Problems

As usual, we let $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$ denote the real, rational, and complex numbers respectively, and let $\mathbf{Z}$ denote the integers. Some of these problems are taken directly from the book, and in such cases a reference to the appropriate section is given.

1. Let $G = D_{2n} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$, and let $\theta = 2\pi/n$. Prove that the map $G \to \mathrm{GL}_2(\mathbf{R})$ given by
$$T \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \qquad R \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
is a homomorphism. (1.6 (25))

2. Prove that every element in S_n can be written as a product of two-cycles. Show that every element in A_n can be written as a product of three-cycles. If $n \geq 5$, prove that every element in A_n can be written as a product of elements of the form $\sigma = (ab)(cd)$ where a, b, c, d, are distinct.

3. **Automorphism Groups**. (see 4.4) Define an automorphism of a group G to be an isomorphism $\phi : G \to G$ from G to itself.

   (a) Prove that the identity map is an automorphism.

   (b) Prove that the composition of two automorphisms is an automorphism.

   (c) Prove that the set of automorphisms forms a group under composition.

   (d) If $g \in G$ is a fixed element, prove that the map $\phi_g : G \to G$ given by $\phi_g(x) = gxg^{-1}$ is an isomorphism.

   (e) Prove that the map $\psi : G \to \mathrm{Aut}(G)$ given by $\psi(g) = \phi_g$ (sending the element g to the automorphism ϕ_g) is a homomorphism of groups.

   (f) Prove that the kernel of the map $\psi : G \to \mathrm{Aut}(G)$ is the center
$$\mathrm{Z}(G) := \{g \in G \mid gx = xg, \ \forall x \in G\}.$$

   (g) * Define the inner automorphism group $\mathrm{Inn}(G)$ of G to be the subgroup of $\mathrm{Aut}(G)$ given by the image of G under ψ. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

   (h) Show that if G is abelian then $\mathrm{Inn}(G) = \{1\}$.

   (i) Let $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Prove that

      i. $\mathrm{Aut}(\mathbf{Z}/3\mathbf{Z}) = \mathrm{Out}(\mathbf{Z}/3\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$,

      ii. $\mathrm{Out}(S_3) = \{1\}$.

      iii. $\mathrm{Aut}(K) = \mathrm{Out}(K) \simeq S_3$, where $K = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is the Klein 4-group.

4. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action (1.7 (23)).

5. Let G be the automorphism group of the octahedron. For the following sets A, determine the order $|A|$ of A, whether the action of G is faithful, and the isomorphism type of the stablizer of an element of A. Using information from the table, deduce that $G \simeq S_4$.

A	$\lvert A\rvert$	Faithful?	Stabilizer of an element of A
Edges	12		
Faces			
Vertices			
Pairs of opposite Faces			
Pairs of opposite Vertices			

6. Prove or disprove: the elements in G of order dividing p are always a subgroup of G.
7. Prove or disprove: There are only finitely many groups that act transitively on 5 points.
8. Prove or disprove: There are only finitely many groups that act faithfully on 5 points.
9. Let G be a finite group and let H be a normal subgroup. Prove that the left action of G on the coset space G/H has kernel H.
10. Let G be a finite group and let H be any subgroup. Prove that the left action of G on the coset space G/H has kernel $N := \bigcap_{g \in G} gHg^{-1}$.
11. Prove that $N := \bigcap_{g \in G} gHg^{-1}$. is the largest normal subgroup of G contained in H.
12. Determine the smallest n such that G is a subgroup of S_n for the following groups G:
    (a) $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
    (b) $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.
    (c) $G = D_6$.
    (d) $G = D_8$.
    (e) $G = D_{10}$.
    (f) $G = D_{24}$.
    (g) $G = S_4 \times \mathbf{Z}/5\mathbf{Z}$.
    (h) $G = A_5 \times A_5$.
    (i) $G = S_5 \times S_5$.
    (j) $G = \mathrm{GL}_2(\mathbf{F}_3)$.
    (k) $G = \mathbf{Z}/15\mathbf{Z}$
    (l) $G = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$
    (m) $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
    (n) $G = \mathbf{Z}/100\mathbf{Z}$.
    (o) G is the quaternion group of order 8.
13. Prove that the center of S_n is trivial if $n \geq 3$.
14. Prove that the center of A_n is trivial if $n \geq 4$.
15. Show that if $\mathrm{Z}(G) = \{1\}$ and H is a subgroup of G, then $\mathrm{Z}(H)$ is not necessarily trivial.
16. If H is a subgroup of G, define the normalizer of H to be:

