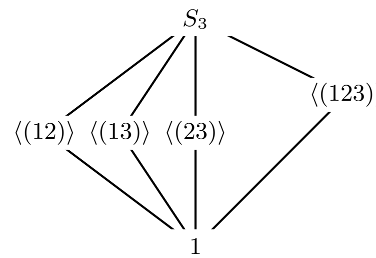
Abstract Algebra I MATH 601 Midterm October 31, 2012

Name:________________ R. Hammack Score:______

1. Short Answer (8 points each)

(a) Draw the subgroup lattice for S_3.



(b) List all generators of $\mathbb{Z}/54\mathbb{Z}$.

These are the elements $\overline{a}$, where a is relatively prime to 54. They are:
$\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}, \overline{37}, \overline{41}, \overline{43}, \overline{47}, \overline{49}, \overline{53}$.

(c) List all Sylow subgroups of $\mathbb{Z}/54\mathbb{Z}$.

Note $|\mathbb{Z}/54\mathbb{Z}| = 54 = 2 \cdot 3^3$

Sylow 2-subgroup: $\langle\overline{27}\rangle = \{\overline{0}, \overline{27}\}$
Sylow 3-subgroup: $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \ldots, \overline{52}\}$

(d) Give an example of two elements of A_5 that are conjugate in S_5 but not conjugate in A_5.
Consider (12345) and (13524) in A_5.
They are conjugate by $\pi = (2354)$ because $\pi(123)\pi^{-1} = (2354)(12345)(4532) = (13524)$.
However π is an odd permutation in S_5 and therefore is not in A_5.

(e) Show $SL_2(\mathbb{F}_3) \ncong S_4$.

You can check that $|SL_2(\mathbb{F}_3)| = 24 = |S_4|$, so mere cardinality will not prove these are non-isomorphic.

Each element of S_4 has one of the following cycle types: $(), (12), (12)(24), (123)$ or (1234). Each of these has order 1, 2, 3 or 4. Thus, in particular, S_4 has no elements of order 6 or greater. To show $SL_2(\mathbb{F}_3) \ncong S_4$, we will produce an element in $A \in SL_2(\mathbb{F}_3)$ of order at least 6.

Consider the element $A = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} \in SL_2(\mathbb{F}_3)$. Notice that repeatedly applying this matrix to the vector $\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathbb{F}_3^2$ produces the sequence

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 0 \\ 2 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathbf{e}_1.$$

This implies that $A^k\mathbf{e}_1 \neq \mathbf{e}_1$, for $k = 1, 2, 3, 4, 5$, but $A^6\mathbf{e}_1 = \mathbf{e}_1$. It follows that $A^k \neq I$ for $k = 1, 2, 3, 4, 5$. Thus the order of A is at least 6. It follows that $SL_2(\mathbb{F}_3) \ncong S_4$.

(On second thought, I guess that was not such a short answer after all. Sorry! RH)

2. Prove that $Z(D_{2n}) = 1$ if n is odd.

   Proof: Let $n = 2k+1$ be odd. Then $D_{2n} = \{1, r, r^2, r^3, \ldots, r^{2k}, s, sr, sr^2, sr^3, \ldots, sr^{2k}\}$. Notice that $(r^\ell)^{-1} = r^{(2k+1)-\ell}$. As ℓ and $(2k-1)-\ell$ have opposite parity, it follows that $\ell \neq (2k-1)-\ell$ and hence $(r^\ell)^{-1} \neq r^\ell$ for all $1 \leq \ell \leq 2k$.

   Now consider an element of of D_{2n} of form r^ℓ with $\ell > 0$. Since $r^\ell s = sr^{-\ell} = s(r^\ell)^{-1} \neq sr^\ell$, it follows that r^ℓ does not commute with s and hence r^ℓ is not in the center of D_{2n}.

   Next, consider an element of D_{2n} of form sr^ℓ with $1 \leq \ell \leq 2k$. Observe that $s(sr^\ell) = r^\ell \neq (r^\ell)^{-1} = r^{-\ell} = r^{-\ell}ss = (sr^\ell)s$. Thus $s(sr^\ell) \neq (sr^\ell)s$, so sr^ℓ does not commute with s. Therefore sr^ℓ is in in the center of D_{2n}.

   The only non-identity element we've not yet checked is s. Notice that $sr = r^{-1}s \neq rs$, so s can't be in the center.

