Firstname Lastname
V00885732

Assignment 3

MATH 312
October 24, 2019

1

1.a

We count the size k of $\{(g,x) \in G \times X : g \cdot x = x\}$ in two ways:

For each $g \in G$, we count the number of points in X fixed by g to get

$$k = \sum_{g \in G} |X_g|,$$

and we count the number of elements in G fixing each $x \in X$ to get

$$k = \sum_{x \in X} |G_x|,$$

so

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

Our action is transitive, so $|\mathcal{O}_x| = |X|$ for any $x \in X$. By the Orbit-Stabilizer theorem, $|\mathcal{O}_x| = [G : G_x]$, so $[G : G_x] = |X|$, and thus $|X| = \frac{|G|}{|G_x|}$. Then $|G_x| = \frac{|G|}{|X|}$ for any $x \in X$, so

$$\begin{aligned}
\sum_{x \in X} |G_x| &= \sum_{x \in X} \frac{|G|}{|X|} \\
&= \frac{|G|}{|X|} \sum_{x \in X} 1 \\
&= \frac{|G|}{|X|} \cdot |X| \\
&= |G|
\end{aligned}$$

So $\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x| = |G|$, thus $\sum_{g \in G} |X_g| = |G|$, and so $\frac{1}{|G|} \sum_{g \in G} |X_g| = 1$ as desired.

1.b

Assume for a contradiction that all $g \in G$ have fixed points. Then $|X_g| \geq 1$ for all $g \in G$. We know that $|X_{1_G}| = |X| > 1$, so

$$\begin{aligned}
|G| &= \sum_{g \in G} |X_g| \\
&= |X_{1_G}| + \sum_{g \in G \setminus \{1_G\}} |X_g| \\
&\geq |X_{1_G}| + |G \setminus \{1_G\}| && G \text{ is non-trivial, so } G \setminus \{1_G\} \neq \emptyset. \\
&\geq |X_{1_G}| + |G| - 1 \\
&\geq 2 + |G| - 1 \\
&= |G| + 1
\end{aligned}$$

So $|G| \geq |G| + 1$, a contradiction. Thus there must exist some $g \in G$ with no fixed points, as desired.

2

2.a

Let $aHa^{-1} \in X$. We show that $\mathcal{O}_{aHa^{-1}} = X$:

Let $hHh^{-1} \in X$.

$$\begin{aligned}
hHh^{-1} &= (ha^{-1}a)H(ha^{-1}a)^{-1} \\
&= (ha^{-1}a)H(a^{-1}ah^{-1}) \\
&= (ha^{-1})aHa^{-1}(ah^{-1}) \\
&= (ha^{-1})aHa^{-1}(ha^{-1})^{-1} \\
&= (ha^{-1}) \cdot (aHa^{-1})
\end{aligned}$$

Thus $hHh^{-1} \in \mathcal{O}_{aHa^{-1}}$, but hHh^{-1} was arbitrary in X, so $\mathcal{O}_{aHa^{-1}} = X$. aHa^{-1} was also arbitrary in X, so $\mathcal{O}_x = X$ for any $x \in X$, thus the action is transitive, as desired.

2.b

We know from class that if $H \leq G$, then $N_G(H) \leq G$. We also know from class that $H \trianglelefteq N_G(H)$.

We show that $|X| = |G/N_G(H)|$:
Define $\varphi : G/N_G(H) \longrightarrow X$ by $gN_G(H) \longmapsto gHg^{-1}$. We show that φ is a bijection.

First, we show that φ is **well-defined**:
Let $gN_G(H) = g'N_G(H)$. Then $g' = gn$ for some $n \in N_G(H)$. So

$$\begin{aligned}\varphi(g'N_G(H)) &= g'Hg'^{-1} \\ &= (gn)H(gn)^{-1} \\ &= gnHn^{-1}g^{-1} \\ &= gHg^{-1} \\ &= \varphi(gN_G(H))\end{aligned}$$

So φ is well-defined.

We now show that φ is **injective**:
Let $\varphi(g_1N_G(H)) = \varphi(g_2N_G(H))$. Then $g_1Hg_1^{-1} = g_2Hg_2^{-1}$, so $g_2^{-1}g_1Hg_1^{-1}g_2 = H$. Thus $g_2^{-1}g_1 \in N_G(H)$, and $g_1 \in g_2N_G(H)$, meaning $g_1N_G(H) = g_2N_G(H)$, and so φ is injective.

Finally, we show that φ is **surjective**:
Let $aHa^{-1} \in X$. Then $\varphi(aN_G(H)) = aHa^{-1}$. Thus φ is surjective. So φ is a bijection, thus $|X| = |G/N_G(H)|$.

