MATH 250A LECTURE RECAPS (GROUPS)

PATRICK OARE

1. 8/24 (Groups, Direct Product)

- **Groups**: A group can be equivalently defined as:
  - The set of symmetries of an object
  - A pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a map satisfying:
    1. Associativity. We have $(ab)c = a(bc)$ for every $a, b, c \in G$.
    2. Identity. There is an $e \in G$ with $ea = ae = a$ for each $a \in G$.
    3. Inverse. For each $a \in G$, we have $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

  G is **Abelian** if the operation commutes.
- **Actions of a group on itself.**

  A **symmetry** preserves an action. An **action** is a map $\cdot : G \times S \to S$ with $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$ and $e \cdot s = s$ for each $g_1, g_2 \in G, s \in S$. Every group has 4 left actions on itself and 4 right actions on itself. The 4 left actions are:
  1. $g \cdot s := s$
  2. $g \cdot s := gs$
  3. $g \cdot s := sg^{-1}$
  4. $g \cdot s := gsg^{-1}$

  The right actions of a group are similar.
- **Lagrange's Theorem**: The order of any subgroup $H \leq G$ divides $|G|$.

  Suppose G acts on a set S **transitively**, so there is one orbit. Fix $s \in S$, and let $H = G_s$ be the **isotropy** group (stabilizer) of s. Then, we have a bijection between G/H and the points of S. The forward direction of the map is mapping $t \in S$ to $t \mapsto \{g \in G : gs = t\}$. This is a coset of H because if $gs = t$, then $(gh)s = g(hs) = gs$, so gH is contained in the set. The reverse direction of the map is given by $gH \mapsto gs$. This is well defined because if $g_1 H = g_2 H$, then $g_1 = g_2 h$, so $g_1 s = g_2 hs = g_2 s$.

  This also gives us that if we fix $s \in S$:

  $$|G| = |H| \#(cosets) = |G_s| \times |S|$$

  which allows us to do some nice counting arguments. For example, the number of rotations of the icosahedron (triangular face, 20-sided) is 60, because the group of its rotations (A_4) acts transitively on the icosahedron. If we fix a face, there are 3 rotations that stabilize it, and the number of elements in S is 20, hence we have 60 rotations.
- **Direct Product**: If $H, K \leq G$ such that:

(1) $H \cap K = \{e\}$
(2) $G = HK$
(3) Either $H, K \trianglelefteq G$ or $\forall h \in H, k \in K$, $hk = kh$
Then $G \cong H \times K$.

2. 8/29 (Normal Subgroups, Semidirect Product)

- **Normal Subgroups**: Equivalently, we have $H \trianglelefteq G$ if:
  (1) $\forall g \in G, gHg^{-1} = H$
  (2) The set of left cosets of H equal the set of right cosets of H.
  (3) H is a union of conjugacy classes.
- **Cauchy's Theorem**: If p is a prime and divides $|G|$, then G has an element of order p.

  Clarification of proof for G abelian: Begin with G abelian and induct on $|G|$. Pick an element of prime power q in G– one way to do this is to pick $x \in G \setminus \{e\}$ with $|x| = aq$ for $a \in \mathbb{N}$ and q a prime power, then take x^a, which has order q. If $p|q$ then we are done, as $q = p^\alpha$ and so $x^{p^{\alpha-1}}$ has order p. Else, $G/\langle x\rangle$ has $p|(G : \langle x\rangle)$, so $G/\langle x\rangle$ has an element b of order p by induction. We **lift** b to $a \in G$ (so we find an element $a \in G$ such that $b = aH$), and let $|a| = m$. As $a^m = e$, $(aH)^m = H$, and thus $|aH| = p$ divides m. So, $a^{m/p}$ has order p in G, and we are done.
- **Theorem**: Let $H \leq G$ be a subgroup with $(G : H) = 2$. Then, $H \trianglelefteq G$.

  This is because if $(G : H) = 2$, then H has two left cosets and two right cosets. As H is itself a left coset and a right coset and the left/right cosets partition G, the elements not in H must be both the left and the right coset, and hence $G/H = H\backslash G$.
- **Semidirect Product**: We can define the **semidirect product** of subgroups A and B of G, $G = A \rtimes B$, if:
  (1) $A \trianglelefteq G$ (not necessarily B).
  (2) $A \cap B = \{e\}$.
  (3) $G = AB$ (note that as $A \trianglelefteq G$, $AB = BA$).

