Homework 6

31. Let G be a group and let M be the intersection of all subgroups of G of finite index. Then note that for any $g \in G$,

$$M = \bigcap_{\substack{H \subset G \\ [G:H] < \infty}} H = \bigcap_{\substack{H \subset G \\ [G:H] < \infty}} gHg^{-1} = gMg^{-1},$$

since conjugation by g is a bijection on the subgroups of G of finite index.

32. a. Let σ and τ be elements of S_n with disjoint support. Suppose $j \in \text{supp}(\sigma)$. Then $\sigma(\tau(j)) = \sigma(j)$, and $\tau(\sigma(j)) = \sigma(j)$, since $\sigma(j) \in \text{supp}(\sigma)$. Likewise for $j \in \text{supp}(\tau)$. If j is in the support of neither, then $\sigma(\tau(j)) = \tau(\sigma(j)) = j$. So $\sigma\tau = \tau\sigma$.

This implication cannot be reversed. Let $\sigma = \tau = (1\ 2)$. Then $\sigma\tau = \tau\sigma = e$, but their supports coincide.

b. Let $\sigma \in S_n$ be a permutation of $[n]$. Then the subgroup $\langle\sigma\rangle$ acts on the set $[n]$, and splits it up into disjoint orbits. Let $\{a_1, a_2, \ldots, a_r\}$ be one of these orbits. Then we can express the action of σ on this set by

$$\sigma = (a_i, \sigma(a_i), \sigma^2(a_i), \ldots, \sigma^{n-1}(a_i))$$

for any $i \in \{1, 2, \ldots, r\}$, since a_i is sent to some $a_j = \sigma(a_i)$, and a_j is sent to some $a_k = \sigma(a_j) = \sigma^2(a_i)$, etc, until we arrive back to a_i. Then we have shown that the action of σ on each of the elements of the orbit can be represented in cycle notation.

Then its action on all of $[n]$ will be represented as a product of each of these disjoint cycles, using the result from part (a.).

For the case of $\text{Sym}(\mathbb{N})$, it is possible that the orbits are not finite, and thus cannot be represented as cycles.

c. Let $\sigma \in S_n$, and write $\sigma = \sigma_1 \cdot \sigma_2 \cdots \sigma_m$ a product of cycles with disjoint support. By part (a.),

$$\sigma^a = \sigma_1^a \cdot \sigma_2^a \cdots \sigma_m^a.$$

Each a_i has order its length. Then if ℓ is the least common multiple of the lengths of each a_i, we have

$$\sigma^\ell = \sigma_1^\ell \cdot \sigma_2^\ell \cdots \sigma_m^\ell = e.$$

Moreover, ℓ is by definition the smallest integer where this occurrs.

d. The greatest order of an element of S_6 is when we have a two and a three cycle, and its order is six. The greatest order of a permutation in S_{10} is when there is a two, three, and five cycle, since each of these are relatively prime. Its order is 30.

e. Let σ be a permutation of cycle type $1^{a_1}2^{a_2}\cdots n^{a_n}$. Its conjugacy class is all elements with this cycle type. Then we need to calculate how many such permutations there are.

We immediately know there will be $n - a_1$ fixed points. For the entries which are not fixed, there will be $n!/a_1!$ choices, where $0! = 1$, and then we must divide by the order of each of the cycles, since a cycle of length r has r ways to represent the same cycle. Then there are

$$\frac{n!}{\left(\prod_{a_i > 0} a_i\right) a_1!}$$

elements in the conjugacy class of λ.

The order of the conjugacy class is the order of the orbit $S_n \cdot \lambda$ of λ under conjugation by S_n. Since S_n is a finite group, we have

$$|S_n \cdot \lambda| = [S_n : (S_n)_\lambda] = |S_n|/|(S_n)_\lambda|,$$

where $(S_n)_\lambda$ is the stabilizer of λ. Then

$$|(S_n)_\lambda| = |S_n|/|S_n \cdot \lambda| = n! \frac{\left(\prod_{a_i>0} a_i\right) a_1!}{n!} = \left(\prod_{a_i>0} a_i\right) a_1!.$$

33. Let p be a prime and consider the group of matrices

$$U := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z}_p \right\}.$$

First we must show that U is a subgroup of $GL(3, \mathbb{Z}_p)$ and that it has order p^3. First note that U is contained in $GL(3, \mathbb{Z}_p)$ since element indeed has determinate 1.

