Modern Algebra II
Notes on MATH 6320

Daniel Koizumi

January 28, 2022

1 January 13

A group G is called **cyclic** if $G = \langle a \rangle$ for some $a \in G$, in which case a is a **generator**. For instance,

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$
$$= \langle 2, 3 \rangle$$

A group that is cyclic is Abelian. Rubiks cube group $< S_{48}$. It is generated by six elements,

$$\langle T, Bottom, L, R, F, Back \rangle$$

The group is

$$\left(\left(\frac{\mathbb{Z}}{2}\right)^{11} \times \left(\frac{\mathbb{Z}}{3}\right)^{7}\right) \rtimes \left((A_8 \times A_{12}) \rtimes \frac{\mathbb{Z}}{2}\right)$$

A_8 and A_{12} are alternating groups, and $\rtimes$ denotes the semi-direct product, which we will define in the future.

If $H < G$ we saw $|G| = |H| \cdot (G : H)$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$. Otherwise, a cyclic group G is isomorphic to $\frac{\mathbb{Z}}{|G|}$. We use additive notation for a group only if it is abelian. If n is a positive integer, $x \in G$,

$$n \cdot x = x + \ldots + x \ (n \text{ times})$$

Likewise,

$$(-n) \cdot x = -x - x - \ldots - x \ (n \text{ times})$$

Any Abelian group G is a $\mathbb{Z}$-module. If G is a finitely generated Abelian group, then the structure theorem for modules over a PID applies. We have

$$G \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \frac{\mathbb{Z}}{m_1} \oplus \frac{\mathbb{Z}}{m_2} \oplus \ldots \oplus \frac{\mathbb{Z}}{m_k}$$

Multiplicative notation: If $x \in G$ and n is a positive integer, then

$$x^n = x \cdot x \cdot \ldots \cdot x$$
$$x^{-n} = x^{-1} \cdot \ldots \cdot x^{-1}$$

Proposition 1.
1. An infinite cyclic group has 2 possible generators, a and a^{-1}.
2. If $G = \langle a \rangle$ is a cyclic group of order n. Then $\langle a^m \rangle = G$ if and only if m is relatively prime to n.
3. If $G = \langle a \rangle = \langle b \rangle$, then $G \to G$ defined by $a \mapsto b$ is an automorphism.
4. If G is cyclic of order n, and $d|n$, then $H = \{x \in G : \text{order of } x \text{ divides } d\}$ is a subgroup of order d.

Proof. 1.

2.

3. The map is surjective, but since it is a map of finite sets, it is also injective.

4. H contains the identity. And $x \in H$ implies that $x^{-1} \in H$. If $x^d = 1$ and $y^d = 1$, then $(xy)^d = 1$, because G is abelian.

□

If $G = \langle x \rangle$, $x^n = 1$, $n = de$, then
$$H = \{x^m : x^{m \cdot d} = 1\}.$$
Note $x^{md} = 1$ if and only if $n = de | md$ if and only if $e|m$. Note that H is the subgroup defined by
$$\left\langle x^{\frac{n}{d}} \right\rangle$$
(Can be used to show that the multiplicative group of a finite field is cyclic.) Suppose $\varphi : G_1 \to G_2$ is a group homomorphism. Let $H_2 < G_2$. Then $\varphi^{-1}(H_2)$ is a subgroup of G_1. We have
$$\varphi^{-1}(\{e_2\}) < G_1$$
But this is the kernel of φ. In fact, it is a normal subgroup, which we denote $\ker \varphi <| G_1$. We say that a subgroup is normal if $gHg^{-1} = H$ for all $g \in G$. Recall $xH = \{xh : h \in H\}$. If A, B are subsets of a group G $AB = \{ab : a \in A, b \in B\}$. Set $K = \ker(G_1 \to G_2)$. If $k \in K$ and $g \in G_1$, then
$$\varphi(gkg^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(e_1) = e_2.$$
Given $K <| G$, there is a canonical surjection $G \twoheadrightarrow \frac{G}{K}$ $g \mapsto gK$ which has kernel K. The group above is defined
$$\frac{G}{K} = \{gK : g \in G\}$$
We want to give this group its structure. So we define
$$(g_1K)(g_2K) = g_1g_2K$$
This is well defined (check this). It also makes $\frac{G}{K}$ a group. A group G acts on a set S if there is a group homomorphism $\pi : G \to \mathrm{Perm}(S)$. For each $g \in G$ we have $\pi_g : S \to S$ a bijection. Now note that the identity element of the group must be the identity of the permutation of the group. In other words,
$$\pi_{g_1g_2} = \pi_{g_1}\pi_{g_2}$$
For shorthand, we often write $\pi_g(x) = gx$ for $x \in S$.

Example. If $H < G$, then G acts on $\frac{G}{H}$ (the set of left cosets). It acts via
$$x \mapsto (gH \mapsto xgH)$$
The kernel of this homomorphism, call it π, is
$$\{x \in G \mid xgH = gH \ \forall\ g \in G\} <| G$$
If $x \in K$, then $g^{-1}xg \in H$ for all $g \in G$. In particular, it happens when $g = id$, so $x \in H$. So $K < H < G$. Since $K <| G$, we also have $K <| H$.

