Down the River: Foundations for Scholarship

Alex Elzenaar

August 14, 2018

Contents

Preface

This set of notes is an introduction to the shallower foundations of mathematics, for those students who are attempting the New Zealand Scholarship examination in Calculus.

I assume knowledge of the breadth of Level 2, but not any material from Level 3. As a guideline, I would expect any student attempting Scholarship to come into Level 3 with the following skills:

- Comfort with basic algebraic manipulations.
- Understanding of exponential and logarithmic functions.
- Understanding of quadratic equations (especially with the link between parabolae and quadratics, and factoring).
- Knowledge of the links between functions and their graphs (in general; particularly, being able to give some kind of definition and knowledge of some basic examples).
- Comfort with the geometry underlying the derivative (slopes of lines, average slopes of curves, and the ability to apply the derivative in geometric situations like finding turning points). [This skill is not explicitly required for these notes.]

Section 1: Set Notation

1.1 Defining Sets

We begin by quoting from Paul Halmos' classic book, *Naive Set Theory.*

> A pack of wolves, a bunch of grapes, or a flock of pigeons are all examples of sets of things. The mathematical concept of a set can be used as the foundation for all known mathematics...
>
> (Halmos)

Like Halmos, we will avoid an exact definition of sets so that we do not need to deal with the logical issues that come with it (does the set of all sets that do not contain themselves contain itself?) — for us, a set is simply a collection of objects.

We can write down a set by placing the names of the objects within the set (the **elements** of the set) inside curly brackets; for example,

$$S = \{1, 2, 3\} \tag{1.1}$$

is a set consisting of three elements. If x is an element of a set S, then we write $x \in S$ (x is in S); otherwise, we can write $x \notin S$.

There are several 'standard' sets:

- $\mathbb{N} = \{1, 2, 3, ...\}$ is the set of natural numbers.
- $\mathbb{N}_0 = \{0, 1, 2, ...\}$ is the set of natural numbers together with zero.
- $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ is the set of integers.[1]
- $\mathbb{Q}$ is the set of rational numbers (that is, all numbers x which can be written in the form a/b for a and b integers).
- $\mathbb{R}$ is the set of real numbers (that is, all possible lengths that can be measured along an infinite line[2]).
- $\emptyset$ is the set containing no elements.

If we construct a set using a rule, then we have another notation: if E is the set containing all even numbers, then we can write

$$E = \{n : n \text{ is an even number}\}. \tag{1.2}$$

This notation is called **set-builder notation**; if $S = \{x \in \mathcal{U} : P(x) \text{ is true}\}$, then we read it as '$S$ is the set of all x in $\mathcal{U}$ such that $P(x)$ is true'.

If S and T are sets such that every element of T is also an element of S, then we say that T is a **subset** of S (or that S **includes** T), and write $T \subseteq S$. In particular, we have $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

1.3 Exercise. Let X be some set. Prove that $\emptyset \subseteq X$, and that $X \subseteq X$.

1.2 Set Operations

If S and T are two sets, then their **intersection** is the set

$$S \cap T = \{x : x \in S \text{ and } x \in T\} \tag{1.4}$$

and their **union** is the set

$$S \cup T = \{x : x \in S \text{ or } x \in T\}. \tag{1.5}$$

1.6 Example. If $S = \{2, 4, 6, 8, 10, 12\}$ and $T = \{1, 4, 9, 16\}$, then $S \cup T = \{1, 2, 3, 6, 8, 9, 10, 12, 16\}$ and $S \cap T = \{4\}$.

[1] The letter Z comes from the German *Zahlen* (number).

[2] There are more rigorous definitions of the real numbers than this, but we do not need to worry too much about defining them properly.

1.7 Exercise (Distributivity)**.** Show that, if R, S, and T are sets, then

1. $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$, and
2. $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$.

Draw Venn diagrams to show each configuration.

Now, suppose S is a subset of $\mathcal{U}$. The **compliment** of S in $\mathcal{U}$ is the set of all elements of $\mathcal{U}$ that are not in S; in other words,

$$\mathcal{U} - S = \{x \in \mathcal{U} : c \notin S\}. \tag{1.8}$$

If the set $\mathcal{U}$ is clear from context, we can just write S^C or $\overline{S}$ in place of $\mathcal{U} - S$.

