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. Many are taken directly from homework from this or previous years.

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

      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.

2. Let $A = (\mathbf{Z}/p\mathbf{Z})^n$ be the direct product of n copies of $\mathbf{Z}/p\mathbf{Z}$. Prove that $\mathrm{Aut}(A) = \mathrm{GL}_n(\mathbf{F}_p)$.

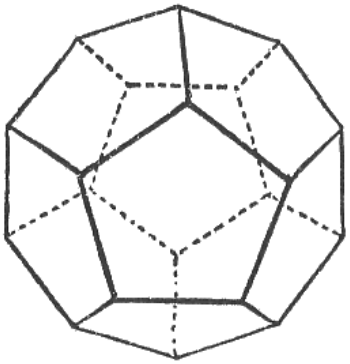
3. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action (1.7 (23)).

4. 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			

5. Let D denote the symmetry group of the Dedecahedron:

   Fill out the missing entries in the table below for various sets X on which D acts transitively. Since the action of D is transitive for each X, all stabilizers S for any point $x \in X$ are conjugate to the stabilizers of any other point. Hence they are isomorphic as subgroups; simply list a group isomorphic to any of the stabilizers.



Dodecahedron.

X	$\lvert X\rvert$	Faithful?	Stabilizer S of any x	Order of S
Dodecahedra	1	No	$S = D \simeq A_5$	60
Inscribed cubes				
Pairs of opposite faces				
Faces				
Vertices				
Edges				

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) $G = Q_8$.

(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) $G = \mathrm{GL}_2(\mathbf{F}_3)$

13. Suppose that $\mathbf{Z}/m\mathbf{Z}$ is a subgroup of S_n for some n. Prove that D_{2m} is also a subgroup of S_n.

14. Let $G = (\mathbf{Z}/m\mathbf{Z})^\times$ denote the integers co-prime to m modulo m under multiplication. Prove that G is an group. Let $\phi(m)$ denote the order of this group, so $\phi(m)$ is the number of integers less than m and co-prime to m.

15. Let $(a, m) = 1$. Prove that $a^{\phi(m)} \equiv 1 \mod m$.

16. Prove that $\mathrm{Aut}(\mathbf{Z}/m\mathbf{Z}) = (\mathbf{Z}/m\mathbf{Z})^\times$.

17. Let $x = (1, 2, \ldots, m)$, and $H = \langle x \rangle \subset S_m$. Let C denote the centralizer of $x \in S_m$, and let N denote the normalizer of H in S_m.

    (a) Prove that $C = H$.

    (b) Prove that $|N| = m\phi(m)$, and that $N/H \simeq (\mathbf{Z}/m\mathbf{Z})^\times$.

    (c) Let q be a prime which divides $\phi(m)$. Prove that N/H contains an element y of order q.

    (d) Let G denote the group generated by x and y. Prove that $|G| = qm$.

    (e) Prove that G is *not* abelian. (Hint: use the fact that $C = H$.)

    (f) Specialize to the case where $m = p$ is prime, and q divides $\phi(p) = p - 1$. Deduce that G is a group of order pq which is not abelian.

18. For each pair (G, A) consisting of a group G and a subset $A \subset G$, determine whether or not A is a left coset of G for some subgroup H.

    (a) $G = S_5$; A the set of elements such that $\sigma(1) = 3$ and $\sigma(3) = 4$.

    (b) $G = S_5$; A the set of elements $\sigma \in G$ such that $\sigma^2 = e$.

    (c) G and H any groups, ψ a surjective homomorphism $\psi : G \to H$; A the set $\psi^{-1}(h)$ for some fixed $h \in H$, where
    $$\psi^{-1}(h) := \{g \in G \mid \phi(g) = h\}.$$

    (d) $G = \mathrm{GL}_2(\mathbf{R})$ the group of invertible 2×2 matrices;
    A is the set of matrices $M \in G$ of determinant $\det(M) = 2$.

19. (a) Find an explicit group G with a normal subgroup H such that G has no subgroups which are isomorphic to G/H.

    (b) Find such an example where G is finite.

20. 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))

21. Prove that the center of S_n is trivial if $n \geq 3$.

22. Prove that the center of A_n is trivial if $n \geq 4$.

23. Show that if $\mathrm{Z}(G) = \{1\}$ and H is a subgroup of G, then $\mathrm{Z}(H)$ is not necessarily trivial.

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

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

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

27. How many conjugacy classes of S_6 contain an element of order 2? Determine the number of elements of S_6 of order exactly 2.

28. Let x, y be elements of a group G. Prove or disprove: the order of xy is always equal to the order of yx.

29. Let G be a group, and let x and y be two fixed elements in G which we assume are conjugate to each other. Let A denote the subset of elements in G such that $gxg^{-1} = y$. Prove that A is a left coset of H for **some** subgroup $H \subset G$.

