Goals

- Investigate consequences of the class equation
- Recognize how and when to apply results from the Class Equation
- Recall and deduce some basic consequences of Sylow's Theorems
- Apply Sylow's Theorem to new contexts to classify certain groups

Introduction

Much of finite group theory has a combinatorial flavor to it, and we exhibit more of that in this section. Namely, we recall the so called Class Equation, and we work through some elementary, yet powerful consequences of it. For example, for an infinite family of groups we can say exactly how many elements commute in each group. We can then turn to one of the most important topics in finite group theory; the so called Sylow Theorems. These give a weakened converse to LaGrange's Theorem, and are the most essential tool we will use in unwinding the structure of finite groups.

1 The Class Equation

Throughout this class we have made use of Equivalence Relations. In the very first week, we saw that the definition of cosets defined an equivalence relation, and we used the corresponding partition to deduce LaGrange's Thrm. Last week, we defined an equivalence relation on bijective functions to show that every permutation can be written as a disjoint union of cycles. The equivalence relation we are now interested in is conjugation. Let us recall it for completion.

1. Define a relation on our group G by $a \sim b \iff a = gbg^{-1}$ for some g
2. In class you showed that this actually gives an Equivalence relation: The only tricky part is transitive. Prove that again here. (Hint: remember that $(xy)^{-1} = y^{-1}x^{-1}$)
   Solution: Indeed suppose $a = g_1bg_1^{-1}$ and $b = g_2cg_2^{-1}$ for some $g_1, g_2 \in G$. Then we can substitute b into the equation with a to get $a = g_1(g_2cg_2^{-1})g_1^{-1} = (g_1g_2)c(g_1g_2)^{-1}$.

3. Great, so we have a new equivalence relation to play with- and with that a new partition of our space! Let us denote $C(a)$ as the equivalence class of a under this relation. In this case, we call this equivalence class the "**Conjugacy Class of a**" As a set we have $C(a) = \{b \in G : a = gbg^{-1}$ for some g $\in G\}$. Then we get that $G = \bigsqcup C(a)$ (that is, G is a disjoint union of these equivalence classes). So our immediate task is simplifying this partition so we can get some useful information out of it.

   (a) Does this partition actually tell us anything new if G is an abelian group?
   Solution: Notice that if G is abelian, the conjugacy class for any element is just the element itself. Indeed $gag^{-1} = agg^{-1} = a$ for all g in G. Thus this partition just says G is the union of all its elements, which is trivial.

   (b) More generally, let $a \in Z(G)$. What is $C(a)$?
   Solution: The same logic above applies here: if a commutes with anything than conjugation to it is trivial. Thus, for $a \in Z(G)$ we have $C(a) = \{a\}$

Now you also showed in class that in general, the size of the conjugacy class of a is precisely the index of the centralizer, that is $|C(a)| = [G : N(a)]$. Then using the above two problems, we can group together those elements in the center, and then take orders of both sides to get the Class Equation

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : N(a)]$$

Let us see why this is so useful!

1. In the previous worksheet we worked through how to show that every group of order p^2, where p is prime, is abelian. So at this point we have

$$|G| = p \implies \text{ G is cyclic}$$
$$|G| = p^2 \implies \text{ G is abelian}$$

   So a natural guess would be that a group of order p^n is abelian for ANY n. However, we saw that failed last worksheet with a simple example of a group of order 8. However- the truth is not much removed from that guess.

2. We saw in class that the Class Equation implies that a group of order p^n has a non-trivial center! This is immensely useful as we will see later in the course- it shows that while p-groups aren't in general Abelian, they are one of the next best thing (so called solvable).

   (a) One might not think this result is so impressive. However, it is definitly not a claim that can be made about other Groups. For example,

i. Show that S_3 has a trivial center.
Solution: Note that $\sigma \in Z(S_3) \iff \gamma\sigma\gamma^{-1} = \sigma$ for any choice of permutation γ. Assume that $\sigma \neq id$. Then $\sigma(i) \neq i$ for some i $\in \{1, 2, 3\}$. Cook up a permutation that can't commute with this sigma, then explain why that shows $Z(G) = e$.

ii. In fact show that S_n for $n \geq 3$ has a trivial center!
Solution: Exact same argument as above! Let me know if you want to go over your attempt of a proof!