1.9 Exercise (de Morgan's laws)**.** Show that, if R and S are subsets of $\mathcal{U}$, then

1. $\overline{R \cup S} = \overline{R} \cap \overline{S}$, and
2. $\overline{R \cap S} = \overline{R} \cup \overline{S}$.

Draw Venn diagrams to show each configuration.

1.3 Functions

We also define the **Cartesian product** of S and T by

$$S \times T = \{(s,t) : s \in S, t \in T\} \tag{1.10}$$

where (s,t) denotes the ordered pair with s in the first position and t in the second; i.e. $(s,t) = (t,s)$ if and only if $s = t$.

A **function** f with **domain** D and **codomain** C (or a function **from** D **(in)to** C) is a subset of $D \times T$ such that if $(x,y_1) \in f$ and $(x,y_2) \in f$ then $y_1 = y_2$. When defining such a function, we can write that $f : D \to C$. If $(x,y) \in f$, we usually write $f(x) = y$.

The set $R = \{r \in C : f(x) = r \text{ for some } x \in D\}$ is called the **range** of f. If $R = C$ (that is, for every value y in the codomain there is some x in the domain so that $f(x) = y$), then the function is called **surjective** or **onto**.

If $f(x_1) = y$ and $f(x_2) = y$ implies that $x_1 = x_2$ (that is, if every member y of the range has precisely one corresponding element x of the domain so that $f(x) = y$) then the function is called **injective** or **one-to-one**.

We say that $f : A \to B$ and $g : C \to D$ are **equal**, writing $f = g$, if and only if both of the following conditions are met:

1. $A = C$ and $B = D$; and
2. For every $x \in A$, $f(x) = g(x)$.

1.11 Example.

1. If $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 3x + 1$, then f is one-to-one and onto.
2. If $g : \mathbb{N} \to \mathbb{N}$ is defined by $f(x) = x + 1$, then f is one-to-one but not onto, since there is no $x \in \mathbb{N}$ such that $1 = x + 1$.

1.12 Theorem. [3] *Let $f : D \to C$ be a function, and let $R \subseteq C$ be the range of f. Then f is one-to-one and onto if and only if there exists a function $g : C \to D$ so that for every $x \in D$, $x = g(f(x))$ and for every $y \in C$, $y = f(g(y))$. This function g is unique.*

Proof. [4] Suppose f is one-to-one and onto. Since f is one-to-one, we can define a new function g so that $g(y) = x$ if and only if $f(x) = y$: since if $g(y) = x_1$ and $g(y) = x_2$, we have $f(x_1) = y = f(x_2)$ and $x_1 = x_2$ by the injectivity of f. This new function g has domain $R = C$ (since f is onto, the two sets are equal) and range D. In particular, if $x \in D$, $f(x) = y$ for some $y \in R$ and hence $x = g(y) = g(f(x))$. Similarly, if $y \in R$, then there exists $x \in D$ such that $f(x) = y$ and so $g(y) = x$; hence $f(g(y)) = y$.

[3] **Theorem**: A statement which has been proved to be true.

[4] **Proof**: A valid argument, from true premises, to obtain a conclusion. The symbol □ denotes the end of a proof.

Conversely, suppose such a g exists. Suppose $f(x_1) = f(x_2) = y$ for some $x_1, x_2 \in D$ and $y \in R$. Then $g(f(x_1)) = g(y)$, so $g(y) = x_1$. Similarly, $g(f(x_2)) = g(y)$ so $g(y) = x_2$. Hence $x_1 = x_2$ and f is injective. Let $y \in C$; then $y = f(g(y))$, and so there exists $x = g(y)$ so that $f(x) = y$; hence $y \in R$, so $C = R$ and f is onto.

Suppose for uniqueness that both g_1 and g_2 satisfy the requirements of the theorem. Then for every $y \in R$, $y = f(g_1(y)) = f(g_2(y))$. But since f is injective, $g_1(y) = g_2(y)$; and since g_1 and g_2 have the same domain and codomain, and agree at every point, they are equal. □

The unique function g defined as in the theorem for some function f is called the **inverse** of f, and we usually write $g = f^{-1}$.

1.13 Exercise. Show that, if f^{-1} is the inverse of f, then f^{-1} has an inverse and that inverse is f.

Section 2: Divisibility

Let a and b be integers. We say that a **divides** b (or a is a **factor** of b) if there is some integer q such that $b = aq$; we write $a \mid b$.