30. Determine whether the following pairs of groups are isomorphic or not:

    (a) The groups $\mathbf{R}^\times$ and $\mathbf{C}^\times$ — these are defined to be the non-zero real and complex numbers respectively under the group operation of multiplication in both cases.

    (b) The groups S_5 and $A_5 \times \mathbf{Z}/2\mathbf{Z}$.

31. 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)).

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

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

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

35. Suppose that G is a group of order p^2. Prove that G is abelian. (Hint: prove that $\mathrm{Z}(G)$ is non-trivial, and use the previous question.)

36. Prove that, for any prime p, there exists a group G of order p^3 which is not abelian.

37. 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)).

38. 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)).

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

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

41. 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.

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

43. 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.

44. 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.

45. 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.

46. 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.

47. 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.)

48. 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.)

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

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

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

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

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

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

51. 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)).

52. 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)).

53. 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))

54. 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))

55. Find the order of the centralizer 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 $S_5 \times S_5$.

56. 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.

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

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

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

(a) $m = 1$ or 2,

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

(c) $n = m$.

60. Which of the following elements are in A_5?

(a) (23)

(b) (23)(34)

(c) (12345)

(d) (123)(234)

61. There are two riffle shuffles of a deck of 52 cards A and B obtained as follows: divide the deck into the top 26 and bottom 26 cards. Then interweave the two decks card by card. (There are two different shuffles depending on whether the top card from the top deck ends up on top, or the top card from the bottom deck ends up on top. If we denote the shuffles by A and B respectively, then we saw in class that $A^8 = 1$ and $B^{52} = 1$. Determine whether every permutation of 52 cards can be obtained by some combination of riffle shuffles.

62. Shuffling Redux. Let G be the subgroup of S_{52} generated by the following elements:

- $(n, 53-n)$ for all n.
- The element $(1, 2, \ldots, 26)(52, 51, \ldots, 27)$ of order 26.
- The element $(1, 2)(51, 52)$.

(a) Prove that the elements of the form $(n, 53-n)$ generate the a subgroup H isomorphic $(\mathbf{Z}/2\mathbf{Z})^{26}$ inside S_{52}.

(b) Show that there is a homomorphism from G to the group S_{26}, such that:

i. The homomorphism is surjective.

ii. The kernel is precisely the subgroup H.

(It follows from this that G has order $2^{26} \cdot 26! = 270644318171066643800402165760000000$.)

(c) Prove that the group generated by the two riffle shuffles is a subgroup of G. (In fact, they are equal.)

(d) Prove that G is the normalizer of H inside S_{52}.

63. Everybody Shuffling. Let $\mathrm{Sh}_n \subset S_{2n}$ be the group generated by the (analogues) of the top and bottom riffle shuffle A and B.

(a) Prove that $Sh_n \to S_n$ acts on the set of n parts of cards $(k, 2n+1-k)$. Deduce that there is a homomorphism $\psi_n : \mathrm{Sh}_n \to S_n$.

(b) Prove that $|\mathrm{Sh}_n|$ divides $2^n \cdot n!$

(c) (*) If $2n = 2^k$, prove that $|\mathrm{Sh}_n| = k \cdot 2^k$.

(d) If $2n = 24$, prove that Sh_{12} is generated by the two elements:

$$(1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13)(5, 10, 20, 15),$$

$$(2, 3, 5, 9, 17, 10, 19, 14, 4, 7, 13)(6, 11, 21, 18, 12, 23, 22, 20, 16, 8, 15)\rangle,$$

and that the image G of Sh_{12} in S_{12} is generated by

$$(1, 2, 4, 8, 9, 7, 11, 3, 6, 12)(5, 10),$$

$$(2, 3, 5, 9, 8, 10, 6, 11, 4, 7, 12).$$

(e) (**) Prove that the group $G \subset S_{12}$ of part (63d) has order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$.

64. **The hypercube group**. Let H_n denote the subgroup of $\mathrm{O}(n)$ which preserves the hypercube in $\mathbf{R}^n$, with vertices $(\pm 1, \pm 1, \ldots, \pm 1)$.

(a) Prove that $H_2 \simeq D_8$.

(b) Prove that $H_3 \simeq S_4 \times S_2$.

(c) Prove that there is a surjection from H_n to S_n with kernel $(\mathbf{Z}/2\mathbf{Z})^n$.

(d) Prove that H_{26} is isomorphic to the group G of question 62, and H_n contains the group Sh_n as a subgroup.

65. Let $n > 1$. Let x and y be two elements chosen randomly from S_n. Prove that the probability that $G = \langle x, y\rangle$ is equal to S_n is bounded above by $3/4$.

