Name: Adam Frank **November 22, 2020**

Math 637: Homework Chapter 3

1. (4.1.1)
   Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$. Deduce that if G acts transitively on A then the kernel of the action is $\bigcap_{g \in G} gG_ag^{-1}$.

   Proof. Let $x \in G_b$ so that x fixes b. Then $g^{-1}xg \cdot a = g^{-1}x \cdot b = g^{-1} \cdot b = a$. Hence $g^{-1}xg \in G_a$ which entails $x \in gG_ag^{-1}$.

   Now let $y \in G_a$ so that $gyg^{-1} \in gG_ag^{-1}$. Then $gyg^{-1} \cdot b = gy \cdot a = g \cdot a = b$ and so we have $gyg^{-1} \in G_b$. So we have shown that $G_b = gG_ag^{-1}$.

   Finally consider if the action is transitive on A and consider some $k \in G$ in the kernel of the action. Let $g \in G$ and let $b = g \cdot a$. Then $gG_ag^{-1} = G_b$ where $b = g \cdot a$. Since $k \in G_b$ for every b then we have

   $$k \in \bigcap_{g \in G} gG_ag^{-1}$$

   So interestingly, the requirement that the action is transitive is not needed to show that the kernel is contained in $\bigcap_{g \in G} gG_ag^{-1}$. Now for the reverse containment, suppose $k \in \bigcap_{g \in G} gG_ag^{-1}$, and let $b \in A$. Since the action is transitive we let $g^* \in G$ such that $g^* \cdot a = b$. Then $k \in g^*G_a(g^*)^{-1} = G_b$ and hence k fixes b. So $\bigcap_{g \in G} gG_ag^{-1}$ is contained in the kernel, and hence must be the kernel. □

2. (4.1.3)
   Assume G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and $a \in A$. Deduce that $|G| = |A|$.

   Proof. For any $a \in A$ and $\sigma \in G - \{\mathbb{1}\}$, we have $\sigma \notin \bigcap_{\tau \in G} \tau G_a \tau^{-1}$ and hence there must be some particular τ such that $\sigma \notin \tau G_a \tau^{-1} = G_a$. This last equation follows from the fact that G is abelian. But since this now tells us that σ does not fix a then we have the desired result.

   To see that $|G| = |A|$ we take an arbitrary $a \in A$ and prove that the function $f_a(g) = g \cdot a$ is a bijection. Because the action is transitive we already have that the function is surjective. Now if $f(g_1) = f(g_2) = g_1 \cdot a = g_2 \cdot a$ then we have $a = g_1^{-1}g_2 \cdot a$ which from the above entails $g_1^{-1}g_2 = \mathbb{1}$ and then $g_1 = g_2$. □

3. (4.1.10(a))
   Let H and K be subgroups of G. For each $x \in G$ define the HK double coset of x in G to be

   $$HxK = \{hxk | h \in H, k \in K\}$$

   Prove that HxK is the union of the left cosets $x_1K, \ldots, x_nK$ where $\{x_1K, \ldots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K.

Proof. To show that HxK is the union of $x_1K, \dots, x_nK$, let $hxk \in HxK$. We need to find some x_iK such that $hxk \in x_iK$. However, the $x_1K, \dots, x_nK$ is the orbit of H acting on xK by left multiplication, so $h \cdot xK = (hx)K = x_iK$ for some i, and so there are k' and k'' such that $hxk' = x_ik''$. Then

$$\begin{gathered} hx = x_ik''(k')^{-1} \implies \\ hxk = x_ik''(k')^{-1}k \in x_iK \end{gathered}$$

and we are done. □

4. (4.2.2)
   List the elements of S_3 as $1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)$ and label these with the integers 1, 2, 3, 4, 5, 6, respectively. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6.

