Supplementary topics for notes on set theory

There are three separate topics in this document, which is a supplement to the following notes:

http://math.ucr.edu/~res/math145A-2014/set-theory-notes.pdf

The first item (which consists of one page) describes all subrings of the rational numbers (subsets closed under addition, subtraction and multiplication) which contain the unit element, and the second item (which also consists of one page) proves an assertion in the exercises for Unit $\mathbf{VI}$ about the cardinal number of non – equivalent partial orderings for the nonnegative integers. Finally, the third item (which consists of the remaining $\mathbf{11}$ pages) discusses the meaning of the term ***transcendental functions***, which is frequently employed in calculus to describe a class of functions including exponential functions, trigonometric functions, and standard algebraic constructions on these examples. The word ***transcendental*** is meant to indicate that the functions in question are not algebraic in some sense (this usage goes back to Leibniz), but generally the textbook discussions are highly informal, and the main purposes of the third part are to give a precise definition of algebraic functions and to show that exponential and trigonometric functions are not algebraic (and by default are transcendental).

Subrings of the rational numbers

The proof of the following basic result is fairly elementary, but it is not always easy to find a proof in undergraduate algebra texts.

THEOREM. *Suppose that A is a subdomain of the rational numbers. Then there is a set of primes $\mathbf{S}$ such that A is isomorphic to the ring $\mathbf{Z}_{\mathbf{S}}$ generated by the integers and the inverses of all elements of $\mathbf{Z}$.*

The ring $\mathbf{Z}_{\mathbf{S}}$ consists of all fractions of the form a/b where a is an integer and b is a monomial in the elements of $\mathbf{S}$ (by convention, the monomial with zero factors is equal to 1, so the integers are contained in $\mathbf{Z}_{\mathbf{S}}$). It is straightforward to check that $\mathbf{Z}_{\mathbf{S}}$ is closed under addition and multiplication and hence is a subdomain of the rationals.

Proof. Since A is a subdomain it must contain both 0 and 1. Also, if n is a positive integer which lies in A, then it follows that $n+1$ also lies in A and hence A by induction A contains all positive integers. Since A is also closed under taking negatives, it also follows that all negative integers lie in A and therefore all of $\mathbf{Z}$ is contained in A.

Now let $A^{\times}$ is the group of units in A, and let $\mathbf{S}$ be the intersection of $A^{\times}$ with the set of positive primes. It follows immediately that A contains $\mathbf{Z}_{\mathbf{S}}$, so we only need to show the reverse inclusion.

We might as well assume that A strictly contains the integers, and hence it contains some rational number r/s where $r, s \in \mathbf{Z}$ and $s \neq 0$; of course we may choose r and s so that they have no common factors other than ± 1. Suppose now that we are given a rational number $k/n \in A$, where k and n are integers such that $n > 2$ and the greatest common divisor of k and n equals 1. By the Chinese Remainder Theorem we can find integers x and y such that $xk = yn + 1$ and therefore we have

$$\frac{1}{n} \quad = \quad \frac{xk - yn}{n} \quad = \quad x \cdot \frac{k}{n} \; - \; y \quad \in \quad A \; .$$

Suppose now that p is a prime divisor of n,and write $n = pq$. It then follows that

$$\frac{1}{p} \quad = \quad \frac{q}{n} \quad = \quad q \cdot \frac{1}{n} \quad \in \quad A$$

and hence $1/p \in \mathbf{S}$. In fact, this is true for **every** prime dividing n, and therefore we have $1/n \in \mathbf{Z}_{\mathbf{S}}$. The latter in turn implies that $k/n \in \mathbf{Z}_{\mathbf{S}}$, and therefore we see that the rational number k/n belongs to $\mathbf{Z}_{\mathbf{S}}$ as required.■

GENERALIZATION TO PRINCIPAL IDEAL DOMAINS. The proof of the theorem can be modified to yield a similar result if $\mathbf{Z}$ and $\mathbf{Q}$ are replaced by a prinicpal ideal domain D and its quotient field F.■

Supplement to VI.4 — Counting order types for a countably infinite set

By Exercise VI.4.6, the number of partial orderings on the set $\mathbf{N}$ of nonnegative integers is equal to $2^{\aleph_0}$, and there is an assertion that this is the same as the cardinality of the set of all order types of partial orderings on $\mathbf{N}$. The purpose here is to prove this fact.