66. **The Orthogonal Group.** For two vectors $\mathbf{v}$ and $\mathbf{w}$ in $\mathbf{R}^n$, let $\langle \mathbf{v}, \mathbf{w} \rangle$ denote the usual dot product of $\mathbf{v}$ and $\mathbf{w}$, so, if $\mathbf{v} = (v_i)$ and $\mathbf{w} = (w_i)$, then $\langle \mathbf{v}, \mathbf{w} \rangle := \sum v_i w_i$. If $M = [a_{ij}]$ is a matrix with coefficients in $\mathbf{R}$, let M^T denote the transpose of M, which is the matrix $[a_{ji}]$.

(a) Let $\mathrm{O}(n) \subset M_n(\mathbf{R})$ denote the set of matrices M such that $MM^T = I$. Prove that $\mathrm{O}(n)$ is a group. (Hint: show that $(AB)^T = B^T A^T$).

(b) Prove that every element in $\mathrm{O}(n)$ has determinant 1 or -1. Let $\mathrm{SO}(n) \subset \mathrm{O}(n)$ denote the matrices $M \in \mathrm{O}(n)$ such that $\det(M) = 1$. Prove that $\mathrm{SO}(n)$ is a group.

(c) Show that any element $M \in \mathrm{SO}(2)$ is of the form $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where a and b are real numbers satisfying $a^2 + b^2 = 1$. Prove that, for such a and b, one can find a unique $\theta \in [0, 2\pi)$ such that $a = \cos(\theta)$ and $b = \sin(\theta)$, and that M is rotation by θ around the origin.

(d) Show that any element of $M \in \mathrm{O}(2)$ not in $\mathrm{SO}(2)$ has the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$. Prove that these elements also have the following properties:

i. M^2 is the identity.

ii. M is a reflection through some line that passes through the origin $(0, 0)$.

iii. If M and N are elements of $\mathrm{O}(2)$ not in $\mathrm{SO}(2)$ then $MN \in \mathrm{SO}(2)$ is a rotation.

(e) Let $\mathbf{u}$ be any non-zero vector in $\mathbf{R}^3$ of length one, so $\|\mathbf{u}\|^2 = \langle \mathbf{u}, \mathbf{u} \rangle = 1$. The vectors $\mathbf{v}$ with $\langle \mathbf{u}, \mathbf{v} \rangle = 0$ live inside the plane orthogonal to $\mathbf{u}$. Show that, with $\mathbf{u}_1 = \mathbf{u}$, there exist vectors $\mathbf{u}_i$ for $i = 1, 2, 3$ in $\mathbf{R}^3$ which are orthonormal and mutually orthogonal, that is, $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$ for $i \neq j$, and $\|\mathbf{u}_i\|^2 = \langle \mathbf{u}_i, \mathbf{u}_i \rangle = 1$. Suppose that $M \in \mathrm{SO}(3)$ is a matrix such that $M\mathbf{u} = \mathbf{u}$. Prove that

$$M\mathbf{u}_1 = \mathbf{u}_1, \ M\mathbf{u}_2 = a\mathbf{u}_2 + b\mathbf{u}_3, \ M\mathbf{u}_3 = -b\mathbf{u}_2 + a\mathbf{u}_1,$$

for some a, b with $a^2 + b^2 = 1$ and $a = \cos(\theta)$ and $b = \sin(\theta)$, and deduce that M is a rotation around the line $\mathbf{u}$ with angle θ.

(f) Prove that any matrix M has the same eigenvalues as the transpose matrix M^T (Hint: show that M and M^T have the same characteristic polynomial). Prove that if M is invertible, then the matrix M^{-1} has eigenvalues which are the inverses of the eigenvalues of M.

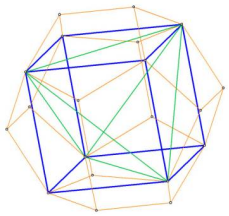
(g) Deduce that if $M \in \mathrm{SO}(3)$, then $M^{-1} = M^T$, and then use part (66f) to deduce that 1 is an eigenvalue of M.

(h) Deduce that every element in $\mathrm{SO}(3)$ is a rotation around some line $\mathbf{u}$ passing through the origin. Deduce that the composition of a rotation in $\mathbf{R}^3$ in some line $\mathbf{u}$ passing through the origin with rotation in any second line $\mathbf{v}$ also passing through the origin is also a rotation through some third line $\mathbf{w}$ passing through the origin. (Here $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ need not be distinct.)

67. If σ is an element of S_n, then σ has a cycle decomposition into disjoint cycles of various lengths (let us include 1-cycles). Since disjoint cycles commute, the shape of the element is determined by the lengths of the various cycles, which we can assume are put in decreasing order. Any two elements with the same cycle shape are conjugate, so the conjugacy classes are determined by writing n ($= 52$ say) as a sum of decreasing integers.

