PMAT 315
SOLUTIONS TO ASSIGNMENT 2
WINTER 2010

1. §1.4, #25. *Show that every even permutation is a product of 3-cycles.* 8 marks

   SOLUTION. Every even permutation is a product of *pairs* of transpositions, and each of these is a product of 3-cycles because $(a\ b)(a\ c) = (a\ c\ b)$ and $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.

2. §2.1, #18 *Show that the following are equivalent for a monoid M :* 8 marks

   (1) *If ab is a unit then both a and b are units.*

   (2) *If $ab = 1$ then $ba = 1$.*

   SOLUTION. (1)⇒(2). If $ab = 1$ then a is a unit by (1). But $a(ba) = (ab)a = 1a = a$. Left multiply by a^{-1} to get $a^{-1}[a(ba)] = a^{-1}a$, that is $ba = 1$.

   (2)⇒(1). If ab is a unit, let c denote its inverse. Then $1 = (ab)c = a(bc)$, so $(bc)a = 1$ by (2). Hence a is a unit (with inverse bc). Similarly b is a unit.

3. *Let H and K denote subgroups of a group G.*

   (1) *Show that $H \cap K$ is a subgroup of G.* 2 marks

   (2) *Show that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.* (§2.3, #17) 6 marks

   SOLUTION. (1). If $x, y \in H \cap K$ then x, $y \in H$ so x^{-1}, $xy \in H$. Similarly x^{-1}, $xy \in K$, so x^{-1}, $xy \in H \cap K$. Since $1 \in H \cap K$ is clear, we can use the subgroup test (Theorem 1 §2.3).

   (2). If $H \subseteq K$ or $K \subseteq H$, then $H \cup K$ equals K or H respectively, so $H \cup K$ is a subgroup. Conversely, suppose $H \cup K$ is a subgroup and $H \nsubseteq K$. We show $K \subseteq H$. Let $h \in H - K$. If $k \in K$, then $kh \notin K$ (if $kh = k_1 \in K$, then $h = k^{-1}k_1 \in K$). Since kh is in $H \cup K$ (because $H \cup K$ is a subgroup), this implies that $kh \in H$. But if $kh = h_1$ where $h_1 \in H$, then $k = h^{-1}h_1 \in H$.

4. (a) *Find the order of $\bar{2}$ in $\mathbb{Z}_{11}^*$.* 4 marks

   (b) *Find the order of* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 9 & 7 & 6 & 3 & 4 & 1 & 5 \end{pmatrix}$ *in S_9.* 4 marks

   SOLUTION. (a) The powers of $\bar{2}$ are $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^4 = \bar{5}$, $\bar{2}^5 = \overline{(-1)}$, so $\bar{2}^{10} = \bar{1}$. Hence $|\bar{2}|$ divides 10 by Theorem 2 §2.4, Since we have shown that $\bar{2}^k \neq \bar{1}$ if $k = 1, 2, 5$, we must have $|\bar{2}| = 10$.

   (b) The cycle factorization is $\sigma = (1\ 2\ 8)(3\ 9\ 5\ 6)(4\ 7)$ so $|\sigma| = lcm(3, 4, 2) = 12$ by Theorem 3 §2.4.

5. *Let a be an element of order $|a| = n$ in a group G. Given any integer m, let $d = gcd(n, m)$. Show that $\langle a^m \rangle = \langle a^d \rangle$.* 8 marks

   SOLUTION. We must show that both $\langle a^m \rangle \subseteq \langle a^d \rangle$ and $\langle a^d \rangle \subseteq \langle a^m \rangle$.

   $\langle a^m \rangle \subseteq \langle a^d \rangle$. As $d \mid m$ we have $m = qd$, $q \in \mathbb{Z}$. Hence $a^m = a^{qd} = (a^d)^q \in \langle a^d \rangle$. It follows that $\langle a^m \rangle \subseteq \langle a^d \rangle$.

   $\langle a^d \rangle \subseteq \langle a^m \rangle$. We have $d = xm + yn$, $x, y \in \mathbb{Z}$, so $a^d = (a^m)^x (a^n)^y = (a^m)^x\, 1 \in \langle a^m \rangle$. Hence $\langle a^d \rangle \subseteq \langle a^m \rangle$.