Math 541

Solutions to HW #6

The following are from Gallian, Chapters 4 and 5 (6th edition).

- *# 4.8*: Let a be an element of a group and let $|\ a\ | = 15$. Compute the orders of the following elements of G:
  - a^3, a^6, a^9, a^{12}
    * For each a^k above, $\gcd(15, k) = 3$. Thus, the order of each is $15/3 = 5$.
  - a^5, a^{10}
    * For each a^k above, $\gcd(15, k) = 5$. Thus, the order of each is $15/5 = 3$.
  - a^2, a^4, a^8, a^{14}
    * For each a^k above, $\gcd(15, k) = 1$. Thus, the order of each is $15/1 = 15$.

- *# 4.14*: Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|\ G\ |$? What can you say if 7 is replaced with p where p is a prime?
  - Since G is cyclic, there is some element a in G such that $\langle a \rangle = G$. Since G has a subgroup of order 7, and G is cyclic, we know that 7 divides the order of G. That is, $|\ \langle a \rangle\ | = |\ G\ | = 7n$ for some positive integer n. We now test a few possible values of n:
    * Suppose $n = 1$. Then G and one of its subgroups both have order 7. By the Fundamental Theorem of Cyclic Groups (FTCG), G and its subgroup of order 7 are the same, contradicting the condition that G has 3 distinct subgroups.
    * Suppose n is 2, 3, 4, 5, or 6. Then, by FTCG, $G = \langle a \rangle$ has a subgroup of order n. Thus, G has at least 4 subgroups: $\{e\}$, the subgroup of order 7, the subgroup of order n, and G itself. This contradicts the fact that G has exactly three subgroups.
    * Suppose $n = 7$. Then $|\ G\ | = 7 \cdot 7 = 49$. Since 7 is the only positive divisor of 49 between 1 and 49, it is the only possible order of a subgroup other than $\{e\}$ or G. FTCG also tells us that there is *exactly* one subgroup of order 7. This fits the supposed criteria.
    * In general, if we suppose that n is any positive integer besides 7, we see that G is guaranteed a subgroup of order n by the FTCG, which means that G will have *at least* 4 distinct subgroups.

    We therefore conclude that the order of G must be $7^2 = 49$.
  - More generally, if 7 is replaced by any prime p under the supposed conditions, the the order of G must be p^2.

- *# 4.16*: Find a collection of distinct subgroups $\langle a_1 \rangle$, $\langle a_2 \rangle$, ..., $\langle a_n \rangle$ of $\mathbb{Z}_{240}$ with the property that $\langle a_1 \rangle \subset \langle a_2 \rangle \subset ... \subset \langle a_n \rangle$ with n as large as possible.
  - Since $\mathbb{Z}_{240}$ is cyclic and the order of a subgroup of a cyclic group divides the order of the group in which it is contained, we see it must be true that

    $$|\ \langle a_i \rangle\ | \text{ divides } |\ \langle a_{i+1} \rangle\ |, ..., |\ \langle a_{n-1} \rangle\ |, |\ \langle a_n \rangle\ |.$$

    That is, the order of a subgroup divides the order of *every* subgroup in which it is contained.
  - Breaking 240 into its prime factorization, we get $240 = 2^4 \cdot 3 \cdot 5$. That is, 240 is the product of 6 primes (note that they need not be distinct).
  - Since $\{e\}$ is a subgroup of every group, it's clear that we must let $\langle a_1 \rangle = \langle 240 \rangle = \{e\}$.
  - Since $\mathbb{Z}_{240}$ is the largest possible subgroup of $\mathbb{Z}_{240}$, we let $\langle a_n \rangle = \langle 1 \rangle = \mathbb{Z}_{240}$.

