Keith Godlewski
Class Notes
11 September 2008

- Review of homework problems
- Functions
- Homomorphisms
- Equivalence Relations

Review of Homework One

Various issues were discussed regarding the homework correction. Issues pertaining to how rational numbers were defined, as well as the order in which stipulations were placed within the definitions. Another semantical mistake that appeared was a lack of assigning $b \neq 0$ and the declaration of a number as rational before the number was actually defined.

Example:

$$\frac{a}{b}+\frac{c}{d}=\frac{(ad+bc)}{bd} \text{ which is rational, since } (ad+bc)\in\mathbb{Z},\ (bd)\in\mathbb{Z},\ bd\neq 0$$

$$\text{since } b\neq 0,\ d\neq 0$$

Here the proof that the rational numbers are closed under addition should show that the sum and product of two integers is indeed an integer; declare that the denominators are not zero and hence the quotient of two integers is rational by definition.

The order of quantifiers was another concern. Throughout the *Group* definitions there were mistakes when using quantifiers incorrectly. Remember that there is a difference between something exists for all elements, and, for all elements there exists.

Group

A nonempty set **G**, closed under a binary operation ***** on **G** is a group if the following conditions hold:

1. $a*(b*c)=(a*b)*c,\ \forall (a,b,c)\in G$ (associativity)
2. $\exists\ e\in G$, *called the identity of* G *such that* $\forall\ a\in G,\ a*e=e*a=a$
3. *for each* $a\in G\ \exists\ (a^{-1}\in G)$, *called the inverse of* a, *such that* $a*a^{-1}=a^{-1}*a=e$

One interesting example which involved the use of logic was also presented.

Do the following statements coincide?

$$2|a^2 \rightarrow 2|a \qquad a,b\in\mathbb{Z}$$

$$8|b^2 \rightarrow 8|b$$

The second implication can be nullified with the use of $b=4$ as a counterexample, but the first was solved using a contrapositive approach.

Recall that a conditional statement and its contrapositive are equivalent.

$$P \rightarrow Q \Leftrightarrow (\neg Q) \rightarrow (\neg P)$$

Therefore a proof by contraposition of $P \rightarrow Q$ makes use of the tautology,[i]

$$(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P).$$

$$\begin{gathered} \textit{The following format may be used } \text{in } \textit{this situation,} \\ \textit{Assume } \neg Q. \\ . \\ . \\ \textit{Therefore, } \neg P. \\ \textit{Thus, } \neg Q \rightarrow \neg P \\ \textit{Therefore, } P \rightarrow Q. \end{gathered}$$

What follows is the proof concerning the the assumption that if $2|a^2$ then $2|a.$ It follows the format outlined above.

$$\begin{gathered} \textit{Assume } 2 \nmid a \quad [\textit{Assume } \neg Q], \\ \textit{so } a = 2\text{b}+1 \textit{ for some integer } b \\ a^2 = (2\text{b}+1)^2 \\ a^2 = 4\text{b}^2 + 4\text{b} + 1 \\ a^2 = 4(b^2+b)+1 \\ \textit{Since} \quad b^2+b \textit{ is even} \rightarrow 4(b^2+b) \textit{ is even, plus one is odd} \\ \text{and} \quad b^2+b \textit{ is odd} \rightarrow 4(b^2+b) \textit{ is even, plus one is odd} \\ \textit{therefore } a^2 \textit{ is not even } \text{and } 2 \nmid a^2 \quad [\textit{Therefore } \neg P] \\ \textit{Thus } 2 \nmid a \rightarrow 2 \nmid a^2 \qquad [\textit{Thus } \neg Q \rightarrow \neg P] \end{gathered}$$

$$\textit{By contraposition, if } 2|a^2, \textit{ then } 2|a.$$

Functions [ii]

$$\begin{gathered} \textit{Let } A \text{ and } B \textit{ be sets.} \\ A \textit{ mapping } f: A \Rightarrow B \textit{ is a function } \text{from } A \text{ to } B \\ \textit{if } \forall x \in A \ \exists! \, y \in B \textit{ with } f(x) = y \\ A \textit{ is the domain, } x \textit{ is an element of the preimage} \\ B \textit{ is the codomain, } y = f(x) \textit{ is an element of the image} \end{gathered}$$

- A *function* $f: X \rightarrow X$ *such that* $f(x) = x,\ \forall x \in X$ *is called the identity mapping on* X
- *Two functions* $f: A \rightarrow B$ and $g: C \rightarrow D$ *are said* to *be equal,* $f = g$, *if* $A = C, B = D,$ and $f(x) = g(x) \ \forall x \in A.$
Notice that the functions f and g *are not equal if they have different codomains*

Definition

$$\text{A function } f: A \to B \text{ is}$$
$$(a)\ \textit{injective } (\text{or } \textit{one}-\text{to}-\textit{one}) \text{ if}, \ \forall x_{1,} x_2 \in A,$$
$$x_1 \neq x_2 \text{ implies } f(x_1) \neq f(x_2)$$
$$\text{or, equivalently, } f(x_1) = f(x_2) \text{ implies } x_1 = x_2;$$
$$(b)\ \textit{surjective } (\text{or } \textit{onto}) \text{ if, for every } y \in B,$$
$$y = f(x) \text{ for some } x \in A.$$
$$\text{A function which is injective and surjective is said to be bijective.}$$

