}$ and consider the sequence $[x^n]f_K(x)$ as $K \to \infty$. Is this sequence eventually constant? Yes it is! If $K > n$ then

$$[x^n]f_K(x) = [x^n]\sum_{k=1}^{K} \frac{x^k}{1-x^k} = [x^n]\sum_{k=1}^{n} \frac{x^k}{1-x^k} = [x^n]f_n(x)$$

since the terms with $k > n$ can only contribute to the coefficients of powers of x which are strictly greater than n. Since this number $[x^n]f_n(x)$ depends only on n and not on K, the sequence $[x^n]f_K(x)$ is eventually constant as $K \to \infty$. Therefore, the infinite summation converges. In fact,

$$\sum_{k=1}^{\infty} \frac{x^k}{1-x^k} = \sum_{n=1}^{\infty} d(n)x^n$$

in which $d(n)$ is the number of positive integers that divide n.

Example 7.13. Consider the infinite product

$$\prod_{k=1}^{\infty} \left(1 + \frac{x}{k^2}\right).$$

Does this converge? To check the definition, for each $K \in \mathbb{N}$ consider the partial product

$$f_K(x) := \prod_{k=1}^{K} \left(1 + \frac{x}{k^2}\right).$$

To show that $\lim_{K\to\infty} f_K(x)$ exists, fix an $n \in \mathbb{N}$ and consider the sequence $[x^n]f_K(x)$ as $K \to \infty$. Is this sequence eventually constant? No, not for all $n \in \mathbb{N}$ – in particular not for $n = 1$. To be precise, the sequence

$$[x^1]f_K(x) = \sum_{k=1}^{K} \frac{1}{k^2}$$

is not eventually constant as $K \to \infty$. Therefore, this infinite product is not convergent in the ring of fomal power series $R[[x]]$.

Examples 7.11(d) and 7.13 might seem strange to you, since the sequence of coefficients of x^1 converges *as a sequence of real numbers*, as does every other sequence of coefficients in these examples. That is, you would like to make use of the concept of convergence in the coefficient ring R (in this case, the field of real numbers). A general coefficient ring R has no such "topological" structure, which is why we require that the coefficient sequences be eventually constant. (In Exercise 12.12 we have occasion to discuss and employ a more flexible definition of convergence for a sequence of formal power series over a "normed" ring.)

The proof of the following proposition is left as an important exercise.

Proposition 7.14. *Let $(f_k(x) : k \in \mathbb{N})$ be an infinite sequence of formal power series in $R[[x]]$. Assume that there are only finitely many $k \in \mathbb{N}$ for which $[x^0]f_k(x) = -1$. Then the following conditions are equivalent:*
(a) *The infinite sum $\sum_{k=0}^{\infty} f_k(x)$ converges;*
(b) *For every $J \in \mathbb{N}$, there are only finitely many $k \in \mathbb{N}$ such that $I(f_k) \leq J$;*
(c) *The infinite product $\prod_{k=0}^{\infty}(1 + f_k(x))$ converges.*

At last, we turn to a discussion of the operation of composition of formal Laurent series. We restrict ourselves to the case in which R is a field, so that $R((x))$ is also a field. Given $f(x) = \sum_{n=I(f)}^{\infty} a_n x^n$ and $g(x) = \sum_{j=I(g)}^{\infty} b_j x^j$ in $R((x))$, we will determine the conditions under which $f(g(x))$ is a well–defined Laurent series. Of course, the symbol $f(g(x))$ is to be interpreted as

$$f(g(x)) := \sum_{n=I(f)}^{\infty} a_n g(x)^n := \lim_{K \to \infty} \sum_{n=I(f)}^{K} a_n g(x)^n.$$

There are a few cases. If $g(x) = 0$ then $g(x)^n$ does not exist for any negative integer n. Thus, if $g(x) = 0$ then $f(g(x)) = f(0)$ exists if and only if $I(f) \geq 0$, in which case $f(0) = [x^0]f(x)$. Assume now that $g(x) \neq 0$, so that $g^{-1}(x)$ does exist in the field $R((x))$. If $f(x)$ has only finitely many nonzero coefficients then $f(g(x))$ is a polynomial function of $g(x)$ and $g^{-1}(x)$, and therefore is an element of $R((x))$. Finally, assume that $f(x)$ has infinitely many nonzero coefficients. Therefore, for every $N \in \mathbb{N}$ there is an $n \geq N$ such that $a_n \neq 0$. Notice that (since R is an integral domain) the index of $a_n g(x)^n$ is $nI(g)$, n times the index of $g(x)$. Therefore, if $I(g) \leq 0$ then condition (b) of Proposition 7.14 is violated for the sequence

$(a_n g(x)^n :\ n \geq I(f))$, so that the infinite summation

$$f(g(x)) = \sum_{n=I(f)}^{\infty} a_n g(x)^n$$

is not defined. Conversely, if $I(g) > 0$ then condition (b) of Proposition 7.14 is satisfied, and $f(g(x))$ does exist. In summary, we have proved the following.

