Brilliant: Group Theory

Dave Fetterman

2/23/22

Note: Latex reference: http://tug.ctan.org/info/undergradmath/undergradmath.pdf

1 Chapter 1.2

1.1 Page 1

$R(R_1(x)) = A \to B, B \to A, C \to C$. So reflection about CE.

1.2 Page 2

$R_2(R_1(x)) = A \to B, B \to C, C \to A$. So rotation clockwise 120°

1.3 Page 5

$R \star R = H \star H = V \star V = I$ on the letter "I".

1.4 Page 6 - 9

Cayley table for rotating letter "I":

	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

Note: check out https://www.tablesgenerator.com/ here.

1.5 Page 10

- Klein four group: $(+, [0,1] \times [0,1])$ is equivalent to the "I" rotation.
- First coord could be: Does it rotate?

- Second coord could be: Does it flip?

2 Chapter 1.3: Group Properties

Group Properties

- Some binary operation $(\cdot)$
- Identity (counterexample: even integers)
- Inverse (counterexample: integers with multiplication modulo non-prime p)
- Associativity (counterexample - on reals with an average $f(x, y) = (x + y)/2$)?

3 Chapter 1.4: Cube symmetries

One way to think about it

- Corner A maps to one of eight corners
- Each mapping has three orientations of that corner spin (0 degrees, 120, 240)
- Therefore 24.

Another way:

- One identity = 1
- Type I: Rotate around line joining two opposite face centers: 3 pairs * 3 non-identity spins = 9
- Type II: Spin around line joining two opposite corners. 4 pairs * 2 non-identiy spins = 8
- Type III: Spin 180 degrees around line from front upper edge to back lower edge. Combo of a spin and a rotate. 6 pairs = 6.
- Sum to 24.

Another way:

- There are four diagonals to a cube.
- Their permutations are in 1:1 correspondence with the transformations possible. (24)
- Type I keeps none fixed. 90 degrees: Chain = 4!/4 = 6. 180 degrees: two pairs. Select who A matches = 3.
- Type II rotates three, keeps one fixed = 8

- Type III does one swap, keeps two fixed = $\binom{4}{2} = 6$

Note also: There are 24 reflection symmetries as well. (1:1 correspondence with rotations via "swap top center labels?")

4 Chapter 2.1

4.1 Page 2-3

The integers under multiplication are not a group, as they have no inverse. The set of rationals with multiplication as the group operation is not a group as 0 has no inverse

4.2 Page 5 - 7

- Dihedral group D_n has $2n$ elements, is not commutative, not cyclical.
- If n is even, there is exactly one rotational symmetry $R \neq I$ which commutes with all the other elements of D_n (the 180 degree rotation)

4.3 Page 8 - 9

- Symmetric group S_n is the set of permutations on n elements.
- "in-shuffle" of a deck of four cards is "split in half, interleave top half with bottom half, top card second", or $\phi = (1, 2, 4, 3)$. $\phi^4 = I$

4.4 Page 10-11

- Cyclic group $\mathbb{Z}_n$ is the set of integers modulo n under addition.
- Note that though usually multiplication is the default group operation, this usually uses "+".

5 Chapter 2.2: More Group Examples

5.1 Page 1-2

- **Order of an element** g is smallest k such that $g^k = e$. Otherwise **infinite order**

5.2 Page 3

Quaternion group Q_8 rules:

- $i^2 = j^2 = k^2 = ijk = -1$

- Implies $ij = k, jk = i, ki = j$
- implies $ji = -k, kj = -i, ik = -j$
- So this is not only *non-commutative* but *anti-commutative*
- $Q = \pm 1, \pm i, \pm j, \pm k$
- So one element of order 1, one of order 2 (element -1), remaining six of these elements have order 4

5.3 Page 4

Note that musical notes ($\mathbb{Z}_{12}$) has only generators 1, 5, 7, 11. These corresponding to chromatic, circle of fourths (anti-fifths), circle of fifths, downwards chromatic scales!

5.4 Page 5

- $GL_n(\mathbb{R})$ is invertible n x n matrices in R.
- $SL_n(\mathbb{R})$ is determinant 1 n x n matrices in R.
- $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ has order 2, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ has order 2, but $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order! Non-commutativity strikes.

