Transcendentals, The Goldbach Conjecture, and the Twin Prime Conjecture

R.C. Churchill

Prepared for the
Kolchin Seminar on Differential Algebra
Graduate Center, City University of New York
August 2013

Abstract

In these notes we formulate a good deal of elementary calculus in terms of fields of real-valued functions, ultimately define differentiation in a purely algebraic manner, and use this perspective to establish the transcendency of the real-valued logarithm, arctangent, exponential, sine, and cosine functions over the field of rational functions on $\mathbb{R}$. Along the way we connect this approach to elementary calculus with Euclid's proof of the infinitude of primes and two well-known conjectures in number theory. References to far deeper applications of these ideas to number theory are included.

The exposition can serve as an introduction to the subject of "differential algebra," the mathematical discipline which underlies a great deal of computer algebra.

Contents

Standing Notation and Conventions

$\mathbb{N}$ denotes the set $\{0, 1, 2, \dots\}$ of natural numbers
$\mathbb{Z}$ denotes the usual ring of integers
$\mathbb{Z}^+ := \{1, 2, 3, \dots\}$
$\mathbb{Q}$ denotes the field of rational numbers
$\mathbb{R}$ denotes the field of real numbers
$\mathbb{C}$ denotes the field of complex numbers

When $\mathbb{R}$ and $\mathbb{C}$ are regarded as topological spaces the usual topologies are always assumed.

All rings are assumed to admit unities (i.e. multiplicative identities) *and all ring homomorphisms are assumed to preserve these unities. If a ring is denoted R the zero and unity are denoted 0_R and 1_R respectively, or simply 0 and 1 when R is clear from context.*

$R^\times$ denotes the group of units of the ring R.
$\mathrm{Mat}_{m,n}(R)$ denotes the collection of $m \times n$ matrices with entries in the ring R (m and n are, of course, positive integers)
$\mathrm{Mat}_n(R)$ is the ring of $n \times n$ matrices with entries in R (and as a set is identical with $\mathrm{Mat}_{n,n}(R)$)

*Let R be a commutative ring. By an R-*algebra *one means a ring homomorphism $f : R \to S$ into a* (not necessarily commutative) *ring S such that $f(r)s = rf(s)$ for all $r \in R$ and all $s \in S$; f is the* structure mapping *of the algebra, and $f(r)s$ generally written as $r \cdot s$ or as rs. When f is clear from context, e.g. when f is an inclusion mapping, one generally refers to S, rather than to the homomorphism f, as the R-algebra.* Examples: *the ring homomorphism $r \in R \mapsto \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \in \mathrm{Mat}_n(R)$ is an R-algebra, although in this particular example one would tend to refer to $\mathrm{Mat}_n(R)$ as the R-algebra; the polynomial ring $R[x]$ in a single indeterminate is an R-algebra which one would generally refer to as "the polynomial algebra $R[x]$."*

1. Introduction - The Integration of Rational Functions

For purposes of this introduction we define a *rational function* to be a function of the form

$$f : r \mapsto p(r)/q(r) \in \mathbb{R}, \tag{1.1}$$

where $p, q \in \mathbb{R}[x]$ are relatively prime polynomials and the domain of f is understood to be the open subset

$$U_f := \{\, r \in \mathbb{R} \,:\, q(r) \neq 0 \,\} \subset \mathbb{R}. \tag{1.2}$$

By taking $q := 1$ we see that all polynomial functions are rational.

A good deal of time in elementary calculus courses is concerned with methods for integrating these entities. One quickly dispenses with polynomials, and to handle the general case one relies heavily on the existence of "partial fraction decompositions," which guarantee that any rational function can expressed as a polynomial function plus a real linear combination of rational functions of one of two forms:

I. $1/(x-r)^n$, with $r \in \mathbb{R}$ and $0 < n \in \mathbb{Z}$; or

II. $(sx+t)/(x^2+bx+c)^n$, where $s, t, b, c \in \mathbb{R}$, $b^2 - 4c < 0$, and $0 < n \in \mathbb{Z}$.

The problem of integration in the quotient field $\mathbb{R}(x)$ of $\mathbb{R}[x]$ is thereby reduced that of rational functions of these two types.

Case (I): The substitution $u = x - r$ reduces this case to the integration of $\frac{1}{x^n}$. Since $\frac{-1}{(n-1)x^{n-1}}$ is an antiderivative for $n > 1$ only $\frac{1}{x}$ requires further investigation.

Case (II): The substitution $u = \frac{2x+b}{\sqrt{4c-b^2}}$ reduces this case to the integration of rational functions of two forms: (IIa) $2x/(x^2+1)^n$; and (IIb) $1/(x^2+1)^n$, where in both cases $0 < n \in \mathbb{Z}$.

Case (IIa): This reduces to Case (I) by means of the substitution $u = x^2 + 1$.

Case (IIb): If we ignore "constants of integration" the formula

$$\frac{d}{dx}\left\{ \frac{x}{(x^2+1)^{n-1}} + (2n-3)\int_0^x \frac{1}{(t^2+1)^{n-1}}\,dt \right\} = \frac{2(n-1)}{(x^2+1)^n}$$

is easily seen to be equivalent to

$$\int \frac{1}{(x^2+1)^n}\,dx = \frac{x}{2(n-1)(x^2+1)^{n-1}} + \frac{2n-3}{2(n-1)}\int \frac{1}{(x^2+1)^{n-1}}\,dx$$

for all $n > 1$, and by repeated applications[1] of this last identity the integration of $\frac{1}{(x^2+1)^n}$ is reduced to the integration of $\frac{1}{x^2+1}$.

The essence of the problem of integrating arbitrary rational functions is thereby reduced to the search for, or the construction of, antiderivatives of $1/x$ and $1/(x^2+1)$. In elementary calculus these antiderivatives are provided by the logarithm and arctangent functions, which are generally defined in terms of definite integrals and/or inverse functions. Our approach will use formal power series, which in many respects is more complicated, but ultimately has the advantage of bringing fields into the picture, thereby allowing for algebraic formulations, proofs, and generalizations of many familiar results.

The logarithm and arctangent functions are generally referred to as "transcendental functions," but the terminology is rarely defined in a first course, and when one eventually does encounter the definition is it inevitably in terms of fields. Moreover, one is often left with the impression that the "right" definition of a transcendental function must involve fields of complex-valued functions having complex domains.

In these notes we indicate how the definition can be applied to fields of real-valued functions defined on real domains, although defining these fields appropriately does require a smattering of complex-function theory.

The required background in both real and complex analytic function theory is given in Part I. In Part II we begin an algebraic approach to differentiation, and indicate how this uncovers surprising connections between elementary calculus and algebraic number theory. In Part III we give the definition of "transcendental" and use the earlier results to prove that the logarithm and arctangent functions, and a few other old favorites, qualify as transcendental functions.

Our presentation is somewhat tongue-in-cheek. At points we formulate definitions as if they were new to the reader, e.g. derivatives of functions, but then make use of non-trivial consequences, undoubtedly thoroughly familiar, without offering proofs, e.g. the chain-rule. Hopefully enough sketches of proofs and references are given to satisfy curious readers.

[1] One can see from the output of symbolic computation programs that formulas of this nature are behind the programs covering integration.

Part I - Topics from Analysis

In the next four sections we review the definition of an analytic function and general properties thereof. So far as seems reasonable we treat the real and complex cases simultaneously[2]. Since this is regarded as background material, proofs of straightforward results are ignored, proofs of some of the remaining results are only sketched, and several key proofs are omitted completely. Our approach was inspired by that found in [Ca] and in [D, Chapter IX]. In particular, by consulting the second reference readers should be able to fill in any details they feel are missing.

2. Analytic Functions

In this section $\mathbb{K}$ *denotes either the real field* $\mathbb{R}$ *or the complex field* $\mathbb{C}$*. We denote the absolute value*[3] *of an element* $k \in \mathbb{K}$ *by* $|k|$*.*

We need to point out explicitly that we distinguish between polynomials and the associated polynomial functions. The former we simply regard as elements of the $\mathbb{K}$-algebra $\mathbb{K}[x]$, to be manipulated in accordance with defining conditions of an arbitrary $\mathbb{K}$-algebra; the latter as functions from $\mathbb{K}$ into $\mathbb{K}$ defined from the former by "substituting for x." One associates "roots" with polynomials, and "zeros" with the corresponding polynomial functions[4]. When $p \in \mathbb{K}[x]$ the associated polynomial function is denoted $p(x) : k \in \mathbb{K} \mapsto p(k) \in \mathbb{K}$.

Since the collection $\mathbb{K}_F[x]$ of polynomial functions is also a $\mathbb{K}$-algebra, isomorphic to $\mathbb{K}[x]$ by means of the ring homomorphism $p \to p(x)$, one might wonder why we bother making the distinction. The immediate answer is that we always have an eye on generalizations: when $\mathbb{K}$ is replaced by an arbitrary field K the mapping $p \in K[x] \mapsto p(x) \in K_F[x]$ may no longer be an isomorphism, e.g. when $K = \mathbb{Z}/2\mathbb{Z}$ the distinct polynomials $p = x^2 + x + 1$ and $q = 1$ are both mapped to the constant function $k \in \mathbb{Z}/2\mathbb{Z} \mapsto 1 \in \mathbb{Z}/2\mathbb{Z}$.

---

[2]The mathematical results relating to complex analytic functions are so spectacular that real analytic functions seem to have been relegated to a secondary role. One the other hand, in a first course in calculus, which is a basic concern in these notes, one seldom (if ever) deals with complex-valued functions, let alone complex analytic functions.

[3]To discourage helpful analogies the absolute value $|c|$ of a complex number c is often called the *modulus of* c.

[4]A *root* of a polynomial $p \in \mathbb{K}[x]$ is an element $\ell \in \mathbb{K}[x]$ such that $x - \ell$ is a factor of p, i.e. such that $p = (x - \ell) \cdot q$ for some $q \in \mathbb{K}[x]$. A *zero* of a $\mathbb{K}$-valued function f is a point ℓ in the domain of f such that $f(\ell) = 0$. When $f = p(x) : \mathbb{K} \to \mathbb{K}$ is a polynomial function an element $\ell \in \mathbb{K}$ is a root of p if and only if ℓ is a zero of $p(x)$.

Since the symbol $\mathbb{K}$ already appears in the notation $\mathbb{K}[x]$, frequent reference to $\mathbb{K}[x]$ as a "$\mathbb{K}$-algebra" seems rather pedantic, and for this reason we generally refer to $\mathbb{K}[x]$ as a "polynomial algebra." In later sections, wherein $\mathbb{K}$ is replaced by an arbitrary commutative ring R, we will use the same informal terminology when referring to the R-algebra $R[x]$.

Since $\mathbb{K}$ is a field the polynomial algebra $\mathbb{K}[x]$, when considered only as a ring, is also integral domain. Since $\mathbb{K}[x]$ and $\mathbb{K}_F[x]$ are isomorphic, the same holds for $\mathbb{K}_F[x]$.

Formal Power Series

Let $a \in \mathbb{K}$. A sequence of polynomials[5] of the form $\{\sum_{j=0}^{n} k_j(x-a)^j\}_{n=0}^{\infty}$, where $\{k_n\}_{n=0}^{\infty}$ is a sequence in $\mathbb{K}$, is called a *formal power series* (*based*) *at* a, and is abbreviated

$$\sum_{n=0}^{\infty} k_n(x-a)^n. \tag{2.1}$$

By a *formal power series* one means any sequence of this form. When $\mathbb{K}$ requires specification one refers to a *real formal power series* if $\mathbb{K} = \mathbb{R}$, and a *complex formal power series* when $\mathbb{K} = \mathbb{C}$. Of course each real series can also be considered a complex series, and this observation will prove quite useful.

Each polynomial $\sum_{j=0}^{n} k_j(x-a)^j \in \mathbb{K}[x]$ provides an example of a formal power series: in this case the corresponding series in $\mathbb{K}$ is $\{k_0, k_1, k_2, \dots, k_n, 0, 0, 0, \dots\}$ and one would replace (2.1) with $\sum_{j=0}^{n} k_j(x-a)^j$. However, if polynomials were the only examples there would be no reason for the concept: regarding a polynomial as a sequence of polynomials can sometimes be useful, but more often than not can be a distraction. The first significant example of a formal power series, one might say the paradigm, is the *geometric series*

$$\sum_{n=0}^{\infty} x^n\,, \tag{2.2}$$

the corresponding sequence in $\mathbb{K}$ being $\{1, 1, 1, \dots\}$.

When $a, b \in \mathbb{K}$ any formal power series based at a can be converted to a formal power series based at b by expressing $x - a$ as $(x-b) + (b-a)$, expanding each

[5] As opposed to a sequence of polynomial functions. A "formal power series" always refers to a sequence in the polynomial algebra $\mathbb{K}[x]$. In elementary calculus the adjective "formal" is generally dropped, which can leave students, particularly those who would truly like to understand the subject, with a rather uneasy feeling.

power $\big((x-b)+(b-a)\big)^n$ by means of the Binomial Theorem, and manipulating the resulting series (completely ignoring any rigorous justification) as follows:

$$
\left\{
\begin{array}{rcl}
\sum_{n=0}^{\infty} k_n(x-a)^n & = & \sum_{n=0}^{\infty} k_n\big((x-b)+(b-a)\big)^n \\
& = & \sum_{n=0}^{\infty} k_n \left(\sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) (x-b)^j (b-a)^{n-j} \right) \\
& = & \sum_{n=0}^{\infty} k_n \left(\sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) (b-a)^{n-j} (x-b)^j \right) \\
& = & \sum_{n=0}^{\infty} \sum_{j=0}^{n} \left(\left(\begin{array}{c} n \\ j \end{array} \right) k_n (b-a)^{n-j} (x-b)^j \right) \\
& = & \sum_{j=0}^{\infty} \sum_{n=j}^{\infty} \left(\left(\begin{array}{c} n \\ j \end{array} \right) k_n (b-a)^{n-j} \right) (x-b)^j \\
& = & \sum_{j=0}^{\infty} \left(\sum_{n=j}^{\infty} \left(\begin{array}{c} n \\ j \end{array} \right) k_n (b-a)^{n-j} \right) (x-b)^j
\end{array}
\right. \tag{2.3}
$$

Here is a simple polynomial example[6] with $a := -2$ and $b := 5$: Replacing $x+2$ by $(x-5)+(5-(-2)) = (x-5)+7$ in the polynomial $5(x+2)^3-47(x+2)^2+131(x_2)-112$ and manipulating as above results in $5(x-5)^3 + 58(x-5)^2 + 208(x-55) + 217$.

Convergence

A formal power series $\sum_{n=0}^{\infty} k_n(x-a)^n$ is said to *converge* at a point $k \in \mathbb{K}$ if the sequence $\{\sum_{j=0}^{n} k_j(k-a)^j\} \subset \mathbb{K}$ converges in $\mathbb{K}$. If this is the case, and if $\ell \in \mathbb{K}$ is the limit of this sequence, we write

$$\ell = \sum_{n=0}^{\infty} k_n(k-a)^n, \tag{2.4}$$

say that the given formal power series *converges to* ℓ *at* $x = k$ (or simply *at* k), and refer to ℓ as the *sum* of the formal power series at k, or as the *sum of the infinite series* $\sum_{n=0}^{\infty} k_n(k-a)^n$. The formal power series *diverges* at k if it does not converge at k.

Examples 2.5 :

(a) Any formal power series $\sum_{n=0}^{\infty} k_j(x-a)^n$ converges to k_0 at $x = a$ (because the corresponding sequence is $k_0, 0, 0, \dots$).

[6] In which the final result can be achieved by a much easier method.

(b) The formal power series $\sum_{n=0}^{\infty} \frac{1}{n!} x^n$ converges to e^k at each $k \in \mathbb{K}$.

(c) The geometric series $\sum_{n=0}^{\infty} x^n$ converges to $1/(1-k)$ at each $k \in \mathbb{K}$ satisfying $|k| < 1$. The series diverges at all k satisfying $|k| > 1$.

For any point $a \in \mathbb{K}$ and any $0 < r \in \mathbb{R}$ define

$$D_r(a) := \{\, k \in \mathbb{K} \,:\, |k - a| < r \,\}. \tag{2.6}$$

This is the *open disk (in $\mathbb{K}$) of radius r centered at a*, and an *open disk (in $\mathbb{K}$)* refers to any set of this form. The "disk" terminology is somewhat misleading when $\mathbb{K} = \mathbb{R}$, since in that context $D_r(a)$ is not actually a disk (in the usual sense): it is the open interval $(a-r, a+r)$. If $\mathbb{K}$ needs clarification we replace $D_r(a)$ by $D_{\mathbb{K},r}(a)$, with $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. In particular, one has

$$D_{\mathbb{R},r}(a) = D_{\mathbb{C},r}(a) \cap \mathbb{R} \qquad \text{for any} \qquad a \in \mathbb{R} \subset \mathbb{C}. \tag{2.7}$$

It proves convenient to allow $r = \infty$ in (2.6), in which case it is immediate from that definition that

$$D_\infty(a) = \mathbb{K}. \tag{2.8}$$

One says that $D_\infty(a)$ has "infinite radius."

Theorem 2.9 : *For any formal power series $\sum_{n=0}^{\infty} k_n (x-a)^n$ precisely one of the following statements holds:*

(a) *the formal power series converges only at $x = a$;*

(b) *there is a positive real number r such that the formal power series converges at all points of $D_r(a)$ and diverges at all points of the complement of the closure of $D_r(a)$;*

(c) *the formal power series converges at all points of $\mathbb{K}$.*

Moreover, if the given formal power series is real, in which case $a \in \mathbb{R}$, the positive number r appearing in (b) *remains the same when the series is considered complex, and* (2.7) *therefore holds.*

The positive real number r introduced in (b) is called the *radius of convergence* of the formal power series $\sum_{n=0}^{\infty} k_j (x-a)^j$. In fact the "radius of convergence" terminology is used with all three possibilities. To indicate that (a) holds one says

the *the radius of convergence is zero*, to indicate (c) one says that *the radius of convergence is infinity*, and for brevity one writes $r = 0$ and $r = \infty$ to distinguish the respective cases.

In practice radii of convergence can often be computed using the "ratio test" familiar from elementary calculus.

Representation by Power Series

Let $U \subset \mathbb{K}$ be a non-empty open set, let $f : U \to \mathbb{K}$, and let $a \in U$. A function $f : U \to \mathbb{K}$ is[7] *represented by* (or is *representable by*) *a power series at* a if there is an open disk $D_r(a) \subset U$ with radius $r \leq \infty$ and a formal power series $\sum_{n=0}^{\infty} k_j(x-a)^n$ such that

$$f(k) = \sum_{n=0}^{\infty} k_j(k-a)^n \qquad \text{for all} \qquad k \in D_r(a). \tag{2.10}$$

When this is the case and specific reference to $D_r(a)$ is needed we refer to the pair $(\sum_{n=0}^{\infty} k_j(k-a)^n, D_r(a))$ as a power series representation of f at a. The disk $D_r(a)$ appearing in (2.10) is not unique: for any $0 < s < r$ the pair $(\sum_{n=0}^{\infty} k_j(k-a)^n, D_s(a))$ would also be a power series representation of f at a. In particular, r need not be the radius of convergence of the given formal power series. On the other hand, since by (2.10) one has convergence for all k satisfying $|k-a| < r$, this radius r cannot be greater than this radius of convergence.

Theorem 2.11 : *Suppose $U \subset \mathbb{K}$ is a non-empty open set, $a \in U$, and $f : U \to \mathbb{K}$ is represented by a power series at a. Then:*

(a) *the formal power series representing f at a is unique; and*

(b) *there is an open disk in $D \subset U$ centered at a such that f is represented by a power series at every point of D.*

The key to the proof of (b) is calculation (2.3).

Theorem 2.11(a) justifies the following terminology: when (2.10) holds one says that f is represented at a by "the" power series $\sum_{n=0}^{\infty} k_n(x-a)^n$; and one refers to (2.10) as "the" power series expansion of f at a.

[7] Here we are conforming with the usual terminology in calculus: "represented by, or representable by, a formal power series" would be more precise.

Examples 2.12 :

(a) Define $f : \mathbb{R} \to \mathbb{R}$ by

$$r \mapsto \begin{cases} e^{-1/r} & \text{if} \quad r > 0, \\ 0 & \text{if} \quad r \leq 0. \end{cases}$$

Then f is representable by a power series at all points of the domain except 0. (This will be easier to establish after some additional theory has been reviewed: see Example 4.11.)

(b) The function $k \in \mathbb{K} \setminus \{1\} \mapsto 1/(1-k) \in \mathbb{K}$ is represented by the geometric series at $k = 0$, a relationship commonly expressed as

(i) $$\frac{1}{1-k} = 1 + k + k^2 + k^3 + \cdots, \qquad |k| < 1.$$

(c) The function given in Example (b) is also represented by a power series at $k = 5$, i.e.

$$\frac{1}{1-k} = -\tfrac{1}{4} + \tfrac{1}{16} \cdot (x-5) - \tfrac{1}{64} \cdot (x-5)^2 + \tfrac{1}{256} \cdot (x-5)^3 - \cdots, \qquad |k-5| < 1.$$

An *entire function* is a function $f : \mathbb{K} \to \mathbb{K}$ which is represented at some point of $\mathbb{K}$ by a power series with infinite radius of convergence. Polynomial functions are examples. Additional examples will be seen in Examples 2.15.

Theorem 2.13 : *A function $f : \mathbb{K} \to \mathbb{K}$ is entire if and only if it is represented at all points by power series with infinite radii of convergence.*

Functions defined by Formal Power Series

Let $a \in \mathbb{K}$, let $\sum_{n=0}^{\infty} k_j (x-a)^n$ be a formal power series based at a which converges at all points of some open set U containing a. Then one can define a function $f : U \mapsto \mathbb{K}$ by

(2.14) $$f : k \in U \mapsto \textstyle\sum_{n=0}^{\infty} k_n (k-a)^n \in \mathbb{K}.$$

Any such function is said to be *defined* by the corresponding formal power series, and is obviously represented at a by this formal power series.

Examples 2.15 :

(a) The formal power series $\sum_{n=0}^{\infty} \frac{1}{n!}x^n$ converges at all points of $\mathbb{K}$, as one can easily verify by means of the ratio test[8]. The entire function defined on $\mathbb{K}$ by this formal power series is called the *exponential function*, and is written $\exp : \mathbb{K} \to \mathbb{K}$. Thus

(i) $$\exp : k \in \mathbb{K} \mapsto \sum_{n=0}^{\infty} \frac{1}{n!}k^n \in \mathbb{K}.$$

Note that

(i) $$\exp(0) = 1.$$

In elementary calculus one writes $\exp(k)$ as e^k. In fact we have employed this notation in Example 2.12(a), although from our work thus far formulating a reasonable intuitive justification is not so straightforward. Defining e is the easy part: $e := \exp(1)$. Interpreting $\exp(k)$ as a "power" of e, particularly when $k \in \mathbb{C}$ or when $k \in \mathbb{R}$ is irrational, is another story[9].

(b) When a polynomial $p \in \mathbb{K}[x]$ is regarded as a formal power series (as discussed immediately following (2.1)), the function defined by that formal power series is simply the polynomial function $k \mapsto p(k)$ associated with p.

(c) The *sine* and *cosine* functions mapping $\mathbb{K}$ into $\mathbb{K}$ are defined by the formal power series $\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}x^{2n+1}$ and $\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!}x^{2n}$ respectively. Since both formal power series converge for all values of k, the sine and cosine functions are entire.

Note that

(i) $$\sin(0) = 0$$

and

(ii) $$\cos(0) = 1.$$

[8]This test for absolute convergence is assumed familiar to readers when $\mathbb{K} = \mathbb{R}$; it is applied in exactly the same way when $\mathbb{K} = \mathbb{C}$.

[9]A rather important subtlety which authors of elementary calculus texts emphasizing "early transcendentals" sometimes dismiss, at best, with a wave of the hand.

(d) One has

(i) $$\exp(ic) = \cos c + i \sin c \qquad \text{for all} \qquad c \in \mathbb{C}.$$

Indeed,

$$\begin{aligned} \exp(ic) &= \textstyle\sum_{n=0}^{\infty} \frac{(ic)^n}{n!} \\ &= 1 + ic - \tfrac{c^2}{2!} - i \cdot \tfrac{c^3}{3!} + \tfrac{c^4}{4!} + i \cdot \tfrac{c^5}{5!} - \cdots \\ &= \left(1 - \tfrac{c^2}{2!} + \tfrac{c^4}{4!} - \cdots\right) + i \cdot \left(c - \tfrac{c^3}{3!} + \tfrac{c^5}{5!} - \cdots\right) \\ &= \textstyle\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n} + i \cdot \sum_{n=0}^{\infty} (-1)^n \frac{c^{2n+1}}{(2n+1)!}, \end{aligned}$$

and (i) follows. From well-known properties of the cosine and sine functions[10] we see from (i) that

(ii) $$\exp(n\pi i) = \cos n\pi = (-1)^n \qquad \text{for all} \qquad n \in \mathbb{Z},$$

thereby generalizing (i) of Example (a).

Analytic Continuation

Let $U \subset \mathbb{K}$ be a non-empty open set. A function $f : U \to K$ is[11] *analytic* if it is represented by a power series at each point $a \in U$. When the choice of $\mathbb{K}$ is relevant one speaks of a *real analytic function* when $\mathbb{K} = \mathbb{R}$, and of a *complex analytic function* when $\mathbb{K} = \mathbb{C}$.

The following observation simplifies the presentation of examples.

Proposition 2.16 : *Suppose $U \subset \mathbb{K}$ is a non-empty open set and $f : U \to \mathbb{K}$ is a function defined by a formal power series. Then f is analytic. If the formal power series is based at $a \in U$ the function is represented at a by that power series.*

Proof : Immediate from Theorem 2.11(b). **q.e.d.**

[10] Which we have no desire to prove.