(a) Find the conjugacy class in S_{52} with the largest number of elements.

(b) Find the conjugacy class in S_{52} which contains the element of largest order.



68. Let $k \leq n$ be even. Prove that every element in S_n can be written as a product of k-cycles.

69. Let D be a regular dodecahedron. It is possible to inscribe a cube on the vertices of D thus:

    (a) Prove that one can inscribe exactly 5 such cubes (of these lengths with vertices in these positions) inside D.

    (b) Deduce that any rigid motion of D (i.e. an element of SO(3) sending D to itself) permutes the 5 cubes. Let Do denote the group of symmetries of D, so this action gives a map from D to S_5.

    (c) Prove that any rigid motion in Do which sends sends all of the five cubes to themselves (and preserves D) must be the identity map on D. Warning! note that "fixing every cube" does not mean that every vertex of the cube is fixed, simply that each cube ends up in the same place but possibly rotated.

    (d) Deduce that the symmetry group Do of the dodecahedron is a subgroup of S_5 of order 60.

70. Embed the cube inside $\mathbf{R}^3$ so that the centers of each face are at $A = (1, 0, 0)$, $B = (-1, 0, 0)$, $C = (0, 1, 0)$, $D = (0, -1, 0)$, $E = (0, 0, 1)$, and $F = (0, 0, -1)$. Considering the symmetry group of C as a subgroup of SO(3), write down the matrix of SO(3) corresponding to the following elements:

    (a) $\sigma = (A, C, E)(B, D, F)$

    (b) $\tau = (C, E, D, F)$

    (c) $\sigma\tau = (A, C, E)(B, D, F)(C, E, D, F) = (A, C)(B, D)(E, F)$

71. Let $\sigma \in S_n$ be an n-cycle, and let $\tau \in S_n$ be a 2-cycle. Show by constructing a counterexample that σ and τ need not generate S_n.

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

73. Let G be any group, and consider the direct product $G \times G$. Let Δ denote the subgroup $\Delta \subset G \times G$ consisting of pairs (g, g) for any $g \in G$. Prove that Δ is a normal subgroup if and only if G is abelian.

74. Let G be a finite group, and let n denote the smallest integer such that G is isomorphic to a subgroup of S_n. Either prove that n divides the order of $|G|$, or give an explicit counterexample of a group G which does not have this property.

75. 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)).

76. Let G be a finite group, and let $g \in G$ and $h \in G$ have orders 2 and 2 respectively. Prove that gh can have any possible finite order.

77. Let G be a finite group, and let $g \in G$ and $h \in G$ have orders 2 and 3 respectively. Determine the possible orders of gh.

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

79. 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.

80. 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 $|G| = (p^2 - 1)(p^2 - p)$.

81. Let H and K be normal subgroups of G such that $H \cap K$ is trivial. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. (3.1, (42)).

82. Show that S_4 does not have a normal subgroup of order 3 or order 8.

83. Let A be an abelian group of order 2^{100}. Prove that A is not a subgroup of S_n for $n < 200$.

84. 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. $(S_4, \langle(1234)\rangle)$,
        ii. $(S_5, \langle(12345)\rangle)$,

85. 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)).

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

87. 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.

88. 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.

89. Let p be an odd prime number. Prove that S_n does not admit a surjective homomorphism to $\mathbf{Z}/p\mathbf{Z}$ for any n. (Hint: consider the image of the two-cycles.)

90. 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 replacing ψ by $\psi_g\psi$ where ψ_g is carefully chosen inner automorphism (given by conjugation by g for some g), 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 replacing ψ again by $\psi_g\psi$ for some g, that $\psi(1i) = (1i)$ for all $i \leq k$.

(i) Deduce that ψ is the identity, and hence that the original ψ was a product of inner automorphisms, and thus $\mathrm{Out}(S_n) = \mathrm{Aut}(S_n)/\mathrm{Inn}(S_n) = 1$ for $n \neq 6$.

91. A_n is simple for $n \geq 5$. Assume that $n \geq 3$, and that H is a normal subgroup of A_n.

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

(b) Prove that for any two three cycles (a, b, c) and (x, y, z) (warning; the sets $\{a, b, c\}$ and $\{x, y, z\}$ may not be disjoint), there exists an element σ of A_n such that

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

(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 proper, 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 $\tau\sigma = (a, b, e)$ that the only normal subgroup of A_n for $n \geq 5$ is either A_n or is trivial.

92. 4.1 (7,8), 4.2 (8,9).

93. Let G be a group and H a subgroup. Let A be a ***left*** coset of H in G. Let

$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

Prove that A^{-1} is a ***right*** coset of H in G.