5.5 Page 6-11

- **isomorphism** is a bjiection preserving group operations.
- Can think of it as a relabeling of the Cayley table.
- Example given is Klein-four and symmetries of tall serif letter "I", or of a diamond/non-square rhombus.
- $\mathbb{Z}_{12}$ is isomorphic to rotational symmetries of a 12-gon.
- Q_8 is isomorphic under matrix multiplication to $\left\{ \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\} \subset GL_2(\mathbb{R})$
- D_3 is isomorphic to S_3 since any permutation is possible in D_3 and no more.

6 Chapter 2.3: Subgroups

6.1 Page 1 - 3

- Subgroups are closure-bound subsets of groups.
- Easy test: $H \subset G$ if for every $h_1, h_2 \in H, h_1 h_2 \in H$, and for any $h \in H, h^{-1} \in H$.

6.2 Page 4

- Cartesian product of groups G, H is also a group: $G \times H = (g, h) \cdot (g', h') = (gg', hh'), g \in G, h \in H$. Also called the **direct product**

6.3 Lagrange's theorem

Theorem: Order of every subgroup divides the containing group.

Lemma: If $H \subset G$. and $r, s \in G$ then $Hr = Hs \iff rs^{-1} \in H$. Otherwise, Hr, Hs have no element in common.

One direction: $rs^{-1} \in H \rightarrow Hr = Hs$

- $rs^{-1} = h \in H$ by supposition
- $H = Hh = Hrs^{-1}$
- $Hr = Hs$

Other direction: $Hr = Hs \rightarrow rs^{-1} \in H$

- $Hr = Hs$ by supposition
- $Hrs^{-1} = H$, so $h_1 rs^{-1} = h_2$ for some h_1, h_2.
- $rs^{-1} = h_1^{-1} h_2 \in H$

Therefore, if Hr and Hs have some element in common, meaning $h_1 r = h_2 s$, then $rs^{-1} = h_1^{-1} h_2 \in H$. So, by the first direction above, $Hr = Hs$.

Lagrange construction of cosets:

- Take $r_1 \in G$, so $Hr_1 = H$.
- If $H \neq G$, take $r_2 \in G - Hr_1$ to create Hr_2.
- Repeat. We wiil thus create disjoint $Hr_1, Hr_2, ...$ of the same size.

6.4 My take on Lagrange

- If $t \in Hr$ via $t = h_1 r$ and $t \in Hs$ via $t = h_2 s$, then $r = h_1^{-1} h_2 s \in Hs$ and likewise for s, so $Hr = Hs$. So every element is in both or neither.
- Therefore $H(x) = Hx$ is a partition relation on the elements of G.
- Size of Hr equals size of H for obvious group reasons.
- Every element g of G is in some coset Hg.
- Therefore G is partitioned into cosets of equal size, which is size of H.
- Therefore size of subgroup H divides size of group G

6.5 Page 7-12

- Note that if H and K are subgroups, so is $H \cap K$.
- $\mathbb{Z}_6$ has subgroups $\mathbb{Z}_6, \{0, 2, 4\}, \{0, 3\}, \{0\}$, all divisors of 6 in this case.
- $\mathbb{Z}_p$, p prime, has only subgroups $\mathbb{Z}_p, 0$
- $\mathbb{Z}_p \times \mathbb{Z}_p$ has p + 3 subgroups
  - $\mathbb{Z}_p \times \mathbb{Z}_p$
  - Generator (0,0)
  - Generator (0,1)
  - All generators $(1, n), n \in [0, p - 1]$. p of those.
- Another way to think about $\mathbb{Z}_p \times \mathbb{Z}_p$: Outside of (0,0), the remaining $p^2 - 1$ elements each have order p. Except the identity, they each generate a group of size p, though groups of $p - 1$ of them are duplicates (the same group). generate a group of size p, minus the identity. So $(p^2 - 1)/(p - 1) + 2$ *(trivial subgroups)*$= p + 3$.
- Subgroup count of $\mathbb{Z}_4 \times \mathbb{Z}_2$: a counting exercise, based on generators.
  - Look at all cyclic groups of each of the elements.
  - (0,0) generates 1 group
  - Order 2: Three elements, which generate three distinct cyclic subgroups
  - Order 4: Four elements, which generate two distinct subgroups
  - Order 8: $\mathbb{Z}_4 \times \mathbb{Z}_2$, non-cyclic
  - And there's one distict $\mathbb{Z}_2 \times \mathbb{Z}_2$ group.