[11] It is unfortunate, to say the least, that presentations of "analytic functions" are so-often restricted to the context of complex valued functions of a complex variable. Many of the major results, e.g. the Principle of Analytic Continuation (see Theorem 2.19), also hold in the real setting.

Examples 2.17 :

(a) Every entire function is analytic (by Proposition 2.16). In particular, the exponential function is analytic, every polynomial function is analytic, and the sine and cosine functions are analytic (see Examples 2.15).

(b) By a *rational function* (*on* $\mathbb{K}$) we mean a function of the form $f : k \mapsto p(k)/q(k)$, where $p, q \in \mathbb{K}[t]$ are relatively prime polynomials and the domain U_f is given by $\{\, k \in \mathbb{K} \,:\, q(k) \neq 0 \,\}$. We refer to p and q as[12] the *defining polynomials* of f. The rational functions form a field which we denote by $\mathbb{K}_F(x)$; it is in fact the quotient field of the integral domain $\mathbb{K}_F(x)$ of polynomial functions.

Every rational function is analytic.

One might suspect that when q has no roots in $\mathbb{K}$ the corresponding rational function $k \in \mathbb{K} \mapsto p(k)/q(k) \in \mathbb{K}$ must be entire, but this is false. To see a counterexample consider the rational function $r \in \mathbb{R} \mapsto 1/(r^2+1) \in \mathbb{R}$: the radius of convergence of the corresponding power series $\sum_{n=0}^{\infty}(-1)^n x^{2n}$ at 0 is 1, which by Theorem 2.13 cannot be the case for an entire function.

(c) Define $f : \mathbb{R}^\times \to \mathbb{R}$ by

$$f : r \mapsto \begin{cases} r/(r^2+1) & \text{if} \quad r < 0 \\ (3r+2)/(r^2+1) & \text{if} \quad r > 0. \end{cases}$$

Then f is analytic but is not a rational function (because the definition requires the use of more that one polynomial pair (p, q)).

(d) Quotients, reciprocals, sums, products and compositions of analytic functions are again analytic, although in each particular context one must be clear about domains. As examples: the tangent function $\tan : k \mapsto \sin k / \cos k$ has domain $\{\, k \in \mathbb{K} \,:\, \cos k \neq 0 \,\}$, whereas the sine and cosine functions each have domain $\mathbb{K}$; the secant function $\sec : k \mapsto 1/\cos k$ has the same domain as the tangent function, which is not the domain of the cosine function; the analytic functions $f : k \mapsto k - 1/k$ and $g : k \mapsto k^2 + 1$ have domains $\mathbb{K}^\times$ and $\mathbb{K}$ respectively, whereas the the composition $f \circ g : k \mapsto k^2(k^2+2)/(k^2+1)$ has domain $\mathbb{R}$ if $\mathbb{K} = \mathbb{R}$ and domain $\mathbb{C}\backslash\{i, -i\}$ if $\mathbb{K} = \mathbb{C}$.

[12] One needs to impose additional conditions to achieve uniqueness for p and q.

Theorem 2.18 : *Suppose* $U \subset \mathbb{C}$ *is a connected open set satisfying* $V := U \cap \mathbb{R} \neq \emptyset$ *and* $f : U \to \mathbb{C}$ *is a complex analytic function. Then the following statements are equivalent:*

(a) $f|_V$ *is a real analytic function;*

(b) $f|_V : V \to \mathbb{R}$*; and*

(c) f *admits a power series representation* $\left(\sum_{n=0}^{\infty} k_n(x-a)^n, D_{\mathbb{C}r}(a)\right)$ *at each point* $a \in V$ *which involves only real coefficients, i.e. with all* $k_j \in \mathbb{R}$.

Note that $V \subset \mathbb{R}$ need not be connected. For example, if U the connected open set $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ then V is the disconnected[13] open set $\mathbb{R}^\times = (-\infty, 0) \cup (0, \infty)$.

Proof :

(a) $\Rightarrow$ (b) : Obvious.

(b) $\Rightarrow$ (c) : If $(\sum_{n=0}^{\infty} k_n(x-a)^n, D_{\mathbb{C},r})$ is a power series representation of f at a point $a \in V$ then

(i) $$f(r) = \sum_{n=0}^{\infty} k_n(r-a)^n \qquad \text{for all} \qquad r \in V.$$

Since $r, f(r) \in \mathbb{R}$ we see by taking complex conjugates in (i) that

$$f(r) = \sum_{n=0}^{\infty} \overline{k}_n(r-a)^n \qquad \text{for all} \qquad r \in V.$$

By Theorem 2.11(a) the formal power series $\sum_{n=0}^{\infty} k_n(x-a)^n$ is uniquely associated with f and a. For all $n \in \mathbb{N}$ we therefore have $k_n = \overline{k}_n$, and (c) follows.

(c) $\Rightarrow$ (a) : Immediate from the definition of an analytic function.

q.e.d.

Theorem 2.19 (The Principle of Analytic Continuation) : *Let* $U \subset \mathbb{K}$ *be a non-empty connected open subset and let* $f, g : U \to \mathbb{K}$ *be analytic functions. Then for any non-empty open subset* $V \subset U$ *the following statements are equivalent:*

(a) $f = g$*;*

(b) $f|_V = g|_V$*; and*

(c) *there is a subset* $S \subset V$ *containing a limit point in* V *such that* $f|_S = g|_S$.

[13] The technical term is "separated."

The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) are obvious: the significance of the result lies in the reverse series of implications. In many applications one takes $V = U$.

Corollary 2.20 : *Suppose* $V \subset U$ *are non-empty connected open sets and* $f : U \to \mathbb{K}$ *is an analytic function with constant restriction to* V *or to some some subset thereof which contains a limit point in* V*. Then* f *is a constant function.*

Corollary 2.21 : *Suppose* $U \subset \mathbb{K}$ *is a non-empty connected open set and* $f : U \to \mathbb{K}$ *is a non-constant analytic function. Then for any subset* $S \subset U$ *admitting a limit point in* U *the restriction* $f|_S : S \to \mathbb{K}$ *cannot be a constant function.*

Corollary 2.22 : *Let* $U \subset \mathbb{C}$ *be a connected open subset having non-empty intersection with* $\mathbb{R}$*, and suppose* $f : U \to \mathbb{C}$ *is an analytic function. Assume there is a non-empty open interval* $(a, b) \subset U \cap \mathbb{R}$ *such that* $f|_{(a,b)} : (a, b) \to \mathbb{C}$ *is a constant function, say* $r \in (a, b) \mapsto c_0 \in \mathbb{C}$*. Then* f *is the constant function* $f : c \in U \mapsto c_0 \in \mathbb{C}$*.*

Proof : Since (a, b) is non-empty it contains a non-empty closed subinterval S. Since every point of S is a limit point of S, the hypotheses of Corollary 2.21 are satisfied. **q.e.d.**

Corollary 2.23 : *Suppose* $U \subset \mathbb{R}$ *is a non-empty open set and* $f : U \to \mathbb{R}$ *is a function admitting a real power series representation* $(\sum_{n=0}^{\infty} r_n(x - a)^n D_{\mathbb{R},r}(a))$ *at a point* $a \in U$*. Then there is a function* $f_{\mathbb{C}} : D_{\mathbb{C},r}(a) \to \mathbb{C}$ *satisfying*

(i) $$f_{\mathbb{C}}|_{D_{\mathbb{R},r}(a)} = f|_{D_{\mathbb{R},r}(a)}$$

which admits the complex power series representation $(\sum_{n=0}^{\infty} r_n(x - a)^n, D_{\mathbb{C},r}(a))$*. Moreover,* $f_{\mathbb{C}}$ *is the unique complex analytic function defined on* $D_{\mathbb{C},r}(a)$ *satisfying* (i).

Note from Proposition 2.16 that $f|_{D_{\mathbb{R},r}(a)}$ is a real analytic function. $f_{\mathbb{C}}$ is the *complex analytic extension* of $f|_{D_{\mathbb{R},r}(a)}$. More generally, suppose $U \subset \mathbb{R}$ is a non-empty open set and $f : U \to \mathbb{R}$ is a real analytic function. A *complex analytic extension of* f consists of an open set $V \subset \mathbb{C}$ satisfying $U = V \cap \mathbb{R}$ and a complex analytic function $g : V \to \mathbb{C}$ such that $g|_U = f$.

Proof : One sees from Proposition 2.16 that quality (i) and the asserted complex power series representation holds if $f_{\mathbb{C}}$ is defined by $c \in D_{\mathbb{C},r}(a) \mapsto \sum_{n=0}^{\infty} r_n(c - a)^n$.

To establish uniqueness suppose $g : D_{\mathbb{C},r}(a) \to \mathbb{C}$ is a complex analytic function which restricts to f on the non-empty interval $D_{\mathbb{R},r}(a)$. Since this interval contains a set with a limit point (in fact many such), we see from Theorem 2.19 that $g = f_{\mathbb{C}}$. **q.e.d.**

We need one result about complex analytic functions which is not always true for real analytic functions.

Theorem 2.24 : *Let $U \subset \mathbb{C}$ be a connected open set, let $f : U \to \mathbb{C}$ be analytic, and let $(\sum_{n=0}^{\infty} c_n(x-a)^n, D_r(a))$ be a power series representation of f at a point $a \in U$. Suppose the radius r of $D_r(a)$ is the radius of convergence of the given formal power series, that $r < \infty$, and that*

$$D_r(a) \subset U.$$

Then at least one point on the boundary $\partial(D_r(a)) := \{\, c \in \mathbb{C} \,:\, |c-a| = r \,\}$ of $D_r(a)$ is not in U or, equivalently, the closure $\mathrm{cl}(D_r(a))$ of $D_r(a)$ satisfies

$$\mathrm{cl}(D_r(a)) \not\subset U.$$

To see a counterexample for the real case take $U = \mathbb{R}$ and let $f : U \to \mathbb{R}$ denote the real analytic function $r \mapsto 1/(1+r^2)$. This has power series representation $(\sum_{n=0}^{\infty}(-1)^n x^{2n}, D_{\mathbb{R},1}(0))$ at 0, and 1 is the radius of convergence of the given series, but here we have $\mathrm{cl}(D_{\mathbb{R},1}(0)) = \mathrm{cl}((-1,1)) = [-1,1] \subset U$. Note, however, that if we consider the corresponding complex analytic function $c \mapsto 1/(1+c^2)$ the domain would then be $\mathbb{C}\backslash\{i,-i\}$, and the function would have the same power series representation at 0, provided the open interval $D_{\mathbb{R},1}(0) \subset \mathbb{R}$ were replaced by the disk $D_{\mathbb{C},1}(0)$. We would then have $i, -i \in \mathrm{cl}(D_{\mathbb{C},1}(0)) \setminus U$, thereby establishing $\mathrm{cl}(D_{\mathbb{C},1}(0)) \not\subset U$ in agreement with Theorem 2.24.

Corollary 2.25 : *Let $U \subset \mathbb{C}$ be a connected open set, let $f : U \to \mathbb{C}$ be analytic, and let $(\sum_{n=0}^{\infty} c_n(x-a)^n, D_{\mathbb{C},r}(a))$ be a power series representation of f at a point $a \in \mathbb{R}$. Suppose $r < \infty$ and*

$$\mathrm{cl}(D_{\mathbb{C},r}(a)) \subset U.$$

Then r is strictly less than the radius of convergence of the given formal power series. (That radius could be infinity.)

3. Fields of Functions

In this section $U \subset \mathbb{C}$ *denotes a connected non-empty open set.*

Let X be a topological space. A subset $S \subset X$ is *discrete* if each point $s \in S$ is contained in an open set V_s which contains no other point of S. The empty subset is always an example. When $X = \mathbb{R}$ with the usual topology examples are provided by $\mathbb{Z}$ and $\{\frac{1}{n}\}_{n=1}^{\infty}$. When $X = \mathbb{C}$ with the usual topology examples are provided by $\mathbb{Z}$, $\{\frac{1}{n}\}_{n=1}^{\infty}$, and the collection of Gaussian integers, i.e. all those $a + ib \in \mathbb{C}$ such that[14] $a, b \in \mathbb{Z}$.

A *meromorphic function* f *(on* U*)* consists of:

- a discrete subset $P_f \subset U$;
- an analytic function $f : U_{P_f} := U \setminus P \to \mathbb{C}$ which cannot be extended to an analytic function on $U_{P_f} \cup \{p\}$ for any $p \in P$; and
- for each $p \in P$ a positive integer $n = n(p)$ and an open disk $D_p \subset U_{P_f} \cup \{p\}$ centered at p such that the function

  (i) $$c \in D_p \setminus \{p\} \mapsto (c - a)^n f(c) \in \mathbb{C}$$

  is the restriction of a complex analytic function with domain D_p having a non-zero value at a.

By abuse of terminology one refers to "the meromorphic function $f : U \to \mathbb{C}$," even though the actual domain U_{P_f} is often (but not always) a proper subset of U. The elements of P_f are called the *poles* of the meromorphic function f, and the negative[15] $-n$ of the integer n is called the *order of* f *at* p and is denoted $\mathrm{ord}_p(f)$. The property described in the second bulleted items is summarized by stating that each element of P is a (*non-removable*) *singularity* of the function f. When confusion cannot otherwise result we will ease notation by dropping the subscript f from P_f.

Examples 3.1 :

(a) The restriction to U of any entire function is a meromorphic function on U. In particular, the restriction to U of any polynomial function $p(x) : \mathbb{C} \to \mathbb{C}$ is meromorphic.

[14] We will have more to say about this collection in Example 14.2(c).

[15] The integer n is called the *order of the pole* p *of* f. However, the negative of this integer proves far more convenient for purposes of analogies with concepts in number theory.

(b) Let $p, q \in \mathbb{C}[x]$ be relatively prime polynomials and let $P := (q(x))^{-1}(\mathbb{C}^\times) \cap U$. Then the rational function $c \in U \setminus P \mapsto p(c)/q(c)$ is a meromorphic function on U. Meromorphic functions of this form are called *rational functions on* U.

(c) The function $f : c \in \mathbb{C}^\times \mapsto \exp(1/c)$ is analytic on $\mathbb{C}^\times$ but is not meromorphic on $\mathbb{C}$.

Our (intuitive, non-rigorous) verification of this statement is based on the fact that any meromorphic function $f : U \to \mathbb{C}$ as given above admits a unique *Laurent series* expansion at each $p \in P$, i.e. a series expansion of the form

$$\frac{c_0}{(x-p)^n} + \frac{c_1}{(x-p)^{n-1}} + \cdots + \frac{c_{n-1}}{x-p} + c_n + c_{n+1}(x-p) + c_{n+2}(x-p)^2 + \cdots .$$

Indeed, let

$$c_0 + c_1(x-p) + c_2(x-p)^2 + \cdots$$

be the power series representation of the analytic function $c \mapsto (c-p)^n f(c)$ appearing in (i) of the definition above, and divide by $(x-p)^n$ term by term to obtain the series indicated above.

Now note from the Taylor expansion

$$\exp(c) = \textstyle\sum_{n=0}^{\infty} \frac{c^n}{n!} = 1 + c + \frac{c^2}{2!} + \cdots + \frac{c^n}{n!} + \cdots$$

that

$$\exp(1/c) = 1 + \frac{1}{c} + \frac{1}{2!c^2} + \cdots + \frac{1}{n!c^n} + \cdots ,$$

from which we see that the analytic function $c \in \mathbb{C}^\times \mapsto \exp(1/c) \in \mathbb{C}$ has no Laurent expansion at the singularity $p = 0$, hence cannot be meromorphic.

(d) Sums, products and reciprocals of meromorphic functions on U are again meromorphic functions on U.

Example 3.1(d) has the following important consequence.

Theorem 3.2 : *The collection $\mathcal{M}(U)$ of meromorphic functions on U is a field, the collection $\mathcal{R}(U)$ of rational functions is subfield, and the collection $\mathcal{P}(U)$ of polynomial functions on U is, in turn, a subring of $\mathcal{R}(U)$.*

One can find a proof in [D, Chapter IX, the first paragraph of §17, p. 246], although there the terminology "field" does not appear.

The advantage in restricting the definition of a meromorphic function to the complex setting is topological: a connected open set in $\mathbb{C}$ remains connected when a discrete subset is removed, whereas this is not the case for a connected open subset of $\mathbb{R}$. Without connectivity one cannot make use of the Principle of Analytic Continuation (Theorem 2.19), which is a fundamental ingredient in the proof of Theorem 3.2.

Corollary 3.3 : *When $V \subset U$ is a non-empty connected open set the restriction mapping*

$$\text{(i)} \qquad f \in \mathcal{M}(U) \mapsto f|_V \in \mathcal{M}(V)$$

is a field embedding. Moreover, when this embedding is restricted to either $\mathcal{R}(U)$ or $\mathcal{P}(U)$ the result is a ring isomorphism between $\mathcal{R}(U)$ and $\mathcal{R}(V)$ or $\mathcal{P}(U)$ and $\mathcal{P}(V)$ respectively.

Recall from the second paragraph of §2. that $\mathbb{C}_F[x]$ denotes the integral domain of polynomial functions $p(x) : \mathbb{C} \to \mathbb{C}$, and from Example 2.17(b) that $\mathbb{C}_F(x)$ denotes the field of rational functions on $\mathbb{C}$. In terms of the notation introduced in Theorem 3.2 we therefore have

$$\mathbb{C}_F[x] = \mathcal{P}(\mathbb{C}) \qquad \text{and} \qquad \mathbb{C}_F(x) = \mathcal{M}(\mathbb{C}).$$

Corollary 3.4 : *The restriction mapping*

$$f \in \mathbb{C}_F(x) \mapsto f|_U \in \mathcal{R}(U)$$

is a field isomorphism, and the restriction mapping

$$f \in \mathbb{C}_F[x] \mapsto f|_U \in \mathcal{P}(U)$$

is an isomorphism of integral domains.

In particular, if one is only working with functions in $\mathcal{P}(U)$ or $\mathcal{R}(U)$ one can assume w.l.o.g. that $U = \mathbb{C}$ and work instead with $\mathbb{C}_F[x]$ or $\mathbb{C}_F(x)$ accordingly.

We will need an analogue of Theorem 3.2 for the real case. To this end define

$$U_{\mathbb{R}} := U \cap \mathbb{R}, \tag{3.5}$$

which could be the empty set, and when not empty need not be connected. When non-empty let $\mathcal{M}_{\mathbb{R}}(U)$, $\mathcal{R}_{\mathbb{R}}(U)$ and $\mathcal{P}_{\mathbb{R}}(U)$ denote denote all those $f \in \mathcal{M}(U)$, $\mathcal{R}(U)$ and $\mathcal{P}(U)$ respectively having real values when restricted to $U_{\mathbb{R}} \setminus P_f$. One then has the following chain of field and (in the final case) ring containments

$$\mathcal{M}(U) \supset \mathcal{M}_{\mathbb{R}}(U) \supset \mathcal{R}_{\mathbb{R}}(U) \supset \mathcal{P}_{\mathbb{R}}(U). \tag{3.6}$$

Examples 3.7 : Let $U \subset \mathbb{C}$ be any non-]empty connected open set with the property that $U_{\mathbb{R}} = U \cap \mathbb{R}$ is also non-empty.

(a) Any entire function which admits a real formal power series representation at some point of $U_{\mathbb{R}}$ restricts to an element of the field $\mathcal{M}_{\mathbb{R}}(U)$. In particular, the exponential function, and the sine and cosine functions, restrict to elements of $\mathcal{M}_{\mathbb{R}}(U)$.

(b) The field $\mathcal{R}_{\mathbb{R}}(U)$ consists of those rational functions in $\mathcal{M}_{\mathbb{R}}(U)$ defined by quotients of real polynomials. The integral domain $\mathcal{P}_{\mathbb{R}}(U)$ consists of those polynomial functions in $\mathcal{M}_{\mathbb{R}}(U)$ defined by real polynomials.

(c) Let $W := \mathbb{C}\backslash\{1+2i, 1-2i\}$ and note that $1 \pm 2i$ are the roots of the polynomial $x^2 - 2x + 5 \in \mathbb{R}[x]$. The function $f : c \in W \mapsto \exp(1/(x^2 - 2x + 5)) \in \mathbb{C}$ is analytic, but is not meromorphic[16] on $\mathbb{C}$. It follows that the restriction of f to U is meromorphic if and only if $U \cap \{1 \pm 2i\} = \emptyset$.

Let U_1 be the interior of the ellipse within $\mathbb{C}$ defined by the equation $9(x-1)^2 + y^2 = 9$ and let $U_2 = D_1(1) \subset \mathbb{C}$. Note that $U_2 \subset U_1$, that $\{1 \pm 2i\} \subset U_1$, and that $\{1 \pm 2i\} \cap U_2 = \emptyset$. It follows that

$$f|_{U_1} \notin \mathcal{M}_{\mathbb{R}}(U_1), \qquad \text{whereas} \qquad f|_{U_2} \in \mathcal{M}_{\mathbb{R}}(U_2).$$

The example illustrates the fact that the field embedding (i) in Corollary 3.3 need not be an isomorphism.

For our purposes the important thing about meromorphic functions is that the collection of all such entities defined on U forms a field. If one wants to introduce the concept of a "real meromorphic function" one would insist on a similar result for connected open subsets of $\mathbb{R}$, as well as analogues of results such as Corollary 3.3. We will achieve analogues in far more direct manner[17]. Specifically, for $U_{\mathbb{R}} \subset \mathbb{R}$ as

[16] Argue as in Example 3.1(c).

[17] Indeed, one rarely (if ever) hears mention of "real" meromorphic functions.

defined in (3.5) let $\mathcal{M}(U_{\mathbb{R}})$, $\mathcal{R}(U_{\mathbb{R}})$ and $\mathcal{P}(U_{\mathbb{R}})$ consist of the restrictions to $U_{\mathbb{R}}$ of all those $f \in \mathcal{M}_{\mathbb{R}}(U)$, $\mathcal{R}_{\mathbb{R}}(U)$ and $\mathcal{P}_{\mathbb{R}}(U)$ respectively. Note from Example 3.7(d) that

$$(U_1)_{\mathbb{R}} = (U_1)_{\mathbb{R}} \qquad \not\Rightarrow \qquad \mathcal{M}((U_1)_{\mathbb{R}}) = \mathcal{M}((U_2)_{\mathbb{R}}). \tag{3.8}$$

This should explain why we have involved U in the notation $\mathcal{M}(U_{\mathbb{R}})$: otherwise, since $(U_1)_{\mathbb{R}} = (U_1)_{\mathbb{R}} = (0,2) \subset \mathbb{R}$ in that example, we would have been forced to write (3.8) in a rather confusing way, i.e. as $(U_1)_{\mathbb{R}} = (U_1)_{\mathbb{R}} \not\Rightarrow \mathcal{M}((0,2)) = \mathcal{M}((0,2))$.

Theorem 3.9 : *$\mathcal{M}(U_{\mathbb{R}})$ is a field, and the mapping $f \in \mathcal{M}_{\mathbb{R}}(U) \mapsto f|_{U_{\mathbb{R}}} \in \mathcal{M}(U_{\mathbb{R}})$ is a field isomorphism. Moreover, the analogous results hold for the subfield $\mathcal{R}(U_{\mathbb{R}})$ and subring $\mathcal{P}(U_{\mathbb{R}})$ of $\mathcal{R}(U_{\mathbb{R}})$.*

Proof : Since addition and multiplication of functions commutes with restriction $\mathcal{M}(U_{\mathbb{R}})$ must at least have the structure of a ring, and f must at least be a ring homomorphism. The surjectivity of the indicated mapping is immediate from the definition of $\mathcal{M}(U_{\mathbb{R}})$. Since $\mathcal{M}(U|_{\mathbb{R}})$ contains all constant functions $r \in U_{\mathbb{R}} \mapsto r_0 \in \mathbb{R}$, f is not the zero mapping. Since $\mathcal{M}(U)$ is a field $\ker(f)$ must be trivial, thereby establishing injectivity. This gives the result for $\mathcal{M}(U_{\mathbb{R}})$; what remains can be established with similar arguments. **q.e.d**.

Any real polynomial function $p(x) : \mathbb{R} \to \mathbb{R}$ can be viewed as a polynomial function from $\mathbb{C}$ into $\mathbb{C}$: substitute complex numbers for x rather than restricting to real numbers. The result is an integral domain embedding $\mathbb{R}_F[x] \to \mathbb{C}_F[x]$ which we simply regard as an inclusion mapping. We denote by $h : \mathbb{R}_F(x) \to \mathbb{C}_F(x)$ the obvious extension of this embedding to $\mathbb{R}_F(x)$.

Corollary 3.10 : *One has a commutative diagram*

$$\begin{array}{ccc} & & \mathcal{M}(U_{\mathbb{R}}) \\ & & \Big| \\ \mathbb{R}(x) & \xrightarrow{f} & \mathcal{R}(U_{\mathbb{R}}) \\ \Big| & & \Big| \\ \mathbb{R}[x] & \xrightarrow{f|_{\mathbb{R}[x]}} & \mathcal{P}(U_{\mathbb{R}}) \end{array}$$

in which the vertical mappings are upward inclusions, the upper horizontal mapping is a field isomorphism, and the lower horizontal mapping is an integral domain isomorphism.

