Homework 1 — Solutions

1. Let $f : A \to B$ be a surjective map of sets. Prove that the relation $a \sim b$ if and only if $f(a) = f(b)$ is an equivalence relation whose equivalence classes are the fibers of f.

   Solution. That $\sim$ is an equivalence relation on A follows directly from the fact that $=$ is an equivalence relation on the set B. Now let $b \in B$ be arbitrary. Since f is surjective, there is an a in A such that $f(a) = b$. Then the equivalence class of a is the set $\{x \in A \mid x \sim a\}$. But by definition of $\sim$, this set is equal to $\{x \in A \mid f(x) = f(a) = b\}$. Therefore the equivalence class of a is precisely the fiber of f over b.

2. Prove that if G is a finite group then each row and each column of the multiplication table of G is a permutation of G.

   Solution. Let's check for row. Suppose $G = \{g_1, g_2, ..., g_n\}$ and $g \in G$. Let's consider the list gg_1, ..., gg_n. We know $gg_i = gg_j \implies g_i = g_j$, so all element are distinct. On the other side $g \cdot (g^{-1}g_i) = g_i$, so any element g_i exist in this list. So, this list contains all elements of G exactly one, so it is permutation of G. (This prove didn't use finiteness).

3. In measure theory one defines the "extended real numbers" to be the set, call it $\mathbb{R}_{\text{ext}}$, consisting of $\mathbb{R}$ together with the symbol ∞ (think "$+\infty$"). Addition is defined on $\mathbb{R}_{\text{ext}}$ as follows: if $x = \infty$ or $y = \infty$ then $x + y = \infty$; otherwise x and y are real numbers and $x + y$ is defined to be the usual sum of $x + y$ in $\mathbb{R}$. Which of the group axioms is/are satisfied by $(\mathbb{R}_{\text{ext}}, +)$? Is $(\mathbb{R}_{\text{ext}}, +)$ a group?

   Solution. 1) set is closed under addition. 2) associativity holds because the result is real or infinity. 3) identity is 0: $0 + x = x$. 4) every element has inverse except ∞. Infinity doesn't have inverse.

4. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{N}\}$.

   a. Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).

   Solution. Let $z, w \in G$ so that $z^n = 1$ and $w^m = 1$. Note that $1 \in G$ since $1^1 = 1$, so G has an identity. And every element of G is nonzero, so for each $z \in G$ we may let $z^{-1} = 1/z$ so that every element in G has an inverse (since $(1/z)^n = 1/z^n = 1$ so $1/z \in G$). By the commutativity of multiplication in $\mathbb{C}$, we have $(zw)^{nm} = z^{nm}w^{mn} = (z^n)^m(w^m)^n = 1^m 1^n = 1$ for each $m, n \in \mathbb{N}$. Therefore, G is closed under multiplication. And associativity follows from associativity of multiplication in $\mathbb{C}$. Therefore G is a group.

   b. Prove that G is not a group under addition.

   Solution. G is a not a group under addition since it is not closed: $1 \in G$ but $1 + 1 = 2 \notin G$ since there is no $n \in \mathbb{N}$ with $2^n = 1$.

5. Suppose $(G, \star)$ is a group, and H is a nonempty subset of G that is closed under inverses and $\star$. Prove that H is a group under the operation $\star$ restricted to H.

   Solution. 1) H is closed under operation. 2) Associativity of $\star$ in H follows from associativity of $\star$ in G. 3) Since H is nonempty, it must have an element a. Then by hypothesis $a^{-1} \in H$ and therefore $aa^{-1} = e \in H$, where e denotes the identity of G. Therefore H has an identity. 4) For each $a \in H$, $a^{-1} \in H$ by hypothesis so every element of H has an inverse in H. This shows that $(H, \star)$ is a group.

6. Suppose $(A, \star)$ and $(B, \blacklozenge)$ are groups. Let $A \times B$ be their direct product, defined in Example 6 (top of page 18). Check that $A \times B$ satisfies the group axioms by verifying each of the group axioms, and prove that $A \times B$ is abelian if and only if both $(A, \star)$ and $(B, \blacklozenge)$ are abelian.

