MA347 – HW16

Jonathan Lam

March 28, 2021

1. Let $f : G \to G'$ be a group isomorphism. Let $g \in G$ and $k \in \mathbb{N}$ and $A = \{a \in G : a^k = g\}$ and $B = \{b \in G' : b^k = f(g)\}$. Prove that A and B have the same number of elements.

   $|A| = |B| \Leftrightarrow$ there exists a bijection $h : A \to B$. In particular, we show that the restriction of f to A meets this condition, i.e., that $h = f|_A : A \to G'$ such that h is defined by $h(x) = f(x)$.

   (All that remains to show is that $h(A) = B \subseteq G'$. Since f is injective, h is also injective; and any map is surjective onto its image.)

   Let $a \in A$. Then $a^k = g \Rightarrow f(a^k) = f(a)^k = g$ (since f is a homo.) $\Rightarrow f(a) = h(a) \in G$. Thus $h(A) \subseteq B$.

   Let $b \in B$. Since $f : G \to G'$ is surjective, $\exists a = f^{-1}(b) \in G$. f is an iso., so f^{-1} is also a homo. Then:

$$g = f^{-1}(f(g)) = f^{-1}(b^k) = f^{-1}(b)^k = a^k$$
$$\Rightarrow f^{-1}(b) \in A$$

   Thus $f^{-1}(B) \subseteq A \Rightarrow B \subseteq f(A) = h(A)$.

   $h(A) \subseteq B \subseteq h(A) \Rightarrow h(A) = B$. By the preceding logic, h is a bijection from A onto B, so $|A| = |B|$.

2. (Lang II.§8.4) Let G be a finite group acting on a finite set S.

   (a) For each $s \in G$, prove that $Gs = Gt$ if $t \in Gs$ and

$$\sum_{t \in Gs} \frac{1}{|Gt|} = 1$$

Proof. ($Gs = Gt$) Let $s, t \in S$, and $t \in Gs$, and let π be the group homomorphism mapping $G \to \mathrm{Perm}(S)$. Then $t = (\pi(x))(s)$ for some $x \in G$. $\pi(x) \in \mathrm{Perm}(S)$ implies that there exists an inverse permutation $\in \mathrm{Perm}(S)$ such that $s = ((\pi(x))^{-1})(t) \in Gt$.

Thus $t \in Gs \Rightarrow s \in Gt$ so $Gs \subseteq Gt$, and $s \in Gt \Rightarrow t \in Gs$ by the same argument so $Gt \subseteq Gs$. Thus $Gs = Gt$. ☐

Then we have $\forall t \in Gs$, $|Gt| = |Gs|$, so

$$\sum_{t \in Gs} \frac{1}{|Gt|} = |Gs| \frac{1}{|Gs|} = 1$$

   (b) Show that the number of orbits of G is S is equal to

$$\sum_{s \in S} \frac{1}{|Gs|}$$

We know (by the previous result that $t \in Gs \Rightarrow Gs = Gt$) that the orbits form a partition over S. Let $\{y_i\}_{i=1}^{m}$ represent the distinct orbits of S. Then we can rewrite this sum as the sum over the orbits of S under G:

$$\sum_{s \in S} \frac{1}{|Gs|} = \sum_{i=1}^{m} \sum_{t \in G_{y_i}} \frac{1}{|Gt|} = \sum_{i=1}^{m} 1 = m$$

which is the number of distinct orbits.