Exercise 1. If $\pi, \tau \in S_n$, then $\pi\tau$ and $\tau\pi$ have the same cycle structure. ($S_n$ denotes the symmetric group of degree $n$.)

Notation: $\exp(x) = e^x$. Two sequences $a_n$ and $b_n$ are asymptotically equal, denote by $a_n \sim b_n$, if $\lim_{n \to \infty} a_n/b_n = 1$.

The Hardy-Ramanujan formula says that $p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right)$.

Exercise 2. $\log p(n) = \Theta(\sqrt{n})$, where $p(n)$ is the partition function.

Exercise 3. $H \leq G$ if and only if $H \neq \emptyset$ and $HH^{-1} \subseteq H$.

Exercise 4. $H \leq G$ implies $HH = H = H^{-1} = HH^{-1}$.

Exercise 5. The intersection of any number of subgroups of a group $G$ is again a subgroup of $G$. (“Any number” could be infinitely many.)

Exercise 6. The number of left cosets of $H$ in $G$ is equal to the number of right cosets of $H$ in $G$. (Hint: find a bijection. Note that the correspondence $aH \mapsto Ha$ does not work. Why?)

Exercise 7. If $G$ is finite then there exists $R \subseteq G$ which is simultaneously a set of left coset representatives of $H$ and a set of right coset representatives of $H$.

Exercise 8. All subgroups of $\mathbb{Z}$ are of the form $a\mathbb{Z}$.

Exercise 9. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ where $m = \text{lcm}(a, b)$. 
Exercise 10. \( a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \) where \( d = \gcd(a, b) \).

Exercise 11. If \( G \) is a finite subgroup of the multiplicative group of a field then \( G \) is cyclic.

Exercise 12. (a) Look up Euler’s \( \varphi \) function.

(b) Let \((\mathbb{Z}/m\mathbb{Z})^\times\) denote the group of units of the ring \( \mathbb{Z}/m\mathbb{Z} \), i.e., those \( \mod m \) residue classes that are relatively prime to \( m \). Prove that this is a group (of order \( \varphi(m) \)).

Exercise 13. Recall that the order of \( a \in G \) is denoted \( |a| \) is defined to be the order of the subgroup \( \langle a \rangle \).

(a) The order of \( a \) is \( m \) if and only if \( m \) is the smallest positive integer such that \( a^m = e \).

(b) \( a^k = e \) if and only if \( m \mid k \).

(c) The order of \( a^\ell \) is \( m/\gcd(\ell, m) \).

Exercise 14. Define the commutator \([a, b] = a^{-1}b^{-1}ab\). Prove that \( a \) and \( b \) commute if and only if \([a, b] = e \).

Exercise 15. If \([a, b] = e \) then \( |ab| \mid \text{lcm}(|a|, |b|) \).

Exercise 16. If \([a, b] = e \) and \( \gcd(|a|, |b|) = 1 \) then \( |ab| = |a| \cdot |b| \).

Exercise 17. If \([a, b] = e \) then
\[
\frac{\text{lcm}(|a|, |b|)}{\gcd(|a|, |b|)} \mid |ab| \mid \text{lcm}(|a|, |b|).
\]

Exercise 18. Every subgroup of a cyclic group is cyclic.

Exercise 19. Lagrange’s Theorem says that if \( H \leq G \) then \( |G| = |H| \cdot |G : H| \). Prove: if \( G \) is finite then \((\forall g \in G)(g^{|G|} = e)\).

Exercise 20. (Euler-Fermat congruence) Recall that \( a \equiv b \pmod m \) means \( m \mid a - b \). Prove the Euler-Fermat congruence as a consequence of the preceding exercise: If \( \gcd(a, m) = 1 \) then \( a^\varphi(m) \equiv 1 \pmod m \).

Exercise 21. Two cyclic groups are isomorphic if and only if they have the same order. In particular, all infinite cyclic groups are isomorphic to \((\mathbb{Z}, +)\).
Exercise 22. \((\mathbb{Q}, +)\) is not finitely generated, but every finitely generated subgroup is cyclic.

Exercise 23. * (Quasicyclic group) Find an infinite commutative group \(G\) such that every proper subgroup of \(G\) is finite cyclic. (Hint: Look inside \(\mathbb{C}^*\).)