   Solution. 1) For all $(a_i, b_i) \in A \times B$ with $i = 1, 2, 3$ we have

   $$(a_1, b_1)((a_2, b_2)(a_3, b_3)) = (a_1, b_1)(a_2a_3, b_2b_3) = (a_1(a_2a_3), b_1(b_2b_3)) = (a_1a_2a_3, b_1b_2b_3)$$

   And similarly from another side. This shows associativity.

   2) For any $(a, b) \in A \times B$ we have $(a, b)(1_A, 1_B) = (a \star 1_A, b \blacklozenge 1_B) = (a, b)$. Therefore $(1_A, 1_B)$ is the identity of $A \times B$.

   3) For any $(a, b) \in A \times B$, $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \blacklozenge b^{-1}) = (1_A, 1_B)$, so $(a, b)^{-1} = (a^{-1}, b^{-1})$.

   4) First, if A and B are abelian and if (a, b) and (c, d) are any members of $A \times B$, then $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$, so $A \times B$ is abelian. For the other direction, suppose $A \times B$ is abelian. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then since $A \times B$ is abelian, we have $(a_1a_2, b_1b_2) = (a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1) = (a_2a_1, b_2b_1)$. Equating components shows that $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$. Therefore A and B are both abelian.

7. Let x and y be elements of a group G. Prove that $xy = yx$ if and only if $yxy^{-1} = x$ if and only if $x^{-1}y^{-1}xy = e$. Prove further that $|yxy^{-1}| = |x|$, and deduce that $|xy| = |yx|$ for all $a, b \in G$.

   Solution. 1) If $xy = yx$, then multiplying by y^{-1} from the left $y^{-1}xy = y^{-1}yx = ex = x$. Multiplying by x^{-1} from the left then gives $x^{-1}y^{-1}xy = e$. On the other hand, if $x^{-1}y^{-1}xy = e$, then we may multiply on the left by x to get $y^{-1}xy = x$. Then multiplying on the left by y gives $xy = yx$ as desired.

   2) A simple induction argument will show that $(g^{-1}xg)^k = g^{-1}x^kg$ for any $k \in \mathbb{N}$. So if $|x| = n$, then $x^n = 1$ and we have $(g^{-1}xg)^n = g^{-1}x^ng = g^{-1}1g = 1$, which shows that $g^{-1}xg$ is of finite order and $|g^{-1}xg| \le |x|$. However, if $|g^{-1}xg| = k$, then $(g^{-1}xg)^k = 1$ so $x^k = gg^{-1}x^kgg^{-1} = g(g^{-1}xg)^kg^{-1} = g1g^{-1} = e$, which shows that x is of finite order and $|x| \le |g^{-1}xg|$. Therefore $|x| = |g^{-1}xg|$. This also shows that if x is of infinite order, then $g^{-1}xg$ is of infinite order and vice versa.

   3) Finally, for any $x, y \in G$, $|xy| = |x^{-1}(xy)x| = |yx|$.

8. Prove that every finite group G of even order contains an element of order 2.

   Solution. Define $t(G)$ to be the set $\{g \in G \mid g \ne g^{-1}\}$. Then $t(G)$ must have an even number of elements because $g \in t(G)$ if and only if $g^{-1} \in t(G)$ and any such g, g^{-1} must be distinct. Since G also has an even number of elements, the set $G - t(G)$ has an even number of elements. Now $G - t(G)$ is nonempty since the identity $e \notin t(G)$. Therefore there is a nonidentity element $a \in G - t(G)$. But since $a \notin t(G)$, we have $a = a^{-1}$ so that $a^2 = e$ but $a \ne e$. Thus a is an element of order 2, completing the proof.

Homework 2 — Solutions

1. Determine the order of each of the elements of the dihedral group D_8.

   Solution.

