Exam #2 Solutions

Problem 1.

(1) The orbits of σ are $\{1, 6, 5, 3, 8, 9\}$ and $\{2, 10, 4, 7\}$.

(2) The discriminant of σ is equal to $10-$#orbits, that is $disc(\sigma) = 10-2 = 8$. Therefore the signature of σ is $sign(\sigma) = (-1)^{disc(\sigma)} = (-1)^8 = 1$.

(3) $\sigma = (1, 6, 5, 3, 8, 9)(2, 10, 4, 7)$.

(4) This is true because C_1 and C_2 commute (which is true because they are disjoint cycles). Indeed, $\sigma^2 = (C_1\, C_2)^2 = C_1\, C_2\, C_1\, C_2$. Since C_1 and C_2 commute, this is $\sigma^2 = C_1\, C_1\, C_2\, C_2 = {C_1}^2\, {C_2}^2$. Thus the result is true for $k = 2$, and it is easy to extend it for any $k \in \mathbb{N}$ by induction.

(5) We can derive from the previous question that $\sigma^k = id$ if and only if ${C_1}^k = id$ and ${C_2}^k = id$. Since the order of a cycle is equal to its length, we have ${C_1}^k = id$ if and only if $k \in m_1\mathbb{Z}$, and ${C_2}^k = id$ if and only if $k \in m_2\mathbb{Z}$. Therefore $\sigma^k = id$ if and only if $k \in m_1\mathbb{Z} \cap m_2\mathbb{Z}$.

(6) We know that $m_1\mathbb{Z} \cap m_2\mathbb{Z} = M\mathbb{Z}$, where M denotes the lowest common denominator of m_1 and m_2. Therefore $\sigma^k = id$ if and only if $k \in M\mathbb{Z}$, which tells us that the order of σ is equal to M. In the present situation, $m_1 = 6$ and $m_2 = 4$ give $M = 12$.

(7)

$$\begin{aligned}\sigma^{18} &= \sigma^{12}\sigma^6 \\ &= \sigma^6 \\ &= {C_1}^6\, {C_2}^6 \\ &= {C_2}^2 \\ &= (2, 4)(10, 7)\ .\end{aligned}$$

(8)

$$\begin{aligned}\sigma^{2017} &= \left(\sigma^{12}\right)^{168}\sigma \\ &= \sigma\ .\end{aligned}$$

Problem 2.

(1) Let $H = \langle x \rangle$. The order of x is the cardinality of H, since $H = \{e, x, x^2, \ldots, x^{n-1}\}$, where n is the order of x. Note that H is finite as a subset of G, therefore x is of finite order (n is well-defined). By the theorem of Lagrange, n divides N.

(2) If x is of order N, then $H = \langle x \rangle$ has cardinality N, the same as G, so $H = G$. Therefore x is a generator of G, which shows that G is cyclic.

(3) Let x be any element of G which is not the identity element (such an x exists, because G has at least 2 elements). The order of x is > 1. By question (1), the order n of x divides N. Since N is prime is $n \neq 1$, we must have $n = N$. Therefore x is of order N, so that G must be cyclic by the previous question.

(4) If G is a cyclic group, then it is generated by some element $x \in G$: $G = \{x^k \mid 0 \leqslant k \leqslant N-1\}$. Let $y \in G$, thus we can write $y = x^k$ for some $k \in \{0, \ldots, N-1\}$. If y is of order 2, then we must have $k > 0$ and $y^2 = x^{2k} = e$. The only possibility for this to happen is $2k = N$. The conclusion follows easily: if N is odd, there are no solutions, and if N is even there is a unique solution.

(5) It is easy to check that any transposition is of order 2, in fact the order of any cycle is equal to its length. There are other element of order 2: any product of disjoint transpositions. These exist as soon as $n \geqslant 4$.

(6) By question (4), if S_n was cyclic, then it would have at most one element of order 2. However, any transposition is an element of order 2. There are more than one transposition as soon as $n \geqslant 3$, in which case S_n is not cyclic. When $n = 2$, S_n is cyclic (for instance, this is a consequence of question (3)).

Problem 3.

We need to show that for every $X_1 = (x_1, y_1)$ and for every $X_2 = (x_2, y_2)$ in Z^2, $\varphi(X_1 + X_2) = \varphi(X_1) + \varphi(X_2)$. This is a straightforward computation:

$$\begin{aligned}
\varphi(X_1 + X_2) &= \varphi((x_1, y_1) + (x_2, y_2)) \\
&= \varphi(x_1 + x_2, y_1 + y_2) \\
&= 2(x_1 + x_2) - 3(y_1 + y_2) \\
&= (2x_1 - 3y_1) + (2x_2 - 3y_2) \\
&= \varphi(X_1) + \varphi(X_2)\,.
\end{aligned}$$

φ is not a group isomorphism because it is not injective: for instance, $\varphi(0, 0) = \varphi(3, 2)$. Note that there cannot exist a group isomorphism between Z and Z^2, because the former group is cyclic and the latter is not.