Algebra, Assignment 6
Solutions

1. Let \( \sigma : G \to G \) be an automorphism of \( G \). Let \( x, y \in G \) with \( y = \sigma(x) \).

   (a) Assume \( x^s = e \). Prove \( y^s = e \).
   
   Solution: \( y^s = \sigma(x)^s = \sigma(x^s) = \sigma(e) = e \)

   (b) Assume \( x^s \neq e \). Prove \( y^s \neq e \).
   
   Solution: As above, \( y^s = \sigma(x^s) \). An automorphism is injective (and surjective, for that matter) so if \( y^s = e \) then \( x^s = e \). The required statement is the contrapositive.

   (c) Show \( o(\sigma(x)) = o(\sigma(y)) \) (You can assume they are both finite.)
   
   Solution: \( o(\sigma(x)) \) is the least \( s \) for which \( x^s = e \) and \( o(\sigma(y)) \) is the least \( s \) for which \( y^s = e \). Since the values \( s \) are the same for both \( x, y \) the least value \( s \) is the same for both.

2. Let \( \sigma \in S_n \) be given by \( \sigma(i) = n+1-i \) (so \( 1 \cdots n \) is “reversed.”) When \( n = 403 \) is \( \sigma \) even or odd? For which \( n \) is \( \sigma \) even?
   
   Solution: We flip 1, 403, 2, 402 all the way to 201, 202 so there are 201 flips so \( \sigma \) is odd. More generally it depends on whether \( n \) is even or odd. When \( n = 2k + 1 \) there are \( k \) flips so it is even when \( k \) is even otherwise odd. When \( n = 2k \) there are \( k \) flips so it is even when \( k \) is even otherwise odd.

3. Here we write permutations in terms of their disjoint cycles.

   (a) Given \( \sigma = (12)(34) \) and \( \gamma = (56)(13) \) find \( \tau \in S_6 \) with \( \tau^{-1}\sigma\tau = \gamma \)
   
   Solution: We send 1234 into 5613. The other 56 go into the other 24 in either order:
   
   \[
   \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 2 & 4 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}
   \]

   (b) Prove that with \( \sigma = (123) \) and \( \gamma = (13)(578) \) there is no \( \tau \) with \( \tau^{-1}\sigma\tau = \gamma \)
   
   Solution: Such a \( \tau \) exists if and only if \( \sigma, \gamma \) have the same cycle sizes with the same multiplicity: these are 3 for \( \sigma \) and 2, 3 for \( \gamma \).

   (c) Set \( \sigma = (12)(34) \). In \( S_8 \) precisely how many \( \gamma \) have the property that \( \tau^{-1}\sigma\tau = \gamma \) for some \( \tau \)?
   
   Solution: We must have \( \gamma = (ab)(cd) \). So there are \( 8 \cdot 7 \cdot 6 \cdot 5 \) choices for \( a, b, c, d \) except we are overcounting by an eight factor as we can flip \( ab \), flip \( cd \), flip \( ab \) with \( cd \). So the number is \( 7 \cdot 6 \cdot 5 = 210 \).
4. Consider the symmetries of the square. Use the table and notation on the website file. For each symmetry \( v \) find the conjugacy class \( C(v) \) and the Normalizer \( N(v) \) as defined in §2.11. Check by calculation that the class equation, the equation at the top of Page 85, holds.

Solution: Call this group \( G \). Copying solution 1, the elements are \( I, R, S, T, V, H, D, A \) and the table is

\[
\begin{array}{cccccccccc}
 & I & R & S & T & V & H & D & A \\
I & I & R & S & T & V & H & D & A \\
R & R & S & T & I & D & A & H & V \\
S & S & T & I & R & H & V & A & D \\
T & T & I & R & S & A & D & V & H \\
V & V & A & H & D & I & S & T & R \\
H & H & D & V & A & S & I & R & T \\
D & D & V & A & H & R & T & I & S \\
A & A & H & D & V & T & R & S & I \\
\end{array}
\]

For the normalizer \( N(g) \) we look at which \( x \) have \( gx = xg \). We see:

\( N(I) = G \) (this is always the case with the identity)
\( N(R) = \{I, R, S, T\} = N(S) = N(T) \)
\( N(V) = \{I, S, V, H\} \)
\( N(H) = \{I, S, V, H\} = N(V) \)
\( N(D) = \{I, S, D, A\} = N(S) \)

The normalizers are always subgroups and so must have 1, 2, 4 or 8 elements.