Exercise 24. Recall that \(D_n\) is the dihedral group of order \(2n\), which is defined as the symmetry group of the regular \(n\)-gon. Let \(C_n\) be the subgroup of rotations. Show that \(|D_n : C_n| = 2\). The next three exercises will help.

Exercise 25. If \(r, s\) are reflections with axes at angle \(\theta\) then \(rs\) is a rotation by angle \(2\theta\).

Exercise 26. In \(D_n\) there are two reflections whose product has order \(n\).

Exercise 27. The order \(|rs| < \infty\) if and only if \(\theta/(2\pi) \in \mathbb{Q}\).

Exercise 28. The transpositions generate the symmetric group \(S_n\).

Exercise 29. Neighbor swaps generate \(S_n\): \(\langle (1, 2), (2, 3), \ldots, (n-1, n) \rangle = S_n\).

Exercise 30. If \(\tau_1, \ldots, \tau_m\) are transpositions which generate \(S_n\) then \(m \geq n - 1\).

Exercise 31. The number of sets of \(n - 1\) transpositions that generate \(S_n\) is \(n^{n-2}\).

Exercise 32. Let \(\tau_1, \cdots, \tau_m\) be transpositions. If \(\tau_1 \cdots \tau_m = e\) then \(2 \mid m\).

Exercise 33. If \(\sigma\) is even then it is not odd.

Exercise 34. \(|S_n : A_n| = 2\). Here \(A_n\) denotes the alternating group of degree \(n\) (set of even permutations in \(S_n\)).

Exercise 35. Let \(G \leq \text{Sym}(A)\) be a permutation group acting on the set \(A\) (\(A\) is called the permutation domain). Let \(a, b \in A\). We say \(a \sim b\) if there exists \(\pi \in G\) such that \(a^\pi = b\). Show that this is an equivalence relation on \(A\). The equivalence classes are called the orbits of \(G\). The orbit of \(a\) is the set \(a^G = \{a^\pi \mid \pi \in G\}\).
Exercise 36. Define \( G_{a \to b} = \{ \pi \in G : a^\pi = b \} \). Show that the right cosets of \( G_a \) are the \( G_{a \to b} \), and that \(|G_{a \to b}| = |G_a|\) when \( b \in a^G \).

Exercise 37. \(|G : G_a| = |a^G|\).

Exercise 38. Let \( O(n) \) denote the group of orthogonal transformations of \( \mathbb{R}^n \). Define the subgroup \( SO(n) \) consisting of the orientation preserving orthogonal transformations. Prove: \(|O(n) : SO(n)| = 2\).

Exercise 39. For a subset \( S \subset \mathbb{R}^n \) let \( G \leq O(n) \) consist of the symmetries of \( S \), i.e., \( G = \{ g \in O(n) \mid S^g = S \} \). Let \( G^+ = G \cap SO(n) \), the subgroup of orientation preserving transformations in \( G \). Then show \(|G : G^+| \leq 2\).

Exercise 40. Show that \( \text{Aut}^+(Q_3) \simeq S_4 \), where \( Q_3 \) is the cube (centered at the origin) and \( \text{Aut}^+ \) is the group of orientation preserving symmetries.

Exercise 41. The automorphism group of a tetrahedron is isomorphic to \( S_4 \), and the orientation preserving subgroup is isomorphic to the alternating group \( A_4 \).

Exercise 42. A \( k \)-cycle is even if and only if \( k \) is odd.

Exercise 43. The 3-cycles generate \( A_n \).

Exercise 44. If \( G \leq S_n \) and \(|S_n : G| = 2\) then \( G = A_n \).

Exercise 45. The automorphism group of the Petersen graph is isomorphic to \( S_5 \).

Exercise 46. The automorphism group of the dodecahedron (a) has order 120, but (b) is not isomorphic to \( S_5 \). (Hint: an element of a group \( G \) is central if it commutes with all elements of \( G \). Prove that the automorphism group of the dodecahedron contains nonidentity central element, but \( S_5 \) does not contain such an element.)

Exercise 47. The orientation preserving part of the automorphism group of the dodecahedron is isomorphic to \( A_5 \).

Exercise 48. Let \( K \leq H \) such that \(|H : K| = 2\). Show that \((\forall b \in H)(b^2 \in K)\).