   Calculation: To find the image of 1 we find the action of 1 on all of the group elements:

$$1 \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \end{pmatrix}$$

   or written with the given labels,

$$1 \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

   which is just the identity permutation. So $1 \mapsto 1$. Continuing likewise,

$$2 = (1\ 2) \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (1\ 2) & 1 & (1\ 2\ 3) & (1\ 3\ 2) & (2\ 3) & (1\ 3) \end{pmatrix} = (1\ 2)(3\ 5)(4\ 6)$$

$$3 = (2\ 3) \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (2\ 3) & (1\ 3\ 2) & 1 & (1\ 2\ 3) & (1\ 3) & (1\ 2) \end{pmatrix} = (1\ 3)(2\ 6)(4\ 5)$$

$$4 = (1\ 3) \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) & 1 & (1\ 2) & (2\ 3) \end{pmatrix} = (1\ 4)(2\ 5)(3\ 6)$$

$$5 = (1\ 2\ 3) \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (1\ 2\ 3) & (1\ 3) & (1\ 2) & (2\ 3) & (1\ 3\ 2) & 1 \end{pmatrix} = (1\ 5\ 6)(2\ 4\ 3)$$

$$6 = (1\ 3\ 2) \mapsto \begin{pmatrix} 1 & (1\ 2) & (2\ 3) & (1\ 3) & (1\ 2\ 3) & (1\ 3\ 2) \\ (1\ 3\ 2) & (2\ 3) & (1\ 3) & (1\ 2) & 1 & (1\ 2\ 3) \end{pmatrix} = (1\ 6\ 5)(2\ 3\ 4)$$

5. (4.2.8)
   Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Proof. Let G/H be the set of cosets of H, and define the group action on this G-set of left-multiplication,

$$g \cdot (g'H) = (gg')H$$

If we label the cosets $H_1, \ldots, H_n$ then we define the following homomorphism $\varphi : G \to S_n$. We map $\varphi(g) = \sigma$ where $\sigma(i) = j$ if according to the action, $g \cdot H_i = H_j$. As the kernel of a homomorphism, $\ker \varphi$ is a normal subgroup of G and is contained in H. So we take $K = \ker \varphi$. Moreover by the first isomorphism theorem, G/K is isomorphic to the image of φ which is a subgroup of S_n and therefore has order bounded by $n!$. Then $|G/K| = |G : K| \leq n!$.

□

6. (4.2.9)
   Prove that if p is prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$ then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

   Proof. p is the smallest prime dividing the order of the group, hence by corollary 5 the subgroup is normal.

   Now consider any non-identity element in a group of order p^2. It either generates the whole group or a subgroup of order p. If this element generates all of G then G is cyclic and hence abelian, so every subgroup is normal. And moreover, since G is cyclic, then for any divisor of the order of G there is a subgroup of order that divisor. So there is a normal subgroup of order p.

   On the other hand if the chosen element has order p then the subgroup it generates satisfies the conditions of the first claim in this exercise. Hence it is a normal subgroup of order p. □

7. (4.2.13)
   Prove that if $|G| = 2k$ where k is odd then G has a subgroup of index 2. [Use Cauchy's Theorem to produce an element of order 2 and then use the preceding two exercises.]

   Proof. By Cauchy's Theorem, since 2 is prime and divides $|G|$, then there must be an element of order 2. By the previous exercises, we take this element to be x and since $|G|/|x| = k$ which is odd, then $\pi(x)$ is an odd permutation. Here π is the left regular permutation representation. Now again by the previous exercises since $\pi(G)$ has an odd element then G has a subgroup of index 2. □

8. (4.3.2(b))
   Find all the conjugacy classes and their sizes in Q_8.

   Proof. $\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$ with apparent sizes 1, 1, 2, 2, 2 which makes sense since every one of these both divides the order of the group and sums to the order of the group—which is what the class equation requires. □

9. (4.3.5)
   If the center of G is of index n, prove that every conjugacy class has at most n elements.

   Proof. We know that in general for any element $g \in G$ that $Z(G) \leq C_G(g) \leq G$ and therefore since the index is finite $|G : Z(G)| = |G : C_G(g)| \cdot |C_G(g) : Z(G)|$. Each of these must be positive integers and

   $$|G : C_G(g)| = n/|C_G(g) : Z(G)| \leq n$$

   □

10. (4.3.20)
Let $\sigma \in A_n$. Show that all elements in the conjugacy class of σ in S_n are conjugate in A_n if and only if σ commutes with an odd permutation. [Use the preceding exercise. This says that if H is a normal subgroup of G and $\mathcal{K}$ is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Then $\mathcal{K}$ is a union of k conjugacy classes of equal size in H where $k = |G : HC_G(x)|$. Therefore a conjugacy class in S_n which consists of even permutations is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n.]

