

M 431: Assignment 3

Nathan Stouffer

Page 48 — Problem 29

Problem. Let G be a finite, nonempty set with an operation $*$ such that:

1. G is closed under $*$
2. $*$ is associative
3. Given $a, b, c \in G$ with $a * b = a * c$, then $b = c$
4. Given $a, b, c \in G$ with $b * a = c * a$, then $b = c$

Prove that G must be a group under $*$.

Proof. To prove that $(G, *)$ is a group, we must show that G contains an identity element and an inverse for each element. Let's begin with the identity element. We must find an element $e \in G$ such that $x * e = e * x = x$ for all $x \in G$. Let $|G| = n < +\infty$ and fix an element $g \in G$ and consider $g, g^2, g^3, \dots, g^{n+1}$. Since G is closed under $*$, every g^k is an element of G , yet G has only n elements so we must at least have $g^i = g^j$ for some $1 \leq i < j \leq n + 1$.

Now let $l = j - i > 0$ (which means $j = l + i = i + l$) and we can say that $g^j = g^{l+i} = g^l * g^i$ and $g^j = g^{i+l} = g^i * g^l$. But then $g^j = g^i$ so we have $g^i = g^i * g^l = g^l * g^i$. Letting $g^i = \bar{g}$ and $g^l = \bar{e}$ (both elements of G by closure under $*$) gives us $\bar{g} = \bar{g} * \bar{e} = \bar{e} * \bar{g}$ for the specific element $\bar{g} \in G$.

We now show that \bar{e} is an identity element for every element of G . Fix any $x \in G$, then $\bar{g} * x = \bar{g} * \bar{e} * x$ since $\bar{g} = \bar{g} * \bar{e}$. But then property 3 says that $x = \bar{e} * x$. Further, $x * \bar{g} = x * \bar{e} * \bar{g}$ since $\bar{e} * \bar{g} = \bar{g}$ and then property 4 allows us to say that $x * \bar{e} = x$. So we have just shown that $x * \bar{e} = \bar{e} * x = x$ for an arbitrary $x \in G$. In other words, \bar{e} is an identity element for G .

Now we must show an inverse element exists for every element of G : that there exists some element $g' \in G$ such that $g * g' = g' * g = \bar{e}$. To do this, we take g and $g^l = \bar{e}$ as before. Pick $g' = g^{l-1} \in G$ then $g * g' = g * g^{l-1} = g^{1+l-1} = g^{l+1-1} = g^l = \bar{e}$ and $g' * g = g^{l-1} * g = g^{l-1+1} = g^l = \bar{e}$ as desired. Since we chose g arbitrarily, we have just shown every element has an inverse in G .

So we have showed that an identity exists in G and each element has an inverse so G satisfies the conditions of a group.

□

Page 54 — Problem 3

Problem. Let S_3 be the symmetric group of degree 3. Find all the subgroups of S_3 .

Proof.

□

Page 55 — Problem 12

Problem. Prove that a cyclic group is abelian.

Proof. Let's first introduce the definition of a cyclic group. A group G is cyclic if there exists some $a \in G$ such every $x \in G$ is a power of a ($x = a^j$ for some $j \in \mathbb{Z}$). Additionally, a group is abelian if $ab = ba$ for all $a, b \in G$.

Suppose we have some cyclic group G . Since G is cyclic, there is some $g \in G$ such that every $x \in G$ is of the form $x = g^j$ for some $j \in \mathbb{Z}$. Now take any $a, b \in G$ and note that $a = g^i$ and $b = g^k$ for some $i, k \in \mathbb{Z}$. Then $ab = g^i g^k = g^{i+k} = g^{k+i} = g^k g^i = ba$ as desired. Therefore, every cyclic group is abelian.

□

Heisenberg group problem

Problem. Recall the general linear group $\mathbb{GL}_3(\mathbb{R})$ of 3×3 invertible matrices with real entries (taken with the matrix product). Verify that the following subset, called the Heisenberg group, is a subgroup of $\mathbb{GL}_3(\mathbb{R})$:

$$\mathbb{H}_3(\mathbb{R}) := \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \mid x, y, z \in \mathbb{R} \right\}$$

Proof.

□

Cube subgroups problem

Problem. Recall the group $Sym(Q)$ of the rigid symmetries of the cube $Q := [-1, 1]^3$ in \mathbb{R}^3 . Describe in words/pictures the following:

- a subgroup of order 4
- a subgroup of order 12
- a subgroup of order 3
- a subgroup of order 6
- a subgroup of order 8

Proof.

□