$|X| = |G/N_G(H)|$, so H has $|G/N_G(H)|$ conjugates in G. Thus

$$\left|\bigcup_{a\in G} aHa^{-1}\right| \leq |G/N_G(H)| \cdot |H|.$$

But $aHa^{-1} \leq G$ for all $a \in G$, so $1_g \in aHa^{-1}$ for all $a \in G$. Thus

$$\bigcup_{a\in G} aHa^{-1} = \{1_g\} \cup \bigcup_{a\in G} aHa^{-1} \setminus \{1_G\}.$$

So

$$\begin{aligned}\left|\bigcup_{a\in G} aHa^{-1}\right| &= \left|\{1_g\} \cup \bigcup_{a\in G} aHa^{-1} \setminus \{1_G\}\right| \\ &= \left|\{1_g\}\right| + \left|\bigcup_{a\in G} aHa^{-1} \setminus \{1_G\}\right| \\ &= 1 + \left|\bigcup_{a\in G} aHa^{-1} \setminus \{1_G\}\right| \\ &\leq 1 + |X|(|H|-1)\end{aligned}$$

Thus we have that $|G| \geq |X| \cdot |H| > 1 + |X|(|H|-1) = |X|\cdot|H| + 1 - |X|$. If $H \trianglelefteq G$, then since every conjugate of H is just H, and since $H \neq G$, clearly $\bigcup_{a\in G} aHa^{-1}$ doesn't cover G. So assume $H \ntrianglelefteq G$. Then there exists some conjugate of H that is not equal to H, so $|X| \geq 2$. So $|X|\cdot|H| + 1 - |X| \leq |X|\cdot|H| - 1 < |X|\cdot|H|$. So $|G| > |X|\cdot|H| - 1 \geq \left|\bigcup_{a\in G} aHa^{-1}\right|$, so $|G| \neq \left|\bigcup_{a\in G} aHa^{-1}\right|$, and therefore $G \neq \bigcup_{a\in G} aHa^{-1}$, as desired.

3

The orbits of the action partition X, so

$$X = \bigcup_{i=0}^{k} \mathcal{O}_{x_i} = X^G \cup \bigcup_{i=0}^{l} \mathcal{O}_{x_i},$$

where $x_0, \ldots, x_k$ are representatives for the distinct orbits of X, and $x_{l+1}, \ldots, x_k$ have trivial orbits. Since X^G and $\bigcup_{i=0}^{l} \mathcal{O}_{x_i}$ are clearly distinct, we have that

$$|X| = |X^G| + \sum_{i=0}^{l} |\mathcal{O}_{x_i}|.$$

We know that $G_{x_i} \leq G$, so $|G_{x_i}|\big||G|$. We also know that $|\mathcal{O}_{x_i}| = \frac{|G|}{|G_{x_i}|}$. Since $\mathcal{O}_{x_i}$ is non-trivial, $\frac{|G|}{|G_{x_i}|} \neq 1$. Thus $|\mathcal{O}_{x_i}| = p^m$ for some $m \geq 1$. Thus all $|\mathcal{O}_{x_i}|$ divide p, where $i \leq l$. Then $|X^G| + \sum_{i=0}^{l} |\mathcal{O}_{x_i}| \equiv |X^G| \pmod{p}$, so $|X| \equiv |X^G| \pmod{p}$, as desired.

4

4.a

Let $k \in K$. $k \cdot aH = kaH = aH$, so $(ka)(a)^{-1} \in H$, thus $k \in H$, and so $K \subseteq H$.

Note first that $K = G_{aH}$, the stabilizer of aH in G, so $K \leq G$. Let $g \in G$, $k \in K$. $(gkg^{-1}) \cdot aH = gkg^{-1}aH$. By definition of K, since $g^{-1}a \in G$, $k \cdot (g^{-1}a)H = (g^{-1}a)H$. Since $k \cdot g^{-1}aH = kg^{-1}aH$, then $gkg^{-1}aH = gg^{-1}aH = aH$, so $gkg^{-1} \in K$, and thus $K \trianglelefteq G$, as desired.

4.b

Let G/K act on G/H by $g_1K \cdot g_2H \longmapsto g_1g_2H$. By definition of K, $kgH = gH$ if and only if $k \in K$, so the action is faithful. Thus there is a correspondence between this action and an injective homomorphism from G/K to $S_{G/H} \cong S_{[G:H]} = S_p$. This homomorphism is injective, so $G/K \cong \operatorname{Im}\varphi \leq S_{G/H} \cong S_p$, and we're done.

4.c

We have $\frac{|H|}{|K|} = k$, $\frac{|G|}{|H|} = p$, $\frac{|G|}{|K|\cdot k} = p$, and $\frac{|G|}{|K|} = [G:K] = pk$. By Lagrange's theorem, $|G/K|\big||S_p|$, thus $[G:K]\big|p!$, and so $pk|p!$, as desired.

4.d

$[G:K] = pk$, and $[G:K] = [G:H][H:K] = pk$, so $\frac{[G:K]}{[G:H]} = [H:K] = \frac{pk}{[G:K]}$. Then $k = [H:K] = \frac{pk}{pk} = 1$. So $[G:K] = 1$. Since $K \leq H$, $K = H$. $K \trianglelefteq G$, so $H \trianglelefteq G$, as desired.

5

5.a

:(

5.b

Let $g \in G$. Then $g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, $g^2 = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$, and $g^3 = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ So $|g|\big|3$. If $|g| = 1$, then $g = 1_G$, otherwise $|g| = 3$.

Let $h \in H$. Then $h = (a, b, c)$, $h^2 = (2a, 2b, 2c)$, and $h^3 = (3a, 3b, 3c) = (0, 0, 0)$. So $|h|\big|3$. If $|h| = 1$, then $h = 1_H$, otherwise $|h| = 3$.

There is clearly a bijective map from G to H in $f\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, b, c)$, so since $G \setminus \{1_G\}$ and $H \setminus \{1_H\}$ contain only elements of order 3 and have the same size, $D_G(3) = D_H(3)$, and trivially $D_G(1) = D_H(1)$.

Let $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G$.

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & a+1 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &\neq \begin{pmatrix} 1 & a+1 & b+c \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

but H is abelian, so $G \ncong H$.