Proof. Suppose $\sigma \in A_n$. Suppose that every τ in the conjugacy class of σ in S_n is conjugate in A_n. Then in particular $(1\ 2)\sigma(1\ 2) = \tau$ must be conjugate to σ in A_n. Hence $\tau = h\sigma h^{-1}$ with $h \in A_n$ and therefore

$$(1\ 2)\sigma(1\ 2) = h\sigma h^{-1} \quad \Rightarrow$$

$$\sigma(1\ 2)h = (1\ 2)h\sigma$$

where $(1\ 2)h$ is odd.

For the converse suppose that σ commutes with g which is odd. Now let τ be conujugate to σ in S_n so that there exists some $h \in S_n$ such that $h\sigma h^{-1} = \tau$. We would like to find some even h' such that $h'\sigma h'^{-1} = \tau$. □

11. (4.3.22)
Show that if n is odd then the set of all n-cycles consists of two conjugacy classes of equal size in A_n.

Proof. We use the previous exercise (21) which establishes that if a conjugacy class's elements have cycle types only of distinct odd integers, then it consists of two conjugacy classes. Since the conjugacy class of an n-cycle only has n-cycles, then the cycle type is just n which is a collection of distinct odd integers. Hence this set consists of two conjugacy classes.

From problem 19, we can infer that the conjugacy classes are of equal size. This is because n is odd and therefore the n-cycles are even permutations. □

12. (4.3.34)
Prove that if p is a prime and P is a subgroup of S_p of order p, then $|N_{S_p}(P)| = p(p-1)$. [Argue that every conjugate of P contains exactly $p-1$ different p-cycles and use the formula for the number of p-cycles to compute the index of $N_{S_p}(P)$ in S_p.]

Proof. Since the order of P is prime then every non-identity element has order a p. But a permutation has order a prime if and only if it is a p-cycle, so P consists of $p-1$ cycles. Any conjugate of a p-cycle has the same cycle type hence is a p-cycle, so for any $\sigma \in S_p$, the set $\sigma P \sigma^{-1}$ consists of $p-1$ distinct p-cycles. (Distinctness follows from the fact that cosets partition a group into equal-size partitions.)

Since the number of p-cycles is given by

$$\frac{p \cdot (p-1) \cdots (p-p+1)}{p} = (p-1)!$$

then the number of conjugates of P is $\frac{(p-1)!}{p-1} = (p-2)!$. Then we have $|S_p : N_{S_p}(P)| = (p-2)!$. Hence

$$p!/|N_{S_p}(P)| = (p-2)! \implies$$

$$|N_{S_p}(P)| = p(p-1)$$

□

13. (4.4.2)
Prove that if G is abelian group of order pq where p and q are distinct primes, then G is cyclic. [Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.]

Proof. By Cauchy's theorem there is an element of order p, call it x, and an element of order q, call it y. Since G is abelian the order of xy is the least common multiple of p, q which is pq since these are prime. Then $|xy| = pq$ and so G is cyclic. □

14. (4.4.7)
If H is the unique subgroup of a given order in a group G prove H is characteristic in G.

Proof. For any automorphism of G, call it φ, the image $\varphi(H)$ is a subgroup of G of order $|H|$ and hence $\varphi(H) = H$. This shows H is characteristic. □

15. (4.4.10)
Let G be a group, let A be an abelian normal subgroup of G, and write $\overline{G} = G/A$. Show that $\overline{G}$ acts (on the left) by conjugation on A by $\overline{g} \cdot a = gag^{-1}$, where g is any representative of the coset $\overline{g}$ (in particular, show that this action is well defined). Give an explicit example to show that this action is not well defined if A is non-abelian.