For the conjugacy classes we first note \( C(I) = \{I\} \) as this is always the case with the identity. Looking at the eight values \( g^{-1}Rg \) we find \( R = IRI, T = VRV \) and no more so \( C(R) = \{R, T\} \). We see that \( S \) commutes with everything so \( C(S) = \{S\} \). (The center of the group, denoted \( Z[G] \), is those elements that commute with everything, here \( Z(G) = \{I, S\} \). Looking at the eight values \( g^{-1}Vg \) we find \( V = IVI, H = RVT \) and no more so \( C(V) = \{V, H\} \). Looking at the eight values \( g^{-1}Dg \) we find \( D = IDI, A = RDT \) and no more so \( C(D) = \{D, A\} \).

To summarize:
\( C(I) = \{I\}, C(S) = \{S\} \)
\( C(R) = C(T) = \{R, T\} \)
\( C(V) = C(H) = \{V, H\} \)
\( C(D) = C(A) = \{D, A\} \) Note that for each symmetry \( g \), \( 8 = o(G) = o(C(x)) \cdot o(N(x)) \). For the Class Equation take one from each equiva-
lence class – say $I, S, R, V, D$. We get

$$8 = o(G) = \frac{o(G)}{o(N(I))} + \frac{o(G)}{o(N(S))} + \frac{o(G)}{o(N(R))} + \frac{o(G)}{o(N(V))} = 1+1+2+2+2$$

5. Let $GL_n(R)$ be, as usual, the $n \times n$ nonsingular matrices over the Reals, under multiplication. Suppose $A \in GL_n(R)$ has real eigenvectors $\vec{v}_1, \ldots, \vec{v}_n$ with distinct real eigenvalues $\lambda_1, \ldots, \lambda_n$, so that $A\vec{v}_i = \lambda_i \vec{v}_i$ for $1 \leq i \leq n$. Recall from Linear Algebra that this implies that the vectors $\vec{v}_i$ form a basis for $R^n$. Let $\sim$ be the conjugacy relation defined in §2.11

(a) Suppose $B \sim A$. Prove that $B$ has the same eigenvalues $\lambda_1, \ldots, \lambda_n$. That is, show that there are real eigenvectors $\vec{w}_1, \ldots, \vec{w}_n$ with $B\vec{w}_i = \lambda_i \vec{w}_i$ for $1 \leq i \leq n$.

Solution: We have $B = P^{-1}AP$ with $P$ nonsingular so set $\vec{w}_i$ to be that vector with $P\vec{w}_i = \vec{v}_i$. Then

$$P^{-1}AP\vec{w}_i = P^{-1}A\vec{v}_i = P^{-1}\lambda_i \vec{v}_i = \lambda_i P^{-1}\vec{v}_i = \lambda_i \vec{w}_i$$

(b) (*) Conversely, Suppose $B$ has real eigenvectors $\vec{w}_1, \ldots, \vec{w}_n$ with distinct real eigenvalues $\lambda_1, \ldots, \lambda_n$, the same values as for $A$. Prove that $B \sim A$.

Solution: As the $\vec{v}_i$ and the $\vec{w}_i$ both form bases there is a matrix $P$ with $P\vec{w}_i = \vec{v}_i$ and then $P^{-1}AP\vec{w}_i = B\vec{w}_i$ for all $i$ so that $P^{-1}AP = B$.

6. The notation $Z_n \times Z_m$ (which we’ll be getting to) is the following group. The elements are the pairs $(i, j)$ where $0 \leq i < n$ and $0 \leq j < m$. The operation is $+$ which is defined coordinatewise, but the first coordinate is done modulo $n$ and the second is done modulo $m$. For example, in $Z_8 \times Z_9$ we have $(5, 6) + (4, 5) = (1, 2)$.