- To maximize the number of subgroups between $\{e\}$ and $\mathbb{Z}_{240}$, we must let a_{n-1} be one of the prime divisors of 240, call it p_1. To see that this is true, simply suppose that a_{n-1} is not prime, but rather a composite of i different prime divisors of 240 ($2 \leq i \leq 5$). You will see that there can be at most $5 - i$ subgroups between $\{e\}$ and $\langle a_{n-1} \rangle$.
- Similarly, we let $a_{n-2} = p_1 p_2$, where p_2 is another prime divisor of 240. Once again, to see that this is the case, suppose that a_{n-2} is the product of i different prime divisors of 240 ($3 \leq i \leq 5$). Then there will be at most $5 - i$ subgroups between $\{e\}$ and $\langle a_{n-2} \rangle$.
- Continuing this process until we have exhausted all of the prime divisors of 240, we see that there can be at most 5 subgroups between $\{e\}$ and $\mathbb{Z}_{240}$. Thus, the greatest possible value for n is $5 + 2 = 7$.
- One such example is $\{e\} = \langle 240 \rangle \subset \langle 48 \rangle \subset \langle 16 \rangle \subset \langle 8 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle = \mathbb{Z}_{240}$.

- *# 4.22*: Prove that a group of order 3 must be cyclic.
  - Seeking a contradiction, let G be a group of order 3 that is not cyclic. Thus G has an identity element e, and two additional elements, call them a and b. Since $\langle a \rangle$ and $\langle b \rangle$ are both subgroups of G, they both contain e. Since G is not cyclic, b is not in $\langle a \rangle$ and a is not in $\langle b \rangle$. Thus, it must be true that $a^2 = e$ and $b^2 = e$, or else we would have that $ea = aa = a$ and $eb = bb = b$, which would mean that not G is not a group (see HW#2, Question 5). Putting all of this into a multiplication table, we see:

$$G = \begin{array}{c|c|c|c|} & \text{e} & \text{a} & \text{b} \\ \hline \text{e} & \text{e} & \text{a} & \text{b} \\ \hline \text{a} & \text{a} & \text{e} & \\ \hline \text{b} & \text{b} & & \text{e} \\ \hline \end{array}$$

  Thus we now only need to determine the products ab and ba. But notice that ab and ba cannot be e, a, or b (by HW#2, Question 5). Thus, G is not closed, which contradicts the fact that G is a group. Since the assumption that G is not cyclic leads to this absurdity, we conclude that G must be cyclic.

- *# 4.24*: For any element a in any group G, prove that $\langle a \rangle$ is a subgroup of $C(a)$ (the centralizer of a).
  - Let $b \in \langle a \rangle$. Then $b = a^n$ for some integer n. Thus, $ab = a \cdot a^n = a^{1+n} = a^{n+1} = a^n \cdot a = ba$. That is, b commutes with a, so $b \in C(a)$. Since b was arbitrary, we can conclude that $\langle a \rangle \subset C(a)$, and since $\langle a \rangle$ is a subgroup of G that is contained in $C(a)$ (with $C(a)$ itself a subgroup), we conclude that $\langle a \rangle$ is also a subgroup of $C(a)$.

- *# 4.32*: Determine the subgroup lattice for $\mathbb{Z}_{12}$.

- *# 5.3*: What is the order of each of the following permutations?
  - (124)(357): disjoint, both of length 3, so the order of the permutation is $lcm(3, 3) = 3$
  - (124)(3567): disjoint and of lengths 3 and 4, so the order of the permutation is $lcm(3, 4) = 12$
  - (124)(35): disjoint and of lengths 3 and 2, so the order of the permutation is $lcm(3, 2) = 6$
  - (124)(357869): disjoint and of lengths 3 and 6, so the order of the permutation is $lcm(3, 6) = 6$
  - (1235)(24567): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (124)(3567), with cycles of orders 3 and 4, so the order of the permutation is $lcm(3, 4) = 12$
  - (345)(245): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (25)(34), so the order of the permutation is $lcm(2, 2) = 2$

- *# 5.4*: What is the order of each of the following permutations?

- $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$
  Writing this as a product of cycles, we get (12)(356). Since this is a disjoint product of cycles of lengths 2 and 3, the order of the permutation is $lcm(2,3) = 6$.
- $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$
  Writing this as a product of cycles, we get (1753)(264). Since this is a disjoint product of cycles of lengths 4 and 3, the order of the permutation is $lcm(4,3) = 12$.

- *# 5.9*: Determine whether the following permutations are even or odd.
  - (135): Written as a product of 2-cycles, we get (15)(13), so this is even.
  - (1356): Written as a product of 2-cycles, we get (16)(15)(13), so this is odd.
  - (13567): Written as a product of 2-cycles, we get (17)(16)(15)(13), so this is even.
  - (12)(134)(152): Written as a product of disjoint cycles, we get (15)(234). Rewritten as a product of 2-cycles, we get (15)(24)(23), so this is odd.
  - (1243)(3521): Written as a product of disjoint cycles, we get (354). Rewritten as a product of 2-cycles, we get (34)(35), so this is even.