Next we will write the product of two elements in U:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus, U is closed under multiplication. Moreover, we can solve this system to see that the inverse of the leftmost matrix is the matrix in U given by

$$\begin{bmatrix} 1 & -a & b-ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}.$$

Then since U clearly contains the identity, it is a subgroup of $GL(3, \mathbb{Z}_p)$. Moreover, there are p^3 choices of a, b, and c, so that $|U| = p^3$.

Now we will show that for $p \geq 3$, every non-identity element of U has order p. From the calculation above, we see that

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^r = \begin{bmatrix} 1 & ra & rb + \sum_{i \leq r} iac \\ 0 & 1 & rc \\ 0 & 0 & 1 \end{bmatrix}.$$

For primes p greater than 2, the sum of itegers less than or equal to p is $p\left(\frac{p+1}{2}\right)$, which is divisible by p. Then for any matrix α with either a, b, or c nonzero, the smallest power of α which is the identity is p, since any of its entries are relatively prime with p.

For the case when $p = 2$, the sum of integers not greater than 2 is odd, because 2 is the only even prime. Thus there are two elements of order 4, both with a and c equal to 1.

The center of U contains all elements which commute with every element of U. For the two arbitrary matrices in the above calculation, we see that they will only commute when $af = cd$. Thus in order for an element of U to commute with all other elements, it must be of the form $\left[\begin{smallmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$. Thus the center has order p.

Given the above calculation, there is a homomorphism φ from U to $\mathbb{Z}_p \oplus \mathbb{Z}_p$, where

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mapsto (a, c).$$

The kernel of φ is exactly the center of U. Then by the first isomorphism theorem, $U/Z(U) \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$.

When $p = 2$, there are 8 elements in U. One is the identity, five have order 2, and two have order 4. Then U is isomorphic to the group D_8 of permutations of the square, where the order 4 elements are the rotations by 90 degrees.

34. Let S_n be the symmetric group for $n \neq 6$. We will show that there are only inner automorphisms.

We are given that any automorphism induces a permutation on the conjugacy classes of S_n. Moreover, since automorphisms are bijecions, a conjugacy class may only be mapped to another if it has the same number of elements as the first. Note that every inner automorphism induces the identity permutation on the conjugacy classes, since it sends elements of one cycle type to another element of the same cycle type.

First, consider the set of involutions in S_n, which are permutations of order 2. I claim that a cycle of type 2^k has order

$$\frac{n!}{2^k(n-2k)!k!},$$

for $2k < n$. Then there are $\frac{n(n-1)}{2}$ 2-cycles. If $n - 2k > 1$ and $k > 1$, there are at least 2 choices for elements not in the cycles. Each pair of elements leaves the rest of the elements to be placed into cycles, of which there are at least two possible choices since $k > 1$. This means there are more than $n(n-1)/2$ possible k cycles, and thus the 2 cycles cannot be sent to these k cycles by an automorphism.

For the case when $0 \leq n - 2k \leq 1$, we can calculate that there will be

$$\frac{n!}{2^k k!}$$

elements of cycle type 2^k. Comparing this to the number of 2-cycles, in order for their sizes to be equal we must have

$$\frac{n!}{2^k k!} = \frac{n(n-1)}{2}.$$

But for $n \leq 5$, we can clearly see this is false, and for $n \geq 7$, the right side is larger and increases faster. In the case of $n = 6$ and $k = 3$, we have equality. This is the special case.

