PROBLEM SET 4

HAMID SAGBAN

Exercise 1. *Let* $S = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbb{R} \setminus 0 \right\}$. *Show that* $(S, *)$ *is a group with* $*$ *the normal multiplication of matricies.*

Proof. We first show closure. Take two elements $\alpha, \beta \in S$. Then $\alpha = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$ and $\beta = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$, for some $a, b \in \mathbb{R} \setminus 0$. We have to show that $\alpha\beta \in S$. Computing $\alpha\beta$, we get $\alpha\beta = \beta\alpha = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}$, with $2ab \in \mathbb{R} \setminus 0$. Thus $\alpha\beta \in S$. We now show that $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is the identity of S. Take $\gamma \in S$, with $\gamma = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$, for some $y \in \mathbb{R} \setminus 0$. Then $\begin{bmatrix} y & y \\ y & y \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$. Finally, take $\eta \in S$, with $\eta = \begin{bmatrix} n & n \\ n & n \end{bmatrix}$, for some $n \in \mathbb{R} \setminus 0$. We show that $\eta^{-1} = \begin{bmatrix} \frac{1}{4n} & \frac{1}{4n} \\ \frac{1}{4n} & \frac{1}{4n} \end{bmatrix}$. But $\begin{bmatrix} n & n \\ n & n \end{bmatrix} \begin{bmatrix} \frac{1}{4n} & \frac{1}{4n} \\ \frac{1}{4n} & \frac{1}{4n} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$. The claim thus follows.

We can also conclude that S is abelian, for, as shown above, $\alpha\beta = \beta\alpha$ for arbitrary $\alpha, \beta \in S$. □

Exercise 2. *A set* $(S, *)$ *is said to be a left-cancellative set if whenever* $a, b, c \in S$ *(not necessarily distinct),* $a * b = a * c$ *implies* $b = c$*. Similarly, a set* $(S, *)$ *is said to be a right-cancellative set if whenever* $a, b, c \in S$ *(not necessarily distinct),* $b * a = c * a$ *implies* $b = c$*.*

(a) *Let* $(G, *)$ *be a group. Prove that* G *is both left-cancellative and right-cancellative.*

(b) *Give an example of a monoid* $(M, *)$ *that is neither left-cancellative nor right-cancellative.*

Proof. For (a), take $a, b, c \in G$. Then $a * b = a * c \implies a^{-1} * a * b = a^{-1} * a * c \implies b = c$. Also, $b * a = c * a \implies b * a * a^{-1} = c * a * a^{-1} \implies b = c$. For (b), take $(\mathbb{Z}, \times)$, with $5, 3, 0 \in \mathbb{Z}$. Then $0 \times 5 = 0 \times 3 \not\Longrightarrow 5 = 3$, and $5 \times 0 = 3 \times 0 \not\Longrightarrow 5 = 3$. □

Exercise 3. *Let $(M, *)$ be a group, and H a subgroup of M.*

(a) *Suppose there is an $a \in M \setminus H$ and choose an element $h \in H$. Prove that the left coset $a * H$ is the same as the left coset $a * h * H$.*

(b) *Suppose there is an $a \in M \setminus H$ and suppose that $a * H = b * H$ for some $b \in M$. Show that $b \in a * H$.*

Proof. To show (a), it suffices to show that $h * H = H$, for $h \in H$. If not, then either $h * H$ is not a subset of H, or H is not a subset of $h * H$.

Suppose the former, then there is at least one element $k \in h * H$ but not in H. We know that $h * H = \{h * j \mid j \in H\}$, so $k = h * h_i$ where $h_i \in H$. But we know that $h \in H$ and H is closed under $*$, so $k \in H$, contradiction. Thus $h * H$ must be a subset of H.

Now suppose the latter, then there is at least one element $k \in H$ but not in $h * H$. That is, $k = h_j$ for some $h_j \in H$ but $k \notin h * H$. But since $k \in H$, then exists some element in $h * H$, call it y, such that $y = h * k$, so that $k = h^{-1} * y = h^{-1} * h * k = h * (h^{-1} * k) \in h * H$ since $h^{-1} * k \in H$, a contradiction. Thus H is a subset of $h * H$.

