Algebra I - MAT1100
Assignment # 2
Due: 20 October 2011
Jerrod Smith, student ID 998 689 138

1. (a) What is the least integer n for which the symmetric group S_n contains an element of order 18?

   We will show that the smallest such integer is 11.

   First we show that the the order of a permutation is the least common multiple, l. c. m., of the lengths of the cycles in its decomposition. Recall that we can write any element $\sigma \in S_n$ as the product of disjoint cycles where the decomposition is unique up to the order of the cycles and cyclic permutations of the entries in each cycle. Also recall that we've shown that disjoint cycles commute. Then if $\sigma = \tau_1\tau_2...\tau_k$ is the cycle decomposition of σ where the τ_j are disjoint cycles of length t_j. Let $n = \text{l. c. m.}(t_1, ..., t_k)$ then $t_j|n$ for all $j = 1, ..., k$ and we can write $n = t_j m_j$ for some integers m_j. Then we have

   $$\begin{aligned} \sigma^n &= (\tau_1....\tau_k)^n \\ &= \tau_1^n....\tau_k^n \\ &= (\tau_1^{t_1})^{m_1}...(\tau_k^{t_k})^{m_k} \\ &= e^{m_1}....e^{m_k} = e \end{aligned}$$

   No smaller integer z can have this property since we must have that $t_j|z$ for all $j = 1, ..., k$ and n is by definition the smallest such integer.

   Therefore, to have an element of order 18 in S_n we must have a permutation σ with a cycle decomposition such that the l. c. m. of the lengths of the cycles in the cycle decomposition is 18. The smallest such choice is a 9-cycle and 2-cycle. Since the cycles much be disjoint we require at least 11 symbols as claimed.

   (b) What is the maximal order of an element of S_{26}?

   By the discussion above, the maximal order of an element is the largest integer n that is the lowest common multiple of the possible lengths of disjoint cycles in S_{26}. The possible cycle decompositions are given by all possible integral partitions of 26 (of which there are many!). It suffices to consider cycle lengths that are powers of distinct primes so as to remove any common factors from the lengths of cycles. The maximal order of an element in S_n is given by Landau's function which calculates the maximum l. c. m. of the lengths of integral partitions of n. Calculating such things is of course better left to computers. For $n = 26$ the maximum is achieved by the partition $26 = 1 + 4 + 5 + 7 + 9$ and the maximal order is 1260. A table of (small) values for the Landau function can be found here *http://oeis.org/A000793*.

2. Let H be a subgroup of index 2 in a group G then H is normal in G.

   By hypothesis there are two left cosets of H in G. Recall that two left cosets are either disjoint or coincide. Let $g \in G - H$ then the two left cosets of H in G are eH and

gH. Since $eH = H$, i.e. H is a subgroup and so contains the identity, we must have that $gH = G - H$. Now the two right cosets of H in G are $He = H$ and Hg; therefore we see that Hg must also equal $G - H$. So we see that $gH = Hg$ which holds for all $g \in G$. In particular we have that $gHg^{-1} = H$ for all $g \in G$ and so $N_G(H) = G$ and by definition H is normal in G as claimed.

3. Let $\sigma \in S_{20}$ be a permutation whose cycle decomposition consists of one 5-cycle, two 3-cycles and one 2-cycle. We determine the order of the centralizer $C_{S_{20}}(\sigma)$.

   S_{20} acts on itself by conjugation. First recall that $|C_{S_{20}}(\sigma)| = \dfrac{|S_{20}|}{|\operatorname{orb}_{S_{20}}(\sigma)|}$. We know that $|S_{20}| = 20!$. We calculate the size of the orbit (conjugacy class) of σ using that permutations are conjugate if and only if they have the same cycle type.