As usual, one distinguishes order types using the properties of specific partial orderings. In fact, the examples of interest of us will all be **linear** orderings.

THE EXAMPLES. Let $A \subset \mathbf{N}$ be an arbitrary subset, and for each such subset A let S_A be given by the set

$$S \;=\; \mathbf{N} \,\cup\, \left(\bigcup_{a \in A} [2a, 2a+1] \,\cap\, \mathbf{Q} \right) .$$

Then each S_A is a subset of the rational numbers which contains the nonnegative integers $\mathbf{N}$, and as such each set S_A is countably infinite and has a linear ordering given by restricting the usual ordering of the rational numbers. We need to show that S_A and S_B have different order types if $A \neq B$. For this we need an auxiliary concept.

Definition. Let Y be a partially ordered set. A point $y_0 \in Y$ is said to be *left semi-isolated* if there is a greatest element of Y which is less than y_0, and the point y_0 is said to be *right semi-isolated* if there is a least element of Y which is greater than y_0.

If S_A is one of the sets described above, then we have the following:

> *The set of left semi-isolated points that are not right semi-isolated is the set of all points of the form $2a$ for some $a \in A$.*

Given a partially ordered set Y, let $\mathbf{SLSI}(Y)$ be the set of all $y \in Y$ that are left semi-isolated but not right semi-isolated (*i.e.*, the set of *strictly* left semi-isolated points). The following result is an immediate consequence of this observation and the definitions.

Proposition. *If U and V are partially ordered sets and $f : U \to V$ is an order-isomorphism, then f maps the set $\mathbf{SLSI}(U)$ onto the set $\mathbf{SLSI}(V)$. Similarly, f maps the set $\mathbf{SI}(U)$ of all left or right semi-isolated points in U onto the set $\mathbf{SI}(V)$ of all left or right semi-isolated points in V.*■

We can now show that S_A and S_B have different order types as follows. If $f : S_A \to S_B$ is an order-isomorphism, then f sends $\mathbf{N}$ to itself because $\mathbf{N} = \mathbf{SI}(S_A)$ and $\mathbf{N} = \mathbf{SI}(S_B)$. Furthermore, since $\mathbf{SLSI}(S_A)$ is equal to $\{n \in \mathbf{N} \mid n = 2a, \text{ some } a \in A\}$ and similarly the set $\mathbf{SLSI}(S_B)$ is equal to $\{n \in \mathbf{N} \mid n = 2b, \text{ some } b \in B\}$, it follows that a nonnegative integer n is equal to $2a$ for some $a \in A$ if and only if it is equal to $2b$ for some $b \in B$. But this means that $A = B$, and therefore we have shown that A must be equal to B if S_A and S_B have the same order type.■

NOTES ON TRANSCENDENTAL FUNCTIONS

Reinhard Schultz

September, 2005

The exponential and trigonometric functions are commonly described as transcendental functions. This name strongly suggests that such functions do not satisfy an identity of the form

$$a_n(x)f(x)^n \; + \; ... \; + \; a_1(x)f(x) \; + \; a_0(x) \quad = \quad 0 \quad (n \quad > \quad 0)$$

where each $a_k(x)$ is a polynomial in x and $a_n(x) \neq 0$. Observe that a function satisfies an identity of this form if and only if it satisfies an identity

$$b_n(x)f(x)^n \; + \; ... \; + \; b_1(x)f(x) \; + \; b_0(x) \quad = \quad 0 \quad (n \quad > \quad 0)$$

where each $b_k(x)$ is a rational function in x and $b_n(x) \neq 0$ (to get an expression with polynomial coefficients, multiply by the product of the denominators of all the nonzero coefficients). The purpose of these notes is to outline proofs of such statements.

I. Elementary methods and examples

We shall begin by defining algebraic and transcendental functions formally, and we shall explain how standard results on solutions of higher order linear differential equations and elementary trigonometric identities imply that e^x, $\sin x$ and $\cos x$ are transcendental.