Proposition 7.15. *Let $f(x)$ and $g(x)$ be formal Laurent series in $R((x))$, in which R is a field. Then $f(g(x))$ is well–defined if and only if one of the following cases holds:*
(i) *$g(x) = 0$ and $I(f) \geq 0$;*
(ii) *$g(x) \neq 0$ and $f(x)$ has only finitely many nonzero coefficients;*
(iii) *$g(x) \neq 0$ and $I(g) > 0$.*

Under some circumstances, it is useful to think of a formal power series $f(x) \in R[[x]]$ as a "change of variables" by considering $u := f(x)$ as another variable itself. Of course, this u does depend on x, but one can consider the ring $R[[u]]$, which will be a subring of $R[[x]]$. The most interesting case is that in which $R[[u]] = R[[x]]$, which occurs exactly when there is a formal power series $g(u) \in R[[u]]$ such that $x = g(u)$. These two equations $u = f(x)$ and $x = g(u)$ imply that $x = g(f(x))$ and $u = f(g(u))$, which is called an *invertible change of variables.*

Proposition 7.16. *Let R be a field, and let $f(x)$ be a formal power series in $R[[x]]$. There exists $g(u) \in R[[u]]$ such that $x = g(f(x))$ and $u = f(g(u))$ if and only if either $I(f) = 1$, or $f(x) = a_0 + a_1 x$ with both a_0 and a_1 nonzero. If such a $g(u)$ exists then it is unique.*

Proof. Consider a pair of formal power series such that $x = g(f(x))$ and $u = f(g(u))$.

First, if $f(x) = 0$ then there is clearly no $g(u) \in R[[u]]$ such that $u = f(g(u))$, so that this case does not arise.

Second, consider the case in which $f(x) = \sum_{n=0}^{\infty} a_n x^n$ has a nonzero constant term $a_0 \neq 0$. In order for the composition $g(f(x))$ to be well-defined, $g(u) = \sum_{j=0}^{\infty} b_j x^j$ must have only finitely many nonzero coefficients, by Proposition 7.15. Since $f(g(x)) = x$ and $a_0 \neq 0$, it follows that $b_0 \neq 0$ as well (for otherwise, if $b_0 = 0$ then $[x^0]f(g(x)) = a_0 \neq 0$, contradicting $f(g(x)) = x$). Now, since $b_0 \neq 0$, for the composition $f(g(u))$ to be well-defined, $f(x)$ must have only finitely many nonzero coefficients, by Proposition 7.15. That is, $f(x)$ and $g(u)$ are polynomials with nonzero constant terms. Now both $f(g(u))$ and $g(f(x))$ are polynomials of degree $\deg(f) \cdot \deg(g)$, and hence $\deg(f) = \deg(g) = 1$. From $f(x) = a_0 + a_1 x$ and $g(u) = b_0 + b_1 u$ we see that $x = g(f(x)) = b_0 + b_1 a_0 + b_1 a_1 x$, so that $b_0 + b_1 a_0 = 0$ and $b_1 a_1 = 1$. That is, $b_1 = a_1^{-1}$ and $b_0 = -a_0 a_1^{-1}$, so that $g(u)$ is uniquely determined. One easily checks that $f(g(u)) = u$ as well, finishing this case.

