MATH40003 - Linear Algebra and Groups
Spring Coursework

Ivan Kirev
CID:01738166

Question 1

(i)

We want to show that if $s \in \mathbb{Z}$ for $s < 0$ we have $g^{s+1} = g^s g$. If $s = -1$, then $g^{-1+1} = g^0 = e = g^{-1}g$. Now suppose $s \leq -2$. By definition we have $g^{-(-s-1)} = (g^{-1})^{-s-1}$. Since $-s-1 > 0$, and we have already seen that $g^{k+1} = g^k g$ for k-positive, we get

$$g^{s+1} = (g^{-1})^{-s-1} = (g^{-1})^{-s-2}(g^{-1}) \implies$$

$$g^{s+1}g = (g^{-1})^{-s-2}(g^{-1})g = (g^{-1})^{-s-2} = g^{s+2}.$$

Now denoting $t = s+1 < 0$, we derived that $g^{t+1} = g^t g$. We can multiply both sides by g^{-1} on the right to get $g^{t+1}g^{-1} = g^t$.

(ii)

We want to show that if $m, n \in \mathbb{Z}$ and $n < 0$ then $g^{m+n} = g^m g^n$. Denote $n = -k$, where k is positive. Now we want to show that $g^{m-k} = g^m g^{-k}$. We will do this by induction on k. For $k = 1$, we have

$$g^{m-1} = g^m g^{-1}$$

since $g^{t+1}g^{-1} = g^t$ from (i) for anty $t \in \mathbb{Z}$.
Suppose now that for some k we have that $g^{m-k} = g^m g^{-k}$. We will show that $g^{m-(k+1)} = g^m g^{-(k+1)}$.
Using our base step, we know that $g^{m-(k+1)} = g^{m-k-1} = g^{m-k}g^{-1}$, which is equal to $g^m g^{-k} g^{-1}$ by the induction hypothesis. Now $g^{-k}g^{-1} = g^{-k-1}$ from the base step of the induction, and therefore we get that

$$g^{m-(k+1)} = g^m g^{-(k+1)} \implies$$

by induction $g^{m-k} = g^m g^{-k}$ for all positive k, or for all $n < 0$, $g^{m+n} = g^m g^n$.

Question 2

(i)

$\boxed{\text{TRUE}}$ Note that

$$\begin{aligned} g^{-1}hg = e &\iff \\ g^{-1}h = g^{-1} &\iff \\ h = e. \end{aligned}$$

Also, $(g^{-1}hg)^n = g^{-1}h^n g$ (since $gg^{-1} = e$)and therefore

$$g^{-1}h^n g = e \iff h^n = e, \text{ ie}$$

$$(g^{-1}hg)^n = e \iff h^n = e.$$

Thus $\mathrm{ord}(h) = \mathrm{ord}(g^{-1}hg)$.

(ii)

$\boxed{\text{TRUE}}$ Let $\mathrm{ord}(g) = \mathrm{ord}(g^2) = n$. Assume $n = 2k, k \in \mathbb{N}/\{0\}$. Then $g^n = g^{2k} = (g^2)^k = e$, but $k \leq n$, so $k = n$. Thus $n = 0$, which is a contradiction. So n must be odd.

(iii)

$\boxed{\text{TRUE}}$ We know by Lagrange's Theorem any group of order p (prime) is cyclic, hence abelian. If $|G| = 4$, then let $g \in G$. We also know that $\mathrm{ord}(g)/4$. Now if $\mathrm{ord}(g) = 4$, G is cyclic, hence abelian. Otherwise all non-identity elements have order 2. But then $(ab)^{-1} = ab, \forall a, b \in G$, so $b^{-1}a^{-1} = ab \implies ba = ab$, and hence G is abelian.

(iv)

$\boxed{\text{FALSE}}$ Consider the set of all 2^k-th roots of unity for all $k \in \mathbb{N}$. This is a group under multiplication (identity element is 1, can easily be seen to be closed under multiplication). It also has infinite order, but any particular element has order 2^n for some $n \in \mathbb{N}$.

(v)

$\boxed{\text{FALSE}}$ Consider the dihedral group

$$D_8 =< r, s \mid \mathrm{ord}(r) = 4, \mathrm{ord}(s) = 2, rs = sr^{-1} >$$

This is clearly non-abelian, as $r \neq r^{-1}$ (the order of r is 4), but has order 8.

(vi)

$\boxed{\text{TRUE}}$ Let $x, y \in G, \operatorname{ord}(x) = n, \operatorname{ord}(y) = m$. Then $(xy)^{mn} = (x^n)^m (y^m)^n = e$, as G is abelian, so xy has finite order.

(vii)

$\boxed{\text{FALSE}}$ Let $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$. Then a and b are of order 2, and $a \cdot b = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$. But $\begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}^n = \begin{pmatrix} (1/2)^n & 0 \\ 0 & 2^n \end{pmatrix}$ which is not equal to the identity matrix for any $n \in \mathbb{N}/\{0\}$.