Proof : First observe that the image of the function $h : \mathbb{R}_F(x) \to \mathbb{C}_F(x)$ introduced just prior to the corollary statement is $\mathcal{R}_{\mathbb{R}}(U)$, and we can therefore assume that h is an isomorphism between $\mathbb{C}_F(x)$ and $\mathcal{R}_{\mathbb{R}}(U)$. However, by Corollary 3.4 there is an isomorphism between the fields $\mathbb{R}(x)$ and $\mathbb{R}_F(x)$ and by Theorem 3.9 there is an isomorphism between the fields $\mathcal{R}_{\mathbb{R}}(U)$ and $\mathcal{R}(U_{\mathbb{R}})$. The composition f of the isomorphisms within the sequence

$$\mathbb{R}(x) \xrightarrow{\approx} \mathbb{R}_F(x) \xrightarrow{\approx} \mathcal{R}_{\mathbb{R}}(U) \xrightarrow{\approx} \mathcal{R}(U_{\mathbb{R}})$$

is then easily checked to have the required properties. **q.e.d.**

4. Derivatives of Analytic Functions

As in the previous section, $\mathbb{K}$ *denotes the real field* $\mathbb{R}$ *or the complex field* $\mathbb{C}$*. The symbol* U *denotes a non-empty open subset of* $\mathbb{K}$*.*

Let a be a point in U. A function $f : U \to \mathbb{K}$ is *differentiable at* a if the associated "Newton Quotient" function

$$k \in U \setminus \{a\} \mapsto \frac{f(k) - f(a)}{k - a} \tag{4.1}$$

extends to a continuous function from U into $\mathbb{K}$, in which case the value

$$f'(a) := \lim_{h->0} \frac{f(a+h) - f(a)}{h} \tag{4.2}$$

of this extension at a is referred to as the *derivative of* f *at* a. The given function is *differentiable* if it is differentiable at all points of U, and when this is the case the corresponding function

$$f' : k \in U \mapsto f'(k) \in \mathbb{K} \tag{4.3}$$

is called the (*first*) *derivative of* f.

Very early in the study of calculus one is made aware of following properties of differentiable functions[18] (although not necessarily the proofs thereof, and no doubt under the assumption that $\mathbb{K} = \mathbb{R}$).

Theorem 4.4 : *Suppose* $f, g : U \to \mathbb{K}$ *are differentiable. Then:*

(a) $fg : U \to \mathbb{K}$ *is differentiable and* $(fg)' = fg' + f'g$*;*

(b) $f + g$ *is differentiable and* $(f + g)' = f' + g'$*;*

(c) f' *is the zero function if* f *is "constant," i.e. is a constant function; and*

(d) *if* U *is connected then* $f' = g'$ *if and only if* f *and* g *"differ by a constant," i.e. if and only if* $f - g$ *is a constant function.*

The relevant associated result for analytic functions is the following.

[18] Which we have no intention of proving.

Theorem 4.5 : *All analytic functions are differentiable, and are therefore continuous. Moreover, if* $f : U \subset \mathbb{K} \to \mathbb{K}$ *is such a function, and if* $(\sum_{n=0}^{\infty} k_n(x-a)^n, D_r(a))$ *is a power series representation of* f *at a point* $a \in U$*, then* $(\sum_{n=0}^{\infty} nk_n(x-a)^{n-1}, D_r(a))$ *is a power series representation of* f' *at* a*. In particular, the derivative of an analytic function is an analytic function.*

Corollary 4.6 :

(a) *For any* $p \in \mathbb{K}[x]$ *the associated polynomial function* $p(x) : \mathbb{K} \to \mathbb{K}$ *is differentiable, and when* $p = \sum_{j=0}^{n} k_j x^j$ *the derivative* $p'(x) \in \mathbb{K}_F[x]$ *is the polynomial function associated with*

$$p' := \sum_{j=0}^{n} j k_j x^{j-1}.$$

(b) *The exponential function* $\exp : \mathbb{K} \to \mathbb{K}$ *is differentiable and admits* $\exp : \mathbb{K} \to \mathbb{K}$ *as derivative, i.e.*

$$\exp' = \exp .$$

(c) *The sine function* $\sin : \mathbb{K} \to \mathbb{K}$ *is differentiable, and one has*

$$\sin' = \cos .$$

(d) *The cosine function* $\cos : \mathbb{K} \to \mathbb{K}$ *is differentiable, and one has*

$$\cos' = -\sin .$$

Corollary 4.7 : *Suppose* $V \subset U \subset \mathbb{K}$ *are non-empty connected open sets and* $f, g : U \to \mathbb{K}$ *are analytic functions. Then:*

(a) $f - g : U \to \mathbb{K}$ *is a constant function if and only if* $f'|_V = g'|_V$*;*

(b) *if* $f - g$ *is a constant function then for any* $k_0 \in V$ *one has* $f = g + (f(k_0) - g(k_0))$*; and*

(c) $f = g$ *if and only if* $f' = g'$ *and there is a point* $k_0 \in V$ *such that* $f(k_0) = g(k_0)$*.*

For many applications[19] one chooses $V = U$.

[19] E.g. see the proof of Corollary 4.9.

Proof :

(a) $\Rightarrow$ By Theorem 4.4(d) we the difference $f' - g' = (f-g)'$ must be the zero function.

$\Leftarrow$ By Theorem 4.4(d) the difference $f - g$ is constant when restricted to V hence by Corollary 2.20 must be constant.

(b) and (c) are immediate from (a).

q.e.d.

The following result is one of the most important tools for calculating derivatives.

Theorem 4.8 (The Chain-Rule) : *Suppose $U, V \subset \mathbb{C}$ are non-empty open sets, $a \in U$, and $g : U \to V$ and $f : V \to \mathbb{K}$ are functions which are differentiable at a and $g(a) \in V$ respectively. Then the composition $f \circ g : U \to \mathbb{K}$ is differentiable at a and*

(i) $$(f \circ g)'(a) = f'(g(a)) \cdot g'(a).$$

Corollary 4.9 : *One has*

(i) $$\cos^2 r + \sin^2 r = 1 \qquad \textit{for all} \qquad r \in \mathbb{R},$$

and, as a consequence,

(ii) $$|\exp(ir)| = 1 \qquad \textit{for all} \qquad r \in \mathbb{R}.$$

Geometrically, (ii) asserts that the image of the function $r \in \mathbb{R} \mapsto \exp(ir) \in \mathbb{C}$ is contained in the *unit circle* $S^1 := \{\, c \in \mathbb{C} \,:\, |c| = 1 \,\}$ of the complex plane. In fact the image is the all of S^1. Indeed, much more is true, but is so-well known that repeating all the proofs would seem silly: the function is a group homomorphism[20] from the additive real numbers onto the multiplicative subgroup $S^1 \subset \mathbb{C}$.

Proof : From the chain-rule one has

$$\begin{aligned} (\cos^2 + \sin^2)' &= 2 \cdot \cos \cdot (\cos)' + 2 \cdot \sin \cdot (\sin)' \\ &= 2 \cdot \cos \cdot (-\sin) + 2 \cdot \sin \cdot \cos \\ &= -2 \cdot \cos \cdot \sin + 2 \cdot \cos \cdot \sin \\ &= 0, \end{aligned}$$

[20] In fancier language, it is a "character" of the additive group $\mathbb{R}$.

and $\cos^2 + \sin^2 : \mathbb{R} \to \mathbb{R}$ and the constant function $r \in \mathbb{R} \mapsto 1 \in \mathbb{R}$ therefore have the same derivative. Since both functions have value 1 at 0 equality (i) now follows from Corollary 4.7(c).

For equality (ii) use (i) of Example 2.15(d). **q.e.d.**

If $f : U \to \mathbb{K}$ is a differentiable function one might ask if this is also true of $f' : U \to \mathbb{K}$. The function f is *infinitely differentiable*, or is a[21] *C^∞-function*, or is a *smooth function*, if f is differentiable and the derivative of each derivative of f is also differentiable. When this is the case the following terminology and notations are employed: the derivative of $f^{(1)} := f'$ of $f^{(0)} := f$ is called the *second derivative of f*, is denoted f'' or $f^{(2)}$, and for $n \geq 2$ the derivative of $f^{(n-1)}$, known as the *n^{th}-derivative of f*, is denoted $f^{(n)}$. On occasion one writes $f^{(3)}$ as f'''.

Corollary 4.10 : *Every analytic function is infinitely differentiable. Moreover, if $f : U \to \mathbb{K}$ is analytic and $(\sum_{n=0}^{\infty} k_n(x-a)^n, D_r(a))$ is a power series representation of f at a point $a \in U$ then*

(i) $$f^{(n)}(a) = n!k_n \qquad \textit{for all} \qquad n \in \mathbb{N}.$$

In particular,

(ii) $$(\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n, D_r(a))$$

is a power series representation of f at a.

The formal power series appearing in (ii) is called the *Taylor series of f at a*. In view of (i) one could think of this formal infinite series as a "storage file" for the values of f, f', f'' and all higher derivatives $f^{(n)}$ of f at a. The definition of this formal power series does not require an analyticity hypothesis for a given function $f : U \to \mathbb{K}$: only the existence of $f^{(n)}(a)$ for all $n \in \mathbb{Z}^+$.

Example 4.11 : The function $f : \mathbb{R} \to \mathbb{R}$ introduced in Example 2.12(a) is the standard example of a smooth non-analytic function. Non-analyticity is immediate from Corollary 2.22: f is not the zero function but agrees with the zero function on the connected open set $(-\infty, 0) \subset \mathbb{R}$. As for smoothness: the restriction $f|_{(-\infty,0)}$ is the zero function, hence analytic, hence C^∞, and $f|_{(0,\infty)}$ is the composition of two analytic functions, is therefore analytic by Example 2.17(d), hence is also C^∞. The

[21] Read C^∞ as "see infinity."

restriction $f|_{\mathbb{R}^\times}$ is therefore smooth. Using L'Hopital's rule and induction one can prove that

(i) $$f^{(n)}(0) = 0 \qquad \text{for all} \qquad n \in \mathbb{N},$$

and smoothness is thereby established.

Note from (ii) of Corollary 4.10 and (i) that the Taylor series of f at 0 is $\sum_{n=0}^{\infty} 0$.

5. Primitives of Analytic Functions

Once again $\mathbb{K}$ *denotes the real field* $\mathbb{R}$ *or the complex field* $\mathbb{C}$*, and the symbol* U *denotes a non-empty open subset of* $\mathbb{K}$*.*

Suppose $f, g : U \to \mathbb{K}$ and g is differentiable. Then g is a *primitive* of f if

$$f = g', \tag{5.1}$$

and to indicate this is the case one writes

$$g = \int f. \tag{5.2}$$

One also refers to primitives as *antiderivatives* and as (*indefinite*) *integrals*, e.g. (5.2) would be indicated by the statement "g is the integral of f" (even though f might admit many primitives).

One might hope for a result analogous to Theorem 4.5 for primitives, but when that is the goal things become far more complicated[22]. One might expect to construct a primitive $g : U \to \mathbb{K}$ for an analytic function $f : U \to \mathbb{K}$ by first defining g "locally," i.e. on small open disks within U as follows: given any $a \in U$ choose a power series representation $(\sum_{n=0}^{\infty} k_n(x-a)^n, D_r(a))$ of f at a and let $g_{D_r(a)} : D_r(a) \to \mathbb{K}$ be the function defined by the formal power series $\sum_{n=0}^{n} k_n \frac{(x-a)^{n+1}}{n+1}$. In fact this series does converge on $D_r(a)$, and one does have $(g_{D_r(a)})' = f|_{D_r(a)}$. The problem is that when two such disks D_1 and D_2 have non-empty intersection the corresponding "local primitives" g_{D_1} and g_{D_2} will not generally coincide on the overlap, thereby bringing into question the existence of a collection of "small domain" primitives which can be amalgamated[23] into a primitive for f defined on U.

Before illustrating the problem with a concrete example we record, for later reference, one positive aspect of the discussion in the previous paragraph.

Theorem 5.3 : *Suppose* $D \in \mathbb{K}$ *is an open disk with center* $a \in \mathbb{K}$*, and* $\sum_{n=0}^{\infty} k_n(x-a)^n$ *is a formal power series defining an analytic function* $f : D \to \mathbb{K}$*. Then the formal power series* $\sum_{n=0}^{\infty} k_n \frac{(x-a)^{n+1}}{n+1}$ *defines an analytic primitive* $g : D \to \mathbb{K}$ *of* f*.*

[22] Or far more interesting, depending on your attitude. However, when one is facing a deadline for finishing a particular set of notes, "complicated" seems more appropriate.

[23] This question would induce instant salivary excitement in anyone with a background in algebraic topology or sheaf theory. In those subjects the "fitting possibilities" for local data are measured in terms of elements of associated groups.

Proof : By means of the ratio test one sees that the two formal power series have the same radius of convergence, and it follows that the second series defines an analytic function $g : D \to \mathbb{K}$. One then sees from Corollary 4.10, with f in that statement replaced by g, that $g' = f$. **q.e.d.**

Example 5.4 : Suppose $U := D_1(0) \cup D_1(1) \subset \mathbb{K}$ and we wish to apply Theorem 5.3 to construct a primitive $g : U \to \mathbb{K}$ for the analytic identity function $f : k \in U \mapsto k \in \mathbb{K}$. (Of course the function $k \in U \mapsto k^2/2 \in \mathbb{K}$ has the required property, but suppose we temporarily suspend awareness of this fact.) A power series representation of f at 0 is given by $(x, D_1(0))$, a power series representation of f at 1 is given by $(1 + (x-1), D_1(1))$, and the respective primitives resulting from Theorem 5.3 are $g_0 : k \mapsto k^2/2$ and $g_1 : k \mapsto (k-1) + (k-1)^2/2$. What we have in mind is to "glue" these two functions together by means of the prescription

$$\text{(i)} \qquad k \in U \mapsto \begin{cases} g_0(k) & \text{if} \quad k \in D_1(0) \\ g_1(k) & \text{if} \quad k \in D_1(1) \end{cases}$$

so as to produce an analytic primitive $g : U \to \mathbb{K}$ of f as desired. However, this definition makes sense for those $k \in D_1(0) \cap D_1(1)$ only if

$$\text{(ii)} \qquad g_0|_{D_1(0)\cap D_1(1)} = g_1|_{D_1(0)\cap D_1(1)},$$

and one can see immediately from $x^2/2 - \big((x-1) + (x-1)^2/2\big) = 1/2$ that this is not the case. On the other hand, in this particular example the problem is easily fixed by replacing g_1 with the analytic function $k \in U \mapsto g_1(k) + 1/2$.

The following result gives a more general version of the construction seen in Example 5.4.

Theorem 5.5 : *Suppose $D_0, D_1, D_2, \cdots \subset \mathbb{K}$ is a sequence of non-empty open disks satisfying*

$$\text{(i)} \qquad D_0 \cap D_i \cap D_j \neq \emptyset \qquad \textit{for all} \qquad j \in \mathbb{Z}^+.$$

Define

$$\text{(ii)} \qquad U := \cup_{n\in\mathbb{N}} D_j,$$

and suppose $f : U \to \mathbb{K}$ is an analytic function which admits a power series representation $(\sum_{n=0}^{\infty} a_{nj}(x - a_j)^n, D_j)$ at the center a_j of each D_j. Then f admits an analytic primitive $g : U \to \mathbb{K}$ which is represented by the formal power series $\sum_{n=0}^{\infty} a_{nj} \frac{(x-a_0)^{n+1}}{n+1}$ on the disk D_0.

Proof : For $j = 0, 1, 2, \ldots$ let $g_j : D_j \to \mathbb{K}$ be the analytic function defined by the formal power series $\sum_{n=0}^{\infty} a_{nj} \frac{(x-a_j)^{n+1}}{n+1}$. By Theorem 5.3 each g_j is a primitive of f on D_j, and for all $i \in \mathbb{Z}^+$ we also have

$$f|_{D_0 \cap D_i \cap D_j} = g_i'|_{D_0 \cap D_i \cap D_j} = g_j'|_{D_0 \cap D_i \cap D_j}.$$

Since each $D_0 \cap D_i \cap D_j$ is non-empty and connected it follows from Theorem 4.4(d) that $g_0 - g_j$ is constant when restricted to this intersection, and since $D_0 \cup D_j$ is also connected it then follows from Corollary 2.20 that $g_0 - g_j$ is a constant function on the intersection $D_0 \cap D_j$. By adjusting each g_j by the addition of an appropriate scalar we can then assume w.l.o.g. that

$$g_0|_{D_0 \cap D_j} = g_j|_{D_0 \cap D_j} \qquad \text{for all} \qquad j \in \mathbb{Z}^+,$$

hence that

$$g_0|_{D_0 \cap D_i \cap D_j} = g_i|_{D_0 \cap D_i \cap D_j} = g_j|_{D_0 \cap D_i \cap D_j} \qquad \text{for all} \qquad i, j \in \mathbb{Z}^+,$$

whereupon the connectivity of $D_0 \cap D_i \cap D_j$ and $D_i \cap D_j$, together with Theorem 2.19, give

$$g_i|_{D_i \cap D_j} = g_j|_{D_i \cap D_j} \qquad \text{for all} \qquad i, j \in \mathbb{N}.$$

An analytic primitive g of f is therefore unambiguously defined at any $k \in U$ by picking any index $j \in \mathbb{N}$ such that $k \in D_j$ and setting $g(k) := g_j(k)$. To complete the proof simply note by construction that $g|_{D_0} = g_0$. **q.e.d.**

Examples 5.6 :

(a) **(The Natural Logarithm Function) :** By replacing k by $x - k$ in the geometric series (i) of Example 2.12(b) one sees that for any $k \in \mathbb{K}^\times$ one has

$$\begin{aligned} \tfrac{1}{x} &= \tfrac{1}{k+(x-k)} \\ &= \tfrac{1}{k} \cdot \tfrac{1}{1+(1/k)(x-k)} \\ &= \tfrac{1}{k} \cdot \left(1 + \tfrac{(x-k)}{k} + (\tfrac{(x-k)}{k})^2 + (\tfrac{(x-k)}{k})^3 + \cdots\right), \end{aligned}$$

and as a result that the analytic function $f : k \in \mathbb{K}^\times \mapsto 1/k$ is represented by the formal power series

(i) $$\sum_{n=0}^{\infty} \tfrac{1}{k^{n+1}} (x-k)^n$$

at any point $k \in K^\times$. Indeed, this series is easily seen to have radius of convergence $|k|$, and $\left(\sum_{n=0}^{\infty} \frac{1}{k^{n+1}}(x-k)^n, D_{|k|}(k)\right)$ is therefore a power series representation of the rational function $f : \mathbb{R}^\times \to \mathbb{R}$ corresponding to $1/x$ at each such k.

For $j = 0, 1, 2, \ldots$ define $D_j := D_{j+1}(j)$ and let $U_1 := \cup_{j \geq 0} D_j$. Thus

$$U_1 = \begin{cases} (0, \infty) \subset \mathbb{R} & \text{if } \mathbb{K} = \mathbb{R}, \\ \text{the open right-half plane} \subset \mathbb{C} & \text{if } \mathbb{K} = \mathbb{C}. \end{cases}$$

By Theorem 5.5 there is an analytic primitive $g_1 : U \to \mathbb{K}$ for $f|_{U_1}$ having formal power series representation $\left(\sum_{n=0}^{\infty} \frac{(x-1)^{n+1}}{n+1}, D_1(1)\right)$. In particular,

(ii) $$g_1(1) = 0.$$

When $\mathbb{K} = \mathbb{R}$ the (*real*) *natural logarithm function* refers to either the analytic function

(iii) $$\ln := g_1 : U_1 = (0, \infty) \to \mathbb{R}$$

or the analytic function[24] $\text{lnabs} : \mathbb{R}^\times \to \mathbb{R}$ defined by

(iv) $$\text{lnabs} : r \in \mathbb{R}^\times \mapsto \ln(|r|) \in \mathbb{R}.$$

Note by construction that

(v) $$\ln'(r) = \frac{1}{r} \qquad \text{for all} \qquad r \in (0, \infty),$$

and from (v) and the chain-rule that

(vi) $$\text{lnabs}'(r) = \frac{1}{r} \qquad \text{for all} \qquad r \in \mathbb{R}^\times.$$

In particular, the introduction of the function lnabs solves the problem (discussed in the introduction) of integrating the rational function $r \in \mathbb{R}^\times \mapsto 1/r \in \mathbb{R}$.

[24]Read "lnabs" as "log absolute (value)," "ell en absolute (value)," or as "Lynn abs." It is not standard notation, but in the current discussion one needs to distinguish this function from the real natural logarithm function.

Even though the vastly expanded domain for lnabs might seem desirable, we will see that the definition creates technical (but surmountable) problems when the aim is to formulate elementary calculus in terms of fields of functions.

To define the natural logarithm function when $\mathbb{K} = \mathbb{C}$ we need to do a bit more work. To that end redo the construction of U_1 in the previous paragraph by replacing $D_1(j+1)$ with $D_1(i(j+1))$ for $j = 0, 1, 2, \ldots$ (wherein $i := \sqrt{-1}$). The union $U_2 := \cup_{j\geq 0} D_j$ is then the open upper-half plane, and we can invoke Theorem 5.5 to define an analytic primitive $g_2 : U_2 \to \mathbb{C}$ for $f|_{U_2}$. Since $g_2|_{U_1\cap U_2}$ and $g_1|_{U_1\cap U_2}$ have the same derivative these two functions differ by a constant, and by adjusting g_2 by adding or subtracting that constant we can assume w.l.o.g. that these two restrictions are identical. This ensures that a primitive $g_{12} : U_1 \cup U_2 \to \mathbb{C}$ of $f|_{U_1\cup U_2}$ extending $g_1 : U_1 \to \mathbb{C}$ is unambiguously defined by

$$g_{12}(c) := \begin{cases} g_1(k) & \text{if} \quad k \in U_1 \\ g_2(k) & \text{if} \quad k \in U_2. \end{cases}$$

Now redo the original construction once more, this time replacing $D_1(j+1)$ with $D_1(-(j+1))$ for $j = 0, 1, 2, \ldots$. In this case the resulting union $U_3 = \cup_{j\geq 0} D_j$ is the open left-half plane, and by means of the obvious modification of the construction of $g_{12} : U_1 \cup U_2 \to \mathbb{C}$ from $g_1 : U_1 \to \mathbb{C}$ we can extend the analytic function g_{12} to an analytic primitive g of f defined on the connected open set

(vii) $$U^{\log} := U_1 \cup U_2 \cup U_3.$$

Note that $U^{\log}$ can be described as the complex plane $\mathbb{C}$ with the non-positive purely imaginary axis removed[25]. When $\mathbb{K} = \mathbb{C}$ the (*complex*) *natural logarithm function* refers (for our purposes[26]) to the function g. When $\mathbb{K} = \mathbb{R}$ we

[25]Or, in more classical terms, the complex plane slit from (and including) 0 down the negative imaginary axis.

[26]There are other conventions for how the plane should be cut in defining the complex logarithm, the most common being "along the closure of the negative real axis." But that particular construction will not suit our needs.

In classical terms we have only constructed one "branch" of the complex logarithm function: additional branches arise by continuing the process beyond the third step. However, at the very next step one finds that the new domain overlaps U_1, whereas the associated primitive g_4 does not agree with g_1. One thus appears to have entered a world of "multi-valued functions," a concept

define

(viii) $$U^{\log} := (0, \infty).$$

When $\mathbb{K}$ is clear from context we will simply refer to the *natural logarithm function*, and in either case we will adopt the standard[27] notation[28]

(ix) $$\ln : k \in U^{\log} \mapsto \ln k \in \mathbb{K}$$

for this function. From the construction we have now achieved

(x) $$\ln'(k) = \frac{1}{k} \qquad \text{for all} \qquad k \in U^{\log}$$

in both cases.

Note from (ii) that

(xi) $$\ln 1 = \text{lnabs } 1 = 0.$$

(b) **(The Arctangent Function) :** The arctangent function is the standard primitive for the analytic function $k \mapsto 1/(k^2+1)$ with domain $\mathbb{R}$ or $\mathbb{C}\backslash\{i, -i\}$ according as $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. It can be constructed in analogy with the construction of the natural logarithm function seen in Example (a), beginning with the the power series representation

$$\frac{1}{x^2+1} = (\textstyle\sum_{n=0}^{\infty}(-1)^n x^{2n}, D_1(0)).$$

However, we prefer to exploit the work already done in that example.

We begin with the injective meromorphic function[29]

$$g : c \in \mathbb{C}\backslash\{-i\} \mapsto -\frac{ic+1}{c+i} \in \mathbb{C}.$$

One checks the following.

---

which renders the introduction of a field structure virtually impossible. Riemann showed long ago how multi-valued function nonsense could be replaced by a spectacular algebraic/geometric theory of "single-valued functions," but one still finds multi-valued functions discussed in contemporary textbooks.

[27]Except for the "log" superscript.

[28]Here we follow custom and write $\ln k$ rather than $\ln(k)$. We will restore the parentheses when confusion might otherwise result.

[29]Meromorphic functions of this quotient form are called *Möbius transformations*.

- The image of $\mathbb{R}$ under this mapping is the unit circle $S^1 := \partial(D_1(0)) \subset \mathbb{C}$ after the "south pole" $-i$ has been removed. Indeed, one can view the restriction $g|_{\mathbb{R}}$ as the composition of the mapping $r \in \mathbb{R} \mapsto -r \in \mathbb{R}$ followed by the inverse of stereographic projection from the south pole of this circle to the real line.
- The image of the imaginary axis $i\mathbb{R}$ with $-i$ removed is again $i\mathbb{R}\backslash\{-i\}$. Moreover, the preimage of the closure of the[30] negative imaginary axis after $-i$ has been removed is $i(-\infty, -1) \cup i[1, \infty)$.