Exercise 49. (a) If \( K \leq H \) with \(|H : K| = 3\), then show that \( b \in H \) does not necessarily imply \( b^3 \in K \) by finding a counterexample. (Hint: your counterexample should be in a very small, familiar group.)
(b) If $K \triangleleft H$ with $|H : K| = 3$, then show that $(\forall b \in H)(b^3 \in K)$.

**Definition 1.** For $a, b \in G$ we define the **commutator** of $a$ and $b$ as $[a, b] = a^{-1}b^{-1}ab$.

**Definition 2.** For a group $G$, we define the center of $G$ as

$$Z(G) = \{ z \in G : (\forall g \in G)[g, z] = e\}.$$

**Exercise 50.** Show that $Z(G)$ is a subgroup of $G$.

**Exercise 51.** Let $G = \text{Aut}(\text{Cube})$. Show that $Z(G) = \{\text{id}, -\text{id}\}$ where $-\text{id}$ is the “central reflection” discussed in class.

**Definition 3.** Let $f : G \to H$. Then $f$ is a **homomorphism** if $(\forall x, y \in G)(f(xy) = f(x)f(y))$. Define the **image** of $f$ by $\text{im}(f) = \{f(x) : x \in G\} = f(G)$. Define the **kernel** of $f$ by $\ker(f) = \{x \in G : f(x) = e_H\} = f^{-1}(e_H)$.

**Exercise 52.** Let $f : G \to H$ be homomorphism. Let $K = \ker(f)$. Show that the set $G/K$ of cosets of $K$ in $G$ is in bijection with $\text{im}(f)$. That is, show $f(x) = f(y)$ if and only if $Kx = Ky$. Conclude $|\text{im}(f)| = |G : K|$.

**Exercise 53.** Note that an automorphism $\phi \in \text{Aut}^+(\text{Cube})$ permutes the four main diagonals of the cube. Thus $\phi$ defines a permutation $\sigma \in S_4$. Define $f : \text{Aut}^+(\text{Cube}) \to S_4$ as the mapping which takes an automorphism $\phi$ to the permutation $\sigma$ of diagonals it defines. Show $\text{im}(f) = S_4$. (Hint: It suffices to show that all transpositions are in the image.)

**Exercise 54.** For $n \geq 3$, show that $|Z(S_n)| = 1$.

**Exercise 55.** Prove that $\text{Aut}^+(\text{Dodecahedron}) \cong A_5$. (Hint: Find 5 geometric objects in the dodecahedron which are permuted by $\text{Aut}^+(\text{Dodecahedron})$.)

**Definition 4.** The **conjugate** of $g \in G$ by $a \in G$ is $g^a = a^{-1}ga$. Conjugation by a fixed element $a$ gives an automorphism $\gamma_a : g \mapsto g^a$.

**Exercise 56.** Prove that the assignment

$$
\gamma : G \longrightarrow \text{Aut}(G)
\begin{array}{c}
a \\
\mapsto \gamma_a
\end{array}
$$

is a homomorphism. That is, $\gamma_{ab} = \gamma_a \gamma_b$.  


Exercise 57. Show that $\ker(\gamma) = Z(G)$, i.e., $\gamma_a = \text{id}$ if and only if $a \in Z(G)$.

Definition 5. Let $\text{Inn}(G) = \{ \gamma_a : a \in G \}$, the set of inner automorphisms of $G$.

Exercise 58. Show $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.

Exercise 59. Let $H \leq G$. Then $H^a = a^{-1}Ha$. Show $H^a$ is a subgroup of $G$. Show that $H^a \cong H$.

Definition 6. A subgroup $H \leq G$ is normal if $(\forall a \in G)(H^a = H)$. In other words, $(\forall a \in G)(Ha = aH)$. We denote this circumstance by $H \unlhd G$.

Exercise 60. If $f : G \to H$ is a homomorphism, then show $\ker(f) \lhd G$.

Definition 7. If $N \leq G$ then we have $G/N = \{ Ng : g \in G \}$, the set of right cosets of $N$ in $G$. In the case $N \lhd G$ then $G/N$ is a group called the quotient group. The group operation is defined by $NxNy = Nxy$.