I.1 : Basic definitions

Let J be an open interval in the real number line. We shall be interested in continuous functions on sets of the form $J - F$ where F (the **exceptional set**) is finite. One reason for choosing this setting is that every quotient of two polynomials (with a nonzero denominator) defines a function of this type. One important feature of such functions is that they can be added and multiplied (at the expense of making the exceptional sets larger).

Definition. In the setting above, a continuous function f with on an interval J with a finite exceptional set is *algebraic* if there is a strongly nontrivial polynomial in two variables $P(x, y)$ such that $P\big(x,\, f(x)\big)$ is identically zero (if one excludes the finite exceptional set of f). The term "strongly nontrivial" means that P cannot be expressed entirely in terms of powers of x (hence is a genuine polynomial in two variables). A continuous function f with on an interval J with a finite exceptional set is *transcendental* if it is not algebraic.

EXAMPLES. Polynomial functions are automatically algebraic, for one can take $P(x,y) = y - f(x)$. Radical functions of polynomials are also algebraic; for example, if $f(x) = \sqrt{1+x^2}$ then we can take $P(x,y) = 1 + x^2 - y^2$; we shall discuss this point further in Part II. Rational functions are also algebraic, for if $f(x) = p(x)/q(x)$ where p and q are nonzero, then we can let $P(x,y) = q(x)y - p(x)$.

Notational point. Sometimes a function is said to be algebraic if it can be obtained from a polynomial by a finite number of steps involving addition, subtraction, multiplication, nonzero division, and taking n^{th} roots for an arbitrary positive integer n. We shall call such objects **radical functions**. The difference between radical functions and those that are algebraic in our sense will be described in Part II of these notes.

The first result gives a criterion for a function to be transcendental in terms of linear independence of functions.

PROPOSITION. *Let the function f be given as above. Then f is transcendental if and only if for all positive integers N the set of all functions*

$$x^j f(x)^k \qquad (0 \;\leq\; j,k \;\leq\; N)$$

is linearly independent.

Proof. We shall prove that f is algebraic if and only if the set of functions as above is linearly dependent for some N. The $(\Longrightarrow)$ implication is clear, for a strongly nontrivial polynomial identity implies a nontrivial linear combination of the functions as above is equal to zero. Conversely, if one has the linear dependence property for some N, then this yields a strongly nontrivial polynomial identity $P\big(x,\ f(x)\big) = 0$; the reason one must have a strongly nontrivial polynomial is because the functions $\{1, x, x^2,\ \ldots\ \}$ are linearly independent.■

The following elementary observation will be helpful at some points.

PROPOSITION. *Suppose that f is a continuous function defined on an open interval J with finitely many exceptions, and let J' be a subinterval of J. If f is algebraic, then so is the restriction of f to J' (with finitely many exceptions). Likewise, if the restriction of f to J' is transcendental, then f is also transcendental.*

Proof. The second statement is just the contrapositive of the first, so it is only necessary to verify the latter. But if one has an identity of the form $P\big(x,\ f(x)\big) = 0$ on J with finitely many exceptions, then the same is clearly true on J'.■

There is a partial converse to the preceding result.

PROPOSITION. *Suppose that f and J are as above such that f is defined at every point of J, and assume in addition that near each point $a \in J$ it is possible to express f as a convergent power series in powers of $x - a$. Then f is algebraic if and only if the restriction to some subinterval J' is algebraic.*

We shall prove this in Section 4 and give examples to show that the conclusion fails without the assumption about power series expansions.

Examples. If $f(x) = |x|$, then $y = f(x)$ satisfies the polynomial identity $y^2 - x^2$, so y is algebraic. Since the existence of a convergent power series expansion near a point a implies infinite differentiability at a, it is also clear that f has no convergent power series expansion at 0. One can construct similar examples of the form $|x|x^k$ which have derivatives of arbitrarily high finite order and are algebraic but also do not have convergent power series expansions at 0.

It is also possible to construct nonzero functions which are algebraic in our sense but are equal to zero on some subinterval. For example, consider the function $f(x) = x + |x|$. This function is equal to zero for $x \leq 0$ and is equal to $2x$ for $x \geq 0$, and it is algebraic because $y = x + |x|$ implies $y - x = |x|$, so that $(y - x)^2 = x^2$ and hence $y^2 - 2yx = 0$.

