MTH6016 Group Theory – Coursework 1 solutions

October 25, 2023

1. Suppose that G is a group. Let $f, g \in G$ and suppose that $\mathrm{ord}(f) = 3$ and $\mathrm{ord}(g) = 6$.

   (i) Since $\mathrm{ord}(f) = 3$ we have $f^2 \neq 1$. (If we had $f^2 = 1$ then $\mathrm{ord}(f)$ would have to be 1 or 2.) We also have $(f^2)^2 = f^4 = f \cdot f^3 = f \neq 1$ since f has order 3 and does not have order 1. On the other hand $(f^2)^3 = f^6 = f^3 \cdot f^3 = 1 \cdot 1 = 1$, so the smallest integer $k \geq 1$ such that $(f^2)^k = 1$ is $k = 3$. Thus $\mathrm{ord}(f^2) = 3$.

   (ii) Since $\mathrm{ord}(g) = 6$ we have $g^3 \neq 1$, so $\mathrm{ord}(g^3) \neq 1$. On the other hand $(g^3)^2 = g^6 = 1$ so $\mathrm{ord}(g)$ must be 2.

   (iii) We have $(fg)^6 = fgfgfgfgfgfg = f^6 g^6 = (f^3)^2 g^6 = 1$ using the fact that f and g commute, and the fact that f has order 3 and g has order 6. This implies that the order of fg divides 6, by Lemma 1.2.

2. In $\mathcal{U}_{31}$, find all elements of the subgroup $\langle 4, 30 \rangle$.

   We have $4^0 = 1$, $4^1 = 4$, $4^2 = 16$, $4^3 = 2$, $4^4 = 8$, $4^5 = 1$, and $30^2 = 1$ in U_{31}. Since multiplication in U_{31} commutes, every product of powers of 4 and 30 must have the form $4^a 30^b$ for some integers a and b. Since $4^5 = 30^2 = 1$, by removing terms of the form 4^5 or 30^2, we can reduce a and b so that $0 \leq a < 5$ and $0 \leq b < 2$. So the elements of $\langle 4, 30 \rangle$ are $1, 4, 4^2, 4^3, 4^4, 30{\cdot}1, 30{\cdot}4^2, 30{\cdot}4^3, 30{\cdot}4^4$; that is, $1, 4, 16, 2, 8, 30, 27, 15, 29, 23$.

3.

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

   We have $\mathrm{ord}(1) = 1$, $\mathrm{ord}(2) = 6$, $\mathrm{ord}(4) = 3$, $\mathrm{ord}(5) = 6$, $\mathrm{ord}(7) = 3$, $\mathrm{ord}(8) = 2$.

4. List all of the elements of $\mathrm{GL}_2(\mathbb{F}_2)$ and find the order of each element.

   The elements are

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \begin{pmatrix}0&1\\1&0\end{pmatrix}, \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$$

$$\begin{pmatrix}1&1\\1&0\end{pmatrix}, \quad \begin{pmatrix}1&0\\1&1\end{pmatrix}, \quad \begin{pmatrix}0&1\\1&1\end{pmatrix}$$

   and their orders are respectively 1, 2, 2, 3, 2, 3.

5. Find two elements g, h of $\mathrm{GL}_2(\mathbb{F}_2)$ such that $\langle g, h\rangle = \mathrm{GL}_2(\mathbb{F}_2)$.

   This can most easily be done by trial and error using the list of elements found earlier. In fact, if g is any element with order 2 and h is any element with order 3 then the result holds.

6. We need to check the four group axioms. It is clear by definition that $A\triangle B$ is a subset of X and is therefore an element of $\mathcal{P}(X)$, so G1 is satisfied. To see that G3 is satisfied we note that the empty set $\emptyset$ has the property $A\triangle\emptyset = \emptyset\triangle A = A$ for every $A \in \mathcal{P}(X)$, and also $A\triangle A = \emptyset$ for every $A \in \mathcal{P}(X)$ so that every element is its own inverse. The most difficult axiom to check is G2: we must show that if A, B, C are subsets of X then $A\triangle(B\triangle C) = (A\triangle B)\triangle C$.

   Perhaps the easiest way to solve this is by considering the eight possibilities for each $x \in X$. If $x \in X$ belongs to none of A, B, C then it is not an element of $A\triangle(B\triangle C)$ and is also not an element of $(A\triangle B)\triangle C$. If x belongs only to A then it is an element of both sets, and this is also the case if it belongs only to B, and if it belongs only to C. It is also not very difficult to see that if $x \in X$ belongs to A and B but not C, or belongs to A and C but not B, or belongs to B and C but not A, then it does not belong to $A\triangle(B\triangle C)$ and also does not belong to $(A\triangle B)\triangle C$. Finally, if $x \in X$ belongs to all three sets then it is an element of both $A\triangle(B\triangle C)$ and $(A\triangle B)\triangle C$. So $x \in X$ belongs to $A\triangle(B\triangle C)$ if and only if it belongs to $(A\triangle B)\triangle C$ and thus the two sets are identical as needed to prove G2. This information could perhaps be summarised in a table. Another way of expressing the same information would be to show that $A\triangle(B\triangle C)$ and $(A\triangle B)\triangle C$ are both equal to the set of all $x \in X$ which belong to an odd number of the sets A, B, C. Yet another approach would be to use the expression $A\triangle B = ((A \cup B) \cap (A \cap B)^c)$ and manipulate the implied formulas for $A\triangle(B\triangle C)$ and $(A\triangle B)\triangle C$ to show that they are the same.