Abstract Algebra | September 27, 2005
Prof Feighn | Exam 1

Name: ______________________________

1. (5 points each)

   (a) Define the term *relation*.

   A *relation* between sets A and B is a subset of $A \times B$.

   (b) Give an example of a relation.

   If $A = \{a, b\}$ and $B = \{1, 2\}$ then the subset $\mathcal{R} = \{(a, 1), (a, 2), (b, 1)\}$ of $A \times B$ is a relation between A and B.

   (c) Define the term *function*.

   A *function* f from a set A to a set B is a relation between A and B such that every element of A is related to exactly one element of B.

   (d) Give an example of a relation that is a function.

   The relation $\{(x, x) \mid x \in \mathbb{R}\}$ is a function from $\mathbb{R}$ to $\mathbb{R}$.

   (e) Give an example of a relation that is not a function.

   The relation $\mathcal{R}$ of Problem 1b is not a function since both $(a, 1)$ and $(a, 2)$ are in $\mathcal{R}$.

   (f) Define the term *one to one*.

   A function f from A to B is one to one if the following holds: if a_1, $a_2 \in A$ and $f(a_1) = f(a_2)$, then $a_1 = a_2$.

   (g) Give an example of a function that is one to one.

   The function of Problem 1d, namely the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x$ is one to one. Indeed, if x_1 and x_2 are real numbers such that $f(x_1) = f(x_2)$ then, by definition of f, $x_1 = x_2$.

   (h) Give an example of a function that is not one to one.

   The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not one to one. For example, $f(-1) = 1 = f(1)$.

(i) Define the term *group*.

A *group* is a binary structure $(G, *)$ such that

- $*$ is associative, namely for all g_1, g_2, and g_3 in G we have $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$;
- there is an element $e \in G$ such that, for all $g \in G$, $g * e = g = e * g$; and
- for all $g \in G$ there is $g' \in G$ such that $g * g' = e = g' * g$.

(j) Give an example of a group with six elements.

$(\mathbb{Z}_6, +_6)$ is a group with six elements.

(k) Define the term *isomorphism of binary structures*.

Two binary structures $(B, *)$ and $(B', *')$ are *isomorphic* if there is a one to one and onto function $f : B \to B'$ such that, for all b_1 and b_2 in B, $f(b_1 * b_2) = f(b_1) *' f(b_2)$.

2. (10 points) Let $f : A \to B$ and $g : B \to C$ be one to one functions. Prove that $g \circ f$ is also one to one.

   Suppose that a, $a' \in A$ and $g \circ f(a) = g \circ f(a')$. Then, $g(f(a)) = g(f(a'))$. Since g is one to one, $f(a) = f(a')$. Finally, since f is one to one, $a = a'$.

3. (10 points) Prove that commutivity is a structural property of binary structures.

   Suppose that $f : (B, *) \to (B', *')$ is an isomorphism and suppose that $(B, *)$ is commutative. We must show that $(B', *')$ is also commutative. To this end, let a', $b' \in B'$. Since f is onto there are a, $b \in B$ such that $f(a) = a'$ and $f(b) = b'$. Therefore,

$$\begin{aligned} a' *' b' =& f(a) *' f(b) \\ =& f(a * b) \text{ since } f \text{ is a homomorphism} \\ =& f(b * a) \text{ since } (B, *) \text{ is commutative} \\ =& f(b) *' f(a) \text{ since } f \text{ is a homomorphism} \\ =& b' *' a'. \end{aligned}$$

4. (20 points)

   (a) Prove that $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

- Let x, $y \in 2\mathbb{Z}$. Then, by definition, there are integers m and n such that $x = 2m$ and $y = 2n$. Therefore,

$$\begin{aligned} x + y =& 2m + 2n \\ =& 2(m+n) \in \mathbb{Z} \text{ since } \mathbb{Z} \text{ is closed under addition.} \end{aligned}$$

  We just checked that $2\mathbb{Z}$ is closed under addition.
- Since $0 = 2 \cdot 0$, $0 \in 2\mathbb{Z}$. We checked that the identity element of $\mathbb{Z}$ is in $2\mathbb{Z}$.
- Let $x \in 2\mathbb{Z}$. Then, $x = 2m$ for some $m \in \mathbb{Z}$. It follows that $-x = 2(-m) \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under taking inverses. We checked that the inverse of an element of $2\mathbb{Z}$ is in $2\mathbb{Z}$.

Hence, $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(b) Is the subgroup $2\mathbb{Z}$ isomorphic to $(\mathbb{Z}, +)$?

We will check that $f : \mathbb{Z} \to 2\mathbb{Z}$ given by $f(x) = 2x$ is an isomorphism.

- Let $a, b \in \mathbb{Z}$ satsify $f(a) = f(b)$. Then $2a = 2b$ and so $a = b$. We checked that f is one to one.
- Let $x \in 2\mathbb{Z}$. Then, there is $m \in \mathbb{Z}$ such that $x = 2m$. It follows that $f(m) = 2m = x$. We checked that f is onto.
- Suppose that m, $n \in \mathbb{Z}$. Then, $f(m+n) = 2(m+n) = 2m + 2n = f(m) + f(n)$. We checked that f is a homomorphism.

Hence, f is an isomorphism.

5. (10 points) Suppose that a is an element of the group $(G, *)$. Prove that the inverse of a in G is unique.

   Suppose that a' and a'' are both inverses for a. Then, $a * a' = e = a * a''$. Left multiplying both sides of the equation $a * a' = a * a''$ by a' gives $a' * (a * a') = a' * (a * a'')$. By associativity, $(a' * a) * a' = (a' * a) * a''$. Hence, $e * a' = e * a''$ and $a' = a''$.

6. (10 points) Is there an isomorphism from $(\mathbb{Z}_6, +_6)$ to $(\mathbb{Z}_6, +_6)$ that takes 5 to 2?

   If $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ is a homomorphism then $f(5 +_6 5 +_6 5 +_6 5) = f(5) +_6 f(5) +_6 f(5) +_6 f(5)$. Evaluating left and right hand sides gives $f(2) = 2$. Since the distinct elements 5 and 2 both are taken to 2 by f, f is not one to one. We have seen that if f a homomorphism taking 5 to 2,then f is not one to one. In particular, there is no isomorphism taking 5 to 2.