Group theory exam 27-3-2018: Solutions

(1) We note that $10 = 61-51$ and $51 = 5\cdot 10+1$, so $1 = 1\cdot 51 - 5\cdot(61-51) = 6\cdot 51 + (-5)\cdot 61$. So the class is $\overline{3\cdot(-5)\cdot 61 + 10\cdot 6\cdot 51} = \overline{-915+3060} = \overline{2145}$.

(2) (a) The order of a product of pairwise disjoint cycles is the least common multiple of the lengths of those cycles. So here there must be a 4-cycle and apart from that only cycles of lengths 1, 2 or 4. In S_7 this gives only a 4-cycle, or a 4-cycle and a 2-cycle. The number of 4-cycles is $\binom{7}{4}\frac{4!}{4} = 7\cdot 6\cdot 5 = 210$, the number of combinations 4-cycle 2-cycle is $210\cdot\binom{3}{2}\frac{2!}{2} = 630$, so in total there are 840 such elements.

(b) $(1\,4\,3)(2\,7)(5\,6)$

(3) (a) $e = r^{2\cdot 0}$ is in H. We check that for x and y in B, also xy^{-1} is in B. With i and j in $\mathbb{Z}$: $r^{2i}(r^{2j})^{-1} = r^{2(i-j)}$, $sr^{2i+1}(r^{2j})^{-1} = sr^{2(i-j)+1}$, $r^{2i}(sr^{2j+1})^{-1} = r^{2i}sr^{2j+1} = sr^{2(j-i)+1}$, $sr^{2i+1}(sr^{2j+1})^{-1} = sr^{2i+1}sr^{2j+1} = r^{2(j-i)}$ are in B.

(b) No: r^2 and sr are in H, but $r^2\cdot sr = sr^{-2}r = sr^7 \neq sr\cdot r^2 = sr^3$.

(4) (a) For $n\geq 1$ we have $\varphi(g^n) = \varphi(g\ldots g) = \varphi(g)\ldots\varphi(g) = \varphi(g)^n$. φ is injective, so $g^n = e_G$ if and only if $\varphi(g^n) = e_H$, and by the previous sentence this is equivalent with $\varphi(g)^n = e_H$. So the smallest $n\geq 1$ with $g^n = e_G$ equals the smallest $n\geq 1$ with $\varphi(g)^n = e_H$.

(b) Let s and t be in H, so $s = \varphi(x)$ and $t = \varphi(y)$ for (unique) x and y in G. Then $\varphi^{-1}(st) = \varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(s)\varphi^{-1}(t)$ because φ is a homomorphism.

(5) (a) (i) $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}^2 = \begin{pmatrix} a^2 & (a+1)b\\ 0 & 1\end{pmatrix}$. If $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}^m = \begin{pmatrix} a^m & (a^{m-1}+a^{m-2}+\cdots+1)b\\ 0 & 1\end{pmatrix}$ for $m\geq 2$, then

$$\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}^{m+1} = \begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}^m\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix} a^m & (a^{m-1}+a^{m-2}+\cdots+1)b\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}$$

$$= \begin{pmatrix} a^{m+1} & a^m\\ 0 & 1\end{pmatrix} b + (a^{m-1}+a^{m-2}+\cdots+1)b = \begin{pmatrix} a^{m+1} & (a^m+a^{m-1}+\cdots+1)b\\ 0 & 1\end{pmatrix},$$

so $\begin{pmatrix} a & b^m\\ 0 & 1\end{pmatrix} = \begin{pmatrix} a^m & (a^{m-1}+a^{m-2}+\cdots+1)b\\ 0 & 1\end{pmatrix}$ for all $m\geq 2$.

(ii) $e_G = \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, so if $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}$ has finite order n then $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}^n = \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$. If $a^m = 1$ for a in $\mathbb{Q}^*$ and some $m\geq 1$, then $a = \pm 1$, so we have two cases.