1	2	4
e	r^2, s, rs, r^2s, r^3s	r, r^3

2. Suppose for some $n \ge 3$ that $z \in D_{2n}$ is a non-identity element such that $zg = gz$ for all $g \in D_{2n}$. Prove that n is even, say $n = 2k$, and $z = r^k$ where r is our order-n generator of D_{2n}.

   Solution. Element z can be written either r^ℓ or $r^\ell s$ for some integer ℓ. In the first case, consider $g = s$.

   $$zg = zs = r^\ell s = sr^{-\ell} = gz = sr^\ell$$

   so $r^{-\ell} = r^\ell \implies r^{2\ell} = e \implies \ell = 0$ or n is even and $\ell = \frac{n}{2}$.

   Now suppose consider $z = r^\ell s$. For simplicity, I will rename vertices of polygon such that now $z = s$. Now consider $g = r$.

   $$zg = zr = sr = r^{-1}s = gz = rs$$

   so $r^{-1} = r^1 \implies r^2 = e$, but we require $n \ge 3$.

   Last part we need to check that r^k commute with any element. It is obvious for r^ℓ, let's check for $r^\ell s$:

   $$r^k \cdot r^\ell s = r^\ell r^k s = r^\ell s r^{-k} = r^\ell s r^{n-k} = r^\ell s \cdot r^k.$$

3. a. Use the generators and relations to show that every element of D_{2n} which is not a power of r has order 2.

   Solution. Such elements are r^ks. r^ks is distinct from the identity, and

   $$(r^ks)^2 = r^ksr^ks = r^kr^{-k}ss = e,$$

   so $|r^ks| = 2$.

   b. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

   Solution. $r = s \cdot sr$, so both s and r can be generated from s and sr, so the whole group D_{2n} can be generated.

   c. Show that

   $$\langle a, b \mid a^2 = b^2 = (ab)^n = e\rangle$$

   gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$.

   Solution. Suppose $a^2 = b^2 = (ab)n = e$. Then $s^2 = a^2 = e$ and $r^n = (s^2r)^n = (ab)^n = e$. Since $b^2 = e$, we have $srsr = e$. Multiplying each side of this equation on the right by r^{-1} and then on the left by s gives $rs = sr^{-1}$. This shows that the relations $s^2 = r^n = 1$ and $rs = sr^{-1}$ follow from the relations for a and b.

   Now suppose $s^2 = r^n = 1$ and $rs = sr^{-1}$. Then $a^2 = s^2 = 1$, $b^2 = srsr = s^2r^{-1}r = 1$, and $(ab)^n = (s(sr))^n = (s^2r)^n = rn = 1$. Therefore the relations for a and b follow from those for r and s, so that the above is a presentation for D_{2n} in terms of a and b.

4. Prove that the group of rigid motions of a regular tetrahedron in $\mathbb{R}^3$ has order 12, and that the group of rigid motions of a regular octahedron in $\mathbb{R}^3$ has order 24.

   Solution. A tetrahedron has 4 vertices. Label them from 1 to 4. Let G be this group of motions. Then a rigid motion in G can send vertex 1 to 4 possible places. Once the new position of vertex 1 has been chosen, there are three adjacent vertices at which to place vertex 2. The positions of the remaining two vertices will then be completely determined by the positions of the first two. Therefore there are $4(3) = 12$ possible symmetries, so $|G| = 12$.

   An octahedron has 6 vertices and each vertex has 4 adjacent vertices. So, using the same reasoning as in the previous two exercises, we get $|G| = 6(4) = 24$.

5. Prove that if $\Omega = \mathbb{N}$ then the group S_Ω is infinite.

   Solution. Let n be any positive integer and consider the permutation σ_n which sends $2n - 1$ to $2n$ and sends $2n$ to $2n - 1$, while fixing all other elements in Ω. Clearly $\sigma_n \in S_\Omega$. Now, if i and j are distinct positive integers, then the numbers $2i - 1$, $2i$, $2j - 1$, $2j$ are distinct from one another, so that σ_i and σ_j have cycle decompositions that are disjoint. Thus σ_1, σ_2, ..., σ_n, ... are distinct elements in S_Ω, and therefore S_Ω is infinite.