2.1 Lemma. [5] *Let a, b, and c be integers. Then:*

1. $a \mid 0$.
2. *If $a \mid b$, and $b \mid c$, then $a \mid c$.*
3. *If $a \mid b$, and $a \mid c$, then $a \mid (b + c)$.*
4. *If $a \mid b$, then $a \mid bc$.*

Proof.

1. We must find an integer q so that $0 = qa$. Let us simply take $q = 0$; then $0 = 0a$ for all a, so $a \mid 0$.
2. Because $a \mid b$, there exists some integer q so that $b = qa$. Similarly, there exists some integer r so that $c = rb$. Putting these together, $c = rb = r(qa) = (rq)a$; so $a \mid c$.
3. Because $a \mid b$, there exists some integer q so that $b = qa$. Similarly, there exists some integer r so that $c = ra$. Adding these, we have that $b + c = qa + ra = (q + r)a$, and so $a \mid (b + c)$.
4. Because $a \mid b$, there exists some integer q so that $b = qa$. Hence $bc = c(qa) = (cq)a$ and so $a \mid bc$.

□

From this point, lower case italic letters will always denote integers unless otherwise stated.

2.2 Corollary. [6] *If $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$, then*

$$d \mid (c_1a_1 + c_2a_2 + \cdots c_na_n)$$

for any integers c_1, ..., c_n.

Proof. By the definition of divisibility, there exist integers q_1, ..., q_n such that $a_1 = q_1d$, ..., $a_n = q_nd$. Hence

$$c_1a_1 + \cdots + c_na_n = c_1q_1d + \cdots + c_nq_nd = d(c_1q_1 + \cdots + c_nq_n)$$

and so the result holds. □

2.3 Exercise. Show that if $a \mid b$, and a and b are positive, then $a \leq b$. Show that this result does not always hold if a and b are non-negative.

2.4 Exercise. If n is an integer, define the **absolute value** of n by

$$|n| = \begin{cases} n & \text{if } n \geq 0 \\ -n & \text{if } n < 0. \end{cases}$$

Show that $|n| \mid n$ and $n \mid |n|$.

2.5 Definition. If a and b are integers, then the integer d is called the **greatest common divisor** of a and b (written $d = (a, b)$) if the following two conditions are met:

1. $d \mid a$ and $d \mid b$ (that is, d is a common divisor of both numbers).
2. If $d' \mid a$ and $d' \mid b$, then $d' \leq d$ (that is, every other common divisor is less than d).

2.6 Example.

1. Since for every a and b we have $1 \mid a$ and $1 \mid b$, it follows that $(a, b) \geq 1$.

[5] **Lemma**: A statement which is proved on the way to a more important result. (Plural: lemmata.)

[6] **Corollary**: A proof which is a direct result of an earlier proof.

2. The greatest common divisor of -3 and 5 is $(-3, 5) = 1$, since $1 \mid -3$ and $1 \mid 5$ but no integer larger than 1 divides both.

3. We also have $(4, 14) = 2$ and $(24, 36) = 12$.

4. For all integers n, $(n, 1) = 1$ (since the only integers dividing 1 are ± 1, and $1 > -1$).

5. For all integers n, $(n, 0) = |n|$ (since $|n| \mid 0$ and $|n| \mid n$, so $(n, 0) \geq |n|$; and no divisors of n are greater than $|n|$, so $(n, 0) \leq |n|$).

2.7 Exercise. Let d be an integer. Prove that if d is a positive integer, then $(d, nd) = d$; and if d is negative, then $(d, nd) = -d$.

If $(a, b) = 1$, then a and b are called **coprime** or **relatively prime**.

2.8 Theorem. *If $(a, b) = d$, then a/d and b/d are coprime.*

This theorem is intuitive: if we divide two numbers out by their greatest common divisor, they no longer have any common divisors greater than 1. This observation essentially proves itself.