Define

$$U^{\rm atn} := \mathbb{C}\backslash\big(i(-\infty, -1] \cup i[1, \infty)\big). \tag{i}$$

From the second bulleted item above one sees that the g-image of the open set $U^{\rm atn}$ is contained in the domain of the complex natural logarithm function defined in the previous example[31]. We can therefore define a complex analytic function $f : U^{\rm atn} \to \mathbb{C}$ by $(1/2i) \cdot (\ln \circ g|_U) - \frac{\pi}{2} : U \to \mathbb{C}$, i.e. by

$$f : c \in U^{\rm atn} \mapsto \frac{1}{2i} \cdot \ln\big(-\frac{ic+1}{c+i}\big) - \frac{\pi}{2} \in \mathbb{C}. \tag{ii}$$

This is the *complex arctangent function*. Note that

$$f(1) = \pi/4, \tag{iii}$$

and by means of the chain-rule that

$$f'(c) = \frac{1}{c^2+1} \qquad \text{for all} \qquad c \in U^{\rm atn}. \tag{iv}$$

Let $U \subset \mathbb{C}$ be that component of $\exp^{-1}(U^{\log})$ containing $\mathbb{R}$. Choose any $r_0 \in \mathbb{R}$, an open disk $D_r(r_0) \subset U$, and consider the complex analytic function

$$h_{r_0,r} : c \in D_r(r_0) \mapsto \ln(\exp(ic)) \in \mathbb{C}.$$

[30] The "negative imaginary axis" refers to the collection of complex numbers $a+ib$ satisfying $a = 0$ and $b \leq 0$. When $a, b \in \mathbb{R} \cup \{\pm\infty\}$ satisfy $a < b$ we denote the open interval $\{\, r + is \in \mathbb{C} : r = 0$ and $a < s < b\,\}$ of the imaginary axis by $i(a, b)$, and we use the obvious analogues for closed and half-open intervals.

[31] The domain in that example was also denoted U, but we are now assuming definition (i) of this example.

By means of a second appeal to the chain-rule one obtains

$$\begin{aligned} h'(c) &= \tfrac{1}{\exp(ic)} \cdot i \cdot \exp(ic) \\ &= i \\ &= i \cdot \mathrm{id}'(c), \end{aligned}$$

where $\mathrm{id} : c \in \mathbb{C} \mapsto c \in \mathbb{C}$ is the identity (polynomial) function, and h from which one sees that the analytic function $i \cdot \mathrm{id}$ therefore differ by a constant. Since $c \in U \mapsto \ln(\exp(ic)) - ic$ is analytic on the connected set U it then follows from Corollary 2.20 that

$$\ln(\exp(ic)) - ic = c_0 \qquad \text{for some} \qquad c_0 \in \mathbb{C}.$$

Taking $c = 0$ and using (i) of Example 2.15(a) together with (v) of Example (a) gives $c_0 = 0$, and we conclude that

(v) $$\ln(\exp(ic)) = ic \qquad \text{for all} \qquad c \in U.$$

Since each complex number in S^1 can be written in the form[32] $\exp(ir)$ for some $r \in \mathbb{R}$ we see from (v) and (ii) that

(vi) $$\arctan := f|_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$$

is a real analytic function. This is the *real arctangent function.* By (iv) we have

(vii) $$\arctan'(r) = \frac{1}{r^2 + 1} \qquad \text{for all} \qquad r \in \mathbb{R},$$

and we have thereby solved the second problem discussed in the introduction, i.e. that of integrating the rational function $r \in \mathbb{R} \mapsto 1/(r^2 + 1)$.

We will require a few standard properties of the natural logarithm function $\ln : U^{\log} \to \mathbb{K}$.

[32]See Corollary 4.9 and the comments following that statement.

Proposition 5.7 :

(a) $\ln(\exp 2\pi i \cdot n) = 0$ *for any* $n \in \mathbb{Z}$*;*

(b) *Choose any* $n \in \mathbb{Z}$*. If* $\mathbb{K} = \mathbb{C}$ *let* $U_n \subset \mathbb{C}$ *denote the open horizontal strip*

$$U_n := \{\, a + ib \in \mathbb{C} \,:\, b \in ((4n-1)\cdot \tfrac{\pi}{2},\, (4n+1)\cdot \tfrac{\pi}{2})\,\};$$

if $\mathbb{K} = \mathbb{R}$ *let set* $U_n := (0, \infty)$*. Then for each* $n \in \mathbb{Z}$ *the restriction* $\exp|_{U_n}$ *is an analytic homeomorphism*[33] *between* U_n *and* $U^{\log}$*.*

(c) *Fix any* $n \in \mathbb{Z}$ *and let* $U_n \subset \mathbb{K}$ *be defined as in* (b)*. Then for* $\mathbb{K} = \mathbb{C}$ *one has*

(i) $$\ln \circ \exp|_{U_n} = \mathrm{id}|_{U_n} - 2\pi i \cdot n,$$

whereas for $\mathbb{K} = \mathbb{R}$ *one has*

(ii) $$\ln \circ \exp|_{U_n} = \mathrm{id}_{U_n} = \mathrm{id}_{(0,\infty)}.$$

(d) *for any* $k_1, k_2 \in U^{\log}$ *such that* $k_1 k_2 \in U^{\log}$ *also holds one has*

(i) $$\ln(k_1 k_2) = \ln k_1 + \ln k_2.$$

Proof :

(a) Use (ii) of Example 2.15(d) together with (xi) of Example 5.6(a).

(b) This is easily seen by examining the exponential function in terms of conformal mappings.

(c) From the Chain-Rule we see that the derivative of the function $h : k \in U_n \mapsto (\ln \circ \exp|_{U_n})(k) \in \mathbb{K}$ is given at each point k of the domain by

$$\ln'(\exp(k)) \cdot \exp'(k) = (1/\exp(k)) \cdot \exp(k) = 1,$$

which is the same as the derivative of the function $\mathrm{id}_{U_n} : k \mapsto k$. The identity (i) then follows from (a) and Corollary 4.7(c).

(d) Let $V \subset U^{\log}$ be a connected open set containing both k_2 and 1 and consider the analytic function $f : k \in V \mapsto \ln(kk_2) \in \mathbb{K}$. From the chain-rule one sees that f and $\ln|_V$ have the same derivative, and therefore differ by a constant. By choosing $k = 1$ one sees that the constant must be $\ln(k_2)$, and (d) follows by choosing $k_1 := k$.

q.e.d.

[33] In fact a conformal equivalence when $\mathbb{K} = \mathbb{C}$.

Proposition 5.8 : *Suppose* $U \subset \mathbb{C}$ *is a non-empty connected open set having non-empty intersection* $U_{\mathbb{R}}$ *with* $\mathbb{R}$ *and satisfying*

(i) $$\mathrm{cl}(U) \subset U^{\log}.$$

Then the following statements are equivalent:

(a) $\ln|_{U_{\mathbb{R}}} \in \mathcal{M}(U_{\mathbb{R}})$*; and*

(b) $U_{\mathbb{R}} \cap (-\infty, 0) = \emptyset$*.*

Proof : Condition (i) is simply to ensure that

(ii) $$\ln|_U \in \mathcal{M}(U).$$

(a) $\Rightarrow$ (b) : If (b) fails there is a non-empty open interval $V \subset U_{\mathbb{R}} \cap (-\infty, 0)$, and since (a) holds it must be the case that the analytic $\ln|_V$ is real-valued. However, by taking $c = \pi$ in (v) of Example 5.6(b) we see that

$$\ln(-1) = i\pi.$$

Moreover, from Proposition 5.7(d) we see that

(iii) $$\ln(-r) = \ln((-1) \cdot r) = \ln(r \cdot (-1)) = \ln r + \ln(-1) = \ln(r) + i\pi,$$

and this contradicts the earlier statement that $\ln|_V$ must be real-valued.

(b) $\Rightarrow$ (a) : $\ln|_{(0,\infty)}$ is real-valued by construction, and (a) therefore holds by (i) (and the definition of $\mathcal{M}(U_{\mathbb{R}})$).

q.e.d.

This result has important ramifications for the "alternate" logarithm function $\mathrm{lnabs} : r \in \mathbb{R}^\times \mapsto \ln|r| \in \mathbb{R}$ introduced in Example 5.6(a).

Corollary 5.9 : *Suppose* $U \subset \mathbb{C}$ *is any connected open set satisfying* $U_{\mathbb{R}} = \mathbb{R}^\times$*. Then the analytic function* $\mathrm{lnabs} : \mathbb{R}^\times \to \mathbb{R}$ *is not contained in the function field* $\mathcal{M}(U_{\mathbb{R}})$*.*

Since lnabs is the generally accepted logarithm function in elementary calculus courses, one now begins to see why that subject is so much easier to formulate algebraically by relocating in the complex domain.

Proof : If not, then for some such U there is a complex analytic function $f : U \to \mathbb{C}$ such that $f|_{\mathbb{R}^\times} = \text{lnabs}$, hence such that $f|_{(0,\infty)} = \ln|_{(0,\infty)}$. The function f thus agrees with ln on a set within U which contains a limit point in U, and therefore agrees with $\ln : U^{\log} \to \mathbb{C}$ on the intersection $U \cap U^{\log}$. But this intersection contains $\mathbb{R}^\times$, and $f|_{(-\infty,0)}$ is real-valued, whereas we have seen in (iii) of the proof of Proposition 5.8 that $\ln|_{(-\infty,0)}$ is not. This contraction establishes the result. **q.e.d.**

Part II - Topics from Differential Arithmetic

6. Differentiation from an Algebraic Perspective

Let R be a ring. A mapping $\delta : r \in R \to r' \in R$ is a *semiderivation* (of [or on] R) if

$$(r_1 r_2)' = r_1 r_2' + r_1' r_2 \qquad \text{for all} \qquad r_1, r_2 \in R. \tag{6.1}$$

This is the *Leibniz rule* or *product rule*. A semiderivation is a *derivation* if

$$(r_1 + r_2)' = r_1' + r_2' \qquad \text{for all} \qquad r_1, r_2 \in R \tag{6.2}$$

also holds. This is *additivity*, or the *additivity rule*.

A *(semi)differential ring* refers to a pair (R, δ) consisting of a ring R and a (semi)derivation $\delta : r \in R \mapsto r' \in R$. In practice explicit mention of δ is often suppressed: one refers to "the (semi)differential ring R with (semi)derivation $r \mapsto r'$," and to the value r' as the *(semi)derivative* of r. Since one reads r' as "are prime," one refers to the use of the symbolism $r \mapsto r'$ as "(indicating the associated [semi]derivation δ with, or using) prime notation."

A (semi)differential ring is (R, δ) is a *(semi)differential domain* when R is an integral domain, and a (semi)*differential field* when R is a field.

Examples 6.3 :

(a) Let $p \in \mathbb{Z}^+$ be a prime, choose any $r \in \mathbb{Z}$, and write r in the form $r = p^n m$, where $m \in \mathbb{Z}$ and $(p, m) = 1$. If we agree to take $n := m := 0$ when $r = 0$ the representation $r = p^n m$ is unique. The mapping $\delta_p : r \mapsto n p^{n-1} m$ is therefore well-defined, and is easily verified to be a semiderivation on $\mathbb{Z}$. In particular, $(\mathbb{Z}, \delta_p)$ is a semidifferential domain. δ_p will be called the *p-adic semiderivation (on $\mathbb{Z}$)*. (The terminology is not standard.) Example: for $p = 5$ and $r = -75$ we see from $-75 = 5^2 \cdot (-3)$ that $n = 2$ and $m = -3$, hence that $\delta_5(-75) = 2 \cdot 5 \cdot (-3) = -30$.

Of course the definition generalizes by replacing $\mathbb{Z}$ by any unique factorization domain[34] and p by any irreducible element of that UFD.

[34] The definition will be recalled in §13.

The mapping $\delta_p : \mathbb{Z} \to \mathbb{Z}$ is a fundamental example of a semiderivation which is not a derivation, e.g. from

$$1 = \delta_5 5 = \delta_5(2+3) \neq 0 = 0 + 0 = \delta_5 2 + \delta_5 3$$

we see that additivity condition (6.2) fails.

Note that

(i) $$\delta_p 0 = \delta_p 1 = \delta_p(-1) = 0.$$

Also note that

(ii) $$\delta_p(p^p) = p^p,$$

i.e., that when the semiderivation is understood to be[35] δ_p the integer p^p is a solution of the "semidifferential equation"

(iii) $$y' = y.$$

(b) Let A be a commutative ring and let $A[x]$ be the associated polynomial algebra in a single indeterminate x. Define $\delta : A[x] \to A[x]$ by

(i) $$\textstyle\sum_{j=0}^{n} a_j x^j \mapsto \sum_{j=0}^{n} j a_j x^{j-1}.$$

Then δ is a derivation on $A[x]$, as one can easily verify directly from definition (i). This is the *usual derivation*, often denoted $\frac{d}{dx}$.

At this point it is probably worth reminding readers[36] that we make a sharp distinction (including notationally) between a polynomial $p \in A[x]$ and the corresponding polynomial function $p(x) : a \in A \mapsto p(a) \in A$ which one encounters in elementary calculus (assuming $A = \mathbb{R}$). In the latter case one defines derivatives in terms of limits, but there is no such concept for more general $A[x]$, and for many purposes definition (i) is far more efficient.

(c) Let $U \subset \mathbb{C}$ be a non-empty connected open set and let $\mathcal{M}(U)$ be the field of meromorphic functions on U (see Theorem 3.2). Then the mapping $f \in \mathcal{M}(U) \mapsto \mathcal{M}(U)$ sending f to the derivative f' of f (as defined in the paragraph surrounding (4.2)) is a derivation on $\mathcal{M}(U)$ (by (a) and (b) of

[35] Prime notation seems to go perfectly with this example.

[36] See the first paragraph of §2.

Theorem 4.4), and $\mathcal{M}(U)$ is thereby endowed with the structure of a differential field. Moreover, this derivation restricts to a derivation on the the subfield $\mathcal{R}(U)$ of rational functions on U, and further restricts to a derivation on the ring $\mathcal{P}(U)$ of polynomial functions on U (again see Theorem 3.2), thereby endowing these two entities with the respective structures of a differential field and a differential ring. These derivations will be called the *standard derivations* on the respective entities. In all three cases these derivations are denoted $\frac{d}{dx}$, thereby introducing a conflict with the notation introduced in Example (b). So be it: the notation is too well-established to attempt a change. Hopefully our "usual derivation" (Example (b)) and "standard derivation" labels will serve to remind readers of the distinction.

(d) Let A be a commutative differential ring, choose any $n \in \mathbb{Z}^+$, and let $R = \mathrm{Mat}_n(A)$. Then a derivation on R is defined by

(i) $$M = [m_{ij}] \in R \mapsto M' := [m'_{ij}] \in R.$$

(e) For any ring R the mapping $r \in R \mapsto 0 \in R$ is a derivation. This is the *trivial derivation*; any other derivation is *non-trivial*.

When dealing with a specific (semi)derivative $\delta : r \mapsto r'$ on a ring R it often proves convenient to define the *second* and *third* (*semi*)*derivatives of* r by

$$r'' := (r')' \quad \text{and} \quad r''' := (r'')' \tag{6.4}$$

respectively. When even "higher" (semi)derivatives come under discussion alternate notation is generally employed: one defines

$$\begin{aligned} r^{(0)} &:= r, \\ r^{(1)} &:= r', \quad \text{and} \\ r^{(n+1)} &:= (r^{(n)})' \quad \text{when } n \geq 1 \text{ and } r^{(n)} \text{ has been defined.} \end{aligned} \tag{6.5}$$

$r^{(n)}$ is the n^{th}-(*semi*)*derivative of* r (*w.r.t.* δ). In particular, $r^{(2)} = r''$ and $r^{(3)} = r'''$.

Let (R, δ) be a (semi)differential ring and let $r, s \in R$.

- The element r is a δ-*constant*, or is (a) *constant* (w.r.t. the given [semi]derivation δ), if

$$r' = 0. \tag{6.6}$$

- The element s is a *δ-primitive* of r, or is a *primitive* of r (w.r.t. the given [semi]derivation δ), if

$$s' = r. \tag{6.7}$$

Primitives are also called *anti(semi)derivatives* or (*indefinite*) *integrals.*

To indicate that (6.7) holds one often writes

$$s = \int r\,. \tag{6.8}$$

One reads this as "s is *the* integral of r" despite the fact that primitives are in general not unique: "s is *an* integral of r" would be preferable.

Producing a primitive for r is referred to as (*semi*)*integrating* r, and methods for doing so are called *techniques of integration.*

Examples 6.9 : Prime notation is used in all three examples.

(a) Let $R := (\mathbb{Z}/5\mathbb{Z})[x]$ with the usual derivation. Then $p = x^5$ is a constant. Indeed, from[37] $[5] = [0]$ we see that $p' = [5]x^4 = [0]$.

(b) Assuming the 2-adic semiderivation on $\mathbb{Z}$, $\int 80 = 32$. When the 5-adic semiderivation is assumed $\int 80 = 200$.

(c) 8 and 5 have the same 3-adic semiderivative, i.e. 0, but their difference $8-5 = 3$ is not a constant w.r.t. this semiderivation. Thus *primitives of the same element need not differ by a constant*[38].

As has already been suggested in (iii) of Example 6.3(a), (semi)derivations allow for an algebraic formulation of ordinary differential equations. Here is a second illustration. If (R, δ) is a differential ring, and if the derivation δ is expressed with prime notation, then for any $r_1, r_2 \in R$ one would write

$$y'' + r_1 y' + r_2 y = 0 \tag{6.10}$$

[37] Normal people would write this sentence as: Indeed, from $5 \equiv 0 \pmod 5$ we see that $p' = 5x^4 = 0$. This classical notation definitely has merits, but uniform notation for equivalence classes seems preferable, since it suggests the generality of particular concepts and distinguishes between elements of a set and equivalence classes of such elements. For example, if one expresses the argument in the form $(x^5)' = 5x^4 = 0$, as many (including this author in weak moments) would be apt to do, the numeral 5 is seen, under pedantic examination, to represent two distinct entities: as an exponent it represents an integer, while as a coefficient it represents a coset in $\mathbb{Z}/5\mathbb{Z}$, i.e. the equivalence class of 5. Note that 0 also represents a coset.

[38] Why would anyone have any reason to suspect otherwise?

to indicate the search for *solutions*, i.e. elements $r \in R$ such that

$$\delta^2 r + r_1 \delta r + r_2 r = 0. \tag{6.11}$$

If such an r has been determined (none may exist), it would be referred to as "a solution of the (linear) (homogeneous) (ordinary) differential equation (6.10)." That particular differential equation would be described as "second-order" since the highest occurring (semi)derivative of y is two.

The search for solutions of (6.10) generalizes the search for primitives.

Proposition 6.12 : *Suppose R is a ring with semiderivation $r \mapsto r'$ and $a \in R^\times$. Then any primitive b of a is a solution of the second-order equation*

$$y'' - a'a^{-1}y' = 0. \tag{i}$$

The quantity $a'a^{-1}$ is called the *logarithmic (semi)derivative* of a (w.r.t. the given semiderivation). It will make additional appearances.

Proof : From $b' = a$ one has

$$b'' = a' = a'a^{-1} \cdot a = a'a^{-1}b',$$

i.e.

$$b'' - a'a^{-1}b' = 0,$$

and the result is thereby established. **q.e.d.**

7. p-Adic Semiderivations vs. p-Adic Valuations

Let R be a commutative ring. A function $\nu : R \setminus \{0\} \to \mathbb{Z}$ is a *valuation* (*on* R) if for all $r_1, r_2 \in R \setminus \{0\}$ one has

$$(7.1) \qquad \begin{cases} \text{(a)} & \nu(r_1 r_2) & = & \nu(r_1) + \nu(r_2), \\ \text{(b)} & \nu(r_1 + r_2) & \geq & \min\{\nu(r_1), \nu(r_2)\} \quad \text{if } r_2 \neq -r_1, \quad \text{and} \\ \text{(c)} & \nu(r) \neq 0 & & \text{for at least one } r \in R \setminus \{0\}. \end{cases}$$

Note that additivity, i.e. $\nu(r_1 + r_2) = \nu(r_1) + \nu(r_2)$, is not assumed. Indeed, it seldom holds in the important examples, but quite often condition (b) turns out to be a useful substitute.

Valuations are often defined only on fields, and frequently one adds ∞ to the range and extends the domain to the entire field by defining $\nu(0) = \infty$. Moreover, the codomain $\mathbb{Z}$ is often replaced by an ordered group. The definition above will suit our purposes.

As the following examples suggest, valuations offer a bridge between number theory and analysis.

Examples 7.2 :

(a) Let $p \in \mathbb{Z}^+$ be a prime, choose any $r \in \mathbb{Q}^\times$, and write r in the unique form $r = p^n s/t$, where $n, s, t \in \mathbb{Z}$, $t > 0$, and p, s, t are pairwise relatively prime. Then the mapping

$$\nu_p : r = p^n s/t \in \mathbb{Q}^\times \mapsto n \in \mathbb{Z}$$

is a valuation on $\mathbb{Q}$ known as the *p-adic valuation*. Example: From the factorization

$$\frac{1331}{1911} = \frac{11^3}{3 \cdot 7^2 \cdot 13}$$

one sees that for $r := 1331/1911$ one has $\nu_3(r) = -1$, $\nu_7(r) = -2$, $\nu_{11}(r) = 3$, $\nu_{13}(r) = -1$, and $\nu_p(r) = 0$ for all other primes p.

Of course one can generalize this definition to arbitrary unique factorization domains.

(b) For any prime p the associated p-adic valuation on $\mathbb{Q}$ restricted to $\mathbb{Z} \setminus \{0\}$ defines a valuation on $\mathbb{Z}$. This is the *p-adic valuation on* $\mathbb{Z}$, and is also denoted ν_p. Examples: $\nu_3(75) = \nu_3(-75) = 1$; and $\nu_p(p) = 1$ for all primes p.

(c) Let $U \subset \mathbb{C}$ be a non-empty connected open set and let $K := \mathcal{M}(U)$ be the field of meromorphic functions on U. Fix any point $c \in U$ and for any $f \in K^\times$ consider the Laurent series expansion

$$c_n(x-c)^n + c_{n+1}(x-c)^{n+1} + \cdots$$

of f at c, wherein $n \in \mathbb{Z}$ and $c_n \neq 0$. Then the mapping

$$\mathrm{ord}_c(f) : f \in K^\times \mapsto n \in \mathbb{Z}$$

is a valuation on K. The integer $\mathrm{ord}_c(f)$ is called the *order* of f at c. The function f is said to have:

- a *pole of order* $-\mathrm{ord}_c(f)$ *at* c if $\mathrm{ord}_c(f) < 0$;
- a *zero or order* $\mathrm{ord}_c(f)$ *at* c, or simply to have (or to be of) *order* $\mathrm{ord}_c(f)$ *at* c, *if* $\mathrm{ord}_c(f) > 0$;
- *order zero at* c if $\mathrm{ord}_c(f) = 0$.

In the case of rational functions on $\mathbb{C}$ these orders can be computed in terms of irreducible factorizations in complete analogy with what was seen in Example (a). To illustrate let f be the meromorphic function on $\mathbb{C}$ defined by the polynomial quotient

$$f(x) = \frac{(x+2i)^3}{(x+1)\cdot(x-i)^2\cdot(x+(4-5i))}.$$

One sees directly from the displayed factorization into irreducibles that f has a zero of order 3 at $-2i$ and poles of respective orders 1, 2 and 1 at -1, i and $-4+5i$, hence that $\mathrm{ord}_{-2i}(f) = 3$, $\mathrm{ord}_{-1}(f) = 1$, $\mathrm{ord}_i(f) = -2$, $\mathrm{ord}_{-4+5i}(f) = -1$, and $\mathrm{ord}_c(f) = 0$ at all other points $c \in \mathbb{C}$. Much more work is involved when these orders are calculated using the corresponding Laurent series definition of the order, e.g. the Laurent series of f at i is

$$\frac{-27i/8}{(x-i)^2} + \frac{-(135/64)\cdot(1-i)}{x-i} + \frac{1}{256}\cdot(135-144i) + \frac{1}{2048}\cdot(553+585i)\cdot(x-i) + \cdots,$$

from which we again see, but with far more effort[39], that $\mathrm{ord}_i(f) = -2$.

[39] Of course the effort was making sure my computer entries were correct.

Let R be a commutative ring and let $r_1, r_2 \in R$. We say that r_1 *divides* r_2, or that r_1 is a *factor* of r_2, if there is an element $r_3 \in R$ such that $r_2 = r_1 r_3$. To indicate this is the case one writes[40] $r_1 | r_2$, and to indicate it is not the case one writes[41] $r_1 \nmid r_2$. Note from the choices $r_2 := r_3 := 0$ that $r_1 | 0$. When $r_1 | r_2$ (*resp.* $r_1 \nmid r_2$) and R is a subring of a ring S we write $r_1 | r_2$ in R (*resp.* $r_1 \nmid r_2$ in R) if confusion might otherwise result. For example, $3 \nmid 5$ in $R = \mathbb{Z}$, whereas $3 | 5$ in $S = \mathbb{Q}$ (since $5 = 3 \cdot \frac{5}{3}$).

For our limited purposes one of the most important properties of p-adic valuations is the following.

Proposition 7.3 : *Suppose* $p, r \in \mathbb{Z} \setminus \{0\}$ *and* p *is a prime. Then*

$$p | r \qquad \Leftrightarrow \qquad \nu_p(r) \neq 0 \qquad \Leftrightarrow \qquad \nu_p(r) > 0.$$

Proof : For $r \in \mathbb{Z} \setminus \{0\}$ the definition of $\delta_p(r)$ given in Example 7.2(a) reduces to $\delta_p(r) = np^{n-1}s$ when $n \in \mathbb{Z}$, $s \in \mathbb{Z} \setminus \{0\}$ and $(p, s) = 1$. The result follows. **q.e.d.**

Proposition 7.4 : *Any valuation* $\nu : R^\times \to \mathbb{Z}$ *defined on a commutative ring* R *has the following properties for all* $r, u, r_1, r_2 \in R^\times$*:*

(a) $\nu(1) = 0$*;*

(b) $\nu(-1) = 0$*;*

(c) $\nu(-r) = \nu(r)$*;*

(d) $\nu(r^n) = n\nu(r)$ *for any* $n \in \mathbb{N}$*;*

(e) $\nu(u^{-1}) = -\nu(u)$ *when* u *is a unit; and*

(f) $\nu(r_1 + r_2) = \min\{\nu(r_1), \nu(r_2)\}$ *if* $\nu(r_1) \neq \nu(r_2)$.