6. Let σ and τ be the permutations

   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix},$$
   $$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}.$$

   Find the cycle decompositions and order of the following permutations: σ, τ, $\sigma\tau$, $\tau\sigma$.

   Solution.

   $$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9),$$
   $$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11),$$
   $$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 11 & 4 & 1 & 2 & 9 & 6 & 10 & 7 & 8 & 15 & 3 & 12 & 14 & 13 & 5 \end{pmatrix}$$
   $$= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14),$$
   $$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 9 & 13 & 1 & 3 & 6 & 7 & 10 & 2 & 14 & 5 & 15 & 12 & 8 & 11 \end{pmatrix}$$
   $$= (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14).$$

7. Let a be the 12-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For which positive integers i is a^i also a 12-cycle?

   Solution. By applying σ twice we can determine that $\sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$. So σ^2 is not a 12-cycle. In this way we can also determine that σ^3 and σ^4 are also not 12-cycles. However, $\sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$ so σ^5 is a 12-cycle. Continuing in this way, we can see that σ^6 consists of a product of 2-cycles, σ^7 is a 12-cycle, σ^8 is a product of 3-cycles, σ^9 is a product of 4-cycles, σ^{10} is a product of 6-cycles, and σ^{11} is a 12-cycle. It is good to use the fact that $\sigma^k = (\sigma^{12-k})^{-1}$. And higher powers will simply repeat the pattern. Therefore, σ^i is a 12-cycle for $i = 1, 5, 7, 11$ as well as any integers which have a remainder of 1, 5, 7, or 11 when divided by 12. We can also characterize these values as being precisely those values of i for which $\gcd(12, i) = 1$.

8. Prove that if a is the m-cycle $(a_1\, a_2 \ldots a_m)$, then for all $i \in \{1, 2, ..., m\}$, $a^i(a_k) = a_{k+i}$ where $k + i$ is replaced by its least residue modulo m when $k + i > m$. Deduce that $|a| = m$.

   Solution. Fix a positive integer m. We will use induction on i to show that $\sigma^i(a_k) = a_{k+i}$ for each positive integer i. Since σ cyclically permutes a_1, ..., a_m, we have $\sigma(a_k) = a_{k+1}$ for each k (taking $a_{m+1} = a_1$), so the base case is satisfied. Now suppose $\sigma_{i(a_k)} = a_{k+i}$ for some positive integer i. Then $\sigma^{i+1}(a_k) = \sigma(\sigma^{i(a_k)}) = \sigma(a_{k+i}) = a_{k+i+1}$, again replacing $k + i$ and $k + i + 1$ with their least positive residues modulo m. This completes the inductive step, so $\sigma^i(a_k) = a_{k+i}$ for each integer $i > 0$.

   Finally, if $1 \le i < m$ then σ^i sends a_1 to $a_{1+i} \ne a_1$ so that σ_i is not the identity. But σ^m sends a_k to $a_{k+m} = a_k$ for each k. Therefore $\sigma_m = 1$, which shows that $|\sigma| = m$.

Homework 3 — Solutions

1. Show that $\mathrm{GL}_2(\mathbb{F}_2)$ is non-abelian.

   Solution.

   $$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \ne \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

2. Let G consist of the invertible upper-triangular real 2×2 matrices, i.e. all matrices of the form $g(a, b, c) := \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ with $a, c \in \mathbb{R}\times$ and $b \in \mathbb{R}$).

   a. Compute the matrix product $g(a_1, b_1, c_1)g(a_2, b_2, c_2)$ to show that G is closed under multiplication. **Solution.** $g(a_1, b_1, c_1)g(a_2, b_2, c_2) = g(a_1a_2, a_1b_2 + b_1c_2, c_1c_2)$.

