Goals

- Build more intuition into the notion of Characteristic Subgroups
- Provide and investigate examples of characteristic subgroups
- Investigate Cayley's Theorem and other related theorems, and provide applications of said theorems.
- Familiarize ourselves with cycle notation for permutations.
- Investigate how to multiply said cycles and their relationship to the corresponding function composition.

Introduction

We begin this worksheet by briefly recalling our discussion of characteristic subgroups. We recall why we might want to investigate subgroups that are "stronger" than normal subgroups, and why the definition of Characteristic Subgroups are a very natural generalization of Normal Subgroups. Once we re-familiarize ourselves with characteristic subgroups, we change gears a bit to investigate the question of embedding our groups into Symmetric groups. We show that every group can be embedded into a symmetric group, and moreover, we can say some things about what that symmetric group looks like. This theorem is historically significant, and, moreover, provides us with some immediate, powerful corollaries. Since we have shown that every group embeds in some symmetric group, it is rather natural that we turn our attention back to symmetric groups at the end. We discuss ways of "decomposing" our bijective functions into more workable cycles, and give some examples of computations.

1 Characteristic Subgroups- The Sequel

Last week we investigated how much of the structure of the group G is reflected in the structure of the group G/N for some normal subgroup N. That discussion in part justified our focus on, and the special role we give to, normal subgroups. However, at the very end of last week we mentioned some shortcomings of normal subgroups: remember that "normality is not a transitive property" (meaning one can find subgroups H, K in G such that $H \trianglelefteq K \trianglelefteq G$ but H is not normal in G). This failure led us searching for a slightly stronger

notion of a subgroup than normal subgroups. Remember that an inner automorphism of G is the group automorphism $f_g : G \to G$ defined by $f_g(h) = ghg^{-1}$. With this notation, we can rephrase our definition of being a normal subgroup as $N \trianglelefteq G$ iff it is fixed by every inner automorphism. This rephrasing provides the best candidate for generalizing normal subgroups- rather than demanding our subgroup be fixed by $Inn(G) \leqslant Aut(G)$ we ask that our new class of subgroups be fixed by ALL automorphisms of G. These subgroups are called Characteristic Subgroups, and you showed in your homework last week that they are a "transitive property." Let us give some examples of characteristic subgroups

1. Recall that $Z(G) = \{x \in G : xy = yx \text{ for all } y \in G\}$ is the center of G. Then you were asked to show in your homework that the center is a characteristic subgroup of G.

2. Now time for an extremely important example. Let $x, y \in G$ be elements of some group G. Define the "commutator" of x and y as $[x, y] = x^{-1}y^{-1}xy$. This commutator provides some measure of how much x and y fail to commute. More precisely

   (a) Show that $xy = yx[x, y]$. In particular xy=yx iff $[x, y] = e_G$

   .....

   .....

   .....

   (b) Let $\sigma \in Aut(G)$ Show that $\sigma([x, y]) = [\sigma(x), \sigma(y)]$

   .....

   .....

   .....

   (c) Let $[G, G]$ denote the subgroup of G generated by all commutators $[x, y]$ for x,y in G. That is $[G, G] = \langle [x, y] : x, y \in G \rangle$. Use part b above to conclude that $[G, G]$ char G.

   .....

   .....

   .....

   (d) Show that $G/[G, G]$ is an abelian group.

   .....

   .....

   .....

   (e) Show that if $H \trianglelefteq G$ with G/H abelian, then $[G, G] \leqslant H$. This shows that $G/[G, G]$ is the largest abelian quotient we can form out of G. Conversely, if $[G, G] \leqslant H$ then we have $H \trianglelefteq G$ and G/H is abelian.

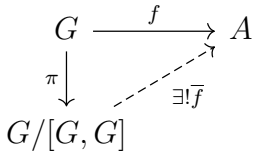
Solution: I will prove the converse for you because it is a great application of the 3rd and 4th isomorphism theorem from last week. Assume $[G,G] \leqslant H$. Now by part d above, we know $G/[G,G]$ is abelian, so all of its subgroups are normal. Since $[G,G] \leqslant H$, we have that $H/[G,G] \trianglelefteq G/[G,G]$. Again by the 4th iso thrm, we have that a subgroup is normal in the quotient group iff the corresponding subgroup is normal in G. Thus $H \trianglelefteq G$.
Now, since $G/[G,G]$ is abelian, all quotients of it are abelian too (see your last homework, or Worksheet 2). Thus $(G/[G,G])/(H/[G,G])$, is abelian. Finally, we note that $G/H \cong (G/[G,G])/(H/[G,G])$ finishing the proof.
Prove the other direction:

. . . . . .

