

MATH 171
SOLUTIONS TO QUIZ 2

Let G be a group with identity e . Let $a \in G$. Define the relation $b \sim c$ if and only if $bc^{-1} \in \langle a \rangle$.

- Prove \sim is an equivalence relation on G .

Solution: (*Reflexive*) $bb^{-1} = e$. $e \in \langle a \rangle$ since it is a subgroup. Hence $b \sim b$. (*Symmetric*) If $b \sim c$ then $bc^{-1} \in \langle a \rangle$. Therefore $(bc^{-1})^{-1} = cb^{-1} \in \langle a \rangle$, since $\langle a \rangle$ is a subgroup. Hence $c \sim b$. (*Transitive*) Let $b \sim c$ and $c \sim d$. Then $bc^{-1} \in \langle a \rangle$ and $cd^{-1} \in \langle a \rangle$. Therefore $bc^{-1}cd^{-1} = bd^{-1} \in \langle a \rangle$. Hence $b \sim d$.

- If G is finite, prove that $|[b]| = |[e]| = |\langle a \rangle|$ for all $b \in G$.

Solution: G finite implies $\langle a \rangle = \{e, a, a^2, \dots, a^n\}$. Since $[b] = \{g \in G \mid bg^{-1} \in \langle a \rangle\}$, $g \in [b]$ implies $g \in \{b, ab, a^2b, \dots, a^nb\}$. Conversely if $g = a^kb$ for some integer k , then $g \in [b]$. Therefore $[b] = \{b, ab, a^2b, \dots, a^nb\}$. Note that $a^ib = a^jb$ if and only if $i = j$. Therefore $|[b]| = |\langle a \rangle|$. (Since $[e] = \{e, a, a^2, \dots, a^n\}$, clearly $|[e]| = |\langle a \rangle|$.)

Remark: In office hours, I presented a different solution. It is essentially the argument that precedes the proof of Lagrange's Theorem on p. 100 in the textbook.

- Deduce that if G is finite, $\text{ord}(a) = |\langle a \rangle|$ divides $|G|$.

Solution: G finite implies there are N equivalence classes $\{P_1, \dots, P_N\}$ for some integer $N > 0$ corresponding to the equivalence relation \sim . By definition of a partition, $G = \bigcup_{i=1}^N P_i$ and $P_i \cap P_j = \emptyset$ for $i \neq j$. Therefore $|G| = \sum_{i=1}^N |P_i|$. For all P_i there exists $b_i \in G$ such that $[b_i] = P_i$ and, by part 2 above, $|[b_i]| = |\langle a \rangle|$. Hence $|G| = \sum_{i=1}^N |P_i| = \sum_{i=1}^N |\langle a \rangle| = N|\langle a \rangle|$. Hence $|\langle a \rangle|$ divides $|G|$. By definition, $\text{ord}(a) = |\langle a \rangle|$. Hence $\text{ord}(a)$ divides $|G|$.