Math 151

Solutions to selected homework problems

Section 2.3, Problem 11:

Prove that in S_n, with $n \geq 3$, any even permutation is a product of cycles of length three.

Hint: $(a, b)(b, c) = (a, b, c)$ *and* $(a, b)(c, d) = (a, b, c)(b, c, d)$.

Solution:

Any even permutation can be written as a product of an even number of transpositions. Pair up the transpositions in the product. For any pair of transpositions, we have to consider three cases:

Case I: they are disjoint. Then their product can be written as a product of two cycles of length three: $(a, b)(c, d) = (a, b, c)(b, c, d)$.

Case II: one element repeats. Let's denote the repeating element b, then the two transpositions have one of the following forms: $(a, b)(b, c)$, $(a, b)(c, b)$, $(b, a)(b, c)$, $(b, a)(c, b)$. Since $(b, a) = (a, b)$ and $(c, b) = (b, c)$, all four of the above products are equal to $(a, b)(b, c) = (a, b, c)$.

Case III: two elements repeat, i.e. the product has either the form $(a, b)(a, b)$ or the form $(a, b)(b, a)$. Again, these two are equal, and they are equal to the identity permutation, thus can be eliminated from the initial product of transpositions.

Thus, each pair of transpositions can be written as a product of cycles of length three, therefore the original permutation can be written as a product of cycles of length three.

Section 2.3, Problem 12:

Prove that (a, b) cannot be written as a product of two cycles of length three.

Solution:

The permutation (a, b) is a transposition, thus is an odd permutation. A cycle of length three is an even permutation: $(a, b, c) = (a, b)(b, c)$. Therefore the product of two cycles of length three is an even permutation, and cannot equal (a, b).

Note: A common mistake is to say that (a, b) only involves two elements (a and b), thus cannot possibly be written as a product of longer cycles (which would have to involve more than two elements). This is actually possible For example, (a, b) can be written as a product of three cycles of lengh four: $(a, b) = (a, c, d, b)(a, c, b, d)(a, b, c, d)$.

Section 2.3, Problem 15:

For $\alpha, \beta \in S_n$, let $\alpha \sim \beta$ if there exists $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that $\sim$ is an equivalence relation on S_n.

Solution:

We will check that $\sim$ is reflexive, symmetric, and transitive.

(i) For any $\alpha \in S_n$, there exists $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \alpha$, e.g. $\sigma = 1_S$, therefore $\alpha \sim \alpha$. Thus $\sim$ is reflexive.

(ii) If $\alpha \sim \beta$, then there exists $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Multiplying by σ^{-1} on the left gives $\sigma^{-1}\sigma\alpha\sigma^{-1} = \sigma^{-1}\beta$, or $\alpha\sigma^{-1} = \sigma^{-1}\beta$. Multiplying by σ on the right gives $\alpha\sigma^{-1}\sigma = \sigma^{-1}\beta\sigma$, or $\alpha = \sigma^{-1}\beta\sigma$. This can be written as $\alpha = \sigma^{-1}\beta(\sigma^{-1})^{-1}$, or $\sigma^{-1}\beta(\sigma^{-1})^{-1} = \alpha$, therefore $\beta \sim \alpha$. Thus $\sim$ is symmetric.

(iii) If $\alpha \sim \beta$ and $\beta \sim \gamma$, then there exist $\sigma_1, \sigma_2 \in S_n$ such that $\sigma_1\alpha\sigma_1^{-1} = \beta$ and $\sigma_2\beta\sigma_2^{-1} = \gamma$. Then $\sigma_2\sigma_1\alpha\sigma_1^{-1}\sigma_2^{-1} = \gamma$, which can be written as $(\sigma_2\sigma_1)\alpha(\sigma_2\sigma_1)^{-1} = \gamma$, therefore $\alpha \sim \gamma$. Thus $\sim$ is transitive.

Section 2.2, Problem 8(a,c):

For integers m, n, define $m \sim n$ if and only if $n|m^k$ and $m|n^j$ for some positive integers k and j.

(a) Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

(c) Give a characterization of the equivalence class $[m]$.

Solution:

(a) We will check that $\sim$ is reflexive, symmetric, and transitive.

(i) For any $m \in \mathbb{Z}$, $m|m^k$ and $m|m^j$ e.g. for $k = j = 1$, therefore $m \sim m$. Thus $\sim$ is reflexive.

(ii) If $m \sim n$, then $n|m^k$ and $m|n^j$ for some positive integers k and j. Then $m|n^j$ and $n|m^k$, so $n \sim m$. Thus $\sim$ is symmetric.

(iii) If $m \sim n$ and $n \sim p$, then $n|m^k$, $m|n^j$, $p|n^i$, and $n|p^l$ for some positive integers k, j, i, l. Then $m^k = an$, $n^j = bm$, $n^i = cp$, and $p^l = dn$ for some integers a, b, c, d. Therefore $m^{ki} = a^i n^i = (a^i c)p$ and $p^l j = d^j n^j = (d^j b)m$, i.e. $p|m^{ki}$ and $m|p^{lj}$. So $m \sim p$. Thus $\sim$ is transitive.

(c) The equivalence class of m consists of all integers equivalent to m. By definition, $m \sim n$ if $n|m^k$ and $m|n^j$ for some positive integers k and j. The condition $n|m^k$

is satisfied if and only if each prime in the prime factorization of n is present in the prime factorization of m (the number k can be chosen equal to the largest exponent of a prime in the prime factorization of n). Similarly, $m|n^j$ is satisfied if and only if each prime in the prime factorization of m is present in the prime factorization of n. Thus two numbers are equivalent if the prime factors that occur in their prime factorizations are the same. So if $m = p_1^{\alpha_1} \dots p_x^{\alpha_x}$ is the prime factorization of m, then $[m] = \{n \in \mathbb{Z} | n = \pm p_1^{\beta_1} \dots p_x^{\beta_x}, \beta_i \geq 1\}$. If $m = \pm 1$, then $[m] = \{1, -1\}$. If $m = 0$, $[m] = \{0\}$.