Finally, consider a nonzero $f(x) \in R[[x]]$ with index at least one. Let $f(x) = \sum_{n=1}^{\infty} a_n x^n$ be given – we are assuming that $a_0 = 0$. To begin with, we seek a formal power series $g(u) = \sum_{j=0}^{\infty} b_j u^j$ such that $g(f(x)) = x$. Expanding this, we have

$$\begin{aligned} x &= g(f(x)) = \sum_{j=0}^{\infty} b_j f(x)^j = \sum_{j=0}^{\infty} b_j \left(\sum_{n=1}^{\infty} a_n x^n \right)^j \\ &= \sum_{m=0}^{\infty} x^m \sum_{j=0}^{\infty} b_j \sum_{n_1+n_2+\cdots+n_j=m} a_{n_1} a_{n_2} \cdots a_{n_j}. \end{aligned}$$

In the inner summation, since $a_0 = 0$ we need only consider those j–tuples $(n_1, \ldots, n_j)$ such that each $n_i \geq 1$. Comparing coefficients of like powers of x, we see that for x^0 we have

$$0 = b_0,$$

for x^1 we have

$$1 = b_1 a_1,$$

and for x^m with $m \geq 2$ we have

$$0 = \sum_{j=1}^{m} b_j \sum_{n_1+n_2+\cdots+n_j=m} a_{n_1} a_{n_2} \cdots a_{n_j}.$$

(The outer summation may be terminated at $j = m$ because each $n_i \geq 1$ and $n_1 + n_2 + \cdots + n_j = m$, and when $j = 0$ the inner summation is empty.)

Now let's solve these equations for the coefficients b_j of $g(u)$. That $b_0 = 0$ is immediate, and b_1 exists if and only if $a_1 \neq 0$, since R is a field. This shows that if $g(u)$ exists then $I(f) = 1$. Conversely, assume that $I(f) = 1$, so that $a_1 \neq 0$ – then $b_1 := a_1^{-1}$ exists. For all $m \geq 2$ we have

$$b_m = -b_1^m \sum_{j=1}^{m-1} b_j \sum_{n_1+n_2+\cdots+n_j=m} a_{n_1} a_{n_2} \cdots a_{n_j}.$$

The RHS is a polynomial function of $\{a_1, \ldots, a_m, b_1, \ldots, b_{m-1}\}$, so that these equations can be solved uniquely by induction on $m \geq 2$ to determine the coefficients of $g(u)$ in the case $I(f) = 1$. This establishes existence and uniqueness of a power series $g(u)$ such that $g(f(x)) = x$ when $I(f) = 1$.

Now, in the case $I(f) = 1$ the power series $g(u)$ we have constructed also has index one: $I(g) = 1$. We want to show that $f(g(u)) = u$ as well. By the preceeding argument, there is a unique formal power series $h(x)$ such that $h(g(u)) = u$. Let's substitute $u = f(x)$ into this – we obtain $h(g(f(x))) = f(x)$. Since $g(f(x)) = x$ this reduces to $h(x) = f(x)$, so that $f(g(u)) = u$, as desired. This completes the proof. $\square$

The unique formal power series $g(u)$ guaranteed by Proposition 7.16 is referred to as the *compositional inverse* of $f(x)$, and is sometimes denoted by $f^{<-1>}(u)$.

Proposition 7.16 is only part of the truth, as the following example shows.

Example 7.17. Consider the rational function $f(x) = (1+x)/(1-x)$. As a formal power series we have

$$\frac{1+x}{1-x} = 1 + 2x + 2x^2 + 2x^3 + 2x^4 + \cdots$$

Algebraically, we can solve $u = f(x)$ for x as follows: $u(1-x) = 1+x$, so that $u - 1 = x(1+u)$, so that $x = (-1+u)/(1+u)$. Hence, $x = g(u)$, where

$$g(u) = \frac{-1+u}{1+u} = -1 + 2u - 2u^2 + 2u^3 - 2u^4 + \cdots$$

Now, even though $u = f(x)$ and $x = g(u)$, neither of the compositions $f(g(u))$ nor $g(f(x))$ are well–defined, by Proposition 7.15.

The trouble with Example 7.17 is only that the compositions of these formal power series do not converge according to Definition 7.10. To circumvent this problem, we can define composition of rational functions instead.

Definition 7.18. Let $f(x) = p(x)/q(x)$ and $g(u)$ be rational functions. The *composition of $g(u)$ into $f(x)$* is defined to be the rational function

$$f(g(u)) := \frac{p(g(u))}{q(g(u))}.$$

Notice that since $p(x)$ and $q(x)$ are polynomials, the expressions $p(g(u))$ and $q(g(u))$ are well–defined rational functions.

Using this definition, all the operations in Example 7.17 are well-defined, resolving the difficulty.

---

7. Exercises.

---

1. Let R be a commutative ring. For $a \in R$ consider the function $\mu_a : R \to R$ defined by $\mu_a(r) := ar$ for all $r \in R$.