Then when $n \neq 6$, we know that every 2 cycle is sent to another 2 cycle. We can use this to show that every conjugacy class is mapped to itself by any automorphism. We can always write an n cycle as a combination of overlapping 2 cycles. For example, consider

$$(1\ 2\ 3) = (1\ 2)(2\ 3).$$

For any automorphism σ, we have $\sigma((1\ 2)(2\ 3)) = \sigma((1\ 2))\sigma((2\ 3))$. Here, $\sigma((1\ 2))\sigma((2\ 3))$ must be an element of order 3, and we know each 2 cycle is mapped to another 2-cycle. Then $\sigma((1\ 2))\sigma((2\ 3)) = (h\ i)(j\ k)$ for some h, i, j, k, and moreover that two of these values are equal, say $i = j$, since if the resulting 2-cycles don't overlap, we wont get an element of order 3. Then this applies to arbitrary n-cycles, showing that σ maps n-cycles to n cycles, and thus sends each conjugacy class to itself.

Now all that is left to show is that an automorphism which preserves each conjugacy class is inner. I could not finish.

For the case $n = 6$, there is an automorphism which sends the set of 2-cycles to the set of 2^3-cycles, and thus is not an inner automorphism.

35. We will find all of the 2-sylow subgroups of S_4. These will have order 8.

Let $\square$ be a square and choose some labelling for its edges:

$$\begin{array}{ccc} 1 & \text{——} & 2 \\ | & & | \\ 4 & \text{——} & 3 \end{array} \tag{1}$$

Then the permutations of this square are elements of S_4, and they form a subgroup of 8 elements. Call this P_1.

Moreover, each of the other 2-sylow subgroups will be conjugates of this one. Then these will be subgroups acting on a square $\sigma(\square)$

$$\begin{array}{ccc} \sigma(1) & \text{——} & \sigma(2) \\ | & & | \\ \sigma(4) & \text{——} & \sigma(3) \end{array} \tag{2}$$

for some $\sigma \in S_4$. Each different labelling generates a subgroup of S_4, but some are the same. For any $\sigma \in P_1$, the subgroup acting on $\sigma(\square)$ is just P_1.

Using sylow theorems, we know that the number of 2-sylow subgroups must divide 3 and equal 1 modulo 2. Then there are either 1 or 3 2-sylow subgroups.

If we consider $\sigma = (12)$, we get a different subgroup P_2 of S_4 which acts on $\sigma(\square)$. The group P_1 contains the cycle (1234) which is not in P_2, while P_2 has the cycle (2134) which is not in P_1.

The same is true for $\sigma = (23)$. Then these are the three 2-sylow subgroups of S_4, each isomorphic to D_8.

36. Let p and q be prime numbers and suppose G is a group of order p^2q. We will show that G has a normal subgroup and that G is solvable.

First consider the p-sylow subgroup. There will be $n_p = 1 \mod p$ many of these groups, and we know that n_p divides q.

(Case 1:) If $p \geq q$, we may only have $n_p = 1$, since $p + 1 > q$. Then the p-sylow subgroup is normal.

(Case 2:) If $p < q$, it is possible that there are more than one p-sylow subgroups.

Consider the q-sylow subgroup. We have $n_q = 1 \mod q$ and n_q divides p^2. Then the only options for n_q are $1, p$, and p^2. If $n_q = 1$ we are done. We cannot have $n_q = p$ because this would mean $p = 1 \mod q$, which is a contradiction as $p < q$.

If $n_q = p^2$, then we have $p^2 = 1 \mod q$, and q must divide $p^2 - 1 = (p + 1)(p - 1)$. Then q must divide either $p + 1$ or $p - 1$ since it is prime. But $p < q$, so we must have $q = p + 1$. This is only possible when $p = 2$, $q = 3$.

Then we can handle this case specifically. n_3 must divide 4, so it is either 1 or 4. If $n_3 = 1$, we are done.

If $n_3 = 4$, this means G has e, eight elements of order three from the four 3-sylow subgroups, and there is only room for three more elements. Then there cannot be more than one 2-sylow subgroup, as each of these has three elements of order four. Then the 2-sylow subgroup is normal.

Now we show G is solvable. We know either subgroup can be normal. Suppose first that the p-sylow subgroup is normal and call it P. From Lang, we know that P is solvable since it is a p-group. We also know G/P is solvable since it is order q. Then G is solvable, by theorem 3.2 in Lang.

If the q subgroup Q is normal, we know that Q and G/Q are both solvable since G/Q is a p-group. Then again by theorem 3.2, G is solvable.