Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 6, 2020

Problems in Section 2.11.

1. List all the conjugate classes in S_3, find the c_a's , and verify the class equation.

Solution. The conjugate classes of S_3 is as follows:

$$\begin{aligned}
&C(id) = \{id\},\\
&C((1,2)) = \{(1,2),(1,3),(2,3)\},\\
&C((1,2,3)) = \{(1,2,3),(1,3,2)\}.
\end{aligned}$$

Consequently, $c_{id} = 1, c_{(1,2)} = 3$, and $c_{(1,2,3)} = 2$. Thus,

$$\sum_a c_a = 1 + 3 + 2 = 6 = o(G).$$

Hence, the class equation is verified. □

2. List all the conjugate classes in S_4, find the c_a's , and verify the class equation.

Solution. The conjugate classes of S_4 is as follows:

$$\begin{aligned}
&C(id) = \{id\},\\
&C((1,2)) = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\},\\
&C((1,2,3)) = \{(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3)\},\\
&C((1,2)(3,4)) = \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\},\\
&C((1,2,3,4)) = \{(1,2,3,4),(1,3,2,4),(1,4,2,3),(1,2,4,3),(1,3,4,2),(1,4,3,2)\}.
\end{aligned}$$

Consequently,

$$c_{id} = 1, \quad c_{(1,2)} = 6, \quad c_{(1,2,3)} = 8, \quad c_{(1,2)(3,4)} = 3, \quad c_{(1,2,3,4)} = 6.$$

Thus,

$$\sum_a c_a = 1 + 6 + 8 + 3 + 6 = 24 = o(G).$$

Hence, the class equation is verified. □

3. List all the conjugate classes in the group of quaternion units, find the c_a's and verify the class equation.

Solution. The conjugate classes of quaternion group $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is as follows:

$$C(1) = \{1\}, \quad C(-1) = \{-1\},$$
$$C(i) = \{i, -i\}, \quad C(j) = \{j, -j\}, \quad C(k) = \{k, -k\}.$$

Consequently,

$$c_1 = 1, \quad c_{-1} = 1, \quad c_i = 2, \quad c_j = 2, \quad c_k = 2.$$

Thus,

$$\sum_a c_a = 1 + 1 + 2 + 2 + 2 = 8 = o(G).$$

Hence, the class equation is verified. $\square$

4. List all the conjugate classes in the dihedral group of order $2n$, find the c_a's and verify the class equation. Notice how the answer depends on the parity of n.

Solution. We find the conjugate classes for which n is odd. Observe that

$$C(e) = \{e\}, \quad C(y) = \{y, y^{n-1}\}, \quad \cdots, \quad C(y^k) = \{y^k, y^{n-k}\}, \quad \left(1 \le k \le \frac{n-1}{2}\right),$$
$$C(x) = \{xy^k : k \equiv 0 \pmod 2, 0 \le k \le n\}, \quad C(xy) = \{xy^k : k \equiv 1 \pmod 2, 0 \le k \le n\}.$$

Consequently,

$$c_e = 1, \quad c_y = 2, \quad \cdots, \quad c_{y^k} = 2, \quad c_x = \frac{n-1}{2}, \quad c_{xy} = \frac{n+1}{2}.$$

Thus,

$$\sum_a c_a = 1 + 2 \cdot \frac{n-1}{2} + \frac{n-1}{2} + \frac{n+1}{2} = 2n = o(G).$$

Now, suppose given n is even. Observe that

$$C(e) = \{e\}, \quad C(y) = \{y, y^{n-1}\}, \quad \cdots, \quad C(y^k) = \{y^k, y^{n-k}\}\,(1 \le k < n/2)\,, C(y^{n/2}) = \{y^{n/2}\},$$
$$C(x) = \{xy^k : k \equiv 0 \pmod 2, 0 \le k \le n\}, \quad C(xy) = \{xy^k : k \equiv 1 \pmod 2, 0 \le k \le n\}.$$

Consequently,

$$c_e = 1, \quad c_{y^{n/2}} = 1, \quad c_y = 2, \quad \cdots, \quad c_{y^k} = 2, \quad c_x = \frac{n}{2}, \quad c_{xy} = \frac{n}{2}.$$

Thus,

$$\sum_a c_a = 1 + 1 + 2 \cdot \left(\frac{n}{2} - 1\right) + \frac{n}{2} + \frac{n}{2} = 2n = o(G).$$

Hence, the class equation is verified. □

5. a) In S_n prove that there are $\dfrac{1}{r}\dfrac{n!}{(n-r)!}$ distinct r cycles.