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

    (a) Prove that $N_G(H) = G$ if and only if H is normal.
    (b) Prove that $N_G(H)$ contains H.
    (c) Prove that H is a *normal* subgroup of $N_G(H)$.
    (d) Compute $N_G(H)$ for the following pairs (G, H):
        i. $(D_8, \langle T \rangle)$,
        ii. $(S_4, \langle (1234) \rangle)$,

iii. $(S_5, \langle(12345)\rangle)$,

17. Prove that $\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}$ are not isomorphic.

18. Prove that $\mathbf{Q} \times \mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Q}$ are not isomorphic.

19. Prove that if G is any group, there is a bijection from the set of homomorphisms from $\mathbf{Z}$ to G and elements of G, given by $\phi : \mathbf{Z} \to G$ goes to $\phi(1)$. (2.3 (19)).

20. Prove that if H is a subgroup of G then $\langle H \rangle = H$.

21. Exhibit a proper subgroup of $\mathbf{Q}$ which is not cyclic (2.4 (15)).

22. Prove that if $G/\mathrm{Z}(G)$ is cyclic then G is abelian. (For a hint, see 3.1 (36)).

23. Let G be a group. Let N be a normal subgroup of G. Let $\overline{x}$ and $\overline{y}$ denote the images of x and y in G/N. Prove that $\overline{x}$, $\overline{y}$ commute in G/N if and only if $x^{-1}y^{-1}xy \in N$. (3.1 (40)).

24. Prove that the subgroup N generated by elements of the form $x^{-1}y^{-1}xy$ for all x, $y \in G$ is normal. (3.1 (41)).

25. Prove that if H and K are finite subgroups of G whose orders are relatively coprime then $H \cap K = \{1\}$. (4.2 (8)).

26. Prove that $\mathbf{Q}$ has no proper subgroups of finite index. (4.2 (21)).

27. Let C be a group. Let B be a normal subgroup of C, and let A be a normal subgroup of B. Show by example that A need not be a normal subgroup of C.

28. Suppose that the map $\phi : G \to G$ given by $\phi(x) = x^2$ is a homomorphism. Prove that G is abelian.

29. Let G be a finite group. Prove that G is equal to the union of its proper subgroups if and only if it is not cyclic.

30. Let G be a finite group, and let $H \subset G$ be a subgroup of index two — i.e. $|G|/|H| = 2$. Prove that H is normal.

31. Let G be a finite group, and let $H \subset G$ be a subgroup of index three — i.e. $|G|/|H| = 3$. Show that H is not necessarily normal.

32. Let G be a finite group. Prove that G admits a subgroup H of index n if and only if G acts transitively on a set A of cardinality n.

33. Let G be a group, and let $N \subseteq G$ be the subgroup generated by the elements $xyx^{-1}y^{-1}$ for all pairs x, $y \in G$. Prove that N is a normal subgroup, and that G/N is abelian.

34. Decide whether the following pairs of groups are isomorphic.

    (a) $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/6\mathbf{Z}$.

    (b) A_4 and D_{12}.

    (c) S_5 and $S_4 \times \mathbf{Z}/5\mathbf{Z}$.

    (d) A_5 and $A_4 \times \mathbf{Z}/5\mathbf{Z}$.

    (e) $A_5 \times \mathbf{Z}/2\mathbf{Z}$ and S_5.

35. Let p be an odd prime number. Prove that S_n does not contain a normal subgroup of index p for any n. (Hint: consider the image of the two-cycles.)

36. Let p be an odd prime number. Prove that A_n does not contain a normal subgroup of index p for any $n \geq 5$. (Do not use the fact that A_n is simple in this case, unless you also prove this fact.)