- *Note: Is there a good (even recursive) formula for this?*

7 Chapter 2.4: Abelian Groups

7.1 Page 1-3

- Theorem: $\mathbb{Z}_a \times \mathbb{Z}_b$ is isomorphic to $\mathbb{Z}_{ab}$ iff a and b are relatively prime.
- DF Proof: If a and b are relatively prime, (1,1) is of order ab. If a and b share factor c, then $\mathbb{Z}_{ab}$ has an element x of order ab, but $\mathbb{Z}_a \times \mathbb{Z}_b$ will have cycled by the time $x^{ab/c}$ rolls around.
- So decompose e.g. $\mathbb{Z}_{12}$ into $\mathbb{Z}_4 \times \mathbb{Z}_3$, for example.

7.2 Page 4-6

- Theorem: Every finite abelian group is isomorphic to a direct product of cyclic groups. *Note: This works because for Abelian groups, subgroups are all normal, so keep decomposing into normal complements $G \cong H \times K$*
- Therefore, the number of these groups of order n is the product of the partitions of each of its prime factors' powers.
- Therefore, the number of abelian groups of size $(24 = 3 * 2^3)$ is $p(1) * p(3) = 1 * 3 = 3 : \mathbb{Z}_3 \times \mathbb{Z}_8, \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- Therefore, the number of abelian groups of size $2310 = 2 * 3 * 5 * 7 * 11$ is one.

7.3 Page 7-11: $\mathbb{Z}_n^*$ or $U(n)$

- Group $\mathbb{Z}_n^*$: elements of $\mathbb{Z}_n$ relatively prime to n, under multiplication.
- $|\mathbb{Z}_n^*| = \phi(n)$, the totient function.
- This is a group even if n not prime because there is $ax + bn = 1$ if x, n are relatively prime.
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ since every element squared is 1.
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ is isomorphic to $\mathbb{Z}_4$ since it is generated by 3.
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ by counting element orders.
- Note: Primitive roots of n are those that generate $\mathbb{Z}_n^*$. There are primitive roots mod n if and only if $n = 1, 2, 4, p^k, 2p^k$. **TODO: Read the primitive roots proof.**

8 Chapter 2.5: Homomorphisms

8.1 Page 1 - 6

- Homomorphism $\phi : \phi(a) *' \phi(b) = \phi(a * b)$. Note that $*$ and $*'$ are different operations.
- This means, "translate each via the function, then combine" yields the same result as "combine first, then translate". So structure is preserved.
- Note that if the domain and range are the same, this is like isomorphism, except homomorphism can squash some items to zero.
- Also, this range can be entirely different than the domain, e.g. $det(AB) = det(A)det(B)$
- Easy to prove homomorphism preserves identities and inverses.
- Order of transformed element $\phi(g)$ divides order of g, since $g^k = e$ and $\phi(g)^k = \phi(e)$, but they're not identical: consider that $\phi(g)$ could hit e at some divisor of k - we could map everything to the identity and make that 1!

8.2 Page 7- 10: Counting homomorphisms

TODO Start here

- Main idea: Knowing where we send identity determines entire homomorphism for a cyclic group.
- Homomorphism count for $\mathbb{Z}_4 \to \mathbb{Z}_{10}$: There are 10 places to send identity, but recall that $\phi(1)$ has to have order 4 since $\phi(1 + 1 + 1 + 1) = \phi(0) = 0$. Therefore, $\phi(1)$ has to be 0 or 5. So 2 possibilities.
- Homomorphism count for $\mathbb{Z}_{99} \to \mathbb{Z}_{100}$: Since $\phi(99) = 0$ and $\phi(1) \times 100 = 0$, and order of $\phi(1)$ must divide both, only one possibility: $\phi(1) = 1$,.
- Homomorphism count for $\mathbb{Z}_{99} \to \mathbb{Z}_{99}$: 99, since $99 \cdot \phi(1) = 0$, so $\phi(1)$ can go anywhere.
- Homomorphism count for $D_3 \to \mathbb{Z}_3$: 1, since D_3 has 3 elements of order 2, 2 of order 3, 1 of order 1. Only mapping everything to 0 works.

8.3 Page 11: Counting automorphisms

- Automorphism is isomorphism from group to itself.
- Count of automorphisms of $\mathbb{Z}_8$: If 1 maps to an order-8 element, we're isomorphic. There are four: $1, 3, 5, 7$
- $Aut(\mathbb{Z}_8)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, since $\phi_3(1)^2 = \phi_5(1)^2 = \phi_7(1)^2 = 1$, where ϕ_a maps a to 1. Three elements of order 2 means it's the Klein 4 group.