Note from (c) that the qualification $r_2 \neq -r_1$ in (f) would be redundant.

Proof :

(a) From (7.1a) we have $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$. Since $\nu(1) \in \mathbb{Z}$, (a) follows.

(b) $0 = \nu(1) = \nu((-1)^2) = \nu((-1) \cdot (-1)) = \nu(-1) + \nu(-1) = 2 \cdot \nu(-1)$.

(c) From (b) we have $\nu(-r) = \nu((-1) \cdot r) = \nu(-1) + \nu(r) =) + \nu(r) = \nu(r)$.

[40] Read $r_1 | r_2$ as "r_1 divides r_2."

[41] Read $r_1 \nmid r_2$ as "r_1 does not divide r_2."

(d) For $n = 1$ this is immediate from (a); for $n > 1$ use (7.1a) and induction.

(e) From (a) we have $0 = \nu(1) = \nu(u^{-1} \cdot u) = \nu(u^{-1}) + \nu(u)$.

(f) W.l.o.g assume $\nu(r_1) < \nu(r_2)$. Note from (c) that $r_1 + r_2 \neq 0$ must then hold, and $\nu(r_1 + r_2)$ is therefore defined. We then have

$$\begin{aligned}
\nu(r_1) &= \nu((r_1 + r_2) - r_2) \\
&\geq \min\{\nu(r_1 + r_2), \nu(-r_2)\} \\
&= \min\{\nu(r_1 + r_2), \nu(r_2)\} \text{ (by (c))} \\
&= \nu(r_1 + r_2) \text{ (otherwise } \nu(r_1) \geq \nu(r_2)) \\
&\geq \min\{\nu(r_1), \nu(r_2)\} \\
&= \nu(r_1),
\end{aligned}$$

and $\nu(r_1 + r_2) = \min\{\nu(r_1), \nu(r_2)\}$ follows.

q.e.d.

Valuations are used in number theory to simplify and/or generalize arguments which depend on unique factorization. Here are two very elementary examples.

Proposition 7.5 : *No prime $p \in \mathbb{Z}^+$ admits an n^{th}-root in $\mathbb{Q}$ for any $1 < n \in \mathbb{Z}^+$.*

Proof : Suppose, to the contrary, that $1 < n \in \mathbb{Z}$ and $r \in \mathbb{Q}$ satisfy $p = r^n$. Applying the p-adic valuation ν_p and using Proposition 7.4(d) then gives

$$1 = \nu_p(p) = \nu_p(r^n) = n\nu_p(r).$$

We conclude that $\nu_p(r) = \frac{1}{n} \notin \mathbb{Z}$, thereby contradicting the fact that ν_p is integer valued. **q.e.d.**

Proposition 7.6 : *Suppose $p, m, n \in \mathbb{Z}$ and p is a prime. Then:*

(a) *$p|m$ and $p|n$ imply $p|(m + n)$;*

(b) *$p|m$ and $p|(m + n)$ imply $p|n$; and*

(c) *$p|m$ implies $p \not| (m \pm 1)$.*

Proof :

(a) Immediate from (7.1b) and Proposition 7.3.

(b) Replacing m and n in (a) by $-m$ and $n + m$ we see that $p|(-m)$ and $p|(m + n)$ imply $p|n$. Since $p|(-m)$ if and only if $p|m$ obviously holds, (b) follows.

(c) Otherwise choosing $n := \pm 1$ in (b) would result in the contradiction $p| \pm 1$.

q.e.d.

As we now show[42], p-adic valuations and p-adic semiderivations are very closely related.

Suppose $p \in \mathbb{Z}^+$ is a prime, $r \in \mathbb{Z} \setminus \{0\}$, and $r = p^n m$, where $n \in \mathbb{Z}^+$ and $(p, m) = 1$. Then by definition we have

$$\nu_p(r) = n \qquad \text{and} \qquad \delta_p(r) = np^{n-1}m = n \cdot \frac{p^n m}{p} = \nu_p(r) \cdot \frac{r}{p}, \tag{7.7}$$

thereby establishing the identity

$$\frac{\nu_p(r)}{p} = \frac{\delta_p(r)}{r} \qquad \text{for all} \qquad r \in \mathbb{Z} \setminus \{0\}. \tag{7.8}$$

Notice that the numerator and denominator on the left-hand side are both non-negative, whereas the best one can say on the right is that both must have the same sign when the numerator is non-zero. In particular,

$$\left| \frac{\delta_p(r)}{r} \right| = \frac{\delta_p(r)}{r} = \frac{\nu_p(r)}{p} \qquad \text{for all} \qquad r \in \mathbb{Z} \setminus \{0\}. \tag{7.9}$$

It is evident from either (of the relations) and (7.9) that we can add one more equivalence to the display seen in Proposition 7.3.

Proposition 7.10 : *Suppose $p, r \in \mathbb{Z} \setminus \{0\}$ and p is a prime. Then*

$$p|r \qquad \Leftrightarrow \qquad \nu_p(r) \neq 0 \qquad \Leftrightarrow \qquad \nu_p(r) > 0 \qquad \Leftrightarrow \qquad \delta_p(r) \neq 0.$$

We can also use identities (7.9) to produce a substitute for the lack of additivity of p-adic semiderivations.

Proposition 7.11 : *Suppose $r_1, r_2 \in \mathbb{Z} \setminus \{0\}$ and $p \in \mathbb{Z}^+$ is a prime. Then*

(i) $$\left|\delta_p(r_1 + r_2)\right| \geq |r_1 + r_2| \cdot \min\left\{ \frac{\delta_p(r_1)}{r_1}, \frac{\delta_p(r_2)}{r_2} \right\},$$

with equality if $\dfrac{\delta_p(r_1)}{r_1} \neq \dfrac{\delta_p(r_2)}{r_2}$.

[42] As if it were not already obvious.

Proof : The result is obvious if $r_1 + r_2 = 0$, so assume this is not the case. Then from (7.9 and (7.1b) we have

$$\begin{aligned} \left|\frac{\delta_p(r_1+r_2)}{r_1+r_2}\right| &= \frac{\nu_p(r_1+r_2)}{p} \\ &\geq \frac{\min\{\nu_p(r_1),\, \nu_p(r_2)\}}{p} \\ &= \min\left\{\frac{\nu_p(r_1)}{p},\, \frac{\nu_p(r_2)}{p}\right\} \\ &= \min\left\{\frac{\delta_p(r_1)}{r_1},\, \frac{\delta_p(r_2)}{r_2}\right\}, \end{aligned}$$

and the result then follows from Proposition 7.4(f). **q.e.d.**

One sees from Proposition 7.10 that the following result can be viewed as a reformulation of Proposition 7.6(a).

Corollary 7.12 :

(a) $r_1 + r_2 \neq 0$ *and* $\delta_p(r_1) \neq 0 \neq \delta_p(r_2)$ *imply* $\delta_p(r_1 + r_2) \neq 0$*;*

(b) $\delta_p(r_1) \neq 0$ *and* $\delta_p(r_1 + r_2) \neq 0$ *imply* $\delta_p(r_2) \neq 0$*; and*

(c) *for any* $r \in \mathbb{Z}$ *satisfying* $\delta_p(r) \neq 0$ *one has* $\delta_p(r \pm 1) = 0$.

Proof :

(a) Immediate from (i) of Proposition 7.11.

(b) If $\delta_p(r_2) = 0$ then $\delta_p(r_1 + r_2) = 0$ by the final assertion of Proposition 7.11.

(c) By (i) of Example 6.3(a) we have $\delta_p(\pm 1) = 0$; the result is therefore a special case of (b).

q.e.d.

8. The Infinitude of Primes

This section represents a brief and hopefully somewhat amusing interlude from our technical presentation: we reformulate Euclid's proof of the infinitude of primes in terms of p-adic semiderivations.

Theorem 8.1 : *There are infinitely many primes in* $\mathbb{Z}$.

Proof : Suppose, to the contrary, that there are only k primes for some $k \in \mathbb{Z}^+$. Since 2 is prime we must have $k \geq 2$. Let $q \in \mathbb{Z}^+$ denote the product of the primes, consider the integer $m := q^2 - 1 \geq 3$, and let p be a prime divisor of m. Note from the definition of q and Proposition 7.10 that

$$\text{(i)} \qquad \delta_p(q) \neq 0.$$

We then have, using prime notation[43] for δ_p:

$$\begin{array}{rcll} 0 & \neq & m' & \text{(by Proposition 7.10)} \\ & = & (q^2-1)' & \\ & = & ((q-1)(q+1))' & \\ & = & (q-1)(q+1)' + (q-1)'(q+1) & \text{(by the Leibniz rule (6.1))} \\ & = & (q-1)\cdot 0 + 0\cdot(q+1) & \text{(by (i), Proposition 7.10, and} \\ & & & \quad \text{Corollary 7.12(c))} \\ & = & 0, & \end{array}$$

and we have thereby achieved a contradiction. **q.e.d.**

In our notation Euclid used $m := q$ rather than $m := q^2 - 1$ to achieve the same result: we required a product form for m so as to be able to invoke the Leibniz rule. Dyed-in-the-wool number theorists will note that one could replace $m := q^2 - 1 = (q-1)(q+1)$ in this argument by

$$\text{(8.2)} \qquad m := q^n - 1 = (q-1)(1 + q + q^2 + \cdots + q^{n-1}) \qquad \text{for any} \qquad 2 < n \in \mathbb{Z},$$

thereby dragging cyclotomic polynomials into the act. Precisely why one would want to do so is not clear[44], but inserting the comment at least adds a bit of padding to a strikingly thin section.

[43] Who could ask for anything more appropriate?

[44] I would be happy to have clarification.

9. Elementary Properties of Semiderivations and Derivations

In this section R *is a ring and* $\delta : r \in R \mapsto r' \in R$ *is a semiderivation.*

The collection of constants of R is denoted[45] R_C. Example: when $p \in \mathbb{Z}^+$ is a prime and $\delta_p : \mathbb{Z} \to \mathbb{Z}$ is the p-adic semiderivation on sees from Proposition 7.10 that the constants are those integers not divisible by p, i.e. that R_C is the complement of the prime ideal $(p) \subset \mathbb{R}$ generated by p.

Proposition 9.1 :

(a) $0 = 0_R$ *is constant.*

(b) $1 = 1_R$ *is constant.*

(c) *When* $c, r \in R$ *and* c *is constant one has*

(i) $$(c \cdot r)' = c \cdot r'.$$

(d) *The set* R_C *is multiplicative, i.e. the product of any two constants is a constant.*

(e) **(The Reciprocal Rule)** *For any unit* $u \in R$ *one has*

(i) $$(u^{-1})' = -u^{-1}u'u^{-1}.$$

In particular, when R *is commutative one has*

(ii) $$(u^{-1})' = -u'u^{-2}.$$

(f) *The set* $R_C \cap R^\times$ *is closed under inversion, i.e. if* $u \in R_C$ *is a unit then* $u^{-1} \in R_C$.

(g) **(The Power Rule)** *Suppose* $r \in R$ *is an element which commutes with* r', *e.g. suppose* R *is commutative. Then for any positive integer* n *one has*

(i) $$(r^n)' = nr^{n-1}r'.$$

Moreover, if r *is a unit then* (i) *holds for all* $n \in \mathbb{Z}$.

[45] The standard notation for this collection is R^δ.

(h) **(The Quotient Rule)** *Suppose* $r, s \in R$ *and* s *is a unit. Then*

(i) $$(rs^{-1})' = -rs^{-1}s's^{-1} + r's^{-1}.$$

In particular, when R *is commutative one has*

(ii) $$(rs^{-1})' = (sr' - s'r)s^{-2}.$$

Proof :

(a) and (b): For $r = 0$ and $r = 1$ we have

$$\delta r = \delta(r \cdot r) = r \cdot \delta r + \delta r \cdot r.$$

When $r = 0$ this gives

$$\delta 0 = 0 \cdot \delta 0 + \delta 0 \cdot 0 = 0 + 0 = 0,$$

thereby establishing (a), and when $r = 1$ it gives

$$\delta 1 = \delta 1 + \delta 1,$$

thereby establishing (b).

(c) Immediate from the Leibniz rule (6.1). Indeed, from that result we have

$$(c \cdot r)' = c \cdot r' + c' \cdot r = c \cdot r' + 0 \cdot r = c \cdot r' + 0 = c \cdot r'.$$

(d) This is also an immediate consequence of the Leibniz rule (6.1).

(e) By (b) and the Leibniz rule we have

$$0 = \delta 1 = \delta(uu^{-1}) = u \cdot (u^{-1})' + u' \cdot u^{-1},$$

and (e) follows.

(f) Immediate from (e) and (d).

(g) For $n = 1$ the result is obvious. If $n \geq 1$ and the result holds for n then from the Leibniz rule we have

$$\begin{aligned}
(r^{n+1})' &= (rr^n)' \\
&= r(r^n)' + r'r^n \\
&= rnr^{n-1}r' + r'r^n \\
&= nr^n r' + r^n r' \qquad \text{(because } nr = rn \text{ and } r'r = rr'\text{)} \\
&= (n+1)r^n r'.
\end{aligned}$$

If r is a unit then r^{-1} and r' commute. Using (i) of (e), with u replaced by r^n (and $n \geq 1$), we see from the work thus far that

$$\begin{aligned}(r^{-n})' &= ((r^n)^{-1})' \\ &= -(r^n)^{-1}((r^n)^{-1})'(r^n)^{-1} \\ &= -r^{-n}(r^n)'r^{-n} \\ &= -r^{-n} \cdot nr^{n-1}r' \cdot r^{-n} \\ &= -nr^{-n-1}r',\end{aligned}$$

and (g) is thereby established.

(h) One has

$$\begin{aligned}(rs^{-1})' &= r(s^{-1})' + r's^{-1} \\ &= r \cdot (-s^{-1}s's^{-1}) + r's^{-1} \quad \text{(by (i) of (e))} \\ &= -rs^{-1}s's^{-1} + r's^{-1},\end{aligned}$$

and the result is thereby established.

q.e.d.

One can say far more about the structure of R_C when $\delta : R \to R$ is a derivation.

Recall that a homomorphism $\mathbb{Z} \to R$ is defined by

$$n \in \mathbb{Z} \mapsto \begin{cases} \sum_{j=1}^{n} 1_R & \text{if } n > 0, \\ 0_R & \text{if } n = 0, \text{ and} \\ \sum_{j=1}^{|n|}(-1_R) & \text{if } n < 0, \end{cases} \tag{9.2}$$

which is generally abbreviated by writing only[46]

$$n \in \mathbb{Z} \mapsto 1 + 1 + \cdots + 1 \in R \qquad (n \text{ occurrences of } 1 = 1_R). \tag{9.3}$$

The image of this homomorphism is called the[47] *prime ring* of R. It is standard practice to write the image in R of an integer $n \in \mathbb{Z}$ under the homomorphism (9.2) as n, and we will adopt this practice. For example, when dealing with the factor ring

[46] $n \in \mathbb{Z}^+$ would make a bit more sense.

[47] When R is a field "prime field" is standard terminology; "prime ring" is not standard terminology, but proves convenient.

$\mathbb{Z}/4\mathbb{Z}$ we might write down equalities such as[48] $6 \cdot [3] = [2]$, wherein the brackets indicate cosets. Note that for all $n \in \mathbb{Z}^+$ and all $r \in R$ one has

$$nr = (1 + 1 + \cdots + 1)r = r + r + \cdots + r = r(1 + 1 + \cdots + 1) = rn, \tag{9.4}$$

and one can easily see that the same holds when $n \leq 0$. The following result is an immediate consequence.

Proposition 9.5 : *Every ring is a $\mathbb{Z}$-algebra.*

Proposition 9.6 : *When $\delta : R \to R$ is a derivation the collection R_C of constants is a subring containing the prime ring, and is a subfield when R is a field.*

One refers to R_C as the *ring of constants* (*of* R), or as the *field of constants* (*of* R) when R is a field.

Proof : We have seen in Proposition 9.1(a) and (b) that R_C contains 0 and 1, and in (d) of the same proposition that it is closed under multiplication. From the additive property (see (6.2)) of derivations it is also seen to be closed under addition, and is therefore a subring of R. It is then evident from (9.2) that this subring contains the prime ring.

The field assertion is a consequence of Proposition 9.1(f). **q.e.d.**

The Leibniz rule for semiderivations generalizes as follows.

Proposition 9.7 ; *Suppose $2 \leq n \in \mathbb{Z}$ and $r_1, r_2, \ldots, r_n \in R$. Then*

$$\text{(i)} \qquad (\textstyle\prod_{j=1}^n r_j)' = \sum_{j=1}^n r_1 \cdots r_{j-1} \cdot r_j' \cdot r_{j+1} \cdots r_n.$$

Proof : We use induction on $n \geq 2$. When $n = 2$ the formula reduces to (6.1). If the formula holds for $n \geq 2$ then for $r_1, r_2, \ldots, r_{n+1} \in R$ we have

$$\begin{aligned}
(\textstyle\prod_{j=1}^{n+1} r_j)' &= ((\textstyle\prod_{j=1}^n r_j) \cdot r_{n+1})' \\
&= (\textstyle\prod_{j=1}^n r_j) \cdot r_{n+1}' + (\textstyle\prod_{j=1}^n r_j)' \cdot r_{n+1} \\
&= (\textstyle\prod_{j=1}^n r_j) \cdot r_{n+1}' + (\sum_{j=1}^n r_1 \cdots r_{j-1} \cdot r_j' \cdot r_{j+1} \cdots r_n) \cdot r_{n+1} \\
&= \textstyle\sum_{j=1}^{n+1} r_1 \cdots r_{j-1} \cdot r_j' \cdot r_{j+1} \cdots r_{n+1},
\end{aligned}$$

[48] Indeed, this particular equality would more likely be expressed as $6 \cdot 3 \equiv 2 \pmod 4$, even though $6 \in \mathbb{Z}$, whereas 3 and 2 are regarded as elements of $\mathbb{Z}/4\mathbb{Z}$.

and the result follows. **q.e.d.**

In the case of derivations there is an alternate generalization of the Leibniz rule which goes by the same name. In the statement $\left(\begin{array}{c} n \\ j \end{array} \right)$ denotes the usual combinatorial coefficient, i.e.

$$\left(\begin{array}{c} n \\ j \end{array} \right) := \frac{n!}{j!(n-j)!}, \qquad \text{where} \qquad 0 \leq j \leq n \in \mathbb{Z}, \tag{9.8}$$

and where $0! := 1$. In particular,

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1 \qquad \text{for all} \qquad 0 \leq n \in \mathbb{Z}. \tag{9.9}$$

We will make use of the easily established *Pascal triangle* (*identity*)

$$\left(\begin{array}{c} n \\ j \end{array} \right) + \left(\begin{array}{c} n \\ j-1 \end{array} \right) = \left(\begin{array}{c} n+1 \\ j \end{array} \right) \qquad \text{for all integers} \qquad 1 < j \leq n. \tag{9.10}$$

Using (9.9) and induction on n it follows easily from (9.10) that

$$\left(\begin{array}{c} n \\ j \end{array} \right) \in \mathbb{Z} \qquad \text{for all integers} \qquad 0 \leq j \leq n. \tag{9.11}$$

Proposition 9.12 (The Generalized Leibniz Rule) : *Suppose* $\delta : R \to R$ *is a derivation. Then for any* $n \in \mathbb{Z}^+$ *and any* $r, s \in R$ *one has*

$$\text{(i)} \qquad (rs)^{(n)} = \textstyle\sum_{j=1}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) r^{(j)} s^{(n-j)}.$$

In the statement and proof we are viewing R as a $\mathbb{Z}$-algebra and regarding binomial coefficients as elements of R. (See Proposition 9.5 and the discussion surrounding (9.2).)

Note that R is not assumed commutative.

Proof : By induction.

For $n = 1$ formula (i) is the Leibniz rule (6.1).

Now suppose $n \geq 1$ and the formula holds for n. Then

$$\begin{aligned}
(rs)^{(n+1)} &= \left(\sum_{j=0}^{n} \binom{n}{j} r^{(j)} s^{(n-j)}\right)' \\
&= \sum_{j=0}^{n} \left(\binom{n}{j} r^{(j)} s^{(n-j)}\right)' \quad \text{(by additivity, i.e. (6.2))} \\
&= \sum_{j=0}^{n} \binom{n}{j} \left(r^{(j)} s^{(n-j)}\right)' \quad \text{(by } \binom{n}{j} \in R_C, \text{ Propositions 9.6, and Proposition 9.1(c)).}
\end{aligned}$$

The Leibniz rule (6.1), (9.9) and (9.10) now give

$$\begin{aligned}
(rs)^{(n+1)} &= \sum_{j=0}^{n} \binom{n}{j} \left(r^{(j)} s^{(n-j)}\right)' \\
&= \sum_{j=0}^{n} \binom{n}{j} \left(r^{(j)} \left(s^{(n-j)}\right)' + \left(r^{(j)}\right)' s^{(n-j)}\right) \\
&= \sum_{j=0}^{n} \binom{n}{j} r^{(j)} \left(s^{(n-j)}\right)' + \sum_{j=0}^{n} \binom{n}{j} \left(r^{(j)}\right)' s^{(n-j)}\right) \\
&= \sum_{j=0}^{n} \binom{n}{j} r^{(j)} \left(s^{(n+1-j)}\right) + \sum_{j=0}^{n} \binom{n}{j} \left(r^{(j+1)}\right) s^{(n-j)}\right) \\
&= \sum_{j=0}^{n} \binom{n}{j} r^{(j)} \left(s^{(n+1-j)}\right) + \sum_{j=1}^{n+1} \binom{n}{j-1} \left(r^{(j)}\right) s^{n-(j-1)} \\
&= \sum_{j=0}^{n} \binom{n}{j} r^{(j)} \left(s^{(n+1-j)}\right) + \sum_{j=1}^{n+1} \binom{n}{j-1} \left(r^{(j)}\right) s^{n+1-j} \\
&= rs^{(n+1)} + \sum_{j=1}^{n} \left(\binom{n}{j} + \binom{n}{j-1}\right) r^{(j)} s^{(n+1-j)} + r^{(n+1)} s \\
&= rs^{(n+1)} + \sum_{j=1}^{n} \binom{n+1}{j} r^{(j)} s^{(n+1-j)} + r^{(n+1)} s \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} r^{(j)} s^{(n+1-j)},
\end{aligned}$$

and (i) follows. **q.e.d.**

Proposition 9.13 :

(a) *Any finite sum of (semi)derivations on R is a (semi)derivation on R.*

(b) *Suppose R is commutative and $t \in R$. Then $t\delta : r \in R \mapsto t \cdot \delta r \in R$ is a semiderivation on R, and is a derivation when δ has this property.*

(c) *The commutator*

(i) $$[\delta_1, \delta_2] := \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$$

of derivations δ_1, δ_2 on R is again a derivation.

The value of the commutator can be regarded as a measure of non-commutativity. Indeed: *δ_1 and δ_2 commute, i.e. $\delta_1 \circ \delta_2 = \delta_2 \circ \delta_1$, if and only if $[\delta_1, \delta_2] = 0$.*

Proof :

(a) It suffices, by induction, to prove that the sum of two (semi)derivations is a (semi)derivation. To this end suppose δ_1, δ_2 are semiderivations on R and $r, s \in R$. Then

$$\begin{aligned}(\delta_1 + \delta_2)(rs) &= \delta_1(rs) + \delta_2(rs) \\ &= r \cdot \delta_1 s + \delta_1 r \cdot s + r \cdot \delta_2 s + \delta_2 r \cdot s \\ &= r \cdot (\delta_1 s + \delta_2 s) + (\delta_1 r + \delta_2 r) \cdot s \\ &= r \cdot (\delta_1 + \delta_2)s + (\delta_1 + \delta_2)r \cdot s,\end{aligned}$$

thereby establishing the Leibniz rule.

If δ_1 and δ_2 are also additive, i.e. derivations, then from

$$\begin{aligned}(\delta_1 + \delta_2)(r + s) &= \delta_1(r + s) + \delta_2(r + s) \\ &= \delta_1 r + \delta_1 s + \delta_2 r + \delta_2 s \\ &= \delta_1 r + \delta_2 r + \delta_1 s + \delta_2 s \\ &= (\delta_1 + \delta_2)r + (\delta_1 + \delta_2)s\end{aligned}$$

we see that $\delta_1 + \delta_2$ is also a derivation.

(b) For $r, s \in R$ we have

$$\begin{aligned}t\delta(rs) &:= t \cdot \delta(rs) \\ &= t \cdot (r \cdot \delta s + \delta r \cdot s) \\ &= r \cdot t \cdot \delta s + t \cdot \delta r \cdot s \\ &= r \cdot (t\delta)s + (t\delta)r \cdot s\end{aligned}$$

and the semiderivation property is thereby established. If δ is also additive, hence a derivation, then from

$$\begin{aligned} t\delta(r+s) &:= t\cdot\delta(r+s) \\ &= t\cdot(\delta r+\delta s) \\ &= t\cdot\delta r + t\cdot\delta s \\ &= t\delta(r)+t\delta(s) \end{aligned}$$

we see that $t\delta$ is also a derivation.