. . . . . .

. . . . . .

(f) Challenge Problem: Suppose $f : G \to A$ is a group homomorphism into an abelian group A. Then show this group homomorphism can be uniquely factored through $G/[G,G]$ as follows,



That is there exists a unique $\overline{f} : G/[G,G] \to A$ such that $f = \overline{f} \circ \pi$. Hint- you will use number 3 on Page 8 of Worksheet 4. You must show that $[G,G] \leqslant ker(f)$ (use part e above, and the 1st isomorphism thrm)

. . . . . .

. . . . . .

. . . . . .

All together, these problems give us the "best possible" way to form an abelian group out of G. Part a shows that a commutator is a measure of how much certain items fail to commute. So if our group is already abelian $[x,y] = e_G$ for all elements x,y which implies our subgroup $[G,G] = \{e_G\}$. So in general, the commutator subgroup is collecting all the elements in our group G that do not commute- so when we quotient by it, we "kill off" all those elements, making the resulting quotient group abelian. The challenge problem states formally what I mean when I say $G/[G,G]$ is the 'best possible abelian quotient group out of G.' You can safely ignore that part if you wish.

2 Cayley's Theorem and Applications

Historically, groups were studied mostly as sets of permutations (ie, bijective functions). For example, the great French Mathematician Évariste Galois, who invented the absolutely beautiful branch of mathematics called "Galois Theory", studied the group of permutations of roots of polynomials to give a necessary and sufficient condition on a polynomial being "solvable by radicals" (the analogue to the quadratic equation for a general polynomial). The fact that groups were often studied concretely as permutations on some set is no accident, given the theorem you learned in class:

Cayleys Thrm: Let G be a group. Then there is a set S and an injective group homomorphism $\psi : G \hookrightarrow A(S)$. In particular, using the first isomorphism theorem, we can identify G with its image $G \cong \psi(G) \leqslant A(S)$.

Now in class you showed that the proof to the above theorem is constructive; meaning you explicitly state what the set S is (S=G) and what the function ψ is ($\psi(x) = l_x$, left multiplication by x).
The problem with this construction is that A(G) might be way to big to make this identification useful. So, in the same spirit as the above, we instead looked for a homomorphism $\pi : G \to A(S)$ into some other set S where we now don't require our map to be injective. Let $H \leqslant G$ and let G/H be the set of left cosets of H in G. Define $l_x : G/H \to G/H$ by $l_x(aH) = xaH$.

1. Show that this function is well defined. That is, if $a_1H = a_2H$ show that $l_x(a_1H) = l_x(a_2H)$

   .....
   .....
   .....

2. In class you then showed that the function $\psi : G \to A(G/H)$ defined by $\psi(g) = l_g$ is in fact

   (a) A group homomorphism
   (b) Where $ker(\psi) \trianglelefteq G$
   (c) And in fact $ker(\psi) \leqslant H$ is the largest normal subgroup contained in H. Therefore, if H has no normal subgroups contained in it, then the map $\psi : G \to A(G/H)$ gives an isomorphism $G \cong \psi(G) \leqslant A(G/H)$ where A(G/H) is much smaller than A(G).

Let us remark why that is important:

3. We have said a lot about why we would want a subgroup to be Normal, however we haven't made many sweeping claims about when we can actually know a normal subgroup exists for an arbitrary group. The above result gives a powerful way to look for normal subgroups of G!

   (a) Recall we defined the index of H in G to be $i(H) = \dfrac{o(G)}{o(H)}$, and remember that the order of the group $A(G/H)$ is o(A(G/H))=i(H)! (that is the index of H factorial). Now by Lagrange's theorem the order of any subgroup of A(G/H) must divide the o(A(G/H))=i(H)!. Thus, if $o(G) \nmid i(H)!$ then there can be no subgroup in A(G/H) isomorphic to G. Hence, the image $\psi(G) \leqslant A(G/H)$ cannot be isomorphic to G, so in other words, there is a non trivial kernal of ψ. This non-trivial kernal will be a non-trivial normal subgroup of G!

   (b) This looks rather mundane, but it is actually a rather nice tool that we will use over and over again. Here are some examples:

      i. Prove every group of order 25 has a normal subgroup of order 5.

      ii. Let G be a group of order p^2. **The point of this problem is to prove that G must be abelian.** Now if G is cyclic we are trivially done, so assume G is not cyclic.