Proposition 2. Suppose G is a finite group and $H < G$ such that
$$p = (G : H)$$
is the smallest prime dividing $|H|$. Then $H <| G$.

Proof. We can define $G \xrightarrow{\pi} \text{Perm}(\frac{G}{H})$. Note the latter group is the symmetric group on p symbols, which is of order $p!$. Then we can factor this map through and get

$$\frac{G}{K} \to \text{Perm}(\frac{G}{H})$$

an injective map. So $(G : K)$ divides $p!$. But

$$(G : K) = (G : H)(H : K)$$

So $(G : H)(H : K)$ divides $p!$. Now $(G : H) = p$, so $(H : K)$ divides $(p-1)!$. Since p is the smallest integer dividing $|G|$, $(H : K) = 1$. Hence $H = K < |G$. $\square$

Proposition 3. If $\varphi : G_1 \to G_2$ has kernel K, then φ factors through $\frac{G}{K}$, meaning there is a suitable map $i : \frac{G_1}{K}$ making the following diagram commute:

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & G_2 \\ & G_1/K \arrow[u, hook, "i"'] \end{tikzcd}$$

where i is an injective homomorphism, and π is the canonical surjection.

Proof. Given $gK \in \frac{G_1}{K}$, define

$$i(gK) = \varphi(g)$$

this is well defined, for given any other representative $hK = gK$, so that $g^{-1}h \in K$, we have

$$i(hK) = \varphi(h)$$

but $\varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) = e_2$, so $\varphi(g) = \varphi(h)$. (Check this gives a homomorphism) $\square$

Example. (Group Action) Suppose G is a group. We have

$$\text{Aut}(G) \text{ (the group of automorphisms of } G)$$

We have a representation $G \mapsto \text{Aut}(G) < \text{Perm}(G)$ defined by $x \mapsto c_x \in \text{Aut}(G)$ where c_x is the conjugation by x.

2 January 18

Suppose $K < H < G$ and $K \lhd G$ and $H \lhd G$. Then $\frac{G}{K}$ and $\frac{G}{H}$ are groups, and

$$\frac{G}{K} \to \frac{G}{H}$$

defined by $gK \mapsto gH$. With kernel $\{gK : gH = H\} = \{hK : h \in H\} = \frac{H}{K}$. Note that $K \lhd H$ so $\frac{H}{K}$ is a group. By the first isomorphism theorem

$$\frac{G/K}{H/K} \xrightarrow{\sim} \frac{G}{H}$$

Suppose $K \lhd G$. Then subgroups of $\frac{G}{K}$ correspond to subgroups of G that contain K. Likewise, normal subgroups of G/K correspond to normal subgroups of G that contain K. Recall: If A, B are subsets of G then

$$AB = \{ab \mid a \in A, b \in B\}$$

Let $S \subset G$. Then $N_S = \{x \in G \mid xSx^{-1} = S\} < G$ is a subgroup of G, called **normalizer** of S in G. Define

$$Z_S = \{x \in G \mid xsx^{-1} = s \forall s \in S\} < G$$

is the centralizer of S in G.

Z_G is the center of the group G. If $H < G$ then $H < N_H < G$. In fact, $H \lhd N_H$ by definition. Let H, K be subgroups of G and $H \subset N_K$. Then $H \cap K \lhd H$. For $s \in H \cap K$ and $h \in H$,

$$hxh^{-1} \in H$$

it is also in K since $h \in N_K$, $x \in K$.

$H \subset N_K$ gives $HK = KH$, which is a group (check).

Exercise 1

Define $\varphi : H \to \frac{HK}{K}$ via $x \mapsto xK$. Check that this is a group homormophism. Also check this is surjective and $\ker \varphi = H \cap K$. We also have by the first isomorphism theorem

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

We stopped last time at the action of a group G on itself via conjugation. $G \to \mathrm{Aut}(G)$ maps via $x \mapsto \left(g \mapsto xgx^{-1}\right)$. (Note the distinction between automorphism and permutation: permutations are not necessarily homomorphisms). The kernel of the action is the center of the group. The image of $G \to \mathrm{Aut}(G)$ is the group of inner automorphisms denoted $Inn(G)$.

Proposition 4. *$Inn(G) \lhd Aut(G)$.*

Proof. Let $\varphi \in Aut(G)$, $c_x \in Inn(G)$. We would like to check that

$$\varphi \circ c_x \circ \varphi^{-1} \in Inn(G)$$

$$\varphi \circ c_x \circ \varphi^{-1}(g) = \varphi(x\varphi^{-1}(g)x^{-1}) = \varphi(x)g\varphi(x^{-1}) = c_{\varphi(x)}(g)$$

□

We are obliged to construct

$$\frac{Aut(G)}{Inn(G)} = Out(G)$$

Suppose G acts on S. Let $s \in S$. Define

$$G_s = \{x \in G : xs = s\}.$$

This is called the **stabilizer of the isotropy subgroup**. This is not to be confused with $G \cdot s = \{xs \mid x \in G\}$, which is called the **orbit of** s. Suppose $t \in G \cdot s$. Then we compare G_s and G_t. In fact, we have G_t is conjugate to G_s. We have

$$G_t = \{x \in G \mid xt = t\} = \{x \in G \mid xys = ys\}$$
$$= \{x \in G \mid y^{-1}xys = s\} = \{x \in G \mid y^{-1}xy \in G_s\} = yG_sy^{-1}$$

Set $K = \ker(G \to Perm(S))$. We can write $K = \bigcap_{s \in S} G_s$. We say that the action of G on S is faithful if $K = \{e\}$. Fixed points in S are those such that $xs = s \forall x \in G$.