(c) For any $r, s \in R$ we have

$$\begin{aligned} (\delta_1\circ\delta_2)(r+s) &= \delta_1(\delta_2(r+s)) \\ &= \delta_1(\delta_2 r+\delta_2 s) \qquad \text{(because } \delta_2 \text{ is additive)} \\ &= \delta_1(\delta_2 r)+\delta_1(\delta_2 s)) \quad \text{(because } \delta_1 \text{ is additive)} \end{aligned}$$

and as a result we see that

(ii) $$(\delta_1\circ\delta_2)(r+s) = (\delta_1\circ\delta_2)r + (\delta_1\circ\delta_2)s.$$

Permuting the indices in this last argument gives

(iii) $$(\delta_2\circ\delta_1)(r+s) = (\delta_2\circ\delta_1)r + (\delta_2\circ\delta_1)s,$$

whereupon subtracting (iii) from (ii) yields the required additivity property

$$[\delta_1,\delta_2](r+s) = [\delta_1,\delta_2]r + [\delta_1,\delta_2]s.$$

Turning to the Leibniz rule, note that for any $r, s \in R$ we also have

$$\begin{aligned} (\delta_1\circ\delta_2)(rs) &= \delta_1(\delta_2(rs)) \\ &= \delta_1(r\cdot\delta_2 s+\delta_2 r\cdot s) \\ &= \delta_1(r\cdot\delta_2 s)+\delta_1(\delta_2 r\cdot s) \quad \text{(because } \delta_1 \text{ is additive)} \\ &= r\cdot(\delta_1(\delta_2 s))+\delta_1 r\cdot\delta_2 s+\delta_2 r\cdot\delta_1 s+\delta_1(\delta_2 r)\cdot s, \end{aligned}$$

which is more conveniently expressed as

(iv) $$(\delta_1\circ\delta_2)(rs) = r\cdot(\delta_1\circ\delta_2)s+\delta_1 r\cdot\delta_2 s+\delta_2 r\cdot\delta_1 s+(\delta_1\circ\delta_2)r\cdot s,$$

and by permuting the indices in this last calculation we simultaneously conclude that

(v) $$(\delta_2\circ\delta_1)(rs) = r\cdot(\delta_2\circ\delta_1)s+\delta_2 r\cdot\delta_1 s+\delta_1 r\cdot\delta_2 s+(\delta_2\circ\delta_1)r\cdot s.$$

Subtracting (v) from (iv) gives

$$\begin{aligned}[\delta_1,\delta_2](rs) &= r\cdot(\delta_1\circ\delta_2)s - r\cdot(\delta_2\circ\delta_1)s + (\delta_1\circ\delta_2)r\cdot s - (\delta_2\circ\delta_1)r\cdot s \\ &= r\cdot(\delta_1\circ\delta_2-\delta_2\circ\delta_1)s + (\delta_1\circ\delta_2-\delta_2\circ\delta_1)r\cdot s \\ &= r\cdot[\delta_1,\delta_2]s + [\delta_1,\delta_2]r\cdot s,\end{aligned}$$

and the Leibniz rule is thereby established.

q.e.d.

When R is commutative we denote the collection of derivations on R by $\mathrm{Der}(R)$. The following result then becomes an immediate consequence of Proposition 9.13. The final assertion can be ignored by readers unfamiliar with Lie algebras, since it will not be used in the sequel.

Corollary 9.14 : *Suppose R is a commutative ring. Then $\mathrm{Der}(R)$ is a left R-module, and is endowed with the structure of an R-Lie algebra when the bracket is understood to be the commutator.*

Examples 9.15 : Let $\frac{d}{dx} : r \mapsto r'$ be the usual derivation on the polynomial algebra $\mathbb{R}[x]$ (as defined in Example 6.3(a)), and let $p, q \in \mathbb{R}[x]$ be arbitrary. Then $p\frac{d}{dx}$ and $q\frac{d}{dx}$ are derivations on $\mathbb{R}[x]$ by Proposition 9.13(b).

We claim that

(i) $$[p\tfrac{d}{dx}, q\tfrac{d}{dx}] = W(p,q)\tfrac{d}{dx},$$

where

(ii) $$W(p,q) := \det\left(\begin{bmatrix} p & q \\ p' & q' \end{bmatrix}\right) = pq' - p'q$$

is the so-called "Wronskian" of p and q (which may or may not be) familiar from ordinary differential equations. In particular, *$p\frac{d}{dx}$ and $q\frac{d}{dx}$ commute if and only if* $W(p,q) = 0$.

To verify (i) simply note that for any $r \in \mathbb{R}[x]$ one has

$$\begin{aligned}[p\tfrac{d}{dx}, q\tfrac{d}{dx}]r &= p\tfrac{d}{dx}(q\tfrac{d}{dx}r) - q\tfrac{d}{dx}(p\tfrac{d}{dx}r) \\ &= p(qr')' - q(pr')' \\ &= p(qr'' + q'r') - q(pr'' + p'r') \\ &= (pq - qp)r'' + (pq' - qp')r' \\ &= (pq' - p'q)\tfrac{d}{dx}r,\end{aligned}$$

and (i) follows.

As for examples:

(iii) $$[-\tfrac{1}{2}x^n\tfrac{d}{dx}, x^{n-2}\tfrac{d}{dx}] = x^{2n-3}\tfrac{d}{dx}$$

for any integer $n \geq 2$. In particular, for $n = 2$ one obtains

(iv) $$[-\tfrac{1}{2}x^2\tfrac{d}{dx}, \tfrac{d}{dx}] = x\tfrac{d}{dx}.$$

The derivation $x\frac{d}{dx}$ is often called the *Euler derivation*. One sees from (i) that

(v) $$[\tfrac{d}{dx}, x\tfrac{d}{dx}] = x\tfrac{d}{dx}.$$

10. The Arithmetic Semiderivation, the Goldbach Conjecture, and the Twin Prime Conjecture

If p and q are primes then by Proposition 9.13(a) the sum $\delta_p+\delta_q$ of the corresponding p and q-adic semiderivations on $\mathbb{Z}$ (see Example 6.3(a)) is again a semiderivation on $\mathbb{Z}$. Since the prime factorization of any particular integer involves only finitely many primes, it follows that for any $n \in \mathbb{Z}$ one has $\delta_p n = 0$ for all but at most finitely many primes p. As a result the infinite series

$$\delta_{\text{arith}} := \delta_2 + \delta_3 + \delta_5 + \delta_7 + \delta_{11} + \cdots , \tag{10.1}$$

where the sum ranges over all primes, also defines a semiderivation on $\mathbb{Z}$ provided we assign

$$\delta_{\text{arith}} n := 0 \qquad \text{for} \qquad n = -1, 0, 1. \tag{10.2}$$

This is the[49] *arithmetic semiderivation*. Note that $-1, 0$ and 1 are the only constants. Also note that for any prime $p \in \mathbb{Z}^+$ one has

$$\delta_{\text{arith}} p^n = np^{n-1} \qquad \text{for all} \qquad n \in \mathbb{Z}. \tag{10.3}$$

In particular,

$$\delta_{\text{arith}} p = 1 \qquad \text{for all primes} \qquad p, \tag{10.4}$$

and

$$\delta_{\text{arith}} p^p = p^p \qquad \text{for all primes} \qquad p. \tag{10.5}$$

Throughout this section the arithmetic derivation will be expressed using prime notation, i.e. for any $n \in \mathbb{Z}$ we will write n' in place of $\delta_{\text{arith}} n$ and n'' in place of $\delta^2_{\text{arith}} n := \delta_{\text{arith}}(\delta_{\text{arith}} n)$, etc.

Ordinary differential equations involving δ_{arith} are called[50] *arithmetic differential equations*. As we will see in this section, finding all solutions of such equations, even those which appear rather innocuous, can be far from straightforward.

[49] The terminology is not standard. In particular, δ_{arith} is also called the *arithmetic derivation*, even though it is not a derivation. For example, $\delta_{\text{arith}}(2+3) = \delta_{\text{arith}}(5) = \delta_5 5 = 1$, whereas $\delta_{\text{arith}} 2 + \delta_{\text{arith}} 3 = \delta_2 2 + \delta_3 3 = 1 + 1 = 2 \neq 1$.

[50] The terminology is not standard.

Examples 10.6 :

(a) From the prime factorization $-75 = (-1) \cdot 3^1 \cdot 5^2$ we see that

$$\begin{aligned} \delta_{\text{arith}}(-75) &= \delta_{\text{arith}}((-1) \cdot 75) \\ &= (-1) \cdot \delta_{\text{arith}} 75 + \delta_{\text{arith}}(-1) \cdot 75 \\ &= (-1) \cdot \delta_{\text{arith}} 75 + 0 \cdot 75 \\ &= (-1) \cdot \delta_{\text{arith}} 75 \\ &= (-1) \cdot \delta_{\text{arith}}(3^1 \cdot 5^2). \end{aligned}$$

From this point one can complete the calculation in (at least) two different ways: using (10.1) we have

$$\delta_{\text{arith}}(3 \cdot 5^2) = (\delta_3 + \delta_5)(3 \cdot 5^2) = \delta_3(3 \cdot 5^2) + \delta_5(3 \cdot 5^2) = 5^2 + 2 \cdot 3 \cdot 5 = 55\,;$$

whereas using (10.3) we have

$$\delta_{\text{arith}}(3 \cdot 5^2) = 3 \cdot \delta_{\text{arith}} 5^2 + \delta_{\text{arith}} 3 \cdot 5^2 = 2 \cdot 2 \cdot 5 + 1 \cdot 5^2 = 55.$$

Thus

$$\delta_{\text{arith}}(-75) = -55.$$

(b) From the prime factorization $6,690,468,488 = 2^3 \cdot 11^4 \cdot 239^2$ we see that

$$\begin{aligned} \delta_{\text{arith}}(6,690,468,400) &= (\delta_2 + \delta_{11} + \delta_{239})(2^3 \cdot 11^4 \cdot 239^2) \\ &= \delta_2(2^3 \cdot 11^4 \cdot 239^2) + \delta_{11}(2^3 \cdot 11^4 \cdot 239^2) \\ &\qquad + \delta_{239}(2^3 \cdot 11^4 \cdot 239^2) \\ &= 3 \cdot 2^2 \cdot 11^4 \cdot 239^2 + 4 \cdot 2^3 \cdot 11^3 \cdot 239^2 \\ &\qquad + 2 \cdot 2^3 \cdot 11^4 \cdot 239 \\ &= 10,035,702,732 + 2,432,897,632 + 55,987,184 \\ &= 12,524,587,548. \end{aligned}$$

(c) *The second-order arithmetic semidifferential equation*

(i) $$y'' = 5y$$

admits $p^p q^q$ *as a solution for any* (not necessarily distinct) *primes* $p, q \in \mathbb{Z}^+$. *In particular, the equation has infinitely many solutions.* Indeed, one sees from (10.5) that

$$(p^p q^q)' = p^p \cdot (q^q)' + (p^p)' \cdot q^q = q^p q^q + p^p q^q = 2p^p q^q,$$

and as a result that

$$(p^pq^q)'' = (2p^pq^q)' = 2(p^pq^q)' + 2'(p^pq^q) = 2(2p^pq^q) + p^pq^q = 5p^pq^q.$$

More generally, if $r \in \mathbb{Z}^+$ is any prime number, and if $s, t \in \mathbb{Z}^+$ satisfy $r = s+t$, then $p^{sp}q^{tq}$ is a solution of the second-order arithmetic semidifferential equation

$$y'' = (r^2 + 1)y.$$

The remainder of the section is adapted from [U-A], where readers will find a far more extensive discussion.

The *Goldbach conjecture* asserts that every positive even integer greater than two is the sum of two primes, i.e. that the list

$$\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 3+7 = 5+5 \\
12 &= 5+7 \\
14 &= 3+11 = 7+7 \\
16 &= 3+13 = 5+11 \\
&\vdots
\end{aligned}$$

continues without interruption and without end.

Theorem 10.7 : *If the Goldbach conjecture is true each arithmetic differential equation*

$$y' = 2n, \qquad \textit{where} \qquad 2 \leq n \in \mathbb{Z}^+,$$

admits at least one solution in $\mathbb{Z}^+$.

In particular, one could disprove the conjecture if one could produce a positive integer n for which the corresponding equation had no solution in $\mathbb{Z}^+$,

One might also express the conclusion of the theorem as: *each even integer greater than two admits an "arithmetic antisemiderivation" in* $\mathbb{Z}^+$.

Proof : If the Goldbach conjecture is true and $2 \leq n \in \mathbb{Z}$ there are (possibly non-distinct) primes $p, q \in \mathbb{Z}^+$ such that $2n = p + q$. One then has

$$(pq)' = pq' + p'q = p + q = 2n.$$

q.e.d.

An odd prime number $p \in \mathbb{Z}^+$ is a *twin prime* if either (or both) of $p+2$ and $p-2$ is also prime. Examples are $3, 5, 7, 11, 13, 17, 19, 27, 29, 31, \ldots$; the first odd prime which is not a twin is 23. The *twin prime conjecture* is: there are infinitely many twin primes. Very recently there have been significant advances toward proving the conjecture, in particular by Y. Zhang of the University of New Hampshire (see [Ell]), and this author suspects this task will be completed very soon (assuming this has not already occurred).

Theorem 10.8 : *If the twin prime conjecture is true the arithmetic differential equation*

$$y'' = 1$$

admits infinitely many solutions in $\mathbb{Z}^+$.

In particular, one could disprove the conjecture if one could show the equation admits only finitely many solutions.

Proof : For any twin primes p, $q := p+2$ we see from (10.4) that

$$(2p)' = 2p' + 2'p = 2 + p = q,$$

hence with a second appeal to (10.4) that

$$(2p)'' = q' = 1.$$

q.e.d.

Part III - Topics from Differential Algebra

The goal in this final group of sections is to assign meaning to the term "transcendental function" in the elementary calculus context and to to prove that the exponential, natural logarithm, cosine, sine and arctangent functions are examples. Additional background material must be developed.

11. Basics

Let (R, δ_R) and (S, δ_S) be (semi)differential rings. A ring homomorphism $f : R \to S$ is a (*semi-*)*differential ring homomorphism* if f commutes with the given derivations, i.e. if

$$f \circ \delta_R = \delta_S \circ f. \tag{11.1}$$

When prime notation is used for both derivations (which can sometimes cause confusion) this condition is expressed as

$$f(r') = (f(r))' \qquad \text{for all} \qquad r \in R. \tag{11.2}$$

Suppose (11.1) holds. Then:

- f is a (*semi-*)*differential ring embedding* if f is an embedding;
- f is a (*semi-*)*differential ring isomorphism* if f is a ring isomorphism;
- f is a (*semi-*)*differential* (R-)*algebra* if f is considered as (the structure mapping of) an R-algebra.

In the last case one would more likely refer to S as the differential (R-)algebra when f is clear from context.

To formulate the analogous concepts for fields replace "ring" by "field" in the previous two paragraphs, always keeping in mind that a homomorphism $f : K \to L$ between fields is automatically an embedding.

Examples 11.3 :

(a) Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, assume the polynomial algebra $\mathbb{K}[x]$ (in a single indeterminate) is endowed with the usual derivation d/dx (see Example 6.3b)), and that the ring $\mathbb{K}_F(x)$ is endowed with the standard derivation (which is also denoted d/dx). Then the ring isomorphism $p \in \mathbb{K}[x] \mapsto p(x) \in \mathbb{K}_F[x]$ introduced in the second paragraph of §2 is a differential ring isomorphism (as one sees by comparing Corollary 4.6(a) with Example 6.3(b)).

(b) Let (R, δ) be a differential ring. An ideal $\mathfrak{i} \subset R$ is a *differential ideal* (w.r.t. the given derivation) if

(i) $$\delta(\mathfrak{i}) \subset \mathfrak{i}.$$

If this is the case then one can easily check that a derivation on the factor ring $R/\mathfrak{i}$ is well-defined by $[r] \in R/\mathfrak{i} \mapsto [r'] \in R/\mathfrak{i}$, and that when this "induced" derivation is assumed the canonical homomorphism $r \in R \mapsto [r] \in R/\mathfrak{i}$ becomes a differential homomorphism.

One begins to see striking differences between commutative algebra and differential algebra when one begins the study of differential ideals. For example, it seems perfectly reasonable to refer to a differential ideal as a *maximal differential ideal* if it is not properly contained in any differential ideal other than the given differential ring, and this is the commonly accepted definition. However, in commutative algebra one learns that an ideal is maximal if and only if the corresponding factor ring is a field, but the analogous statement in differential algebra is false. For example, assuming the usual derivation one sees from the fact that differentiating decreases the orders of polynomials that the principal ideal domain $\mathbb{Q}[x]$ has no non-trivial differential ideals, and as a result that the zero ideal (0) is a maximal differential ideal. However, the corresponding factor ring $\mathbb{Q}[x]/(0) \simeq \mathbb{Q}[x]$ is not a field.

(c) Let $U \subset \mathbb{C}$ be any non-empty connected open set having the property that $U_{\mathbb{R}} := U \cap \mathbb{R}$ is non-empty. Then both horizontal mappings within the commutative diagram

$$\begin{array}{ccc} & & \mathcal{M}(U_{\mathbb{R}}) \\ & & \Big| \\ \mathbb{R}(x) & \xrightarrow{f} & \mathcal{R}(U_{\mathbb{R}}) \\ \Big| & & \Big| \\ \mathbb{R}[x] & \xrightarrow{f|_{\mathbb{R}[x]}} & \mathcal{P}(U_{\mathbb{R}}) \end{array}$$

of Corollary 3.10 are differential isomorphisms, assuming the usual and standard derivations on the left and right respectively, and all the vertical (upward) inclusions are differential embeddings.

Proposition 11.4 : *Any semidifferential ring homomorphism carries constants to constants and primitives to primitives.*

Proof : In fact this is a simple consequence of (11.1), but the results are perhaps more quickly appreciated when one sees proofs in terms of prime notation. Assume, therefore, that $f : R \to S$ is a differential ring homomorphism, that prime notation is used with both derivations, and that $r_1, r_2 \in R$. Then (11.2) gives

$$\text{(i)} \qquad f(r_1') = (f(r_1))'.$$

If r_1 is a constant then $f(r_1') = f(0) = 0$ (the final equality since f is a ring homomorphism), hence $(f(r_1))' = 0$ by (i), and $f(r_1)$ is therefore constant.

As for primitives: if $r_1' = r_2$ then $f(r_2) = (f(r_1))'$, again by (i). **q.e.d.**

Suppose $f : R \to S$ is ring (*resp.* field) isomorphism and δ is a derivation on R. Then a derivation $f_*\delta$ on S, called the *push-forward* (*derivation*) *of* δ (*by* f), is defined by

$$(11.5) \qquad f_*\delta := f \circ \delta \circ f^{-1}.$$

One then sees directly from the definition that when the push-forward derivation on S is assumed, f becomes a differential ring (*resp.* field) isomorphism.

Theorem 11.6 : *Let $f : K \to L$ be an embedding of differential fields. Then there is a differential field M containing K as a differential subfield and a differential field isomorphism $\widehat{f} : M \to L$ such that $\widehat{f}|_K = f$.*

Less formally, every differential field embedding can be "extended" (although not uniquely) to a differential field isomorphism. This result will be used in to view real or complex valued functions within a purely algebraic context (see, e.g. Corollary 11.7).

One can see from the following proof that one can replace differential fields by differential rings in the statement. The construction involved is fairly typical in the theory of fields[51].

Proof : If $f(K) = L$ there is nothing to prove, so assume this is not the case and pick a set S disjoint from K and L having the same cardinality as $L \setminus f(K)$. Specifically, let $\beta : L \setminus f(K) \to S$ be a (set-theoretic) bijection.

[51] See, for example, the proof of Proposition 2.3 in [Lang, Chapter V, §2, p. 231].

Set $M := K \cup S$ (at this point M is simply regarded as a set) and define a (set-theoretic) bijection $\alpha : L \to M$ by

$$\alpha : \ell \mapsto \begin{cases} \beta(\ell) & \text{if } \ell \in L \setminus f(K), \\ f^{-1}(\ell) & \text{otherwise, i.e. if } \ell \in f(K). \end{cases}$$

By means of α we can create a field structure on M which renders α an isomorphism of fields, e.g. addition in M is given by

$$m_1 + m_2 := \alpha(\alpha^{-1}(m_1) + \alpha^{-1}(m_2)) \qquad \text{for all} \qquad m_1, m_2 \in M.$$

Moreover, the push-forward by α of the derivation on L is a derivation on M which renders α a differential field isomorphism. Now simply observe that since f is differential embedding the transferred field structure and push-forward derivation must, when restricted to K, agree with the original field structure and derivation on K. The mapping $\widehat{f} := \alpha^{-1} : M \to L$ is therefore a differential isomorphism as asserted. **q.e.d.**

Corollary 11.7 : *Let $U \subset \mathbb{C}$ be any non-empty connected open set having the property that $U_{\mathbb{R}} := U \cap \mathbb{R}$ is non-empty. Then the commutative diagram of* Example 11.3(c) *can be extended to a commutative diagram of the form*

$$\begin{array}{ccc} L & \xrightarrow{\widehat{f}} & \mathcal{M}(U_{\mathbb{R}}) \\ | & & | \\ \mathbb{R}(x) & \xrightarrow{f=\widehat{f}|_{\mathbb{R}(x)}} & \mathcal{R}(U_{\mathbb{R}}) \\ | & & | \\ \mathbb{R}[x] & \xrightarrow{f|_{\mathbb{R}[x]}} & \mathcal{P}(U_{\mathbb{R}}) \end{array}$$

in which L is a differential field, $\widehat{f}$ is a differential field isomorphism, and the mapping $\mathbb{R}(x) \to L$ indicated by the upper left vertical line segment is a differential inclusion.

The important thing to keep in mind about this result is that *by working strictly within the left column one is freed from having to regard the elements of M as functions.*[52] This eliminates such bothersome chores as having to consider domains when dividing one element by another. On the other hand, because $\widehat{f}$ is a differential isomorphism anything that one can establish by working on the left will automatically have a functional interpretation.

[52]This philosophy is pervasive in algebraic geometry.

12. Extending Derivations

Let $S \supset R$ be an extension of rings[53] and let $\delta_S : S \to S$ be a derivation on S. If $\delta_S(R) \subset R$ the restriction $\delta_R := \delta_S|_R$ is a derivation on R, and when this is the case we refer to δ_S as an *extension* of δ_R and to the containment $S \subset R$ as a *differential ring extension*. When these relationships hold it is common practice to denote both δ_S and δ_R using prime notation, and we will follow this custom unless confusion might otherwise result.

When S and R are fields one speaks of *differential field extensions*.

Examples 12.1 :

(a) Let A be any commutative ring and let $A[x]$ be the associated polynomial algebra in a single indeterminate. Then the usual derivation $\frac{d}{dx}$ on $A[x]$ is an extension of the trivial derivation on A. This may be viewed as an expanded version of the statement that *the derivative of a constant polynomial is zero.*

(b) Let (A, δ) be a commutative differential ring and let $A[x]$ be the polynomial algebra, in a single indeterminate, associated with A. Then δ extends to a derivation on $A[x]$, again denoted δ, such that

(i) $$\delta x = 0.$$

Indeed, any element $p \in A[x]$ can be written uniquely in the form $p = \sum_{j=0}^{n} a_j x^j$, where $0 \leq n \in \mathbb{Z}$. If the derivation $\delta : A \to A$ is expressed as $a \mapsto a'$, define a function from $A[x]$ into $A[x]$ extending δ, and also denoted δ, by

(ii) $$\delta : p = \textstyle\sum_{j=0}^{n} a_j x^j \mapsto p' := \sum_{j=0}^{n} a_j' x^j.$$

Since $x = 0 + 1 \cdot x$ we see from definition (ii) and (a) and (b) of Proposition 9.1 that (i) must hold, and it therefore remains to prove the given extension is a derivation.

To verify the Leibniz rule and additivity suppose $p = \sum_{i=0}^{n} a_i x^i$, $q = \sum_{j=0}^{m} b_j x^j \in A[x]$. By allowing $a_n = 0$ or $b_m = 0$ we may assume $n = m$ and write p and q, as well as their product, without specifying the upper indices (i.e. the respective degrees). From

$$pq = \textstyle\sum_i a_i x^i \cdot \sum_j b_j x^j = \sum_{ij} a_i b_j x^{i+j} = \sum_k a_i b_{k-i} x^k$$

[53] In other words, suppose R is a subring of S.

we then have

$$\begin{aligned}(pq)' &= (\textstyle\sum_k a_i b_{k-i} x^k)' \\ &:= \textstyle\sum_k (a_i b_{k-i})' x^k \\ &= \textstyle\sum_k (a_i b'_{k-i} + a'_i b_{k-i}) x^k \\ &= \textstyle\sum_k a_i b'_{k-i} x^k + \sum_k a'_i b_{k-i} x^k \\ &= \textstyle\sum_{ij} a_i b'_j x^{i+j} + \sum_{ij} a'_i b_{k-i} x^{i+j} \\ &= pq' + p'q.\end{aligned}$$

The required additivity property $(p+q)' = p' + q'$ is obvious from (ii).

