Homework 7

1. Consider the following group, which you may think of as $\mathrm{GL}_2(\mathbb{Z}_2)$:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad a, b, c, d \in \mathbb{Z}_2, \quad ad - bc \equiv 1 \pmod 2 \right\}$$

The operation is matrix multiplication, although we now use addition and multiplication in $\mathbb{Z}_2$ instead of $\mathbb{R}$. You may verify that this is a group, although you do not need to prove it on your homework. Show that G is isomorphic to the group S_3.

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

order 1 2 2 2 3 3

$\phi: G \to S_3$

This is 1-1 and onto.

$\phi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = e$ $\quad \phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = (1\,2)$

$\phi\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = (2\,3)$ $\quad \phi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (3\,1)$

$\phi\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1\,3\,2)$ $\quad \phi\left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right) = (1\,2\,3)$

Check ϕ is homomorphism:

$$\phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = \phi\left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right) = (1\,2\,3) = (1\,2)(2\,3) = \phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)\phi\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)$$

$$\phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \phi\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1\,3\,2) = (1\,2)(3\,1) = \phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)\phi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$$

etc. So ϕ is a homomorphism

This gives an isomorphism $G \cong S_3$.

2. In class we applied the construction of Cayley's Theorem to the quaterion group Q_8 to produce a 1-1 homomomorphism $\phi : Q_8 \to S_8$. Apply the same construction to the following groups, to get homomorphisms into symmetric groups:

   (a) $(\mathbb{Z}_3, +)$

   (b) $(\mathbb{Z}_8^\times, \times)$

   (c) S_3

(a) $\mathbb{Z}_3 = \{0,1,2\}$ $a_1 = 0$, $a_2 = 1$, $a_3 = 2$

$a = 0$:
$a + a_1 = 0 + 0 = 0 = a_1$ $\sigma_0(1) = 1$
$a + a_2 = 0 + 1 = 1 = a_2$ $\sigma_0(2) = 2$
$a + a_3 = 0 + 2 = 2 = a_3$ $\sigma_0(3) = 3$
$\sigma_0 = e$ identity permutation

$a = 1$:
$a + a_1 = 1 + 0 = 1 = a_2$ $\sigma_1(1) = 2$
$a + a_2 = 1 + 1 = 2 = a_3$ $\sigma_1(2) = 3$
$a + a_3 = 1 + 2 = 0 = a_1$ $\sigma_1(3) = 1$
$\sigma_1 = (1\,2\,3)$

$\sigma_2 = \sigma_1^{-1} = (1\,3\,2)$ (since Cayley construction is a homomorp.)

Thus $\phi : \mathbb{Z}_3 \to S_3$ is $\phi(0) = e$, $\phi(1) = (1\,2\,3)$, $\phi(2) = (1\,3\,2)$.

(b) $\mathbb{Z}_8^\times = \{1,3,5,7\}$ $a_1 = 1$, $a_2 = 3$, $a_3 = 5$, $a_4 = 7$

$a = 3$:
$a \cdot a_1 = 3 \cdot 1 = 3 = a_2$ $\sigma_3(1) = 2$
$a \cdot a_2 = 3 \cdot 3 = 1 = a_1$ $\sigma_3(2) = 1$
$a \cdot a_3 = 3 \cdot 5 = 7 = a_4$ $\sigma_3(3) = 4$
$a \cdot a_4 = 3 \cdot 7 = 5 = a_3$ $\sigma_3(4) = 3$
$\sigma_3 = (1\,2)(3\,4)$

$a = 5:$ $\quad a \cdot a_1 = 5 \cdot 1 = 5 = a_3 \qquad \sigma_5(1) = 3$

$a \cdot a_2 = 5 \cdot 3 = 7 = a_4 \qquad \sigma_5(2) = 4 \qquad \sigma_5 = (13)(24)$

$a \cdot a_3 = 5 \cdot 5 = 1 = a_1 \qquad \sigma_5(3) = 1$

$a \cdot a_4 = 5 \cdot 7 = 3 = a_2 \qquad \sigma_5(4) = 2$

Cayley constr. is a homomor.

$\sigma_7 = \sigma_{3 \cdot 5} = \sigma_3 \cdot \sigma_5 = (12)(34) \cdot (13)(24) = (14)(23).$

Thus $\phi : \mathbb{Z}_8^\times \to S_4$ is: $\phi(1) = e$, $\phi(3) = (12)(34)$, $\phi(5) = (13)(24)$, $\phi(7) = (14)(23)$.

(c) $S_3 = \{e, (12), (23), (31), (123), (132)\}$

$$\begin{array}{cccccc} e & (12) & (23) & (31) & (123) & (132) \\ \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array}$$

$a = (12):$ $\quad a \cdot a_1 = (12)e = (12) = a_2 \qquad \sigma_{(12)}(1) = 2$

$a \cdot a_2 = (12)(12) = e = a_1 \qquad \sigma_{(12)}(2) = 1$

$a \cdot a_3 = (12)(23) = (123) = a_5 \qquad \sigma_{(12)}(3) = 5$

$a \cdot a_4 = (12)(31) = (132) = a_6 \qquad \sigma_{(12)}(4) = 6$

$a \cdot a_5 = (12)(123) = (23) = a_3 \qquad \sigma_{(12)}(5) = 3$

$a \cdot a_6 = (12)(132) = (13) = a_4 \qquad \sigma_{(12)}(6) = 4$

$\longrightarrow \sigma_{(12)} = (12)(35)(46)$

$a = (23):$ $\quad a \cdot a_1 = (23)e = (23) = a_3 \qquad \sigma_{(23)}(1) = 3$

$a \cdot a_2 = (23)(12) = (132) = a_6 \qquad \sigma_{(23)}(2) = 6$

$a \cdot a_3 = (23)(23) = e = a_1 \qquad \sigma_{(23)}(3) = 1$

$a \cdot a_4 = (23)(31) = (123) = a_5 \qquad \sigma_{(23)}(4) = 5$

$a \cdot a_5 = (23)(123) = (13) = a_4 \qquad \sigma_{(23)}(5) = 4$

$a \cdot a_6 = (23)(132) = (12) = a_2 \qquad \sigma_{(23)}(6) = 2$

$\longrightarrow \sigma_{(23)} = (13)(26)(45).$

Now use that the Cayley construction is a homomorphism.