  If A and B are arbitrary groups and $\psi : B \to Aut(A)$ is a homomorphism, then the group law on $A \times B$ given by:

  $$(a_1, b_1) \cdot (a_2, b_2) := (a_1\psi(b_1)(a_2), b_1b_2)$$

  gives a semidirect product of A and B.

  When $A \trianglelefteq G$ and $B \leq G$, then the inner semidirect product is isomorphic to the outer semidirect product given with the map $\psi : B \to Aut(A)$, $b \mapsto \gamma_b$, where γ_b is conjugation by b by the correspondence $(a, b) \mapsto ab$.

  Note that the **number of semidirect products of A with B** is the **number of homomorphisms** $\psi : B \to Aut(A)$
- **Short Exact Sequences**: An exact sequence is a sequence of morphisms (f_i) where $f_i : A_i \to A_i + 1$ such that $im(f_i) = ker(f_{i+1})$. A short exact sequence is an

exact sequence of the form:

$$0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$$

In this case, f is injective, g is surjective, and $G/G' \cong G''$ by the first isomorphism theorem.

Given a sequence of the above form, the **extension problem** is to find all groups G that make the sequence exact. Note that **in general it is not the case that either $G \cong G' \times G''$ or $G \cong G' \rtimes G''$.**

- **Automorphisms of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$**: This group has automorphism group:

$$Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

where the star indicates these are the elements coprime to n. This group has order $\phi(n)$, where ϕ is the totient function. This is because any automorphism is completely determined by its action on a generator of $\mathbb{Z}/n\mathbb{Z}$, and so we have $\phi(n)$ automorphisms. In the case where $n = p$ is prime, we have:

$$Aut(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

For the group $(\mathbb{Z}, +)$, we have:

$$Aut(\mathbb{Z}) \cong \{\pm 1\}$$

as there are only two automorphisms, the identity, and the one sending $1 \mapsto -1$ (1 and -1 are the generators of $\mathbb{Z}$).

- **Groups of order 6**: There are two groups of order 6, $\mathbb{Z}/6\mathbb{Z}$ and S_3.

If G has an element of order 6, $G \cong \mathbb{Z}/6\mathbb{Z}$, so suppose not. G has an element y of order 2 and x of order 3 by Cauchy. $H := \langle x \rangle$ has index 2 in G and is hence normal. Let $K := \langle y \rangle$. We will show $G \cong H \rtimes K$. Every nonidentity element of H has order 3, so $y \notin H$, and $G/H = \{H, yH\}$. For every $a \in G$, either $a \in H$, or $aH = yH$, in which case $a = yh$, $h \in H$, which imples $a \in KH = HK$. Thus $G = HK$, and as $H \cap K = \{e\}$ (as they are generated by elements of coprime order), $G \cong H \rtimes K \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. This is characterized by the homomorphisms $\mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. The trivial homomorphism gives the direct product which is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ as $gcd(2,3) = 1$, and the nontrivial one sends 1 (where 0 is the identity) to the automorphism $x \mapsto x^{-1}$), and this yields a group isomorphic to S_3.

- **Groups of order 8**: The groups of order 8 are $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, Q (quaternion group), and D_8.

Suppose $|G| = 8 = 2^3$. G has an element of order 2 by Cauchy. If every element of $G \setminus \{e\}$ is order 2, we can view G as a vector space over F_2 and hence $G \cong (\mathbb{Z}/2\mathbb{Z})^3$. Another way to view this is to pick $x \in G \setminus \{1\}$. Then, $|x| = 2$, and pick $y \in G \setminus \langle x \rangle$. $\langle x \rangle \cap \langle y \rangle$ is trivial, so $\langle x \rangle \langle y \rangle \cong \langle x \rangle \times \langle y \rangle$. Pick $z \in G \setminus \langle x \rangle \langle y \rangle$, and $\langle z \rangle \cap \langle x \rangle \langle y \rangle = \{e\}$, so $G \cong \langle x \rangle \times \langle y \rangle \times \langle z \rangle \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Now suppose every non-identity element in G does not have order 2. If there is an element of order 8, then $G \cong \mathbb{Z}/8\mathbb{Z}$, so suppose not, and G has nonidentity elements of order 2 or 4. Let $g \in G$ have order 4. Then, $H := \langle g \rangle \trianglelefteq G$ as it has index 2.n Pick $x \in G$ such that $xH \neq H$. We have $xHx^{-1} = H$, so $xgx^-1 = g'$ with $g' \in H$. Conjugation by x is an automorphism, so it preserves order, thus $xgx^{-1} = g$ or $xgx^{-1} = g^3$. Also, $(xH)^2 = H$, so $x^2 \in H$. **If $x^2 = g^3$, then change g to g^-1** and carry out the same argument. We then have a table of presentations and can deduce the isomorphisms.