(a) Show that if R is an integral domain and $a \neq 0$, then $\mu_a : R \to R$ is an injection.

(b) Show that if R is a finite integral domain then R is a field. (The ring $\mathbb{Z}$ of integers is an integral domain which is not a field. Thus, finiteness of R is essential for this problem. See Exercise 1.4.)

---

2. Let R be a commutative ring.

(a) Show that if R is an integral domain, then $R[x]$ is an integral domain.

(b) Show that neither of $R[[x]]$ nor $R(x)$ contains the other.

(c) Show that if R is a field then $R(x)$ is a proper subset of $R((x))$.

(d) Find an element of $\mathbb{Z}(x)$ which is not in $\mathbb{Z}((x))$.

(e) Show that $R[[x]][y]$ is a proper subset of $R[y][[x]]$.

---

3. Recall the notation of Example 7.8.

(a) Show that in $R[y][[x]]$, $(1-x)^{-y} = \sum_{n=0}^{\infty} \binom{y+n-1}{n} x^n$.

(b) Show that in $R[y,z][[x]]$,

$$\frac{1}{(1-x)^{y+z}} = \frac{1}{(1-x)^y} \cdot \frac{1}{(1-x)^z}.$$

---

4. Let $f(x)$ and $g(x)$ be in $R((x))$. Show that

$$\frac{d}{dx}\left(f(x)g(x)\right) = f'(x)g(x) + f(x)g'(x).$$

---

5. Prove Proposition 7.14.

---

6. Define a sequence of formal power series in $\mathbb{Z}[[x]]$ by $f_0(x) := 1$, $f_1(x) := 1$, and $f_{k+1}(x) := f_{k-1}(x) + x^k f_k(x)$ for all $k \geq 1$. Prove that the limit $\lim_{k\to\infty} f_k(x)$ exists.

---

7. Define a sequence of formal power series in $\mathbb{Z}[[x]]$ by $g_0(x) := 1$, and $g_{k+1}(x) := (1 - xg_k(x))^{-1}$ for all $k \in \mathbb{N}$.

(a) Prove that the limit $g(x) = \lim_{k\to\infty} g_k(x)$ exists.

(b) Show that $g(x)$ satisfies the equation $g(x) = (1 - xg(x))^{-1}$, and thus is the generating function for SDLPs in Theorem 6.9.

---

8. Consider the Chain Rule: for $f(x)$ and $g(x)$ in $R((x))$ such that $f(g(x))$ is defined,

$$\frac{d}{dx} f(g(x)) = f'(g(x))g'(x).$$

(a) Prove this for $f(x)$ and $g(x)$ in $R[[x]]$.

(b) Prove this for $f(x)$ and $g(x)$ in $R((x))$.

---

9. Does the following limit exist in $R[[x]]$? Explain.

$$\lim_{k\to\infty}\left(1+\frac{x}{k}\right)^k.$$

---

10. Does the following limit exist in $R((x))$? Explain.

$$\lim_{k\to\infty}\frac{x^{-k}}{1-x^k}$$

---

11. Show that, as a sequence of formal power series in $\mathbb{Z}[[q]]$,

$$\lim_{a\to\infty}\begin{bmatrix} a+b \\ b \end{bmatrix}_q = \frac{1}{(1-q)(1-q^2)\cdots(1-q^b)}.$$

12(a) Show that if $f(x)\in R[[x]]$ is such that $[x^0]f(x)=1$, then $\log(f(x))$ converges.

12(b) With $f(x)$ as in part (a), show that

$$\frac{d}{dx}\log(f(x)) = f^{-1}(x)\frac{d}{dx}f(x).$$

12(c) Show that $\log(\exp(x)) = x$.

12(d) Show that

$$\exp\left(\log\left(\frac{1}{1-x}\right)\right) = \frac{1}{1-x}.$$

---

7. Endnotes.

What we have in this section is just a tiny glimpse into the subject of commutative algebra. Most of the motivation for this subject is quite separate from the concerns of enumerative combinatorics – it aims towards algebraic geometry, which describes sets of solutions to a collection of polynomial equations, among other things. If you want to read up on this I recommend the following books, with the caveat that they are really intended for graduate students.

- M.F. Atiyah and I.G. Macdonald, “Introduction to Commutative Algebra,” Addison–Wesley, Reading MA, 1969.

- D. Eisenbud, “Commutative Algebra – with a view toward Algebraic Geometry,” *Graduate Texts in Mathematics,* **150**, Springer–Verlag, New York, 1995.