(c) Let A be an integral domain and let $\delta \in \mathrm{Der}(A)$. We claim that δ *admits a unique extension to the quotient field* K *of* A*, and that this extension is well-defined by the "quotient rule"*

(i) $$(a/b)' := (ba' - a'b)/b^2, \qquad a, b \in A, \qquad b \neq 0.$$

To verify that the function presumed to extend δ is well-defined choose $a, c \in A$ and $b, d \in A^\times$ such that $a/b = c/d$ or, equivalently, such that

(ii) $$ad = bc$$

holds in A. Since $\delta \in \mathrm{Der}(A)$ it follows from (ii) that

$$ad' + a'd = bc' + b'c$$

or, equivalently, that

(iii) $$b'c - a'd = ad' - bc'.$$

Multiplying (iii) by bd and using (ii) justifies the string of implications

$$\begin{aligned}& b'c \cdot bd - a'd \cdot bd = ad' \cdot bd - bc' \cdot cd \\ \Rightarrow\ & bc \cdot b'd - a'b \cdot d^2 = ad \cdot bd' - c'd \cdot b^2 \\ \Rightarrow\ & ad \cdot b'd - a'b \cdot d^2 = bc \cdot bd' - c'd \cdot b^2 \\ \Rightarrow\ & ab' \cdot d^2 - a'b \cdot d^2 = cd'b^2 - c'd \cdot b^2 \\ \Rightarrow\ & (ab' - a'b)/b^2 = (cd' - c'd)/d^2,\end{aligned}$$

precisely as required for the presumed extension to be well-defined.

Taking $b = 1$ in (i) as using Proposition 9.1(b) we see that $(a/1)' = a'/1$. With the understanding that A is to be identified with the image of the canonical embedding $a \in A \mapsto a/1 \in K$, we conclude that the function defined in (i) does extend the initial derivation δ to K.

The verification that (i) defines a derivation is elementary, and is safely left to readers.

The uniqueness of this extension is a simple consequence of Proposition 9.1(h).

When K is a field and x is a single indeterminate we see from Example 12.1(c) that the usual derivation $\frac{d}{dx}$ on $K[x]$ admits a unique extension to the quotient field $K(x)$. That extension will be called the *usual derivation* on $K(x)$, and will also be denoted $\frac{d}{dx}$.

Proposition 12.2 : *Let (A, δ) be a differential ring and let $A[x]$ be the polynomial ring over A in a single indeterminate x. Then:*

(a) *δ admits an extension to a derivation $p \mapsto p'$ on $A[x]$ such that $x' = 1$; and*

(b) *if A is an integral domain with quotient field K, and if $q \in K(x)$ is arbitrary, then δ admits an extension to a derivation $r \mapsto r'$ on $K(x)$ such that $x' = q$.*

In the statement, and henceforth, $K(x)$ denotes the quotient field of the polynomial algebra $K[x]$.

Proof :

(a) From Example 12.1(a) we see that the usual derivation $\frac{d}{dx}$ on $A[x]$, which obviously satisfies

$$\text{(i)} \qquad \frac{d}{dx}x = 1,$$

extends the trivial derivation on A. From Example 12.1(b) we see that there is derivation $\widehat{\delta} : A[x] \to A[x]$ extending δ such that

$$\text{(ii)} \qquad \widehat{\delta}(x) = 0.$$

By Proposition 9.13(a) the sum $\frac{d}{dx} + \widehat{\delta}$ is a derivation on $A[x]$, which by construction is an extension of δ with the required property.

(b) In view of Example 12.1(c) we can assume w.l.o.g. that δ is defined on K. We can then extend δ as in Example 12.1(b) to a derivation $\widehat{\delta}$ on $K[x]$ such that

$\widehat{\delta}x = 0$. Indeed, by means of a second appeal to Example 12.1(c) we may assume $\widehat{\delta}$ is defined on $K(x)$.

Now consider the usual derivation $\frac{d}{dx}$ on $K[x]$, which as above we may assume has been extended to $K(x)$. By Proposition 9.13(b) the product $q\frac{d}{dx}$ is a derivation on $K(x)$ which is easily seen to extend the trivial derivation on A, and which obviously satisfies

$$q\tfrac{d}{dx}x = q.$$

By Proposition 9.13(a) the sum $\widehat{\delta} + q\frac{d}{dx}$ is a derivation on $K(x)$, and the asserted properties clearly hold.

q.e.d.

13. Differential Unique Factorization Domains

In this section R denotes a commutative ring in which $1 \neq 0$, i.e. having at least two elements.

We begin by reviewing a few definitions and results related to the divisibility concept in commutative rings introduced immediately following Examples 7.2. As a general reference for those aspects not involving derivations [Hun, Chapter III, §3, pp. 135-142] is highly recommended[54].

A element $r \in R$ is:

- a *unit* if $r|1$;
- *prime* if r is a non-zero non-unit and for any $r_1, r_2 \in R$ the condition $r|r_1r_2$ implies $r|r_1$ or $r|r_2$ (or both);
- *irreducible* if r is a non-zero non-unit and the condition $r = r_1r_2$ for some $r_1, r_2 \in R$ implies that one of r_1 and r_2 must be a unit.

According to this definition of 'prime' the elements $-2, -3, -5, -7, -11, \cdots \in \mathbb{Z}$ would qualify along with the usual suspects[55] $2, 3, 5, 7, 11, \ldots$. When dealing with $\mathbb{Z}$ we follow custom and restrict application of the word to positive primes.

In elementary calculus the important irreducible elements are those of the polynomial algebra $\mathbb{R}[x]$, i.e. all linear polynomials, meaning polynomials of the form $x - r$, and all quadratic polynomials $ax^2 + bx + c$ satisfying $b^2 - 4ac < 0$. In $\mathbb{C}[x]$ only the linear polynomials are irreducible.

Elements $r_1, r_2 \in R$ are

- *associates* if $r_1|r_2$ and $r_2|r_1$;
- *relatively prime*[56], which one indicates by writing $(r_1, r_2) = 1$, if these elements have no common irreducible factor.

Note that any two units are associates.

[54] In particular, there one will find an example of a prime which is not irreducible and an example of an irreducible which is not prime. Readers are challenged to find an example of a ring having two associates with the property that neither is the product of a unit with the other.

[55] Number theorists refer to elements of the collection $\{2, 3, 5, 7, 11, \ldots\}$ as *rational primes*; the terminology is explained in Footnote 60.

[56] Or *coprime*.

Proposition 13.1 :

(a) *If* $r_1, r_2, r \in R$ *and* r_1 *and* r_2 *are associates then* $r_1|r \Leftrightarrow r_2|r$ *;*

(b) *If* $r, s_1, s_2 \in R$ *and* s_1 *and* s_2 *are associates then* $r|s_1 \Leftrightarrow r|s_2$*;*

(c) *associates of primes are prime; and*

(d) *associates of irreducibles are irreducible.*

In particular, elements $r_1, r_2 \in R$ *have a common irreducible factor if and only if there are associate irreducibles* $s_1, s_2 \in R$ *such that* $s_j|r_j$ *for* $j = 1, 2$*.*

Proposition 13.2 : *Suppose* R *is an integral domain. Then:*

(a) *elements* $r_1, r_2 \in R$ *are associates if and only if there is a unit* $u \in R$ *such that* $r_2 = r_1 u$*;*

(b) *an element* $r \in R$ *is prime if and only if it is irreducible.*

Let $r \in R \setminus \{0\}$.

- A *factorization of* r *into irreducibles* consists of a unit $u \in R$ together with a finite (possibly empty) set $p_1, p_2, \ldots, p_m$ of pairwise non-associate irreducibles and a finite set $n_1, n_2, \ldots, n_m$ of positive integers such that

  (13.3) $$r = u \cdot \prod_{j=1}^{m} p_j^{n_j}.$$

  In particular, a factorization of a unit u into irreducibles is given by $u = u$. The factorization (13.3) into irreducibles is (by abuse of language) *unique* if for any other such factorization

  $$r = v \cdot \prod_{k=1}^{s} q_k^{t_k}$$

  one has $m = s$, and if when $m > 0$ there is a permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$ such that the irreducibles p_j and $q_{\sigma^{-1}(j)}$ are associates and $m_j = t_{\sigma^{-1}(j)}$ for $j = 1, 2, \ldots, m$. (The units u and v are automatically associates, as are any two units of R.)

The ring R is said to

- *admit unique factorization* if each non-zero element of R admits a unique factorization into irreducibles, and

- be a *unique factorization domain*, or simply a UFD, if it is an integral domain and admits unique factorization. When this is the case one regards $0 = 0$ as a unique irreducible factorization of 0.

Examples 13.4 :

(a) The usual ring $\mathbb{Z}$ of integers is a UFD.

(b) For any field K the polynomial algebra $K[x]$ in a single indeterminate is a UFD.

(c) When $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$ the algebra $\mathbb{K}_F[x]$ of polynomial functions $p(x) : \mathbb{K} \to \mathbb{K}$ is a UFD. Since $\mathbb{K}_F[x]$ and $\mathbb{K}[x]$ are isomorphic as rings (see the second paragraph of §2) this is immediate from Example (b).

(d) Any field is a UFD (because all elements of $K^\times$ are units).

Proposition 13.5 : *Suppose R is a* UFD *and $r \in R \setminus \{0\}$ admits a factorization*

(i) $$r = u \cdot \prod_{j=1}^{m} p_j^{n_j}$$

into irreducibles with $m \geq 1$.

(a) *Suppose $q_j \in R$ is an associate of p_j for $j = 1, 2, \ldots, m$. Then each q_j is irreducible and r admits a factorization into irreducibles of the form*

$$r = v \cdot \prod_{j=1}^{m} q_j^{n_j}.$$

(b) *Suppose $s, t_1 \in R$ satisfy*

$$s = \prod_{j=1}^{m} p_j^{n_j} \cdot t_1.$$

Then $r|s$. Specifically, there is an element $t_2 \in R$ such that

$$s = r \cdot t_2.$$

Proof :

(a) Each q_j is irreducible by Proposition 13.1(d), and the existence of the asserted units u_j is ensured by Proposition 13.2(a). We then have

$$\begin{aligned} r &= u \cdot \prod_{j=1}^{m} p_j^{n_j} \\ &= u \cdot \prod_j (q_j u_j)^{n_j} \\ &= u \cdot \prod_j u^{n_j} u_j \cdot \prod_j q_j^{n_j} \\ &= v \cdot \prod_{j=1}^{m} q_j^{n_j}, \end{aligned}$$

and $v := u \cdot \prod_{j=1}^{m} u_j^{n_j} \in R^\times$ since $R^\times$ is a group.

(b) For $t_2 := u^{-1} \cdot t_1$ we see that

$$s = \prod_j p_j^{n_j} \cdot t_1 = u \cdot \prod_j p_j^{n_j} \cdot u^{-1} \cdot t_1 = r \cdot t_2.$$

q.e.d.

For our purposes the important property of a UFD is the following.

Proposition 13.6 : *Suppose* R *is a* UFD, $r_1, r_2, r \in R$, *and* $(r_1, r_2) = 1$. *Then*

(i) $$r_1 | r_2 r \qquad \Leftrightarrow \qquad r_1 | r.$$

Proof :

$\Rightarrow$ By assumption there is an element $s \in R$ such that

$$r_1 s = r_2 r.$$

Write out factorizations of r_1 and s into irreducibles and multiply these together to obtain a corresponding factorization of $r_1 s$. Do the same for r_2 and r. The results give two factorizations of the same element into irreducibles, and by Proposition 13.5(a) we may assume both sides involve exactly the same irreducibles to exactly the same powers.

If we cancel those irreducible factors of r_2, then from the relatively prime hypothesis we see that all the irreducible factors p_j of r_1 remain on the left, each to at least the same power n_j occurring in the initial factorization of r_1. It follows that $\prod_j p_j^{n_j} | v \cdot r$, where $v \in R^\times$, whence from Proposition 13.5(b) that $r_1 | v \cdot r$, and (i) is then seen from Proposition 13.1(b).

$\Leftarrow$ Obvious.

q.e.d.

For the remainder of the notes a *(semi)differential* UFD will refer to a (semi)differential unique factorization domain.

We can now return to elementary calculus.

Theorem 13.7 : *Let* R *be a semidifferential* UFD, *let* K *be the quotient field of* R, *and let* $\delta : k \mapsto k'$ *denote both the semiderivation on* R *and the unique extension of that semiderivation to* K. *Suppose*

(i) $$r \not| \, r'$$

holds for every $r \in R \backslash R_C$. *Then no reciprocal* $1/p \in K$ *of any irreducible* $p \in R$ *admits a primitive in* K.

Proof : Suppose, to the contrary, that $r \in R$ and $s \in R^\times$ satisfy $(r/s)' = 1/p$ for some irreducible element $p \in R$. Assume w.l.o.g. that r and s are relatively prime. From

$$\frac{1}{p} = \left(\frac{r}{s}\right)' = \frac{sr' - s'r}{s^2} \tag{ii}$$

we obtain

$$p(sr' - s'r) = s^2, \tag{iii}$$

from which we see (by unique factorization and Proposition 13.6) that

$$p|s. \tag{iv}$$

On the other hand, by expressing (iii) in the form

$$s(pr' - s) = s'rp$$

and using (i) (with r replaced by s) we see from the relatively prime assumption $(r, s) = 1$ that $s|p$, whence from (iv) that p and s are associates. Since R is an integral domain this forces $s = pu$ for some unit $u \in R$. This gives $r/s = r/pu = ru^{-1}/p$, and by replacing r by ru^{-1} we see that we may assume $s = p$ in the work we have done thus far. In particular, equality (ii) now becomes

$$\frac{1}{p} = \left(\frac{r}{p}\right)' = \frac{pr' - p'r}{p^2}, \tag{v}$$

which immediately gives

$$p(r' - 1) = p'r.$$

From this last equality and (i) (with r now replaced by p) we conclude that $p|r$, which in combination with (iv) contradicts the assumption that $(r, s) = 1$. **q.e.d.**

Corollary 13.8 : *Assume the standard derivation $\frac{d}{dx}$ on $\mathbb{R}_F(x)$. Then the rational functions $1/x$ and $1/(x^2 + 1)$ have no primitives in $\mathbb{R}_F(x)$.*

The "standard derivation $\frac{d}{dx}$ on $\mathbb{R}_F(x)$" was introduced in Example 6.3(c).

The consequence of this result for elementary calculus is that to have any hope of integrating the two indicated functions one must move beyond the field $\mathbb{R}_F(x)$.

Proof : Condition (i) of Theorem 13.7 obviously holds, and x and $x^2 + 1$ are irreducible elements of $\mathbb{R}[x]$. **q.e.d.**

The remaining results in this section will be needed when "transcendental elements" are investigated.

Theorem 13.9 : *Let R be a semidifferential domain having the property that*

(i) $$r \not| \, r' \qquad \textit{for any} \qquad r \in R \setminus R_C.$$

Then

(a)

(ii) $$u' = 0 \qquad \textit{for any} \qquad u \in R^\times,$$

i.e.

(iii) $$R^\times \subset R_C \, ;$$

and

(b) *if R is a* UFD*, if R_C is a field, and if K is the quotient field of R endowed with the derivation uniquely extending that on R, then*

(iv) $$K_C = R_C.$$

Note that $K_C \supset R_C$ is automatic since $K \supset R$ is a semidifferential ring extension. This explains why (iv) is generally summarized by the statement "K has no new constants."

Let $\mathbb{K}$ denote either $\mathbb{R}$ or $\mathbb{C}$. Since the usual derivation on $\mathbb{K}[x]$ lowers degrees of non-constant polynomials, the proposition applies to these particular differential algebras.

Proof : In the proof both derivations are indicated with prime notation.

(a) Suppose $u \in R^\times$ is such that $u \notin R_C$. Then from Proposition 9.1(e) and the integral domain hypothesis we see that $v := (u^{-1})' = -u'u^{-2} \neq 0$, whence from $u \cdot (u \cdot (-v)) = u'$ that $u | u'$, thereby contradicting (i).

(b) Suppose $k \in K_C$, say $k = p/q$ with $p, q \in R$ relatively prime. Then

$$\begin{aligned} 0 &= k' \\ &= \left(\frac{p}{q}\right)' \\ &= \frac{qp' - q'p}{q^2} \\ &\Leftrightarrow \; qp' - q'p = 0 \\ &\Leftrightarrow \; qp' = q'p. \end{aligned}$$

By Proposition 13.6 and the relatively prime hypothesis this last equality implies $q|q'$, thereby contradicting (i) if $q \notin R_C$. However, if $q \in R_C$ then from the last line of the calculation we see that $p' = 0$ (since $q \neq 0$ is implicit), hence that $p \in R_C$ also holds. Since R_C is assumed to be a field we then see from (f) and (d) of Proposition 9.1 that $k = p/q = pq^{-1} \in R_C$, and the proof is complete. **q.e.d.**

Let $\delta : R \to R$ be a (semi)derivation. The associated *logarithmic (semi)derivation* refers to the mapping

$$\ln \delta : r \in R^\times \mapsto r'r^{-1} \in R. \tag{13.10}$$

This concept was encountered earlier in Proposition 6.12.

Theorem 13.11 : *Let R be a semidifferential* UFD*, let K be the quotient field of R, and let $\delta : k \mapsto k'$ denote both the semiderivation on R and the unique extension of that semiderivation to K. Suppose that*

$$r \not| \, r' \qquad \textit{for all} \qquad r \notin R_C \tag{i}$$

and that R_C is a field. Then $K \setminus K_C$ is preserved by the logarithmic semiderivation $\ln \delta$, i.e.

$$\ln \delta|_{K \setminus K_C} : K \setminus K_C \to K \setminus K_C. \tag{ii}$$

Proof : By Theorem 13.9 the hypothesis imply both

$$R^\times \subset R_C. \tag{iii}$$

and

$$K_C = R_C. \tag{iv}$$

Choose $k \in K \setminus K_C$ and write k in the form p/q, where $p, q \in R$ are relatively prime. Suppose, to achieve a contraction, that $c := \ln \delta(k) = k'/k \in K_C$. Then

$$\begin{aligned} k' = \frac{qp' - q'p}{q^2} \quad &\Rightarrow \quad \frac{k'}{k} = \frac{qp' - q'p}{q^2} \cdot \frac{q}{p} \\ &\Rightarrow \quad c = \frac{qp' - q'p}{pq} \\ &\Rightarrow \quad pqc = qp' - q'p \\ &\Leftrightarrow \quad p(qc + q') = p'q \end{aligned}$$

Since $c \in K_C$ we see from (iii) that all terms appearing in this last expression belong R, hence that $p|qp'$. Theorem 13.6 and the relatively prime assumption $(p,q) = 1$ then force $p|p'$, whereupon from (i) we conclude that $p \in R_C$. Thus $p' = 0$, and since $p \neq 0$ (because $k \notin K_C$) that final line of the calculation above now gives $qc + q' = 0$, hence that $q|q'$. From a second appeal to (i) we conclude that $q \in R_C$ also holds. Since R_C is a field we then see, as in the final line of the proof of Theorem 13.9, that $k \in R_C = K_C$, contrary to the choice of k. **q.e.d.**

14. Transcendental Functions

In this section we will deal with fields and polynomials with coefficients therein. The fields will be denoted by K *and the corresponding polynomial indeterminates by* t*. We use*[57] t *because the fields* K *will often be extensions of polynomial algebras involving a second indeterminate* x*.*

Prime notation will be used with all derivations.

Let $L \supset K$ be an extension of fields. (Example: $K = \mathbb{R}$ and $L = K(x)$.) An element $\ell \in L$ is:

- *algebraic over* K if there is a polynomial $p \in K[x]$ such that $p(\ell) = 0$;
- *transcendental over* K if it is not algebraic over K.

Examples 14.1 :

(a) $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2} \in \mathbb{R}$ is a root of the polynomial $p = t^2 - 2 \in \mathbb{Q}[t]$. (In practice one would simply say that $\sqrt{2}$ is algebraic over $\mathbb{Q}$.)

(b) $-\frac{1}{3}(1 + i\sqrt{14}) \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since $-\frac{1}{3}(1 + i\sqrt{14})$ is a root of the polynomial $3x^2 + 2x + 5 \in \mathbb{Q}[t]$.

(c) The real numbers e and π are transcendental over $\mathbb{Q}$. Readers can easily find proofs elsewhere, e.g. see [Lang, Appendix 1]; writing out the details here would involve too great a diversion.

(d) $\sqrt{x}$ is algebraic over $\mathbb{R}(x)$ since $\sqrt{x}$ is a root of the polynomial $t^2 - x \in (\mathbb{R}(x))[t]$. Here one could take[58] A to be the field $\mathbb{R}(x)[\sqrt{x}] := \mathbb{R}(x)[t]/(t^2 - x)$, where $(t^2 - x) \subset \mathbb{R}(x)[t]$ is the principal ideal generated by $t^2 - x$ and[59] $\sqrt{x} := [t]$ is the image of t under the canonical homomorphism of $\mathbb{R}(x)[t]$ into $\mathbb{R}(x)[t]/(t^2 - x)$.

(e) Since any $k \in K$ is a root of $t - k \in K[t]$, every element of K is algebraic over K.

---

[57] Many authors would use X.

[58] Readers unfamiliar with constructions using ideals should not spend time worrying about this sentence: it amounts to a proof of the existence of a ring containing both $\mathbb{R}(x)$ and an element worthy of the label $\sqrt{x}$.

[59] In other words, the symbol $[t]$ in the definition $\sqrt{x} := [t]$ denotes a the equivalence class (i.e. coset) of x in the indicated factor ring. This choice $[t]$ for notation is discussed in Footnote 37.

Readers curious about number theory should be aware of a related concept for ring extensions $R \supset S$. An element $r \in R$ is

- *integral over* S if there is a monic polynomial $p \in S[t]$ such that $S(r) = 0$.

When S and R are fields this is equivalent to r being algebraic over S.

Examples 14.2 :

(a) $2+i\sqrt{13} \in \mathbb{C}$ is integral over $\mathbb{Z}$ since $2+i\sqrt{13}$ is a root of the monic polynomial $t^2 - 4t + 17 \in \mathbb{Z}[t]$.

(b) $\frac{1}{2}$ is not integral over $\mathbb{Z}$ since it is not a root of any monic polynomial in $\mathbb{Z}[t]$. Indeed, if $\frac{1}{2}$ were a root of a monic polynomial $t^n + \sum_{j=0}^{n-1} s_j t^j \in \mathbb{Z}[t]$ then upon multiplying $(\frac{1}{2})^n = -\sum_{j=0}^{n} s_j (\frac{1}{2})^j$ by 2^n one finds that

$$1 = -\sum_{j=0}^{n-1} s_j 2^{n-j}.$$

By defining $m := -\sum_{j=0}^{n-1} s_j 2^{n-j-1}$ one can write this displayed equation as $1 = 2 \cdot m$, and since $m \in \mathbb{Z}$ this is obviously not possible.

(c) The *Gaussian integers* consist of all complex numbers of the form $a+ib$, where $a, b \in \mathbb{Z}$. Since each such "integer" is a root of the corresponding polynomial $t^2 - 2at + (a^2 + b^2) \in \mathbb{Z}[t]$," each Gaussian integer[60] is integral over $\mathbb{Z}$.

(d) The element $\sqrt{5 + \sqrt{x}} \in \mathbb{Z}[x, \sqrt{5 + \sqrt{x}}\,]$ is integral over $\mathbb{Z}[x]$; it is a root of the monic polynomial $t^4 - 10t^2 + 25 - x \in (\mathbb{Z}[x])[t]$.

(e) Since any element $s \in S$ is a root of the monic polynomial $t - s \in S[t]$, every element of S is integral over S.

[60] Number theorists use the terms "integral" and "integer" somewhat interchangeably, and to avoid confusion with the special case of what practically everyone else calls integers, i.e. elements of $\mathbb{Z}$, they refer to the latter as *rational integers*. The terminology arises from the following observation:

Theorem : *A rational number $r \in \mathbb{Q}$ is an integer, i.e. satisfies $r \in \mathbb{Z}$, if and only if r is integral over $\mathbb{Z}$.*

One begins to sense from this result why a "Gaussian integer" in $\mathbb{Q}(i)$ is regarded as the "correct" generalization of a "rational integer" in $\mathbb{Q}$. Additional support for this viewpoint is provided by the fact that the integral elements of R over S form subring of R (see, e.g. [Lang, Chapter VII, §1, Proposition 1.4, p. 336]).

Theorem 14.3 : *Suppose $L \supset K$ is an extension of fields. Then the collection of elements of L which are algebraic over K forms a subfield of L containing K.*

Proof : See, e.g. [Hun, Chapter V, §1, Theorem 1.14, p. 238]. **q.e.d.**

Proposition 14.4 : *Suppose $L \subset K$ is an extension of fields and $\ell \in L$ is such that ℓ^2 is algebraic over K. Then ℓ is algebraic over K.*

As one can see from the proof, one can replace ℓ^2 in this statement by any positive power of ℓ.

Proof : By assumption there is a polynomial $x^n + \sum_{j=0}^{n-1} k_j x^j \in K[x]$ which is satisfied by ℓ^2; the element ℓ therefore satisfies the polynomial $x^{2n} + \sum_{j=1}^{n-1} k_j x^{2j} \in K[x]$. **q.e.d.**

Proposition 14.5 : *Suppose $L \supset K$ and $N \supset M$ are field extensions and $f : L \to N$ is a field isomorphism of K which restricts to a field isomorphism of K with M. Then an element $\ell \in L$ is*

(a) *algebraic over K if and only if $f(\ell)$ is algebraic over M, and is*

(b) *transcendental over K if and only if $f(\ell)$ is transcendental over M.*

Proof : If $\sum_{j=0}^{n} k_j x^j \in K[x]$ is a polynomial satisfied by ℓ then $\sum_{j=0}^{n} f(k_j) x^j \in M[x]$ is a polynomial satisfied by $f(\ell)$. The result follows. **q.e.d.**

Theorem 14.6 : *Suppose $L \supset K$ is an extension of differential fields of characteristic zero. Assume $\ell \in L \backslash K$ is such that*

(a) *$\ell' \in K$, and*

(b) *ℓ' has no primitive in K.*

Then ℓ is transcendental over K.