Example:

$$\text{Is the following map bijective?}$$
$$f: R \to R$$
$$f(x) = mx + b$$

$$\text{Yes: Proof.}$$
$$\text{Suppose for some } x_{1,} x_2 \in X,\ m \neq 0$$
$$\text{that } mx_1 + b = mx_2 + b$$
$$\text{then } mx_1 = mx_2$$
$$\text{so } x_1 = x_{2,} \text{ hence the map is injective.}$$

$$y = mx + b, \text{ such that } m \neq 0$$

$$\text{Given } y \in \mathbb{R}$$
$$\text{let } x = \frac{(y-b)}{m}, \text{ then } f(x) = m\left[\frac{(y-b)}{m}\right] + b$$
$$\text{hence } f(x) = y$$
$$\text{therefore the map is surjective and hence bijective.}$$

The assumption $m \neq 0$ assures that each element in the codomain is the image of at most one element in the domain. Therefore if m were allowed to be zero, the function would fail to be injective.

Homomorphisms

$$\text{A special function } f \text{ from a group } (G_{1,} *) \text{ to a group } (G_{2,} .)$$
$$\text{such that } \forall a, b \in G_1$$
$$f(a * b) = f(a).\ f(b)$$
$$\text{is called a group homomorphism.}$$
$$\text{We say that } f \text{ preserves the group operation.}$$

A homomorphism is a function from one algebraic system to another under which results of operations correspond. A homomorphism is not necessarily injective.

A few examples of group homomorphisms involving the integers:

$$h:(\mathbb{Z},+)\rightarrow(\mathbb{Z},+)$$
$$h(n)=2\text{n}$$
$$\textit{Take } a, b\in\mathbb{Z}$$
$$\textit{then } h(a+b)=2(a+b)=2\text{a}+2\text{b}$$
$$=h(a)+h(b)$$
$$\textit{Hence } h \textit{ is a homomorphism}.$$

$$\textit{Also},$$
$$f:(\mathbb{Z},*)\rightarrow(\mathbb{Z},*)$$
$$f(n)=2\text{n}$$
$$f(ab)=2(ab)=2\text{ab}$$
$$\textit{which} \text{ in } \textit{general is not equal} \text{ to } 2\text{a}*2\text{b}$$
$$\textit{as a counterexample, let } a=3, b=2$$
$$f(ab)=2(3*2)=2(6)=12$$
$$f(a)=f(3)=2*3=6$$
$$f(b)=f(2)=2*2=4$$
$$\text{and } \textit{therefore } f(ab)\neq f(a)*f(b)$$
$$\textit{Thus } f \textit{ is not a homomorphism.}$$

Instead look at the group of real numbers with the operation of addition.

$$f:(\mathbb{R},+)\rightarrow(\mathbb{R},+)$$
$$f(x)=x^2$$
$$\textit{Given } a, b\in\mathbb{R}$$
$$f(a+b)=(a+b)^2$$
$$f(a+b)=a^2+2\text{ab}+b^2$$
$$f(a+b)=a^2+b^2+2\text{ab}$$
$$f(a+b)=f(a)+f(b)+2\text{ab}$$
$$\textit{this is true for } f(a)+f(b) \textit{ only when } (a \text{ or } b)=0.$$
$$\textit{Hence, this is not a group homomorphism.}$$

Further examples and non-examples,

$$f:(\mathbb{R},+)\to(\mathbb{R},+)$$
$$f(x)=\sin(x)$$
$$\textit{a common error among high school students would be } \text{to } \textit{assume}$$
$$f(a+b)=f(a)+f(b)$$
$$\textit{but},\ \sin(\pi)\neq\sin(\frac{\pi}{2})+\sin(\frac{\pi}{2})$$
$$\textit{therefore the function is not a homomorphism.}$$

$$\textit{Now look at the cubic function},\ f(x)=x^3$$
$$f:(\mathbb{R},*)\to(\mathbb{R},*)$$
$$a,b\in\mathbb{R}\ f(a*b)=(ab)^3=a^3*b^3=f(a)*f(b)$$
$$\textit{therefore it is a group homomorphism.}$$

$$\textit{But},$$
$$f:(\mathbb{R},+)\to(\mathbb{R},+)$$
$$f(a+b)=(a+b)^3\ \textit{which } \text{in } \textit{general } \text{is } \textit{not } a^3+b^3$$
$$\textit{so this is not a group homomorphism.}$$

Equivalence Relation[ii]

A relation ~ on a nonempty set S is an equivalence relation on S if it satisfies the following three properties:

(a) *If* $a\in S$, *then* $a\sim a$ *reflexive*

(b) *If* $a,b\in S$ and $a\sim b$, *then* $b\sim a$ *symmetric*

(c) *If* $a,b,c\in S$ and $a\sim b$ and $b\sim c$, *then* $a\sim c$ *transitive*

An equivalence relation always partitions the set into disjoint subsets called equivalence classes.

i Smith, Douglas, Eggen, M., St. Andre, R. A Transition to Advanced Mathematics. CA; Thomson, 2006.
ii Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R. Basic Abstract Algebra. New York; Cambridge University Press, 1986.
ii Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R. Basic Abstract Algebra. New York; Cambridge University Press, 1986.