

Supplement for MAA 3200, S Hudson (updated Oct 2010)
Construction of Number Systems

One goal of MAA 3200 is to understand more deeply our main number systems, N , Z , Q and especially the real numbers R . We'll examine the properties these systems have in common, and also how they differ. A focal point - Why is the real number system the standard choice in courses like Calculus?

I hope you will see that every term, such as '0' and '1' and '<', can be defined precisely, and that every well-known fact and formula, such as $n + m = m + n$, can be proven (though we won't have time to prove all these). There aren't many books that cover these topics in detail, but these notes should be enough to outline the main definitions and sample theorems. Also, my lectures will include enough proofs to demonstrate the main methods. You can find this material in more detail, if you like, in the text by Morash, which I plan to put on reserve in our library. There are minor differences among textbooks; for example, in Morash, $0 \notin N$, and ordered fields are defined via P instead of via $<$, etc).

These notes assume you are familiar with sets, functions etc in the abstract [from early MAA 3200], but not with the basics of algebra, such as addition and $x < y$. The whole point is that these things can be developed rigorously, from almost nothing.

I. Outline of the Construction

A) The natural numbers, N .

- 1) Define N as a set.
- 2) Define $+$ on N and prove formulas [like $n + m = m + n$, etc].
- 3) Define nm on N and prove related formulas.
- 4) Define $<$ on N and prove related formulas.

B) The integers, Z [with the same 4 steps as in A), and also subtraction, absolute value, etc]

C) The rational numbers, Q [with the steps in B), and also division, etc]

D) The real numbers, R [with the steps in C), and also completeness, etc]

The main methods in part A) are recursive definitions and inductive proofs. In part B) we'll define Z as equivalence classes in $N \times N$, and use what we learned in part A) to go on. Parts C and D are similar in that the previous system is used to build the next one. Completing all these steps rigorously would take months, so we will cover A), B) and C) rather lightly, and will focus on D) later [It is easier to handle R after we have learned some basic Analysis ideas, such as Cauchy sequences]. In this phase, we will also practice proof-writing, and previous topics such as recursion, induction and equivalence relations.

II. Some details of Part A); Constructing N

We want to define N and the binary operations $+$ and \cdot , and prove some of their properties. A *binary operation* on a set A is a function $f : A \times A \rightarrow A$. For example, we are planning to define a binary operation $f(n, m) = n + m$.

In the following axiom, which is the definition of N , the notation $\sigma(m)$ refers to the next number after m . So, $\sigma(2) = 3$, for example. We won't talk about many specific numbers like 3 here (just 0 and 1). But we could define 3 as $\sigma \circ \sigma \circ \sigma(0)$, for example. Later, we'll see that $\sigma(m) = m + 1$, but not yet; we haven't defined "+" yet.

Axiom: There is a set N with an element called 0, and a mapping $\sigma : N \rightarrow N$ such that:

- a) σ is 1-1, but not onto (0 is not in $\text{rng}(\sigma)$). And
- b) If $S \subseteq N$ and $0 \in S$ and $\forall m \in N, (m \in S \rightarrow \sigma(m) \in S)$ then $S = N$.

The induction method is based on part b), and is the main tool in proofs about N . In fact, if you didn't understand the last 5-10 lines, they are basically saying "Accept that N exists and induction is valid". The next steps aim to define "+" recursively on N . We introduce a function s_m , planning soon to define $m + n = s_m(n)$.

Thm: $\forall m \in N$ there is a unique function $s_m : N \rightarrow N$ such that

a) $s_m(0) = m$ and

b) $\forall n \in N, s_m(\sigma(n)) = \sigma(s_m(n))$.

In the Morash book, part a) may appear as $s_m(1) = \sigma(m)$, since he begins N at 1 instead of 0 (various books differ on this). I've tried to make these notes consistent with the N we've used so far.

Def: Given any $m, n \in N$ their *sum* is $s(m, n) = s_m(n)$; this may also be written " $m + n$ ".

Sample Thm: N is closed under addition, and $m + n = n + m$. [We will state and prove a few familiar theorems like this in class, but we won't have time for very many]. The next steps aim to define multiplication recursively on N .

Def: For each $m \in N$ let $p_m : N \rightarrow N$ be such that a) $p_m(0) = 0$, and b) $\forall n \in N, p_m(\sigma(n)) = p_m(n) + m$. Define the product (often written $m \cdot n$ or just mn) by $p(m, n) = p_m(n)$.

Sample theorems: $mn = nm$ and $m(n + k) = mn + mk$.

Def: $a < b$ means $\exists c \neq 0$ in N such that $a + c = b$.

Thm: If $a < b$ then $a \neq b$; and $\forall c \in N, a + c < b + c$; and $<$ has the transitive property.

Thm (trichotomy) Given any $a, b \in N$ exactly one of these three is true: $a < b, b < a$ or $a = b$.

III. About Z and Q

Our first goal is to define Z . Since we can use facts about N now, this section is actually much easier than the previous one.

Def: Let $A = N \times N$. Define a relation \sim on A by: $(a, b) \sim (c, d)$ means $a + d = b + c$.