- *# 5.18*: Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$. Write α, β, and $\alpha\beta$ as
  - products of disjoint cycles,
    * $\alpha = (12345)(678)$
    * $\beta = (23847)(56)$
    * $\alpha\beta = (12345)(678)(23847)(56) = (12485736)$
  - products of 2-cycles.
    * $\alpha = (15)(14)(13)(12)(68)(67)$
    * $\beta = (27)(24)(28)(23)(56)$
    * $\alpha\beta = (16)(13)(17)(15)(18)(14)(12)$

- *# 5.20*: Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?
  - Referencing the table for A_4 given in Chapter 5, we see that
    * α_1 has order 1 (the identity)
    * α_2, α_3, and α_4 have order 2
    * α_5 through α_{12} have order 3
  - The order of each permutation divides the order of A_4, which is $4!/2 = 4 \cdot 3 = 12$.

- *# 5.28*: Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.
  - In disjoint cycle form, $\beta = (14523)$. Thus, the permutation has order 5, and $\beta^5 = e$. Therefore,

$$\begin{aligned} \beta^{99} &= \beta^{5\cdot 19+4} \\ &= (\beta^{5\cdot 19})\beta^4 \\ &= (\beta^5)^{19}\beta^4 \\ &= e^{19}\beta^4 \\ &= \beta^4 \end{aligned}$$

- Now we compute $\beta^4 = (14523)(14523)(14523)(14523) = (13254)$. Thus, $\beta^{99} = (13254)$.

- *# 5.30*: What cycle is $(a_1 a_2 ... a_n)^{-1}$?
  - We can restate this question as: what cycle β gives $\beta(a_1 a_2 ... a_n) = (a_1 a_2 ... a_n)\beta = e$? Our knowledge of the Socks-Shoes Lemma might lead us to try $(a_n ... a_2 a_1)$, and in fact letting $\beta = (a_n ... a_2 a_1)$ gives the desired result.

- *# 5.34*: Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \textit{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. Is your argument valid when 5 is replaced by any $n \geq 3$?
  - We use the Two-Step Subgroup Test. Let α, γ be elements of H. Then:

$$\begin{aligned} \alpha\gamma(1) &= \alpha(\gamma(1)) \\ &= \alpha(1) = 1, \end{aligned}$$

    and

$$\begin{aligned} \alpha\gamma(3) &= \alpha(\gamma(3)) \\ &= \alpha(3) = 3, \end{aligned}$$

    so $\alpha\gamma$ is in H. Also, since $1 = \alpha^{-1}(\alpha(1)) = \alpha^{-1}(1)$ and $3 = \alpha^{-1}(\alpha(3)) = \alpha^{-1}(3)$, we see that α^{-1} is in H. This gives the desired result.
  - Replacing S_5 with S_n for any $n \geq 3$ does not affect the argument.

- *# 5.36*: In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.
  - The subgroup of S_4 generated by (1234) is cyclic, since $(1234)^4 = e$, and the set $\{e, (1234), (1234)^2, (1234)^3\}$ is closed under composition.
  - Referencing the table given for A_4 in chapter 5 (note that A_4 is a subgroup of S_4), we can see readily that $\{(1), (12)(34), (13)(24), (14)(23)\}$ gives a non-cyclic subgroup of S_4 that has order 4.

- *# 5.46*: Show that for $n \geq 3$, $Z(S_n) = \{\epsilon\}$.
  - Seeking a contradiction, assume that this statement is not true. That is, assume that there is at least one permutation (call it α) besides ϵ with the property that $\alpha\beta = \beta\alpha$ for all β in S_n. Since α is itself a permutation, it can be written as a product of disjoint cycles $\gamma_1\gamma_2...\gamma_{r-1}\gamma_r$. If $r > 1$, we can consider the decomposition of γ_1 and γ_r into products of 2-cycles as follows:
    * If $\gamma_1 = (a_1 a_2 ... a_s)$, then γ_1 can be written $(a_1 a_s)(a_1 a_{s-1})...(a_1 a_3)(a_1 a_2)$.
    * If $\gamma_r = (b_1 b_2 ... b_t)$, then γ_r can be written $(b_1 b_t)(b_1 b_{t-1})...(b_1 b_3)(b_1 b_2)$.