   Dummit and Foote give a formula for the size of each conjugacy class in S_n (pp. 132). Our permutation σ can be thought of consisting of one 5-cycle, two 3-cycles, one 2-cycle and seven "one-cycles".

$$|\operatorname{orb}_{S_{20}}(\sigma)| = \frac{20!}{(1!5^1)(2!3^2)(1!2^1)(7!1^7)}$$

   Then

$$|C_{S_{20}}(\sigma)| = \frac{|S_{20}|}{|\operatorname{orb}_{S_{20}}(\sigma)|} = 20!\frac{(1!5^1)(2!3^2)(1!2^1)(7!1^7)}{20!} = (5)(2 \cdot 3^2)(2)(7!) = 907200$$

4. Let G be a group of odd order. Show that x ix not conjugate to x^{-1} unless $x = e$.

   Let $x \in G$ be given. Suppose that there exists $g \in G$ such that $x^{-1} = gxg^{-1}$. Then we have

$$x = (x^{-1})^{-1} = (gxg^{-1})^{-1} = gx^{-1}g^{-1}. \tag{1}$$

   Since $|G|$ is odd it must be finite. Let $n = |g|$ which is odd since it divides the order of G. Then $n = 2m + 1$ for some $m \in \mathbb{N}$. We claim that $x^{-1} = x$ and we show this by inductively conjugating by g. We show that for all $1 \leq k \leq m$ we have $x = g^{2k}xg^{-2k}$. Indeed for $k = 1$, by (1) we have

$$g^2xg^{-2} = g(gxg^{-1})g^{-1} = gx^{-1}g^{-1} = x.$$

   Suppose that the claim holds for all $1 \leq k \leq m - 1$ then for $k = m$ we have

$$g^{2m}xg^{-2m} = g^2(g^{2(m-1)}xg^{-2(m-1)})g^{-2} = g^2xg^{-2} = x.$$

   Thus we can compute

$$x^{-1} = gxg^{-1} = g(g^{2m}xg^{-2m})g^{-1} = g^nxg^{-n} = exe = x.$$

   This implies that $x^2 = xx^{-1} = e$ which is impossible unless $x = e$ since the order of x must divide G which is odd.

5. Prove that if $G/Z(G)$ is cyclic then G is abelian.

   Suppose that $G/Z(G)$ is cyclic then there exists some element x of $G - Z(G)$ such that $xZ(G)$ generates $G/Z(G)$. Since the cosets of $Z(G)$ partition G, we have that G is the disjoint union

$$G = \bigsqcup_{n=0}^{\infty} x^n Z(G).$$

   Let a, b be arbitrary elements of G. Then there exists integers n, m and elements $z, w \in Z(G)$ such that $a = x^n z$ and $b = x^m w$. Since z, w are in the centre of G and powers of x commute, we have that

$$ab = (x^n z)(x^m w) = x^{n+m} zw = (x^m w)(x^m z) = ba.$$

   Since a, b were arbitrary we have that G is abelian.

6. Prove that if $\mathrm{Aut}(G)$ is cyclic then G is abelian.

   Suppose that $\mathrm{Aut}(G)$ is cyclic. Then every subgroup of $\mathrm{Aut}(G)$ is cyclic, including the group of inner automorphisms $\mathrm{Inn}(G)$. Define a homomorphism $\varphi : G \to \mathrm{Aut}(G)$ by $g \mapsto \phi_g$ where $\phi_g(x) := gxg^{-1}$ for all $x \in G$. This map is indeed a homomorphism since if $g, h \in G$ for all $x \in G$ we have

$$\phi(gh)(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \phi_g(hxh^{-1}) = \phi_g(\phi_h(x)) = \phi_g \circ \phi_h(x),$$

   i.e., $\varphi(gh) = \varphi(g) \circ \varphi(h)$.

   If $z \in Z(G)$ then

$$\phi_z(x) = zxz^{-1} = xzz^{-1} = xe = x \text{ for all } x \in G,$$

   i.e., $\varphi(z) = \mathrm{Id}_G \in \mathrm{Aut}(G)$; therefore $Z(G) \subset \ker \varphi$. Now suppose that $g \in \ker \varphi$. Then for all $x \in G$ we have

$$x = \mathrm{Id}_G(x) = \varphi(g)(x) = \phi_g(x) = gxg^{-1}$$

   and so $gx = xg$ and thus $g \in Z(G)$. Therefore $\ker \varphi = Z(G)$. By the first isomorphism theorem we have that $G/Z(G)$ is isomorphic to $\mathrm{Im}\, \varphi < \mathrm{Aut}(G)$ which is cyclic. Therefore by result of problem (5) we have that G is abelian.