Proof. Note that for an r-cycle $(a_1, a_2, \cdots, a_r)$ we can choose $\binom{n}{r}$ elements for the candidates $a_1, a_2, \cdots, a_r$. Now, in a cycle of length r, the number of cases of arranging the sequence a_i is given by $\dfrac{r!}{r}$. Thus, the number of total distinct r-cycles is:

$$\binom{n}{r} \cdot \frac{r!}{r} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{r} = \frac{n!}{r(n-r)!}.$$

□

b) Using this, find the number of conjugates that the r-cycle $(1, 2, \cdots, r)$ has in S_n.

Solution. We know that any two permutations having the same cycle decomposition are conjugate. Therefore, the number of conjugates of r-cycle $(1, 2, \cdots, r)$ is exactly the number of all distinct r-cycles in S_n. That is, $\dfrac{n!}{r(n-r)!}$. □

c) Prove that any elements σ in S_n which commutes with $(1, 2, \cdots, r)$ is of the form $\sigma = (1, 2, \cdots, r)^i \tau$, where $i = 0, 1, 2, \cdots, r$, τ is a permutation leaving all of $1, 2, \cdots, r$ fixed.

Proof. It is obvious that the permutations of the form $\sigma = (1, 2, \cdots, r)^i \tau$ commutes with $(1, 2, \cdots, r)$. Note that there are $(n-r)!$ possibilities for $\tau \in S_n$. Thus, in total, there are $r \cdot (n-r)!$ distinct σ in S_n. Recall that the number of conjugates of $(1, 2, \cdots, r)$ is $\dfrac{n!}{r(n-r)!}$, hence

$$o(N((1, 2, \cdots, r)) = \frac{o(G)}{c_{(1,2,\cdots,r)}} = \frac{n!}{\dfrac{n!}{r(n-r)!}} = r \cdot (n-r)!$$

so that there are at most $r \cdot (n-r)!$ distinct permutations in S_n commute with $(1, 2, \cdots, r)$. But since there are $r \cdot (n-r)!$ distinct σ in S_n, any element in S_n which commutes with $(1, 2, \cdots, r)$ is of the form $\sigma = (1, 2, \cdots, r)^i \tau$. □

6. a) Find the number of conjugates of $(1, 2)(3, 4)$ in S_n, $n \geq 4$.

Solution. The number of conjugates of $(1,2)(3,4)$ is exactly the number of all possible $(a_1,a_2)(a_3,a_4) \in S_n$, $a_i \in J_n$. Thus, first we choose 4 distinct $a_i \in J_n$, and partition into 2 halves. Thus,

$$\binom{n}{4} \cdot \frac{4!}{2! \cdot 2!} = \frac{n!}{8 \cdot (n-4)!}$$

is the number of whole conjugates of $(1,2)(3,4)$ in S_n. $\square$

b) Find the form of all elements commuting with $(1,2)(3,4)$ in S_n

Solution. We claim that the permutations of the form $\sigma = \theta \cdot \tau \in S_n$, $\theta \in N((1,2)(3,4)) \subset S_4$ and $\tau \in S_n$ is a permutation leaving all of $1,2,3,4$ fixed are the elements in S_n which commute with $(1,2)(3,4)$. Clearly, σ commutes with $(1,2)(3,4)$. Moreover, there are $(n-4)!$ distinct τ in S_n and 8 distinct elements in $N((1,2)(3,4))$. Hence, $8 \cdot (n-4)!$ distinct σ are in S_n. Note that the order of $N((1,2)(3,4))$ in S_n is $\dfrac{n!}{\dfrac{n!}{8 \cdot (n-4)!}} = 8 \cdot (n-4)!$.
Therefore, we established every possible cases of the elements of $N((1,2)(3,4)$ in S_n. Hence, our claim is proved. $\square$

