Solutions to Sample First Test

1. Since $|S_3 \times S_5| = 3! \cdot 5! = 6!$, and $|S_n| = n!$, we see that the only possible $n$ for which $|S_3 \times S_5|$ can be isomorphic to $S_n$ is 6. Now we look at the orders of the elements. The order of $((123), (12345))$ is the lowest common multiple of 3 and 5, which is 15; thus $S_3 \times S_5$ has an element of order 15. The cycle shapes of elements of $S_6$ are $(1), (12), (123), (1234), (12345), (12)(34), (12)(34)(56), (12)(345), (12)(3456), (123)(456)$, and these have orders $1, 2, 3, 4, 5, 2, 2, 6, 4, 3$ respectively; in particular $S_6$ has no elements of order 15. Therefore $S_3 \times S_5$ is not isomorphic to $S_6$, and the result follows.

2. (i) First $G \neq \emptyset$: this is obvious because $I^t = I$ which tells us that $I \in G$.
(ii) Now let $A, B \in G$. We next show that $AB \in G$. The definition of $G$ tells us that $AA^t = BB^t = I$, and we need to establish that $(AB)(AB)^t = I$. But $(AB)(AB)^t = ABB^tA^t = AAA^t = AA^t = I$, as required.
(iii) Finally we must show that $G$ is closed under taking inverses, so let $A \in G$. We want to prove that $A^{-1} \in G$, in other words $A^{-1}(A^{-1})^t = I$. But $A \in G$ implies $AA^t = I$, implies $A^t = A^{-1}$, implies $A = (A^{-1})^t$, implies $I = A^{-1}(A^{-1})^t$ and the proof is complete.

3. To show that we have an action, we have two things to check.
(i) $(1, 1) \cdot x = 1 \cdot x = x$.
(ii) $(p, q) \cdot ((g, h) \cdot x) = (p, q) \cdot (gh^{-1}) = pgxh^{-1} = (pg)x(qh)^{-1}$ (remember that the inverse of a product is the product of the inverses in the reverse order).
Finally if $Z(G) \neq 1$, there exists $z \in Z(G) \setminus 1$. Now set $k = (z, z)$, which is not equal to 1. Then $k \cdot x = (z, z) \cdot x = zxz^{-1} = xzz^{-1} = z$.

4. Let $G = \langle x \rangle$. Then the elements of $G$ are $x^i$ where $0 \leq i \leq 7$, and these have orders $8/(8, i)$, where $(8, i)$ denotes the greatest common divisor of 8 and $i$. Since $8/(8, i) = 2$ if and only if $i = 4$ (at least when $0 \leq i \leq 7$), we see that $G$ has a unique element of order 2, namely $x^4$.

There does exist a nonabelian group of order 8 with the property that it has exactly one element of order 2, namely the quaternion group $Q_8$. This has elements $\pm 1, \pm i, \pm j, \pm k$ where 1 is the identity element, which multiply according to the rules $(-1)^2 = 1$, $(\pm i)^2 = -1$, $(\pm j)^2 = -1$, $(\pm k)^2 = -1$, $ij = k, jk = i, ki = j, (−1)i = −i$, $−1j = −j$, and $−1k = −k$. It follows immediately that $Q_8$ is nonabelian (because for example, $ij = k$ and $ji = −k$) and that the orders of 1, $−1, i, −i, j, −j, k, −k$, are $1, 2, 4, 4, 4, 4, 4$, respectively.

5. Let $g \in C_G(\langle a \rangle)$. Then $ga^i = a^i g$ for all $i \in \mathbb{Z}$, in particular $ga = ag$. This shows that $g \in C_G(\{a\})$ and hence $C_G(\langle a \rangle) \subseteq C_G(\{a\})$. 
Now let \( g \in C_G(\{a\}) \). Then \( ga = ag \), and we see by induction on \( i \) that \( ga^i = a^i g \) for all \( i \in \mathbb{Z}^+ \). Also \( a^{-1}g = ga^{-1} \), and again by induction on \( i \), we see that \( (a^{-1})^i g = g(a^{-1})^i \) for all \( i \in \mathbb{Z}^+ \) and hence \( a^{-i}g = ga^{-i} \). Finally \( ga^0 = a^0 g \) because both sides are equal to \( g \). We have now established that \( ga^i = a^i g \) for all \( i \in \mathbb{Z} \), which shows that \( g \in C_G(\langle a \rangle) \) and we conclude that \( C_G(\{a\}) \subseteq C_G(\langle a \rangle) \). This completes the proof.

6. By Lagrange’s theorem, \(|G| = |G/N||N|\), so \(|G/N||G|\). Recall that if \( C \) is a cyclic group, then \( C \) has a cyclic subgroup of order \( n \) if and only if \( n \mid |C| \). It follows immediately that \( G \) has a cyclic subgroup \( H \) of order \( |G/N| \). Now \( G \) is cyclic, hence so is \( G/N \) and we deduce that \( G/N \) is a cyclic group of order \( |G/N| \). Since two cyclic groups are isomorphic if and only if they have the same order, we see that \( G/N \cong H \), as required.

An infinite cyclic group must be isomorphic to \( \mathbb{Z} \). Here the result is false, which we demonstrate with the example \( G = \mathbb{Z} \) and \( N = 2\mathbb{Z} \), the subgroup of all even integers. Then \( N \) is a normal subgroup of index 2 in \( G \), yet all nonidentity elements of \( G \) have infinite order. Therefore any subgroup of \( \mathbb{Z} \) not equal to 1 has infinite order, in particular \( G \) has no subgroup of order 2.

Test on Monday, February 21. Material as far as (and including) section 3.2, approximately. One problem will be identical to one of the ungraded homework problems. Review session on Sunday, February 20 at 4:45 p.m. in McBryde 210.