Math 541 Spring 2011
Homework#1—Answers, 8/2/11

Definition. A group is a triple $(G, \cdot, 1_G)$, where G is a set, $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h$, is a map, called *operation,* and $1_G \in G$ a specific element, called *identity*, such that the following axioms are satisfied:

- Associativity. We have $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for every $g_1, g_2, g_3 \in G$.
- Identity. The element 1_G satisfies $1_G \cdot g = g \cdot 1_G = g$ for every $g \in G$.
- Inverse. For every $g \in G$ there exists $g' \in G$ such that $g \cdot g' = g' \cdot g = 1_G$. We will denote such a g' (it turns out that it is unique see $2.b.$ below) usually by g^{-1}.

1. Check which of the following is a group

   (a) The set $\mathbb{R}$ with the standard operation of addition $+$ and identity element 0.

      1. Answer. It is a group.
      2. Main points: Usual properties of addition of real numbers.
      3. Checking :
         1. Operation. Indeed the addition $+$ is an operation on the reals, i.e., for every $x, y \in \mathbb{R}$, also $x + y \in \mathbb{R}$.
         2. Associativity. Holds for addition of real numbers.
         3. Identity. Indeed, if $\in \mathbb{R}$, then $x + 0 = 0 + x = x$.
         4. Inverse. Indeed, if $x \in \mathbb{R}$, then $x' = -x$ satisfies $x + x' = x' + x = 0$.

   (b) The set $\mathbb{N} = \{0, 1, 2, ...\}$ of natural numbers, with the standard operation of addition and the element 0 as identity.

      1. Answer. It is not a group.
      2. Main points. Inverse.
      3. Checking. The inverse axioms is not satisfied. There is no $x \in \mathbb{N}$ so that $1 + x = 0$.

   (c) The set $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ of integers, with the standard operation of addition and the element 0 as identity.

      1. It is a group.
      2. Main points. Standard properties of integers.
      3. Checking. Nothing really to check.

   (d) The triple $(\mathbb{R}^\times, \cdot, 1)$ where $\mathbb{R}^\times = \mathbb{R} - 0$ the set of all non-zero real numbers, $\cdot$ is the usual multiplication of real numbers, and 1 is the usual number 1.

      1. Answer. It is a group.
      2. Main points. Closure, and inverses.
      3. Checking:

1. Operation. Indeed, if x, y are non-zero real numbers then also $x \cdot y \in \mathbb{R} - 0$.
2. Associativity. Standard property of $\cdot$ of real numbers.
3. Identity. $1 \cdot x = x$ for every $x \in \mathbb{R}$.
4. Inverse. If x is a non zero real number then we know that there exists x' nonzero real such that $x \cdot x' = x' \cdot x = 1$.

(e) Denote by $GL_2(\mathbb{R})$ the set of all 2×2 invertible matrices with real entries

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R} \text{ and there exists } A^{-1} \right\}.$$

Show that with the operation $\circ$ of matrix multiplication the triple $(GL_2(\mathbb{R}), \circ, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$ is a group.

1. Answer. It is a group.
2. Main points. Closure.
3. Checking.
   1. Operation. Indeed, if $A, B \in GL_2(\mathbb{R})$ then also $A \circ B$. In fact we can even compute the inverse and we have $(A \circ B)^{-1} = B^{-1} \circ A^{-1}$.
   2. Associativity. We have for matrix multiplication in general.
   3. Identity. I satisfies what is required.
   4. Inverse. In this case it is by definition of $GL_2(\mathbb{R})$.

(f) The triple $(M_2(\mathbb{R}), +, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix})$ where $M_2(\mathbb{R})$ denotes the set of all 2×2 matrices with real entries, and $+$ denotes standard addition of matrices.

1. Answer. It is a group.
2. Main points. Regular checking of axioms.
3. Checking. Standard.

2. Properties of groups. Let $(G, \cdot, 1)$ be a group. Show that:

(a) If e and e' are elements of G which satisfy $e \cdot g = g \cdot e = g$ and $e' \cdot g = g \cdot e' = g$ then $e = e'$.