Useful observation. The discussion of this section works for complex valued functions as well as real valued functions.∎

Additional basic formalism

We shall conclude this section by formalizing things a little more and making some observations that will be useful later.

Definition. Let J be an open interval in the real numbers. Then $\mathbf{C}^{\#}(J)$ is defined to be the set of all continuous functions f defined on some set of the form $J - F(f)$, where $F(f)$ is some finite subset of J which depends upon f.

LEMMA. *Let f be a rational function defined as the quotient of two polynomials p/q where q is not the zero polynomial. Then f determines an element of $\mathbf{C}^{\#}(J)$.*

Proof. In this case the set of exceptional points is given by the roots for q which lie in the interval J. Since q is nonzero, it has only finitely many roots.∎

The ideas in the preceding argument also yield the following important conclusions.

PROPOSITION. *Let $\mathbf{R}(x)$ be the algebra of rational forms over the real numbers;* i.e., *all quotients p/q where p and q are real polynomials such that $q \neq 0$ and with $p/q = r/s$ if and only if $ps = qr$. Then the following hold:*

(i) The map $\mathbf{R}(x) \to \mathbf{C}^{\#}(J)$ sending each rational form to the associated continuous function is $1-1$.

(ii) The algebra $\mathbf{C}^{\#}(J)$ is a vector space over the field $\mathbf{R}(x)$.

Proof. Clearly the map from $\mathbf{R}(x)$ to $\mathbf{C}^{\#}(J)$ sends sums to sums and products to products. In particular, it is a linear transformation of vector spaces over the real numbers, and therefore by standard results in linear algebra the proof of (i) reduces to showing that the kernel is equal to $\{0\}$. However, if $p(x)/q(x) = 0$ for all but finitely many $x \in J$, then multiplication by the nonzero polynomial q shows that $p(x)$ is also equal to 0 for all but finitely many $x \in J$. Since the complement of a finite set in J is infinite and nonzero polynomials have only finitely many roots, it follows that p must be the zero polynomial, which means that f must also be equal to zero.

The truth of the second conclusion follows immediately from the standard rules of algebra which apply in $\mathbf{C}^{\#}(J)$.∎

The preceding leads to the following abstract characterization of algebraic functions.

COROLLARY. *In the setting above, a function is algebraic if and only if it is the root of some polynomial with coefficients in $\mathbf{R}(x)$.*∎

I.2 : Exponential functions

The first proposition of the previous section leads directly to a proof of the following (expected) conclusion.

THEOREM. *Let $a \neq 0$ be an arbitrary real or complex number. Then the function e^{ax} is transcendental over an arbitrary open interval J.*

Proof. We need to show that for all positive integers N the functions $x^j \exp(kax)$, where $0 \leq j, k \leq N$ are linearly independent over J.

This follows immediately from basic facts about solutions to homogeneous linear differential equations with constant coefficients. All the functions described above are solutions to the equation

$$D^{N+1}(D-a)^{N+1}(D-2a)^{N+1}...(D-Na)^{N+1}y \quad = \quad 0$$

and standard results about Wronskians for such solutions show that the family described in the previous paragraph is linearly independent on an arbitrary interval J. Further details on these points appear in the book by Trench cited in the references.■

I.3 : Sines and cosines

We would like to prove an analogous result for sine and cosine functions, where we shall now assume that the interval J is **bounded**. In order to prove this we need some general comments about trigonometric identities for powers of $\sin x$ and $\cos x$.

It is well known that $\sin^k x$ and $\cos^k x$ are (finite) linear combinations of the functions $\sin nx$ and $\cos mx$ for $m, n \leq k$. We shall prove these assertions here, both for the sake of completeness and because we need a small amount of specific information about the formulas themselves. In order to do things quickly we shall use the standard identity

$$e^{ix} \quad = \quad \cos x \;+\; i\,\sin x$$

and the corresponding expressions for $\sin x$ and $\cos x$ as complex linear combinations of $e^{\pm\, i\, x}$.