   b. Compute the inverse of $g(a, b, c)$ and deduce that G is closed under inverses. **Solution.** $g(a, b, c)^{-1} = g(a^{-1}, -ba^{-1}c^{-1}, c^{-1})$.

   c. Deduce that G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. **Solution.** By the problem 5 from HW1 set closed under product and inverse is a subgroup.

   d. Prove that G is not commutative, but its subset consisting of $g(a, b, c)$ with $b = 0$ is a commutative subgroup. **Solution.** For example

   $$g(1, 1, 1)g(1, 0, 2) = g(1, 2, 2) \ne g(1, 1, 2) = g(1, 0, 2)g(1, 1, 1)$$

   but $\forall a_1, a_2, c_1, c_2 \in \mathbb{R}^*$

   $$g(a_1, 0, c_1)g(a_2, 0, c_2) = g(a_1a_2, 0, c_1c_2) = g(a_2, 0, c_2)g(a_1, 0, c_1)$$

   Actually $G|_{b=0} \cong \mathbb{R}^* \times \mathbb{R}^*$.

3. a. Compute the order of each of the elements in Q_8.

   Solution.

1	2	4
1	-1	i, j, k, $-i$, $-j$, $-k$

   b. Prove that D_8 and Q_8 are not isomorphic.

   Solution. Group D_8 has 5 elements of order 2, but Q_8 only 1.

4. Let $M_{\pm 1}$, $M_{\pm i}$, $M_{\pm j}$, $M_{\pm k}$ be the following 2×2 matrices with complex entries:

   $$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad M_{-1} = -M_1; \quad M_i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \quad M_{-i} = -M_i;$$
   $$M_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad M_{-j} = -M_j; \quad M_k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad M_{-k} = -M_k.$$

   Note that M_1 is the identity matrix in $\mathrm{GL}_2(\mathbb{C})$. Check that these matrices satisfy the Q8 identities

   $$M_{-1}^2 = M_1, \quad M_i^2 = M_j^2 = M_k^2 = M_{-1}, \quad M_iM_j = M_k, \quad M_jM_i = M_{-k}.$$

   (you're welcome to use a computer algebra program for this). Deduce that these eight matrices constitute a subgroup of $\mathrm{GL}_2(\mathbb{C})$ with the same multiplication table as Q_8, and thus in particular that Q_8 is a group.

   Solution. After checking whose identities, we conclude that we can compute any product of 2 elements using them, like:

   $$M_{-j} = M_{-1}M_j \quad \text{and} \quad M_iM_k = M_i(M_iM_j) = M_j.$$

5. Let $\varphi : G \to H$ be a homomorphism.

   a. Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{N}$. **Solution.** We use induction on n. The case for $n = 1$ is clear. Suppose $\varphi(x^n) = \varphi(x)^n$ for some particular $n \in \mathbb{N}$. Then $\varphi(x^{n+1}) = \varphi(xx^n) = \varphi(x)\varphi(x^n) = \varphi(x)\varphi(x)^n = \varphi(x)^{n+1}$, so the result holds for all $n \in \mathbb{N}$.

   b. Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. **Solution.** We know that $\varphi(1_G) = 1_H$. Since the identity is preserved, we will simply use 1 to denote the identity of both groups from this point forward. Now, for any $x \in G$, $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1$, which shows that $\varphi(x^{-1}) = \varphi(x)^{-1}$. Then for $n \in \mathbb{N}$, $\varphi(x^{-n}) = \varphi((x^n)^{-1}) = \varphi(x^n)^{-1} = (\varphi(x)^n)^{-1} = \varphi(x)^{-n}$. Therefore $\varphi(x^n) = \varphi(x)^n$ holds for all $n \in \mathbb{Z}$.

6. Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$: let $\theta : \Delta \to \Omega$ be a bijection. Define

   $$\varphi : S_\Delta \to S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

   and prove the following:

   a. φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

   Solution. For any permutation σ of Δ, it is clear that $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ is a function from Ω to itself. We want to show that it is a bijection. Suppose $a, b \in \Omega$ are such that $\varphi(\sigma)(a) = \varphi(\sigma)(b)$. Since θ is an injection, this implies that $(\sigma \circ \theta^{-1})(a) = (\sigma \circ \theta^{-1})(b)$. But σ is also an injection, so $\theta^{-1}(a) = \theta^{-1}(b)$ and, similarly, we have $a = b$. This shows that $\varphi(\sigma)$ is an injection.

   Now let $y \in \Omega$ be arbitrary. Then we may take $x = \varphi(\sigma^{-1})(y) = (\theta \circ \sigma^{-1} \circ \theta^{-1})(y)$ so that $\varphi(\sigma)(x) = y$. This shows that $\varphi(\sigma)$ is a surjection. Hence $\varphi(\sigma)$ is a bijection from Ω to itself, that is, $\varphi(\sigma)$ is a permutation of Ω.

   b. φ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ.] **Solution.** Define $\psi : S_\Omega \to S_\Delta$ by $\psi(\tau) = \theta^{-1} \circ \tau \circ \theta$ for any $\tau \in S_\Omega$. By the same argument as in part (a), ψ is well-defined. Moreover, for any $\sigma \in S_\Delta$, $(\psi \circ \varphi)(\sigma) = \psi(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta = \sigma$, and for any $\tau \in S_\Omega$, $(\varphi \circ \psi)(\tau) = \varphi(\theta^{-1} \circ \tau \circ \theta) = \theta \circ \theta^{-1} \circ \tau \circ \theta \circ \theta^{-1} = \tau$. Therefore ψ is a two-sided inverse of φ, so that φ is a bijection.

   c. φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$. **Solution.** Let $\sigma, \tau \in S_\Delta$. Then $\varphi(\sigma) \circ \varphi(\tau) = \theta \circ \sigma \circ \theta - 1 \circ \theta \circ \tau \circ \theta - 1 = \theta \circ \sigma \circ \tau \circ \theta - 1 = \varphi(\sigma \circ \tau)$. Therefore φ is a homomorphism, and hence an isomorphism.

7. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of $\varphi(G)$, is a subgroup of H (cf. Exercise 5 of Homework 1). Prove that if φ is injective then $G \cong \varphi(G)$.

   Solution. Let $a, b \in \varphi(G)$ be arbitrary. Then there exist $\alpha, \beta \in G$ such that $\varphi(\alpha) = a$, and $\varphi(\beta) = b$. Then $ab = \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta)$, so $ab \in \varphi(G)$ and $\varphi(G)$ is closed under the binary operation of H. Moreover, $a^{-1} = \varphi(\alpha)^{-1} = \varphi(\alpha^{-1})$, so $\varphi(G)$ is closed under inverses. Hence $\varphi(G)$ is a subgroup of H.

   Now, if we define $\varphi^* : G \to \varphi(G)$ by $\varphi^*(\gamma) = \varphi(\gamma)$ for each $\gamma \in G$, then φ^* is surjective by definition. If, in addition, φ is injective, then φ^* is a bijection and $G \cong \varphi(G)$.

8. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the kernel of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 5 of Homework 1) of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

   Solution. We know that $\varphi(1_G) = 1_H$ so the kernel of φ is nonempty. Suppose $a, b \in \ker\varphi$. Then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H1_H = 1_H$, and $ab \in \ker\varphi$. additionally, if $a \in \ker\varphi$ then $\varphi(a^{-1}) = \varphi(a)^{-1} = 1_H^{-1} = 1_H$ and $a^{-1} \in \ker\varphi$. Therefore $\ker\varphi$ is a subgroup of G.

Homework 4 — Solutions

1. Let G be a group acting on a set A and fix some $a \in A$. Show that the $G_a = \{g \in G \mid ga = a\}$ is a subgroup of G (this subgroup is called the *stabilizer* of a in G.