Proof. We must show that $(a/d, b/d) = 1$. Let $(a/d, b/d) = c$. Then $c \mid a/d$ and $c \mid b/d$; so there exist q_1 and q_2 such that $a/d = cq_1$ and $b/d = cq_2$; hence $a = cq_1 d$ and $b = cq_2 d$. This implies that cd is a common divisor of a and b, and so $cd \leq d$. Since $d = (a, b) \geq 1$ (by example 2.6.1 above), we can divide through by d and obtain $c \leq 1$. Applying the same example again, since c is itself a greatest common divisor by definition, we have $c \geq 1$. Combining these two inequalities, $c = 1$. □

Our next goal is to find an easy (well, easier) way to compute the greatest common divisor of two numbers. To do this, we must develop the idea of division with remainder like we learned in primary school. The main theorem which ensures that we can divide properly in the integers is the following

2.9 Theorem (The division algorithm)**.** *Let a and $b \neq 0$ be positive integers. Then there exist* unique *integers q and r, so that $0 \leq r < b$, and so that $a = qb + r$. The integers q and r are respectively called the **quotient** and **remainder**.*

For the proof of this, we must use the **well-ordering principle**:

(2.10) If S is a non-empty set of integers which is bounded below (i.e. there is some $b \in \mathbb{Z}$ so that if $n \in S$ then $n \geq b$), then S has a smallest element.

Proof of the division algorithm. Consider the set S defined by

$$S = \{a - nb : n \in \mathbb{Z}\} \cap \mathbb{N}_0. \tag{2.11}$$

This is just the set of all non-negative numbers which can be written in the form $a - nb$, for some integer n. Since $a \in S$, the set is non-empty; and since every $x \in S$ satisfies $x \geq 0$, x is bounded below by 0. Hence S has a least element, $a - qb$. This element is non-negative by definition, and must be less than b: if it were larger than b, we could consider $a - (q + 1)b = (a - qb) - b$, which is in S and less than $a - qb$, which is impossible since $a - qb$ is the least element in S. So if we let $r = a - qb$, then $0 \leq r < q$, and $a = ab + r$. So suitable q and r exist.

For uniqueness, suppose that q_1, r_1 and q_2, r_2 both satisfy the conclusion of the theorem. Hence $a = bq_1 + r_1 = bq_2 + r_2$, and so

$$0 = b(q_1 - q_2) + (r_1 - r_2). \tag{2.12}$$

Since $b \mid 0$ and $b \mid b(q_1 - q_2)$, it follows that b divides $r_1 - r_2$. But we have $0 \leq r_1 < b$ and $0 \geq -r_2 > -b$, so $-b < r_1 - r_2 < b$. The only multiple of b in between $-b$ and b is zero, so $r_1 = r_2$ and hence (by 2.12) $q_1 = q_2$. □

In order to compute the greatest common divisor easily, we will create a chain of integers so that the pairs of integers next to each other share the same GCD. The division algorithm allows us to do this, because of the following lemma.

2.13 Lemma. *If $a = bq + r$, then $(a, b) = (b, r)$.*

Proof. By the hypothesis, $(a,b) \mid r$, and so (a,b) is a common divisor of b and r. Hence $(a,b) \leq (b,r)$. On the other hand, $(b,r) \mid a$ (since it divides both numbers on the right-hand side of the equality in the hypothesis) and so $(b,r) \leq (a,b)$ (since (b,r) is a common divisor of a and b). Combining both inequalities, $(b,r) = (a,b)$. □

Finally, we have an algorithm for computing the greatest common divisor.

2.14 Theorem (The Euclidean algorithm)**.** *If a and $b \neq 0$ are positive integers, and*

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots \\ r_k &= r_{k+1} q_{k+2} + r_{k+2} \end{aligned}$$

where each r_{k+2} is bounded like $0 \leq r_{k+2} < r_{k+1}$, then for k large enough we have $r_{k-1} = r_k q_{k+1}$ (i.e. $r_{k+1} = 0$) and $(a,b) = r_k$.