Let $s \in S$. We can define $G \to Gs$ by $x \mapsto xs$. This yields a map $\frac{G}{G_s} \to Gs\ xG_sxs$. If $xG_s = yG_s$, then $y^{-1}x \in G_s$. So $yx^{-1}s = s$ so $xs = ys$. Hence the map is well defined, surjective, and injective. Hence $\frac{G}{G_s \to Gs}$ is a bijection. We have

$$|Gs| = (G : G_s)$$

Two orbits Gs and Gt are either equal or disjoint. If they shared an element $gs = ht$. But this implies $Gs \subset Gt$, since for any $g's \in Gs$, $g's = g'g^{-1}gs = g'g^{-1}ht \in Gt$. Similarly, $Gt \subset Gs$. We can then write

$$S = \bigcup Gs_i$$

so $|S| = \sum |Gs_i| = \sum (G : G_{s_i})$. Class formula?

Let G act on a set S. The action is transitive if for some $s \in S$ $Gs = S$. Equivalently, we say the same if there is only one orbit.

The action of G on S restricts to an action on each orbit. On each orbit, the group is transitive.

Theorem 1. Cauchy's theorem: Suppose G is a finite group and p is a prime dividing $|G|$. Then G has an element of order p.

Definition 1. Let p be a prime integer. A group G is a p-group if $|G| = p^n$ for some $n \in \mathbb{N}$.

Lemma 1. Suppose G is a $p-$ group acting on a set S. Let $F =$ fixed points in$S = \{s \in S \mid xs = s \forall x \in G\}$. Then $|S| \equiv |F|$ modulo p.

Proof. Apply the class formula $|S| = \sum (G : G_{s_i})$. We have $|S| = |F| + \sum_{\text{other } i} (G : G_{s_i})$. For $s_i \notin F$, $G_{s_i} \subsetneq G$, so $p | (G : G_{s_i})$. ☐

Proof. (of Cauchy's theorem): Let $S = \{(x_1, \ldots, x_p) \mid x_i \in G, x_1 \cdots x_p = e\}$. We have

$$|S| = |G|^{p-1}.$$

Define $\sigma \in \text{Perm}(S)$ by $\sigma : (x_1, \ldots, x_p) \mapsto (x_p, x_1, \ldots, x_{p-1})$. We have

$$x_1 \ldots x_{p-1} = x_p^{-1}$$

$$x_p x_1 \ldots x_{p-1} = e$$

So σ maps elements of S to S. σ has order p. Hence $\langle \sigma \rangle$ is a p-group acting on S, so $|F| \equiv |S| \mod p$ by the lemma. But $|S| \equiv 0 \mod p$, since p divides $|G|$ which divides $|S|$. $e, \ldots, e) \in F$, so $|F| \geq p$. But elements of F are of form $(x, \ldots, x)$, which implies that any nonidentity in F corresponds to a desired element. ☐

Suppose p divides $|G|$ and p is a prime. Let p^n be the highest power of p dividing $|G|$.

Theorem 2. G has a subgroup of order p^n. Such a subgroup called a p-Sylow subgroup.

Lemma 2. Fix a prime p dividing $|G|$. Suppose G acts on S with the property that $\forall s \in S$,there exists a p-subgroup of G that fixes only s. Then the action of G is transitive.

Proof. Suppose P is a p-subgroup fixing only $s \in S$. We have that $|S| \equiv 1 \mod p$ by a preceding lemma. If S has multiple orbits, we can write

$$S = S_1 \cup S_2$$

a disjoint union. Each subset has the same property as S that satisfies the theorem hypotheses, so $|S_1| \equiv 1 \mod p$ and $|S_2| \equiv 1 \mod p$. Hence

$$|S| \equiv |S_1| + |S_2| \mod p$$

implies

$$|S| \equiv 2 \mod p$$

Hence the action is transitive. ☐

3 January 20

Let G be a finite group, p be a prime dividing $|G|$. A **p-Sylow subgroup of** G is a subgroup of order p^n where p^n is the highest power of p dividing $|G|$.

Theorem 3. If a prime p divides $|G|$, then a p-Sylow subgroup exists.

Proof. We will work on induction on $|G|$. If $|G| = p$, then we are done, since G is the desired group. If $H < G$ and $p \not| (G : H)$ (so that in this case the highest power of p dividing $|G|$ is also the highest power for $|H|$), then a $p-$ Sylow subgroup of H is also a p-Sylow subgroup of G. We may therefore assume that for all subgroups $H \subsetneq G$, we have $p|(G : H)$.