94. The action of $G = S_n$ on itself by left multiplication induces a homomorphism ϕ

$$\phi : S_n = G \longrightarrow S_G \simeq S_{n!}$$

Determine the cycle decomposition of $\phi((12)(34))$.

95. Let A and B be normal subgroups of G, and suppose that the intersection $A \cap B$ consists only of the identity. Prove that if $a \in A$ and $b \in B$ then a and b commute, that is, $ab = ba$.

96. Let $G = S_6$, and let $\sigma = (12)(34)(56) \in G$. Let

$$C_G(\sigma) = \{g \mid g \in G,\ g\sigma = \sigma g\}$$

be the centralizer of σ.

(a) Prove that $|C_G(\sigma)| = 48$.

(b) Determine whether $C_G(\sigma)$ is isomorphic to $S_4 \times S_2$ or not.

97. Suppose that G acts transitively and faithfully on a finite set X, and that G is abelian. Prove that $|G| = |X|$. Show that the equality need not hold if G is not abelian.

98. **The Quaternions.** Let $\mathbf{H} = \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$ be a 4-dimensional vector space over $\mathbf{R}$. Define a non-commutative associative multiplication structure on $\mathbf{H}$ by the formulae

$$ij = -ji = k, jk = -kj = i, ki = -ik = j; \quad i^2 = j^2 = k^2 = -1.$$

(a) Show that there is a map ϕ from $\mathbf{H}$ to 2×2 matrices $M_2(\mathbf{C})$ over $\mathbf{C}$ by sending

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

so that:

i. ϕ is injective as a map of vector spaces over $\mathbf{R}$

ii. ϕ respects multiplication; if q_1 and q_2 are two quaternions then $\phi(q_1 q_2) = \phi(q_1)\phi(q_2)$. This should reduce easily enough to the case when q_i and q_j are elements of the set $\phi(1), \phi(i), \phi(j), \phi(k)$. The map ϕ is not a group homomorphism since 0 is not an invertible quaternion, but we shall see below in part (98c) hat non-zero quaternions form a group, so ϕ restricted to $\mathbf{H}^\times$ is actually a homomorphism from $\mathbf{H}^\times$ to $\mathrm{GL}_2(\mathbf{C})$.

(b) Define the conjugate of a quaternion $q = a + bi + cj + dk$ by $\overline{q} := a - bi - cj - dk$. Prove that $N(q) := q\overline{q} = a^2 + b^2 + c^2 + d^2$.

(c) Prove that non-zero quaternions $\mathbf{H}^\times$ form a group under multiplication.

(d) Let $Q = \langle i, j \rangle$ be the subgroup of $\mathbf{H}^\times$ generated by i and j. Prove that Q is a group of order 8. (Q is known as the "quaternion group".)

(e) Prove that every subgroup of Q is normal.

(f) Let Γ be the subgroup of $\mathbf{H}^\times$ generated by the elements of Q together with $\dfrac{1+i+j+k}{2}$. Prove that Γ is a group of order 24.

(g) Prove that Γ is *not* isomorphic to S_4, and Q is *not* isomorphic to D_8. In fact, $\Gamma = \mathrm{SL}_2(\mathbf{F}_3)$.

(h) Construct a surjective homomorphism from Γ to A_4.

(i) Prove that the subgroup $\mathbf{H}^1$ of quaternions q with $N(q) = 1$ is a subgroup of $\mathbf{H}^\times$. Deduce that the 3-sphere $S^3 \subset \mathbf{R}^4$ defined by $a^2 + b^2 + c^2 + d^2 = 1$ has a natural structure of a group. Note that S^1 also has a natural group structure given by rotations in SO(2). It turns out that S^n has a natural (= continuous) group structure only for $n = 1$ and $n = 3$.

(j) Say that a quaternion is *pure* if it is of the form $bi + cj + dk$, i.e. $a = 0$. We may identify pure quaternions with $\mathbf{R}^3$. Show that if u is a pure quaternion then quq^{-1} is still a pure quaternion for any $q \in \mathbf{H}^\times$.

(k) Prove that the action of q on $\mathbf{R}^3$ by $q.u = quq^{-1}$ is via element of SO(3), and deduce that there is a homomorphism $\mathbf{H}^\times \to \mathrm{SO}(3)$.

(l) Prove that the restriction of this homomorphism to $\mathbf{H}^1 \to \mathrm{SO}(3)$ is surjective and has kernel of order 2.

99. **Projective Linear Groups over Finite Fields.** Let p be prime, and let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Note that one can add and multiply elements of $\mathbf{F}_p$. Let $\mathrm{GL}_2(\mathbf{F}_p)$ be the group of invertible matrices over $\mathbf{F}_p$, and let $\mathrm{SL}_2(\mathbf{F}_p) \subset \mathrm{GL}_2(\mathbf{F}_p)$ denote the subgroup of matrices of determinant one.