   Now we've seen that any non-identity element is not in the center of D_{2n}. Conclusion: $Z(D_{2n}) = 1$.

3. Prove that if the center of G is of index n, then every conjugacy class of G has at most n elements.

   Proof: Let A be a conjugacy class in G that contains $a \in G$. Recall that $|A| = |G : C_G(a)|$. Also, $Z(G) \leq C_G(a)$ because if $g \in Z(G)$, then $gag^{-1} = agg^{-1} = a$, hence $g \in C_G(a)$. Then $Z(G) \leq C_G(a) \leq G$. Therefore $|G : Z(G)| = |G : C_G(a)| \cdot |C_G(a) : Z(G)|$, and hence

$$|G : C_G(a)| = \frac{|G : Z(G)|}{|C_G(a) : Z(G)|} = \frac{n}{|C_G(a) : Z(G)|} \leq n.$$

   This shows that the conjugacy class containing a has at most n elements.

4. Use Sylow's Theorem to prove Cauchy's Theorem.

Proof: Suppose p is a prime dividing $|G|$. Let P be a Sylow p-subgroup, so its order is some power p^α of p. Take a non-identity element $a \in P$. As the order of a must divide $|P| = p^\alpha$, we have $|a| = p^\beta$ for some $\beta \leq \alpha$. Then $(a^{p^{\beta-1}})^p = a^{p^\beta} = 1$. Now, if $n < p$, then $(a^{p^{\beta-1}})^n = a^{np^{\beta-1}} \neq 1$ because $np^{\beta-1}$ is smaller than the order p^β of a. It follows that the element $a^{p^{\beta-1}} \in P \leq G$ has order p. ■

5. Prove that if $H \leq G$ has index n, then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Proof: Let G act on the set $A = \{aH : a \in G\}$ of left-cosets of H by the action $g.aH = gaH$. (This is an action because $g.(g'.aH) = g.g'aH = gg'aH = (gg').aH$ and $1.aH = 1aH = aH$.) Now, because $|G : H| = n$, we have $|A| = n$. Consider the permutation representation $\varphi : G \to S_A \cong S_n$. The kernel K of this homomorphism is a normal subgroup of G. Given an element $k \in K$, we must have $k.1H = 1H$, that is $kH = H$, so $k \in H$. Therefore $K \leq H$.

By the First Isomorphism Theorem, $G/K \cong \varphi(G) \leq S_A \cong S_n$. Then $|G : K| = |G/K| = |\varphi(G)| \leq |S_n| = n!$. We have now produced a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$. ■

6. Let G be a group and $\sigma \in \text{Aut}(G)$. Suppose $\varphi_g \in \text{Aut}(G)$ is conjugation by g, that is, $\varphi_g(x) = gxg^{-1}$. Prove that $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.

   Proof: Note that, in particular, σ is a homomorphism from G to G. Using the definitions of composition, conjugation, and the homomorphism properties $\sigma(gh) = \sigma(g)\sigma(h)$ and $\sigma(g^{-1}) = \sigma(g)^{-1}$, we obtain the following, for any $x \in G$.

$$\begin{aligned}
\sigma\varphi_g\sigma^{-1}(x) &= \sigma\varphi_g(\sigma^{-1}(x)) \\
&= \sigma(g\sigma^{-1}(x)g^{-1}) \\
&= \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1}) \\
&= \sigma(g)x\sigma(g^{-1}) \\
&= \sigma(g)x\sigma(g)^{-1} \\
&= \varphi_{\sigma(g)}(x).
\end{aligned}$$

   This shows $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$.

   We've now shown that for any $\varphi_g \in \text{Inn}(G) \leq \text{Aut}(G)$ and any $\sigma \in \text{Aut}(G)$, we have

$$\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)} \in \text{Inn}(G).$$

   This means that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. ■

7. Let G be a group of order 462. Prove that G is not simple.

   Note $462 = 2 \cdot 3 \cdot 7 \cdot 11$.

   Let P be a Sylow 11-subgroup. Then $n_{11}(G) \equiv 1 (\text{mod } 11)$ which means $n_{11}(G) \in \{1, 12, 23, 34, 45, \ldots\}$. Also $n_{11}(G)$ divides $m = 2 \cdot 3 \cdot 7 = 42$. From this, we see that the only possibility is $n_{11}(G) = 1$, so P must be normal. Thus G is not simple.