MAE 501
February 3, 2009

As we continue to talk about numbers, we come to find the way in which we can explain these sets (**N, W, Z, Q, R,** and **C**) to our future students at the junior high and high school level. Our objective in this course is to be able to use the advanced concepts that we have learned about math through undergraduate and graduate studies, and apply them to the learning process of our students. In order for us to effectively communicate these mathematical ideas, we must break these concepts down so we can explain to the student the meaning of even the simplest concepts, for example, addition, subtraction, multiplication, and division. During this lecture, we were able to build numbers to include each of these four operations.

We begin by referring to **N,** as a **semigroup** consisting of **N** and the operation +, noted as (**N**, +). This semigroup is commutative, and associative, meaning that the following is true for any a, b, c $\in$ **N**, a+b = b+a and a+(b+c) = (a+b) +c.

Knowing this to be a semigroup, what else is an example of a semi-group?
Lets take a function *f*: **R**$\rightarrow$**R**, and use the operation of composition (•) to make another semi-group, i.e. $f \bullet g = f \bullet g(x) = f(g(x))$, under composition we see that in fact, $(f \bullet g) \bullet h = f \bullet (g \bullet h)$, which means this semigroup is associative, however, not commutative, $f(g(x)) \neq g(f(x))$. We can generate this semigroup by taking any number of functions (one will do), and consider all possible compositions of the resulting function.

> In an example, $f(x)=x^2$ we can generate more functions by taking compositions, giving us $f(f(x)) = x^4$, again $f(f(f(x))) = (x^4)^2 = x^8$, etc. In this way, we get all functions of the form x^{2n} for any natural number n.

A **monoid** is a set M with binary operation *: $M \times M \rightarrow M$, with the following axioms:
- associativity : for all a, b, c in M, (a*b)*c = a*(b*c)
- identity element: there exists an element e in M, such that for all a in M, a*e =e*a = a
- closure: for all a, b in M, a*b is in M.

> We can extend our previous example to a monoid by adding the identity function $f(x)=x$ to our set of functions.

A **group** is a monoid with the additional property of inverses. Therefore adding the following axiom to the above definition of monoid :
- inverses: for all a in a set S, there exists a^{-1} so that $a^{-1}*a = a*a^{-1} = e$

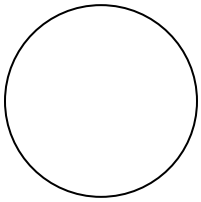
> If we wish to extend our example to a group, we need to add an inverse for everything in the monoid. We can use $f^{-1}(x) = x^{1/2}$, and then include all possible compositions. We note that this example is isomorphic to the integers **Z.**

Now that we have a definition of a group, lets think about the groups that children first encounter in school.

- a light switch: $\mathbf{Z}_2$ = {on, off}
- falling down, and getting up again: $\mathbf{Z}_2$ = {up, down}
- a clock: $\mathbf{Z}_{12}$ = {1 o'clock, 2 o'clock, 3 o'clock, ..., 12 o'clock}
- a square (with rotation by 90 degrees): $\mathbf{Z}_4$ = {$side_1$, $side_2$, $side_3$, $side_4$}
- the integers: $\mathbf{Z}$ = {...,-3, -2, -1, 0, 1, 2, 3, …, n-1, ...}

Students don't usually deal with $\mathbf{Z}_n$ for general n.

What is the difference between the group $\mathbf{Z}_n$ and $\mathbf{Z}$?
$\mathbf{Z}_n$ is finite and has a repetitive nature, e.g. rotation of a circle through a fixed fraction of a turn, that is, 360/n degrees.
We can rotate around a circle in different increments. Even though there are infinitely many possible rotations, we will still come back to the beginning and repeat the positions, like a clock's repetitive nature. For example, we can wait any number of hours, but it the time will always be between 1:00 and 12:59.



$\mathbf{Z}$ is infinite, e.g. a straight line

---

which can go either way to negative and positive infinity and does not repeat. The only way we can get from a number *n* back to *0* is by subtraction.

We have the idea that we can build integers through pairs of natural numbers via an **equivalence relation**, a binary relation that satisfies the properties of reflexivity, symmetry, and transitivity.

We have seen that the set of integers can be built from pairs of the natural numbers: $\mathbf{Z=NxN/\sim}$, where (a,b) ~ (c,d), when a + d = c + b.

Similarly, the rational numbers can be built from the integers, as shown below in equivalence relation terms:

$\mathbf{Q}$={p/q such that p,q ∈ $\mathbf{Z}$, q≠0, p,q in least terms}
= ($\mathbf{ZxZ}$ – $\mathbf{Z}$x{0})/~ , where (p/q) ~ (r/s), when ps = rq

Note that using the equivalence relation method enables us to discuss Q without having to worry about what "p,q in least terms" means, nor explicitly try to define division when it doesn't "make sense" for natural numbers (for example, 5/3).

We have now been able to build numbers to include, addition, subtraction, and multiplication from a semigroup to a monoid to a group…

($\mathbf{Z}$, +) is a group, and in this group we can define multiplication as repeated addition, which is the elementary concept for students to learn to multiply. We must note though that ($\mathbf{Z}$, •) is $\mathbf{Z}$

with multiplication, and it is NOT a group because every element does not have an inverse. For example, 3 has no multiplicative inverse, 1•3 = 3, but there is no integer x such that 3x=1.

This gives us a motivation to build to the rational numbers (**Q**) so we can solve for this x above. We will try to make **Z** a multiplicative group by assigning inverses, let there be fractions so inverses exist. Note that denominator as 0 is a problem; we'll come back to that presently. For now, let us exclude it.

When we have **Q**, this gives us a new kind of group, called a **field**, which is a set of numbers that has the four operations, addition, subtraction, multiplication, and division (except by 0).

(**Q**, +, 0) is a group, and (**Q** – {0}, •, 1) is a group.

What if we tried to make a group **Q'**, which is both an additive and multiplicative group? That is, we try to treat 0 the same way as 1.

Lets say that **Q'**={p/q such that p,q ∈ **Z**, p,q in least terms}, where q can be 0, i.e. **Z**x**Z**/**~** , where (p,q) **~** (q,r) whenever ps = qr.
We can define p/q + r/s = (sp+rq)/qs and p/q • r/s = pr/ps.

Let's find out why this can't work when we let q be 0.

We have: 1/0, which we will say equals 1', then when 2/0, we will call it 2'. Note that we must have 1' = 2', since using the equivalence relation above , we have
(1,0) **~** (2,0) because 1 • 0= 2 • 0 = 0. So, let's give any number of the form *(n,0)* a new name: ∞. If we have ∞ in our group, then what about ∞ + 1?

Lemma: If p/q is any rational number, we have ∞ + p/q = ∞.

How do we prove? Just apply the definition:

$$\infty + p/q = 1/0 + p/q = q \bullet 1 + p \bullet 0 = q/0 = \infty,$$

meaning that if we add ∞ to anything we get ∞ again. But this is a problem, since

$$\infty + \infty = 1/0 + 1/0 = (0 + 0)/0 = 0/0 = 0 \bullet (1/0) = 0 \bullet \infty$$

This gives us a problem with the law for the identity of the group. Consequently we have a second "special" element of the group (∞), so it can't be both a multiplicative and additive group.

Homework:
a) what is wrong with this statement:
p/q + r/s = (p+r)/(q+s)
That is, why can't we define addition differently?
b) can we do anything different from: p/q + r/s = (ps + rq)/qs ? What would be the consequences?

Epp, Susanna S. Discrete Mathematics with Applications, Second Edition, 1995, Brooks/Cole Publishing Company