- Count of *automorphisms* (meaning, we need all the elements in the codomain) of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: Think of $\phi((1,0,0)), \phi((0,1,0)), \phi((0,0,1))$ as the basis for the group. There are seven choices for the first, six for the next, and *four* for the third.
- The above group is $(\phi(e_1)|\phi(e_2)|\phi(e_3)) = GL(\mathbb{F}_2)$, invertible matrices of 3x3.

9 Chapter 2.6: Quotient Groups

9.1 Aside: Complex multiplication

- Complex modulus (size) of $a + bi$ is defined as $root(a^2 + b^2)$
- Complex multiplication: Angles add, moduli multiply
- One proof of moduli: $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ and $\sqrt{a^2+b^2}\sqrt{c^2+d^2} = \sqrt{a^2c^2 + b^2d^2 - 2abcd + ad^2 + bc^2 + 2adbc}$
- One proof of angles: Convert to $r_1(cos(a) + sin(a))r_2(cos(b) + sin(b))$ and multiply
- More visual proof: Think of $c_1(a + bi) = c_1a + i(c_1b)$. a scales original vector, and bi rotates by 90 degrees and scales.

9.2 Page 1-6

- S^1, is defined as the group of complex numbers with modulus 1.
- The coset zS^1 is any complex number multiplied by S^1 , which is a circle about the origin. $z = 2$ and $z = 2i$ would be in the same coset. These cosets are members of $\mathbb{C}^*$ with the same modulus (length).
- These are disjoint cosets that fill out $\mathbb{C}^*$ (don't include the zero, since no inverse).
- If you consider $H = x + iy$, $x > 0, y = 0$ (positive reals) then the cosets are rays from the origin. Any zH is just the different sizes of that (say, unit) vector. These cosets are members of $\mathbb{C}^*$ with the same angle.
- **quotient group** of $\mathbb{C}^*$ by $S^1 : \mathbb{C}/S^1$
  - Members are cosets
  - Multiplying is defined as $aH \times bH = abH, H \in S^1, a, b \in \mathbb{C}^*$
  - S^1 is therefore the identity.
  - This group is isomorphic to R^+ under multiplication (or really, like H).
  - "A ray of angle A and a ray of angle B multiply to a ray of angle AB, forget about the size".

  - This is like collapsing out the divisor, in this case, S^1.
  - size $|G/H| = |G|/|H|$ since cosets are equally sized.
  - **Gotcha**: Only works (meaning, $g_1, g_1' \in C_1, g_2, g_2' \in C_2$ implies g_1g_2 in same coset as $g_1'g_2'$) if H is **normal** in G.
  - Note: Normal means $xH = Hx$, so that makes sense that $g_1Cg_2C = g_1g_2C*C = g_1g_2C$
- So $\mathbb{C}^*/H$ is all the rays with the same modulus, or S^1.
- "A ray of size X and a ray of size Y multuply to a ray of size XY, and forget about the angles".
- So $\mathbb{C}^*/S^1 = H$ and $\mathbb{C}^*/H = S^1$!

9.3 Page 7-12

- Another example: $\mathbb{Z}/10\mathbb{Z} = \mathbb{Z}_{10}$ under addition. Forget about the non-unit digits!
- Another example: $\mathbb{Q}/\mathbb{Z}$ is $\overline{q} = q + \mathbb{Z}$, so $\overline{1/2} + \overline{2/3} = \overline{1/6}$
- Another example: if N is the **center** (omni-commuter subgroup) of D_4, then N is two elements I, R_{180}. Forgetting about those we have cosets $(I, R_{180})N, (R_{90}, R_{270})N, (D_1, D_2)N, (V, H)N$. All non-identity are degree 2, so isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$
- Another example: $\mathbb{Z}_{13}^*$ with multiplication mod 13. $N = 1, 12$ is a normal subgroup. $\mathbb{Z}_{13}^*/N$ is "forget about the +/- 1 of it and think of these as 1 through 6.
- Another example: **commutator subgroup** [a,b] is generated by all $aba^{-1}b^{-1}$ for all $a, b \in G$. (Note: group members are products of these guys, not necessarily all of that form.) This is just e for an Abelian group. Its size measures "how far" the group is from being Abelian.
- **Main idea** of quotients: "what do we force to the identity?" If we say every $\overline{aba^{-1}b^{-1}} = \overline{1}$, then you can multiply by ba to get $\overline{ab} = \overline{ba}$. So $G/[G, G]$ is necessarily Abelian.