3. 8/31 (Orbits, Quaternions)

- **Counting Rooks**: A chessboard has 8 columns by 8 rows.

  Q. How many ways are there to arrange 8 non-attacking rooks on a chessboard?

  A. For the first rook, you have the choice of 8 rows/cols. When you put it down, you eliminate that row and column, so you have 7 options. This continues, so the answer is 8!. Let the set of all non-attacking configurations be A, so $|A| = 8!$

  Q. How many ways are there up to symmetry? (What this means is that if one configuration differs from another up to a rotation/flip or composition of the two, they are equivalent)

  A. The idea is to act the group D_8 on the set A. If $a \in A$ is a configuration, all the symmetries of a are given the set $D_8 \cdot a$, which is the orbit of a under D_8. So, to find all the configurations up to symmetry, we must count the number of orbits with Burnside's Lemma; we compute $f(g)$, the number of fixed elements of A, for each $g \in G$. See the notes for how to do this; we end up with 5282 ways.
- **Quaternions**:
  - The quaternions $\mathbb{H}$ "extend" $\mathbb{C}$. We can think of $\mathbb{H}$ as having the base set of $\mathbb{R}^4$ and inheriting the addition and scalar multiplication, but having a different multiplication structure given by quaternion multiplication. A general quaternion $z \in \mathbb{H}$ is of the form:

    $$z = a + bI + cJ + dK$$

    where I, J, and K obey the relations:

    $$IJ = K, JK = I, KI = J, I^2 = J^2 = K^2 = 1$$
  - We can embed the quaternions into $M_{2x2}(\mathbb{C})$ by identifying:

    $$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

    These are almost the Pauli matrices; notice that each Pauli matrix is just i times a quaternion. You can see that as each of these matrices is invertible, every quaternion has an inverse.
  - We define **quaternion conjugation** as:

    $$\bar{z} := a - bI - cJ - dK$$

    You can then show from the relations that:

    $$z\bar{z} = a^2 + b^2 + c^2 + d^2$$

This gives an easy way to show that every nonzero quaternion z has an inverse $z^{-1} = \frac{\bar{z}}{a^2+b^2+c^2+d^2}$, and so $(\mathbb{H}^*, \times)$ forms a group. Likewise, defining the norm to be:

$$|z| := z\bar{z}$$

we see that

$$\psi : \mathbb{H}^* \to \mathbb{R}^*, z \mapsto |z|$$

is a homomorphism from $\mathbb{H}^*$ to $\mathbb{R}^*$. Furthermore, the kernel of ψ is:

$$S^3 := ker(\psi) = \{a + bI + cJ + dK \in \mathbb{H}^*\}$$

This is the **3-sphere**, which is the unit sphere in 4-dimensional Euclidean space.

  - Quaternion rotations. **TODO**

- **Burnside's Lemma**: Let a group G act on a set S, and for each $g \in G$, let $f(g)$ be the number of elements of S fixed by g. Then:

$$\#(orbits) = \frac{1}{|G|} \sum_{g \in G} f(g)$$

- **The Class Equation**: Let G act on a group S. Let $\{s_i\}$ be representatives of the distinct orbits of S under G. Then:

$$|S| = \sum_i (G : G_{s_i})$$

- **Center of p-groups**: Any group of order p^n with p prime and $n \in \mathbb{N}$ has a nontrivial center.
- **Groups of order p^2**: Let $|G| = p^2$, for some prime p. Then, either $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.
- **Nilpotent Groups**: A group G is nilpotent if it can be reduced to $\{e\}$ by repeatedly quotienting out the center.

  All groups of order p^n are nilpotent, and any finite nilpotent group is the product of p-groups.
- **Groups of order 2p**: If $|G|$ is a group of order $2p$ for some prime p, then G is either cyclic or dihedral.