- J.M. Ruiz, “The Basic Theory of Power Series,” Braunschweig Vieweg, 1993.

The last of these also develops the foundations of geometry for categories other than the algebraic one. It is all very fascinating stuff, but quite complicated, and not really relevant to our present purpose. More down–to–earth expositions of what we need of formal power series are given in Chapter 2 of

- H.S. Wilf, “Generatingfunctionology,” Academic Press, New York, 1994

and in Chapter 3 of

- C.D. Godsil, “Algebraic Combinatorics,” Chapman and Hall, New York, 1993.

8. The Lagrange Implicit Function Theorem.

The topic of this section – the Lagrange Implicit Function Theorem – is **the most widely applicable technique** for the enumeration of recursively defined structures. As we saw in Section 6, recursive structure leads to a functional equation for the relevant generating function. When this equation is quadratic it can be solved by the Quadratic Formula, as in Section 6. In most cases, however, the equation is **not** quadratic and simple high–school tricks do not suffice. Instead, Lagrange's Theorem is perfectly suited to such tasks.

Theorem 8.1 (LIFT)**.** *Let $\mathbb{K}$ be a commutative ring which contains the rational numbers $\mathbb{Q}$. Let $F(u)$ and $G(u)$ be formal power series in $\mathbb{K}[[u]]$ such that $[u^0]G(u)$ is invertible in $\mathbb{K}$.*
(a) *There is a unique (nonzero) formal power series $R(x)$ in $\mathbb{K}[[x]]$ such that*

$$R(x) = x\,G(R(x)).$$

(b) *The constant term of $R(x)$ is 0, and for all $n \geq 1$,*

$$[x^n]F(R(x)) = \frac{1}{n}[u^{n-1}]F'(u)G(u)^n.$$

Before proceeding to the proof, let's apply this theorem to Example 6.15.

Example 8.2. As in Example 6.15, let $\mathcal{W}$ be the set of ternary rooted trees, and let $W(x)$ be the generating function for $\mathcal{W}$ with respect to number of nodes. We have derived the functional equation

$$W = x(1+W)^3$$

for this generating function. This fits perfectly into the hypothesis of LIFT, using $\mathbb{K} = \mathbb{Q}$, $F(u) = u$ and $G(u) = (1+u)^3$. Thus, we calculate that the number of ternary rooted trees with $n \geq 1$ nodes is

$$[x^n]W(x) = \frac{1}{n}[u^{n-1}](1+u)^{3n} = \frac{1}{n}\binom{3n}{n-1}.$$

That's a piece of cake!

In order to prove Lagrange's Theorem we need to develop a few more facts about formal Laurent series. These have to do with the *formal residue operator*, which is merely the operator $[x^{-1}]$ that extracts the coefficient of x^{-1} from a formal Laurent series. (The terminology is by analogy with the case $\mathbb{K} = \mathbb{C}$ of complex numbers and the Cauchy Residue Theorem.) We require three facts about it, and then we can prove LIFT.

Lemma 8.3. *Let $F(x)$ be a formal Laurent series. Then*

$$[x^{-1}]\frac{d}{dx}F(x) = 0.$$

Proof. If $F(x) = \sum_{n=I(F)}^{\infty} a_n x^n$ then

$$[x^{-1}]\frac{d}{dx}F(x) = [x^{-1}]\sum_{n=I(F)}^{\infty} na_n x^{n-1} = 0a_0 = 0.$$

□

Lemma 8.4. *Let $F(x)$ and $G(x)$ be formal Laurent series. Then*

$$[x^{-1}]F'(x)G(x) = -[x^{-1}]F(x)G'(x).$$

Proof. This follows by applying Lemma 8.3 to $F(x)G(x)$, since

$$\frac{d}{dx}(F(x)G(x)) = F'(x)G(x) + F(x)G'(x),$$

by Exercise 7.3. □

Lemma 8.5 (Change of Variables)**.** *Let $F(u)$ and $B(x)$ be formal Laurent series. Assume that $I(B) > 0$, and that $[x^{I(B)}]B(x)$ is invertible in $\mathbb{K}$. Then*

$$[x^{-1}]F(B(x))B'(x) = I(B)[u^{-1}]F(u).$$

Proof. First, we consider the case in which $F(u) = u^k$ for some integer k. If $k \neq -1$ then we may write the LHS of the formula as

