Solutions to Homework 4  
Math 600, Fall 2007

15 a) (5 pts) \(Z(S_n) = 1\) for \(n \geq 3\)
If \(g \in Z(S_n)\), then by normality, \(Z(S_n)\) contains all \(g'\) which have the same cycle structure as \(g\). We know that any such \(g'\) is conjugate to \(g\), but \(g \in Z(S_n)\) implies \(g = g'\). Thus \(g\) is the unique element of \(S_n\) with the cycle structure of \(g\), which can only happen if \(n = 2\) and \(g\) is the nontrivial element of \(S_2\).

16 (10 pts) \(|G| > 2 \Rightarrow |\text{Aut}(G)| > 1\)
If \(G\) is nonabelian then \(G\) has \([G : Z(G)] > 1\) number of inner automorphisms. If \(G\) is abelian \(g \mapsto g^{-1}\) is an automorphism which is nontrivial unless \(g^2 = 1\ \forall g \in G\). Examples of the latter case are \(G = \prod_{a \in A} C_2\) where \(A\) is a possibly uncountable index set, or the subgroup of \(G\) consisting of tuples with only finitely many nonzero entries. The second example shows that \(G\) need not be a direct product of \(C_2\)'s as groups. However, we see that \(G\) is always a \(\mathbb{F}_2\) vector space, simply by using additive notation. In fact, the notions \(\mathbb{F}_2\)-vector space and abelian group \(G\) with \(2G = 0\) are identical. Since every vector space has a basis \(\{x_\beta, \ \beta \in B\}\), we have \(G = \oplus_{\beta \in B} \mathbb{F}_2 x_\beta\). Using the axiom of choice, there is a nontrivial permutation \(\sigma\) of \(B\). Consider \(\phi : G \to G\) specified by \(\phi(x_\beta) = x_{\sigma \beta}\) and extend linearly over \(\mathbb{F}_2\). Again \(\phi\) being a vector space homomorphism means that it is a group homomorphism.

17a) (5 pts) Let \(\pi = (12345)\) in \(S_5\), show \(Z(\pi) = \langle \pi \rangle\)
Let \(\sigma \in Z(\pi)\) then we have
\[(12345) = \sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))\]
This implies \(\sigma = \pi^i\) where \(i = \sigma(1)\). Thus \(Z(\pi) \subset \langle \pi \rangle\) which together with \(Z(\pi) \supset \langle \pi \rangle\) (since \(\langle \pi \rangle\) is abelian) implies \(Z(\pi) = \langle \pi \rangle\)

17b) (5 pts) \(\pi = (12345)\) and \(\tilde{\pi} = (13524)\) are conjugate in \(S_5\) but not in \(A_5\)
We want to find \(\sigma \in S_n\) such that \(\tilde{\pi} = \sigma \pi \sigma^{-1}\), which is the same as
\[(13524) = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))\]
Therefore \(\sigma\) is determined once we pick \(\sigma(1)\). We have five possibilities for \(\sigma(1)\), namely 1, 3, 5, 2, 4 which are also \(\tilde{\pi}^i(1)\) for \(i = 0..4\) respectively. Let us call the \(\sigma\) resulting from the choice \(\sigma(1) = \tilde{\pi}^i(1)\)
by \(\sigma_i\), \(i = 0.4\). We have, \(\sigma_0 = (2354)\) and for \(i = 1.4\) we get \(\sigma_i = \pi^i\sigma_0\). Note that \(\pi \in A_5\) and \(\sigma_0 \notin A_5\), therefore \(\sigma_i \notin A_5\ \forall i\).

17c) (5 pts) If we are working in \(S_7\) instead of \(S_5\), then in the notation of part b), we have ten choices for \(\sigma\) namely \(\sigma_i\) and \(\sigma_i(67)\). The latter five are in \(A_7\) but not in \(A_6\).

18) (10 pts) Let \(S_n\) act on the set \(\{x_1, x_2, \cdots, x_n\}\) by \(\sigma : x_i \mapsto x_{\sigma(i)}\). Let \(\mathbb{F}\) be a field, for example \(\mathbb{F}_2\) and let \(V\) be the \(\mathbb{F}\)-vector space with basis \(\{x_1, x_2, \cdots, x_n\}\). We have \(V = \oplus_{i=1}^n \mathbb{F}x_i\). Extend the action of \(S_n\) on the basis linearly to get action of \(S_n\) on \(V\). This action satisfies the property that \(\sigma(k \cdot v) = k \cdot \sigma(v)\) where \(k \in \mathbb{F}\), \(v \in V\). This means we have a homomorphism \(\rho : S_n \to GL(n, \mathbb{F})\). It is clear that the matrices in \(\rho(S_n)\) have the property that each column contains exactly one entry with value 1 and other entries are zero. In fact \(\rho(\sigma)_{ij} = 1\) iff \(\sigma(j) = i\).