  By Cauchy, we can find an element $h \in G$ of order p and $k \in G$ of order 2; let $H = \langle h \rangle$ and $K = \langle k \rangle$. Then, $H \trianglelefteq G$ as $(G : H) = 2$, and $H \cap K = \{e\}$, so $HK = G$ and thus $G = H \rtimes K$. This semidirect product is characterized by the homomorphisms $\psi : K \to Aut(H)$. As $H \cong \mathbb{Z}/p\mathbb{Z}$, $Aut(H) \cong (\mathbb{Z}/p\mathbb{Z})^*$, which is cyclic. There are only two elements of order 2 in $(\mathbb{Z}/p\mathbb{Z})^*$, so we get two homomorphisms; the trivial one and the one sending $\bar{2} \mapsto -id$. The trivial one makes $H \rtimes K \cong H \times K \cong \mathbb{Z}/2p\mathbb{Z}$. The other homomorphism makes $G \cong D_{2p}$, by the isomorphism $\phi : (h^i, k^j) \mapsto r^i s^j$. To show this is a homomorphism:

$$\phi((h^{i_1}, 1)(h^{i_2}, k^j)) = \phi(h^{i_1+i_2}, k^j) = r^{i_1+i_2}s^j = \phi(h^{i_1}, 1)\phi(h^{i_2}, k^j)$$

$$\phi((h^{i_1}, k)(h^{i_2}, k^j)) = \phi(h^{i_1-i_2}, k^{j+1}) = r^{i_1-i_2}ss^j = \phi(h^{i_1}, k)\phi(h^{i_2}, k^j)$$

This is obviously a surjection and an injection as the generators have the same orders.

4. 9/5 (Sylow, Abelian)

- **Sylow Theorems**: Let G be a finite group. A p-Sylow subgroup of G is a subgroup of order p^n, where p^n divides $|G|$ but p^{n+1} does not divide $|G|$. Suppose $|G| = p^n m$, with $gcd(p^n, m) = 1$. Let n_p be the number of p-Sylow subgroups of G.
  1. p-Sylow subgroups of G exist, i.e. $n_p \neq 0$.
  2. $n_p \equiv 1 \mod p$, and $n_p | m$.
  3. Any p-subgroup of G is contained within a p-Sylow subgroup.
  4. All the p-Sylow subgroups of G are conjugate, and every conjugate of a p-Sylow subgroup is a p-Sylow.
  5. Let P be a p-Sylow. Then $P \trianglelefteq G$ iff $n_p = 1$.
- **Solvable Groups**: A group G is said to be **solvable** if either it is cyclic or it has a normal subgroup $N \trianglelefteq G$ with N and G/N solvable.

  If G has no normal subgroups, G is called **simple**. The **Jordan Holder Theorem** states the choice of simple groups in the chain does not depend on the choice of splitting; essentially, if we have two composition series for a group, then they are equivalent.

  We can show that A_5 is simple by considering the rotations of the icosahedron, which is the group A_5. The order of the conjugacy classes are $1, 12, 12, 15, 20$, and the only way that we can add these up to divide 60 is 1 or 60, thus any union of conjugacy of conjugacy classes must be trivial or the group itself.
- **Groups of order pq, $p < q$**: We have a normal subgroup of order q by Cauchy, $H = \langle h \rangle \trianglelefteq G$ as $(G : H) = p$. We also have a subgroup $K = \langle k \rangle \leq G$ with order p. It is easy to show $G = H \rtimes K$, so we can classify G by homomorphisms $\psi : K \to Aut(H)$. As $H \cong \mathbb{Z}/q\mathbb{Z}$ and $K \cong \mathbb{Z}/p\mathbb{Z}$, we need to find all homomorphisms:

  $$\psi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^*$$

  $\mathbb{Z}/q\mathbb{Z}$ is cyclic of order $q - 1$, so if p does not divide $q - 1$, we have only the trivial homomorphism and thus:

  $$p \not| \, (q-1) \implies G \cong \mathbb{Z}/pq\mathbb{Z}$$

  If not, then we can still classify the groups by looking at the semidirect product.
- **Finitely Generated Abelian Groups**: Any finitely generated abelian group is isomorphic to the direct sum:

  $$G \cong \mathbb{Z}^r \bigoplus (\mathbb{Z}/m_1\mathbb{Z}) \bigoplus (\mathbb{Z}/m_2\mathbb{Z}) \bigoplus ... \bigoplus (\mathbb{Z}/m_n\mathbb{Z})$$

  where $r \geq 0$ and $m_1 | m_2 | ... | m_n$.
- **Abelian Groups**: TODO

5. 9/7 (Symmetric Groups)