(a) There are $p^2 - 1$ non-zero vectors $v \in \mathbf{F}_p^2$. Let a "line" $\ell = [v] \subset \mathbf{F}_p^2$ denote the scalar multiples λv of a non-zero vector v. Prove that the set X of lines has cardinality $|X| = p+1$.

(b) Prove that $\mathrm{SL}_2(\mathbf{F}_p)$ and $\mathrm{GL}_2(\mathbf{F}_p)$ act naturally on X by $g.[v] = [g.v]$.

(c) Prove that this action is transitive for both $\mathrm{GL}_2(\mathbf{F}_p)$ and $\mathrm{SL}_2(\mathbf{F}_p)$.

(d) Prove that the kernel of the action consists precisely of the scalar matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ in either $\mathrm{SL}_2(\mathbf{F}_p)$ or $\mathrm{GL}_2(\mathbf{F}_p)$.

(e) Let $\mathrm{PGL}_2(\mathbf{F}_p)$ and $\mathrm{PSL}_2(\mathbf{F}_p)$ denote the quotient of G and H by the subgroup of scalar matrices. Prove that $|\mathrm{PGL}_2(\mathbf{F}_p)| = (p^2 - 1)p$ and $|\mathrm{PSL}_2(\mathbf{F}_p)| = 6$ if $p = 2$ and $\frac{1}{2}(p^2 - 1)p$ otherwise.

(f) Prove that $\mathrm{PGL}_2(\mathbf{F}_2) = \mathrm{PSL}_2(\mathbf{F}_2) = S_3$.

(g) Prove that $\mathrm{PGL}_2(\mathbf{F}_3) = S_4$ and $\mathrm{PSL}_2(\mathbf{F}_3) = A_4$.

(h) Prove that $\mathrm{PSL}_2(\mathbf{F}_5) = A_5$ and $\mathrm{PGL}_2(\mathbf{F}_5) = S_5$. (Hint: using that A_6 is simple, prove that any index 6 subgroup of A_6 or S_6 is A_5 or S_5 respectively).

100. Suppose that $\mathbf{Z}/m\mathbf{Z}$ is a subgroup of S_n for some n. Prove that D_{2m} is also a subgroup of S_n.

101. 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)).

102. (See (4.2 (8))) 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 $n = |A|$, and consider the associated homomorphism $G \to S_A \simeq S_n$. 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.

103. 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.

104. 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.

105. Compute the order of the following groups as well as a set of generators:

(a) The centralizer of (12345) in A_7.

(b) The centralizer of $((12), (123))$ in $S_5 \times S_5$.

(c) The normalizer of $H = \langle (12), (34), (56), (78) \rangle$ in S_8.

106. The "exotic" automorphism of S_6. You may use the fact proved in class that, for $n \geq 5$, the only normal subgroups of S_n are the trivial group, A_n, and S_n.

(a) Let $G = S_5$. Prove that there are 24 elements of G of order 5, and 6 subgroups of G of order 5. Prove they are all conjugate.

(b) Let $P = \langle (12345) \rangle \subset G = S_5$. Prove that the normalizer $N = N_G(P)$ of P has order 20. (Hint: use the Orbit–Stabilizer Theorem to determine the order of N.)

(c) Show that the left action of G on G/N gives rise to a homomorphism $\phi : G \to S_6$.

(d) Prove that ϕ is injective, and deduce that $G \simeq \mathrm{im}(\phi)$.

(e) Prove that $\mathrm{im}(\phi)$ inside S_6 is not one of the "natural" copies of S_5 in S_6 given by subgroups which stabilize a point. (Hint: use the fact that the action in part 106c is transitive.) It is an "exotic" copy of S_5 inside S_6.

(f) Since $[S_6 : \mathrm{im}(\phi)] = 6$, show that the left action of S_6 on $S_6/\mathrm{im}(\phi)$ gives rise to a homomorphism $\psi : S_6 \to S_6$.

(g) Prove that ψ is injective and deduce that ψ is automorphism.

(h) Prove that the the image of the exotic $S_5 \simeq \mathrm{im}(\phi) \subset S_6$ maps under ψ to a copy of $S_5 \subset S_6$ which stabilizes a point.

(i) Deduce that ψ is *not* given by conjugation by some element of S_6.

(j) Prove that $\mathrm{Out}(S_6) = \mathbf{Z}/2\mathbf{Z}$ is generated by ψ. Hint: by using results from Problem 90, show that any automorphism of S_6 which is not inner must send the conjugacy class $(**)$ to $(**)(**)(**)$ and send $(**)(**)(**)$ to $(**)$. Deduce that the product of any two elements in $\mathrm{Aut}(S_6)$ not in $\mathrm{Inn}(S_6)$ are inner, and hence trivial in $\mathrm{Out}(S_6)$.