Let G act on itself via conjugation

$$G \to \mathrm{Aut}(G)$$

The kernel of the homomorphism is also the center of the group denoted Z. Use the class equation:

$$|G| = |Z| + \sum_i (G : G_{x_i})$$

Here G is the set, Z is the set of fixed points, and the last set is the size of larger orbits. Here G_{x_i} is an isotropy subgroup, so $(G : G_{x_i})$ is the cardinality of the orbit of x_i. By our hypothesis, $(G : G_{x_i})$ is divisible by p for all i.

So $|G| \equiv |Z| \mod p$. This implies that p divides the order of Z since $|G| \equiv 0 \mod p$. We have $e \in Z$, so that $\exists a \in Z$ of order p by Cauchy's theorem. Now $\langle a \rangle$ has order p, and $a \in Z$ implies

$$\langle a \rangle \lhd G.$$

$\frac{G}{\langle a \rangle}$ has smaller order than G, so it must have some p-Sylow subgroup P by induction hypothesis. Then $|P|$ is p^{n-1} where p^n is the highest order of p dividing $|G|$. Now note that P corresponds to a subgroup of G which must have order p^n. It is $\varphi^{-1}(P)$ where

$$\varphi : G \to \frac{G}{\langle a \rangle}$$

is the natural map. □

Lemma 3. Suppose A, B are finite subgroups of G. Then AB is a set of products of elements of A, B. Then $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$.

Proof. $A \cap B < A$, so A can be written as a disjoint union of cosets

$$\bigsqcup_{i \in I} a_i (A \cap B)$$

for some $a_i \in A$. So

$$AB = \bigcup_{i \in I} a_i (A \cap B) B$$
$$= \bigcup_{i \in I} a_i B$$

Claim: $AB = \bigsqcup_{i \in I} a_i B$ (the unioin is disjoint)

If $a_i b = a_j b'$ for $i \neq j$, $b, b' \in B$, then

$$a_i = a_j b' b^{-1}$$

so that $a_j^{-1}a_i = b'b^{-1} \in A \cap B$ so that

$$a_i \in a_j(A \cap B)$$

and $i = j$.

Claim yields

$$|AB| = \sum_{i \in I} |a_i B| = |I| \cdot |B| = |B| \cdot \frac{|A|}{|A \cap B|}$$

□

Theorem 4. Let p be a prime dividing $|G|$. Then:

1. Each p-subgroup is contained in a p-Sylow subgroup
2. The p-Sylow subgroups are conjugate.
3. Let s_p be the number of p-Sylow subgroups. Then $s_p \big| |G|$ and $s_p \equiv 1 \mod p$.

Proof. Let $\mathcal{S}$ be the set of all p-subgroups. Then G acts on $\mathcal{S}$ by conjugation, since $|H| = |xHx^{-1}|$. Let $\mathcal{M}$ be the set of maximal elements of $\mathcal{S}$ (under inclusion). Claim: The action restricts to an action on $\mathcal{M}$. Let $p \in \mathcal{M}$. Suppose $xPx^{-1} \subset Q$ for some $Q \in \mathcal{S}$. Then $P \subset x^{-1}Qx \in \mathcal{S}$. But P was maximal, so $P = x^{-1}Qx$. This implies $xPx^{-1} = Q$, so that xPx^{-1} is maximal.

Now note that any p-Sylow subgroup must be in $\mathcal{M}$. We would like to prove that any $P \in \mathcal{M}$ is a p-Sylow subgroup, giving property 1 above. We know G acts on $\mathcal{M}$ by the above argument. If P is a p-Sylow subgroup, then $P \in \mathcal{M}$. Since G acts on $\mathcal{M}$, any subgroup also does. In particular, P acts on $\mathcal{M}$ via conjugation, and P fixes P since $xPx^{-1} = P \forall x \in P$. Suppose P fixes some $Q \in \mathcal{M}$. Then $xQx^{-1} = Q$ for all $x \in P$, so $P < N_Q$, and PQ is a subgroup of G. So

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}$$

($|P|, |Q|$ are powers of p and the quotient is an integer, so it must be a power of p) so PQ is a p-group. Then P, Q are maximal, so $P \subset PQ$ implies $P = PQ$ and $Q \subset PQ$ implies $Q = PQ$. So $P = Q$.

We have that P acts on $\mathcal{M}$ and fixes **only** itself. This implies the action by P is transitive by a previous lemma from class, which we recall:

Remark. Fix prime p. If G acts on $\mathcal{S}$ with the property that $\forall s \in S$, $\exists$ a p-subgroup fixing only s, then G is transitive on S.

In our context, G acts on $\mathcal{M}$. Each $P \in \mathcal{M}$ is a p-group that fixes **only** $P \in \mathcal{M}$. Hence G is transitive on $\mathcal{M}$. But then $\mathcal{M}$ is precisely the set of p-Sylow subgroups, and they are all conjugate. This also gives us property 2. Lastly, we figure out the deal with s_p. We know $s_p = |\mathcal{M}|$. $P \in \mathcal{M}$ acts on $\mathcal{M}$ with 1 fixed point, so $|\mathcal{M}| \equiv (\text{number of fixed points} = 1) \mod p$. So $s_p \equiv 1 \mod p$. Now also G is transitive on $\mathcal{M}$, so $|\mathcal{M}| = (G : G_P)$ for $P \in \mathcal{M}$. Hence $s_p = \frac{|G|}{|G_P|}$. We have 3. □

Example. Suppose $|G| = 15$. We look at s_3, s_5. By the above theorem, $s_3 \equiv 1 \mod 3$ and $s_3 | 15$, so $s_3 = 1$.