- The **symmetric group** on n letters is the group of all permutations of n points, denoted S_n. It has $|S_n| = n!$.
- **Alternating Group,** A_n: Examine the action of S_n on $\{x_1, ..., x_n\}$. We define:
$$\Delta(x_1, ..., x_n) := \prod_{i<j}(x_i - x_j)$$
Any element of S_n maps Δ to $\pm\Delta$, and we define the **sign** of a permutation $\sigma \in S_n$, $\epsilon : S_n \to \{\pm 1\}$ to satisfy:
$$\sigma\Delta = \epsilon(\sigma)\Delta$$
We define A_n to be the kernel of the sign homomorphism,
$$A_n := ker(\epsilon) \subset S_n$$
We see $|A_n| = \frac{n!}{2}$.
- Recall some facts about S_n:
  (1) Each element in S_n can be decomposed into a product of at most $\frac{n-1}{2}$ disjoint cycles.
  (2) A **transposition** is a 2-cycle. Every element in S_n can be decomposed into a product of transpositions (not necessarily disjoint)
  (3) The order of a k-cycle is k.
  (4) The sign of a transposition is -1. The sign of a product of cycles is the product of their signs.
  (5) Conjugation is really nice on cycles. If $\gamma \in S_n$ and $(a_1 a_2 ... a_k)$ is a k-cycle, then:
$$\gamma(a_1\ a_2\ ...\ a_k)\gamma^{-1} = (\gamma(a_1)\ \gamma(a_2)\ ...\ \gamma(a_k))$$
- **The Platonic Solids**: These are, with the number of rotations and total symmetries:

	Faces	Face Shape	Rotation Group	Symmetry Group
Tetrahedron	4	Triangle	A_4	S_4
Cube	6	Square	S_4	$S_4 \times (\mathbb{Z}/2\mathbb{Z})$
Octahedron	8	Triangle	S_4	$S_4 \times (\mathbb{Z}/2\mathbb{Z})$
Dodecahedron	12	Pentagon	A_5	$A_5 \times (\mathbb{Z}/2\mathbb{Z})$
Icosahedron	20	Triangle	A_5	$A_5 \times (\mathbb{Z}/2\mathbb{Z})$

Table 1. Platonic Solids

Note the symmetries of the cube and octahedron are the same and the dodecahedron and the icosahedron are the same (we can embed them into the same rigid object). Also recall the number of rotations is $\#(faces)\#(edges/face)$ by Burnside's Lemma. We can see the symmetry group of the cube is S_4 because any symmetry is a unique permutation of the 4 diagonals and hence it must be a subgroup of S_4.

- **Cycle Shape**: Let $\sigma \in S_n$ be decomposed into unique cycles. If σ is the product of n_i k_i cycles, we say the cycle shape of σ is:

$$\prod_i k_i^{n_i}$$

For example, the cycle $(194)(273)(68)(0)(5)$ has cycle shape $3^2 2^1 1^2$ in S_{10}.
- **Conjugacy Classes**: Two elements in S_n are conjugate if and only if they have the same cycle shape.

Q. Given $a, b \in S_n$ with the same cycle shape, how do we find $g \in S_n$ such that $a = gbg^{-1}$?

A. Line their cycles up, and take g to be the permutation between the corresponding symbols in their cycle shapes, starting with b and bubbling up to a.

If $\sigma \in S_n$ has cycle shape $1^{n_1} 2^{n_2} 3^{n_3} \ldots$, then the order of the centralizer of σ is:

$$|C_{S_n}(\sigma)| = 1^{n_1}(n_1)! 2^{n_2}(n_2)! 3^{n_3}(n_3)! \ldots$$

This enables us to find the conjugacy classes of S_n. We do an example with S_4:

Partitions of 4	Cycle shape	size(centralizer)	size(conjugacy class)	Rotation of cube
$1+1+1+1$	1^4	$4! = 24$	$24/24 = 1$	id
$2+1+1$	$2^1 1^2$	$2^1 1! 1^2 2! = 4$	$24/4 = 6$	rotation by π
$3+1$	$3^1 1^1$	3	$24 \ / \ 3 = 8$	rotation by $2\pi/3$
$2+2$	2^2	8	$24/3 = 8$	rotation by π
4	4^1	4	$24/4 = 6$	rotation by $\pi/2$

Table 2. Conjugacy classes of S_4 with geometric interpretation on cube.

- Problem: All normal subgroups of S_n: Obvious ones: $1, A_n, S_n$. Are there any others? Look for homomorphisms.