37. Let $G = S_5$, and let $H = \langle (12345) \rangle$.

    (a) Compute the left coset $[(143)H]$.

    (b) Compute the right coset $[H(51)]$.

38. Let $G = S_5$, and let $H = \langle (35), (325) \rangle$.

    (a) Compute the left coset $[(143)H]$.

    (b) Compute the right coset $[H(51)]$.

39. Show that the 2-Sylow subgroup of S_4 is isomorphic to D_8.

40. Show that the 2-Sylow subgroup of A_4 is isomorphic to the Klein 4-group.

41. Show that the 2-Sylow subgroup of S_5 is isomorphic to D_8.

42. Show that the 2-Sylow subgroup of A_5 is isomorphic to the Klein 4-group.

43. Let p be prime, and let $G = \mathrm{GL}_2(\mathbf{F}_p)$ be the group of invertible 2×2 matrices modulo p. Prove that $|G| = (p^2 - 1)(p^2 - p)$.

44. Let p be prime, and let $G = \mathrm{GL}_n(\mathbf{F}_p)$ be the group of invertible $n \times n$ matrices modulo p. Prove that $|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

45. Let H be the subset of $\mathrm{GL}_3(\mathbf{F}_p)$ of matrices of the form:

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}.$$

    (a) Prove that H is a subgroup of $\mathrm{GL}_3(\mathbf{F}_p)$.

    (b) Prove that $|H| = p^3$.

    (c) Show that H is not commutative.

    (d) Prove that H is a p-Sylow subgroup of $\mathrm{GL}_3(\mathbf{F}_p)$.

    (e) Prove that H is not normal.

    (f) Generalize this problem to $\mathrm{GL}_n(\mathbf{F}_p)$.

46. Let $H = \langle x, y \rangle \subset S_n$ be generated by the 3-cycles x and y. Prove that either:

    - $H \simeq \mathbf{Z}/3\mathbf{Z}$.
    - $H \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.
    - $H \simeq A_4$.
    - $H \simeq A_5$.

    See (3.5 (17)).

47. Let G be a finite group acting on a set A. For $a \in A$, let $G_a = \mathrm{Stab}(a)$.

    (a) If $\sigma \in G$, prove that
    $$G_{\sigma(a)} = \sigma G_a \sigma^{-1}.$$

    (b) Fix $a \in A$. If the action of G is transitive, prove that the kernel of the action is
    $$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1}.$$
    Hint: show that any element in A is of the form $\sigma(a)$ for some $\sigma \in G$.

    (c) If the action of G on A is transitive and faithful, deduce that
    $$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{1\}.$$

    (d) If G is *abelian*, and the action of G on A is transitive and faithful, deduce that $G_a = \{1\}$ for any $a \in A$.

    (e) Prove that if an abelian group G acts transitively and faithfully on a finite set A, then $|G| = |A|$.

    See (4.1 (2)).

48. Let H be a finite subgroup of G of index n. Let A be the set of left cosets G/H, and consider the left action of G on A.

    (a) Let $n = |G/H|$, and consider the associated homomorphism $G \to S_{G/H} \simeq S_n$. Prove that the kernel of this map is a subgroup of H.

    (b) By considering the kernel of the map $G \to S_n$, deduce that G contains a normal subgroup N contained in H of index dividing $n!$ and divisible by n.

    See (4.2 (8))

49. Let $\sigma = (12345) \in S_5$. Find an element $\tau \in S_5$ satisfying the following properties:

    (a) $\tau\sigma\tau^{-1} = \sigma^2$.

    (b) $\tau\sigma\tau^{-1} = \sigma^{-1}$.

    (c) $\tau\sigma\tau^{-1} = \sigma^{-2}$.

    See (4.3 (10))

50. Find the order of the commutator of the following elements g in the following groups G.

    (a) (1234) in S_4

    (b) (1234) in S_5

    (c) (12)(34)(56) in S_7

    (d) (12)(34) in S_7

    (e) (12)(34) in A_7.

    (f) (12345) in A_7.

    (g) A rotation of order n in D_{2n}

    (h) $((12), (123))$ in $S_5 \times S_5$.