$$[x^{-1}]B(x)^k B'(x) = \frac{1}{k+1}[x^{-1}]\frac{d}{dx}B(x)^{k+1} = 0,$$

by Lemma 8.3. Also, if $k \neq -1$ then $[u^{-1}]u^k = 0$ on the RHS, so the formula holds in this case. In the remaining case, $k = -1$, we have $I(B)[u^{-1}]u^{-1} = I(B)$ on the RHS. On the LHS we have $[x^{-1}]B(x)^{-1}B'(x)$. To compute this, write

$$B(x) = cx^{I(B)}H(x),$$

in which $c \in \mathbb{K}$ is invertible and $H(x)$ is a formal power series with $[x^0]H(x) = 1$. By Proposition 7.5, $H(x)^{-1}$ exists and is a formal power series – also

$$B(x)^{-1} = c^{-1}x^{-I(B)}H(x)^{-1}$$

and

$$B'(x) = cx^{I(B)}H'(x) + cI(B)x^{I(B)-1}H(x).$$

Therefore,

$$\begin{aligned}
[x^{-1}]B(x)^{-1}B'(x) &= [x^{-1}](c^{-1}x^{-I(B)}H(x)^{-1})(cx^{I(B)}H'(x) + cI(B)x^{I(B)-1}H(x)) \\
&= [x^{-1}](H(x)^{-1}H'(x) + I(B)x^{-1}) = I(B),
\end{aligned}$$

since $H(x)^{-1}H'(x)$ is a formal power series. This establishes the formula whenever $F(u) = u^k$ for some integer $k \in \mathbb{Z}$.

Now consider any formal Laurent series $F(u) = \sum_{k=I(F)}^{\infty} a_k u^k$. We have

$$F(B(x))B'(x) = \sum_{k=I(F)}^{\infty} a_k B(x)^k B'(x),$$

and so, by using the cases we have already proven, we see that

$$\begin{aligned}
[x^{-1}]F(B(x))B'(x) &= \sum_{k=I(F)}^{\infty} a_k [x^{-1}]B(x)^k B'(x) \\
&= \sum_{k=I(F)}^{\infty} a_k I(B)[u^{-1}]u^k \\
&= I(B)[u^{-1}] \sum_{k=I(F)}^{\infty} a_k u^k = I(B)[u^{-1}]F(u).
\end{aligned}$$

This proves the lemma. □

Now we can prove the Lagrange Implicit Function Theorem. I admit that this argument can be verified line–by–line, but that it does not convey an overall sense of understanding. For that deeper understanding, I present a second – combinatorial – proof of LIFT in Section 13. This second proof is usually postponed until C&O 430/630.

Proof of LIFT. For part (a), let $R(x) = \sum_{n=0}^{\infty} r_n x^n$, and let $G(u) = \sum_{k=0}^{\infty} g_k u^k$ with $g_0 \neq 0$ in $\mathbb{K}$. (We do not need g_0 to be invertible for this part of the proof.) Consider the equation $R(x) = xG(R(x))$. We will show that it has a unique solution $R(x)$ (which is nonzero) by showing that for each $n \in \mathbb{N}$, r_n is determined by the previous coefficients $r_0, r_1, \ldots, r_{n-1}$ and by the coefficients $g_0, g_1, \ldots, g_{n-1}$ of $G(x)$, and that a suitable value for r_n always exists. First of all, notice that

$$r_0 = [x^0]R(x) = [x^0]xG(R(x)) = 0,$$

so we may write $R(x) = \sum_{n=1}^{\infty} r_n x^n$ instead. Next, expand both sides of the equation $R(x) = xG(R(x))$ and equate like powers of x:

$$\begin{aligned}
\sum_{n=1}^{\infty} r_n x^n &= x \sum_{k=0}^{\infty} g_k \left(\sum_{n=1}^{\infty} r_n x^n \right)^k \\
&= \sum_{n=1}^{\infty} x^n \left(\sum_{k=0}^{\infty} g_k \sum_{n_1+n_2+\cdots+n_k=n-1} r_{n_1} r_{n_2} \cdots r_{n_k} \right).
\end{aligned}$$

The inner sum on the RHS is over all ordered k–tuples of positive integers which sum up to $n-1$. For a given value of n, this implies that $k \leq n-1$, and so for every $n \geq 1$,

$$r_n = \sum_{k=0}^{n-1} g_k \sum_{n_1+n_2+\cdots+n_k=n-1} r_{n_1} r_{n_2} \cdots r_{n_k}.$$

Notice that since $r_1 = g_0 \neq 0$, the index of R is $I(R) = 1$. The proof of part (a) is completed by showing that r_n is a polynomial function of $g_0, \ldots, g_{n-1}$. This is accomplished by an easy induction on $n \in \mathbb{N}$, which we leave to the reader.

