Solutions 03

1. Let H and K be two subgroups of a group G. For any element g in G, the set

$$H\,g\,K := \{f \in G \mid f = h\,g\,k \text{ for some } h \in H, k \in K\}$$

is called a ***double coset***.

i. Prove that the double cosets partition G.

ii. Do all double cosets have the same cardinality?

iii. When G has finite order, must the cardinality of a double coset divide $|G|$?

Solution.

i. We claim that the following is an equivalence relation on G: for any elements f and g in the group G, set $f \approxeq g$ if $f = h\,g\,k$ for some element h in H and some element k in K.

(reflexive) Consider an element g in G. Since the identity element $e \in G$ belongs to both H and K, we have $g = e\,g\,e$ and $g \approxeq g$.

(symmetric) When $f \approxeq g$, there exists an element h in H and an element k in K such that $f = h\,g\,k$. Since H and K are subgroups, we have $h^{-1} \in H$ and $k^{-1} \in K$. It follows that $g = h^{-1}\,f\,k^{-1}$ and $g \approxeq f$.

(transitive) Suppose that $f \approxeq g$ and $g \approxeq g'$. By definition, there exists elements h and h' in H and elements k and k' in K such that $f = h\,g\,k$ and $g = h'\,g'\,k'$. Hence, we obtain $f = (h\,h')g'(k'\,k)$. Since H and K are subgroups, it follows that $h\,h' \in H$ and $k'\,k \in K$. Thus, we deduce that $f \approxeq g'$.

Since the double cosets are the equivalence classes, they partition the underlying set of G.

ii. Double cosets need not have the same cardinality. For example, consider the group $\mathfrak{S}_3$ and the subgroups $H = K := \{\mathrm{id}_3, (2\ 1)\}$. The double cosets are

$$\begin{aligned} H\ \mathrm{id}_3\ H &= \{\mathrm{id}_3, (2\ 1)\} = H\,(2\ 1)\,H \\ H(3\ 1)H &= \{(3\ 1), (3\ 2), (3\ 1\ 2), (3\ 2\ 1)\} \\ &= H\,(3\ 2)\,H = H\,(3\ 1\ 2)\,H = H\,(3\ 2\ 1)\,H\,. \end{aligned}$$

iii. The example in part *iii* satisfies $|\mathfrak{S}_3| = 6$ and $|H\,(3\ 1)\,H| = 4$. Therefore, the cardinality of a double coset does not have to divide the order of the group. □

2. Let G be a group and let $\mathrm{Aut}(G)$ be its automorphism group. For any element g in G, consider the map $\gamma_g : G \to G$ defined, for any element f in G, by $\gamma_g(f) := g\,f\,g^{-1}$.

i. For any element g in G, show that γ_g is an automorphism.

ii. Prove that the map $\Gamma\colon G \to \mathrm{Aut}(G)$ defined, for any g in G, by $\Gamma(g) := \gamma_g$ is a group homomorphism.

iii. Show that $\mathrm{Ker}(\Gamma) = Z(G)$.

iv. Prove that the image $\mathrm{Im}(\Gamma)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Solution.

i. For any elements f and f' in the group G, we have

$$\gamma_g(f f') = g(f f')g^{-1} = (g f g^{-1})(g f' g^{-1}) = \gamma_g(f)\,\gamma_g(f')\,,$$

so the map γ_g is a group homomorphism. For any elements f, g, and h in G, we also have

$$(\ddagger) \qquad (\gamma_g \circ \gamma_h)(f) = \gamma_g(h f h^{-1}) = g(h f h^{-1})g^{-1} = (gh)(f)(gh)^{-1} = \gamma_{gh}(f)\,.$$

We deduce that $\gamma_g \circ \gamma_{g^{-1}} = \gamma_e = \mathrm{id}_G = \gamma_{g^{-1}} \circ \gamma_g$, so the map γ_g is an automorphism.

ii. The equation $(\ddagger)$ implies that $\Gamma(gh) = \gamma_{gh} = \gamma_g \circ \gamma_h = \Gamma(g)\,\Gamma(h)$, so the map Γ is a group homomorphism.

