Math 541 Spring 2011
Solutions – Homework#6

1. *Homomorphism.*

   (a) Let $\alpha : G \to H$, $\beta : H \to K$ be two homomorphisms of groups. Show that the composition $\gamma = \beta \circ \alpha : G \to K$ is also homorphism.

   1. *Main points.* Definition.
   2. *Proof.* We have $\gamma(g \cdot g') = (\beta \circ \alpha)(g \cdot g') \overset{\text{def}}{=} \beta(\alpha(g \cdot g')) \overset{\alpha \text{ is hom}}{=} \beta(\alpha(g) \cdot \alpha(g')) \overset{\beta \text{ is hom}}{=} \beta(\alpha(g)) \cdot \beta(\alpha(g')) \overset{\text{def}}{=} (\beta \circ \alpha)(g) \cdot (\beta \circ \alpha)(g') = \gamma(g) \circ \gamma(g')$.

   (b) Show that if $\varphi : G \to H$ is an homomorphism which is a bijection, i.e., isomorphism, then $\varphi^{-1} : H \to G$ is also an homomorphism.

   1. *Main points.* $1 - 1$.
   2. *Proof.* Let $h_1, h_2 \in H$. We need to show that $\varphi^{-1}(h_1 \cdot h_2) \overset{?}{=} \varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2)$. Indeed, because of the fact that φ is $1-1$, it is enough to show that applying φ on both sides of what we want to check we get identity. Let us check this

   $$\varphi[\varphi^{-1}(h_1 \cdot h_2)] = h_1 \cdot h_2 = \varphi[\varphi^{-1}(h_1)] \cdot \varphi[\varphi^{-1}(h_2)] \overset{\varphi \text{ is hom.}}{=} \varphi[\varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2)].$$

   (c) Suppose G is a group acting on a set X. Consider the map $\alpha : G \to Aut(X)$, given by $g \mapsto \alpha[g]$, where $\alpha[g](x) = g \cdot x$. Show that α is a homomorphism.

   1. *Main points.* Associativity.
   2. *Proof.* For $g, h \in G$, we have

   $$\alpha[gh](x) = (gh) \cdot x \overset{\text{By assoc.}}{=} g \cdot (h \cdot x) = \alpha[g](\alpha[h](x)) = (\alpha[g] \circ \alpha[h])(x),$$

   and since this is true for every $x \in X$, we have the desired equality $\alpha[gh] = \alpha[g] \circ \alpha[h]$.

2. *The sign homomorphism.* Consider the sign homomorphism $sgn : S_n = Aut(\{1, ..., n\}) \to \{\pm 1\}$.

   (a) Show that every permutation $\sigma \in S_n = Aut(\{1, ..., n\})$ can be written as a product of disjoint cycles

   $$\sigma = c_k \circ ... \circ c_1, \tag{1}$$

   where by a cycle $c \in S_n$ we mean a permutation of the form

   $$c = (a_1 \ a_2 \ ... \ a_l), \quad 1 \leq a_i \leq n,$$

   i.e., $c(a_1) = a_2, ..., c(a_{l-1}) = a_l$, $c(a_l) = a_1$.

   1. *Main points.* Direct verification.

2. *Proof.* Take an element $a_1 \in \{1, ..., n\}$. Denote the element $a_2 = \sigma(a_1)$, if $a_2 \neq a_1$, then continue till (by the $1-1$ assumption on σ) we get after l steps, $\sigma(a_l) = a_1$. Hence,

$$\sigma = (a_1 \ a_2 \ ... \ a_l) \circ \tau,$$

for some "shorter" τ. Continue with the same method for τ. The process will stop after $1 \leq k \leq n$ steps and we get a decomposition of the form (1). In fact our proof show that the decomposition is unique up to reordering of the cycles $c_j^{\prime}s$.

(b) Decompose the following permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 1 & 3 & 8 & 6 & 7 \end{pmatrix} \in S_8,$$

to a product of disjoint cycles.

1. *Main points.* Follow the algorithm developed in paragraph (a) above.
2. *Computation.* We get

$$\sigma = (1\ 2\ 4) \circ (3\ 5) \circ (6\ 8\ 7). \tag{2}$$

(c) Show that every cycle $c = (a_1 \ a_2 \ ... \ a_l) \in S_n$ can be written as a product of transpositions.

1. *Main points.* Formula.
2. *Proof.* We have

$$(a_1 \ a_2 ... a_l) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ ... \circ (a_{l-1} \ a_l). \tag{3}$$

(d) Decompose the cycles that appear in 2(b), above, to product of transpositions.

1. *Main points.* Formula *(3)*.
2. *Solution.* We have

$$\begin{aligned} (1\ 2\ 4) &= (1\ 2) \circ (2\ 4), \\ (6\ 8\ 7) &= (6\ 8) \circ (8\ 7). \end{aligned} \tag{4}$$

(e) Compute the sign $sgn(\sigma)$ for σ above.

1. *Main points.* We have $sgn(\tau) = -1$ for every transposition τ.
2. *Computation.* Using (2), and (4) we get

$$sgn(\sigma) = (-1)^5 = -1.$$

(f) Can you suggest other ways how to compute $sgn(\sigma)$, for $\sigma \in S_n$?

1. *Main points.* Intersection method.
2. *Computation.* By looking on σ and connect the each number $1 \leq a \leq 8$ in the first row by a line with itself in the second row, and count the number of intersections m you get the result

$$sgn(\sigma) = (-1)^m = (-1)^7 = -1.$$

3. *Chinese reminder theorem.* Let m, n be two positive natural numbers which are co-prime, i.e., the greatest common devisor of m and n is 1 (notation: $\gcd(m, n) = 1$). Consider the groups $\mathbb{Z}_{mn} = \{0, 1, ..., mn-1\}$, $\mathbb{Z}_m = \{0, 1, ..., m-1\}$, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ with the natural addition modulo mn, m, n respectively.

   (a) Show that the map

$$\begin{aligned} \varphi &: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \\ x &\mapsto (x \bmod m,\ x \bmod n), \end{aligned}$$

   is an homomorphism.

   1. *Main points.* Division with reminder.
   2. *Proof.* Let $x, y \in \mathbb{Z}_{mn}$, consider the integer $x + y$ and write it as $x + y = z + q \cdot (mn)$, with $0 \leq z < mn$. We can write also $x = z' + q' \cdot m$, $y = z'' + q'' \cdot m$, with $0 \leq z', z'' < m$. So we see that $z = z' + z'' \bmod m$, which means $x + y \bmod m = (x \bmod m) + (y \bmod m)$. The same for mod n.

   (b) Show that there exist a unique integer $0 \leq x \leq 98$ such that

$$\begin{cases} x = 3 \mod 11, \\ x = 7 \mod 9. \end{cases}$$

   Find such an x.

   1. *Main points.* Chinese reminder theorem.
   2. *Calculation.* The uniqueness is because of the $1-1$ property of the map $\varphi : \mathbb{Z}_{99} \widetilde{\to} \mathbb{Z}_{11} \times \mathbb{Z}_9$, and the existence is because of the onto property of φ. The unique solution is $x = 25$.

Remark • I will be happy to help you with any questions on the solution. Please visit me in my office hours.

Good Luck!