(k) Prove that the group $\mathrm{Aut}(S_6)$ has order $2 \times 6! = 1440$.

107. 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 primitive 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 $G \simeq S_2 \wr S_{26}$).

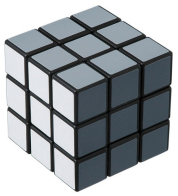
108. The Rubix Cube.

(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.)

109. Let G be any group, and consider the direct product $G \times G$. Let Δ denote the subgroup $\Delta \subset G \times G$ consisting of pairs (g, g) for any $g \in G$. Prove that Δ is a normal subgroup if and only if G is abelian.

110. Let G be a finite group, and let n denote the smallest integer such that G is isomorphic to a subgroup of S_n. Either prove that n divides the order of $|G|$, or give an explicit counterexample of a group G which does not have this property.

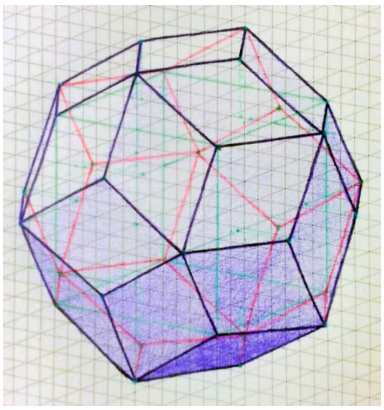
111. The Rhombic Triacontahedron. Let Ri denote the symmetry group of the Rhombic Triacontahedron R (pictured above). The solid R has of 30 faces of R which all all isometric rhombi, but the vertices come in two flavours: one where three faces meet and a second where five faces meet.

(a) Show that Ri acts transitively on the 30 faces of R which all all isometric rhombi.

(b) Show that R has 60 edges, and that Ri acts transitively on the set of edges.

(c) Show that R has 32 vertices, and that the action of Ri has two orbits of size 20 and 12 respectively.

(d) Prove that Ri $\simeq$ Ic $\simeq$ Do is A_5.



112. Sylow Subgroups as imprimitive groups.

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

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

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

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

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

113. **For this question, do not assume the Sylow Theorems.** Let G be a finite group, and suppose that G has a p-Sylow subgroup $|P|$. Let H be a subgroup of G. Suppose that

$$|H| = p^m \cdot A, \quad \text{where } A \text{ is an integer prime to } p,$$

$$|G| = p^{m+n} \cdot AB, \quad \text{where } A \text{ and } B \text{ are integers prime to } p.$$

(a) There is an action of G on G/H by left multiplication. Restricting this action to P, one obtains an action by P on G/H by left multiplication. For this action of P on $X = G/H$, prove there exists at least one element $x \in X$ such that the orbit $\mathrm{Orbit}_P(x)$ of x under P satisfies:

$$|\mathrm{Orbit}_P(x)| \not\equiv 0 \mod p^{n+1}.$$

(b) Suppose that p^n exactly divides $\mathrm{Orbit}_P(x)$. Prove that the stabilizer $Q := \mathrm{Stab}_P(x)$ is a subgroup of P of order exactly p^m.

(c) With $Q = \mathrm{Stab}_P(x)$ of order p^m as above, write $x = gH \in X = G/H$. Prove that $g^{-1}Qg$ is a p-Sylow subgroup of H. (This shows that, in order to prove Sylow I for a group H, it suffices to prove it for a group G with $H \subset G$. For example, one can reduce to the case when $G = S_n$ for some n.)

114. Let $G = S_6$, so $|G| = 720$.

(a) Prove that any 2-Sylow subgroup of G is isomorphic to $H = D_8 \times \mathbf{Z}/2\mathbf{Z}$.

(b) Let $g = (1, 2, 3, 4) \in G$. Prove that there exists a 2-Sylow subgroup P such that $Q = \langle g \rangle$ is contained in P.

(c) Prove that there are precisely 45 subgroups of G generated by 4-cycles.

(d) Prove that the normalizer $N_G(Q)$ of Q in G has order 16. (Hint: consider the action of G by conjugation on subgroups of G generated by 4-cycles).

(e) Prove that the normalizer $N_G(P)$ of P is equal to P. (Hint: prove that $Q \subset P$ is the unique subgroup of P generated by a 4-cycle).

(f) Compute the number n_2 of 2-Sylow subgroups of G.

115. Prove that $\mathrm{SL}_2(\mathbf{F}_3)$ and S_4 are not isomorphic.

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

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

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

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

120. 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) Determine the number n_p of P-Sylow subgroups of $\mathrm{GL}_3(\mathbf{F}_p)$.

(g) Determine the normalizer of H.

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

121. 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)).

122. 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)).

123. 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.