10 Chapter 3.1: Number Theory

10.1 Page 1- 7

- A Fermat's little theorem proof
  - Take prime p, and a not divisible by p.

- $\{a, 2a, 3a..., (p-1)a\} = \{1, 2, 3, ...(p-1)\}$ mod p after rearrangement since they're the same elements mod p.
- Take the product of each: $a^{p-1}(p-1)! \equiv (p-1)!$ mod p
- Divide $(p-1)!$ out (there's an inverse mod p) and you get $a^{p-1} \equiv 1$ mod p

- Another: Since the order of a in $\mathbb{Z}_p^*$ is $p-1$, $a^{p-1} \equiv 1$ mod p.
- Note: Generalization of Fermat's little theorem using same group argument: $a^{\phi(n)} \equiv 1$ if a and n relatively prime, since $\phi(n)$ is the order of the group $\mathbb{Z}_n$, and every element to the power of the group order is 1.

10.2 Page 8-11

- Wilson's theorem: $1 * 2 * ... * (p-1) \equiv -1$ mod p.
- One proof: These all have inverses, except 1 and -1 mod p, which are self-inverting ($x^2 = 1$ solutions).
- This also proves that the product of all elements of a finite Abelian group *which has a single element g of order 2* is that element, g.
- The powers of a **primitive root of p** yield all elements a mod p. So $\mathbb{Z}_p^*$ is cyclical for any prime p.
- One more proof: if k relatively prime to p-1, where p a prime > 2, then $1^k + 2^k + ... + (p-1)^k \equiv 0$ mod p, since each of these summands is a different member of the group: ($a^k = b^k, k < p \rightarrow a = k$ mod p, after looking at the binomial elements) summing to $\frac{p(p-1)}{2}$

11 Chapter 3.2: Games

11.1 15 puzzle

You can't keep 1-13 fixed, blank (16) in the lower right corner, and swap 14 and 15.

Their proof: Think of this as a series of swaps with $(j, 16)$, 16 being the blank tile. To return to the bottom right corner, 16 must make an even number of moves. So only even permutations allowed. So (14,15) is not a viable swap, nor any of the odd permutations.

12 Chapter 3.3: Peg solitaire

- Consider Klein four group: $xy = yx = z, yz = zy = x, xz = zx = y$.

- Label all pegs such that three consecutive in any direction on the board are always, in some order: x, y, z
- Invariant: product of all occupied spaces. If x jumps over y to get to z, eliminating jumped peg, xy = z.
- 11 x's, 11 z's, 10 y's yield xz = y as the total board product, an invariant.

13 Chapter 3.4: Rubix's Cube

- Each element is the state $(S_{12}, S_8, (\mathbb{Z}_2)^{12}, (\mathbb{Z}_3)^8)$, representing around a fixed set of centers: (middle selections, corner selections, middle orientation, corner orientation). Each permutation is basically what you swap from starting state.
- Invariant: First and second terms of the 4-tuple for all F,B,D,U,L,R are odd, so first two args need same permutation parity
- Invariant: (Not proven here): Sum of edge orientations (0,1) is zero, sum of corner orientations (0, 1, 2) is zero.
- **Commutator**: $ghg^{-1}h^{-1}$ measure how entangled g and h are. If they're commutatitive, it is e.
- For Rubix's cube, commutators $ghg^{-1}h^{-1}$ are great for only moving pieces where effects of g and h overlap.
- g and h are **conjugates** if some x such that $h = x^{-1}gx$. "h is same as g, just in a different location".
- Conjugate interpretation: "h is move via x, operate with g, move back via x. "
- For Rubix's cube - you can use conjugates to make whatever change to a different part of the cube (move it to the operating table, operate, move it back).

14 Chapter 4.1: Normal Subgroups

14.1 Normal definition

- **Normal subgroup intuition**: Every conjugacy $g^{-1}Hg$ moves a group to another subgroup. Normal subgroups $g^{-1}Ng = N$ are the ones *that don't move* when you conjugate them.
- Example of non-normal: Any one of the n sets of S_{n-1} among conjugates of S_n. Move it, mess with it, move it back - it's broken free by then.
- Normal definition: Group N is normal if and only if (all equivalent):

- $gN = Ng$ for all $g \in G$
- $gNg^{-1} = N$ for all $g \in G$ (equiv to above)
- $gng^{-1} \in N$ for all $g \in G$

