Problem 1 (Ch. 1.2)

Determine $\alpha\beta$, $\beta\alpha$, and α^{-1} in S_5 if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

Solution. We can compose our two permutations to get:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

To get our inverse, we will just reverse the permutation of α:

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

We can confirm that this is an inverse by confirming that

$$\alpha\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1_{S_5}$$

$$\alpha^{-1}\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1_{S_5}$$

Problem 4 (Ch. 1.2)

Let G be the set of pairs of real numbers (a, b) with $a \neq 0$ and define: $(a, b)(c, d) = (ac, ad + b), 1 = (1, 0)$. Verify that this defines a group.

Solution. Let $(a, b), (c, d), (e, f) \in G$. Note that the group is indeed closed under the multiplication: since G is the set of all pairs of real numbers, and the reals are closed under addition and multiplication, the resulting product is a pair of real numbers as well.

Now we verify that the multiplication is associative. See

$$\begin{aligned} \big((a, b)(c, d)\big)(e, f) &= (ac, ad + b)(e, f) \\ &= (ace, acf + ad + b) \\ &= (ace, a(cf + d) + b) \\ &= (a, b)(ce, cf + d) \\ &= (a, b)\big((c, d)(e, f)\big) \end{aligned}$$

where we use the distributive property of the reals in the third line.

Next, we show that $1 = (1, 0)$ is an inverse. See

$$1(a, b) = (1, 0)(a, b) = (a, b)$$

$$(a, b)1 = (a, b)(1, 0) = (a, b)$$

Finally, we confirm that every element has an inverse. We do this by providing it explicitly for the arbitrary element (a, b), namely $(a, b)^{-1} = (\frac{1}{a}, \frac{-b}{a})$. See

$$(a, b)(a, b)^{-1} = (a, b)\left(\frac{1}{a}, \frac{-b}{a}\right) = (1, 0)$$

$$(a, b)^{-1}(a, b) = \left(\frac{1}{a}, \frac{-b}{a}\right) = (1, 0)$$

This is sufficient to show G with the given multiplication is a group.

Problem 7 (Ch. 1.2)

Show that if an element a of a monoid has a right inverse b, that is, $ab = 1$; and a left inverse c, that is, $ca = 1$; then $b = c$, and a is invertible with $a^{-1} = b$. Show that a is invertible with b as inverse if and only if $aba = a$ and $ab^2a = 1$.

Solution. We have that $(ca)b = c(ab)$ by associativity, but then $1 \cdot b = c \cdot 1 \implies b = c$. Then we have an element such that $ab = ba = 1$ (we replaced b with c since they are equal), which satisifies the condition that a is invertible with inverse $a^{-1} = b$.

Now let a be invertible with b as an inverse. Then $ba = 1$ and so $a(ba) = a \cdot 1 \implies aba = a$. Additionally, we have $ba = 1 \implies 1 \cdot ba = 1 \cdot 1$ and since $ab = 1$, we get $(ab)ba = 1 \implies ab^2a = 1$, as desired. To show the other direction, assume $aba = a$ and $ab^2a = 1$. The second equation gives that ba is a right inverse of ab, but we just proved that this implies ba is also a left inverse, so we have $baab = 1$. We can multiply both sides of the equation by a to get $baaba = a$, and subbing in with $aba = a$, we have $baa = a$. Subbing back into $baab = 1$, we have $ab = 1$. So b is a right inverse of a. Note that a also has a left inverse, namely ab^2 (from $ab^2a = 1$), and existence is enough to invoke what we proved in the first part of this problem, specifically that a is invertible with b as inverse, and so we have proven both directions.

Problem 8 (Ch. 1.2)

Let α be a rotation about the origin in the plane and let ρ be the reflection in the x-axis. Show that $\rho\alpha\rho^{-1} = \alpha^{-1}$.