We also have $s_5 \equiv 1 \mod 5$, $s_5 | 15$, implies $s_5 = 1$.

In general $s_p = 1$ if and only if a (the) p-Sylow is normal.

If Q is a 5-Sylow, then $(G : Q) = 3$, which is the smallest prime dividing $|G| = 15$. This implies that Q is normal. This is an alternative way to see that $s_5 = 1$.

Say $|P| = 3, |Q| = 5$. Then $PQ = 15$, so $PQ = G$. We can say more: let $[P, Q] = \langle [p, q] : p \in P, q \in Q \rangle$ where $[p, q] = pqp^{-1}q^{-1}$ (the commutator). If $P \lhd G$, $Q \lhd G$, then $pqp^{-1}q^{-1} \in P \cap Q$ so that in particular elements of P commute with those of Q (see proposition ahead). So

$$P \times Q \xrightarrow{(p,q)\mapsto pq} G$$

is a group homomorphism. We have

$$(p_1, q_1) \mapsto p_1q_1$$

$$(p_2, q_2) \mapsto p_2q_2$$

$$(p_1, q_1)(p_2, q_2) = p_1q_1p_2q_2 = p_1p_2q_1q_2$$

We know that the only groups of order $3, 5$ respectively are $\frac{\mathbb{Z}}{3}$, $\frac{\mathbb{Z}}{5}$. Hence G must be $\frac{\mathbb{Z}}{15}$.

Proposition 5. Suppose

1. $P \lhd G$, $Q \lhd G$
2. $PQ = G$
3. $P \cap Q = \{e\}$

Then $G \cong P \times Q$.

Proof. Consider $pqp^{-1}q^{-1}$ for $p \in P, q \in Q$. Now because $P \lhd G$, $qp^{-1}q^{-1} \in P$ and so $pqp^{-1}q^{-1} \in P$. Likewise, $Q \lhd G$ implies $pqp^{-1} \in Q$ and $pqp^{-1}q^{-1} \in Q$. Hence

$$pqp^{-1}q^{-1} \in P \cap Q = \{e\}$$

so that $pqp^{-1}q^{-1} = e$. In other words, $pq = qp$. Now define $P \times Q \to G$ by

$$(p, q) \mapsto pq$$

The fact that elements of P commute with those of Q ensures that this is a group homomorphism. It is surjective because of property 2. It is also injective. Given (p, q) mapping to e, we have $pq = e$. But $p = q^{-1} \in P \cap Q = \{e\}$, so that $p = e = q$. Hence it is also injective. $\square$

4 January 25

Last time: Let G be a finite group and p be a prime dividing $|G|$. Then each subgroup is contained in a p-Sylow subgroup. Only 2 p-Sylow subgroups P, Q are conjugate. If s_p is the number of p-Sylow subgroups, then

$$s_p \big| |G|$$

and $s_p \equiv 1 \mod p$.

Corollary 1. Suppose that $|G| = pq$ where $p \neq q$ are primes. Suppose $p < q$, and that $p \not| q - 1$. Then G is cyclic.

Proof. Let Q be a q-Sylow subgroup. Its index is p, which is the smallest prime dividing the order of G, which implies $Q \lhd G$. Alternatively, $s_q \equiv 1 \mod q$ and $s_q \big| |G|$ so $s_q = 1$. Therefore $xQx^{-1} = Q$ for all $x \in G$.

Q is normal, so conjugation by any element of G takes Q to itself. That is $\forall x \in G$

$$c_x : Q \to Q$$

An automorphism of Q is determined by one is sent in $Q \cong \frac{\mathbb{Z}}{q}$, so $AutQ \cong \frac{\mathbb{Z}}{q}^*$ (multiplicative group which is of order $q-1$).

We have a map $G \to \frac{\mathbb{Z}}{q}^*$. Since p doesn't divide $q-1$, the map must be trivial.

Restating, $G \to \text{Aut}Q$ must be trivial, ie, $xyx^{-1} = y$ for all $y \in Q$. This means Q is a subgroup of $Z(G)$.

If we take an element x of order p, $y \in Q$ of order q, then xy has order pq. Hence xy generates G. Note that Q is cyclic because any element divides the order of Q, so there is a generator of Q. □

Suppose $|G| = pq$ where $p \neq q$ are primes. Say $p < q$. Then there exists q-Sylow Q, $Q \lhd G$, and we can't say that G is necessarily cyclic, but we have $G \rhd Q \rhd \{e\}$. We have $\frac{G}{Q}$ and $\frac{Q}{\{e\}}$ is cyclic. We will eventually define G to be in this case a **solve-able group**. We say $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{e\}$ is a **normal tower** of subgroups of G. A normal tower as above is a **cyclic tower** if $\frac{G_i}{G_{i+1}}$ is cyclic for all i. It is an **abelian tower** if $\frac{G_i}{G_{i+1}}$ is abelian for all i. For instance $\mathbb{Q} \rhd \{1\}$ is an Abelian tower but not a cyclic tower.

