

Solutions to Homework 3

Problem 1. Problem E to chapter 4.

Solution. 1. Let G be a finite group and $S = \{g \in G : g \neq g^{-1}\}$ be the set of all elements in G which are not equal to their own inverse. Note that if $g \in S$ then also $g^{-1} \in S$. So pairing every element from S with its inverse partitions the set S into some number k of pairs of the form $\{g, g^{-1}\}$. Thus S has $2k$ elements, so $|S|$ is even.

2. Let T be the set of all elements in G which are equal to their own inverse and let $t = |T|$. Then $|G| = |T| + |S| = t + 2k$, so t and $|G|$ have the same parity, i.e. they are either both odd or both even.

3. Suppose $|G|$ is even. By 2. we know T is even as well. Since $e \in T$, we must have at least one $x \in T$ such that $x \neq e$.

Suppose now that G is a finite abelian group. Let u be the product of all elements in G , s be the product of all elements in S , and t be the product of all elements in T (since G is abelian, order of multiplication does not matter). Then $u = st$. Recall that the set S is partitioned into pairs of the form $\{g, g^{-1}\}$ and the product of each such pair is the identity. This shows that $s = e$ and therefore $u = t$.

4. Note that if $a \in T$ then $a = a^{-1}$ so $a^2 = e$. If $T = \{t_1, \dots, t_m\}$ then $t = t_1 t_2 \dots t_m$ and

$$t^2 = (t_1 t_2 \dots t_m)^2 = t_1^2 t_2^2 \dots t_m^2 = e.$$

This shows that $u^2 = e$.

5. If $T = \{e\}$ then $t = e$ so $u = e$.

6. If $T = \{e, x\}$ with $x \neq e$ then $t = ex = x$ so $u = x$.

Remark. It is not hard to show that if G is abelian and $|T| > 2$ then $u = e$.

Remark. Let p be an odd prime. Take for G the group $\mathbb{Z}_p^\times = \{1, 2, \dots, p-1\}$ with multiplication modulo p . In this case $T = \{1, p-1\}$ (if $a^2 \equiv 1 \pmod{p}$ then $p|(a^2 - 1) = (a-1)(a+1)$ so $p|a-1$ or $p|a+1$, i.e. $a \equiv 1 \pmod{p}$ or $a \equiv p-1 \pmod{p}$). We have $u \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) = (p-1)! \pmod{p}$, thus part 6 above implies the following classical result:

Wilson's Theorem. Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$.

Problem 2. Problem G to chapter 4.

Solution. 1. We need to check the axioms. For associativity,

$$\begin{aligned} [(a, b)(m, n)](g, h) &= (am, bn)(g, h) = ((am)g, (bn)h) = (a(mg), b(nh)) = \\ &= (a, b)(mg, nh) = (a, b)[(m, n)(g, h)]. \end{aligned}$$

The identity of $G \times H$ is (e_G, e_H) :

$$(g, h)(e_G, e_H) = (ge_G, he_H) = (g, h) = (e_G g, e_H h) = (e_G, e_H)(g, h).$$

Finally, the inverse of (g, h) is (g^{-1}, h^{-1}) :

$$(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H).$$

2. The elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are

$$(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2).$$

The operation table of the group is

+	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

3. Suppose that G and H are abelian. Then for any $(g_1, h_1), (g_2, h_2)$ in $G \times H$ we have

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) = (g_2g_1, h_2h_1) = (g_2, h_2)(g_1, h_1).$$

Thus $G \times H$ is abelian.

4. Let (g, h) be any element of $G \times H$. Since $g = g^{-1}$ and $h = h^{-1}$, we have

$$(g, h)^{-1} = (g^{-1}, h^{-1}) = (g, h)$$

so every element in $G \times H$ is its own inverse.

Problem 3. a) Find the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

b) Find the cycle decomposition and order of

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix};$
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix};$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}.$

c) Express the following permutations as products of disjoint cycles and find their orders

1. $(1, 2, 3, 4, 5)(1, 2, 3, 4, 6)(1, 2, 3, 4, 7);$
2. $(1, 2, 3)(3, 4, 5, 6)(1, 2, 3)^{-1};$
3. $(1, 2, 3, 4, 5, 6)^3.$

Express each of these permutations as a product of transpositions.

d) Find a permutation $\rho \in S_n$ such that $\rho\tau\rho^{-1} = \sigma$ or prove that no such ρ exists, where

1. $\tau = (1, 3, 4), \sigma = (2, 3, 5), n = 5$;
2. $\tau = (1, 4)(2, 3, 5), \sigma = (2, 4, 1)(5, 3), n = 5$;
3. $\tau = (1, 3, 5, 7)(2, 4, 6), \sigma = (1, 6)(4, 5, 7, 3, 2)$.