- *Theorem: Any subgroup of index 2 is normal.* Proof: G has two distinct cosets N, gN, but also N and Ng so $gN = Ng$.
- Normal doesn't recursively nest.
- H can be normal in G (e.g. (I, R_{180}, F_v, F_h) in D_4, K can be normal in H (e.g. I, V, but K is not normal in $G : VR_{90} = D_{ul}, R_{90}V = D_{ur}$
- Normal examples in $GL_2(\mathbb{C})$: $SL_2(\mathbb{C})$ (determinant 1) and non-zero diags zI_2.
- Non-normal examples in $GL_2(\mathbb{C})$: $GL_2(\mathbb{R})$. Non-zero diags with different entries. Easy to throw some arbitrary ones in Wolfram Alpha and see everything messed up after conjugation.
- G's **Center**: $Z(G)$ are the omni-commuters. Always normal.
- G's **Commutator group** $[G, G]$: Product of any $aba^{-1}b^{-1}$ for $a, b \in G$. is normal, since $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$, and this can be extended inductively over the constituents.

14.2 Normal properties and examples

- S_3 has three normal subgroups: two trivial ones, and $([], [123], [321])$ since it's of index 2.
- Q_8 has four non-trivial subgroups, all normal: those generated by i, j, or k are all of order 4, index 2. -1 also generates an order 2 group, but it's the center.
- Definition: Product $HK = hk : h \in H, k \in K$.
- Property: If $H \cap K = \{1\}$, and H, K are finite, $|HK| = |H| \cdot |K|$. Why? $h_1k_1 = h_2k_2 \implies h_2^{-1}h_1 = k_1^{-1}k_2$, proving they're both e since left is in H, right in K.
- Property : If H, K subgruops of G, then HK is a subgroup too if H or K is normal, otherwise not always. Why?
  - Assume H is normal.
  - Identity: $e_he_k = e$ is in there.
  - Inverse: If $hk \in HK$, then $k^{-1}h^{-1} = k^{-1}h^{-1}k^1 * k^{-1}$ is in H, K due to H's normality.

- Closure: $h_1k_1 * h_2k_2 = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1h_3 * k_1k_2$ for some h_3

- Property: If H, K are normal subgroups of G, HK is normal. Why? More tricks. $ghkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1}) = h'k'$ for some other $h' \in H, k' \in K$. If they're not both normal, no guarantee about HK (e.g. take $H = \{1\}, G$ a non-normal subgroup).
- **Centralizer** of G's subgroup H is a subgroup of G which commutes with all H: $C_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$. This is G if and only if G is Abelian (almost definitional). May not contain H.
- **Normalizer** of G's subgroup H is a subgroup of G which makes H normal: $N_G(H) = \{g \in G : gH = Hg\}$. This is G if and only if H is normal in G (almost definitional). Largest subgroup of G where H is normal. Definitely contains H.
- Centralizer is a normal subgroup of normalizer with two different proofs:
  - With $n \in N_G(H), c \in C_G(s)$, show that ncn^{-1} commutes with members of H, so it's in C_G, therefore normal. hn is some nh', and same for n^{-1}, so $ncn^{-1}h = nch'n^{-1} = nh'cn^{-1} = hncn^{-1}$ so ncn^{-1} passed through h, is therefore in the centralizer ($ncn' \in C_G(s)$), and so $C_G(H)$ is normal.
  - Using First isomorphism theorem (later):
    * $N_G(H)$ is the big "dividend" group, $C_G(H)$ is the "divisor", and Aut(H) the "quotient" (codomain of the homomorphism)
    * The homomorphism $\phi : N_G(H) \to Aut(H)$ is $g \to \phi_g(x) = gxg^{-1}$.
    * The kernel of this homomorphism is that which maps to $I \in Aut(H)$.
    * The kernel is the centralizer, since $\phi_c(x) = cxc^{-1} = cc^{-1}x = x$, identity.
    * Therefore, $N_G(H)/Ker(\phi) = N_G(H)/C_G(H) \to Aut(H)$. so $C_G(H)$ must be normal!
    * (Kernels of homomorphisms always normal (DSF Proof): If $\phi : G \to H$ is a homormophism, and $g \in G, k \in Ker(\phi)$, then $gkg^{-1} \in K$ since $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e$. So K is normal in G.

15 Chapter 4.2: Isomorphism theorems

- Example of intuitive isomorphism: $M_2(\mathbb{Z})/N \cong (\mathbb{Z}_2)^4$, where N is the subgroup with even entries. How? Can *either list all cosets* or construct a homomorphism $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a \bmod 2, b \bmod 2, c \bmod 2, d \bmod 2))$.

