MTH6016 Group Theory – Solutions 2

November 21, 2023

1. If a is odd then you should get $\{1, r^2, rs, r^3s\}$ and if a is even then you should get $\{1, r^2, s, r^2s\}$.

   By Lagrange's theorem the order of a subgroup of $\mathcal{D}_8$ must be 1, 2, 4 or 8. Now, repeated (inductive) application of the relation $rs = sr^{-1}$ implies $r^k s = sr^{-k}$ for every $k \in \mathbb{Z}$. This means that $(sr^a)^2 = (r^{-a}s)^2 = r^{-a}sr^{-a}s = r^{-a}r^a ss = 1$ irrespective of the value of a, and $(sr^{a+2})^2 = 1$ by similar reasoning. On the other hand $sr^a sr^{a+2} = ssr^2 = r^2$ and $sr^{a+2}sr^a = r^{-2} = r^2$. So the subgroup contains at least $1, r^2$, $r^a s = sr^{a+2}$ and $r^{a+2}s = sr^a$, i.e. the subgroup contains $\{1, r^2, r^a s, r^{a+2}s$. So the order of $\langle sr^a, sr^{a+2}\rangle$ is either 4 or 8. It is not hard to see that we cannot create all elements of $\mathcal{D}_8$ from sr^a and sr^{a+2}, in particular we cannot generate r, so the order of the generated subgroup cannot be 8 and therefore it is 4. So the answer is $\{1, r^2, r^a s, r^{a+2}s\}$.

2. Recall that $\mathbb{F}_3$ is the set $\{0, 1, 2\}$ equipped with multiplication modulo 3, with respect to which $\mathbb{F}_3$ is a field. Let G be the group of 2×2 upper-triangular invertible matrices with entries in $\mathbb{F}_3$.

   We have

   $$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\}$$

   which gives

   $$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot H = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\}$$

   $$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot H = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

   $$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \right\}$$

   and for this example every right coset is equal to the corresponding left coset. (This fact is not obvious.) Computations can be simplified using the fact that once the first two cosets are known, the third coset necessarily consists precisely of the matrices which were not in the first two cosets.

3. The easiest way to approach this question is to decide whether the equation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

can be solved with the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belonging to the relevant group. This equation rewrites as

$$\begin{pmatrix} a & 2a+b \\ c & 2c+d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix}.$$

Clearly $a = a - c$ implies that c must be zero, so we need to solve

$$\begin{pmatrix} a & 2a+b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b-d \\ 0 & d \end{pmatrix}.$$

Thus we need to choose the coefficients a, b, d such that $2a = -d$ and such that the matrix belongs to the relevant group.

(i) $G = GL_2(\mathbb{R})$: yes, the two matrices are conjugate (take e.g. $a = -1/2$, $d = 1$, $b = c = 0$ to solve the required equation with a real invertible matrix.)

(ii) $G = SL_2(\mathbb{R})$: no, the matrices are not conjugate; we would need $2a = -d$ but also $ad = 1$ in order for the determinant of the matrix to be 1, and this implies $2a^2 = -ad = -1$ so that $a^2 = -1/2$ which is insoluble for real a.

(iii) $G = SL_2(\mathbb{C})$: yes, the matrices are conjugate; we need $2a = -d$ and $ad = 1$, but we are now allowed complex entries, so this can be solved with $a = -i/\sqrt{2}$, $d = i\sqrt{2}$, $b = c = 0$.

(iv) $G = GL_2(\mathbb{F}_3)$: yes, but this is a trick question since in this field the two matrices are identical.

4. Let G be a group of order 14 and H a subgroup of G. By Lagrange's theorem the order of H divides the order of G, so the order of H must be 1, 2, 7 or 14. Furthermore, if h is any element of H, then since $\mathrm{ord}(h) = |\langle h \rangle|$, the order of h must divide $|H|$.

If H has order 1 then it is the trivial group $\{1\}$ and we are done. If H has order 2 then it contains a non-identity element g, say, whose order must divide $|H|$. Since $|H| = 2$ and $g \neq 1$, the order of g must by elimination by equal to 2 and we are done in this case. If H has order 7 then it contains six non-identity elements, each of which cannot have order 1 but must have order equal to a factor of 7. All of these elements therefore have order 7 and we are done in this case. Finally, if H has order 14 then all of its non-identity elements have order 2, 7 or 14. If an element g has order 14, then it follows easily from the definition of order that g^2 has order 7 and g^7 has order 2. So in all cases where H is not the trivial subgroup, H contains an element of order 2 or 7 or both.

Now suppose that H has an element of order 2 *and* and element of order 7. Since the order of every element of H must divide the order of H, the order of H must be divisible by both 2 and 7, and by Lagrange's theorem it also must divide $|G|$, which is 14. This is only possible when $|H| = 14$.

5. Write $f = hgh^{-1}$ with $h \in G$. For every $k \geq 1$ we have $f^k = (hgh^{-1})^k = hg^kh^{-1}$. If $f^k = 1$ then $hg^kh^{-1} = 1$ so $g^k = 1$. Equally, if $g^k = 1$ then $f^k = h1h^{-1} = 1$. So $f^k = 1$ if and only if $g^k = 1$. In particular, f has infinite order if and only if g has infinite order; and in the finite-order case, the smallest integer $k \geq 1$ such that $f^k = 1$ is also the smallest integer $k \geq 1$such that $g^k = 1$. This completes the proof.

6. (i). If $X = \{x_1, x_2, \ldots, x_n\}$ then $\mathcal{P}(X) = \langle \{x_1\}, \{x_2\}, \ldots, \{x_n\} \rangle$. To actually prove this, it would be enough to show that these elements generate at least 2^n different elements of $\mathcal{P}(X)$, and this is most easily proved by induction on the cardinality of the set X. This result can be verified to be true directly when n is small, e.g. 3 or 4. In general, if $A = \{x_{i_1}, \ldots, x_{i_k}\} \subseteq X$ then $A = \{x_{i_1}\} \triangle \cdots \triangle \{x_{i_k}\}$. However, the question only asks you to write down a generating set, not to prove that this set generates the group.

   (ii). Observe that $A \triangle B = B \triangle A$ and $A \triangle A = \emptyset = \mathrm{id}_{\mathcal{P}(X)}$ for all $A, B \in \mathcal{P}(X)$, so the group is abelian and all of its elements have order 2 (except for the identity which has order 1). In particular if $g_1, \ldots, g_k \in \mathcal{P}(X)$ then $\langle g_1, g_2, \ldots, g_k \rangle = \{g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k} : n_i \in \{0, 1\}\}$ and this set has *at most* 2^k elements. So the subgroup generated by any $n - 1$ elements will contain not more than $2^{n-1} < 2^n = |\mathcal{P}(X)|$ elements and therefore cannot equal $\mathcal{P}(X)$.