For this proof of part (b) we require g_0 to be invertible in $\mathbb{K}$, so that $G(u)^{-1}$ exists in $\mathbb{K}[[u]]$. Consider the formal power series $P(u) := uG(u)^{-1}$. Let $R(x)$ be defined as in part (a), and make the change of variables $u := R(x)$. Then, since $R(x) = xG(R(x))$, we get

$$x = R(x)G(R(x))^{-1} = uG(u)^{-1} = P(u),$$

so that $x = P(u)$ is the change of variables inverse to $u = R(x)$. By Proposition 7.16 both of the compositions $x = P(R(x))$ and $u = R(P(u))$ are well–defined.

Now, for $n > 0$ we may calculate, using Lemma 8.4, that

$$\begin{aligned} [x^n]F(R(x)) &= [x^{-1}]x^{-1-n}F(R(x)) = -\frac{1}{n}[x^{-1}]\left(\frac{d}{dx}x^{-n}\right)F(R(x)) \\ &= \frac{1}{n}[x^{-1}]x^{-n}F'(R(x))R'(x) = \frac{1}{n}[x^{-1}]H(R(x))R'(x), \end{aligned}$$

in which we have put $H(u) := P(u)^{-n}F'(u)$, so that $H(R(x)) = x^{-n}F'(R(x))$. Continuing, by Lemma 8.5 we have

$$\begin{aligned} [x^{-1}]H(R(x))R'(x) &= I(R)[u^{-1}]H(u) = [u^{-1}]P(u)^{-n}F'(u) \\ &= [u^{-1}]u^{-n}G(u)^nF'(u) \\ &= [u^{n-1}]F'(u)G(u)^n. \end{aligned}$$

This completes the proof. □

I warned you... it makes sense line–by–line... but where the heck did all that algebra come from?! All I can say is that in Section 13 we find a way to interpret this formula combinatorially and prove it in a conceptual manner (and under slightly weaker hypotheses). In the meantime, here is an illustration of the method in practice.

Example 8.6. What is the expected number of terminals among all ternary rooted trees with n nodes? Let $\tau(T)$ denote the number of terminals of $T \in \mathcal{W}$, and consider the bivariate generating function

$$W(x,y) := \sum_{T \in \mathcal{W}} x^{n(T)} y^{\tau(T)}.$$

Analogously with Question 6.2, the average we seek is A_n/T_n in which

$$T_n = [x^n]W(x,1) = \frac{1}{n}\binom{3n}{n-1}$$

from Example 8.2, and

$$A_n = [x^n]\ \frac{\partial}{\partial y}W(x,y)\bigg|_{y=1}.$$

To compute A_n we begin by deriving a functional equation for $W(x,y)$ from the recursive structure of ternary rooted trees:

$$\begin{array}{rcl}
\mathcal{W} & \rightleftharpoons & \{\odot\} \times (\{\varnothing\} \cup \mathcal{W})^3 \\
T & \leftrightarrow & (\odot, L, M, R) \\
n(T) & = & 1 + n(L) + n(M) + n(R) \\
\tau(T) & = & \begin{cases} 1 & \text{if } L = M = R = \varnothing, \\ \tau(L) + \tau(M) + \tau(R) & \text{otherwise.} \end{cases}
\end{array}$$

This yields the functional equation

$$W = x(y + 3W + 3W^2 + W^3)$$

for the generating function $W(x,y)$. Now LIFT applies with $\mathbb{K} = \mathbb{Q}(y)$, $F(u) = u$, and $G(u) = y + 3u + 3u^2 + u^3$. The following calculation is a bit sneaky, so read carefully and think about why each step is valid.

$$\begin{aligned}
A_n &= [x^n]\ \frac{\partial}{\partial y}W(x,y)\bigg|_{y=1} = \frac{\partial}{\partial y}[x^n]W(x,y)\bigg|_{y=1} \\
&= \frac{\partial}{\partial y}\frac{1}{n}[u^{n-1}](y+3u+3u^2+u^3)^n\bigg|_{y=1} \\
&= \frac{1}{n}[u^{n-1}]\ \frac{\partial}{\partial y}(y+3u+3u^2+u^3)^n\bigg|_{y=1} \\
&= \frac{1}{n}[u^{n-1}]\ n(y+3u+3u^2+u^3)^{n-1}\big|_{y=1} \\
&= [u^{n-1}](1+u)^{3n-3} = \binom{3n-3}{n-1}.
\end{aligned}$$

