Abstract Algebra

Math 113, UC Berkeley

D. Zack Garza

September 2, 2014

1. Getting to know me.

   a) Major: Mathematics and Computer Science.

   b) In the past year, I've taken Vector/Multivariate Calculus, Linear Algebra, Differential Equations, Discrete Mathematics, and Statistics. I am currently taking Berkeley's CS70, a survey course in Finite Mathematics, and am following an Algebraic Topology video series online.

   c) Oddly enough, the most difficult topic for me has been coming to terms with induction. The mechanics of carrying out inductive proofs are pretty straightforward, but I've always had trouble with the idea that it really proves any kind of objective truth.

2. Distinguishing *binary operations*.

   We start with a definition - denote a *binary operation* $\star$ on a nonempty set S as a map satisfying $\star : S \times S \mapsto S$.

   a) Composition on the set S of functions $\mathbb{R} \mapsto \mathbb{R}$.

      Yes - if $f \in S$ maps $\mathbb{R}$ to $\mathbb{R}$, and $g \in S$ also maps $\mathbb{R}$ to $\mathbb{R}$, then the composition $f \circ g$ is *also* a function that maps $\mathbb{R}$ to $\mathbb{R}$ and thus $f \circ g \in S$. From this, it follows that $f \circ g$ is a binary operation $\forall f, g \in S$.

   b) Composition on the set S' of functions $\mathbb{R} \mapsto \mathbb{R}^2$.

      No - this is because the operation of function composition $f \circ g$ is not well-defined when the image of g is not in the domain of f. In other words, since all $g \in S'$ map $\mathbb{R}$ to $\mathbb{R}^2$, and f can only be applied to elements in $\mathbb{R}$, f can't be applied to any output of g. In order for the operation to be binary, the elements must be have a kind of "closed" mapping, in the sense that they map back into their own set.

   c) $\star : a \star b = \frac{1}{2}(a + b) \forall a, b \in \mathbb{Q}$

      Yes - to prove this, we use the definition of a binary operation to show that $\star$ is a map from $\mathbb{Q} \times \mathbb{Q}$ to $\mathbb{Q}$ for all arbitrary elements a and b in $\mathbb{Q}$.

Since $\mathbb{Q}$ and $\mathbb{Q} \times \mathbb{Q}$ are trivially nonempty, consider $a, b \in \mathbb{Q}$. Then, by the definition of a rational number, $a = \frac{r}{s}$ and $b = \frac{u}{v}$ for some $r, s, u, v \in \mathbb{Z}$. Thus, we have,

$$\begin{aligned} a \star b &= \frac{1}{2}(a + b) \\ &= \frac{1}{2}(\frac{r}{s} + \frac{u}{v}) \\ &= \frac{rv + us}{2sv}, \end{aligned}$$

and from the closure of multiplication and addition in $\mathbb{Z}$, we have

$$a \star b = \frac{w}{x}$$

where $w = rv + us \in \mathbb{Z}$ and $x = 2sv \in \mathbb{Z}$. Since this shows that $a \star b$ is the ratio of two integers, it is in $\mathbb{Q}$, and $\star$ thus satisfies the definition of a binary operation.

d) $\star : a \star b = \max(a, b) \forall a, b \in \mathbb{R}$.

Yes - because as long as either a or b is in $\mathbb{R}$, $\star$ is guaranteed to pick one of them out (as long as the *max* operator is defined to handle the edge case of $a = b$). Since the output of $\star$ is identical to one of the inputs in every case, $a \star b$ is always in $\mathbb{R}$, and $\star$ is a binary operation.

e) $\star : X \star Y =$ 3 oz of X mixed with 5 oz of Y, where $X, Y \in$ the set D of all possible things you can drink.

In most cases, yes, although it entirely depends on how the set D is defined. If D includes all liquids (which are all technically possible to drink), then there are many edge cases - for example, there may exist pairs of liquids which, when combined, react to form a non-liquid. In these cases, $\star$ is not a binary operation, as its output is not in D. If D is defined as all of the drinkable liquids that won't kill you, a similar argument suggests that there may be some $X \star Y$ that is not in D - that is, a combination of non-toxic liquids that is toxic. In this case, D would have to be *defined* to have the type of set closure necessary for $\star$ to be a binary operation.

3. Give an example of another set with a binary operation.

Addition, on the set of linear n^{th} order differential equations, defined by adding corresponding coefficients of $y', y'', \ldots y^n$.

4. Which of the binary operations in questions (2) and (3) are associative and/or commutative?

a) 2-a:

Associativity: Yes, since $f \circ (g \circ h) = (f \circ g) \circ h$.

Commutativity: No, since $f \circ g \neq g \circ f$ for most functions.

b) 2-b: Neither, since the operation is not well-defined.

c) 2-c: Associativity: No. Assuming it is, we have

$$\begin{aligned}(a \star b) \star c &= a \star (b \star c) \\ \frac{a+b}{2} \star c &= a \star \frac{b+c}{2} \\ \frac{\frac{a+b}{2} + c}{2} &= \frac{a + \frac{b+c}{2}}{2} \\ a + b + 2c &= 2a + b + c\end{aligned}$$

which is a contradiction.

Commutativity: Yes, by the commutativity of addition in $\mathbb{Z}$, and since division distributed over addition commutes as well. (i.e., $\frac{1}{2}(a+b) = \frac{1}{2}(b+a)$).

d) 2-d:

Associativity: Yes, by inheriting the associativity of $>$ in $\mathbb{R}$.