- $\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}^n = \begin{pmatrix} 1 & nb\\ 0 & 1\end{pmatrix}$, so for $n\geq 1$ this can be $\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$ only if $b = 0$. This gives the element $\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, of order 1.
- $\begin{pmatrix} -1 & b\\ 0 & 1\end{pmatrix}^2 = \begin{pmatrix} (-1)^2 & (-1+1)b\\ 0 & 1\end{pmatrix} = \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, and as $\begin{pmatrix} -1 & b\\ 0 & 1\end{pmatrix} \neq \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, these elements have order 2.

(b) Take $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}$ in G and $\begin{pmatrix} -1 & B\\ 0 & 1\end{pmatrix}$ in A, so B is in $\mathbb{Z}$. Then $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}\begin{pmatrix} -1 & B\\ 0 & 1\end{pmatrix} = \begin{pmatrix} -a & aB+b\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix} -1 & B\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix} -a & B-b\\ 0 & 1\end{pmatrix}$. So $\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}$ is in $C_G(A)$ if and only if $aB+b = B-b$ for all B in $\mathbb{Z}$. Taking $B = 0$ shows $b = 0$. Taking

$B=1$ shows $a=1$. So the only possible element in $C_G(A)$ is $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, and this one satisfies the requirement, hence $C_G(A)=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$.

(c) Take $\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}$ in $N_G(A)$ and $\begin{pmatrix}-1 & B\\ 0 & 1\end{pmatrix}$ in A, so B is in $\mathbb{Z}$. Then

$$\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & B\\ 0 & 1\end{pmatrix}\begin{pmatrix}a^{-1} & -a^{-1}b\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-a & aB+b\\ 0 & 1\end{pmatrix}\begin{pmatrix}a^{-1} & -a^{-1}b\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & aB+2b\\ 0 & 1\end{pmatrix}.$$

With B in $\mathbb{Z}$ this has to give all elements of A.

- Taking $B=0$ shows $2b$ is in $\mathbb{Z}$.
- Say $2b=m$. Then $\{aB+m|B\in\mathbb{Z}\}=\{aB|B\in\mathbb{Z}\}$ must be $\mathbb{Z}$, so $a=\pm 1$: taking $B=1$ shows a is in $\mathbb{Z}$, and for $a\in\mathbb{Z}\setminus\{\pm 1\}$ we do not get $\mathbb{Z}$. So $N_G(A)=\left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\text{ with } a=\pm 1 \text{ and } b\in\{\frac{m}{2}|m\in\mathbb{Z}\}\right\}$.

(6) $\mathbb{Z}/100\mathbb{Z}\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/25\mathbb{Z}$, so we compute $\overline{27^{2018}}$ in $\mathbb{Z}/4\mathbb{Z}$ and in $\mathbb{Z}/25\mathbb{Z}$.

- $\overline{27^{2018}}=\overline{27}^{2018}=\overline{3}^{2018}=(\overline{3}^2)^{1009}=(\overline{1})^{1009}=\overline{1}$ in $\mathbb{Z}/4\mathbb{Z}$.
- As $\text{lcm}(25,27)=1$, $\overline{27}=\overline{2}$ is in $(\mathbb{Z}/25\mathbb{Z})^*$. By Euler's theorem $\overline{2}^{20}=\overline{1}$: $\varphi(25)=5\cdot(5-1)=20$. So $\overline{27^{2018}}=\overline{27}^{2018}=\overline{2}^{2018}=\overline{2}^{-2}$. But $\overline{2}\cdot\overline{13}=\overline{1}$, so $(\overline{2})^{-2}=\overline{13}^2=\overline{169}=\overline{19}$.

Therefore $\overline{27^{2018}}$ maps to $(\overline{1},\overline{19})$, which is the image of $\overline{69}$. So $\overline{27^{2018}}=\overline{69}$, hence the last two digits of 27^{2018} are 69.