$\sigma_{(123)} = \sigma_{(12)}\sigma_{(23)} = (12)(35)(46)\cdot(13)(26)(45) = (156)(243)$

$\sigma_{(132)} = \sigma_{(23)}\sigma_{(12)} = (13)(26)(45)\cdot(12)(35)(46) = (165)(234)$

$\sigma_{(31)} = \sigma_{(132)}\sigma_{(23)} = (165)(234)\cdot(13)(26)(45) = (14)(25)(36)$

Thus $\phi : S_3 \to S_6$ is given by

$\phi(e) = e$

$\phi((12)) = (12)(35)(46)$

$\phi((23)) = (13)(26)(45)$

$\phi((31)) = (14)(25)(36)$

$\phi((123)) = (156)(243)$

$\phi((132)) = (165)(234)$

3. Consider the quaternion group $Q_8 = \{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$.

   (a) List all subgroups of Q_8, and explain why your list is complete.

   (b) Show that every subgroup of Q_8 is normal.

   (c) Construct an onto homomorphism $Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$. From your homomorphism, what does the 1st Isomorphism Theorem imply?

(a) Suppose $H \leq G$ is a subgroup and $i \in H$ or $-i \in H$.
Then $\langle i \rangle = \{1, -1, i, -i\} \subseteq H$.
If $H \neq \langle i \rangle$ then $j, -j, k,$ or $-k \in H$. But i together with any one of these generates Q_8, so $H = Q_8$.
Otherwise $H = \langle i \rangle$.
Similarly if j or $-j \in H$ then either $H = \langle j \rangle$ or $H = Q_8$.
if k or $-k \in H$ then either $H = \langle k \rangle$ or $H = Q_8$.
If none of $\pm i, \pm j, \pm k$ are in H then $H = \{1, -1\}$ or $H = \{1\}$.
This exhausts all possibilities.
Thus the subgroups of Q_8 are $\{1\}$, $\{1, -1\}$, Q_8 and
$\langle i \rangle = \{1, -1, i, -i\}$, $\langle j \rangle = \{1, -1, j, -j\}$, $\langle k \rangle = \{1, -1, k, -k\}$.

(b) $\{1\}$ is clearly normal, and same for Q_8.
-1 commutes with everything so $\{1, -1\}$ is normal.
$\langle i \rangle = \{1, -1, i, -i\}$ is normal: $j i j^{-1} = j i (-j) = (-k)(-j) = -i$
$j(-i)j^{-1} = i$
so $j \langle i \rangle j^{-1} = \langle i \rangle$.
Similarly $k \langle i \rangle k^{-1} = \langle i \rangle$. So $\langle i \rangle$ is normal.
Same argument for $\langle j \rangle$, $\langle k \rangle$.

(c) $\phi : Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$

$\phi(1) = (0,0)$ $\phi(-1) = (0,0)$

$\phi(i) = (1,0)$ $\phi(-i) = (1,0)$

$\phi(j) = (0,1)$ $\phi(-j) = (0,1)$

$\phi(k) = (1,1)$ $\phi(-k) = (1,1)$.

Clearly ϕ is onto.

Check it's a homomorphism:

$$\phi(ij) = \phi(k) = (1,1) = (1,0) + (0,1) = \phi(i) + \phi(j)$$
$$\phi(jk) = \phi(i) = (1,0) = (0,1) + (1,1) = \phi(j) + \phi(k)$$
$$\phi(ki) = \phi(j) = (0,1) = (1,1) + (1,0) = \phi(k) + \phi(i)$$

Similarly $\phi(-i \cdot j) = \phi(-k) = (1,1) = (1,0) + (0,1) = \phi(-i) + \phi(j)$ etc.

$\ker(\phi) = \{1, -1\}$.

By the 1st Iso. Theorem:

$$\frac{Q_8}{\ker \phi} = \frac{Q_8}{\{1,-1\}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

4. Use the last result stated in Lecture 18 to show the following: a group of order p^2, where p is a prime, must have a normal subgroup of order p.

The result: G finite group, $H \subsetneq G$ proper subgroup suppose $|G|$ doesn't divide $[G:H]!$ Then H contains a non-trivial normal subgroup of G.

Now let G have $|G| = p^2$, p prime.

Let $a \in G$, $a \neq e$. If $\langle a \rangle = G$ then G is cyclic and isomorphic to $\mathbb{Z}_{p^2}$ which has a normal subgroup $\{0, p, 2p, \dots, (p-1)p\} \cong \mathbb{Z}_p$.

So suppose $\langle a \rangle \neq G$. Then $H = \langle a \rangle$ must have $|H| = p$.

Now $|G| = p^2$ doesn't divide $[G:H]! = p! = p(p-1)\cdots 2 \cdot 1$ because p is prime.

By the result, H contains a nontrivial normal subgroup of G, say N.

But $[G:N]$ divides p^2 and $\neq p^2$ so $[G:N] = p$ $\Rightarrow N = H$.

Thus H is normal and of order p. $\blacksquare$