(b) Moreover, we can use the fact that the center has more than 1 element in many cases to say exactly how many elements it has.

i. Let G be a non-Abelian group of order 7^3. Then we claim exactly 7 elements commute with every element in G.
Solution: By the class Equation we know $|Z(G)| > 1$ so by LaGrange's Thrm we have $|Z(G)| \in \{7, 7^2, 7^3\}$. However, we are assuming G is non-Abelian, so the center cannot be all of G, hence $|Z(G)| \neq 7^3$. Now I claim that if $|Z(G)| = 7^2$ then G would actually be Abelian, a contradiction. Prove this claim and show why that finishes the proof. (Hint: How did we prove that all groups of order p^2 must be Abelian?)
If $|Z(G)| = 7^2$ then G/Z(G) would be cyclic (since it is of order 7, a prime number). Yet we showed before that if G/Z(G) is cyclic then G is abelian, a contradiction.

ii. How many elements commute with every element in a Non-Abelian group of order $357,911 = 71^3$?
Solution: Exact same logic above applies here. 71 is a prime number, so this group has nontrivial center, so it is of order $|Z(G)| \in \{71, 71^2, 71^3\}$. By the same reasoning as above, we can conclude it must be of order 71.

iii. For p a prime, find the size of the center for a non-Abelian group of order p^3.
Solution: It is of order exactly p.

Hopefully you can see that this is a rather powerful tool! If I asked you on week one to find how many elements commute in a group of order 357,911 I think you would quit the class!

3. Here is a good challenge problem that we will come back to later in the course hopefully. The content of this problem more or less shows every p-group is solvable (whatever that means)!

(a) Let G be a group of order 7^3. Then I claim there is a subgroup H_1 of order 7 and a subgroup H_2 of order 49 such that $H_1 \trianglelefteq H_2 \trianglelefteq G$
Proof: By Cauchy's Theorem there is a subgroup of order 7 in G, so let's call that subgroup H_1. If G is abelian, this subgroup is normal, and if G is non-abelian than problem 2 above shows that Z(G) has order 7- so either way we have a normal subgroup of order 7. Now let us consider the quotient group G/H_1. This is a group of order $49 = 7^2$ and thus also has a (normal) subgroup

$\overline{H}$ of order 7. By the Fourth Isomorphism Thrm (See worksheet 5) this subgroup is of the form $\overline{H} = H_2/H_1$ for some subgroup $H_2 \leqslant G$ containing H_1. Since $7 = |\overline{H}| = \frac{|H_2|}{|H_1|} = \frac{|H_2|}{7}$ we get that $|H_2| = 49$.

Finally, I claim that $H_2 \trianglelefteq G$ and $H_1 \trianglelefteq H_2$. I leave these parts to you (again use the 4th Iso Thrm and Problem 3.(c) in Cayle's Thrm Section of worksheet 6)
H_2 is of index 7 and is thus normal in G (since its index is the smallest prime dividing the order of G). Moreover, $H_1 \trianglelefteq G \implies H_1 \trianglelefteq H_2$ trivially.

(b) Let $G = 7^4$. Show there exists subgroups $H_1, H_2.H_3$ of order $7, 7^2, 7^3$ respectively such that $H_1 \trianglelefteq H_2 \trianglelefteq H_3 \trianglelefteq G$.
I will leave this mostly unsolved- come talk to me about it if you want to go over your attempt of a proof, I think it's a great exercise. You can do this in cases- if G is abelian, and if G is not abelian. If G is abelian you can prove it rather quickly (use the result from part a). If G is not abelian, use that Z(G) is non trivial, and again use part a.

(c) This is true more generally! State the more general claim for an arbitrary prime p, and positive integer n- and then prove it if you can!
Let G be a group of order $|G| = p^n$ for p a prime, $n \geq 2$. Show there exists a chain of subgroups $H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq G$ where $|H_i| = p^i$ and $H_{i-1} \trianglelefteq H_i$. You can prove this rather easily using induction and the results from part a and b. (Use the Lattice Isomorphism Thrm).