For (b), certainly $b \in b * H$ since $b * e = b$. We also know that $b * H = a * H$, so $b \in a * H$ and we are done. □

Exercise 4. *Let $(M, *)$ be a group. Then*

(a) *Suppose that $a * b = b * a$ for some $a, b \in M$. Prove that $a * b^{-1} = b^{-1} * a$ and $a^{-1} * b^{-1} = b^{-1} * a^{-1}$.*

(b) *Suppose that $a \in M$ and $|a| = m$. Show that $|a^{-1}| = m$.*

(c) *Let $\alpha = (2\ 3\ 4) \circ (2\ 3\ 4) \circ (1\ 3\ 4\ 2\ 5) \in S_5$. Find $|\alpha|$.*

Proof. For the first part of (a), we have $a * b^{-1} = e * a * b^{-1} = b^{-1} * b * a * b^{-1} = b^{-1} * a * b * b^{-1} = b^{-1} * a * e = b^{-1} * a$. For the remaining part of (a), we have $a^{-1} * b^{-1} = a^{-1} * b^{-1} * e = a^{-1} * b^{-1} * a * a^{-1} = a^{-1} * a * b^{-1} * a^{-1} = e * b^{-1} * a^{-1} = b^{-1} * a^{-1}$ by an application of the first part of (a).

For (b), we make use of the fact that $(x^a)^b = x^{ab}$ for $a, b \in \mathbb{Z}$. We have $(a^{-1})^m = a^{-m} = (a^m)^{-1} = e$. It remains to show that m is the least positive integer such that $(a^{-1})^m = e$. If $m = 1$, then we are done. Otherwise asssume that $m > 1$. If m is not the order of a^{-1}, then we can find an integer $k < m$ such that $(a^{-1})^k = e$. That is, $(a^k)^{-1} = e$, so that $a^k = e^{-1} = e$. But m is the least such positive integer, contradiction.

Finally, for part (c), we have $\alpha = (1\ 2\ 5) \circ (3) \circ (4) = (1\ 2\ 5)$. Thus $|\alpha| = 3$. □

Exercise 5. *Let M be a finite set with a binary operation $*$ acting on M. Suppose $(M, *)$ is a semigroup that is left and right-cancellative. Show that $(M, *)$ is a group, and give an example of a semigroup that is cancellative from both sides but is not a group.*

Proof. Choose $\phi \in M$, and construct $M * \phi = \{m * \phi \mid m \in M\}$. Suppose $|M| = k$, we show that the order of $|M| = |M * \phi|$, but this is clear by choosing $m_i, m_j \in M$ for some $i, j \in \{1, 2, \ldots, k\}$, since we have $m_i * \phi = m_j * \phi \implies m_i = m_j$ by the right-cancellative property. By construction, $M * \phi \subset M$, so this, combined with the fact that $|M| = |M * \phi|$, gives us $M = M * \phi$. By an application of the left-cancellative property, one can construct and show, using an argument similar to the above, that $M = \phi * M$.

Since $\phi \in M$, by construction, we have $\phi = e * \phi$ for some $e \in M$. Now take any element $\alpha \in M$, we have $\alpha * \phi = \alpha * e * \phi \implies \alpha = \alpha * e$ by the right-cancellative property. We have thus found a right identity for M, referred to as e. Similarly, we can find a left identity by an application of the left-cancellative property. So now we have $e * \alpha = \alpha * e = \alpha$ for any $\alpha \in M$.

We have a two-sided identity. To imply a group structure, it suffices to show existence of right-inverse. We know that $e = \phi * m_l$ for some $m_l \in M$. Thus m_l is the right-inverse of ϕ. But note that the choice of ϕ is arbitrary; we can similarly form $\gamma * M$ to get an element m_k such that $e = \gamma * m_k$, and so forth; this process will end since we have finitely many elements. This completes the argument.

$(\mathbb{N}, +)$ can serve as an example of a right and left cancellative semigroup that is not a group. ☐