Thm: This is an equivalence relation on A .

Def: Let $Z = A / \sim$ be the set of equivalence classes, and call the elements of Z *integers*.

You can think of $[(a, b)]$ as the integer $a - b$. For example, $(3, 5)$ and $(10, 12)$ are in the same eq. class, and they both correspond to the element $-2 \in Z$. Now, we'll define $+$ and \cdot on Z .

Def: The *sum* of two integers is $[(a, b)] + [(c, d)] = [(a + c, b + d)]$.

Def: The *product* of two integers is $[(a, b)] \cdot [(c, d)] = [(ac + bd, bc + ad)]$.

For example, $[(3, 5)] + [(7, 2)] = [(10, 7)]$, which corresponds to the more familiar $-2 + 5 = 3$. From now on, we will usually prefer notation such as $n \in Z$ rather than $[(a, b)] \in Z$. Notice that $[(3, 5)] = [(10, 12)]$. If we use $[(10, 12)]$ instead of $[(3, 5)]$, do we still get the same answer? Yes, we get $[(17, 14)]$, which is the same as $[(10, 7)]$. The next theorem says this always works out OK, and also does for multiplication.

Thm: These operations are well-defined.

Thm: There is a unique integer a such that $\forall x \in Z, a + x = x + a = x$. We call this integer "0".

Thm: For each $z \in Z$, there is a unique $y \in Z$ such that $z + y = y + z = 0$. We write " $y = -z$ " and call it the additive inverse of z .

There are many other theorems about Z including ones similar to those discussed for N above. Number systems with nice properties like the ones above get special labels like *groups*, *rings* and *fields*. Z is not a field because it doesn't have multiplicative inverses, but our theorems do imply that Z is a *ring*. N is not even a ring, since it doesn't have additive inverses. You may learn more properties of rings and fields in an Algebraic Structures course. Next, we define $<$ on Z from $<$ on N :

Def: Let $x = [(a, b)]$ and $y = [(c, d)]$. Then $x < y$ means $a + d < b + c$. [Thm: this is also well-defined].

There are many more simple theorems about Z . Example: if $x < y$

and $0 < z$, then $xz < yz$. We may look at some of these in class or in HW exercises. Define $>$ as the inverse relation of $<$. Define \leq as the relation $= \cup <$.

We define Q from Z as follows (using equivalence classes again). Let $A = Z \times Z^+$ and define \sim on A by: $(p, q) \sim (r, s)$ means $ps = rq$. Let $Q = A / \sim$. Ex: $(2, 3) \sim (4, 6)$ and both ordered pairs may be thought of as $2/3$.] We can now define $+$, \cdot and $<$ on Q using Z . The next formula below is based on $\frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}$.

Def: Let $x = [(p, q)]$ and $y = [(r, s)]$. Then set $x + y = [(ps + rq, qs)]$ and $xy = [(pr, qs)]$.

Thm: Q is a *field* (which means the operations defined above satisfy the *field axioms*; for example, that every nonzero $q \in Q$ has a q^{-1}).

An *ordered* field is one with a relation $<$ defined on it, that satisfies certain *order axioms*. Define $x < y$ to mean $y - x \in P = \{[(p, q)] \in Q \mid pq > 0\}$, which is the set of *positive* rational numbers. This leads to another theorem: that Q is an ordered field. Even so, Q is not the most useful field, because it is not *complete*. We'll discuss that problem, and eventually solve it once we define R , which is the only complete ordered field. The complex numbers C form another complete field, but they cannot be ordered.

Quite a few theorems can be proven directly from the axioms, which means we don't have to prove them all separately for Q and R and C . Let F stand for any field.

Sample Thm: For all $x \in F$, $x \cdot 0 = 0$.

Sample Thm: If F is ordered then $1 > 0$, and if $x > 0$ then $x^{-1} > 0$. Also, we can define \leq and $|x|$ the usual way, and then \leq is a partial order on F .

It is best to postpone the definition of R . Most Analysis books (including Calculus books, and Shilov's book) use the field R as the universal set U , without including a careful construction of R . So, delaying R may seem wrong. But almost all the early material works just as well if $U = Q$, or any

other ordered field. While reading these early sections, you may imagine that $U = Q$, until we learn about Cauchy sequences. With that, we can carefully define R from Q , and discuss its properties. We'll prove that R is an ordered field (if time permits) and say "So, the Analysis we've learned so far works on R , too". Or you can simply accept that we will come back to the definition of R and trust me that the presentation is not circular. In a nutshell, here's what makes R better than Q :

Def: An ordered field F is *complete* if every nonempty set S with an upper bound has a lub (also known as a *supremum*).

Ex: Let $F = Q$ and let $S = \{x \in Q \mid x^2 < 2\}$. If F were R the lub would be $\sqrt{2}$, but since that doesn't belong to Q , S has no lub in Q . So, Q is not complete. It has "holes" at places like $\sqrt{2}$. Many Analysis / Calculus theorems, such as the Intermediate Value Theorem, depend on completeness and would fail if Q were used instead of R . Completeness is not used very early in Analysis, so there is no danger in imagining that $F = Q$ for a little while.