7. If p is a prime number, show that in S_p there are $(p-1)!+1$ elements x satisfying $x^p = e$.

Proof. Note that if p is prime, any $\sigma \in S_p$ having order p must be a cycle of length p. Since there are $(p-1)!$ distinct p-cycles in S_p and $e^p = e$, there are $(p-1)!+1$ elements $x \in S_n$ satisfy $x^p = e$. $\square$

8. If in a finite group G an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq (e), G$.

Proof. Suppose $a \in G$ has exactly two conjugates in G. Then $[G : N(a)] = 2$ so that $N(a)$ is a non-trivial normal subgroup in G. $\square$

9. a) Find two elements in A_5, the alternating group of degree 5, which are conjugates in S_5 but not in A_5.

Solution. First we verify the existence of such two elements in A_5. Note that the size of conjugacy class of $(1,2,3,4,5)$ in S_5 is $4! = 24$. But since size of every conjugacy class of an element of group must divide the order of the group, as $24 \nmid 60$, there must be two permutations in A_5 which are not conjugate to each other. We claim that $(1,2,3,4,5)$ and $(1,2,3,4,5)^2 = (1,3,5,2,4)$ are two non-conjugate 5 cycles. Suppose they were conjugate, there must be a $\sigma \in A_5$ such that $\sigma^{-1}(1,2,3,4,5)\sigma = (1,3,5,2,4)$. From this we see that σ must fix 1, so σ is a permutation moving only in $\{2,3,4,5\}$. Observe that if

$$\begin{aligned}
\sigma = (2,3,4) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,3,4,2,5),\\
\sigma = (2,4,3) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,4,2,3,5),\\
\sigma = (2,3,5) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,3,5,4,2),\\
\sigma = (2,5,3) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,5,2,4,3),\\
\sigma = (2,4,5) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,4,3,5,2),\\
\sigma = (2,5,4) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,5,3,2,4),\\
\sigma = (3,4,5) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,2,4,5,3),\\
\sigma = (3,5,4) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,2,5,3,4),\\
\sigma = (2,3)(4,5) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,3,2,5,4),\\
\sigma = (2,4)(3,5) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,4,5,2,3),\\
\sigma = (2,5)(3,4) &\implies \sigma^{-1}(1,2,3,4,5)\sigma = (1,5,4,3,2)
\end{aligned}$$

so that none of the cases yields $(1,3,5,2,4)$. Hence, $(1,2,3,4,5)$ and $(1,3,5,2,4)$ are the permutations which are not conjugate in A_5(Instead of brief proof, I made a brute force calculation since this calculations will be made use in next Problem). $\square$

b) Find all the conjugate classes in A_5 and the number of elements in each conjugate class.

Solution. The conjugate classes in A_5 are:

$$\begin{aligned}
C(id) &= \{id\},\\
C((1,2,3)) &= \{(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,2,5),(1,5,2),(1,3,4),\\
&\quad (1,4,3),(1,3,5),(1,5,3),(1,4,5),(1,5,4),(2,3,4),(2,4,3),\\
&\quad (2,3,5),(2,5,3),(2,4,5),(2,5,4),(3,4,5),(3,5,4)\},\\
C((1,2)(3,4)) &= \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(2,3)(4,5),(2,4)(3,5),\\
&\quad (2,5)(3,4),(1,3)(4,5),(1,4)(3,5),(1,5)(3,4),(1,2)(4,5),\\
&\quad (1,4)(2,5),(1,5)(2,4),(1,2)(3,5),(1,3)(2,5),(1,5)(2,3)\},\\
C((1,2,3,4,5)) &= \{(1,2,3,4,5),(1,3,4,2,5),(1,4,2,3,5),(1,3,5,4,2),(1,5,2,4,3),\\
&\quad (1,4,3,5,2),(1,5,3,2,4),(1,2,4,5,3),(1,2,5,3,4),(1,3,2,5,4),\\
&\quad (1,4,5,2,3),(1,5,4,3,2)\},\\
C((1,3,5,2,4)) &= \{(1,3,5,2,4),(1,2,3,5,4),(1,2,4,3,5),(1,2,5,4,3),(1,3,2,4,5),\\
&\quad (1,3,4,5,2),(1,4,2,5,3),(1,4,3,2,5),(1,4,5,3,2),(1,5,2,3,4),\\
&\quad (1,5,3,4,2),(1,5,4,2,3)\}.
\end{aligned}$$