         A. In your homework (and basically, in the problem above) you show that there exists a normal subgroup H of order p. Show $H = \langle x \rangle$ for some x in G.

         B. Now let $y \in G - H$ (that is, y is in G but not in H). Show that $\langle y \rangle$ is a normal subgroup of G.

         C. Find $\langle x \rangle \cap \langle y \rangle$

D. Use a previous HW problem to conclude that xy=yx. Since x is a generator for H and that y was arbitrary, conclude that yh=hy for all h in H so that $H \subseteq Z(G)$

. . . . . .

. . . . . .

. . . . . .

E. If $Z(G) = G$ then G is abelian so we are done. Therefore, for the sake of contradiction assume $Z(G) \subset G$ is a strict subset. Then conclude that H=Z(G)
(Hint: we have $H \subseteq Z(G)$ has order p. If Z(G) is a strict subset of G, what is its size?)

. . . . . .

. . . . . .

. . . . . .

F. Using the quotient group G/H, conclude that G is abelian.
(Hint: Look at Problem 2 on Pg 2 of Worksheet 5).

. . . . . .

. . . . . .

. . . . . .

iii. Is the same true for groups of order p^3. Or even more generally, are all groups of order p^n abelian for any n? Try to prove it or give a counter-example.

. . . . . .

. . . . . .

. . . . . .

(c) Recall that we previously showed that a subgroup of index 2 is normal in G. We can now generalize that. Let p be the smallest prime number that divides the order of the group G, and let $H \leqslant G$ have index p.

i. First, because we never explicitly mentioned this I believe, consider the following set up: Suppose $H_1 \leqslant G, H_2 \leqslant G$ are two subgroups and that $H_1 \subset H_2$. Show that Langrange's Thrm is multiplicative: That is show that $[G : H_1] = [G : H_2][H_2 : H_1]$ (where $([- : -]$ is the index of the smaller group in the larger group)

. . . . . .

. . . . . .

. . . . . .

ii. Now let H be the subgroup of index p as mentioned above, and consider the group homomorphism $\psi : G \to A(G/H)$ given by $\psi(g) = l_g$ as above. Show that $[G : K]$ divides $p!$ (p factorial- it's not just me being really excited)

(Hint- First isomorphism Thrm!!)

. . . . . .

. . . . . .

. . . . . .

iii. We know that $ker(\psi) = K \subseteq H$ from class so let $[H : K] = n$. Use the decomposition of $[G : K] = [G : H][H : K]$ given in part (i), and the result of part (ii) to conclude that n divides (p-1)!

. . . . . .

. . . . . .

. . . . . .

iv. By the minimality of p, conclude that n=1, and explain why that shows H is a normal subgroup of G.

. . . . . .

. . . . . .

. . . . . .

3 Cycle Decomposition of Permutation Groups

Let $S = \{1, 2, 3, 4, 5\}$ and consider the function $\psi \in A(S) = S_5$ given by

$$\psi(1) = 2$$
$$\psi(2) = 1$$
$$\psi(3) = 3$$
$$\psi(4) = 5$$
$$\psi(5) = 4$$

This is one function that sends each of the 5 elements to one of the 5 elements- however, notice that we can more or less break apart this function into different pieces. We have 1 goes to 2 and 2 goes back to 1; 3 is fixed, and 4 goes to 5 which goes back to 4. The idea is that we can view this one function ψ above as being more or less the combination of these three more simple functions.

Therefore, we can (as a means of notation) write this function as $\psi = (1, 2)(3)(4, 5)$, where (i,j) means i goes to j, and j goes to i. We call such a product a "cycle decomposition of ψ". It is common to not include the cycles of length one corresponding the the elements that are fixed by our function (in the case above, this is the cycle (3)). I won't do that at first to avoid confusion, but I will do that in the last example.

The intuition we should build is that any such bijective function can be broken down into

such a cycle decomposition, in such a way as we just did to ψ above. One just looks at what happens to each element and eventually one will come back to where we started. Our intuition in this case is correct, however, proving such a result actually is rather tricky it turns out! You will prove it in class, and the proof relies on defining another equivalence relation- so rather than rehash the proof here, I think it is worthwhile developing some practice on computing things with these cycle decompositions.

1. One huge piece of warning up front. Remember that if $A \xrightarrow{f} B \xrightarrow{g} C$ are two functions then Herstein writes the composite as fg and NOT the more common way of gf. This will be important below.

2. If we are going to express our functions as cycles like we did for ψ above, we are going to need to learn how to "multiply" these cycles together.

