Solutions to Midterm

1. (*35 points*) Let G be a group of order $5 \cdot 7 \cdot 47$.

   (1) Prove that G has a unique p-Sylow subgroup for each prime p dividing its order.

   Proof. For $p = 5, 7, 47$ let n_p be the number of p-Sylow subgroups. Then $n_p \equiv 1 \pmod p$ and $n_p | \frac{5\cdot 7\cdot 47}{p}$.

   For $p = 5$ the possibilities are $n_5 = 1, 7, 47, 7 \cdot 47$. Since $7 \equiv 2 \pmod 5$ and $47 \equiv 2 \pmod 5$ it follows that $7 \cdot 47 \equiv 4 \pmod 5$ and so only 1 satisfies the condition of being congruent to 1 modulo 5.

   For $p = 7$ the possibilities are $n_7 = 1, 5, 47, 5 \cdot 47$. Since $47 \equiv 5 \pmod 7$ it follows that $5 \cdot 47 \equiv 25 \equiv 4 \pmod 7$ and so only 1 satisfies the condition of being congruent to 1 modulo 7.

   For $p = 47$ the possibilities are $n_5 = 1, 5, 7, 5 \cdot 7$. Since $5, 7, 35$ are smaller than 47 only 1 satisfies the condition of being congruent to 1 modulo 47.

   We conclude that $n_5 = n_7 = n_{47} = 1$. So each p-Sylow is unique, hence normal. $\square$

   (2) Prove that G is abelian.

   Proof. Let A, B, C be, respectively, the unique 5, 7, 47 Sylow subgroup. We have that A, B, C are all normal in G. It follows that AB is a normal subgroup of G (as we proved in class). Then, $|(AB)C| = |AB| \cdot |C|/|(AB) \cap C| = |A| \cdot |B| \cdot |C|/(|(AB) \cap C| \cdot |A \cap B|)$.

   Now, the order of $A \cap B$ divides the order of A and of B and so must be one. Thus, the order of AB is $5 \cdot 7$. The order of $(AB) \cap C$ similarly divides 35 and 47 and so must be one. We conclude that $|ABC| = |G|$ and hence every element in G has the form abc with $a \in A, b \in B, c \in C$. Since A, B, C are of prime order they are cyclic and so abelian. It is therefore enough to prove that the elements of A commute with the elements of B and of C, and that the elements of B commute with the elements of C. This follows from the following statement.

   Let G be a finite group and P, Q two normal Sylow subgroups belonging to different primes. Then the elements of P and Q commute. Indeed, $P \cap Q$ must be the trivial group, by the same arguments as above. On the other hand, if $x \in P, y \in Q$ then $(xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in P \cap Q$ because P, Q are normal. It follows that $[x, y] = 1$ and so x and y commute.

   $\square$

2. (*30 points*) Let $\mathbb{F}_p$ be the field of p elements. Let the group S_3 act on $\mathbb{F}_p^3$ by

$$\sigma(x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

(it is the action taking the standard basis vector e_i to $e_{\sigma(i)}$). Let V the subspace of $\mathbb{F}_p^3$ consisting of vectors (x_1, x_2, x_3) such that $x_1 + x_2 + x_3 = 0$. Then S_3 acts on V by the same formula.

Calculate the number of orbits of S_3 in V. (Remark: the case $p = 3$ may require special attention.)

Solution. By the Cauchy-Frobenius formula we have

$$N = \frac{1}{6} \sum_{\sigma \in S_3} I(\sigma),$$

where N is the number of orbits, $I(\sigma)$ is the number of elements in V that σ fixes and where we have used $6 = |S_3|$.

Let $\sigma = 1$. Then σ fixes every element of V. Since for any choice of $x_1, x_2 \in \mathbb{F}_p$ there is a unique x_3 such that $(x_1, x_2, x_3) \in V$, the number of elements of V is p^2 and so $I(1) = p^2$.

Let $\sigma = (12)$. Then σ fixes (x_1, x_2, x_3) if and only if $x_1 = x_2$. The number of vectors of the form (x, x, y) that are in V is p (choose any x and let $y = -2x$). Thus, $I((12)) = p$. In the same way, for any transposition σ we have $I(\sigma) = p$.

Let $\sigma = (123)$ or (132). Then σ fixes (x_1, x_2, x_3) if and only if $x_1 = x_2 = x_3$. If (x, x, x) is in V then $3x = 0$. This implies for $p \neq 3$ that $x = 0$ and so σ fixes only the vector $(0, 0, 0)$; for $p = 3$ any x is possible and so σ fixes 3 vectors (choose $x = 0, 1, 2$).

Put together we get that

$$N = \frac{1}{6}(p^2 + 3 \times p + 2 \times 1) = \frac{(p+1)(p+2)}{6}, \qquad p \neq 3,$$

and

$$N = \frac{1}{6}(p^2 + 3 \times p + 2 \times 3) = \frac{24}{6} = 4, \qquad p = 3.$$

3. (*35 points*) Let G be a group of order p^n, where p is a prime and n is a positive integer.

   (1) Prove that the center $Z(G)$ of G is not trivial.

   Proof. Repeat the proof given in class. One did not need to prove the class equation. □

   (2) If $n = 3$ (so G is a group of order p^3), what are the possibilities for the order of $Z(G)$?
   Solution. We proved that $G/Z(G)$ cannot be a non-trivial cyclic group. If the order of $Z(G) = p^2$ then $G/Z(G)$ is of order p, hence cyclic and we get a contradiction. Using the first part of the question we get that $|Z(G)| = p, p^3$. The last case happens if and only if $G = Z(G)$, namely, if and only if G is abelian. Since we proved in class and assignments that there are always abelian and non-abelian groups of order p^3, indeed both possibilities occur.