# HW 6

## 3.2.9

### a

We can rewrite $S$ as $S = \{(x_1, \dots x_{p-1}, (x_1 \dots x_{p-1})^{-1}) | x_i \in G\}$. Since there are no restrictions on the $x_i$ and there are $p-1$ choices of the $x_i$, the size of this set is $|G|^{p-1}$.

### b

We prove this for the cyclic permutation $x_k \dots x_{k-1}, k \in [1, p)$ by induction on $k$, where the base case $k = 1$ holds by definition of $S$. For the inductive step, we are given $x_k \dots x_{k-1} = 1$. Multiplying by $x_k^{-1}$ on the left, we have $x_{k+1} \dots x_{k-1} = x_k^{-1}$. Multiplying by $x_k$ on the right, we have $x_{k+1} \dots x_k = 1$.

### c

Notation: let $S_p$ (the symmetric group on $[1, p]$) act on $S$ by permuting the indices, that is for $\tau \in S_p$ we have $\tau \cdot (x_1, \dots x_p) = (x_{\tau(1)}, \dots x_{\tau(p)})$.

I will assume that a cyclic permutation of $(x_1, \dots x_p)$ is $\sigma^j \cdot (x_1, \dots x_p) = (x_{\sigma^j(1)}, \dots x_{\sigma^j(p)})$ where $\sigma^j$ is some power of the $p$-cycle $\sigma = (1, \dots p)$.

Reflexive: this holds because $\sigma^0$ is the identity.

Symmetric: this holds because $\sigma^{-1} = \sigma^{p-1}$.

Transitive: this holds because $\sigma^a \sigma^b = \sigma^{a+b}$.

### d

$\Longleftarrow$ : clearly $(x, \dots x) \in S$. Every cyclic permutation is also of the form $(x, \dots x)$. Hence the equivalence class has exactly 1 element.

$\Longrightarrow$ : let $E = \{(x_1, \dots x_k)\}$ be the equivalence class. For any $k \in [1, p)$ we have $(x_1, \dots x_k) = (x_k, \dots x_{k-1})$ since both the LHS and RHS belong to $E$, hence $x_1 = x_k$. Hence $x_1 = x_2 \dots = x_p$.

### e

Let $E$ be the equivalence class, and fix some $X = (x_1, \dots x_p) \in E$. Let $j$ be the smallest positive integer such that $\sigma^j \cdot X = X$. We have $j \leq p$ since $\sigma^j = e$. If $j = p$ then all $p$ cyclic permutations are distinct and $|E| = p$. Otherwise, $j$ and $p$ are coprime so the sequnce $\sigma, \sigma^j, \sigma^{2j} \dots$ contains every power of $\sigma$. Every cyclic permutation of $X$ is $\sigma^k \cdot X$, and there exists $t$ such that $\sigma^k = \sigma^{jt}$, and $\sigma^k \cdot X = \sigma^{jt} \cdot X = \sigma^j \cdot \sigma^j \ldots \cdot X = X$.

Since $S$ is a disjoint union of its equivalence classes, we have $|S| = |G|^{p-1} = \sum_E |E| = \sum_{E,|E|=1} |E| + \sum_{E,|E|=p} |E| = k + pd$ where the summation is over equivalence classes.

### f

Consider the equation $|G|^{p-1} = k + pd$ modulo $p$. The LHS is 0 since $p$ divides $|G|$ and the RHS is $k$. Hence $p|k$. Since $p \geq 2$ and $k \geq 1$ (since we have at least one equivalence class of size 1) we have $k > 1$, hence there are at least two equivalence classes of size 1, hence at least one of the form $\{x, \ldots x\}$ where $x \neq 1$. By the definition of $G$, $x$ satisfies $x^p = 1$.

## 3.2.11

We know that the left cosets of $H$ partition $K$ (and that the left cosets have equal cardinality) and the left sets of $K$ partition $G$. Let $P_c$ be the partition of $G$ by $H$. There are two natural finer partitions on $G$ to consider:

1. By left cosets of $K$, i.e. by the equivalence relation $g_1 \sim g_2 \iff g_1 K = g_2 K$.

2. By translating the partition of $H$ by $K$ to cover $G$.

It suffices to show that these are the same partitions (call them $P_1$ and $P_2$ respectively).

We will work out what is the equivalence relation in (2); let $g_1, g_2$ be in the same part of $P_2$. Then they are in the same part of $P_c$, hence $g_1 H = g_2 H$.

## 3.2.16

Notation: let $U = (\mathbb{Z}/pZ)^x$. We have $|U| = p - 1$ because the $p - 1$ elements $1, \ldots p - 1$ are distinct modulo $p$, and coprime to $p$. Let $a \in U$. By Lagrange's theorem, $ord(a)$ divides $|U| = p - 1$. We have $a^{ord(a)} = 1$ hence $a^{p-1} = (a^{ord(a)})^{\frac{p-1}{ord(a)}} = 1$ hence $a^p = a$.