Solution. We can represent our elements as coordinates in the plane (x, y). Then α is $(x, y) \to (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$ where θ is the angle swept by our arbitrary rotation, and ρ is $(x, y) \to (x, -y)$. Note then that $\rho^{-1} = \rho$, since one can see $\rho\rho = 1$. Note that α^{-1} is just a rotation by θ in the opposite direction, or $-\theta$, so $\alpha^{-1} = (x, y) \to (x\cos(-\theta) - y\sin(-\theta), x\sin(-\theta) + y\cos(-\theta))$. See that

$$\begin{aligned}
\rho\alpha\rho^{-1}(x, y) &= \rho(x\cos\theta + y\sin\theta, x\sin\theta - y\cos\theta) \\
&= (x\cos\theta + y\sin\theta, -x\sin\theta + y\cos\theta) \\
&= (x\cos(-\theta) - y\sin(-\theta), x\sin(-\theta) + y\cos(-\theta) \\
&= \alpha^{-1}(x, y)
\end{aligned}$$

where we used the evenness of cos and the oddness of sin in the third line. Thus, since x, y were arbitrary points in the plane, we have $\rho\alpha\rho^{-1} = \alpha^{-1}$.

Problem 11 (Ch. 1.2)

Show that in a group, the equation $ax = b$ and $ya = b$ are solvable for any $a, b \in G$. Conversely, show that any semigroup having this property contains a unit and is a group.

Solution. We want to show that for all $a, b \in G$ fixed, there exists $x, y \in G$ such that $ax = b$ and $ya = b$ (ie. its solvable). Note that since G is a group, inverses of all elements exist, and so if we multiply the first equation on the left by a^{-1}, we get $a^{-1}ax = a^{-1}b \implies x = a^{-1}b$. Since $a^{-1}, b \in G$ and a group is closed under its operations, $x \in G$ as well. We can repeat this with our second equation to get $y = ba^{-1}$, so $y \in G$. Thus there exists $x, y \in G$ such that our equalities hold, namely $x = a^{-1}b$ and $y = ba^{-1}$.

Conversely, let us assume S is a semigroup such that for all $a, b \in S$, there exists $x, y \in S$ such that $ax = b$ and $ya = b$. We first prove that S contains a unit. Note that our assumptions gaurantees existence of x, y with the restriction of our equations where $a = b$. Then we know there exists $r, l \in S$ such that $ar = la = a$. We prove that $sr = s$ for all $s \in S$ now. We know that there exists $y \in S$ such that $s = ya$. Then $s = y(ar) \implies s = (ya)r \implies s = sr$ as desired. We prove the same for l, that is $ls = s$ for all $s \in S$. We know that there exists $x \in S$ such that $s = ax$. Then $s = (la)x \implies s = l(ax) \implies s = ls$ as desired. Now since we have $lr = r$ and $lr = l$ we have $l = r$.

Denote our identity 1_S (so $r = l = 1_S$). Now we use the assumption again with arbitrary $a \in S$ and $b = 1_S$. So we have that there exists $x, y \in S$ such that $ax = 1_S$ and $ya = 1_S$. But since S is a monoid (a semi-group with a unit), we proved in Problem 7 that since a has a left and right inverse, $x = y$ and a is invertible with $a^{-1} = x$. Thus, S is associative and closed under its operations, has a unit, and each element has an inverse. This is sufficient to show that S is a group.

Problem 13 (Ch. 1.2)

Show that any finite group of even order contains an element $a \neq 1$ such that $a^2 = 1$.

Solution. We prove the contrapositive, that is, given a finite group G, if for all $a \neq 1$, $a^2 \neq 1$, then G is not of even order, that is, of odd order. Note that given any $a \in G$ where $a \neq 1$, we have a corresponding unique $a^{-1} \in G$ such that $a \neq a^{-1}$ (else $a^2 = 1$). Note that a is the inverse of a^{-1} as well, and so this pairs up elements together. The only element that is not paired up with another distinct element is 1, since 1 is its own inverse ($1 \cdot 1 = 1$). Thus we have some number of pairs of elements, and the identity, all distinct, thus G is of odd order, as desired.