Solutions to Final Exam

1. Let G be a group of order $21 = 3 \cdot 7$.

   (a) Use the Sylow theorems to show that G contains an element x of order 7, and an element y of order 3, and that $yxy^{-1} = x^k$ for some integer k.

   Solution: By Sylow's first theorem, there is a subgroup $H \subset G$ of order 7. Every group of order 7 is cyclic, so let x be a generator. Similarly, there is a subgroup $K \subset G$ of order 3, and every group of order 3 is cyclic, so let y be a generator. Finally, by Sylow's third theorem, the number n_7 of subgroups of order 7 satisfies $n_7 \equiv 1 \pmod{7}$ and $n_7 \mid 3$, so $n_7 = 1$. Now yHy^{-1} is a subgroup of order 7, so $yHy^{-1} = H$, so $yxy^{-1} = x^k$ for some $k \in \mathbb{Z}$.

   (b) Show that every element of G can be written uniquely as $x^i y^j$, for some $i \in \{0, 1, 2, \ldots, 6\}$ and $j \in \{0, 1, 2\}$.

   Solution: Since $H \cap K$ is a subgroup of H, we know that $|H \cap K|$ divides $|H| = 7$. Similarly, $|H \cap K|$ divides $|K| = 3$. Thus $|H \cap K| = 1$. So in particular y and y^2 are not in H, so $H \neq Hy$, so $H \cap Hy = \emptyset$, and similary $H \cap Hy^2 = \emptyset$ and $Hy \cap Hy^2 = \emptyset$. Thus $H \cup Hy \cup Hy^2$ is a subset of G with $7+7+7 = 21$ elements, hence is all of G. Any element of H can be written uniquely as x^i for some $i \in \{0, 1, 2, \ldots, 6\}$, and similarly any element of Hy can be written uniquely as $x^i y$, and any element of Hy^2 as $x^i y^2$.

   (c) Show that $k^3 \equiv 1 \pmod{7}$. Which values of k satisfy this equation?

   Solution: Since $y^3 = 1$, we have

   $$x = y^3 x y^{-3} = y^2 x^k y^{-2} = (y^2 x y^{-2})^k$$
   $$= (y x^k y^{-1})^k = (y x y^{-1})^{k^2} = x^{k^3}.$$

   If you want to say this more succinctly, that's OK. Since x has order 7, we conclude that $k^3 \equiv 1 \pmod{7}$. Thus $k \equiv 1$, 2, or 4 $\pmod{7}$.

(d) If $k = 1$, show that the map $\varphi\colon \mathbb{Z}_7 \times \mathbb{Z}_3 \to G$ given by $\varphi(i, j) = x^i y^j$ is an isomorphism.

Solution: From part (b) we know that φ is bijective. If $yxy^{-1} = x$ then $yx = xy$, so

$$\begin{aligned}
\varphi(i + i', j + j') &= x^{i+i'} y^{j+j'} \\
&= x^i x^{i'} y^j y^{j'} \\
&= x^i y^j x^{i'} y^{j'} \\
&= \varphi(i, j)\varphi(i', j'),
\end{aligned}$$

so φ is a homomorphism.

(e) Let $T \subset \mathrm{GL}_2(\mathbb{Z}_7)$ be the set of matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a \in \{1, 2, 4\}$ and $b \in \{0, 1, 2, \ldots, 6\}$. Show that T is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_7)$.

Solution: First note that $\{1, 2, 4\}$ is a subgroup of $\mathbb{Z}_7^\times$: we have $2 \cdot 4 = 1$ and $4 \cdot 4 = 2$, and $2^{-1} = 4$ and $4^{-1} = 2$.

Next, we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix},$$

which lies in T because $\{1, 2, 4\} \subset \mathbb{Z}_7^\times$ is closed under multiplication.

Next, we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -ba^{-1} \\ 0 & 1 \end{pmatrix},$$

which lies in T because $\{1, 2, 4\} \subset \mathbb{Z}_7^\times$ is closed under inverses.

