

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 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. First note that we always have the trivial subgroups $\{id\}$ and S_3 . We must now find the remaining subgroups of S_3 . Note that $|S_3| = 3! = 6$ and for any subgroup $H \leq S_3$, we must have $id \in H$. This leaves us only 5 options to include in a subgroup H . If we choose one of the elements $(12), (23), (13)$ to accompany id then we have a subgroup for each of those elements is it's own inverse. So in addition to the trivial subgroups we also have $\{id, (12)\}, \{id, (23)\}, \{id, (13)\}$.

Note that the remaining elements we can choose to accompany id are $(123) = (312) = (231)$ and $(132) = (213) = (321)$. Now suppose we choose one of $(123), (132)$ to accompany id . Then Figure 1 shows that the other must also be in the subgroup to satisfy closure. Also each of them applied 3 times to the themselves so we have inverses as well. Therefore $\{id, (123), (132)\}$ constitutes a subgroup as well.

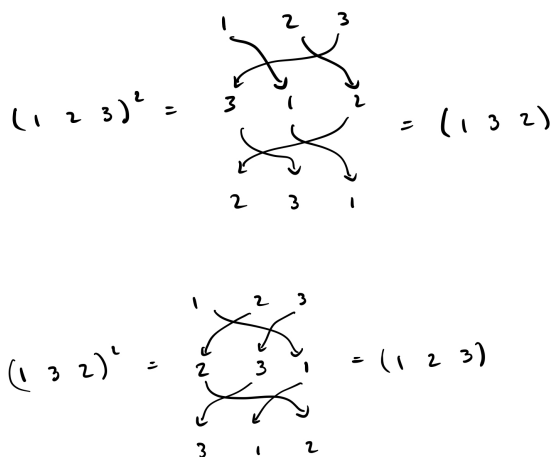


Figure 1: Necessary closure for 3 cycles

We now show that we have listed all subgroups of S_3 . We can deduce this from the requirement that a subgroup requires closure. Of the remaining combinations of elements we could choose to accompany id in a subgroup, all of them require including the whole group. This is shown in Figures 2 and 3. As an example pick elements (12) , (23) to accompany id . To satisfy closure, we must include (123) (Figure 2) but then we must include (132) (Figure 1) and then we must include (13) (Figure 3) which is the entire set.

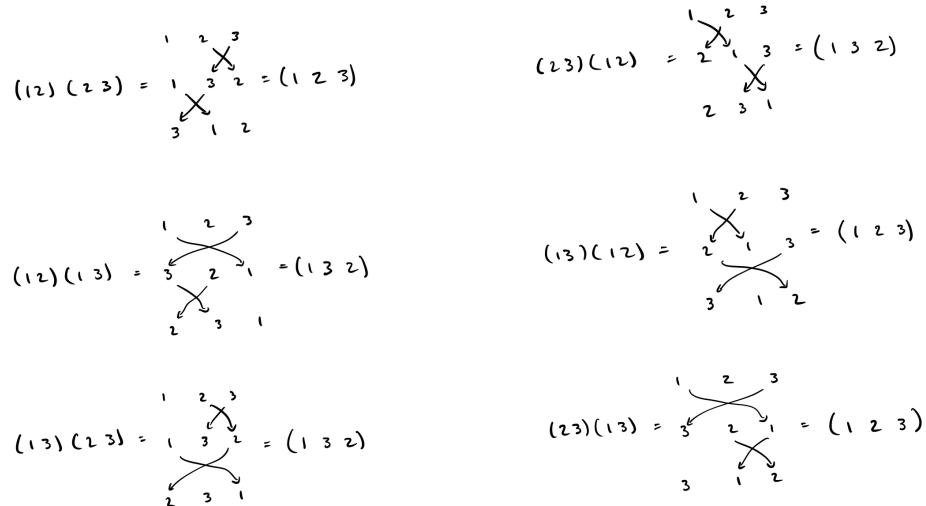


Figure 2: Necessary closures

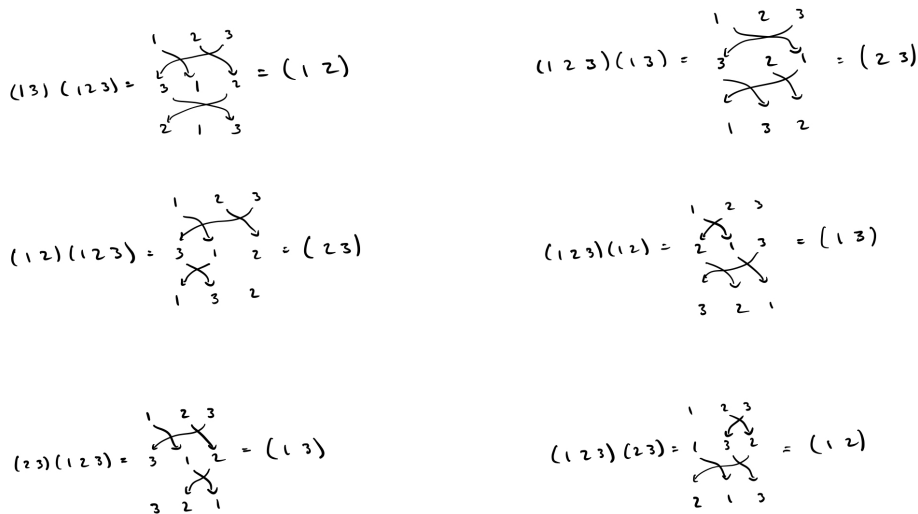


Figure 3: Necessary closures

□

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 $\mathrm{GL}_3(\mathbb{R})$ 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 $\mathrm{GL}_3(\mathbb{R})$:

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

Proof. First we note that $\mathbb{H}_3(\mathbb{R})$ is a (nonempty) subset of $\mathrm{GL}_3(\mathbb{R})$ since $I_3 \in \mathbb{H}_3(\mathbb{R})$ and every matrix in $\mathbb{H}_3(\mathbb{R})$ has rank 3. Then since $\mathbb{H}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R})$ we automatically inherit the associativity of matrix multiplication. So only two conditions remain for $\mathbb{H}_3(\mathbb{R})$ to be a subgroup: closure and the existence of an inverse in $\mathbb{H}_3(\mathbb{R})$. The previous two conditions imply $I_3 \in \mathbb{H}_3(\mathbb{R})$ but this was also verified by inspection.

Let's first prove closure. Pick $A, A' \in \mathbb{H}_3(\mathbb{R})$ and compute

$$AA' = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x' + x & z' + xy' + z \\ 0 & 1 & y' + y \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \bar{x} & \bar{z} \\ 0 & 1 & \bar{y} \\ 0 & 0 & 1 \end{bmatrix} \in \mathbb{H}_3(\mathbb{R})$$

where $\bar{x}, \bar{y}, \bar{z} \in \mathbb{R}$ by the closure of \mathbb{R} under addition and multiplication. So $\mathbb{H}_3(\mathbb{R})$ is closed under matrix multiplication. We must now show that for every $A \in \mathbb{H}_3(\mathbb{R})$ we also have $B \in \mathbb{H}_3(\mathbb{R})$ such that $AB = BA = I_3$. For A , choose

$$B = \begin{bmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{bmatrix}$$

Certainly B is in the set $\mathbb{H}_3(\mathbb{R})$ and we have

$$AB = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} = BA$$

So we have checked that $\mathbb{H}_3(\mathbb{R})$ is closed under matrix multiplication and every element has an inverse in the subset so $\mathbb{H}_3(\mathbb{R})$ is a subgroup of $\mathrm{GL}_3(\mathbb{R})$.

□

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. For the purposes of this problem, we label the initial faces of the cube as you would a die (with side one facing us and side 6 opposite and so on).

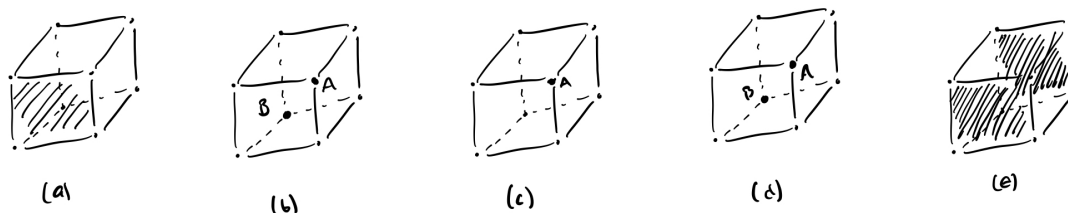


Figure 4: Subgroups of a cube

Order 4: We can make subgroup of order 4 by keeping all rigid symmetries of Q that keep us looking at the same face. In Figure 4(a) we shaded in this face. The subgroup is any symmetric rotation about the x axis, of which there are 4.

Order 12: I found an order 12 subgroup to be the most difficult to find. Here is what I have landed on: any rigid symmetry that preserves A 's position in Figure 4(b) and a rotation by π about the z axis. The next part says that preserving A is a group of order 3 and then we get four distinct subgroups from the points that could end up in A 's location (these are A and each of the points across the diagonal of a *square* touching A). Then the subgroup is of order 12.

Order 3: A subgroup of order 3 can be found by requiring that the vertex labeled A in Figure 4(c) stays in the same location. This allows us three actions, synonymous with spinning the cube about A and the point diagonally through the cube from A .

Order 6: An order 6 subgroup is pretty similar to the order 3 subgroup we just discussed. Instead of requiring that A stays in the same location, we say that A and B in Figure 4(d) must remain on the diagonal they begin on. This gives the three actions when A is stationary and another three actions when we flip A and B (which can be done by a rotation by π about z axis and then a rotation by $\pi/2$ about x axis).

Order 8: For a subgroup of order 8, we require that we look at one of the two shaded faces shown in Figure 4(e). This gives us four actions while looking at face 1 and another four while looking at face 6.

□