S_4 is the group of symmetries of the cube, so it acts on the set of lines through opposite faces of the cube. There are 3 of them, so we get a nontrivial homomorphism $S_4 \to S_3$ with the kernel being the identity and rotations by π. This has order 4, and is thus a normal subgroup of S_4 of order 4. This generalizes, giving surjective homomorphisms from $S_2 \to S_1$, $S_3 \to S_2$, and $S_4 \to S_3$.

It does not work with $S_5 \to S_4$ because $A_5 \trianglelefteq S_5$ is simple. If $N \trianglelefteq S_5$, then $N \cap A_5 \trianglelefteq S_5$, so $N \cap A_5 \trianglelefteq A_5$ and this means $N = 1$ or A_5 or S_5, so **no** epimorphism $S_5 \to S_4$.
- **Simplicity of A_n**: For $n \geq 5$, A_n is simple.

TODO read and understand a proof of this.
- Groups of order 120 containing A_5 and $\mathbb{Z}/2\mathbb{Z}$. We have:
  1. $A_5 \times \mathbb{Z}/2\mathbb{Z}$: Symmetries of the dodecahedron and icosahedron.
  2. S_5, subgroup A_5, quotient $S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$ ($S_5 = A_5 \rtimes \mathbb{Z}/2\mathbb{Z}$).
  3. Binary icosahedral group: Use the homomorphism $S^3 \to SO_3(\mathbb{R})$ to lift A_5 (rotations of ico/dodeca, so subgroup of $SO_3(\mathbb{R})$) to S^3 for a group of twice the order. If G is this group,the **Poincare 3-sphere** is the quotient S^3/G.

- **Inner and Outer Automorphisms**: An **inner automorphism** of a group G is of the form $x \mapsto gxg^{-1}$. We have the exact sequence:

$$1 \to Z(G) \to Inn(G) \to Aut(G) \to Out(G) \to 1$$

The map $Z(G) \to Inn(G)$, $g \mapsto \gamma_g$ is exact because it maps to the trivial automorphism, as conjugation by an element in the center of G is the identity. The **outer automorphisms** of G is the group

$$Out(G) := Aut(G)/Inn(G)$$

Except for $n = 6$, we have $Aut(S_n) \cong S_n \cong Aut(A_n)$, and all these automorphisms are inner. S_6 is really weird. S_5 has a subgroup of order 20 (index 6), so this gives us a homomorphism $S_5 \to S_6$. S_6 has 12 subgroups isomorphic to S_5, not 6 as one might expect. The "weird" ones (not S_5 or conjugates of S_5) give non-inner automorphisms.

6. 9/12 (Categories)

- **Definitions**: A **category** C consists of a set of **objects**, $Obj(C)$, and given two objects $A, B \in Obj(C)$, a set $Mor(A, B)$, called the set of **morphisms** of A into B. For $A, B, D \in Obj(C)$, we have a law of composition, i.e. a map:

$$Mor(B, D) \times Mor(A, B) \to Mor(A, D)$$

  (1) $Mor(A, B)$ and $Mor(A', B')$ are disjoint unless $A = A'$ and $B = B'$.
  (2) For each object $A \in Obj(C)$ there is a morphism $id_A \in Mor(A, A)$ that is a right identity on $Mor(A, B)$ and a left identity on $Mor(B, A)$.
  (3) The law of composition is associative.
- Examples:
  - A category which has a single object and whose morphisms are the elements of a fixed group G. Composition in this category is the group product.
  - Posets (partially ordered sets with $\leq$). We can let the objects of C be the elements of the poset, and $Mor(a, b)$ have 1 element if $a \leq b$ and no elements if not.
  - Grp is the category of Groups, Ab is the category of Abelian Groups, and Set is the category of Sets.
- **Functors**: "Maps" between different categories. A **covariant functor** F from a category C to a category D consists of a a map from $Obj(C) \to Obj(D)$ and a map $Mor(C) \to Mor(D)$ such that:
  (1) For each object $A \in Obj(C)$, $F(id_A) = id_{F(A)}$
  (2) $F(f \circ g) = F(f) \circ F(g)$, i.e. F preserves arrows

  A **contravariant functor** is like a covariant functor, but $F(f \circ g) = F(g) \circ F(f)$, i.e. it reverses all the arrows.
- Examples of Functors:
  (1) Forgetful functor: Map from an algebraic object to Set that forgets about the structure. This is covariant.