7. (a) Let G be a group and let H be a subgroup of finite index. Prove that there is a normal subgroup N of G, contained in H, so that $(G : N)$ is also finite.

   Let $(G : H) = n < \infty$ we find a homomorphism $\Phi : G \to S_n$ with kernel contained in H.

   Consider the left cosets of H in G (which partition G); the index of H is the number of left cosets in G. Since H has finite index we have that $G/H = \{g_1 H, ..., g_n H\}$. The group G acts transitively on G/H by left multiplication. Indeed, $e(g_j H) = (eg_j)H = g_j H$ for all $1 \leq j \leq n$. If $x, y \in G$ then $x(y \cdot g_j H) = (xy) \cdot (g_j H)$ for all $1 \leq j \leq n$ and this defines an action. Finally if $gH, hH \in G/H$ then we have

$$hH = h(g^{-1}g)H = (hg^{-1})gH,$$

where $hg^{-1} \in G$ and thus the action is transitive.

Define the map $\Phi : G \to S_n$ by $h \mapsto \sigma_h$ defined by $\sigma_h(i) = j$ if and only if $h(g_iH) = g_jH$. The map Φ is clearly well-defined. We show Φ is a homomorphism. Suppose that $h, k \in G$ we show that $\Phi(hk) = \Phi(h)\Phi(k)$. For any $1 \leq i \leq n$ we have $\Phi(hk)(i) = \sigma_{hk}(i) = j$ if and only if $hk(g_iH) = g_jH$, that is, if and only if $h(kg_iH) = g_jH$ which occurs if and only if $k(g_iH) = g_lH$ and $h(g_lH) = g_jH$; therefore we have that

$$\sigma_h \circ \sigma_k(i) = \sigma_h(l) = j = \sigma_{hk}(i),$$

i.e., $\Phi(h)\Phi(k) = \Phi(hk)$ as required.

If $x \in \ker \Phi$ then $\sigma_x(i) = i$ for all $1 \leq i \leq n$ which occurs if and only if $x(gH) = (gH)$ for all $g \in G$; in particular, if we take $g = e$ we have that $xH = H$ which implies that $x \in H$. Therefore we have that $\ker \Phi \subset H$ as desired.

We conclude that $G/\ker \Phi$ is isomorphic to a subgroup of the finite group S_n and so $\ker \Phi$ is a normal subgroup of G with finite index which is contained in H.

(b) Let G be a group and H_1 and H_2 be subgroups of G. Suppose that $(G : H_1) < \infty$ and $(G : H_2) < \infty$. We show that $(G : H_1 \cap H_2) < \infty$.

Suppose that $(G : H_1) = n$ and $(G : H_2) = m$ are finite. The left cosets of H_1 in G partition the group G into n disjoint sets of size $|H_1|$. Since $H_1 \cap H_2$ is a subgroup of H_1 (and H_2) we have that the left cosets of $H_1 \cap H_2$ partition H_1 into $(H_1 : H_1 \cap H_2)$ disjoint sets of size $|H_1 \cap H_2|$. Similarly, $H_1 \cap H_2$ is a subgroup of G and thus partitions G into left cosets the number of which is the index. Putting this information together we see that

$$(G : H_1 \cap H_2) = n(H_1 : H_1 \cap H_2) = (G : H_1)(H_1 : H_1 \cap H_2).$$

We do not assume that H_1 or H_2 is normal in G so the product H_1H_2 may not be a subgroup of G but it is certainly a subset of G. If we consider the groups H_1 and H_2 in their own right we may form the direct product $H_1 \times H_2 \cong H_1H_2$ (as a group in its own right) with $H_1 \lhd H1H_2$, $H_2 \lhd H_1H_2$. By the second isomorphism theorem we have

$$H_1H_2/H_2 \cong H_1/H_1 \cap H_2.$$

Therefore $(H_1 : H_1 \cap H_2) = (H_1H_2 : H2)$. Since H_1H_2 is a subset of G we certainly have that $(H_1H_2 : H_2) \leq (G : H_2) = m < \infty$.

We have shown that

$$(G : H_1 \cap H_2) = (G : H_1)(H_1 : H_1 \cap H_2) = (G : H_1)(H_1H_2 : H_2) \leq (G : H_1)(G : H_2) < \infty$$

as claimed.