Math 453

Selected Solutions to Assignment 10

Problem 1: Let $H = \{\beta \in S_5 | \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup. What is the order of H?

Solution: Let $e \in S_5$ denote the identity; then $e(1) = 1$ and $e(3) = 3$ by definition of S_5, so $e \in H$. Now, let $\beta \in H$, so $\beta(1) = 1$ and $\beta(3) = 3$. Again by definition of S_5, $(\beta^{-1} \circ \beta)(1) = e(1) = 1$ and $(\beta^{-1} \circ \beta)(3) = e(3) = 3$, so $\beta^{-1}(1) = \beta^{-1}(\beta(1)) = 1$ and $\beta^{-1}(3) = \beta^{-1}(\beta(3)) = 3$. Hence, $\beta^{-1} \in H$. Finally, let $\beta, \gamma \in H$, so $\beta(1) = \gamma(1) = 1$ and $\beta(3) = \gamma(3) = 3$. Then $(\beta \circ \gamma)(1) = \beta(\gamma(1)) = \beta(1)$ and $(\beta \circ \gamma)(3) = \beta(\gamma(3)) = \beta(3) = 3$, so $\beta\gamma \in H$. Hence, H is a subgroup of S_5.

The number of elements of H is simply the number of one-to-one functions f from $\{1, 2, 3, 4, 5\}$ onto $\{1, 2, 3, 4, 5\}$ such that $f(1) = 1$ and $f(3) = 3$. Note that since any such f is one-to-one, it must map $\{2, 4, 5\}$ onto $\{2, 4, 5\}$. There are 3 possible choices for $f(2)$ (2, 4, or 5), then 2 possible choices for $f(4)$ (2, 4, or 5, except $f(2)$), and 1 possible choice for $f(5)$ (2, 4, or 5, except $f(2)$ or $f(4)$). Thus, there are six such functions, so $|H| = 6$.

Problem 5: How many elements of order p are there in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$? Here p is a prime.

Solution: Let $g \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, so $g = (a, b)$ for some $a, b \in \mathbb{Z}_{p^2}$.

Suppose one of a, b has order p^2; without loss of generality, assume $|a| = p^2$. Then by definition of product group, $g^n = (a^n, b^n) \neq (0, c)$ for any $c \in \mathbb{Z}_{p^2}$ for $1 \leq n \leq p^2 - 1$; in particular, $g^n \neq (0, 0)$ for $1 \leq n \leq p^2 - 1$, so $|g| \geq p^2$. Since by Lagrange's Theorem, $|g| \mid \left|\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}\right|$, we have $|g| = p^2$. Taking the contrapositive, $|g| \neq p^2$, we have that neither $|a| = p^2$ nor $|b| = p^2$. Hence, again by Lagrange's Theorem $|a|, |b| \mid \left|\mathbb{Z}_{p^2}\right|$, $|a|$ is either 1 or p, and $|b|$ is either 1 or p. On the other hand, if $|g| = 1$, clearly we have $|a| = 1$ and $|b| = 1$. Hence, if $|g| = p$, we have that $|a| = 1, |b| = p$, $|a| = p, |b| = p$, or $|a| = p, |b| = 1$.

On the other hand, suppose one of a and b has order p, and the other has order 1 or p. Without loss of generality, assume $|a| = p$, and $|b| = 1$ or $|b| = p$. Then by definition of product group, $g^p = (a^p, b^p) = (0, 0)$, so $|g| \leq p$. On the other hand, let $n \in \mathbb{N}$, $1 \leq n \leq p - 1$. Then $g^n = (a^n, b^n) = (c, d)$, where $c \neq 0$ since $|a| = p$. Thus, $|g| = p$. Together with the previous paragraph, we have that $|g| = p$ if and only if $|a| = 1, |b| = p$, $|a| = p, |b| = p$, or $|a| = p, |b| = 1$.

Note that these three cases are mutually exclusive. In the first case, since is 1 distinct element of $\mathbb{Z}_{p^2}$ with order 1 and $p-1$ distinct elements of $\mathbb{Z}_{p^2}$, there is one possibility for a and $p-1$ distinct possibilities for b, so there are $p-1$ distinct possibilities in total. Similarly, in the second case, there are $p-1$ distinct possibilities for a and $p-1$ distinct possibilities for b, so there are $(p-1) = p^2-2p+1$ distinct possibilities in total. In the third case, there are $p-1$ distinct possibilities for a and one possibility for b, so again there are $p-1$ distinct possibilities in total.

Hence, there are $(p-1)+(p^2-2p+1)+(p-1) = p^2-1$ distinct possibilities for g.

Problem 7: Find a homomorphism $\phi : \mathbb{Z}_{30}^\times \to \mathbb{Z}_{30}^\times$ with kernel $\{1, 11\}$ such that $\phi(7) = 7$.

Solution: First, note that $\mathbb{Z}_{30}^\times = \{1, 7, 11, 13, 17, 19, 23, 29\}$ with the group operation being multiplication modulo 30. We must find the action of ϕ on each element. We have $\phi(1) = 1$, $\phi(7) = 7$, and $\phi(11) = 1$. Then by definition of homomorphism, we have

$$
\begin{aligned}
&\phi(13) = \phi(7^3) = \phi(7)^3 = 7^3 = 13,\\
&\phi(17) = \phi(7 \cdot 11) = \phi(7)\phi(11) = 7 \cdot 1 = 7,\\
&\phi(19) = \phi(7^2) = \phi(7)^2 = 6^2 = 19,\\
&\phi(23) = \phi(7^3 \cdot 11) = \phi(7)^3\phi(11) = 7^3 \cdot 1 = 13, \text{ and}\\
&\phi(29) = \phi(7^2 \cdot 11) = \phi(7)^2\phi(11) = 7^2 \cdot 1 = 19.
\end{aligned}
$$