Thus we see that \(\rho(\sigma) = 1\) implies \(\sigma = 1\). We can therefore identify \(S_n\) with \(\rho(S_n)\).

Now let \(\gamma = \sigma_1 \cdots \sigma_k\) be a \(d\)-cycle where the \(\sigma_i\) are transpositions. Let \(H_i\) be the subspace of \(V\) on which \(\sigma_i\) acts as identity. Then clearly \(\gamma = \sigma_1 \cdots \sigma_k\) acts as identity on \(\cap H_i\). In other words \(K \supseteq \cap H_i\), where \(K\) is the subspace of \(V\) fixed by \(\gamma\). If \(\sigma_i = (12)\) then it is easily seen that \(H_i = \mathbb{F}(x_1 + x_2) \oplus_{i=3}^n \mathbb{F}x_i\) thus we see in general that \(\dim(H_i) = n - 1\). Similarly \(K = \mathbb{F}(x_1 + \cdots + x_d) \oplus_{i=d+1}^n \mathbb{F}x_i\) (when \(\gamma = (12 \cdots d)\)) so that \(\dim(K) = n - d + 1\). Define an inner product on \(V\) by \(\langle x_i, x_j \rangle = \delta_{ij}\) (in other words \(\langle v, w \rangle = v^t w\)). Pick vectors \(z_i\) such that \(H_i^\perp = \mathbb{F}z_i\). Now \(x \in \cap H_i \iff x \in (\bigoplus_{i=1}^k \mathbb{F}z_i)^\perp\). Thus \(\dim(\cap H_i) = n - \dim(\bigoplus_{i=1}^k \mathbb{F}z_i)\), and clearly \(k \geq \dim(\bigoplus_{i=1}^k \mathbb{F}z_i)\), therefore \(\dim(\cap H_i) \geq n - k\). Thus \(n - d + 1 \geq n - k\) or \(k \geq d - 1\).

Another direct proof of 18) (by Ryan Zavislak)

Proposition: Let \(\sigma \in S_n\) and \(\sigma = \sigma_1 \cdots \sigma_k\) where the \(\sigma_i\) are transpositions. Let \(\sigma = c_1c_2 \cdots c_l\) be the cycle decomposition of \(\sigma\) (including 1-cycles), then \(l \geq n - k\).

Corollary: If \(\sigma = (1, 2, \cdots, d) = \sigma_1 \cdots \sigma_k\) where the \(\sigma_i\) are transpositions, then \(k \geq d - 1\).

Proof of Corollary: In the notation of the proposition, we have \(l = n - d + 1\) by definition of \(\sigma\), and we have \(l \geq n - k\) by the proposition, whence \(k \geq d - 1\).

Proof of Proposition: We will use the formulae:

\[
(1, j)(1, 2, \cdots, m) = (1, 2, \cdots, j - 1)(j, j + 1, \cdots, m)
\]

\[
(1, 2, \cdots, j)(j, j + 1)(j + 1, j + 2, \cdots, m) = (1, 2, \cdots, j - 1, j + 1, j + 2, \cdots, m)
\]

The proposition is true for \(k = 1\). Assume it is true for \(k \leq m - 1\). Given \(\sigma = \sigma_1 \cdots \sigma_m\), let \(l\) denote the number of cycles (including 1-cycles) in the decomposition of \(\sigma_2 \cdots \sigma_m\). Consider the
product of $\sigma_1$ with the cycle decomposition of $\sigma_2 \cdots \sigma_m$, then we are (essentially) in the situation of the two formulae mentioned, whence the number of cycles in the decomposition of $\sigma$ is $l \pm 1$. By the inductive step, we have $l \geq n - m + 1$. Therefore, $l \pm 1 \geq l - 1 \geq n - m$ as was to be shown.

19) (10 pts) Let $n$ be the number of orbits. Let $x_i, \ i = 1..n$, be the representatives of the $n$ orbits which we denote by $O_{x_i}$. By definition $g$ fixes $x$ iff $g \in G_x$. Also recall that $|G_{gx}| = |G_x|$ because $G_{gx} = gG_x g^{-1}$. Thus:

$$\sum_{g \in G} f(g) = \sum_{x \in X} |G_x| = \sum_{i=1}^{n} \sum_{x \in O_{x_i}} |G_{x_i}| = \sum_{i=1}^{n} |G| = n |G| \quad \text{QED}$$