   Solution. The stabilizer of a is nonempty since e is a member. Now let g, h be any members of the stabilizer. Then $(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$, so the stabilizer is closed under the group operation. It is also closed under inverses, since $a = e \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$. Therefore the stabilizer is a subgroup of G.

2. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by $a \sim b$ if and only if there exists $h \in H$ such that $a = hb$ is an equivalence relation.

   Solution. Since $a = e_Ha$ we have $a \sim a$. And if $a = hb$ for $h \in H$ then $h^{-1}a = h^{-1}(hb) = (h^{-1}h)b = b$, so $a \sim b$ implies $b \sim a$. Lastly, suppose $a \sim b$ and $b \sim c$ and let $h_1, h_2 \in H$ be such that $a = h_1b$ and $b = h_2c$. Then $a = h_1(h_2c) = (h_1h_2)c$ and $a \sim c$. Hence $\sim$ is an equivalence relation.

3. Let G be any group.

   a. Prove that $(g_1, g_2) \cdot a = g_1ag_2^{-1}$ gives an action of $G \times G$ on G. **Solution.** Identity in $G \times G$ is (e, e), so we need to check two things
   - $(e, e) \cdot a = eae^{-1} = a$,
   - $(g_1, g_2) \cdot ((h_1, h_2) \cdot a) = (g_1, g_2) \cdot (h_1ah_2^{-1}) = g_1h_1ah_2^{-1}g_2^{-1} = (g_1h_1)a(g_2h_2)^{-1} = (g_1h_2, g_2h_2) \cdot a$.

   b. Prove that the kernel of this action is $\{(g, g) \mid g \in Z(G)\}$. **Solution.** Kernel consists of elements (g_1, g_2) such that $(g_1, g_2) \cdot a = a$ for all $a \in G$.

   $$(g_1, g_2) \cdot e_G = g_1e_Gg_2^{-1} = g_1g_2^{-1} = e_G \iff g_1 = g_2$$
   $$\forall a : (g_1, g_1) \cdot a = g_1ag_1^{-1} = a \iff \forall a : g_1a = ag_1 \iff g_1 \in Z(G)$$

4. Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by $x \to gxg^{-1}$. For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an *automorphism* of G. Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$.

   Solution. Fix a $g \in G$ and let $\varphi : G \to G$ denote the map $x \mapsto gxg^{-1}$. Then for any $x_1, x_2 \in G$ we have $\varphi(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \varphi(x_1)\varphi(x_2)$ so φ is a homomorphism. Next, suppose $\varphi(x_1) = \varphi(x_2)$. Then $gx_1g^{-1} = gx_2g^{-1}$ and multiplying both sides of this equation on the left by g^{-1} and on the right by g gives $x_1 = x_2$, so that φ is injective. Now let $y \in G$ be arbitrary. Then $x = g^{-1}yg$ is such that $\varphi(x) = y$, so φ is surjective. Therefore φ is an automorphism. (Actually, conjugation by g^{-1} is inverse map).

   Since isomorphisms preserve order, we see that each element $x \in G$ has the same order as its conjugate gxg^{-1}. Moreover, if $A \subseteq G$ then the restriction of φ to A, $\varphi|_A : A \to gAg^{-1}$, is still a bijection, so $|A| = |gAg^{-1}|$.

5. Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G. **Solution.** $G = \mathbb{Z}$, $H = \mathbb{N}$. Or $G = \mathbb{Q}^\times$, $H = \mathbb{N}$.

6. a. Prove that if H and K are subgroups of G then so is their intersection $H \cap K$. **Solution.** Since $1 \in H$ and $1 \in K$, $1 \in H \cap K$ and the intersection is nonempty. For any $a, b \in H \cap K$, we must have $ab^{-1} \in H$ since $a, b \in H$ and H is a subgroup. Similarly we must have $ab^{-1} \in K$, so $ab^{-1} \in H \cap K$ and $H \cap K \le G$.

   b. Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G. [Do not assume the collection is countable.] **Solution.** Let H_α be a subgroup of G for all α belonging to some set of indices A. Let $H = \cap_{\alpha \in A} H_\alpha$. Then $1 \in H$ so H is nonempty. If $a, b \in H$, then for any α we have $a, b \in H_\alpha$, so $ab^{-1} \in H_\alpha$ and we see that $ab^{-1} \in H$ as well. Hence $H \le G$.