Commutativity: Yes, since the greatest number in an ordered pair will not change based on their order (i.e., $\max(a,b) = \max(b,a)\ \forall a, b \in \mathbb{R}$).

e) 2-e:

Associativity: No, because the relative amounts of each liquid in $(X \star Y) \star Z$ and $X \star (Y \star Z)$ would be different. Take X to be gin, Y to be tonic, and Z to be grenadine. In the first case, you get an 8 oz gin and tonic that is 3/8 alcoholic, take 3 oz of it, and drown it in 5 oz of flavoring (which may in fact be impossible to drink). In the second case, you get tonic water that is 3/8 flavoring, take 5 oz of that, and add 3 oz of gin (which is much more palatable).

Commutativity: No, as 3oz of tonic to 5oz of gin packs much more of a punch than 3oz of gin to 5oz of tonic.

f) 3:

Associativity: Yes, by the associativity of addition in $\mathbb{R}$.

Commutativity: Yes, by commutativity of addition in $\mathbb{R}$.

5. Is the set D of all things you can drink, with the operation $\star$, a group? Why or why not?

No - by definition, D equipped with $\star$ is a group if:

a) $\exists! e\ (e \star a = a \star e = a\ \forall a \in D)$

b) $\exists! a^{-1}\ \forall a \in D\ (a \star a^{-1} = a^{-1} \star a = e)$

c) $(a \star b) \star c = a \star (b \star c)\ \forall a, b, c \in D$

The existence of a single identity element for all liquids poses a problem, as there is no liquid in D that can be added to every other liquid without changing it.

Although water might be a possible choice, there is a distinction between a given liquid and its diluted form.

If water did serve as the identity element, however, it is not clear there would exist inverses - that is, that every liquid had a co-liquid that turned it back into water. From this, we conclude $(D, \star)$ does not form a group.

6. Modular arithmetic (residue classes)

   a) Prove that $1243 + 1985^2 - 4827 + 4 \neq 4839 + 753^3 - (56)81$ by finding some n such that

   $$1243 + 1985^2 - 4827 + 4 \not\equiv 4839 + 753^3 - (56)81 \pmod{n} \tag{1}$$

   We begin by assuming $\exists n$ such that two expressions in (1) *are* equal. By definition, $a \equiv b \pmod{n} \implies n \mid (a - b)$. Substituting (1) into this expression and simplifying addition and subtraction yields

   $$n \mid 9709 + 1985^2 + 753^3. \tag{2}$$

   We know that an odd squared is odd, as is an odd cubed, so n must divide the sum of three odd numbers. Thus, n must divide an *odd* number if the expression in (1) were congruent mod n.

   So, in order to prove they are *not* congruent, we select a number that is *not* odd. For the simplest case, let $n = 2$. Using the lemma that $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$, applying mod 2 to each term in (1) gives

   $$1 + 1 - 1 + 0 \overset{?}{\not\equiv} 1 + 1 - 0 \pmod{2} \tag{3}$$

   where we have used the fact that the any odd number mod 2 = 1, an odd squared is odd, an odd cubed is odd, and an odd times an even is even. Simplifying (3) gives

   $$\begin{aligned} 1 &\overset{?}{\not\equiv} 2 \pmod{2} \\ 1 &\not\equiv 0 \pmod{2}. \end{aligned} \tag{4}$$

   And since (4) is a true statement, (1) is also true, and the original statement is proved.

   b) Let $\mathbb{Z}/n\mathbb{Z}^x = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a}\bar{c} = \bar{1}\}$. Show that $\mathbb{Z}/n\mathbb{Z}^x$ with multiplication is a group.

   To prove $\mathbb{Z}/n\mathbb{Z}^x$ is a group, we simply show that all three group conditions are satisfied.

      i. The identity element e.

      The equivalence class $\bar{1}$ serves as e, and it can be shown to be in the set for every n by naming $\bar{1}$ as c in the definition.

ii. Existence of inverses.

Since the identity element is simply $\bar{1}$, the original set is guaranteed to have inverses for every element by its own definition. In fact, the only items *in* $\mathbb{Z}/n\mathbb{Z}^x$ are those which *have* multiplicative inverses.

iii. Associativity

Since $G_1 = (\mathbb{Z}/n\mathbb{Z}^x, \star)$ would be a subgroup of $G_2 = (\mathbb{Z}/n\mathbb{Z}^x, \star)$, if we can show that associativity holds in G_2, it will also hold in G_1.

By definition, $a \equiv b \bmod \text{n} \implies n \mid (a - b)$. If associativity holds, we have

$$\begin{aligned} &(ab)c \equiv a(bc) \bmod n \\ \implies &n \mid (ab)c - a(bc) \end{aligned}$$

But since the RHS is simply multiplication and subtraction over $\mathbb{Z}$, it is equal to 0. Since $n \mid 0 \ \forall n$, multiplication is associative in $\mathbb{Z}/n\mathbb{Z}$, and thus also associative in the subset $\mathbb{Z}/n\mathbb{Z}^x$.

From this, we can conclude that $(\mathbb{Z}/n\mathbb{Z}^x, \star)$ is indeed a group.

c) (Bonus) Prove that if a and n have a common divisor other than 1, then $a \notin \mathbb{Z}/n\mathbb{Z}^x$.

No idea!