15.1 First Isomorphism Theorem and example

- $G = GL_2(\mathbb{R})$, invertible 2x2 real matrices
- $N = SL_2(\mathbb{R})$ is subgroup of G with determinant 1.
- φ is det, since $det(AB) = det(A)det(B)$.
- $G/N \cong \mathbb{R}^*$ intuitively, since for any matrix, you can divide by the determinant scalar, and find the representative in the group N. Can think of N as the kernel of the homomorphism - it doesn't matter, it's mapped to identitty.
- **First isomorphism theorem**: given surjective homomorphism $\varphi : G \mapsto H$ with kernel $Ker(\varphi) = \{g \in G | \varphi(g) = e_H\}$, then $G/Ker(\varphi) \cong H$.
- Note: This directly implies $G = H \times K \leftrightarrow G/K = H$, with the isomorphism $\phi : (h, k) \to H$. The kernel $Ker(\phi) = (0, k) \cong K$, so $G/Ker(\phi) = G/K = H$
- Another example in the above, if $a = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then $(aN)(bN)$ is some cN, where $det(c) = 4$, like $2I$

15.2 Third Isomorphism theorem

- Theorem: If G / N is abelian, then every subgroup H of G containing N is normal in G.
  - $H/N \subset G/N$, and so H/N is abelian too.
  - Abelian means $ghN = hgN$
  - This also shows there is some n such that $gh = hgn$.
  - But since N is normal in G, $gn = n'g \to hgn = (hn')g$, and $hn' \in H$, therefore $gh = (hn')g$, and H is normal in G.
- Actual theorem says subgroups of G containing N correspond to subgroups of G/N.
- Also, $\frac{G/N}{H/N} \cong \frac{G}{H}$

15.3 Second Isomorphism theorem

- Actual theorem says: if H is a subgroup of G, and N is a normal subgroup of G, then $\frac{H}{H \cap N} \cong \frac{HN}{N}$
- In particular, if $H \cap N = \{1\}$, then $\frac{HN}{N} \cong H$.
- Proof:

- HN contains both H and N (since identity in both), and N is normal in H ($hnh^{-1} \in N$) since it is normal in G ($h \in G$).
- Therefore $(HN)/N$ is a group.
- $\varphi(h) = hN$ is a surjective homomorphism to $(HN)/N$
- The kernel is anything in N, which would be $H \cap N$.
- Result follows from first isomorphism theorem.

15.4 Examples using the first isomorphism theorem

- Typically, in order to identify $G/N \cong K$, find the surjective homomorphism $G \to K$ where $Ker(\varphi) = N$.
- Example: $G = \mathbb{Z} \times \mathbb{Z}$ with addition, N = group generated by $(1, 0)$. $G/N \cong \mathbb{Z}$ intuitively, since you're forgetting the first coordinate. To make it formal : $\varphi((x, y) = y)$.
- Harder example: $G = \mathbb{Z} \times \mathbb{Z}$ with addition, H = group generated by $(2, 3)$, or $(2a, 3a)$. $G/H \cong Z$, actually, since $\phi((x, y) = 3x - 2y)$ is surjective (think of $\phi((a, a)) = a$ and its kernel is H.
- Harder example: $G = \mathbb{Z} \times \mathbb{Z}$ with addition, H = group generated by $(2, 4)$, or $(2a, 4a)$. $G/H \cong Z \times \mathbb{Z}_2$, actually, since $\phi((x, y) = 2x - y, x(mod2))$ is surjective and its kernel is H.
- TODO: Get a better intuition here. Is this group like, how far away from this null space line am I?

16 4.3a: Interlude: Group actions

16.1 Group Actions

Reference: https://brilliant.org/wiki/group-actions

Think of group actions like S_n acting on the *set* (not necessarily group) of $\{1, 2, ...n\}$.

- **group action** on group G, set X, is function $f : G \times X \to X$. It's often written $f(g, x) = g \cdot x$. which has some groupy properties.
  - $f(e_G, x) = x$ for all $x \in X$, or $e_G \cdot x = x$
  - $f(g, f(h, x)) = f(gh, x)$ for all $x \in X$,or $g \cdot (h \cdot x) = (gh) \cdot x$.
  - Canonical Example: if G is S_n, and $X = \{1, 2, ...n\}$.

