## HOMEWORK 9 (DUE: 11:15 AM, NOV 14 WED)

1. Do Exercise 13.J.1–6 in [Pin10].

**1.** We have

- For $u \in A$, $eu = u$, thus $u \sim u$.
- For $u, v \in A$, if $u \sim v$ then $\exists g \in G$ such that $gu = v$, thus $u = g^{-1}v$ which means $v \sim u$.
- For $u, v, w \in A$, if $u \sim v$ and $v \sim w$ then $\exists g, h \in G$ such that $gu = v$ and $hv = w$, thus $(hg)u = w$ which means $u \sim w$.

Therefore $\sim$ is an equivalence relation. Also, the equivalence class of $u$ is by definition $\{v \in A \mid \exists g \in G \text{ such that } gu = v\} = \{gu \mid g \in G\} = O(u)$.

**2.**
- If $g, h \in G_u$, then $gu = hu = u$ thus $(gh)u = g(hu) = u$ which means $gh \in G_u$.
- $eu = u$ thus $e \in G_u$.
- If $g \in G_u$, then $gu = u$ thus $g^{-1}u = g^{-1}(gu) = u$ which means $g^{-1} \in G_u$.

Therefore $G_u$ is a subgroup of $G$.

**3.** $G$ is a group generated by $\alpha$ and $\beta$. By direct calculation we have

$$O(1) = O(2) = \{1, 2, 3, 4\}, \quad O(5) = \{5, 6\},$$
$$G_1 = \{e, \beta\}, \quad G_2 = \{e, \alpha\beta\alpha\}, \quad G_4 = \{e, \beta\},$$
$$G_5 = \{e, \beta, \alpha\beta\alpha, (\alpha\beta)^2\}.$$

**4.** $fG_u = gG_u \Leftrightarrow g^{-1}f \in G_u \Leftrightarrow g^{-1}fu = u \Leftrightarrow fu = gu$.

**5.** By part 4, $G/G_u \to O(u) : fG_u \mapsto fu$ is a well-defined injective map. Also it is surjective as any element of $O(u)$ is written as $fu$ for some $f \in G$. Thus this correspondence is a bijection, which means that $|O(u)| = (G : G_u)$.

**6.** Since $(G : G_u) = |G|/|G_u|$ when $G$ is finite, $|O(u)| \cdot |G_u| = |G|$ and the first claim follows. In particular, (if $A$ is finite then) the length of each cycle of $f$ is the same as the size of each orbit of $f$, thus the second claim also follows.

2. Do Exercise 16.K.1–3 in [Pin10].

**1.** If $C_a \subsetneq G$, then the result follows from induction on the order of $G$ since $|C_a| < |G|$ and $p$ is a divisor of $|C_a|$. (An element of order $p$ in $C_a$ is also an element of order $p$ in $G$.) If $C_a = G$, then $ga = ag$ for all $g \in G$, thus $a \in C$ which is impossible by assumption.

**2.** As $|C_a| \cdot (G : C_a) = |G|$ and $p$ divides $|G|$, $p$ should divide at least one of $|C_a|$ or $(G : C_a)$.

**3.** If $p$ divides $|C_a|$ for some $a \in G - C$, then we are done by part 1. Otherwise, by part 2 $p$ should divide every $(G : C_a)$ for $a \in G - C$, which is the same as the size of the orbit of $a$. Thus from the class equation $k = c + k_s + \cdots + k_t$, we have $k \equiv c + k_s + \cdots + k_t \equiv c \pmod{p}$. As $p$ is a factor of $|G|$ by assumption, it means that $c \equiv 0 \pmod{p}$, i.e. $p$ divides the order of $C$. As $C$ is an abelian group, we are done by Exercise 15.H.4.

## References

[Pin10] Pinter, C. C., *A Book of Abstract Algebra*, 2nd ed., Dover Publications, 2010.