(f) Show that the matrix

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in T$$

satisfies $x^7 = 1$.

For each of the two interesting values of k in part (c), find a matrix $y \in T$ with $y^3 = 1$ and $yx = x^k y$.

Solution: We have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b + 1 \\ 0 & 1 \end{pmatrix},$$

so by induction,

$$x^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}.$$

Thus $x^7 = 1$, and $x^i \neq 1$ for $0 < i < 7$.
For $k = 2$ we can take

$$y = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix},$$

so that $y^3 = 1$ and

$$yx = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = x^2 y.$$

Similarly, for $k = 4$ we can take

$$y = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus you have shown that a group of order 21 is either isomorphic to $\mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{21}$, or to T. By our earlier study of groups of order 9 and 15, we see that T is the smallest non-Abelian group of odd order.

2. Consider $\mathbb{Z}_2$ as a field with elements $\{0, 1\}$. Let G be the group of 3×3 upper triangular matrices with entries in $\mathbb{Z}_2$:

$$\begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix},$$

with implied zeroes below the diagonal.

(a) For each of the eight elements $g \in G$, compute g^2. Circle the elements of order 2, and put a box around the elements of order 4.
Solution:

$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \qquad \boxed{\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}}^2 = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \qquad \boxed{\begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}}^2 = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

(b) We have seen that there are two non-Abelian groups of order 8, up to isomorphism: the dihedral group D_4 and the quaternion group Q. Show that our group $G \not\cong Q$. (So we must have $G \cong D_4$.)

Solution: In the quaternion group, there are six elements of order 4: $\pm i$, $\pm j$, and $\pm k$. In our group G there are only two elements of order 4.

(c) Choose an element $r \in G$ of order 4, and an element $s \in G$ of order 2 that is different from r^2. Verify that $rs = sr^3$.

Solution: I will take

$$r = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \qquad\qquad s = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix},$$

but of course there is another choice for r and three other choices for s. Then r^3 must be the other element of order 4, and we have

$$\begin{aligned} rs = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix} = sr^3. \end{aligned}$$

(d) Let G act on the set of column vectors $(\mathbb{Z}_2)^3$ by left multiplication. The orbit of $\left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right)$ has four elements. Write them in a square, so that r acts as a clockwise rotation. Does s act on this square by reflection left-to-right, top-to-bottom, or diagonally?

Solution: The answer depends on your choice of r and s. For me, the square is

$$\begin{tikzcd} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \arrow[r, dash] \arrow[d, dash] & \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \arrow[d, dash] \\ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \arrow[r, dash] & \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \end{tikzcd}$$

and s acts by reflection across the diagonal of negative slope, that is, it switches the top right and bottom left.

I wanted to include the following problem, but the exam was getting too long. Of course I would have broken it into many parts.

3. In lecture we showed that the alternating group A_n has no non-trivial normal subgroups for $n \geq 5$. Use this to show that the only non-trivial normal subgroup of S_n is A_n, again for $n \geq 5$.

   Solution: Let $N \subset S_n$ be a normal subgroup. Then $N \cap A_n$ is normal in A_n, by homework 6 problem 3(e). Thus $N \cap A_n = \{1\}$, or $N \cap A_n = A_n$, that is, $A_n \subset N$.

   If $A_n \subset N$ then $|A_n|$ divides $|N|$, which divides $|S_n|$; since $|S_n|/|A_n| = 2$, we see that either $|N| = |A_n|$, so $N = A_n$, or $|N| = |S_n|$, so $N = S_n$.

   If $A_n \cap N = \{1\}$ then the sign homomorphism : $S_n \to \mathbb{Z}_2$ is injective on N: if we had $\text{sign}(\sigma) = +1$ for some $\sigma \in N$ then $\sigma \in A_n$, so $\sigma \in A_n \cap N$, so $\sigma = 1$. Thus $|N| \leq 2$. If $|N| = 1$ then we are done. If $|N| = 2$ then the non-trivial element of N must be a product of disjoint transpositions; but this has many conjugates, so N would not be normal.