51. Let G be the symmetry group of the dodecahedron.

    (a) Determine the stabilizer of G on the vertices.

    (b) Determine the stabilizer of G on the edges.

    (c) Using either (a) or (b), deduce that $|G| = 60$.

    (d) Prove that G acts faithfully on the pairs of opposite faces.

    (e) Deduce that G is a transitive subgroup of S_6.

    (f) Construct a set A (geometrically or otherwise) of order $|A| = 5$ so that G acts faithfully on A.

    (g) Deduce that G is a subgroup of S_5.

    (h) Deduce that $G \simeq A_5$.

    (i) Construct an action of A_5 on 6 points which is transitive.

52. Prove that the symmetry group of the cube is isomorphic to the symmetry group of the octahedron.

53. Prove that the symmetry group of the dodecahedron is isomorphic to the symmetry group of the icosahedron.

54. Let $G = \mathrm{SL}_2(\mathbf{F}_3)$. Prove that the subgroup H generated by

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle$$

    is the unique 2-Sylow subgroup of G. (4.5 (10)).

55. Suppose that P is a p-Sylow subgroup of G. Prove that P is the unique such subgroup if and only if it is normal.

56. Suppose that P is a normal p-Sylow subgroup of G. Suppose that H is a subgroup of G. Prove that $P \cap H$ is the unique p-Sylow subgroup of H. (4.5 (31)).

57. Prove that $\mathrm{SL}_2(\mathbf{F}_4) \simeq A_5$. (4.5 (41)).

58. Prove that there is a surjective map $\mathrm{SL}_2(\mathbf{F}_5) \to A_5$. What is the kernel?

59. Prove that there is a surjective map $\mathrm{SL}_2(\mathbf{F}_9) \to A_6$. What is the kernel?

60. Suppose $\phi : S_n \to S_m$ is surjective. Prove that either:

    (a) $m = 2$,

    (b) $n = 4$ and $m = 3$,

    (c) $n = m$.

61. Which of the following elements are in A_5?

    (a) (23)

    (b) (23)(34)

    (c) (12345)

    (d) (123)(234)

62. Prove that there do not exist any simple groups of the following orders.

    (a) 30
    (b) 72
    (c) 132
    (d) 144
    (e) 200
    (f) 300
    (g) 1176

63. Prove that if $n < p^2$, the p-Sylow subgroup of S_n is abelian. Prove that if $n \geq p^2$, the p-Sylow subgroup of S_n is *not* abelian.

64. Let P be a p-Sylow subgroup of S_{p^2}. Compute the center $\mathrm{Z}(P)$ of P.

65. Let p be prime, and let $G = S_p$.

    (a) Prove that $n_p = (p-2)!$. (Hint: compute the number X of elements of order p and deduce that the number n_p of groups of order p inside G is $X/(p-1)$.)
    (b) Deduce Wilson's Theorem: $(p-2)! \equiv 1 \mod p$ for all primes p.
    (c) The group $P = \langle (1, 2, 3, 4, \ldots, p) \rangle$ is a p-Sylow subgroup of G. If N is the normalizer of P, show that $|N| = p(p-1)$. Show that elements of N can be described explicitly as those which send $x \mod p$ to $ax + b \mod p$ for some $a \not\equiv 0 \mod p$, where $i \mod p$ is interpreted to be an element of the set $\{1, 2, 3, 4, \ldots, p\}$.

66. Prove that if N is a normal subgroup of G, and the largest power of p dividing $|N|$ is equal to the largest power of p dividing $|G|$, then the number of p-Sylow subgroups of N is equal to the number of p-Sylow subgroups of G.

67. Let $G = \mathrm{GL}_3(\mathbf{F}_2)$ be the group of 3×3 matrices with coefficients modulo two. Let A denote the 7 vectors: $(1,0,0)$, $(1,0,1)$, $(1,1,0)$, $(1,1,1)$, $(0,1,0)$, $(0,1,1)$, $(0,0,1)$.