2 Sylow's Theorems

One of the first major Theorems we learned in this course was LaGrange's Theorem- which said the order of a subgroup divides the order of the group. We have made clear however that the converse does not hold- there might not be a subgroup of order n for all n that divide the order of G. However, we have made some partial results in that direction, as that last section shows. In particular, we have Cauchy's Theorem, which says that there is a subgroup of order p for each prime dividing the order of G. We also know that the converse for LaGrange's Thrm DOES hold for cyclic groups, and the Challenge problem above shows it also holds for p-groups. These results hint that we should pay special attention to subgroups of prime orders, and powers of prime order.

1. Rather than looking at just P-groups, we will be interested in p-subgroups of a given group G. In other words, G itself won't be a p-group, but we will be interested in studying subgroups inside G that are p-groups.
2. To this end, we want to group together all powers of p that divide the group G and

look at subgroups of that order. Let G be a group of order $p^\alpha m$ where $p \nmid m$ (that is, we have grouped together all powers of a given prime in the prime factorization of G). Then a subgroup of order p^α is called a "Sylow p-Subgroup of G"

Now, apriori, given a group G, we have no reason to expect that there is a subgroup of a given order sitting inside it. So you should be very skeptical of the definition given above: how do we know such a subgroup exists inside of G? It is a remarkable fact that such a subgroup always exists in a group- and moreover, we can say a lot about how many exist!

For completion I will state the theorem here, however, it makes more sense to focus on applications in this worksheet- so I won't mention anything about the proof of this theorem here, you will prove it in class! Let G be a group of order $p^\alpha m$ where $p \nmid m$ is prime not dividing m. Then

1. There exists (at least 1) Sylow p-subgroup
2. Any two Sylow p-subgroups are conjugate to one another. That is for two Sylow p-subgroups P_1, P_2 there exists a g such that $P_2 = gP_1g^{-1}$
3. Let n_p = the number of Sylow p-subgroups. Then $n_p \equiv 1$ (mod p) and we have $n_p = [G : N_G(P)]$ (ie n_p is the index of the normalizer of P for any Sylow subgroup P). In particular $n_p | m$

This is truly a remarkable theorem as we shall see. Using 1 and 2 of the theorem let us first prove a nice consequence: Let P be a Sylow p-Subgroup of G, then

1. If $n_p = 1$, then $P \trianglelefteq G$ (in words, if P is the unique Sylow p-subgroup, then it is normal).
   Proof: Note that conjugation is an automorphism. Finish the proof.
   Since conjugation is an automorphism, for any $g \in G$ gPg^{-1} is again a Sylow p-subgroup. Yet we are assuming that P is the only one, whence $gPg^{-1} = P$
2. If $P \trianglelefteq G$ then $n_p = 1$. Combining these two results shows this is an iff.
   Proof: Use part 2 of the theorem, and what it means to be normal to conclude that P is unique. Finish the proof.
   We have that if Q is a Sylow p-subgroup, then $Q = gPg^{-1}$ for some g. Yet P is normal, so $gPg^{-1} = P$, whence Q=P.
3. As an application of the above, show that if G is an abelian group, then for any prime p dividing the order of the group, the corresponding Sylow p-subgroup P is unique.
   We have that every subgroup in an abelian group is normal. Hence a Sylow p-subgroup P is normal in G, which by the above proves it is unique.

Okay great- so parts 1 and 2 of the theorem give a nice way of looking for normal subgroups! We just want to check if $n_p = 1$ or not! Now, in practice, how do we do that? This is where number 3 of the theorem comes into play- let us see the power of this by way of examples.

1. Let G be a group of order $|G| = 15 = 3 \times 5$. Then

   (a) Show there exists a normal subgroup of order 5.
   Proof: Let P_5 be a Sylow 5-subgroup, that exists by part 1 of Sylow's Theorem. Then we just want to show that $n_5 = 1$ (using the results above). Now part 3 of the theorem says that $n_5|3$ and $n_5 \equiv 1 \pmod 5$. Since 3 is prime the only options are that $n_5 = 1$ or $n_5 = 3$. However, 3 isn't congruent to 1 mod 5, so we get that $n_5 = 1$ showing that $P_5 \trianglelefteq G$.

