Algebraic Structures (MST20010)

Problem sheet 3

1. (a) There are at least 3 ways to proceed (they are actually more or less the same):
(i) We can multiply both sides by a^{-2} (for instance on the left):

$$a^{-2}a^2 = a^{-2}e, \quad a^{-2+2} = a^{-2}, \quad a^0 = a^{-2}, \quad e = a^{-2}.$$

(ii) Multiply twice by a^{-1} (for instance on the left):

$$a^{-1}a^2 = a^{-1}e, \quad a = a^{-1},$$

and then

$$a^{-1}a = a^{-1}a^{-1}, \quad e = a^{-2}.$$

(iii) Take the inverse of both sides:

$$(a^2)^{-1} = e^{-1}, \quad a^{-2} = e.$$

(b) The proof is similar. The easiest to write are probably to multiply both sides by a^{-k} or to take the inverse of both sides.

(c) The order of a is the smallest integer k such that $a^k = e$. But $a^t = e$ exactly when $(a^{-1})^t = e$ (since $(a^{-1})^t = a^{-t}$) by (b). So the smallest integer k such that $a^k = e$ is exactly the smallest integer k such that $(a^{-1})^k = e$, i.e., the order of a is the same as the order of a^{-1}.

2. (a) $(\{-1, 1\}, \cdot)$:
(1) Is the product of two elements of $\{-1, 1\}$ again an element of $\{-1, 1\}$?. Clearly yes.
(G1): Is the product associative? Since it is the usual product, yes (we know it is associative).
(G2): Is there an identity element, i.e., an element e such that $e \cdot a = a$ and $a \cdot e = a$ for every $a \in \{-1, 1\}$? Yes, take $e = 1$.
(G3): For every $a \in \{-1, 1\}$ is there $b \in \{-1, 1\}$ such that $a \cdot b = 1$ (since $e = 1$) and $b \cdot a = 1$? Yes, if $a = 1$ take $b = 1$ and if $a = -1$ take $b = -1$.
So $(\{-1, 1\}, \cdot)$ is a group.

(b) $(\mathbb{N} \cup \{0\}, +)$:
(1) The sum of two elements of $N \cup \{0\}$ is again in $\mathbb{N} \cup \{0\}$.
(G1): The sum is associative (it is the usual sum).
(G2): The identity element if 0.
(G3): This is where it does not work: Not every element has an inverse. The inverse of a would be an element b in $\mathbb{N} \cup \{0\}$ with the property that $a + b = 0$. But 1 does not have an inverse in $\mathbb{N} \cup \{0\}$: If we want $1 + b = 0$ we must take $b = -1$, which is not in $\mathbb{N} \cup \{0\}$.
So $(\mathbb{N} \cup \{0\}, +)$ is not a group.

3. There are 6 elements in S_3, so we just have to find the 6 different ways to list the numbers 1,2,3 (to put on the second row of the permutation).

4. (a)
$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \ \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

(b) $k = 3$.

(c) Since $\alpha^3 = \mathrm{Id}$, we have $\alpha^2\alpha = \alpha^3 = \mathrm{Id}$ and $\alpha\alpha^2 = \alpha^3 = \mathrm{Id}$. Therefore (by definition of the inverse) $\alpha^2 = \alpha^{-1}$.

(d) $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (we saw how to do this in class).

5. (a) We know that S_2 has $2! = 2$ elements. They can we written in the form $\begin{pmatrix} 1 & 2 \\ a & b \end{pmatrix}$ with $a, b \in \{1, 2\}$, so they are $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \mathrm{Id}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. So if we want to check $\sigma\gamma = \gamma\sigma$ for all $\sigma, \gamma \in S_2$ we only have 4 possibilities to check: 2 choices for σ, 2 choices for γ. If $\sigma = \mathrm{Id}$ or $\gamma = \mathrm{Id}$ we have $\sigma\gamma = \gamma\sigma$ (since $\mathrm{Id} \circ f = f \circ \mathrm{Id} = f$ not matter what $f \in S_n$ is. You can do the computation if you prefer). The only remaining case is $\sigma = \gamma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, and then $\sigma\gamma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ while $\gamma\sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$.

(b) It suffices to find two elements α and β in S_n such that $\alpha\beta \neq \beta\alpha$. There are many possibilities (but it needs to use that $n \geq 3$ since we know that the product of elements of S_2 is commutative). The approach here is to try a few at random (you know that one choice of α, β will work, since the exercise asked you to do this). For instance:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$$

$(\alpha(n) = n$ for $n \geq 4)$ and

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$$

$(\beta(n) = n$ for $n \geq 4)$. Computing their products we get

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

(with $\alpha\beta(n) = n$ for $n \geq 4$) and

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

. (with $\beta\alpha(n) = n$ for $n \geq 4$) and We see that $\alpha\beta \neq \alpha\beta$.