Exercise 61 (The First Isomorphism Theorem). If $f : G \to H$ is a homomorphism then prove that $G/\ker(f) \cong \text{im}(f)$.

Exercise 62. Show $\text{Inn}(G) \lhd \text{Aut}(G)$.

Definition 8. We define the outer automorphisms by $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$.

Exercise 63. Show $Z(G) \lhd G$.

Definition 9. We say $g$ and $h$ are conjugates, tentatively denoted by “$g \sim h$,” if there exists $a \in G$ such that $g^a = h$.

Exercise!!! 64. Prove that $\sigma_1, \sigma_2 \in S_n$ are conjugates in $S_n$ if and only if they have the same cycle structure. (Hint: Start by proving the conjugate of a 3-cycle is a 3-cycle.)

Exercise 65. In $O(n)$, the orthogonal group (the set of orthogonal transformations of $\mathbb{R}^n$), a conjugate of a reflection is a reflection. (Hint: First show it for $n = 2, 3$. Then define reflection in $\mathbb{R}^n$ and prove for higher $n$.)

Exercise 66. Show $|g| = |g^a|$.

Exercise 67. Show that conjugacy is an equivalence relation.
Exercise 68. Prove that the conjugacy classes (equivalence classes with respect to conjugacy) are the orbits of \( \text{Inn}(G) \).

Definition 10. The quaternion group is defined by \( Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \} \) subject to the relations \(-1 = i^2 = j^2 = k^2\) as well as \( ij = k, jk = i, ki = j \) and \( ji = -k, kj = -i, ik = -j \).

Exercise!!! 69 (Practice with small groups). For the small groups \( G = C_n, S_3, D_4, Q_8 \) describe as explicit permutations the inner automorphisms of the group, find the center \( Z(G) \), find \( G/Z(G) \), and determine the conjugacy classes of the group. Also find all subgroups of \( G \) and show which are normal and which are Sylow subgroups. Verify that the Sylow subgroups satisfy the conclusions of Sylow’s theorems.

Exercise 70. Complete the Cayley table (multiplication table) for \( Q_8 \). Give the Cayley table for \( S_3 \).

Definition 11. The direct product of groups \( G \) and \( H \) is \( G \times H = \{ (g, h) : g \in G, h \in H \} \) where the group operation is defined component-wise so that \( (g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) \).

Exercise 71. Let \( G^* = \{ (g, e_H) : g \in G \} \) and define analogously \( H^* = \{ (e_G, h) : h \in H \} \). Then show that \( G^*, H^* \triangleleft G \times H \) and that \( G^* \cong G \) and \( H^* \cong H \).

Exercise 72. For \( A, B \leq G \) let \([A, B]\) = \( \langle [a, b] : a \in A, b \in B \rangle \). Show that \( [G^*, H^*] = \text{id} \) in \( G \times H \), i.e., that for \( g^* \in G^* \) and \( h^* \in H^* \), \( [g^*, h^*] = \text{id} \).

Exercise 73. Show that \( G^* \cap H^* = \{ \text{id} \} \).

Exercise 74. If \( G, H \triangleleft K \) such that \( G \cap H = \text{id} \) and \( \langle G, H \rangle = K \), i.e., \( G \) and \( H \) have trivial intersection and together generate \( K \), then prove that \( K \cong G \times H \).

Exercise 75. Show that if \( G, H \triangleleft K \) and \( G \cap H = \text{id} \) then \( [G, H] = \text{id} \).

Exercise!!! 76. Prove \( C_k \times C_\ell \) is cyclic if and only if \( \gcd(k, \ell) = 1 \).

Exercise 77. Show that \( |G \times H| = |G||H| \).

Exercise 78 (Dimension invariance). Prove that \( \mathbb{Z}^k \cong \mathbb{Z}^\ell \) implies \( k = \ell \).
Exercise 79. In contrast to the above exercise, show that \((\mathbb{R}, +) \cong (\mathbb{R}^k, +)\) for all \(k\).

Exercise!! 80. If \(G\) is not abelian then \(G/Z(G)\) is not cyclic. (Hint: Prove the contrapositive.)

Exercise* 81. If \(|G| = p^k\) for some prime \(p\) and \(k \geq 1\), then \(Z(G) \neq \text{id}\).