In particular, the identities in the preceding sentence imply that

$$\sin^k x \quad = \quad \left(\frac{e^{ix}-e^{-ix}}{2i}\right)^k \quad = \quad \frac{1}{2^k i^k}\cdot\left[e^{ikx}+(-1)^k e^{-ikx}\right] \;+\; \frac{1}{2^k i^k}\cdot\sum_{\ell=1}^{k-1}\binom{k}{\ell}(-1)^\ell e^{i(2\ell-k)x} \quad =$$

$$Af(x) \;+\; B(x)$$

where A is a nonzero constant, the function $f(y)$ is given by $\cos ky$ if k is even and $\sin ky$ if k is odd, and $B(x)$ is a linear combination of terms involving $\sin px$ and $\cos qx$ where p and q are integers in the interval $[2-k, k-2]$. A similar expansion holds for $\cos^k x$ except that the lead term is always a nonzero constant times $\cos kx$.

We now need to show how one can use such formulas to prove that the functions $x^p \sin^q x$ and $x^m \cos^n x$ are linearly independent for $0 \leq m, n, p, q \leq k$.

Let V_r be the set of all trigonometric functions that are linear combinations of $\sin px$ and $\cos qx$ for $0 \leq p, q \leq r$. By the preceding discussion we have that

$$\begin{aligned} \sin^{r+1} x &= A \cdot f\big((r+1)x\big) + F_r(x) \\ \cos^{r+1} x &= A \cdot \cos(r+1)x + G_r(x) \end{aligned}$$

where $F_r, G_r \in V_r$.

We shall now apply the preceding observations and the methods of the previous section to the sine and cosine functions.

THEOREM. *For each open interval J, the functions $\sin x$ and $\cos x$ are transcendental on J.*

Proof. In this case a Wronskian argument shows that the set of all products of the form $x^p \sin qx$ and $x^m \cos nx$, where $0 \leq m, n, p, q \leq n$, is linearly independent (after eliminating obvious redundancies). Standard computations show that these functions form a basic set of solutions for the following differential equation:

$$D^{r+1}(D^2 - 1)^{r+1}(D^2 - 2)^{r+1} \ldots (D^2 - r)^{r+1} y = 0$$

The preceding discussion and the trigonometric identities provide the raw material for proving that the sets

$$\{\ x^p \sin^q x \mid 0 \leq p, q, \leq N\ \}$$

$$\{\ x^p \cos^q x \mid 0 \leq p, q, \leq N\ \}$$

are linearly independent, but some additional notation is also necessary. Let $H_{m,n,T}(x) = x^m\, T(nx)$ where $T(u) = \sin u$ or $\cos u$, and order these functions lexicographically with $\cos u$ preceding $\sin u$. Similarly take the lexicographic orderings on the functions $K_{m,n}(x) = x^m \sin^n x$ and $L_{m,n}(x) = x^m \cos^n x$. Define $W_{m,n}$ to be the subspace spanned by the functions $H_{p,q,T}(x)$ where both $p \leq m$ and $q \leq n$, and in addition either $p < m$ or $q < n$. Then the trigonometric identities imply that $K_{m,n}$ does not lie in the subspace $W_{m,n}$ but all functions which precede it in the sequence do lie in that subspace. This means that the set of functions $K_{p,q}$ up to and including $K_{m,n}$ is linearly independent for all m and n. The same considerations apply to show that the set of functions $L_{p,q}$ up to and including $L_{m,n}$ is linearly independent for all m and n. Thus it follows that both of the sets of functions displayed above are linearly independent.■

I.4 : Restriction principle

In this section we shall prove a result stated in Section 1 regarding conditions under which one can detect whether a function is algebraic by restricting to a subinterval. Once again we introduce some formalism.

Definition. Let J be an open interval in the real numbers. A function f defined on J is said to be real analytic if for each point $a \in J$ there is an interval $(a-r, a+r) \subset J$ such that $f|(a-r, a+r)$ has a convergent power series expansion of the form $\sum_k\ c_k(x-a)^k$.

Here are some basic properties of real analytic functions that we shall use.