    Let us now consider the effect of multiplying α on the left, then on the right by the cycle $(a_1 b_1)$.
    * Multiplying on the left, we get

$$\begin{aligned} (a_1 b_1)\alpha &= (a_1 b_1)\gamma_1\gamma_2...\gamma_r \\ &= (a_1 b_1)(a_1 a_s)(a_1 a_{s-1})...(a_1 a_3)(a_1 a_2)\gamma_2...\gamma_r \\ &= (a_1 a_2 ... a_s b_1)\gamma_2...\gamma_r \\ &= (a_1 a_2 ... a_s b_1)\gamma_r\gamma_2...\gamma_{r-1} \end{aligned}$$

      This step is justified since γ_2, γ_3,...γ_r are disjoint and therefore commutative. Furthermore,

$$\begin{aligned} (a_1 a_2 ... a_s b_1)\gamma_r\gamma_2...\gamma_{r-1} &= (a_1 a_2 ... a_s b_1)(b_1 b_2 ... b_t)\gamma_2...\gamma_{r-1} \\ &= (a_1 a_2 ... a_s b_1 b_2 ... b_t)\gamma_2...\gamma_{r-1} \end{aligned}$$

* Multiplying on the right, we get

$$\begin{aligned}\alpha(a_1b_1) &= \gamma_1\gamma_2...\gamma_r(a_1b_1)\\ &= \gamma_1\gamma_2...\gamma_{r-1}(b_1b_t)(b_1b_{t-1})...(b_1b_3)(b_1b_2)(a_1b_1)\\ &= \gamma_1\gamma_2...\gamma_{r-1}(a_1b_2b_3...b_{t-1}b_tb_1)\\ &= \gamma_1(a_1b_2b_3...b_{t-1}b_tb_1)\gamma_2...\gamma_{r-1}\end{aligned}$$

  The facts that γ_1, γ_2,...,γ_{r_1}, γ_r are disjoint and $(a_1b_2b_3...b_{t-1}b_tb_1)$ contains only elements from γ_1 and γ_r imply that $(a_1b_2b_3...b_{t-1}b_tb_1)$ commutes with γ_2,...,γ_{r-1}. This is what justifies the preceding step. Furthermore,

$$\begin{aligned}\gamma_1(a_1b_2b_3...b_{t-1}b_tb_1)\gamma_2...\gamma_{r-1} &= (a_1a_2...a_s)(a_1b_2b_3...b_{t-1}b_tb_1)\gamma_2...\gamma_{r-1}\\ &= (a_1b_2b_3...b_tb_1a_2a_3...a_s)\gamma_2...\gamma_{r-1}\end{aligned}$$

Since $(a_1a_2...a_sb_1b_2...b_t)\gamma_2...\gamma_{r-1} \neq (a_1b_2b_3...b_tb_1a_2a_3...a_s)\gamma_2...\gamma_{r-1}$, we conclude that $(a_1b_1)\alpha \neq \alpha(a_1b_1)$. That is, we have found a β, namely (a_1b_1), that contradicts our assumption that $\alpha\beta = \beta\alpha$ for all β in S_n.

We are left now with the case when $r = 1$.

* When α can be written as a single disjoint cycle $(a_1a_2...a_t)$ with $t \geq 3$, consider multiplying α on the left and right by (a_1a_2):
  · $(a_1a_2)(a_1a_2...a_t) = (a_2a_3...a_t)$.
  · $(a_1a_2...a_t)(a_1a_2) = (a_1a_3...a_t)$.
* When α is a single 2-cycle (a_1a_2), the fact that $n \geq 3$ guarantees the existence of some a_3 that is not equal to a_1 or a_2. Multiplying on the left and right by $(a_1a_2a_3)$ gives:
  · $(a_1a_2a_3)(a_1a_2) = (a_1a_3)$
  · $(a_1a_2)(a_1a_2a_3) = (a_2a_3)$

It's now clear that for all $r \geq 1$, there exists no α besides ϵ in S_n such that $\alpha\beta = \beta\alpha$ for all β in S_n.