Exercise 82. Prove the following two statements:

1. If \(G\) is abelian then every \(H \leq G\) is normal.

2. There exists a non-abelian group every subgroup of which is normal. (Hint: One of the familiar small group.)

Exercise 83. Show that there are two groups order \(p^2\), namely \(C_{p^2}\) and \(C_p \times C_p\). Show that \(C_{p^2} \not\cong C_p \times C_p\) (\(p\) is prime.)

Exercise 84. Find an undirected graph \(X\) such that \(\text{Aut}(X) \cong C_3\).

Exercise 85. (Frucht’s Theorem, 1938) Prove that for every finite group \(G\) there exists a finite graph \(X\) such that \(\text{Aut}(X) \cong G\).

Exercise* 86. Show that if \(X\) is a planar graph then \(\text{Aut}(X) \not\cong Q_8\). (Instructor’s theorem from college.)

Definition 12. A group \(G \leq S_n\) is transitive if there is just one orbit for the \(G\)-action on \(\{1, \ldots, n\}\). In other words, if \(A\) denotes the permutation domain, then \((\forall x, y \in A)(\exists \pi \in G)(x^\pi = y)\).

A graph \(X\) is vertex-transitive if \(\text{Aut}(X)\) acts as a transitive group on the set of vertices.

A graph \(X\) is edge-transitive if \(\text{Aut}(X)\) acts transitively on the set of edges.

Exercise 87. Show that the following graphs are vertex-transitive:

(a) \(K_n\), the \(n\)-cycle, the graphs of the regular solids (tetrahedron, cube, octahedron, dodecahedron, icosahedron), the Petersen graph.

(b) The “regular tilings” and the “Archimedean tilings” of the (euclidean) plane. (Look them up - check “tiling by regular polygons” in Wikipedia. In the same article you will also find some beautiful vertex-transitive tilings of the hyperbolic plane. Compare with Escher’s art.)
Exercise 88. Show $\text{Aut}(\text{Cube}) \cong \text{Aut}^+(\text{Cube}) \times C_2$.

Exercise 89. Prove: If $H \leq G$ and $|G : H| = 2$, then $H \triangleleft G$.

Exercise 90. Prove: If $H \triangleleft G$ and $|H| = 2$, then $H \leq Z(G)$.

Exercise 91. Let $B \subseteq \mathbb{R}^3$ be a centrally symmetric ($B = -B$), full-dimensional (not in a plane), and bounded subset. Then show $\text{Aut}(B) = \text{Aut}^+(B) \times C_2$. (Hint: Bounded implies central reflection is in the center of $\text{Aut}(B)$.)

Exercise 92. Show that the preceding exercise becomes false if we omit the condition that $B$ is bounded. Hint: In the group of symmetries of the square/cubic grid, show that the central reflection, $-\text{id}$, together with $\text{id}$, is not a normal subgroup. Note: Since $-\text{id}$ is an involution (has order 2), this statement is equivalent to proving that $-\text{id}$ is not in the center (Ex. 90).

Definition 13. Let $G \leq \text{Sym}(A)$, a group of permutations of the set $A$. The orbit of $x \in A$ is $x^G = \{x^\sigma : \sigma \in G\}$. Thus $x$ and $y$ are in the same orbit if there is a $\sigma \in G$ such that $x^\sigma = y$. The stabilizer subgroup $G_x$ of $x \in A$ is $G_x = \{\sigma \in G : x^\sigma = x\}$.

Exercise 93. If $x, y \in A$ are in the same orbit, then prove that $G_x$ and $G_y$ are conjugate.

Definition 14. An action (or representation) of a group $G$ on a set $A$ is a homomorphism $\phi : G \to \text{Sym}(A)$. The action $\phi$ is faithful if $\ker(\phi) = 1$, i.e., every element of $G \setminus \{1\}$ actually moves an element of $A$.

Exercise!!! 94 (Orbit-Stabilizer Theorem). Prove that $|G : G_x| = |x^G|$.

Definition 15. The action of $G$ on $A$ is transitive if for all $x, y \in A$ there exists $\pi \in G$ such that $x^\pi = y$. Hence $A$ has only one $G$-orbit.

Definition 16. The induced action on pairs $\phi : S_n \to S_{\binom{n}{2}}$ is defined by $\binom{n}{m}^{\phi(\sigma)} = \{n^\sigma, m^\sigma\}$.