(a) List the elements and the table for $Z_2 \times Z_3$.

Solution: For clarity we leave out parentheses and commas so that 12 is shorthand for $(1, 2)$. The elements are then $00, 01, 02, 10, 11, 12$. 
(b) Find an explicit isomorphism $\phi : Z_2 \times Z_3 \rightarrow Z_6$. (Here $Z_6$ has the operation $+$, whenever we write $Z_n$ (without the asterisk!) it is under addition.)

**Solution:** Identity must go to identity so $\phi(00) = 0$. Now whatever goes to 1 determines $\phi$. One thing that works is to send 11 to 1. So $\phi(11) = 1$. As $\phi$ is a homomorphism $\phi(11 + 11) = \phi(11) + \phi(11) = 1 + 1 = 2$ so $\phi(02) = 2$. Continuing $\phi(10) = 3$, $\phi(01) = 4$ and $\phi(12) = 5$. Any group with $n$ elements that has an element $\alpha$ of order $n$ (as $Z_2 \times Z_3$ has 11) is isomorphic to $Z_n$ by setting $\phi(\alpha) = 1$.

7. (a) List the elements and the table for $Z_2 \times Z_4$.

**Solution:** The elements are 00, 01, 02, 03, 10, 11, 12, 13.

(b) Find the order of each element of the above group. (Note, as we are under $+$ we want to look at $x, x + x, x + x + x, \ldots$ until we reach $(0, 0)$.)

**Solution:** 00 has order 1. (The identity is always the only element with order one.) 12, 02 have order two and the rest have order four.
(c) Argue that $Z_2 \times Z_4$ is not isomorphic to $Z_8$.  
Solution: In $Z_8$ the element 1 has order eight but there is no element of order eight in $Z_2 \times Z_4$. 

8. Call (for the this problem only) a nearflip a transposition $\gamma = (s, s+1)$, that is, of consecutive terms. Recall that $A[\tau]$ is the number of pairs $1 \leq i < j \leq n$ with $\tau(i) > \tau(j)$. Call such $i, j$ reversals for $\tau$.

(a) Following the argument given in class show that $A[\gamma \tau] = A[\tau] + 1$ if $\tau[s] < \tau[s + 1]$, and $A[\gamma \tau] = A[\tau] - 1$ if $\tau[s] > \tau[s + 1]$. Call such $i, j$ reversals for $\tau$.
Solution: When neither $i, j$ is either $s, s+1$, they are either both or neither reversals for $\tau, \gamma \tau$. For $i \neq s, s + 1$, $is$ is a reversal for $\tau$ iff $i, s + 1$ is a reversal for $\gamma \tau$. Similary for $js, j, s + 1$. So their contributions to the counts of reversals are the same for $\tau, \gamma \tau$. If $\tau[s] < \tau[s + 1]$ then $s, s + 1$ is not a reversal for $\tau$ but is for $\gamma \tau$ and if $\tau[s] < \tau[s + 1]$ then $s, s + 1$ is not a reversal for $\gamma \tau$ but is for $\tau$.

(b) Write an arbitrary transposition $\kappa = (u, v)$ (say $u < v$) as an explicit product of nearflips. How many nearflips did you use?
Solution: First $(u, u+1) \cdot (u+1, u+2) \cdot \ldots \cdot (v-1, v)$ moves $u$ to $v$ and all else down one. Then $(v-2, v-1) \cdot (v-2, v-3) \cdot \ldots \cdot (u, u+1)$ moves $v$ (which starts at $v-1$ down to $u$ and all else back up one to where it was before. The total number of nearflips is $v - u$ for the first part and $v - u + 1$ for the second part, for $2v - 2u + 1$.

(c) Using the above given an alternate proof that $A[\kappa \tau]$ and $A[\kappa]$ have different parities.
Solution: The value changes by one everytime you multiply by a nearflip. Since you do that an odd ($2v - 2u + 1$) number of times the parity of the value changes. (Note: You can’t say exactly what the change is since when you multiply by a nearflip you might go up one or you might go down one.)