7. a. If $H \le G$ and $K \le G$ then $H \cup K$ is not closed under multiplication unless $H \le K$ or $K \le H$. **Solution.** Suppose $H \cup K$ is closed, i.e. for any $h \in H$, $k \in K$ we have $hk \in H \cup K$. Suppose both $H \le K$ or $K \le H$ fails, i.e. exists $h_1 \in H - K$ and $k_1 \in K - H$. We know $h_1k_1 \in H \cup K$, suppose $h_1k_1 \in H$, so $h_1^{-1}h_1k_1 \in H$, so $k_1 \in H$, contradiction.

   b. Suppose H_n $(n = 1, 2, 3, ...)$ are subgroups of G such that $H_n \le H_{n+1}$ for each n. Prove that the union $\cup_{n=1}^{\infty} H_n$ is a subgroup of G. [Do we actually need countable union here?] **Solution.** Let $H = \cup_{\infty}^{i=1} H_i$. Obviously $1 \in H$, so H is nonempty. Let $a, b \in H$. Then $a \in H_i$ for some i and $b \in H_j$ for some j. If $k = \max(i, j)$, then a and b both belong to H_k, so ab^{-1} belongs also to H_k. Therefore $ab^{-1} \in H$ as required. Hence $H \le G$.

8. Let H be a subgroup of the group G.

   a. Show that $H \subseteq N_G(H)$. **Solution.** Let $g \in H$. Since H is a subgroup and thus closed under the group operation, we have $gHg^{-1} \subseteq H$. Conversely, $H = (gg^{-1})H(gg^{-1}) = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$. Therefore $gHg^{-1} = H$ and we see that $g \in N_G(H)$. Since this is true for all $g \in H$, it follows that $H \le N_G(H)$.

   b. Give an example of a group G and a subset $A \subset G$ (necessarily not a subgroup) such that $N_G(A)$ does not contain A. **Solution.** As a counterexample for the case where H is not a subgroup, consider $G = D_4$ and $H = \{1, r, s\}$. Then $sHs^{-1} = \{1, r^3, s\} \ne H$, so $s \notin N_G(H)$ and $H \not\subseteq N_G(H)$. There is an example in $S_3 \simeq D_6$ as well.

   c. Show that $H \subseteq C_G(H)$ if and only if H is abelian. **Solution.** Suppose $H \le C_G(H)$ and let $a, b \in H$. Then $a \in C_G(H)$ so in particular, $aba^{-1} = b$, or equivalently, $ab = ba$. Therefore H is abelian. Conversely, suppose H is abelian. If $a \in H$, then $ah = ha$ for each $h \in H$. Equivalently, $aha^{-1} = h$, so that $a \in C_G(H)$. This shows that $H \le C_G(H)$.

9. Suppose $G = Q_8$, $A = \{i, -i\}$. Find $Z(G)$, $C_G(A)$, $N_G(A)$. **Solution.** i and j are not commute with each other (other pairs similarly), so $Z(Q_8) = \{1, -1\}$. Elements 1, -1, i, $-i$ are commute with elements from A, so $\{1, -1, i, -i\} \in C_{Q_8}(A)$. On the other side $jij^{-1} = ji(-j) = (-k)(-j) = (-i)$, so $j \notin C_{Q_8}(A)$ and similarly another elements, $C_{Q_8}(A) = \{1, -1, i, -i\}$. Lastly, using previous identity (-1 is in the center so we have $j(-i)j^{-1} = i$ as well) we have $j \in N_{Q_8}(A)$, so $N_{Q_8}(A) = Q_8$.