(2) Homology groups H_i provide a functor from topological spaces to abelian groups.
(3) Abelianization of a group G. Let H be the commutator subgroup, i.e. $H = \langle \{xyx^{-1}y^{-1} \in G : x, y \in G\} \rangle$. The quotient $G_{ab} := G/H$ is an Abelian group, and there is a functor F taking G to G_{ab}. Given a homomorphism $f : G \to G'$, we have an induced homomorphism $f_{ab} : G_{ab} \to G'_{ab}$. This is because if G_C is the commutator subgroup of G, then $G_C \leq ker(\pi_{G'} \circ f)$, and so the homomorphism f factors through the quotient $G/G_C = G_{ab}$ uniquely, giving a unique homomorphism $f_{ab} : G_{ab} \to G'_{ab}$.
(4) The free abelian group on a set S. This is a functor $F_{ab}(\cdot) : Set \to Ab$ which sends each set S to $F_{ab}(S)$ and each set map $\lambda : S \to S'$ to a map $F(\lambda) : F(S) \to F(S')$.
(5) Category has one object (single point) with morphisms as members of a group G. We define a functor $F : C \to Set$ where $F(\text{point})$ =some set S and $F(g)$ is a function from S to S; then $g \cdot s := F(g)(s)$ is an action on S, as $1 \cdot s = F(1)(s) = id(s) = s$ and $g \cdot h \cdot s = g \cdot F(h)(s) = F(g)(F(h)(s)) = F(g) \circ F(h)(s) = F(gh)(s) = (gh) \cdot s$.
(6) Dual of a vector space. The functor $F(V) := V^*$ and for a morphism $f : V \to W$ gives a morphism $F(f) : F(W) \to F(V)$ is contravariant.

- $Hom(\cdot, \cdot)$ is a **bifunctor**, and it is covariant in one argument and contravariant in the other argument. If we fix B, then $Hom(\cdot, B)$ is contravariant. This is because if we have $f : A_1 \to A_2$, then a map $\phi \in Hom(A_2, B)$ has $\phi \circ f : A_1 \to B \in Hom(A_1, B)$ and so we have a natural map $Hom(A_2, B) \to Hom(A_1, B)$. Likewise, $Hom(A, \cdot)$ is covariant.
- **Natural transformations**: TODO
- **Universal objects**: Universal property means that any other object with this property factors uniquely through the object. Check notes for examples of this with products, coproducts, pullbacks, pushouts, and equalizers. Universal objects are unique up to isomorphism, as a universal object allows a unique morphism on itself which must be id, and it must admit a map into and out of the universal object.
- **Equilaser**: The equaliser of two maps $f, g : A \to B$ is an object X equipped with a morphism $h : X \to A$ such that $f \circ h = g \circ f$. Furthermore, if $\iota : Y \to A$ satisfies $f \circ \iota = g \circ \iota$, then this diagram factors through X, i.e. there exists a unique morphism $\phi : Y \to X$ such that $\iota = h \circ \phi$.
- A **final object** in a category is universally repelling, i.e. it admits a unique morphism out of it into any other object in the category. Examples are $\{e\} \in Obj(Grp)$ and the empty set in Set.
- **Limits**: A limit is an object X with morphisms making an arbitrary diagram commute, and it is universal with respect to this property, i.e. any other object that makes the diagram commute factors through X. Products are limits of the diagram A, B with no arrows, pullouts are limits of the diagram with morphisms

$f : X \to Z$ and $g : Y \to Z$, and equalisers are limits of the diagram with $f : A \to B$ and $g : A \to B$.

- **Duality**: Every construction has a co-construction which essentially just reverses all the arrows.
- Examples of Universal objects: Note how in general, **the pullback is some subobject of the product** and the **pushout is a quotient of the coproduct**.
  - Groups:
    * Product: Direct Product with projection maps.
    * Coproduct: Free Product with inclusion maps.
    * Pullback (Fiber Product): Let $f : X \to Z$ and $g : Y \to Z$ be homomorphisms. The pullback is the subgroup of the direct product $\{(x, y) \in X \times Y : f(x) = g(y)\}$.
    * Pushout (Fiber Coproduct): Free Product with Amalgamation. This is the free product quotiented by the subgroup generated by objects of the form $\{\iota_1(f(z))\iota_2(g(z))^{-1})\}$
  - Abelian Groups:
    * Product: Direct product with projection maps.
    * Coproduct: Direct sum with inclusion maps.
    * Pullback: Let $f : X \to Z$ and $g : Y \to Z$ be homomorphisms. The pullback is the subgroup of the direct product $\{(x, y) \in X \times Y : f(x) = g(y)\}$.
    * Pushout: Let $f : Z \to X$ and $g : Z \to Y$ be homomorphisms. The pushout is the direct sum $X \bigoplus Y$ quotiented by elements of form $(f(z), -g(z))$.
  - Set:
    * Product: Cartesian Product with projection maps.
    * Coproduct: Disjoint union with inclusion maps.
    * Pullback: Let $f : X \to Z$ and $g : Y \to Z$ be maps. The pullback is the subset of the Cartesian product $\{(x, y) \in X \times Y : f(x) = g(y)\}$.
    * Pushout: Disjoint union quotiented by some equivalence relation.