A group G is **solvable** if it has an abelian tower. Note:

- Abelian groups are solvable. Because $G \rhd \{e\}$ works.
- If $|G| = pq$ for primes $p \neq q$ then G is solvable.
- Let's examine $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$, which is solvable.

Definition 2. $G \to \mathbb{R}^\times \times \mathbb{R}^\times$ where G is as above, and define

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

which is a group homomorphism. The group of the latter matrices is isomorphic to $\mathbb{R}^\times \times \mathbb{R}^\times$. The kernel is

$$K = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{R} \right\}$$

Since the map is surjective,

$$\frac{G}{K} \cong \left(\mathbb{R}^\times\right)^2$$

So $G \rhd K \rhd \{1\}$, which gives the abelian tower.

- (Feil-Thompson Theorem 1963, 255 pages :O) Any group of odd order is solvable.

We will see soon that for $n \geq 5$, the group S_n is **not** solvable.

Corollary 2. Overkill consequence of the Feil-Thompson theorem) $|S_5| = 120$ is even.

Given a group G, what is the smallest normal subgroup you could mod out by to make it abelian? We define

$$G' = \left\langle [a, b] = aba^{-1}b^{-1} : a, b \in G \right\rangle$$

where $[a, b]$ denotes a commutator. In other words G' is generated by the commutators of G. Then $G' \lhd G$. We prove normality: given $x \in G$, and $aba^{-1}b^{-1} \in G'$,

$$xaba^{-1}b^{-1}x^{-1} = [xax^{-1}, xbx^{-1}]$$

In $\frac{G}{G'}$, we have that $aG'bG'a^{-1}G'b^{-1}G' = eG'$, so $\frac{G}{G'}$ is commutative. Conversely, if $N \lhd G$ and $\frac{G}{N}$ is abelian, then

$$G' \subset N$$

The reason is that $aNbNa^{-1}Nb^{-1}N = eN$ implies

$$aba^{-1}b^{-1}N = eN$$

or $[a,b] \in N$, so $G' \subset N$.

Remark. Any homomorphism $G \to H$ with H abelian factors as $G \to \frac{G}{G'} \to H$ where the composition is the original map.

Proposition 6. Suppose $H \lhd G$. Then G is solvable if and only if H and $\frac{G}{H}$ are solvable.

Proof. Lets prove the if direction. If we have abelian tower

$$H = H_0 \rhd H_1 \rhd \ldots \rhd H_m = \{e\}$$

and abelian tower of $\frac{G}{H}$, we can get

$$\frac{G}{H} \rhd \frac{G_1}{H} \rhd \frac{G_2}{H} \rhd \ldots \rhd \frac{G_n}{H}\frac{H}{H}$$

where G_1 is a normal subgroup of G, G_i is a normal subgroup of G_{i-1}, and

$$\frac{G_i/H}{G_{i+1}/H}$$

Then G is solvable since we have abelian tower

$$G \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = H \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_m = \{e\}$$

Now we prove the only if direction. Suppose there exists Abelian tower

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$$

and define $H_i = G_i \cap H$. We have a natural inclusion

$$H_i \hookrightarrow G_i$$

and map

$$H_i \to \frac{G_i}{G_{i+1}} = H_i \cap G_{i+1} = (G_i \cap H \cap G_{i+1}) = H_{i+1}$$

Now we have an induced map

$$\frac{H_i}{H_{i+1}} \hookrightarrow \frac{G_i}{G_{i+1}}$$

To see $\frac{G}{H}$ is solvable, use

$$\frac{G}{H} = \frac{G_0}{H} \rhd \frac{G_1}{G_1 \cap H} \rhd \frac{G_2}{G_2 \cap H} \rhd \ldots \rhd \frac{G_n}{G_n \cap H} = \{e\}$$

and we have

$$\frac{G_i/G_i \cap H}{G_{i+1}/G_{i+1} \cap H} \cong G_i/G_{i+1}$$

which is abelian by assumption. The isomorphism comes from the first isomorphism theorem (exercise for later maybe). ☐

We now provide a more formal discussion on symmetric groups. We look at $S_n = \text{Perm}\{1, \ldots, n\}$. Let $e_1, \ldots, e_n$ be standard basis vectors for $\mathbb{R}^n$. We can view S_n as $\text{Perm}\{e_1, \ldots, e_n\}$, and it provides an action on $\mathbb{R}^n$. Each element of S_n acts on $\mathbb{R}^n$ as a permutation matrix. For $\sigma \in S_n$, define $\text{sgn}(\sigma) = \det(\text{permutation matrix of } \sigma) = \pm 1$. An element $\pi \in \text{Perm}\{1, \ldots, n\}$ can be written as

$$\begin{pmatrix} 1 & 2 & .. & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

Fix π as above. Let $\langle \pi \rangle$ act on $\{1, \ldots, n\}$, and like any group acting on any set it partitions it into disjoint orbits. We can use this to write π in **cyclic notation**. The action of π on each orbit can be represented as a **cyclic** permutation.

Example. A **cyclic permutation** can for instance be written $(1, \pi(1), \pi^2(1), \pi^3(1), \ldots, \pi^m(1))$ where m is the smallest integer so that $\pi^{m+1}(1) = 1$.