Exercise 95. Prove that the induced action on pairs is faithful for $n \geq 3$.

Definition 17. Let $G = \langle S \rangle$ be a group generated by $S \subseteq G$. Define the Cayley diagram to be the colored directed graph $D(G, S) = (V, E, c)$ where $V = G$, and $E = \{(g, sg) : g \in G, s \in S\}$, and the coloring of the edges, $c : E \to S$, is defined as $c((g, sg)) = s$. (We think of the elements of $S$ as colors.)
Exercise 96. Demonstrate an isomorphism $Q_8/Z(Q_8) \cong V_4$ where $V_4 = C_2 \times C_2 = \text{Aut(Rectangle)}$. $V_4$ is called the “Klein 4-group” after Felix Klein.

Definition 18. An element $g \in G$ is an involution if $|g| = 2$.

Exercise 97. Let $H = \{ \text{id}, (12)(34), (13)(24), (14)(23) \}$. Show $H \triangleleft S_4$. (Robin’s tangential note: Note $H \leq A_4$, so $H \triangleleft A_4$. So $A_4$ contains a non-trivial normal subgroup. Perhaps surprisingly, this is the only $A_n$ which has this property.)

Exercise 98. Draw the Cayley diagram for $Q_8$ with respect to two generators (e.g. $\{i, j\}$).

Definition 19. The right regular representation of $G$ is a map $\rho : G \to \text{Sym}(G)$ denoted $g \mapsto \rho_g$ where $\rho_g : G \to G$ is defined as the right multiplication by $g$: $\rho_g(a) = ag$.

Exercise 99. Show that the action $\rho$ is faithful. Hence, $G \cong G^\rho = \{ \rho_g : g \in G \}$.

Exercise 100. Show that $G^\rho \leq \text{Aut}(D(G,S))$.

Exercise!!! 101. In fact, show that $G^\rho = \text{Aut}(D(G,S))$.

Exercise 102. Prove $G^\rho$ is transitive.

Definition 20. The Cayley graph $\Gamma(G,S)$ is an undirected graph obtained from $D(G,S)$ by ignoring colors and orientation.

Exercise 103. Prove that the triangular prism is a Cayley graph of $S_3$ as well as of $C_3 \times C_2 = C_6$.

Exercise 104. Let $X = (G,E)$ be a graph with vertex set $G$. Show that $X$ is a Cayley graph of $G$ if and only if $X$ is connected and $G^\rho \leq \text{Aut}(X)$.

Exercise 105. Find a graph which is vertex-transitive but not edge-transitive (see Definition 12).

Exercise 106. Find a graph which is edge-transitive but not vertex-transitive. Prove that such a graph is necessarily bipartite.
Definition 21. Let \( p \) be a prime. Let \( H_p \) be the group of matrices

\[
\begin{bmatrix}
1 & x & y \\
0 & 1 & z \\
0 & 0 & 1
\end{bmatrix} \mod p
\]

under multiplication.

Exercise 107. (a) Prove that \( H_p \) is a nonabelian group of order \( p^3 \).
(b) \( H_2 \) is isomorphic to which of \( D_4 \) and \( Q_8 \)?

Definition 22. \( G \) is simple if \(|G| > 1\) and \( G \) has no nontrivial normal subgroup.

Exercise 108. If \( G \) is abelian and simple then \(|G| = p\).

Exercise 109.
(a) \( A_4 \) is not simple.
(b) \( A_5 \) is simple.
(c) \( A_n \) is simple for all \( n \geq 5 \).

Exercise* 110. \( A_5 \) is the smallest nonabelian simple group.

Definition 23. Let \( n \geq 2 \). Let \( q \) be a prime power.

(a) The general linear group over the field \( F_q \) denoted \( GL(n, q) \), is the group of \( n \times n \) nonsingular matrices over \( F_q \), under multiplication.

(b) The special linear group \( SL(n, q) \) is the subgroup of \( GL(n, q) \) consisting of matrices with determinant 1.

(c) The projective special linear group, \( PSL(n, q) \), is the quotient \( SL(n, q)/Z(SL(n, q)) \).