Consequently,

$$c_{id} = 1, \quad c_{(1,2,3)} = 20, \quad c_{(1,2)(3,4)} = 15, \quad c_{(1,2,3,4,5)} = 12, \quad c_{(1,3,5,2,4,)} = 12.$$

□

10. a) If N is a normal subgroup of G and $a \in N$, show that every conjugate of a in G is also in N.

Proof. Let $a \in N$. Since N is normal, for any its conjugate gag^{-1}, $gag^{-1} \in N$. □

b) Prove that $o(N) = \sum c_a$ for some choices of a in N.

Proof. We prove that if N is normal, it is union of conjugacy classes of G. We denote the conjugacy class of any $n \in N$ in G as $C(n)$. Then by above problem a), $C(n) \subset N$ for all $n \in N$. Clearly, $\bigcup_{n \in N} C(n) \subset N$. Note that for any $n \in N$, $n \in C(n)$ so that $N \subset \bigcup_{n \in N} C(n)$. Thus, $N = \bigcup_{n \in N} C(n)$. Denote the size of $C(a)$ as c_a. Hence, $o(N) = \sum c_a$ for some choices of $a \in N$.

† **Remark:** This problem implies that any normal group N can be expressed as union of conjugacy classes of G, but does not imply that this partition derived from G is the conjugate partition **of** N. In fact, from Problem 9, we can see that the conjugate partition of A_5 is not that of S_5. □

c) Using this and the result for Problem 9b), prove that in A_5 there is no normal subgroup N other than (e) and A_5.

Proof. Note that the conjugacy class sizes of A_5 are: 1,12,12,20,15. Since any non-trivial normal subgroup must contain conjugacy class of size 1(the identity) and one or more other conjugacy class, the possible order of such normal group is given by the summations of such conjugacy sizes. By simple calculations, the possible candidates for the order of the normal subgroups are: 13,16,21,25,28,33,36,40,45,48,60. Now applying the Lagrange's theorem, the only possible non-trivial normal subgroup is A_5 itself. Hence A_5 is simple. □

11. Using Theorem 2.11.2 as a tool, prove that if $o(G) = p^n$, p a prime number, then G has a subgroup of order p^α for all $0 \leq \alpha \leq n$.

Proof. We make induction on the order of group G with $o(G) = p^n$. If $n = 1$, this trivially satisfies our hypothesis. Also, if $\alpha = 0$, there is no more to say. Thus, suppose every p-group of order p^{n-1}, has a subgroup of order p^α for all $1 \leq \alpha \leq n-1$. Let $o(G) = p^n$. We know that every p-group has non-trivial centre. By applying Cauchy's theorem, we have an $b \in Z(G)$ with order p. Let $B = (b)$. Since $b \in Z(G)$, B is normal in G. Thus, considering the factor group G/B, $o(G/B) = p^{n-1}$. Now by our induction hypothesis, there is a subgroup $\overline{P}$ of G/B with order p^{a-1}, $0 \leq a-1 \leq n-2$. Let $P = \{x \in G : xZ \in \overline{P}\}$.

Clearly P is a subgroup of G, and by second isomorphism theorem, $\overline{P} \simeq P/Z(G)$. Thus, P is a subgroup of order p^a, $1 \leq a \leq n-1$. Thus by induction process, we have proved that every p-group has a subgroup of order p^α for all $0 \leq \alpha \leq n$, for any n.

† **Remark:** Note that the problem still holds even if we have considered subgroup to be "NORMAL". Procedure for the proof is exactly the same. □

12. If $o(G) = p^n$, p a prime number, prove that there exist subgroups N_i, $i = 0, 1, \cdots, r$ (for some r) such that $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_r = (e)$ where N_i is a normal subgroup of N_{i-1} and where N_{i-1}/N_i is abelian.