5 January 27

Last time, we defined $\text{sgn}\pi$, for π a permutation, as the determinant of the corresponding matrix. Notation:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

Alternatively, we can write π with cyclic notation. Consider the orbits of $\langle \pi \rangle$ acting on $\{1, \ldots, n\}$. We can write each cycle as

$$(1\ \pi(1)\ \pi^2(1)\ \ldots\ \pi^{k-1}(1))$$

and likewise for other orbits. Since orbits partition the entire set into disjoint subsets, π can be expressed as a product of disjoint cycles.

Example. Consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$
$$= (1)(2\ 5)(3\ 4) = (2\ 5)(3\ 4)$$

Example. We can compose cycles: $(1\ 2\ 3)(3\ 4\ 5) = (1\ 2\ 3\ 4\ 5)$ Also note that the order of a cycle is discernible from its length. The above cycle has order 5. Also, for example, $(1\ 2\ 3)(4\ 5)$ has order 6.

We have

$$\pi(x_1\ x_2\ \ldots\ x_k)\pi^{-1} = (\pi(x_1)\ \ldots\ \pi(x_k))$$

Check that:

$$\left(\pi(x_1\ x_2\ \ldots\ x_k)\pi^{-1}\right)(\pi(x_i)) = \pi(x_{i+1})$$

(maybe except when $i = k$, in which case the resulting element is $\pi(x_1)$. We have

$$\left(\pi(x_1\ x_2\ \ldots\ x_k)\pi^{-1}\right)(\pi(y)) = \pi(y)$$

for $y \neq x_i$ for all i. By the cycle structure of $\sigma \in S_n$, we mean the number of 2 cycles, number of 3 cycles, etc when σ is written as disjoint cycles. Disjoint cycles commute, so the order doesn't matter. By what we have proved above, conjugation preserves the cyclic structure. For example,

$$\pi(1\ 2)(3\ 4\ 5)\pi^{-1} = (a\ b)(c\ d\ e)$$

We have

- Each element of S_n can be written as a product of disjoint cycles.
- It can be wirtten as a product of 2-cycles (ie we can write it as a product of transpositions).

- Every element can be written as a product of 2-cycles involving 1. For example,

$$(2\ 3) = (1\ 2)(1\ 3)(1\ 2)$$

- $S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$. We can also write

$$S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$$

- $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle$. If we call the latter generator π, we have this because $\pi(1\ 2)\pi^{-1} = (2\ 3)$, and so on, giving the generators for the previous item.

We have a caveat:

$$S_4 \neq \langle (1\ 3), (1\ 2\ 3\ 4) \rangle$$

Call the former $\sigma = (1\ 3)$ and $\tau = (1\ 2\ 3\ 4)$. We have

$$\sigma\tau\sigma^{-1} = (3\ 2\ 1\ 4) = (4\ 3\ 2\ 1) = \tau^{-1}$$

so $\langle \tau \rangle \lhd \langle \sigma, \tau \rangle = \langle \sigma \rangle \langle \tau \rangle$. We will later come to the conclusion that this is a **dihedral group**. On the other hand, τ is not a normal subgroup of S_4, because

$$(1\ 2)\tau(1\ 2) = (2\ 1\ 3\ 4) \notin \langle \tau \rangle$$

Let p be prime. Then $S_p = \langle (1\ 2), \tau \rangle$ for any p-cycle τ. because some power of τ has the form $(1\ 2\ 3\ \ldots\ p)$. In other news, we have

$$\mathrm{sgn} : S_n \to \{\pm 1\}$$

is a group homomorphism, since determinants are multiplicative. We call $A_n = \ker \mathrm{sgn}$, called the **alternating group**. We automatically have $A_n \lhd S_n$ because it is a kernel. If $n \geq 2$, $(S_n : A_n) = 2$. Also $\mathrm{sgn}(i\ j) = -1$.

Elements of A_n are precisely those that are a product of an even number of 2-cycles. We can make a conclusion about the commutator subgroup S_n'. We have $S_n' \subset A_n$. Are they always equal? Let's look at examples:

$$S_1' = A_1$$

$$S_2' = A_2$$

After some work, $S_3' = A_3$.

Lemma 4. A_n is generated by 3-cycles.

Proof. If $n = 1, 2$ then this is vacuously true. For $n = 3$,

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

so it is true for $n = 3$. Otherwise, any element can be written an even product of 2-cycles. Each pair is a product of 3-cycles:

$$(1\ 2)(2\ 3) = (1\ 2\ 3)$$

$$\begin{aligned}(1\ 2)(3\ 4) &= [(1\ 2\ 4), (1\ 2\ 3)]\\ &= (1\ 2\ 4)(1\ 2\ 3)(4\ 2\ 1)(3\ 2\ 1)\\ &= (1\ 2\ 4)(4\ 3\ 2) = (1\ 2)(3\ 4)\end{aligned}$$

□

Proposition 7. $S_n' = A_n$.