Therefore, the average number of terminals among all ternary rooted trees with n nodes is

$$\frac{A_n}{T_n} = \frac{\binom{3n-3}{n-1}}{\frac{1}{n}\binom{3n}{n-1}} = \frac{(2n+1)(2n)(2n-1)}{3(3n-1)(3n-2)},$$

after some simplification. As $n \to \infty$ this is asyptotic to $8n/27$, so that in a large random ternary rooted tree one expects about $8/27 = 0.\overline{296}$ of the nodes to be terminals.

8. Exercises.

1. Fix a positive integer c. For each $n \in \mathbb{N}$, determine the number of plane planted trees with n nodes in which the number of children of each node is divisible by c. (I remind you that 0 is divisible by every such c.)

2. For a plane planted tree T, let $h(T)$ denote the number of nodes of T which have an even number of children. For each $n \in \mathbb{N}$, determine the average value of $h(T)$ among all the PPTs with n nodes.

3. Fix an integer $k \geq 2$. A *k–ary rooted tree* T has a root node $\odot$, and each node may have at most one child of each of k "types". (The case $k = 2$ gives BRTs, and the case $k = 3$ gives TRTs.)

(a) Show that the number of k–ary rooted trees with n nodes is $\frac{1}{n}\binom{kn}{n-1}$.

(b) Show that, as $n \to \infty$, the expected number of terminals among all k–ary rooted trees with n nodes is asymptotically $(1 - 1/k)^k n$.

4. For a plane planted tree (PPT) T, let $f(T)$ be the number of nodes of T with at least three children. Show that for $n \geq 4$, the average value of $f(T)$ among all the PPTs with n nodes is $(n^2 - 3n)/(8n - 12)$.

5. If an SDLP P touches the diagonal $x = y$ at points

$$(0, 0) = (k_0, k_0), (k_1, k_1), \ldots, (k_r, k_r) = (n, n),$$

then the sub–path of P between the points (k_{i-1}, k_{i-1}) and (k_i, k_i) is called the i–th *block* of P. Show that the expected number of blocks among all SDLPs to (n, n) is $3n/(n + 2)$.

6. For a plane planted tree (PPT) T, let $d(T)$ be the degree of the root nodes of T. Show that for $n \geq 1$, the average value of $d(T)$ among all the PPTs with n nodes is $(3n - 3)/(n + 1)$.

7. For a plane planted tree T, a *middle child* is a non–root node which is neither the leftmost nor the rightmost child of its parent. Let $p(T)$ denote the number of middle children in T. For each $n \in \mathbb{N}$, determine the average value of $p(T)$ among all the PPTs with n nodes.

8. (a) Let α and x be indeterminates. Find a formal power series $f(y)$ such that $\exp(\alpha x) = f(x\exp(-x))$.
(b) Let β be another indeterminate. Prove that

$$(\alpha+\beta)(n+\alpha+\beta)^{n-1} = \alpha\beta\sum_{k=0}^{n}\binom{n}{k}(k+\alpha)^{k-1}(n-k+\beta)^{n-k-1}.$$

(For $n \geq 1$, the polynomial $z(n+z)^{n-1}$ is known as an *Abel polynomial.*)

8. Endnotes.

Incidentally, Lagrange was not a combinatorialist. In fact, combinatorics as such did not even exist during his lifetime (with the exception of a few things which Euler investigated). Lagrange discovered this theorem in order to solve functional equations which he derived in calculations of the orbital motion of the moon. These calculations were by far the most accurate ever done up to that time, and for many decades thereafter. All without electricity, too, of course!

For some entertaining reading, and somewhat fictionalized biographies of famous mathematicians, I recommend the following dated and sexistly titled classic:

- E.T. Bell, "Men of Mathematics," Simon & Schuster, New York, 1986.

The proof of the Lagrange Implicit Function Theorem presented here is adapted from Goulden and Jackson's monumental book:

- I.P. Goulden and D.M. Jackson, "Combinatorial Enumeration," John Wiley & Sons, New York, 1983.