MATH 403 Winter 2018
Homework I
Winter 2018

(Problem Set 1)

Problem 1.1. (Goodman 10.1.1) Let us prove the following statement: If G is a simple group of order p^n then $n = 1$ and G is $\mathbf{Z}/p$. If G is abelian and $n > 1$, one uses the structure theorem on finitely generated abelian groups to construct explicitly a proper , non-trivial subgroup of G. If G is not abelian, we have $Z(G) \neq G$. Recall the class equation for a finite group G. If $Z(G)$ is the center and g_i for $i = 1, \cdots, r$ are elements in the conjugacy classes disjoint from $Z(G)$, we have the counting

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

where $C_G(g_i)$ denotes the centralizer of g_i. Then $p|Z(G)|$. But $e \in Z(G)$ so $|Z(G)|$ can be divided by a power l of p where $l > 0$. This means $|Z(G)| > 1$ so that $e \neq Z(G)$. If $n > 1$ since we assumed G is not abelian we have

$$e \subsetneq Z(G) \subsetneq G$$

, with $Z(G)$ a proper nontrivial normal sub-group of G. This contradicts the assumption that G is simple. Hence $n = 1$. The only group of order p has to be cyclic.

We now proceed to the problem. When G is abelian, we know there is a composition series of G with successive quotients equal to $\mathbf{Z}/p$. When G is not abelian, n is necessarily greater than 1. By theorem, there is always for a finite group G a composition series. The successive quotients have to be simple and of order p^k. But we proved that any simple group of order p^k is cyclic of order p.

For part b, this follows from the arguments presented in a.

Problem 1.3. (Goodman 10.1.3) Suppose G has a chain of subgroups with abelian successive quotients. Then apply problem 1.b to the quotient groups G_i/G_{i-1}. Then the chain can be refined to a composition series. For this, you might want to review the correspondence: If G is a group and $H \subset G$ is a normal subgroup, every normal subgroup in G/H can be written uniquely as N/H where N is a normal subgroup of G containing H. You also have to know the third isomorphism theorem which symbolically says in the previous setting, we have

$$\frac{G/H}{N/H} \simeq G/N.$$

Problem 1.7. (Goodman 10.3.4)

1. Let $\sigma \in A_4$ be a non-trivial element. Then there exists a pair $i \neq j$ such that $\sigma(i) = j$. Since we are in A_4, one chooses pairwise distinct i, j, k, l. Now $\tau = (jkl) \in A_4$ and

   $$\sigma\tau(i) = \sigma(i) = j$$

   and

   $$\tau\sigma(i) = \tau(l) = i.$$

   Hence σ is not in the center of A_4.

2. This follows from the above argument.

3. A_n is of index 2 in S_n. Hence A_n is normal in S_n. By exercise 10.3.3, $Z(A_n)$ is normal in S_n. By theorem 10.3.2, $Z(A_n)$ is either A_n or e.

Problem 1.8. (Goodman 10.3.6) Since G is simple, $e \subset G$ is composition series. By Jordan Hölder theorem, if G has a solvable series, $G/e \simeq G$ has to be abelian. Theorem 10.3.4 tells us that A_n is simple. We have seen that A_n is not abelian as well. Hence A_n is not solvable. As subgroups of a solvable group is solvable, S_n is not solvable.

Problem 1.9. Let p be an odd prime. Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in the center of $SL_2(\mathbf{Z}/p)$. Consider the matrices
$B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $C = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Solving for $BAB = A$ and $CAC = A$ gives us $b = c = 0$ and $a = d$ with $a^2 = 1$.

Problem 1.10. For $|GL_2(\mathbf{Z}/p)|$, note that the first row of a matrix A in $GL_2(\mathbf{Z}/p)$ can be anything but the zero vector. So there are $p^2 - 1$ choices for the first row. Check that $\det A = 0$ is equivalent to the condition that the secod row of A is a multiple of the first. So the second row only has $p^2 - p$ choices. Hence

$$|GL_2(\mathbf{Z}/p)| = (p^2 - 1) \cdot (p^2 - p).$$

For $|SL_2(\mathbf{Z}/p)|$, the first row for $A \in SL_2(\mathbf{Z}/p)$ can have $p^2 - 1$ choices. Since $\det A = 1$, if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we have

$$ad - bc = 1.$$

For a fix row a, b, suppose $a \neq 0$. Then a has a multiplicative inverse. Then $d = a^{-1}(1 + bc)$. As b runs through the entire $\mathbf{Z}/p$, we see that the second row c, d has p choices. Hence

$$|SL_2(\mathbf{Z}/p)| = (p^2 - 1) \cdot p.$$

Finally,

$$|PSL_2(\mathbf{Z}/p)| = |SL_2(\mathbf{Z}/p)|/|Z| = (p^2 - 1) \cdot p/2.$$