Math 531 Homework 4

Theo Koss

February 2021

1 Section 3.1

- Problem 2: For each binary operation $*$ defined on a set below, determine whether or not $*$ gives a group structure on the set. If it is not a group, say which axioms fail to hold.

  (a) Define $*$ on $\mathbb{Z}$ by $a * b = ab$. This is not a group. It fails to have inverses for every elements except -1 and 1.

  (b) Define $*$ on $\mathbb{Z}$ by $a * b = \max\{a, b\}$. This operation fails to have an identity.

  (c) $*$ on $\mathbb{Z}$, $a*b = a-b$. This is not a group. It fails to be associative.

  (d) $*$ on $\mathbb{Z}$, $a * b = |ab|$. This is not a group. It fails to have inverses.

  (e) $*$ on $\mathbb{R}^+$, $a * b = ab$. This is a group, Identity: 1. Inverses: $\forall a \in \mathbb{R}^+, a \cdot \frac{1}{a} = e$, and $\frac{1}{a}$ is of course in $\mathbb{R}^+$.

  (f) $*$ on $\mathbb{Q}$, $a * b = ab$. This is a group, Identity: 1. $\forall a \in \mathbb{Q}, a \cdot \frac{1}{a} = e$, and $\frac{1}{a}$ is again in $\mathbb{Q}$.

- Problem 3: Let $(G, \cdot)$ be a group. Define a new bin. op. $*$ on G by the formula $a * b = b \cdot a$, for all $a, b \in G$.

  (a) Show that $(G, *)$ is a group.

  Proof. Without loss of generality, assume $\cdot$ is defined by $a \cdot b = a+b$, for some $a, b \in G$, and where $+$ denotes traditional addition. Then $*$ is defined as $a * b = b \cdot a = b + a$. This is clearly a group. QED

(b) $(G, *) = (G, \cdot)$ iff $(G, \cdot)$ is an abelian group.

- Problem 11: Show that the set of all 2×2 matrices over $\mathbb{R}$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$ forms a group under matrix multiplication.

  Proof. For notation's sake, call this set G. To prove this is a group, we N2S three things,

  i There exists an identity element. Naturally, the identity element is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, this is of course in the set, as $1, 0 \in \mathbb{R}$.

  ii There exists inverses for each element in $\mathbb{R}$. The inverse for each matrix $A \in G$ is $A^{-1} = \frac{1}{m}\begin{bmatrix} 1 & -b \\ 0 & m \end{bmatrix} = \begin{bmatrix} \frac{1}{m} & -\frac{b}{m} \\ 0 & 1 \end{bmatrix} \in G$. Therefore, each element has an inverse.

  iii The group operation is associative. Here we check: $\forall A, B, C \in G$, $(AB)C = A(BC)$.
  $(AB) = \begin{bmatrix} m_a & b_a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_b & b_b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_a m_b & m_a b_b + b_a \\ 0 & 1 \end{bmatrix}$.
  $(AB)C = \begin{bmatrix} m_a m_b & m_a b_b + b_a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_c & b_c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_a m_b m_c & m_a m_b b_c + m_a b_b + b_a \\ 0 & 1 \end{bmatrix}$.
  $A(BC) = \begin{bmatrix} m_a & b_a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_b m_c & m_b b_c + b_b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_a m_b m_c & m_a m_b b_c + m_a b_b + b_a \\ 0 & 1 \end{bmatrix}$
  $= (AB)C$. Therefore it is associative.

  QED

- Problem 24: Let G be a group. Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G$.

  Proof. Using these definitions,

  $$ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$$

  Therefore, if $(ab)^{-1} = a^{-1}b^{-1}$, then G must be abelian.
  For the other direction, if G is abelian, then $ab = ba$. So we N2S that $(ab)^{-1} = a^{-1}b^{-1}$ follows from this. Indeed it does:

  $$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \text{ Since } G \text{ is abelian}$$

  As required. QED

2 Section 3.2

- Problem 1:

  (a) $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ Has order 6, because $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^6 = I$.

  (b) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^4 = I$, order 4.

  (c) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, therefore this element has infinite order.

  (d) $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}^2 = I$, order 2.

- Problem 3: Prove that the set of all rational numbers of the form $\frac{m}{n}$ where $m, n \in \mathbb{Z}$ and n is square-free, is a subgroup of Q under addition.

  Proof.

  Theorem 1 (Subgroup Test)**.** *Let G be a group and let H be a nonempty subset of G. If for all $a, b \in H$, $ab^{-1} \in H$, then $H \leqslant G$.*

  Proof of 1 here.
  Using 1, we N2S $\forall a, b \in H, ab^{-1} \in H$. In this case, that looks like

  $$ab^{-1} = \frac{m_a}{n_a} - \frac{m_b}{n_b} \in H$$

  This is of course true, because one of two things can happen, either

  (i) n_a and n_b will share a divisor, in this case, the lcm of the two is that shared (prime, and therefore squarefree) factor.

  (ii) n_a and n_b will be relatively prime, in this case, their product will be squarefree, so the denominator will be squarefree, as required.

  QED

- Problem 7: Give an example of 3 permutations $\alpha, \beta, \gamma \neq e \in S_4$. Such that $\alpha\beta = \beta\alpha$ and $\beta\gamma = \gamma\beta$, but $\alpha \neq \gamma$.
  Let $\beta = (23), \alpha = (1342), \gamma = (14)$, of course, since β and γ are disjoint, they commute. $\alpha\beta = (1342)(23) = (12)(34) = (23)(1342) = \beta\alpha$ as required.

- Problem 12: Let $\sigma \in S_n$, and suppose σ is written as a product of disjoint cycles. Show that σ is even iff the number of cycles of even length is even. And show σ is odd iff number of cycles of even length is odd.*Ask in class*

  Proof. QED