FACT 1. *If f has a convergent power series expansion on an interval of the form $(b - h, b + h)$, then f is real analytic on the latter interval.*

This may seem tautological but it is not. One needs to show that for each a in the interval one can find a convergent power series expansion in terms of powers of $(x - a)$. The most direct approach is simply to exploit the identity

$$(x - b)^k \quad = \quad \sum_{\ell=0}^{k} \binom{\ell}{k} (x - a)^\ell (a - b)^{k-\ell} \ .$$

Formally this yields an expansion in terms of powers of $(x - a)$ from the expansion in terms of powers of $(x - b)$. It is then necessary to prove that the formally derived power series actually has a positive radius of convergence.■

FACT 2. *If f is given as in the previous statement and $P(x, y)$ is a polynomial in two variables, then*

$$g(x) \quad = \quad P\big(\, x, \, f(x)\,\big)$$

also has a convergent power series expansion on the interval $(b-h, b+h)$ and hence is real analytic on that interval.

Once again it is not difficult to figure out what the power series for the function $g(x)$ should be, but after doing so it is necessary to prove that it works.■

FACT 3. *If f is once again given as in the previous statements and f is not identically zero, then the zeros of f are isolated; in other words, if $f(a) = 0$ then there exists some $\delta > 0$ such that f is never zero on $(-\delta, a) \cup (a, \delta)$.*

The first key step in verifying Fact 3 is to show that if $f(a) = 0$ then there exists some $\delta > 0$ such that either f is never zero on $(-\delta, a) \cup (a, \delta)$ or else f is identically zero on that interval. — One proves this by looking at a power series expansion at a on some interval of radius equal (say) to r. If all the coefficients of the powers of $(x - a)$ vanish, then it follows that f is identically zero on the interval. If some coefficient does not vanish, then one can use Taylor's Formula and the infinite differentiability of f to show that for all points in some small subinterval of radius (say) δ, the only solution to the equation $f(x) = 0$ is $x = a$.

The argument in the preceding paragraph shows that either a is an isolated zero of f or else there is an open subinterval J_0 containing a such that $f = 0$ on all of a. To complete the argument, it is necessary to prove that the second alternative implies $f = 0$ at all points of the original interval.

It is easy to do this with a few tools from point set theory but very difficult otherwise, so we shall give the proof using concepts from point set theory; a reader who wishes to accept this step without proof may do so because we shall not use it subsequently. The proof is based upon the following property of an open interval which follows from connectedness (compare Rudin, *Principles of Mathematical Analysis*):

> It is not possible to split an open interval into two nonempty pairwise disjoint open subsets (*i.e.*, each point lies in an open interval entirely contained in one of the subsets).

Let J be the interval on which f is defined, and let B be the set of points x such that at least one of the quantities $f^{(k)}(x) \neq 0$ for some $k \geq 0$. By the continuity of f and all its derivatives, this set is open. Let C be the set of points where all the above quantities vanish. By the observations of the preceding paragraph, this set is also open, and by construction it is disjoint from C. If the second alternative in the previous paragraph holds, then C is nonempty, and therefore by the connectedness property of J it follows that $C = J$, which means that $f = 0$ everywhere.■

We are now ready to prove the result stated in Section 1.

PROPOSITION. *Suppose that f and J are as above such that f is defined at every point of J, and assume in addition that near each point $a \in J$ it is possible to express f as a convergent power series in powers of $x - a$. Then f is algebraic if and only if the restriction to some subinterval J' is algebraic.*

As noted in Section 1, if f is algebraic then it follows that the restriction to every subinterval is algebraic.

Proof. Let J' be the interval on which f is algebraic, and let P be a polynomial in two variables such that

$$0 \quad = \quad P\big(x,\, f(x)\big)$$

for all $x \in J'$. As noted in Fact 2, the expression on the right hand side defines a real analytic function on all of J, and we have seen that it is zero on J'. Therefore by Fact 3 this function is equal to 0 at all points of J. This proves one direction of the implication. The other was established in Section 1.■

Example. Consider the function $(x + |x|)e^x$. The restriction of this function to $(-1, 0)$ is equal to 0 and hence is algebraic. On the other hand, the restriction to $(0, 1)$ is equal to $2xe^x$, and this function is transcendental (if it were algebraic, then e^x would also be algebraic. Therefore one cannot generalize the proposition to arbitrary continuous functions. There are similar examples for functions with k continuous derivatives, where k is an arbitrary positive integer (and there are even infinitely differentiable examples, but they are a little more complicated to construct and analyze).