    (a) Prove that G acts transitively on A, by the usual action of matrices on vectors.
    (b) Prove that G acts faithfully on A.
    (c) Prove that G has order $(2^3-1)(2^3-2)(2^3-4) = 168$.
    (d) Exhibit a p-Sylow subgroup for $p = 2$, 3 and 7.
    (e) Prove that the 2-Sylow subgroups of G are isomorphic to D_8.
    (f) Let S be the stabilizer of $(1,0,0)$. Prove that $|S| = 24$, and that $S \simeq S_4$.
    (g) Show there is no surjective morphism from S_4 to $\mathbf{Z}/3\mathbf{Z}$.
    (h) Deduce that there is no surjective morphism ϕ from G to $\mathbf{Z}/3\mathbf{Z}$, since the kernel of ϕ would contain S.
    (i) Prove that $n_7 > 1$, and hence that $n_7 = 8$.
    (j) Let N be a normal subgroup of G. Show that if $7 \mid |N|$, then $56 || N|$. Show that G does not contain a normal subgroup of order 56, and hence, if N is proper, that $|N| \mid 24$.
    (k) Let P be a 3-Sylow subgroup of G, and let $N_G(P)$ be the normalizer of P. Prove that $|N_G(P)| \geq 12$. (Hint: show that one may assume that $P \subset S$, show that $N_S(P) \subset N_G(P)$, and use the fact that $S = S_4$.)

(l) Deduce that $n_3 \mid 14$, and by explicitly showing that $n_3 \neq 1$, that $n_3 = 7$.

(m) Suppose that $3 \mid |N|$. Prove that $7 \mid |N|$ (Hint: show that all the 3-Sylow subgroups of G lie in N, and hence that $n_3 \mid |N|$.)

(n) Deduce that if N is a normal subgroup, then $|N| \mid 8$, and thus N is contained in one (and hence any) 2-Sylow subgroup.

(o) Deduce that $N \subset S$, and hence N stabilizes $(1, 0, 0)$.

(p) Using that N is normal, deduce that N stabilizes all elements of A.

(q) Conclude that G is a simple group.

68. Automorphisms of S_n.

(a) Let $\psi : G \to G$ be an isomorphism. If $\langle c \rangle$ is a conjugacy class of G, prove that the image $\psi(\langle c \rangle)$ of $\langle c \rangle$ under ψ is the conjugacy class $\langle \psi(c) \rangle$.

(b) Deduce that $|\langle c \rangle| = |\langle \psi(c) \rangle|$.

(c) Let $G = S_n$. Prove that $|\langle (12) \rangle| = n(n-1)/2$.

(d) If $n \neq 6$, and $\sigma \in S_n$ has order 2, prove that $|\langle \sigma \rangle| = |\langle (12) \rangle|$ if and only if σ is a 2-cycle.

(e) Deduce that if $\psi : S_n \to S_n$ is an isomorphism, and $n \neq 6$, then ψ takes 2-cycles to 2-cycles.

(f) Suppose that $\psi(12) = (ij)$, prove that, after possibly swapping i and j, that $\psi(13) = (ik)$ for some $k \notin \{i, j\}$.

(g) Deduce that, after composing ψ with an inner automorphism (i.e. conjugation), one has $\psi(12) = (12)$ and $\psi(13) = (13)$.

(h) Assume that $\psi(1i) = (1i)$ for all $i < k$, with $k > 3$. Prove that $\psi(1k) = (1j)$ for some $j \geq k$. Deduce that, after composing with an inner automorphism, that $\psi(1k) = (1k)$.

(i) Deduce that ψ is the identity, and hence that any automorphism of S_n (for $n \neq 6$) is given by conjugation, i.e., $\mathrm{Out}(S_n) = 1$ for $n \neq 6$.

69. The "exotic" automorphism of A_6.

(a) Thinking of A_n inside S_n, if $\sigma \in S_n$, prove that the map $\psi : A_n \to A_n$ given by conjugation by σ is well defined and is an automorphism.

(b) Prove that A_5 has $n_5 = 6$, and show that this gives rise to a morphism $\phi : A_5 \to S_6$.

(c) Prove that the image of ϕ has order 120 and lands in A_6. Call this image H.