   (b) Show that there exists a normal subgroup of order 3.
   Proof: Hint- Use Sylow's theorem like we did above. (Note that in this case, the order of G does divide the index of H factorial- so we really do need new tools to conclude that H is normal)
   We again will consider $n_3 =$ the number of Sylow 3-subgroups. Note by Sylow's 3rd thrm, $n_3|5$ and $n_3 \equiv 1$ mod 3. Combining these forces $n_3 = 1$ so the Sylow 3 subgroup is normal by the above results.

   (c) Since P_3, P_5 are of prime order they are cyclic- so let $\langle x \rangle = P_5, \langle y \rangle = P_3$ for some x, y. Show that $xy = yx$.
   Proof: Hint- we already showed this to some extent. Think about how we showed a subgroup of order p is contained in the center for a group of order p^2. Change the details accordingly for this context:
   Indeed $P_3 \trianglelefteq G, P_5 \trianglelefteq G$ and $P_3 \cap P_5 = e$ (by LaGrange's Thrm.) Thus by a previous HW elements from P_3 and P_5 commute.

   (d) Use this to show that G must be a cyclic group.
   Hint: Use the following fact- if $ab = ba$ then the order of ab divides the least common multiple of a and b.
   BY part c we get that elements from P_3, P_5 commute so we can apply the hint to the generators of P_3, P_5. Indeed, if we let x, y be generators for P_3, P_5 respectively (as in part c) then we can use the hint and the work we did in part c to get that $|xy| = 15$. That is $G = \langle xy \rangle$ is cyclic.

2. Let G be a group of order $|G| = pq$ for primes $p < q$ such that $p \nmid q - 1$. Show that G is cyclic.
   Proof: Solution: The exact same solution that we did above applies here. Show there are normal Sylow p and q subgroups that are cyclic because they are prime order. Then the product of their generators generate the whole group.

3. Challenge Problem:

(a) Let G be a group of order 12= $2^2 \times 3$. Then if G doesn't have a normal subgroup of order 3 show that $G \cong A_4$

Proof: We have that $n_3 \equiv 1 \pmod 3$ and $n_3|4$. Since we are assuming no Sylow 3-subgroup P is not normal, this forces $n_3 = 4$. Recall that $n_3 = [G : N_G(P)]$ yet also $[G : P] = 4$ so (since $P \leqslant N_G(P)$) we have $P = N_G(P)$. (Use the problem about how LaGrange's theorem is multiplicative from last worksheet if you don't buy that).

Finally, explain how the function defined last week $\psi : G \to A(G/P) \cong S_4$ and the lemma about normal subgroups contained in P from last week as well to conclude that ψ is injective. Explain why that finishes the proof.

Indeed, recall that we saw that $ker(\psi)$ is the largest normal subgroup contained in P. Yet P is of prime order, and so it has no nontrivial subgroups. Since we are assuming P itself is not normal, this forces $ker(\psi) = e$. Hence G is isomorphic to a subgroup of order 12 in S_4 (by the 1st Iso Thrm) and is thus isomorphic to A_4.

(b) More generally, assume G is a group of order $G = p^2q$ for $2 < p < q$. Show that G has a normal subgroup of order q.

Proof: We need to show that $n_q = 1$. Assume it is greater than 1, and get a contradiction.

Indeed we have that $n_q|p^2$ and $n_q \equiv 1 mod q$. Since we are assuming $q > p$ we must have that $n_q \in \{1, p^2\}$ (since there is no way q divides p-1). Assume for the sake of contradiction that $n_q = p^2$. Then we have that $q|p^2 - 1 = (p-1)(p+1)$. Now recall that q is a prime number, and that if a prime number divides a product of numbers, it must divide one of them. Hence $q|p-1$ or $q|p+1$. Yet we already remarked that q can't divide p-1 so q must divide p+1. Note however that $q > p \implies q \geq p+1$. Thus q=p+1 (since it divides it and is greater than or equal to it). Yet the only consecutive primes are 2 and 3, so this would force p=2, q=3. Yet we are assumming that $2 < p$ a contradiction. ■