Solution: a)

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

b)

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix} = (1, 3, 4, 2)(5, 7, 9)$. It has order 12;
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1, 7)(2, 6)(3, 5)$. It has order 2;
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 3 & 2 & 1 & 4 \end{pmatrix} = (1, 6)(2, 5)(3, 7, 4)$.
It has order 6.

c)

1. $(1, 2, 3, 4, 5)(1, 2, 3, 4, 6)(1, 2, 3, 4, 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \end{pmatrix} = (1, 4, 7, 3, 6, 2, 5) = (1, 5)(1, 2)(1, 6)(1, 3)(1, 7)(1, 4)$; It has order 7.
2. $(1, 2, 3)(3, 4, 5, 6)(1, 2, 3)^{-1} = (1, 4, 5, 6) = (1, 6)(1, 5)(1, 4)$. It has order 4.;
3. $(1, 2, 3, 4, 5, 6)^3 = (1, 4)(2, 5)(3, 6)$. It has order 2.

d)

1. Since $\tau = (1, 3, 4)$ and $\sigma = (2, 3, 5)$ have the same type of cycle decomposition, they are conjugate in S_n . Any ρ such that $\rho(1) = 2, \rho(3) = 3$ and $\rho(4) = 5$ will work. For example, $\rho = (1, 2)(4, 5)$.
2. Since $\tau = (1, 4)(2, 3, 5)$ and $\sigma = (2, 4, 1)(5, 3)$ have the same type of cycle decomposition, they are conjugate in S_n . Any ρ such that $\rho(1) = 5, \rho(4) = 3, \rho(2) = 2, \rho(3) = 4, \rho(5) = 1$ will work. There is only one such ρ : $\rho = (1, 5)(4, 3)$.
3. The permutations $\tau = (1, 3, 5, 7)(2, 4, 6)$ and $\sigma = (1, 6)(4, 5, 7, 3, 2)$ have different structure of cycle decomposition so they are not conjugate. In fact, for any ρ we have

$$\rho\tau\rho^{-1} = (\rho(1), \rho(3), \rho(5), \rho(7))(\rho(2), \rho(4), \rho(6))$$

which is a product of a 4-cycle and a 3-cycle which are disjoint, hence $\rho\tau\rho^{-1}$ can not be equal to σ (by the uniqueness of the decomposition into a product of disjoint cycles).

Problem 4. a) Let σ, τ be two transpositions in $S_n, n \geq 3$. Show that $\sigma\tau$ can be expressed as a product of 3-cycles (not necessarily disjoint).

b) Prove that every element of $A_n, n \geq 3$ is a product of 3-cycles.

Solution: a) If σ, τ are disjoint then $\sigma = (a, b), \tau = (c, d)$ and a, b, c, d are pairwise different. Then

$$(a, b)(c, d) = (a, b, c)(b, c, d).$$

If the supports of σ and τ have exactly one element in common then we can write $\sigma = (a, b), \tau = (a, c)$, where a, b, c are pairwise different. Thus

$$(a, b)(a, c) = (a, c, b).$$

Finally, if the supports of σ and τ have more than one element in common then $\sigma = \tau$ (note that both supports have 2 elements) so $\sigma\tau = id = (1, 2, 3)(1, 2, 3)(1, 2, 3)$.

b) If τ is an even permutation then it is a product of an even number of transpositions: $\tau = \sigma_1\sigma_2 \dots \sigma_{2k}$, where each σ_i is a transposition. By part a), each of $\sigma_1\sigma_2, \sigma_3\sigma_4, \dots, \sigma_{2k-1}\sigma_{2k}$ is a product of 3-cycles and therefore τ is a product of 3-cycles.

Problem 5. a) Which of the following permutations are even?

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix};$
2. $(1, 2, 3, 4, 5, 6)(7, 8, 9);$
3. $(1, 2)(1, 2, 3)(4, 5)(5, 6, 8)(1, 7, 9).$

b) Prove that a k -cycle is even iff k is odd.

c) In the even permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & & & 7 & 8 & 9 & 6 \end{pmatrix}$$

two entries are missing. Find the missing entries.