The groups \( PSL(n, p) \) are simple for \( n \geq 3 \) for all \( q \), and for \( n = 2, q \geq 4 \). The second smallest nonabelian simple group is \( PSL(2, 7) \cong PSL(3, 2) \), of order 168.

Exercise 111. \( Z(GL(n, q)) = \{ \lambda I : \lambda \in F_q^\times \} \) (matrices of the form \( \lambda I \) are called scalar matrices).
Exercise 112. Prove: $|GL(2, p)| = (p^2 - 1)(p^2 - p)$. Compute the orders of $SL(2, p)$ and $PSL(2, p)$.

Exercise 113.

(a) $Z(SL(n, q)) = \{\lambda I : \lambda \in \mathbb{F}_q, \lambda^n = 1\}$.

(b) The order of the center is $\gcd(n, q - 1)$.

Exercise 114. Prove: $PSL(2, 4) \cong PSL(2, 5) \cong A_5$.

Exercise 115. Recall Definition 19 of a right regular representation of a group $G$, with $\rho_g : x \mapsto gx$ and $\lambda_g : x \mapsto g^{-1}x$. Prove $\rho_g \lambda_h = \lambda_h \rho_g$.

Definition 24. Let $G$ be a group, and $S$ a generating set for $G$. The Cayley graph $\Gamma(G, S)$ is the graph $(G, E)$ (i.e., $G$ is the set of vertices) where $E = \{(g, sg) : g \in G, s \in S\}$.

Exercise 116. The Petersen graph is not the Cayley graph of any group.

Exercise 117. The only groups of order 10 are $C_{10}$ and $D_5$.

Definition 25. Let $X, Y \subseteq \mathbb{R}^n$. We call $X$ and $Y$ homomorphic if there exists a map $f : X \to Y$, called a homeomorphism, such that $f$ and $f^{-1}$ are continuous.

Exercise 118. Recall that a tree is a connected graph with no cycles. Prove that every tree has a vertex of degree 1.

Definition 26. A plane drawing of a graph is an embedding of the graph in the plane with no edge intersections. A graph is planar if it admits a plane drawing.

Exercise 119. If a planar graph has $v \geq 3$ vertices (no multiple edges) then it has $e \leq 3v - 6$ edges.

Exercise 120. Prove that the complete graph $K_5$ is not planar.

Exercise 121. If a planar graph has $v \geq 3$ and no triangles (i.e., no cycles of length three) then $e \leq 2v - 4$. 

12
Exercise 122. The complete bipartite graph $K_{3,3}$ is the graph

Prove that $K_{3,3}$ is not planar.

Exercise 123. Prove that the Petersen graph is not planar.

Definition 27. $G \leq S_n$ is a regular permutation group if $G$ is a transitive and $|G_x| = 1$ for some $x$ (and therefore, for all $x$) in the permutation domain.

Exercise 124. (a) The right regular representation of $G$ is a regular permutation group. (Same about the left regular representation.)

(b) Every regular permutation group is equivalent to its own right regular representation (equivalence here meaning a relabeling of the permutation domain).

Exercise 125.

(a) Draw the complete graph $K_7$ on the torus.
(b) Draw $K_6$ on the Klein bottle.
(c) Draw $K_5$ on the projective plane.

Exercise 126. Let $\chi$ denote the Euler characteristic of a closed surface. Prove that

(a) $\chi($sphere$) = 2$;
(b) $\chi($torus$) = 0$;
(c) $\chi($sphere with $k$ handles$) = 2 - 2k$;
(d) $\chi($sphere with $k$ crosscaps$) = 2 - k$.

Exercise 127. $C_5 \times C_5$ (the $5 \times 5$ toroidal grid) cannot be embedded on the Klein bottle.
Exercise 128. The $5 \times 5$ grid on the Klein bottle is not vertex-transitive.

Definition 28. An embedding of a graph $X$ on a surface $\Sigma$ is symmetrical if all automorphisms of $X$ extend to the faces.

Exercise 129. (a) The natural embedding of each Platonic solid on the sphere is symmetrical.

(b) The natural embedding of each Archimedean plane tiling in the plane is symmetrical.

(c) For $n \geq 5$, the complete graph $K_n$ does not have a symmetrical embedding on any surface.

The subject of the last class was an outline of the following result.