Proof. We make use of the Problem 11. Since $o(G) = p^n$, we have a normal subgroup N_1 of order p^{n-1}. Since G/N_1 is of order p, the factor group is cyclic and hence abelian. Now since $o(N_1) = p^{n-1}$, it again has a normal(in N_1) subgroup N_2 of order p^{n-2} and N_1/N_2 is clearly abelian. Continuing this process, we have series of N_i's satisfying the conditions given in the problem, i.e. G is solvable. □

13. If $o(G) = p^n$ p a prime number, and $H \neq G$ is a subgroup of G, show that there exists an $x \in G$, $x \notin H$ such that $x^{-1}Hx = H$.

Proof. Let S be a set of all left cosets of H. We consider a left group action from H on S defined by:

$$h \cdot (xH) = (hx)H.$$

Note that the orbit of H under such group action is $Orb_H(H) = \{H\}$ so that $|Orb_H(H)| = 1$. But since H has order a multiple of p, there must be also another orbit of $xH \in S$ with its size not a multiple of p, that is, 1. Hence, for some $x \notin H$, $|Orb_H(xH)| = 1$. Thus, for any $h \in H$, $hxH = xH$ so that $x^{-1}hxH = H$. This further implies that $x^{-1}hx \in H$ for all $h \in H$, where $x \in H$. Therefore, $x^{-1}Hx = H$ where $x \notin H$. □

14. Prove that any subgroup of order p^{n-1} in a group of G order p^n, p a prime number, is normal in G.

Proof. Note that $N(H)$ is a subgroup of G and $H \subset N(H)$. By the Problem 13, $H \lneqq N(H)$. Since $o(H) = p^{n-1}$, it is must that $N(H) = G$, and hence, H is normal in G. □

15. If $o(G) = p^n$, p a prime number, and if $N \neq (e)$ is a normal subgroup of G, prove that $N \cap Z \neq (e)$, where Z is the center of G.

Proof. Suppose N is non-trivial subgroup of G. From the Problem 10 b), we know that N is an union of its conjugacy classes of G. In particular, $e \in N$. Since the size of every conjugacy classes must be a power of p, and N being a subgroup of p-group, it must admit one or more conjugacy class of size 1. That is, there is an $a \in N$, where $gag^{-1} = a$ for all $g \in G$. □

16. If G is a group, Z its center, and if G/Z is cyclic, prove that G must be abelian.

Proof. Suppose $G/Z(G)$ is cyclic, then we can write $G/Z(G) = (aZ)$ for some $a \in G$. Note that for any $x \in G$ lies in one of the coset $a^k Z$. Thus, we can represent x as $x = a^{k_1} z_1$, $y = a^{k_2} z_2$ for some $k_1, k_2 \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$. Consequently,

$$xy = (a^{k_1} z_1)(a^{k_2} z_2) = a^{k_1}(z_1 a^{k_2}) z_2 = a^{k_1} a^{k_2} z_1 z_2 = a^{k_1 + k + 2} z_1 z_2,$$

while

$$yx = (a^{k_2} z_2)(a^{k_1} z_1) = a^{k_2}(z_2 a^{k_1}) z_1 = a^{k_2} a^{k_1} z_2 z_1 = a^{k_1 + k_2} z_1 z_2,$$

so that $xy = yx$. Hence, G is abelian. $\square$

17. Prove that any group of order 15 is cyclic.

Proof. Apply Cauchy's theorem to obtain elements of order 3 and 5 respectively. Note that $3 \nmid 4 = 5 - 1$, so by the Problem 10 of Section 2.9, the given group is cyclic. $\square$

18. Prove that a group of order 28 has a normal subgroup of 7.

Proof. By Cauchy's theorem, we have an element of order 7. Let H be the subgroup generated by this element. Then since $28 \nmid 4! = 24$, H must contain a non-trivial normal subgroup. Since H is of prime order, H itself is the normal subgroup. Hence proved. $\square$

19. Prove that if a group G of order 28 has a normal subgroup of order 4, then G is abelian.

Proof. Suppose H be the subgroup of G with order 7 and K be the normal subgroup of G of order 4. Note H is always normal in G. Then since $\gcd(4, 7) = 1$, H and K are normal, HK is abelian and $HK = G$ so that G is abelian. $\square$