Proof. Since each r_k is non-negative, and each r_k is less than r_{k-1}, the sequence $b > r_1 > \cdots > r_k$ has a least non-negative element, r_k, which must be zero or we would be able to divide again by the division algorithm. Then $r_{k-1} = r_k q_{k+1}$, and (by repeated application of lemma 2.13) we have

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{k-1},r_k) = (r_k,0) = r_k.$$

□

2.15 Example. Let us compute $(240, 373)$. We have:

$$\begin{aligned} 373 &= 1 \times 240 + 133 \\ 240 &= 1 \times 133 + 107 \\ 133 &= 1 \times 107 + 26 \\ 107 &= 4 \times 26 + 3 \\ 26 &= 8 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 1 \times 1 + 1 \\ 1 &= 1 \times 1. \end{aligned}$$

2.16 Example. Let us compute $(120, 340)$. We have:

$$\begin{aligned} 340 &= 2 \times 120 + 100 \\ 120 &= 1 \times 100 + 20 \\ 100 &= 5 \times 20. \end{aligned}$$

2.17 Corollary (Bézout's Lemma)**.** *If a and b are positive integers, then there exist integers x and y such that $ax + by = (a,b)$.*

Proof. By the proof of the Euclidean algorithm, for some k we have

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k, \\ r_{k-1} &= r_k q_{k+1}, \end{aligned}$$

and $r_k = (a, b)$. Rearranging:

$$\begin{aligned} a - bq_1 &= r_1, \\ b - r_1 q_2 &= r_2, \\ r_1 - r_2 q_3 &= r_3, \\ &\vdots \\ r_{k-2} - r_{k-1} q_k &= r_k = (a, b), \end{aligned}$$

and it is clear that we can substitute each equation into the one below it, eliminating every r_i until we (in the final line) arrive at some equation of the form $ax + by = (a, b)$. □

Bézout's Lemma is surprisingly useful; in fact, we will use it later this year to prove various properties of a particular system in algebra.[7]

Since we know that (a, b) divides $ax + by$ for all x and y, the lemma tells us that for every n, the equation

$$ax + by = n(a, b) \tag{2.18}$$

has an integer solution for x and y. In fact, it has infinitely many:

2.19 Theorem. *If (x, y) solves $ax + by = z$, then all solutions are of the form $(x - bn, an + y)$ for some $n \in \mathbb{Z}$.*

Proof. Clearly $a(x - bn) + b(an + y) = z$, so all expressions of that form are indeed solutions. On the other hand, suppose (x', y') is a solution. Then $0 = a(x - x') + b(y - y')$; it follows that $a \mid (y - y')$. Rearranging, we obtain $x' = x - b\frac{(y'-y)}{a}$, where $(y' - y)/a = n$ is an integer. Hence $z = a(x - bn) + by' = ax - abn + by' = ax + b(y' - an)$, and hence $y' = y + an$. □

2.20 Example. The equation $18x + 24y = 23$ has no solutions, since $(18, 24) = 6$ does not divide 23.

2.21 Example. We will solve $18x + 24y = 36$ for all the integer solutions x, y. Since $(18, 24) = 6$, we will begin by solving $18x + 24y = 6$:

$$\begin{aligned} 24 &= 1 \times 18 + 6 \\ 18 &= 6 \times 3 \end{aligned}$$

Hence $6 = 1 \times 24 + (-1) \times 18$, and $36 = 6 \times 24 + (-6) \times 18$. By the theorem above, all the solutions are given by $(6 - 24n, -6 + 18n)$ for $n \in \mathbb{Z}$.

[7] For those following along from the future, it will be used when we study **primitive roots**.

Section 3: Next Steps

As well as the material in the level three standards (differentiation, integration, algebra, linear systems, linear programming, path analysis, trigonometry, and conic sections) it is advantageous for Scholarship students to be aware of mathematics as a broader discipline. In the 2017 paper, for example, the opening question part was on number theory.

As such, I have here a list of books and topics which Scholarship students may wish to look over. I have included the University of Auckland library call number in brackets.

- **Culture:** *A Mathematician's Lament* by Paul Lockhart [510.71 L81].
- **Proofs:** *How to Think Like a Mathematician* by Kevin Houston [510 H84].
- **Number theory:** *Elementary Number Theory* by Underwood Dudley [512.72 D84].
- **Linear algebra:** *Linear Algebra: A Modern Introduction* by David Poole [512.5 P82].
- **Geometry:** *Geometry: A High School Course* by Serge Lang and Gene Murrow [516 L27].
- **Set theory:** *Naive Set Theory* by Paul Halmos [511.322 H19].
- **Calculus:** *Calculus* by Paul Spivak [515 S76].

I must stress that a comprehensive understanding of the content in the above books is *not required*; in most cases, a read of the first three sections will suffice to obtain an overview of the relevant parts of the subject (not that that precludes interested students from reading further).