Theorem. For every closed surface $\Sigma$ there is an $n_0$ such that if a connected vertex-transitive graph $X$ with at least $n_0$ vertices embeds on $\Sigma$ then $X$ in fact embeds on a surface of non-negative Euler characteristic (sphere, projective plane, torus, or Klein bottle); moreover, either $X$ is one of 8 types of explicitly defined “stripe graphs” or $X$ has a symmetrical embedding on a surface of non-negative Euler characteristic.

The details can be found in


The exercises below support the proof.

Definition 29. A signed rotation system on a connected graph is an assignment of a cyclic permutation (a rotation) to each vertex, which cyclically permutes the edges incident with the vertex, and of a sign ($+1$ or $-1$) assigned to each edge. A signed rotation system defines a cell embedding of the graph on a closed surface. The surface is determined by the signed rotation system.

Exercise 130. (a) If we switch the sign of an edge, the Euler characteristic (of the surface defined by the signed rotation system) changes by $\leq 1$.

(b) If we change the rotation at a vertex of degree $d$, the Euler characteristic changes by $\leq d$. 

14
**Definition 30.** Two signed rotation systems on a graph are *equivalent* if there is a subset $W$ of the vertices such that each rotation is inverted on $W$ and each sign is changed on edges connecting $W$ to $V \setminus W$; otherwise the two systems agree.

**Exercise 131.** A signed rotation system defines an orientable surface if and only if it is equivalent to one with all signs $+1$.

**Exercise 132.** A signed rotation system defines an orientable surface if and only if there is an even number of $-1$’s on each cycle.

**Definition 31.** An infinite graph is *locally finite* if every vertex has finite degree. (Note: the degrees do not need to be bounded.)

**Definition 32.** (Limit of graph sequences) Let $X$ be an infinite, locally finite, connected, rooted graph, and let $\{X_n\}$ be a sequence of finite, connected, rooted graphs. We say $\{X_n\}$ converges to $X$, and write $X_n \rightarrow X$, if for every $d$, there exists an $n_0$, such that for all $n > n_0$, the $d$-neighborhood of the root in $G_n$ is isomorphic to the $d$-neighborhood of the root in $G$.

**Exercise 133.** (Compactness) Every sequence $\{X_n\}$ of finite, connected, rooted graphs of uniformly bounded degree has a convergent subsequence.

**Exercise 134.** If $X_n \rightarrow X$ and for every $n$, $X_n$ is vertex-transitive, then $X$ is vertex-transitive.

**Exercise 135.** For every surface $\Sigma$ there is an $n_0$ such that if the graph $X$ embeds into $\Sigma$ and $v(X) \geq n_0$ then $X$ has a vertex of degree $\leq 6$.

**Exercise 136.** Let $\Sigma$ be a closed surface and $X$ an infinite, connected, locally finite, vertex-transitive graph. If every finite subgraph of $X$ embeds on $\Sigma$ then $X$ is planar.

**Exercise 137.** (Whitney) If $X$ is a (finite or infinite) connected, locally finite, 3-connected planar graph then $X$ is uniquely embeddable on the sphere.

**Definition 33.** (Ends of graphs) Let $X$ be an infinite, locally finite graph.

(a) Let $r_1$ and $r_2$ be rays (one-way infinite paths) of $X$. We say $r_1$ and $r_2$ are *equivalent* if for every finite $C \subseteq V(X)$, the rays $r_1$ and $r_2$ can be linked without going through $C$. 

15
(b) An end of \( X \) is an equivalence class of rays.

**Exercise 138.** If \( X \) is an infinite, connected, locally finite, vertex-transitive graph with \( \geq 3 \) ends, then it has infinitely many ends (in fact, continuum many).

**Exercise 139.** Let \( X_n \to X \) where the \( X_n \) are connected finite vertex-transitive graphs of uniformly bounded degree. Suppose \( X \) has \( \geq 3 \) ends. Prove: \((\forall k \text{ and for all sufficiently large } n)(X_n \text{ has a contraction to a graph } Y_n \text{ such that all vertices of } Y_n \text{ have degree } \geq k))\).

**Exercise 140.** If \( X \) is an infinite, connected, locally finite, vertex-transitive graph with one end and degree \( \geq 3 \), then \( X \) is 3-connected.