Solution: a) Checking whether a given permutation is odd or even directly from the definition is not the most efficient way. Instead we will use part b) and the fact that a product of several permutations is even (odd) if the number of odd factors is even (odd).

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix} = (1, 2, 4)(3, 5)(6, 7, 8, 9).$ The 3-cycle $(1, 2, 4)$ is even and both $(3, 5)$ and $(6, 7, 8, 9)$ are odd. We have an even number of odd factors so our permutation is even.
2. The first factor of $(1, 2, 3, 4, 5, 6)(7, 8, 9)$ is odd and the second factor is even, so the product is odd;
3. The product $(1, 2)(1, 2, 3)(4, 5)(5, 6, 8)(1, 7, 9)$ has two odd permutations and three even permutations so it is an even permutation. .

b) Let $(a_1, a_2, \dots, a_k)$ be a k -cycle. We have seen that

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2)$$

is a product of $k - 1$ transpositions. Thus $(a_1, a_2, \dots, a_k)$ is odd if $k - 1$ is odd, i.e. k is even, and it is even if $k - 1$ is even, i.e. k is odd. This proves our claim.

c) One of the missing entries is 4 and the other is 5. If the first missing entry is 4 then our permutation is $(1, 3, 2)(6, 7, 8, 9)$, which is an odd permutation. If the first missing entry is 5 then our permutation is $(1, 3, 2)(4, 5)(6, 7, 8, 9)$, which is even. Thus only the latter case is possible and our permutation is equal to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix}.$$

Problem 6. Let H be a subgroup of S_n generated by $(1, 2)$ and $(1, 2, 3, \dots, n)$. Prove that $H = S_n$. Hint: Show that H contains all transpositions.

Solution: Let $\tau = (1, 2, 3, \dots, n)$. Since H is a subgroup and both $\tau, (1, 2)$ are in H , we have

$$\tau^k(1, 2)\tau^{-k} = (\tau^k(1), \tau^k(2)) = (k+1, k+2) \in H$$

for $k = 1, 2, \dots, n-2$ and $\tau^{n-1}(1, 2)\tau^{1-n} = (n, 1) \in H$. Thus H contains the transpositions $(1, 2), (2, 3), \dots, (n-1, n)$ and $(1, n)$. Note now that for $s < k < n$ we have $(k, k+1)(s, k)(k, k+1) = (s, k+1)$. This means that if $(i, j) \in H$ with $0 < i < j < n$ then also $(i, j+1) \in H$. Starting with $(1, 2) \in H$ and applying the last observation we see that $(1, k) \in H$ for $k = 1, 2, \dots, n$. Similarly, starting with $(i, i+1) \in H$ we see that $(i, k) \in H$ for $k = i+1, \dots, n$. Thus H contains all transpositions. Since every permutation is a product of transpositions, we see that H contains all permutations, i.e. $H = S_n$.

Problem 7. Let G be a group. Define the **center** of G as the subset $Z(G)$ of all elements which commute with every element of G , i.e.

$$Z(G) = \{g \in G : ag = ga \text{ for every } a \in G\}.$$

- a) Prove that $Z(G)$ is a subgroup of G .
- b) Find $Z(D_3)$, $Z(D_4)$, $Z(Q_8)$ and $Z(D_\infty)$.
- c) What is $Z(D_n)$?
- d) What is $Z(S_n)$?

Solution: a) Clearly $e \in G$. Let $a, b \in Z(G)$. For any $g \in G$ we have

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$$

so $ab \in Z(G)$. Also

$$a^{-1}g = (a^{-1}g)(aa^{-1}) = a^{-1}(ga)a^{-1} = (a^{-1}a)ga^{-1} = ga^{-1}$$

so $a^{-1} \in G$. Thus G is a subgroup of G .

Another way is to use the observation that

$$Z(G) = \bigcap_{g \in G} C(g)$$

where $C(g)$ is the centralizer of g , defined in solution to Quiz 2. Since each $C(g)$ is a subgroup and intersection of subgroups is a subgroup, we conclude that $Z(G)$ is a subgroup.

b) Recall that D_3 contains two elements T and S such that $ST = T^{-1}S$, $T^3 = I = S^2$ and $D_3 = \{I, T, T^2, S, ST, ST^2\}$.