II. More advanced methods and examples

In this part of the notes we shall approach the topic from a slightly more advanced standpoint using algebraic tools from the theory of extension fields and some Galois theory. One application will be proofs that the remaining trigonometric functions, the inverse trigonometric functions, and the logarithmic functions are transcendental. Another will involve the relation between algebraic functions and the radical functions described in Part I. In particular, we shall define an infinitely differentiable algebraic function that cannot be expressed in terms of addition, subtaction, multiplication, nonzero division, and taking n^{th} roots for arbitrary positive integers n.

II.1 : Some general observations

At the end of Section I.1 we mentioned that the space $\mathbf{C}^{\#}(J)$ of functions under consideration is a vector space over the field $\mathbf{R}(x)$ of rational forms or functions in the indeterminate x with respect to the usual algebraic operations. One can characterize the algebraic functions very simply in terms of this vector space structure.

PROPOSITION. *A function $f \in \mathbf{C}^{\#}(J)$ is algebraic if and only if the span of the k-fold power functions f^k for $k \geq 0$, viewed as an $\mathbf{R}(x)$-vector subspace, is finite-dimensional.*

Note on terminology. Throughout Part II we shall notation like f^k to denote the k-fold algebraic product (and not a k-fold composite).

Proof. A nontrivial polynomial identity

$$0 \quad = \quad P\big(x,\, f(x)\big)$$

implies that some function f^m is a linear combination of the lower powers, and by induction every higher power is also a linear combination of these lower powers. Thus the subspace spanned by the powers of f is actually spanned by the powers $1, f, ... f^{m-1}$. Conversely, if f is algebraic, then a polynomial identity of the form

$$a_n(x)f(x)^n \;+\; ... \;+\; a_1(x)f(x) \;+\; a_0(x) \quad = \quad 0 \quad (n \;>\; 0)$$

with $a_n \neq 0$ will imply that f^n is a linear combination of the lower powers of f with coefficients in $\mathbf{R}(x)$.■

COROLLARY 1. *Let f be as above, assume f is algebraic, and suppose further that g is a polynomial in f. Then g is also algebraic.*

Proof. Let W be the subspace spanned by the powers of f and let W_1 be the subspace spanned by the powers of g. By the proposition we know that W is finite-dimensional, and therefore its subspace W_1 is finite-dimensional, which in turn means that g is algebraic.■

COROLLARY 2. *Let f be as in the proposition, and let g be a nontrivial polynomial such that $g^\circ f$ is algebraic. Then f is algebraic.*

Proof. Let E be the subfield generated by the powers of $g \circ f$, so that E is finite-dimensional over $\mathbf{R}(x)$ by the hypothesis. If K is the subfield generated by E and the powers of f, then $g \circ f \in E$ implies that K is finite-dimensional over E. By the product formula for iterated extension fields, it follows that K is also a finite-dimensional extension of $\mathbf{R}(x)$. By construction it contains all the powers of f, and therefore the subfield generated by the latter is a finite-dimensional extension of $\mathbf{R}(x)$.■

The following change of variables formula is also useful for certain purposes.

PROPOSITION. *Suppose that f is a continuous strictly increasing function on the interval J and that $g = f^{-1}$. If f is algebraic on J, then g is algebraic on $f(J)$.*

Proof. Suppose we have

$$0 \quad = \quad P\big(x,\, f(x)\big)\ .$$

Then we also have

$$0 \quad = \quad P\big(g(y),\, y\big)\ .$$

Conversely, if the second equation is true then so is the first.■

COROLLARY. *The natural logarithm function (and in fact the logarithmic function for an arbitrary nontrivial base) is transcendental).*

This follows immediately from the proposition and the fact that the natural logarithm and exponential functions are inverse to each other.■

II.2 : The remaining trigonometric functions

The results of the preceding section will be used to prove that the remaining four basic trigonometric functions and their standard inverses are all transcendental.

