Problem sheet 10

1. (a) We saw in class that if a has order n, then $\langle a\rangle = \{e, a, \dots, a^{n-1}\}$, so here $\langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2\}$. I leave it to you to compute σ^2.

   (b) The element (1 2) has order 2, and is contained in H which is a group (because it is a subgroup). We have seen that, in a group, the order of an element always divides the order of the group. So 2 divides $|H|$. Similarly, 3 divides $|H|$ since (1 2 3) has order 3 and belongs to H.

   Therefore H has at least 6 elements. But it is included in S_3 which has 6 elements. So $H = S_3$.

   This provides a quick way to show that every element of S_3 can be written as a product of powers of (1 2) and of (1 2 3).

2. (a) Assume $a^n = a^m$ for some $n \neq m$, say $m > n$. Then $a^{m-n} = e$ (multiply both sides by a^{-n}). So the order of a is finite, $|a| = t$, and thus

   $$G = \{a^k \mid k \in \mathbb{Z}\} = \{e, a, a^2, \dots, a^{t-1}\}$$

   is not infinite. Contradiction.

   (b) Let b be a generator of G: $G = \{b^n \mid n \in \mathbb{Z}\}$, and thus $a = b^t$ for some $t \in \mathbb{Z}$. Since $b \in G$, we have $b = a^k$ for some $k \in \mathbb{Z}$. So $a = b^t = a^{kt}$. We observed that if $n \neq m$ then $a^n \neq a^m$, so we can deduce from $a = a^{kt}$ that $kt = 1$. Since $k, t \in \mathbb{Z}$ we must have $k = t = 1$ or $k = t = -1$. So $b = a$ or $b = a^{-1}$.

3. (a) We prove both directions.

   Assume that $x^k = e$. Then

   $$(yxy^{-1})^k = yxy^{-1}yxy^{-1}\cdots yxy^{-1}.$$

   All the $y^{-1}y$ inside cancel out and we have $(yxy^{-1})^k = yx^ky^{-1} = yey^{-1} = e$.

   Assume that $(yxy^{-1})^k = e$. As above, we have $(yxy^{-1})^k = yx^ky^{-1}$, so $yx^ky^{-1} = e$. Multiplying both sides on the left by y^{-1} and on the right by y gives $x^k = e$.

   (b) The order of an element a is the smallest positive integer k such that $a^k = e$. Therefore question (a) gives the result.

   (c) We have $ba = b(ab)b^{-1}$ and the result follows from (b).

4. Computing that $A^4 = I_2$ and $B^6 = I_2$ is direct. We have $AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, and more generaly $(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ (by induction –in such a simple case you can leave it at this; if you prefer, or if it is complicated, write down the induction step explicitly–)), which proves the result.