(d) Prove H (which is isomorphic to A_5) is not conjugate to any of the "natural" copies of A_5 in A_6, generated by elements that stabilize a point.

(e) Since $[A_6 : H] = 6$, the action of A_6 on left cosets gives rise to a homomorphism $A_6 \to S_6$. Prove that the image is exactly A_6, and hence we have constructed an automorphism $A_6 \to A_6$.

(f) Prove that this automorphism is *not* given by conjugation by some element of S_6. (Hint: consider the image of H under this automorphism).

70. A_n is simple for $n \geq 5$. Assume that $n \geq 5$, and that H is a normal subgroup of A_n.

(a) Prove that A_n is generated by 3-cycles.

(b) Prove that, if $n \geq 5$, that for any three cycle (a, b, c), there exists an element σ of A_n such that

$$\sigma(a, b, c)\sigma^{-1} = (x, y, z)$$

for any distinct x, y, and z.

(c) Deduce that if H contains a 3-cycle, then H contains all 3-cycles, and hence $H = A_n$.

(d) Suppose that $\sigma = (a_1, a_2, a_3, a_4, \ldots)(\ldots)$ contains a cycle of length ≥ 4. Prove that σ is conjugate (in A_n) to $\tau = (a_2, a_3, a_1, a_4, \ldots)(\ldots)$, where all the other entries of σ remain unchanged.

(e) Show that $\sigma\tau^{-1} = (a_1, a_4, a_2)$, and deduce that either $H = A_n$ or all the cycles in the cycle decomposition of $\sigma \in H$ have length ≤ 3.

(f) Suppose that $\sigma = (a, b, c)(d, e, f)\ldots$ contains at least two 3-cycles. Prove that σ is conjugate (in A_n) to $\tau = (a, b, d)(e, c, f)\ldots$, where all the other entries of σ remain unchanged.

(g) Show that $\tau\sigma = (a, d, c, b, f)\ldots$, and, by part (e), deduce that either $H = A_n$ or all the cycles in the cycle decomposition of $\sigma \in H$ have at most one 3-cycle and are otherwise composed of 2-cycles.

(h) If the cycle decomposition of σ is a 3-cycle times a product of 2-cycles, show that σ^2 is 3-cycle. Deduce that either $H = A_n$ or that all the cycles in the cycle decomposition of $\sigma \in H$ are products of 2-cycles.

(i) Suppose that $\sigma = (a, b)(c, d)(e, f)\ldots$. Prove that σ is conjugate to $\tau = (a, c)(e, b)(d, f)\ldots$.

(j) Show that $\tau\sigma = (a, e, d)(c, f, b)\ldots$, and by part (g), deduce that either $H = A_n$ or that all the cycles in the cycle decomposition of $\sigma \in H$ consist of at most two 2-cycles.

(k) Deduce that if H is normal, then every non-trivial element of H has cycle decomposition $(a, b)(c, d)$.

(l) If $n \geq 5$, prove that $\sigma = (a, b)(c, d)$ is conjugate to $\tau = (a, e)(c, d)$, and deduce from the fact that $\sigma\tau = (a, b, e)$ that the only normal subgroup of A_n for $n \geq 5$ is either A_n or is trivial.

71. Imprimitive subgroups. Let G act on a set A of n points. Recall that G is imprimitive (equivalently, not primitive) if and only if there does exists a decomposition

$$A = \coprod A_i$$

of A into distinct sets A_i such that:

(a) There is at least one i such that $|A_i| \geq 2$.

(b) If $g \in G$ and a, $a' \in A_i$, then $g.a$ and $g.a'$ both lie in A_j for some j.

(a) If G is not transitive, prove that G is not imprimitive by taking A_i to be the orbits of G.

(b) If G is 2-transitive, prove that G is primitive.

(c) If G is transitive, but not primitive, prove that $|A_i| = |A_j|$ for all i and j.

(d) Deduce that if G is transitive, and $|A|$ is prime, then G is primitive.