   (a) Consider $\psi \in S_5$ as above and let $\phi \in S_5$ be given by $\phi = (1,3,4)(2,5)$ written in cycle notation. Write out what this function actually is
   Solution: We have $\phi(1) = 3, \phi(2) = 5$ Fill in the rest.

   .....

   .....

   .....

   (b) Since $\psi, \phi \in S_5$ we can form their composite $\gamma = \psi\phi$ (where again this means $S \xrightarrow{\psi} S \xrightarrow{\phi} S$). Now we would like to be able to write the cycle decomposition of γ just from the cycles of ψ and ϕ. Indeed we can do so as follows:

      i. Write the cycles of $\psi\phi$ back to back. That is write (1,2)(3)(4,5)(1,3,4)(2,5). Now we want our cycles to be disjoint! That is, we don't want any number to appear in two different cycles- so we will read off this cycle product as follows: We read LEFT TO RIGHT (because of Herstein's function composition convention); in our case, we have that:

         A. 1 first goes to 2, then we look to the right to see if there are any mentions of 2 in the future cycles. In our case we have that 2 goes to 5. So for the product we get **1 goes to 5.** Now we repeat.

         B. The cycle on the far left says 2 goes to 1- looking to the right we get 1 goes to 3, **so 2 goes to 3.**

         C. Now we look at 3. 3 at first is fixed so we keep looking to the right and see that 3 goes to 4. There are no more 4's to the right so we get that **3 goes to 4.**

         D. Now 4 originally goes to 5 and looking to the right we get 5 goes to 2, so **4 goes to 2.**

         E. Finally 5 originally goes to 4 and looking to the right 4 goes to 1 so **5 goes to 1.**

Putting this all together, we get that multiplying our cycles in this way gives us the cycles decomposition (1,5)(2,3,4). The reason we do the cycle multiplication this way is because this cycle decomposition we get IS the cycle decomposition for the function composition.

A. Using your work from part a above, find what the function $\psi\phi$ is.
Solution. We have $\psi(1) = 2$ and $\phi(2) = 5$ so $\phi(\psi(1)) = 5$. Fill in the rest

. . . . . .

. . . . . .

. . . . . .

B. Find the cycle decomposition of the function $\psi\phi$ you computed above.

. . . . . .

. . . . . .

. . . . . .

C. Compare that cycle decomposition with the way we multiplied the cycles above. Check that they are the same.

. . . . . .

. . . . . .

. . . . . .

(c) This above result is of course true in general. It is a result that in my opinion just requires a lot of practice to get used to.

i. Let $\pi = (1, 2)(4, 9)$ and $\gamma = (1, 7)(2, 3, 9)$ be two elements of S_9. Write out explicitly what these functions are.

. . . . . .

. . . . . .

. . . . . .

ii. Find the cycle product of π and γ like we did above.

. . . . . .

. . . . . .

. . . . . .

iii. Find the function composite $\pi\gamma$ (Again, this means the composite $S \xrightarrow{\pi} S \xrightarrow{\gamma} S$ where S is some set of 9 elements).

. . . . . .

. . . . . .

. . . . . .

iv. Write the cycle decomposition of the function you found above. Compare to

part ii.

. . . . . .

. . . . . .

. . . . . .

(d) So we have learned how to multiply cycles and see that they correspond to the cycle we get from function composition. The only thing left to determine is how to read off the inverse of a function from its cycle. Let's do that by way of example.

i. Let $\psi = (1, 3, 2)(4) \in S_4$. This is the function

$$\begin{aligned} \psi(1) &= 3 \\ \psi(2) &= 1 \\ \psi(3) &= 2 \\ \psi(4) &= 4 \end{aligned}$$

Then the inverse of this function is given by

$$\begin{aligned} \psi^{-1}(1) &= 2 \\ \psi^{-1}(2) &= 3 \\ \psi^{-1}(3) &= 1 \\ \psi^{-1}(4) &= 4 \end{aligned}$$

Find the cycle decomposition of ψ^{-1} and compare it to the cycle decomposition of ψ

. . . . . .

. . . . . .

. . . . . .

ii. Let $\psi = (1, 3)(2, 4, 5) \in S_5$.

A. Find ψ^{-1}.

. . . . . .

. . . . . .

. . . . . .

B. Find the cycle decomposition of ψ^{-1} and compare it to the cycle decomposition of ψ

iii. With these two examples in mind, create a conjecture as to a formula for $(a_1, a_2, \ldots a_n)^{-1}$.

. . . . . .

. . . . . .

. . . . . .