Proof : Otherwise ℓ is algebraic over K. If $p = x^n + \sum_{j=0}^{n-1} k_j x^j \in K[x]$ is the corresponding irreducible polynomial then $n \geq 1$, since $\ell \notin K$, and we have

(i) $$0 = \ell^n + \sum_{j=0}^{n-1} k_j \ell^j.$$

Note that $n \geq 1$ since $\ell \notin K$. Applying the derivation to (i) gives

$$\begin{aligned} 0 &= (\ell^n)' + \textstyle\sum_{j=0}^{n-1}(k_j\ell^j)' \\ &= n\ell^{n-1}\ell' + \textstyle\sum_{j=0}^{n-1}(k_j(\ell^j)' + k_j'\ell^j) \\ &= n\ell^{n-1}\ell' + \textstyle\sum_{j=0}^{n-1} k_j j\ell^{j-1}\ell' + \sum_{j=0}^{n-1} k_j'\ell^j \\ &= n\ell^{n-1}\ell' + \textstyle\sum_{j=1}^{n-1} k_j j\ell^{j-1}\ell' + \sum_{j=0}^{n-1} k_j'\ell^j \\ &= n\ell^{n-1}\ell' + \textstyle\sum_{j=0}^{n-2}(j+1)k_{j+1}\ell'\ell^j + \sum_{j=0}^{n-2} k_j'\ell^j + k_{n-1}'\ell^{n-1} \\ &= (n\ell' + k_{n-1}')\ell^{n-1} + \textstyle\sum_{j=0}^{n-1}\left((j+1)k_j\ell' + k_j'\right)\ell^j, \end{aligned}$$

and we conclude that ℓ must also be a zero of the polynomial

$$q := (n\ell' + k_{n-1}')x^{n-1} + \textstyle\sum_{j=0}^{n-1}\left((j+1)k_j\ell' + k_j'\right)x^j.$$

But $q \in K[x]$ by (a), hence $q = 0$ since p has minimal degree among polynomials which admit ℓ as a root. In particular, $n\ell' + k_{n-1}'$ must be zero, and we therefore have

(i) $$\ell' = (-1)\cdot\tfrac{1}{n}\cdot k_{n-1}'.$$

By Proposition 9.6 we also have $(-1)\cdot\frac{1}{n} \in K_C \subset K$, whence

$$\ell' = \left((-1)\cdot\tfrac{1}{n}\cdot k_{n-1}\right)'$$

by (i) and Proposition 9.1(c). Since $(-1)\cdot\frac{1}{n}\cdot k_{n-1} \in K$, this contradicts (b). **q.e.d.**

Corollary 14.7 : *Let K be an field and let x be a single indeterminate. Then $x \in K(x)$ is transcendental over K.*

This is not hard to prove without the aid of differential algebra, but the following argument ties the result in with several of our subsequent proofs of transcendency.

Proof : Endow $K[x]$ with the usual derivation and $K(x)$ with the unique extension of this derivation to the field $K(x)$. We then have $x' = 1 \in K$, and since $K_C = K$ (as was already seen in Example 12.1(a)), the element 1 has no primitive in K. Theorem 14.6 therefore applies. **q.e.d.**

We can now offer justification for referring to the natural logarithm and arctangent functions as "transcendental functions" in a first calculus course.

Corollary 14.8 : *Let L be a differential field extension of $\mathbb{R}(x)$, with the usual derivation assumed on the latter. Suppose $\ell \in L \backslash \mathbb{R}(x)$ satisfies either*

(a) $\ell' = 1/x$ *or*

(b) $\ell' = 1/(x^2 + 1)$.

Then ℓ is transcendental over $K(x)$.

Proof : Condition (a) of Theorem 14.6 is ensured by either of (a) and (b) above, and condition (b) of the theorem is ensured by Corollary 13.8. **q.e.d**.

The subset $U^{\log} \subset \mathbb{C}$ of the following statement was defined in Example 5.6(a).

Corollary 14.9 : *Let U be a non-empty connected open subset of $U^{\log} \subset \mathbb{C}$ such that $\emptyset \neq U_{\mathbb{R}} := U \cap \mathbb{R} \subset (0, \infty)$. Then $\ln|_U \in \mathcal{M}(U_{\mathbb{R}})$, and this function is transcendental over $\mathcal{R}(U_{\mathbb{R}})$.*

Proof : By (our) definition the domain of the natural logarithm function ln is $U^{\log}$, and the assumption that $U \subset U^{\log}$ therefore ensures the membership $\ln|_U \in \mathcal{M}(U)$. Since $\ln|_{(0,\infty)}$ is real-valued, the assumption that $U_{\mathbb{R}} \subset (0, \infty)$ guarantees, in turn, that $\ln|_U \in \mathcal{M}(U_{\mathbb{R}})$. Using the notation of Corollary 11.7 and the fact that the $(\ln_U)' = 1/x \in \mathcal{M}(U_{\mathbb{R}})$, there must be a corresponding element $\ell \in L$ such that $\ell' = 1/x \in \mathbb{R}(x)$. It follows from Corollary 14.8 that ℓ is transcendental over $\mathbb{R}(x)$, whence from Proposition 14.5(b) that $\ln|_U$ is transcendental over $\mathcal{R}(U_{\mathbb{R}})$. **q.e.d**.

The subset $U^{\mathrm{atn}} \subset \mathbb{C}$ of the following statement was defined in Example 5.6(b).

Corollary 14.10 : *Let $U \subset \mathbb{C}$ be any connected open subset satisfying $\mathbb{R} \subset U \subset U^{\mathrm{atn}}$. Then $\arctan|_{\mathbb{R}} \in \mathcal{M}(U_{\mathbb{R}})$, and this function is transcendental over the field $\mathcal{R}(U_{\mathbb{R}})$.*

Proof : The proof is easily adapted from that given for Corollary 14.9, and is safely left to the reader. **q.e.d**.

The following result will be used to prove the exponential functions are transcendental over the appropriate fields.

Theorem 14.11 : *Let R be a* UFD *with quotient field K. Assume a derivation on R has been extended* (in the only way possible) *to K, and that $L \supset K$ is a differential field extension. Suppose, in addition, that*

(i) $$r \not| \, r' \qquad \text{for all} \qquad r \in R \setminus R_C,$$

that R_C is a field, and that

(ii) $$L_C = K_C.$$

Then any element $\ell \in L \setminus K$ satisfying

(iii) $$\ell'/\ell \in K_C$$

is transcendental over K.

Proof : Let

(iv) $$c := \ell'/\ell \in K_C,$$

so that

(v) $$\ell' = c\ell.$$

We claim that

(vi) $$c \neq 0.$$

For if that were the case (v) would imply $\ell' = 0$, hence that $\ell \in L_C = K_C \subset K$, contrary to the choice of ℓ.

If the theorem is false there must be a monic polynomial $p = x^n + \sum_{j=0}^{n-1} k_j x^n \in K[x]$ with $n \geq 2$ which is satisfied by ℓ.

We claim that

(vii) $$k_j \neq 0 \qquad \text{for at least one} \qquad 0 \leq j \leq n-1.$$

Otherwise $\ell^n = 0$, hence $\ell = 0 \in K$, again contrary to the choice of ℓ.

Differentiating $0 = p(\ell)$ gives

$$\begin{aligned} 0 &= \left(\ell^n + \textstyle\sum_{j=0}^{n-1} k_j \ell^j\right)' \\ &= (\ell^n)' + \textstyle\sum_{j=0}^{n-1} (k_j \ell^j)' \\ &= n\ell^{n-1}\ell' + \textstyle\sum_{j=0}^{n-1} \left(k_j j \ell^{j-1}\ell' + k_j' \ell^j\right) \\ &= nc\ell^n + \textstyle\sum_{j=0}^{n-1} \left(jck_j + k_j'\right) \ell^j. \end{aligned}$$

By (vi) and the characteristic zero hypothesis we can divide this last polynomial by nc, obtaining

(viii) $$0 = \ell^n + \sum_{j=0}^{n-1} \frac{jck_j + k_j'}{nc} \cdot \ell^n,$$

Since the irreducible polynomial of ℓ is the unique polynomial of degree n in $K[x]$ satisfied by ℓ, and since each of the coefficients appearing in (viii) is (by (iv)) in K, it must be the case that that $p = x^n + \sum_{j=0}^{n-1} k_j x^j = x^n + \sum_{j=0}^{n-1} \frac{jck_j + k_j'}{nc} x^j$. We conclude that

$$k_j = \frac{jck_j + k_j'}{nc} \qquad \text{for} \qquad j = 0, 1, \ldots, n-1$$

or, equivalently, that

$$(n-j)ck_j = k_j' \qquad \text{for all such } j.$$

By (vii) there is a j such that $k_j \neq 0$, hence such that

$$\ln \delta(k) = \frac{k_j'}{k_j} = (n-j)c.$$

By Proposition 9.6 we have $n - j \in K_C$, whence $(n-j)c \in K_C$ by (iv) and Proposition 9.1(d), and we have thereby contradicted Theorem 13.11. **q.e.d.**

Corollary 14.12 : *Let $\mathbb{K} := \mathbb{R}$ or $\mathbb{C}$ and let $L \supset \mathbb{K}(x)$ be a differential field extension of $\mathbb{K}(x)$, with the usual derivation assumed on the latter. Then any $\ell \in L^\times$ satisfying*

(i) $$\ell'/\ell \in \mathbb{K}(x)_C$$

is transcendental over $\mathbb{K}(x)$.

Proof : First note from Theorem 13.9(b) that $\mathbb{K}(x)_C = \mathbb{K}[x]_C$; then from (i) and Theorem 13.11 that $\ell \notin \mathbb{K}(x)$; then from the final comment before the proof of Theorem 13.9 that the remaining hypotheses of Theorem 14.11 are satisfied. **q.e.d.**

Corollary 14.13 : *Let $U \subset \mathbb{C}$ be any non-empty connected open set. Then:*

(a) $\exp|_U \in \mathcal{M}(U)$ *is transcendental over $\mathcal{R}(U)$; and*

(b) *if $U_{\mathbb{R}} := U \cap \mathbb{R}$ is non-empty then $\exp|_{U_{\mathbb{R}}} \in \mathcal{M}(U_{\mathbb{R}})$ is transcendental over $\mathcal{R}(U_{\mathbb{R}})$.*

Corollary 14.14 : *Let* $U \subset \mathbb{C}$ *be any non-empty connected open set. Then:*

(a) $\cos|_U$ *and* $\sin|_U$ *are transcendental over* $\mathcal{R}(U)$*; and*

(b) *if* $U_{\mathbb{R}} := U \cap \mathbb{R}$ *is non-empty then* $\cos|_{U_{\mathbb{R}}}$ *and* $\sin|_{U_{\mathbb{R}}}$ *are transcendental over* $\mathcal{R}(U_{\mathbb{R}})$.

Proof :

(a) If either of $\cos|_U$ and $\sin|_U$ is algebraic over $\mathcal{R}(U)$ the same must hold for the sum $\cos|_U + i\sin|_U$ by Theorem 14.3. It would then follow from (i) of Example 2.15(d) that the function $c \in U \mapsto \exp(ic) \in \mathbb{C}$ is algebraic over $\mathcal{R}(U)$, and since (by the chain-rule) the logarithmic derivative of this function is the constant function $c \in U \mapsto i$, this would contradict Corollary 14.12. We have therefore established that at least one of $\cos|_U$ and $\sin|_U$ is transcendental over $\mathcal{R}(U)$.

Suppose one of these restrictions, say $\cos|U$, is algebraic over $\mathcal{R}(U)$. Then from $\sin^2|_U = 1 - \cos^2|_U$ and Theorem 14.3 one sees that $\sin^2|_U$ is algebraic over $\mathcal{R}(U)$, whence from Proposition 14.4 that $\cos|_U$ is algebraic over $\mathcal{R}(U)$, and we have achieved a contradiction.

(b) If either restriction satisfies a polynomial in $\mathcal{R}(U_{\mathbb{R}})[t]$ from Corollary 2.22 one can easily see that the corresponding restrictions to U will satisfy that polynomial when regarded as an element of $\mathcal{R}(U)[t]$

q.e.d.

When viewed from the perspective of differential algebra transcendency has some rather surprising consequences.

Theorem 14.15 : *Suppose that* $L \supset K$ *is an extension of fields, that* $\ell \in L$ *is transcendental over* K*. Then:*

(a) *the subalgebra* $K[\ell]$ *of* L *is isomorphic to the polynomial algebra* $K[x]$*, and as a result each element of this subalgebra can be written uniquely in the form* $\sum_{j=0}^{n} k_j \ell^j$ *where* $k_j \in K$ *for* $j = 1, 2, \ldots, n$*; and*

(b) *if* K *is a differential field and* $m \in K(x) \subset L$ *is arbitrary the derivation on* K *can be extended to a derivation on* $K(\ell)$ *such that, when this extended derivation is denoted by primes,*

(i) $$\ell' = m$$

Proof :

(a) If the substitution homomorphism from $K[x]$ to $K[\ell]$ uniquely determined by $x \mapsto \ell$ has a non-trivial kernel then any non-zero polynomial in that kernel would be satisfied by ℓ, thereby contradicting transcendency.

(b) Use Proposition 12.2(b).

q.e.d.

Examples 14.16 :

(a) Let $U \subset \mathbb{C}$ be non-empty, connected, and open. Then for any choice of f in the subfield $\mathcal{R}(U)(\exp|_U)$ of $\mathcal{M}(U)$ one can extend the standard derivation on $\mathcal{R}(U)$ to a derivation on $\mathcal{R}(U)(\exp|U)$ satisfying

$$(\exp|_U)' = f$$

for any choice of $f \in \mathcal{R}(U)(\exp|U)$.

(b) For any choice of r in the subfield $\mathbb{Q}(\pi) \subset R$ one can extend the trivial derivation on $\mathbb{Q}$ to a derivation on $\mathbb{Q}(\pi)$ satisfying

$$\pi' = r.$$

(c) Assuming the usual derivation on $\mathbb{R}(x)$ there is a differential field extension $L \supset \mathbb{R}(x)$ containing an element ℓ such that $\ell' = 1/x$. To prove this take U in Corollary 11.7 to be the right-half plane, in which case $\ln|_U \in \mathcal{M}_{\mathbb{R}}(U)$. One then takes ℓ to be the corresponding element of L in that statement.

Example 14.16(c) leaves a somewhat unsatisfying after-taste when one realizes that it is not clear how, or even if, the elements of L can be regarded as functions. To circumvent this problem, and thereby achieve a proof of the transcendency over $\mathbb{R}_F(x)$ of the "alternate logarithm function"

$$\text{lnabs} : r \in \mathbb{R}^\times \mapsto \ln|r| \in \mathbb{R} \tag{14.17}$$

introduced in Example 5.6(a), one must wean oneself from a dependency on meromorphic functions. Indeed, one sees immediately from Proposition 5.8 that lnabs is not the restriction to $\mathbb{R}^\times$ of a meromorphic function defined on a connected open subset of $\mathbb{C}$.

Proposition 14.18 : *There is differential field extension* $F \supset \mathbb{R}_F(x)$ *such that:*

(a) *the elements* $f \in F$ *are real-valued functions having dense open subsets* $U_f \subset \mathbb{R}$ *as domains;*

(b) *the derivation on* F *is defined by the standard derivative;*

(c) F *contains the function* $\text{lnabs} : \mathbb{R}^\times \to \mathbb{R}$ *defined in* (14.17)*; and*

(d) $\text{lnabs} \in F$ *is transcendental over* $\mathbb{R}_F(x)$.

Proof : Consider the algebra A of real-valued functions f defined on dense open subsets $U_f \subset \mathbb{R}$ generated by $\mathbb{R}_F(x)$ and lnabs. A typical element $f \in A$ can be written in the form

(i) $$f := \textstyle\sum_{j=0}^{n} r_j \cdot \text{lnabs}^j, \quad \text{where} \quad r_j \in \mathbb{R}_F(x) \quad \text{for} \quad j = 0, 1, 2, \ldots, n.$$

We claim that the given expression for f is unique. Indeed, if f had two distinct such representations then by subtraction we could assume that f is the zero function and that r_j is not the zero function for at least one j. Choose a non-empty connected open subset $U \subset U^{\log} \subset \mathbb{C}$ which intersects $\mathbb{R}$ in a non-empty open interval[61] $U_{\mathbb{R}}$ on which all r_j are defined. Since $\text{lnabs}|_{U_{\mathbb{R}}} = \ln|_{U_{\mathbb{R}}}$ we then see from (i), with f now replaced by the zero function, that $\ln|_{U_{\mathbb{R}}} \in \mathcal{M}(U_{\mathbb{R}})$ must be algebraic over $\mathcal{R}(U_{\mathbb{R}})$, thereby contradicting Corollary 14.9, and the claim follows.

As a consequence of uniqueness in (i) we see that A must be an integral domain, and as a result a ring isomorphism $g : \mathbb{R}(x)[t] \to A$ is uniquely determined by requiring that

(ii) $$t \mapsto \text{lnabs},$$

and that the restriction $g|_{\mathbb{R}[x]}$ is the mapping $p \mapsto p(x)$ of Example 11.3(a). We thus have a commutative diagram

$$\begin{array}{ccc} \mathbb{R}(x)[t] & \xrightarrow{g} & A \\ \big| & & \big| \\ \mathbb{R}(x) & \xrightarrow{g|_{\mathbb{R}(x)}} & \mathbb{R}_F(x) \\ \big| & & \big| \\ \mathbb{R}[x] & \xrightarrow{g|_{\mathbb{R}[x]}} & \mathbb{R}_F[x] \end{array}$$

[61] OK, I lied: we are not yet weaned. But you have to admit that you had to look at the proof to realize this!

in which the vertical bars are upward inclusions. Extend g to an isomorphism $\widehat{g} : (\mathbb{R}(x))(t) \to F$ of the respective quotient fields of $(\mathbb{R}(x))[t]$ and A in the only possible way, thereby enlarging the commutative diagram to

(iii)
$$\left\{\begin{array}{ccc} \mathbb{R}(x)(t) & \stackrel{\widehat{g}}{\longrightarrow} & F \\ | & & | \\ \mathbb{R}(x)[t] & \stackrel{g}{\longrightarrow} & A \\ | & & | \\ \mathbb{R}(x) & \stackrel{g|_{\mathbb{R}(x)}}{\longrightarrow} & \mathbb{R}_F(x) \\ | & & | \\ \mathbb{R}[x] & \stackrel{g|_{\mathbb{R}[x]}}{\longrightarrow} & \mathbb{R}_F[x] \end{array}\right.$$

If the standard derivative is used define derivations on each of $\mathbb{R}_F[x]$, $\mathbb{R}_F(x)$, A and F assertions (a)-(c) of the proposition follow immediately, and the right-hand-side of diagram (iii) becomes a sequence of differential inclusions. Moreover, if the usual derivation is assumed on $\mathbb{R}[x]$ and $\mathbb{R}(x)$ the bottom rectangle becomes a commutative diagram of differential mappings. Now invoke Proposition 12.2(b) to extend the derivation on $\mathbb{R}(x)$ to one on $\mathbb{R}(x)(t)$ satisfying

(iv)
$$t' = 1/x.$$

It then follows from (ii) and (iv) that the subdiagram

$$\begin{array}{ccc} \mathbb{R}(x)(t) & \stackrel{\widehat{g}}{\longrightarrow} & F \\ | & & | \\ \mathbb{R}(x) & \stackrel{g|_{\mathbb{R}(x)}}{\longrightarrow} & R_F(x) \end{array}$$

of (iii) is a commutative diagram of differential fields.

Since $t' = 1/x$ we see from Corollary 14.8(a) that t is transcendental over $\mathbb{R}(x)$, whence from (ii) and Proposition 14.5 that $\mathrm{lnabs} \in F$ is transcendental over $\mathbb{R}_F(x)$. **q.e.d.**

When one deals with algebraic functions over $\mathbb{R}(x)$ the interpretation problem discussed immediately following Example 14.16(c) again arises. For example, since the domain of the real-valued function $\sqrt{x}$ is only $[0, \infty)$, how is one to interpret $\sqrt{x}$ as a function adjoined the field $\mathbb{R}_F(x)$? One way is to use Corollary 3.3 to embed

this differential field into a larger differential field having a domain appropriate to the function being introduced. Another way is to pass to germs of functions. But by far the most elegant solutions involve moving into the complex domain and working with fields of meromorphic functions on Riemann surfaces or, for even greater generality, with algebraic function fields.

Acknowledgements

These notes represent a minor modification of notes originally prepared for a talk in the Number Theory Nosh at the University of Calgary in July of 2013. I am grateful to Drs K. Bauer, C. Cunningham and R. Scheidler for arranging that presentation.

Notes and Comments

Fields of meromorphic functions are ubiquitous in analysis, but the real counterparts $\mathcal{M}(U_{\mathbb{R}})$ introduced in Part I are not. For this author they seemed the most efficient and most easily generalized way to formulate the notion of a transcendental function in the real variables context. There is certainly no claim to originality: the same construction has undoubtedly been used by many others for well over a century.

Semiderivations are but one aspect of the mathematical specialty of "differential algebra," which one can view as an approach to differential equations, both ordinary and partial, modeled on classical algebraic geometry. The algebraic foundations were formulated in a precise manner in the middle of the last century by J.F. Ritt and E.R. Kolchin (see [Kol] and the first line of the introduction to [Kap]). Even though the original edition was written almost 60 years ago, the cited book by Kaplansky is probably still the best entry point into the subject (although much of the terminology is outdated).

There are far deeper applications of differential algebra to number theory than are covered here. Specifically, see [Bo, Bu_1, Bu_2, Bu_3, Hru, P]. These references appeared in the last twenty years, but one can find earlier applications, e.g. logarithmic derivatives are used to derive number-theoretic results in the 1949 book [S] (see §10, pages 59-62).

Arithmetic derivations date back at the very least to 1961 [Ba]. I thank Peter Landesman for bringing [U-A] to my attention.

For general connections between abstract differential fields and fields of meromorphic functions see [S_1, S_2] and [M].

Additional results on semiderivations can be found in [Ch_2] (which was written before I was aware of [U-A]). In particular, in §5 of that reference the unique extension of a semiderivation on an integral domain is generalized to rings of fractions.

Further applications of differential algebra to elementary calculus can be found in [Ros_2]. (This paper is based on [Ros_1], which is generalized in [Ros_3].) In particular, there one can find a a definition of an "elementary function" and a proof that the function $x \mapsto (\sin x)/x$ cannot be integrated in terms of such functions. Addtional detail for [Ros_2] can be found in [Ch_1].

References

[Ba] E.J. Barbeau, Remarks on an Arithmetic Derivative, *Canad. Math. Bulletin*, **4**, (1961), 117-122.

[Bo] E. Bouscaren (Ed.), *Model theory and algebraic geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*, LNM **1696**, (1998), Springer-Verlag, New York.

[Bu_1] A. Buium, Differential Algebra and Diophantine Geometry, Hermann, Paris, 1994.

[Bu_2] A. Buium, Arithmetic analogues of derivatives, *J. Algebra*, **198**, (1997), 290-299.

[Bu_3] A. Buium, Arithmetic Differential Equations, *Mathematical Surveys and Monographs*, **18**, AMS, 2005.

[Ca] H. Cartan, *Elementary Theory of Analytical Functions of One or Several Complex Variables*, Addison-Wesley, Reading, MA, 1963.

[Ch_1] R.C. Churchill, *Liouville's Theorem on Integration in Terms of Elementary Functions*, posted on the website of the Kolchin Seminar in Differential Algebra, September, 2006.

[Ch_2] R.C. Churchill, *Differential Arithmetic*, posted on the website of the Kolchin Seminar in Differential Algebra, May, 2008.

[D] J. Dieudonné, *Foundations of Modern Analysis*, Academic Press, New York, 1969.

[Ell] J. Ellenberg, The Beauty of Bounded Gaps, *Slate*, posted 22 May 2013.

[Hru] E. Hrushovski, The Mordell-Lang Conjecture for Function Fields, *J. Amer. Math. Soc.*, **9**, (1996), 667-690.

[Hun] T.W. Hungerford, *Algebra*, GTM 73, Springer, New York, 1974.

[Kap] I. Kaplansky, *Introduction to Differential Algebra*, Second Edition, Hermann, Paris, 1976.

[Kol] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[Lang] S. Lang, *Algebra*, Revised Third Edition, GTM 211, Springer, New York, 2002.

[M] D. Marker, Model theory of differential fields, *Lecture Notes in Logic* 5, D. Marker et. al. eds., Springer-Verlag, New York, 1996.

[P] A. Pillay, Model Theory and Diophantine Geometry, *Bul. AMS,* **34**, no. 4, (1997), 405-422.

[Ros_1] M. Rosenlicht, Liouville's Theorem on Functions with Elementary Integrals, *Pac. J. Math.*, **24**, (1968), 153-161.

[Ros_2] M. Rosenlicht, Integration in Finite Terms, *Am. Math. Monthly*, **79**, (1972), 963-972.

[Ros_3] M. Rosenlicht, On Liouville's Theory of Elementary Functions, *Pac. J. Math.*, **65**, (1976), 485-492.

[S] C.L. Siegel, Transcendental Numbers, *Annals of Math. Studies*, **16**, Princeton University Press, Princeton, 1949.

[S_1] A. Seidenberg, Abstract Differential Algebra and the Analytic Case, *Proc. AMS*, **9**, (1958), no. 1, 159-164.

[S_2] A. Seidenberg, Abstract Differential Algebra and the Analytic Case II, *Proc. AMS*, **23**, (1969), no. 3, 689-691.

[U-A] V. Ufnarovski and B. Ahlander, How to differentiate a number, *Journal of Integer Sequences*, **6**, (2003), Article 03.3.4.

R.C. Churchill
Department of Mathematics
Hunter College and the Graduate Center of CUNY, and
the University of Calgary
August, 2013

e-mail rchurchi@hunter.cuny.edu