iii. From the sequence of equivalences

$$\begin{aligned} g \in Z(G) \quad &\Leftrightarrow \quad g f g^{-1} = f \quad \text{for any element } f \text{ in } G \\ &\Leftrightarrow \quad \gamma_g(f) = f \quad \text{for any element } f \text{ in } G \\ &\Leftrightarrow \quad \gamma_g = \mathrm{id}_G \\ &\Leftrightarrow \quad \Gamma(g) = e_{\mathrm{Aut}(G)}\,, \end{aligned}$$

we deduce that $\mathrm{Ker}(\Gamma) = Z(G)$.

iv. Fix an element g in the group G, so that the automorphism $\Gamma(g) = \gamma_g$ is in $\mathrm{Im}(\Gamma)$. When φ is an element in $\mathrm{Aut}(G)$, it follows that, for any element f in G, we have

$$(\varphi \circ \gamma_g \circ \varphi^{-1})(f) = \varphi\big(g\,\varphi^{-1}(f)\,g^{-1}\big) = \varphi(g)\,f\,\varphi(g)^{-1} = \gamma_{\varphi(g)}(f)\,.$$

We deduce that $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)} = \Gamma\big(\varphi(g)\big) \in \mathrm{Im}(\Gamma)$, so the image $\mathrm{Im}(\Gamma)$ is a normal subgroup of $\mathrm{Aut}(G)$. □

3. Fix a nonnegative integer n. Two permutations σ and τ in the symmetric group $\mathfrak{S}_n$ have the ***same cycle structure*** if, for any nonnegative integer k, their factorizations into disjoint cycles have the same number of cycles of length k. The ***cycle type*** of a permutation is the list λ of cycles lengths from its factorization into disjoint cycles arranged in nonincreasing order.

i. For any permutations σ and τ in $\mathfrak{S}_n$, prove that the conjugate permutation $\sigma\,\tau\,\sigma^{-1}$ has the same cycle structure as τ and may be obtained by applying σ to the entries in the cycles of τ.

ii. Prove that permutations are conjugate if and only if they have the same cycle type.

Solution.

i. Let ϖ the permutation in $\mathfrak{S}_n$ with the same cycle structure as τ obtained by applying σ to the entries in the cycles of τ. We consider two cases.

- Suppose that $\tau(i) = i$ for some $i \in [n]$. The permutation ϖ fixes the element $\sigma(i) \in [n]$ because $\sigma(i)$ lies in a cycle of length 1. Since

$$(\sigma\,\tau\,\sigma^{-1})\big(\sigma(i)\big) = (\sigma\,\tau)(i) = \sigma(i) = \varpi\big(\sigma(i)\big)\,,$$

the permutation $\sigma\,\tau\,\sigma^{-1}$ also fixes $\sigma(i)$.

- Suppose that $\tau(i) = j \neq i$ for some $i \in [n]$. The definition of φ implies that $\varpi(\sigma(i)) = \sigma(j)$. On the other hand, we also have

$$(\sigma\,\tau\,\sigma^{-1})(\sigma(i)) = (\sigma\,\tau)(i) = \sigma(j) = \varpi(\sigma(i)).$$

Since the permutations ϖ and $\sigma\,\tau\,\sigma^{-1}$ agree on every $i \in [n]$, we conclude that $\varpi = \sigma\,\tau\,\sigma^{-1}$.

ii. Part *i* shows that conjugate permutations have the same cycle type. For the converse, suppose that permutations ϖ and τ have the same cycle type. We need to produce a permutation σ in $\mathfrak{S}_n$ such that $\varpi = \sigma\,\tau\,\sigma^{-1}$. To define the permutation σ, place the factorization of τ into disjoint cycles over that of ϖ so that the cycles of the same length correspond. Let σ be the function sending the top row to the bottom. For example, when $\tau := (3\ \ 1\ \ 2)(5\ \ 4)(6)$ and $\varpi := (3\ \ 1)(4)(6\ \ 2\ \ 5)$, we have the array

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

so $\sigma = (6\ \ 4\ \ 1\ \ 2\ \ 5\ \ 3)$. Observe that the permutation σ is not uniquely determined by this procedure—it implicitly depends on the choice of bijection between the cycles of the same lengths in τ and ϖ. Nevertheless, part *i* establishes that $\varpi = \sigma\,\tau\,\sigma^{-1}$, so the permutations ϖ and τ are conjugate. □