Proof. $\subset$ is true as remarked before the lemma. For $\supset$, it suffices to do it for $n \geq 3$ (we already noted $n = 1, 2$). Note

$$[(1\ 2\ 3), (1\ 2)] = (1\ 2\ 3)(1\ 2)(3\ 2\ 1)(1\ 2) = (1\ 2\ 3)(3\ 1\ 2) = (1\ 3\ 2)$$

So S_n' contains $(1\ 3\ 2)$, and hence every 3-cycle by a similar argument. $\square$

Proposition 8.

$$A_1' = A_1$$
$$A_2' = A_2$$
$$A_3' = \{e\}$$
$$A_4' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = N$$
$$A_n' = A_n\ \forall\ n \geq 5$$

Proof. By explicit calculation, N is a subgroup. Conjugation preserves cycle structure, and N contains all of the possible pairs of disjoint 2-cycles. So conjugation by any element gives back an element in N.

$$\left|\frac{A_4}{N}\right| = 3$$

SO A_4/N is Abelian. Hence $A_4' \subset N$. But

$$(1\ 2)(3\ 4) \in A_4'$$

which is equal to

$$[(1\ 2\ 4), (1\ 2\ 3)]$$

The typical element of N can be written as a commutator. Hence $A_4' = N$. We now prove the conclusion for $n \geq 5$.

We saw $[(1\ 2\ 3), (1\ 2)] = (1\ 3\ 2)$. We do have, however

$$[(1\ 2\ 3), (1\ 2)(4\ 5)] = (1\ 3\ 2)$$

giving us all 3-cycles. $\square$

Corollary 3. If $n \geq 5$, we have $A_n^{(k)} = A_n \forall k \geq 1$. Recall that $G' = [G, G] = \langle [\sigma, \tau] : \sigma, \tau \in G \rangle$. We now define

$$G^{(2)} = G'' = (G')'$$

and so on for $G^{(n)}$.

We also have A_4 is solvable because $A_4 \rhd N \rhd \{e\}$ is an Abelian tower. $|\frac{A_4}{N}| = 3$ so its abelian. Also, $|N| = 4$, so it is also abelian (in particular, it is $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$). Our corollary implies that A_n is not solvable. Anything that contains the commutator which we would mod out by to make an Abelian group must be the entirety of A_n, which is no abelian alone.

Proposition 9. G is solvable if and only if $G^{(n)} = \{e\}$ for some n.

Proof. The if direction comes from our previous discussion. Because then

$$G = G^{(0)} \triangleright G^{(1)} \triangleright \ldots \triangleright G^{(n)} = \{e\}$$

is an Abelian tower. For the other direction, if G is solvable, we have

$$G = G_0 \triangleright G_2 \triangleright G_3 \triangleright \ldots \triangleright G_m = \{e\}$$

where G_i/G_{i+1} is abelian for all i. This fact says $G_0' \subset G_1$, and $G_i' \subset G_{i+1}$ in general. We have that $G_0^{(n)} \subset G_n$, so $G^{(m)} = \{e\}$. □

We saw $S_n' = A_n$ for all n. The shape of the tower for symmetric groups?

$$S_2' = \{e\}$$

$$S_3 \triangleright S_3' = A_3 \triangleright \{e\}$$
$$S_4 \triangleright S_4' = A_4 \triangleright A_4' = N \triangleright \{e\}$$
$$S_5 \triangleright S_5' = A_5 \triangleright A_5' = A_5 \triangleright \ldots$$

so S_5 not solvable. We would like to prove that A_5 and higher are simple in some future class. For now, we talk about dihedral groups.

$$A_n < S_n$$

Definition 3. $D_n < S_n$ is the group of rigid symmetries of a regular n-gon. Meaning:

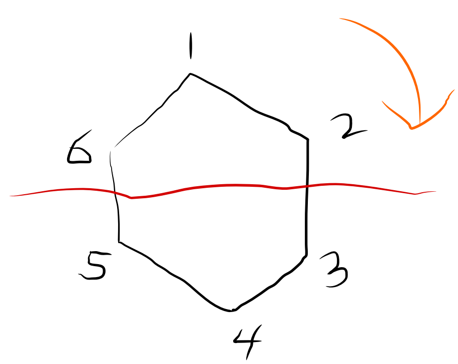

Figure 1: Symmetries include rotations and reflections

We have two kinds of elements in D_n :

- Rotations $a = (1\ 2\ \ldots\ n)$ and
- Reflections

$$b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

We have $b^2 = e$, $a^n = e$. We also have

$$bab^{-1} = (1\ n\ n-1\ \dots\ 2) = a^{-1}$$

Said otherwise,

$$\langle a \rangle \lhd \langle a, b \rangle$$

and

$$\langle a, b \rangle = \langle b \rangle \langle a \rangle$$

is a group of order $2n$. One might ask if a and b together give us other reflections. Is D_n solvable? Yes!

$$D_n \rhd \langle a \rangle \rhd \{e\}$$

shows that D_n is solvable, since

$$\left| \frac{D_n}{\langle a \rangle} \right| = 2$$

What is D_n'?

$$[a, b] = aba^{-1}b^{-1}$$

$$= (1\ 2\ \dots\ n)(2\ 3\ \dots\ n\ 1) = a^2$$

So $a^2 \in D_n'$. And $\left| \frac{D_n}{\langle a^2 \rangle} \right| = 4$.