(e) Suppose that G is transitive, imprimitive, and acts faithfully on A.

i. Let B denote the set of sets $\{A_i\}$. Prove that G acts transitively on B.

ii. Show there exists integers a, b, and n such that $|A| = n$, $|B| = b$, $|A_i| = a$ for all i, and $ab = n$.

iii. Let H denote the kernel of G acting on B. Prove that H is isomorphic to a transitive subgroup of $(S_a)^b = S_a \times S_a \times \ldots S_a$.

iv. Prove that G/H is isomorphic to a subgroup of S_b.

v. Deduce that G has order dividing $b! \cdot (a)!^b$.

vi. * Let N be any group which acts faithfully and transitively on a points, and let Γ be any group which acts faithfully and transitively on b points. Prove that there is a group $N \wr \Gamma$ which acts faithfully, transitively, and imprimitively on a set A of order $n = ab$ points, where G preserves a decomposition of A into sets A_i of order $|A_i| = a$.

vii. Prove that if $G = N \wr \Gamma$, then $H = N^b$ and $G/H = \Gamma$ respectively.

viii. Prove that G is subgroup of $S_a \wr S_b$.

(f) Let G be the group of shuffles generated by the two up and down riffle shuffles.

i. Prove that G acts transitively on the set of 52 cards.

ii. Prove that G acts imprimitively, by showing that A can be decomposed into the sets $A_i = (i, 53 - i)$ for $i = 1$ to 26.

iii. Deduce that G is a subgroup of $S_2 \wr S_{26}$.

iv. Deduce that G has order dividing $2^{26}26! = 270644318171066643800402165760000000$. (In fact, it turns out that $G \simeq S_2 \wr S_{26}$).

(g) Prove that the 2-Sylow of S_4 is $S_2 \wr S_2$.

(h) Prove that the 3-Sylow of S_9 is $\mathbf{Z}/3\mathbf{Z} \wr \mathbf{Z}/3\mathbf{Z}$.

(i) If N is the p-Sylow of S_{p^n}, prove that $N \wr \mathbf{Z}/p\mathbf{Z}$ is the p-Sylow of $S_{p^{n+1}}$.

(j) Deduce that any p-group is a subgroup of $\mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \ldots \mathbf{Z}/p\mathbf{Z}$.

(k) Deduce that any p-group is solvable.

72. The Rubix Cube.

(a) Find out what a Rubix cube is.

(b) Let G be the group defined by the possible combinations of moves.

(c) Prove that the action of G on the $9 \cdot 6 = 54$ has orbits of size 24, 24, and 6 orbits of size 1.

(d) Prove that G admits a quotient N which is a subgroup of S_{24} by showing that some quotient acts faithfully on the corner squares.

(e) Prove that the action of N on the corner squares is imprimitive, by taking A_i to be the triples of squares along each corner.

(f) Deduce that N is a subgroup of $S_3 \wr S_8$, and hence $|N|$ divides $3!^8 \cdot 8! = 67722117120$.

(g) Prove that the action of N on the 8 corners of the cube gives a surjection of N into S_8.

(h) Prove that the stabilizer H in N of the cubes always preserves the orientation of the triple of colours around the corners, and hence that H is actually a subgroup of $(\mathbf{Z}/3\mathbf{Z})^8$.

(i) Deduce that N is a subgroup of $(\mathbf{Z}/3\mathbf{Z}) \wr S_8$, and hence $|N|$ divides $3^8 \cdot 8! = 264539520$.

(j) Let M be the quotient on which G acts on the edge squares of the cube. Prove that M is a subgroup of S_{24}.

(k) Prove that M acts imprimively on the set of edges, since it preserves the squares on each pair.

(l) Deduce that M is a subgroup of $\mathbf{Z}/2\mathbf{Z} \wr S_{12}$.

(m) Prove that G is a subgroup of $M \oplus N$.

(n) Deduce that G is a subgroup of

$$(\mathbf{Z}/3\mathbf{Z}) \wr S_8 \oplus (\mathbf{Z}/2\mathbf{Z}) \wr S_{12},$$

and hence that G has order dividing

$$|G| = 3^8 \cdot 8! \cdot 2^{12} \cdot 12! = 519024039293878272000.$$

(In fact, it turns out that G has index 12 in this group.)