PROPOSITION. *The functions* $\sec x$ *and* $\csc x$ *are transcendental.*

Proof. Suppose that $0 = P(x, \sec x) = \sum_{j,k}\ c_{i,j}\, x^j \sec^k x$. If we multiply through by some large power of the cosine function this becomes

$$0 \quad = \quad \sum_{j,k} c_{i,j}\, x^j \cos^{M-k} x$$

and hence the function $\cos x$ would be algebraic if $\sec x$ were algebraic. Similar considerations work for the cosecant function.■

PROPOSITION. *The functions* $\tan x$ *and* $\cot x$ *are transcendental.*

Proof. Once again, if we can prove this for the tangent function the same sort of proof will work in the other case.

If $f(x) = \tan x$ were algebraic, then the same would be true for $1 + f(x)^2 = \sec^2 x$. However, we have just shown that $\sec x$ is transcendental, and hence the same must be true for its square, and consequently it follows that $\tan x$ must be transcendental.■

COROLLARY. *The inverse trigonometric functions are all transcendental.*

Proof. Apply the final proposition from the previous section.■

II.3 : Radical functions and algebraic functions

The purpose of this section is to prove the following.

THEOREM. *There is an infinitely differentiable algebraic function* $f : \mathbf{R} \to \mathbf{R}$ *such that* f *is not a radical function.*

This example is related to the fact that there is no quintic formula giving the roots of an arbitrary fifth degree equation in terms of the four basic arithmetic operations and extractions of roots.

We begin by formalizing the notion in the final clause of the previous sentence.

Definition. A function f is a *radical function* if it lies in a finite extension of $\mathbf{R}(x)$ by radicals inside $\mathbf{C}^{\#}(J)$.

It follows immediately that radical functions are algebraic functions. The point of this section is that the converse is not true.

BASIC EXAMPLE. Let $f(x) = x^5 + x^3 + x$. The derivative of this function is $5x^4 + 3x^2 + 1$, which is positive, and hence f is always strictly increasing. Taking limits as $x \to \pm\infty$ we see that f maps $\mathbf{R}$ onto itself. Therefore there is an inverse function g, and hence by the final proposition of Section II.1 this inverse function $g = f^{-1}$ is algebraic.

If g were a radical function then one could express the unique solution to $g(y) = -1$ in terms of the standard four arithmetic operations and extraction of roots. In the terminology of Galois theory, the equation $h(x) = x^5 + x^3 + x + 1$ would be solvable in radicals. We shall use Galois theory in a fairly standard fashion to show this is impossible.

The standard method for showing such an equation is not solvable by radicals is fairly classical and can be found in Section 61 of the second edition of van der Waerden's *Modern Algebra*. According to the methods developed there, it is only necessary to prove the following result:

CLAIM. *The polynomial* $h(x) = x^5 + x^3 + x + 1$ *is irreducible over the integers modulo* 3.

In order to prove this is irreducible over the ring $\mathbf{Z}_3$ of integers mod 3, it suffices to show it has no linear or quadratic factors. Linear factors correspond to roots over $\mathbf{Z}_3$, and it is easy to check there are no such roots, so all we have to do is eliminate the possibility of quadratic factors. We shall do so in an elementary but slightly tedious manner.

There is a field $\mathbf{F}_9$ with exactly 9 elements which contains $\mathbf{Z}_3$ and also contains a square root i of -1. This is true because $x^2 + 1$ has no roots in $\mathbf{Z}_3$. If there are irreducible quadratic factors, the theory of finite fields implies that there must be a root for $h(x)$ mod 3 in the field $\mathbf{F}_9$. Every element in $\mathbf{F}_9$ is uniquely expressible in the form $a + b\,i$ where $a, b \in \mathbf{Z}_3$. One can check directly that none of these elements can be a root of the polynomial $h(x)$ reduced mod 3; an argument of this sort is definitely not elegant, but it works and does not require additional digressions.■

REFERENCES

W. F. Trench, *Elementary Differential Equations*. Brooks/Cole (Thomson Learning), Pacific Grove CA, 2000. ISBN: 0-534-36841-7.

B. L. van der Waerden. *Modern Algebra, Vol. 1* (Transl. from the 2^{nd} Rev. German Ed. by F. Blum). Ungar, New York, 1953.