124. Let $\mathbf{F}_2$ denote the field with three elements. Define $\mathbf{F}_4$ to consist of sums $a + b\omega$, where i is a new symbol which satisfies $\omega^2 + \omega + 1 = 0 \mod 2$. Under addition, $\mathbf{F}_4$ has the structure of the group $(\mathbf{Z}/2\mathbf{Z})^2$, but is also closed under multiplication, which commutes with addition in all the expected ways. Moreover, the multiplication is commutative. (The relationship between $\mathbf{F}_4$ and $\mathbf{F}_2$ is similar to the relationship between $\mathbf{C}$ and $\mathbf{R}$.)

(a) Show that $\omega^3 = 1$.

(b) Show that $N(a+b\omega) = (a+b\omega)(a+b\omega^2) = a^2+ab+b^2$ is never zero in $\mathbf{F}_2$ unless $a = b = 0$.

(c) Deduce that every non-zero element $z = a + b\omega \in \mathbf{F}_4$ has a multiplicative inverse z^{-1} such that $z \cdot z^{-1} = 1$.

(d) Prove that the set of invertible matrices $\mathrm{GL}_2(\mathbf{F}_4)$ and matrices $\mathrm{SL}_2(\mathbf{F}_4)$ with determinant one are groups of orders $(4^2-1)(4^2-4) = 180$ and $4(4^2-1) = 60$ respectively.

(e) Arguing as in question 99, show that there are 5 lines in $\mathbf{F}_4^2$, and construct quotient groups $\mathrm{PGL}_2(\mathbf{F}_4)$ and $\mathrm{PSL}_2(\mathbf{F}_4)$ of orders 60 and 60 respectively.

(f) Prove that $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4) = A_5$.

125. Let $\mathbf{F}_3$ denote the field with three elements. Define $\mathbf{F}_9$ to consist of sums $a + bi$, where i is a new symbol which satisfies $i^2 = -1 = 5 \bmod 3$. Under addition, $\mathbf{F}_9$ has the structure of the group $(\mathbf{Z}/3\mathbf{Z})^2$, but is also closed under multiplication, which commutes with addition in all the expected ways. Moreover, the multiplication is commutative. (The relationship between $\mathbf{F}_9$ and $\mathbf{F}_3$ is similar to the relationship between $\mathbf{C}$ and $\mathbf{R}$.)

(a) Show that $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$ is never zero in $\mathbf{F}_3$ unless $a = b = 0$.

(b) Deduce that every non-zero element $z = a + bi \in \mathbf{F}_9$ has a multiplicative inverse z^{-1} such that $z \cdot z^{-1} = 1$.

(c) Prove that the set of invertible matrices $\mathrm{GL}_2(\mathbf{F}_9)$ and matrices $\mathrm{SL}_2(\mathbf{F}_9)$ with determinant one are groups of orders $(9^2-1)(9^2-9) = 5760$ and $9(9^2-1) = 720$ respectively.

(d) Arguing as in question 99, show that there are 10 lines in $\mathbf{F}_9^2$, and construct quotient groups $\mathrm{PGL}_2(\mathbf{F}_9)$ and $\mathrm{PSL}_2(\mathbf{F}_9)$ of orders 720 and 360 respectively.

126. Suppose that G is a p-group, and $H \subset G$ has index p. Prove that H is normal in G.

127. 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.

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

129. 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, or equivalently, since $p-1 \equiv -1 \mod p$, that $(p-1)! \equiv -1 \mod p$.

(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 $\{1,2,3,4,\ldots,p\}$.

130. 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.

131. Prove that there do not exist any simple groups of the following orders. (Warning: not in order of difficulty)

(a) 30

(b) 72

(c) 90

(d) 112

(e) 120

(f) 126

(g) 132

(h) 140

(i) 144

(j) 150

(k) 156

(l) 200

(m) 300

(n) 336

(o) 1176

(p) 2907

(q) 6545

132. Let N be a normal subgroup of G, and suppose that the largest power of p dividing $|N|$ is equal to the largest power of p dividing $|G|$. Prove that the p-Sylow subgroups of G are precisely the p-Sylow subgroups of N.

133. (Small Index Subgroups of A_n and S_n)

(a) Prove that there is a transitive action of A_n and S_n on $\binom{n}{2}$ points. (This is optimal for actions on $m > n$ points for S_n for $n > 6$ and A_n for $n > 8$.)

(b) Prove that there is a transitive actions of A_6 and S_6 on 10 points.

(c) (*) Prove that there is a transitive action of A_7 on 15 points. (Hint: show that the group $\mathrm{GL}_3(\mathbf{F}_2)$ acts on 7 points)

(d) (*) Prove that there is a transitive action of A_8 on 15 points. (Hint: show that the group

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix} \cap \mathrm{GL}_4(\mathbf{F}_2)$$

acts on 8 points.