Proof. First we show that the action is well-defined, since it is given in terms of representatives of cosets. If $a, b \in G$ such that $\overline{a} = \overline{b}$, and if $x \in A$, then first notice that $aA = bA$ so that there exists some $y \in A$ such that $a = by$. Next, the penultimate equality below follows because A is assumed to be an abelian subgroup.

$$\overline{a} \cdot x = axa^{-1} = byx(by)^{-1} = bxb^{-1} = \overline{b} \cdot x$$

Since the action is well-defined, showing that it is a group action is straight-forward. Since A is the identity and $A \cdot x = (eA) \cdot x = exe^{-1} = x$ then the identity acts trivially. If $a, b \in G$ then $a \cdot b \cdot x = abxb^{-1}a^{-1} = (ab) \cdot x$.

For an example of a non-abelian subgroup take $G = S_4$ and $A = \langle (1\ 2), (1\ 2\ 3) \rangle$. Then $(1\ 4)A \cdot (1\ 4) = (1\ 4)(1\ 4)(1\ 4) = (1\ 4)$. However, $(1\ 4)(1\ 2) = (1\ 2\ 4) \in (1\ 4)A$ and yet $(1\ 2\ 4)A \cdot (1\ 4) = (1\ 2\ 4)(1\ 4)(4\ 2\ 1) = (2\ 1)$. Hence the action is not well-defined. □

16. (4.4.12)
Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 then $H \leq Z(G)$.

Proof. (Skipped) □

17. (4.5.1)
Let G be a finite group and p a prime.

Prove that if $P \in Syl_p(G)$ and H is a subgroup of G containing P then $P \in Syl_p(H)$. Give an example to show that, in general, a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G.

Proof. Since $P \leq H$ then we must have that $|P|$ divides $|H|$. Since $|P| = p^\alpha$ then we must have $|H| = p^{\alpha+k}m$ for some $k \geq 0$ and $p \nmid m$, since it is always possible to group all factors of p into a single factor $p^{\alpha+k}$. This makes P a Sylow p-subgroup of H.

With the group $G = S_4$ and the subgroup $H = \langle(1\ 2)\rangle$ we have that the subgroup $P = H$ is a Sylow 2-subgroup of H. However, because $|S_4| = 24 = 2^3 \cdot 3$ then a Sylow 2-subgroup of S_4 would have order 8. Hence P cannot be a Sylow 2-subgroup of S_4. □

18. (4.5.5)
Show that a Sylow p-subgroup of D_{2n} is cyclic and normal for every odd prime p.

Proof. Suppose P is a Sylow p-subgroup, so that $|P| = p^\alpha$. Then P cannot have any element of even order and cannot have any reflection. Hence P is a subgroup of the group of rotations $R \leq D_{2n}$, hence P is cyclic. Therefore P is the unique subgroup of R of order p^α and hence the unique such subgroup of D_{2n}. So P is normal in D_{2n}. □

19. (4.5.13)
Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Proof. Since $56 = 2^3 \cdot 7$ then

$$n_2 | 7$$

$$n_7 | 8$$

therefore $n_2 \in \{1, 7\}$ and $n_7 \in \{1, 2, 4, 8\}$. Moreover $n_7 \equiv 1 \mod 7$ so then we only have $n_7 \in \{1, 8\}$. If $n_2 = 1$ then already the Sylow 2-subgroup is normal so suppose $n_2 = 7$. Then there are $7 \cdot 7 = 49$ non-identity elements in these 7 different Sylow 2-subgroup, leaving $56 - 49 = 7$ elements remaining. Hence there can only be one Sylow 7-subgroup and therefore this is one is normal. □

20. (4.5.23)
Prove that if $|G| = 462$ then G is not simple.

Proof. (Skipped) □

21. (4.5.32)
Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K. Deduce that if $P \in Syl_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$.

Proof. (Skipped) □

22. (4.5.44)
Let p be the smallest prime dividing the order of the finite group G. If $P \in Syl_p(G)$ and P is cyclic prove that $N_G(P) = C_G(P)$.

Proof. (Skipped) $\square$