7. 9/14 (Free Groups)

- **Free Abelian Group**: A free abelian group $F_{ab}(S)$ on a set S can be thought of as the set of all commuting words of elements of S. If $|S| = n$, then $F_{ab}(S) \cong \mathbb{Z}^n$, and n is called the **rank** of $F_{ab}(S)$. The rank of any subgroup of $F_{ab}(S)$ is less than or equal to the rank of $F_{ab}(S)$. A **basis** of an abelian group G is a subset $\{e_i\}_{i\in I} \subset G$ such that any element of G has a unique expression of a $\mathbb{Z}$-linear combination of the e_i. If an abelian group has a basis, it is called **free**.

  Furthermore, we have a universal property. Let $\iota : S \to F_{ab}(S)$ be the canonical inclusion map. If $\phi : S \to G$ is a map from S to **any abelian group** G, then ϕ factors through $F_{ab}(S)$, i.e. there exists a unique group homomorphism $\Phi : F_{ab}(S) \to G$ such that $\phi = \Phi \circ \iota$. If $\lambda : S \to S'$ is any set map, then we get a unique group homomorphism $\bar{\lambda} : F_{ab}(S) \to F_{ab}(S')$ where $\bar{\lambda} \circ \iota = \iota' \circ \lambda$.

- The **free group** on $\{g_1, ..., g_n\}$ is the "universal group" generated by these letters. It is the coproduct of $\mathbb{Z}$.
- Ex: Free group on $\{a, b, c\}$. It is the set of all reduced words on $\{1, a, b, c, a^{-1}, b^{-1}, c^{-1}\}$ where a reduced word takes out any aa^{-1}, etc. and the operation is concatenation. Different reduced words correspond to different elements of the free group. We can show this by considering a permutation argument if the size of the reduced word is n on S_n.
- **Universal Property**: Same as the universal property on free abelian groups, but with an arbitrary G rather than an abelian G.
- **Subgroups of Free Groups**: Suppose that $G \leq F$ for a free group F with $(F : G) = n$ finite. We can draw a picture with dots representing the cosets and the action of the generators on the cosets as the edges. This graph must be connected because each coset must be able to be multiplied into another coset, so there must be a generator that does this. Thus, **we get a correspondence between subgroups of index n and connected graphs on n points with $g_1, ..., g_n$ colored cycles**.
- **Fundamental Group**: First, we need homotopy classes. Essentially, two graphs are in the same homotopy class if we can flatten out a loop. The set of homotopy classes is a group, and the fundamental group is the group of homotopy classes of loops from the base point to itself.
- **Finding generators of subgroups**: Suppose $(F : G) = n$. Draw out the graph of F/G, where we have n vertices and the number of cycles is the number of generators of F. Then:
  1. Contract the edges of the graph with distinct vertices down to a point.
  2. Use these contractions to draw a maximal tree where you contracted the edges.
  3. To find the generators, go along the edges of the maximal tree until you find a loop, do the loop, then go back along the edge.

  We can see that a subgroup of infinite index can have infinite generators (even if F has 2 generators), so subgroups of free groups can have a larger rank than the original group.
- Free groups are **residually finite**: Nontrivial elements can be detected by maps into finite groups. More precisely, G is residually finite if for every nontrivial element $g \in G$, there is a map f from G into a finite group such $f(g) \neq 1$. This means that for any nontrivial element of a free group, there is a subgroup of finite index not containing this element, for the kernel of this map f gives the desired subgroup.
- **Number of Generators**: If $G \leq F$ has index n and G has m generators, then F has $n(m-1)+1$ generators.

  This follows because if G has m generators, then there are mn edges on the graph (as each coset has an edge into and out of it) and there are n vertices for an index n subgroup, so the Euler characteristic of the graph is $\chi = V - E = n - mn$. The number of generators is 1 minus the Euler characteristic, so the number of generators is $1 - n(1-m) = n(m-1) + 1$.