We first determine which elements $S^a T^b$ ($0 \leq a \leq 1$, $0 \leq b \leq 2$) commute with S . Note that $S(S^a T^b) = S^{a+1} T^b$ and $(S^a T^b)S = S^a (T^b S) = S^a S T^{-b} = S^{a+1} T^{-b}$. Thus $S(S^a T^b) = (S^a T^b)S$ iff $T^b = T^{-b}$, i.e. $T^{2b} = I$. This implies that $T^{4b} = I$. Since $T^3 = I$, we have $T^{3b} = I$ and therefore $T^b = (T^{4b})(T^{3b})^{-1} = I$. Thus the only elements which commute with S are I and S (i.e. the centralizer $C(S) = \{I, S\}$). Note that S does not commute with T . Since elements of $Z(D_3)$ commute with all elements of D_3 , we have $Z(D_3) = \{I\}$.

Similarly, $D_4 = \{I, T, T^2, T^3, S, ST, ST^2, ST^3\}$. As before, $S(S^a T^b) = S^{a+1} T^b$ and $(S^a T^b)S = S^a (T^b S) = S^a S T^{-b} = S^{a+1} T^{-b}$, so $S(S^a T^b) = (S^a T^b)S$ iff $T^b = T^{-b}$, i.e. $T^{2b} = I$. This holds iff $b = 0$ or $b = 2$ (we only consider $b \in \{0, 1, 2, 3\}$). Thus the only elements which commute with S are I, S, T^2, ST^2 . Note that neither S nor ST^2 commute with T . This implies that $Z(D_4) \subseteq \{I, T^2\}$. On the other hand, T^2 commutes with S and T so it commutes with all elements in D_4 . Thus $Z(D_4) = \{I, T^2\}$.

Recall that $Q_8 = \{I, -I, i, -i, j, -j, k, -k\}$ (see Problem 6 of homework 2). Note that $\pm i$ does not commute with $\pm j$ and it does not commute with $\pm k$. Thus none of the elements $i, -i, j, -j, k, -k$ is in the center of Q_8 . On the other hand, both I and $-I$ commute with all elements in Q_8 . Thus $Z(Q_8) = \{I, -I\}$.

In D_∞ we have $T^m S = ST^{-m} \neq ST^m$ for $m \neq 0$, so neither S nor any non-trivial power of T belong to $Z(D_\infty)$. Furthermore, $(ST^m)T = ST^{m+1}$ and $T(ST^m) = (TS)T^m = (ST^{-1})T^m = ST^{m-1} \neq (ST^m)T$. Thus no element of the form ST^m belongs to $Z(D_\infty)$. It follows that the only element in $Z(D_\infty)$ is I , i.e. $Z(D_\infty) = \{I\}$.

c) Recall that $D_n = \{I, T, T^2, \dots, T^{n-1}, S, ST, ST^2, \dots, ST^{n-1}\}$, $T^n = I$, and $ST = T^{n-1}S = T^{-1}S$. As in b), we first find the centralizer of S . Since $S(S^a T^b) = S^{a+1} T^b$ and $(S^a T^b)S = S^a (T^b S) = S^a S T^{-b} = S^{a+1} T^{-b}$, we have $S(S^a T^b) = (S^a T^b)S$ iff $T^b = T^{-b}$ iff $T^{2b} = I$. In n is odd this holds only when $b = 0$ and when n is even then $b = 0$ or $b = n/2$ (we only consider b from the set $\{0, 1, \dots, n-1\}$). We see that

$$C(S) = \begin{cases} \{I, S\} & \text{if } n \text{ is odd;} \\ \{I, S, T^{n/2}, ST^{n/2}\} & \text{if } n \text{ is even.} \end{cases}$$

Note also that neither S nor $ST^{n/2}$ commute with T . Thus if n is odd then $Z(D_n) = \{I\}$. For n even, $T^{n/2}$ commutes with all elements of D_n (since it commutes with S and T) so $Z(D_n) = \{I, T^{n/2}\}$ for n even.

d) If $n = 2$ then $S_n = S_2$ is abelian and therefore $Z(S_2) = S_2$. Suppose now that $n \geq 3$. Let τ be a non-trivial permutation in S_n . Thus $\tau(a) = b \neq a$ for some a . Since $n \geq 3$, there is a c different from a and b . Note that $\tau(a, c)\tau^{-1} = (\tau(a), \tau(c)) = (b, \tau(c)) \neq (a, c)$. Thus τ and (a, c) do not commute, so τ is not in the center of S_n . This proves that the center of S_n is trivial, i.e. $Z(S_n) = \{e\}$.