1. Main points. Definition of identity.
2. Proof. We have $e = e \cdot e' = e'$, where the first equality follows from the fact that e' is an identity and the second from the fact that e' is an identity.

(b) If g,g', g'' are elements of G, and $g \cdot g' = g' \cdot g = 1$ and $g'' \cdot g = g \cdot g'' = 1$ then $g' = g''$.

1. Main points. Definition of an inverse.
2. Proof. $g' = g' \cdot 1 = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = 1 \cdot g'' = g''$.

(c) If $g, g' \in G$ and $g \cdot g' = 1$ then $g' \cdot g = 1$.

1. Main points. Inverse.

2. Proof. Multiply both sides of $g \cdot g' = 1$ by an inverse g'' of g we see that $g' = g''$ so we conclude again that the inverse is unique and that $g' \cdot g = g''g = 1$.

(d) For every $g \in G$ we have $(g^{-1})^{-1} = g$.

1. Main points. Definition of inverse.
2. Proof. Indeed, g is the inverse of g^{-1}.

(e) For every $g, h \in G$ we have $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

1. Main points. Definition of inverse.
2. Proof. Compute $(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) = h^{-1} \cdot (g \cdot g^{-1}) \cdot h = h^{-1} \cdot h = 1$.

3. Permutations. Let X be the set $X = \{a, b, c\}$. A function $\sigma : X \to X$ is called *bijection*, or *permutation*, or *isomorphism*, or *automorphism* if it is: (A) One-to-one, also denoted $1-1$, i.e., σ satisfies the property that $\sigma(x) = \sigma(y)$ implies $x = y$ for every $x, y \in X$,and (B) Onto, i.e., σ satisfies the property that for every $y \in X$ there exists $x \in X$ with $\sigma(x) = y$.

(a) Denote by $Aut(X) = \{\sigma : X \to X \,;\, \sigma \text{ is a bijection}\}$ the set of ALL bijections from X to itself. Show that with the operation of standard composition $\circ$ of functions, and the element $id : X \to X$, $id(x) = x$ for every $x \in X$, we have that the triple $(Aut(X), \circ, id)$ is a group. The group $Aut(\{a, b, c\})$ is also denoted by S_3 and is called sometime the symmetric group on three letters.

1. Main points. Closure and inverse.
2. Proof. In fact we will show that for any non-empty set X the triple $(Aut(X), \circ, id)$ is a group.
   1. Closure. We know from set theory that the composition of two one-to-one and onto functions is a one-to-one and onto function. So $Aut(X)$ is close under $\circ$, i.e., for every $\sigma, \tau \in Aut(X)$ we have also that $\sigma \circ \tau \in Aut(X)$.
   2. Associativity. Holds for composition of any three functions in general.
   3. Identity. For any $x \in X$, and any $\sigma \in Aut(X)$ we have $(\sigma \circ id)(x) = \sigma(id(x)) = \sigma(x) = id(\sigma(x)) = (id \circ \sigma)(x)$. So, $\sigma \circ id = \sigma = id \circ \sigma$.
   4. Inverse. A function from X to itself is invertible if and only if it is one-to-one and onto.

(b) Show that the number of elements in S_3 is 6.

1. Main points. Counting.
2. Proof. How we build a function in $Aut(X)$? We can send a to any of the three options a, b, c. Once we are done with it we can send b to two options, and then there is only one option for c. So, $3 \cdot 2 \cdot 1 = 6$ functions in $Aut(X)$.

(c) Write all the elements of S_3.

1. Answer.

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

(d) A group G is called *commutative* if $g \cdot h = h \cdot g$ for every $g, h \in G$. Show that the group $(\mathbb{Z}, +, 0)$ of integers is commutative. Show that the group S_3 is not commutative.

1. Answer. About $\mathbb{Z}$ we know this. About S_3 lets compute

$$\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \neq \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}.$$

- **Remark:**
  - I will be happy to answer any question related to these solutions. Please visit me in my office hours.

Good Luck!