- **fixed point of a group element** $g \in G$ is $x \in X$ such that $g \cdot x = x$. So, $f = g(x)$ is the (very straightforward) mapping, g is the function, and x would be a point that doesn't change.
- For point x, **stabilizer of the point** is called G_x, and is the set of $g \in G$ that map x as a fixed point: $g(x) = x$ of element $g \in G$ is $x \in X$ such that $g \cdot x = x$. So, it's the *subgroup* of elements that each act stably on x.
- **fixed point** of element $g \in G$ is $x \in X$ such that $g \cdot x = x$. So, $f = g(x)$ is the (very straightforwardx) mapping, g is the function, and x would be a point that doesn't chagne.
- **orbit of element** $x \in X$ is how far x reaches, the set of $y \in X$ such that there's a $g \cdot x = y$.
- Example: So if $G = \mathbb{Z}_2 = e, g, X = \mathbb{Z}$, and the action is $e \cdot x = x, g \cdot x = -x$, then
  - Fixed points of e are all of them, of g is 0.
  - Stabilizers of x are e for all, e, g for 0.
  - Orbit of 0 is $\{0\}$, orbit of every other n is $\{n, -n\}$
  - *orbits* are an equivalency relation! So they partition X.
- Action is **transitive** if there is only one orbit in the relation (sounds like a regular group): for any $x, y \in X$, there is a g such that $g \cdot x = y$.
- Action is **faithful** If only e_G if the only omni-stabilizer element is e_G. Intersection of all G_x is e_G.
- Another way to think about faithful: Think of G as a homomorophism to $Sym(X)$, permutations of the group. Faithful actions are injective / have a trivial kernel.
- Examples of actions
  - Every group acts on itself by left multiplication. It is transitive and faithful (since the Cayley table is a latin square). One orbit.
  - Every group acts on itself by conjugation $g \cdot x = gxg^{-1}$. Orbits are the conjugacy classes. The **centralizer** $C_G(x)$ is the stabilizer of x.
  - If H is a subgroup of G, then cosets G/H and left multiplication are a group action. They are a transitive action since there is one orbit: you can always get from gH to kH by $(kg^{-1})H$.
  - **Core Group**: The group $\bigcap_{g \in G} gHg^{-1}$ of G's subgroup H is the largest normal subgroup of H. Proof:

        * It's contained in H since $hHh^{-1} \in H$, and it's an intersection.
        * It's normal because $kCore_G(H)k^{-1} = k(\bigcap_{g \in G} gHg^{-1})k^{-1} = \bigcap_{g \in G} kgHg^{-1}k^{-1} = Core_G(H)$ since every kg is just a g but permuted.
        * It's the largest normal one since if there were another normal subgroup $N' \in H$, then $gn'g^{-1} \in N'$ and $gn'g^{-1} = h$ for some $h \in H$, so $n' = g^{-1}hg$, and therefore n' is somewhere in the core group.
        * Therefore, the core group is the kernel of the map $G \to Sym(G/H)$, since those map to H. So if H doesn't contain any nontrivial normal subgroups, it's faithful, and is called **simple**
    - Another group action: $PGL_2(\mathbb{C})$ = projective linear group of 2x2 matrices on the complex plane (plus infinity), sending $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$.

- **Orbit stabilizer theorem**: If G is finite, and $x \in G$ has a stabilizer G_x and orbit orb(x), then $|G| = |G_x||orb(x)|$. Proof:
    - Since stabilizer is a subgroup, the count of distinct cosets (index) times the subgroup is the size by Lagrange.
    - Consider homomorphism $G/G_x \to orb(x) : \phi(gG_x) = g \cdot x$
    - And the set aG_x and bG_x are equal under ϕ iff $a(x) = b(x)$, since $b^{-1}aG_x = G_x$, implying $b^{-1}a \in G_x \to b^{-1}a(x) = x \to a(x) = b(x)$. So the stabilizer takes care of the injective part.
    - Also, this map is onto since every element $y \in orb(x)$, meaning some $g \cdot x = y$ is in that gG_x . So the orbits take care of the surjective part.
    - Example: *symmetric group*: $S_n : G_x \cong S_{n-1}! \to |G_x| = (n-1)!$. $orb(x) = n$. So $|G| = n!$.
    - Example: *cube symmetries*: Vertex is x, rotation of adjacent vertices is G_x. $|G_x||O_x| = 3 * 8 = 24$. Can also do with edges and faces. Turns out cube symmetries $\cong S_4$

17 Aside: Conjugacy classes

17.1 Conjugacy classes defined

- Note: It's easy to take a group to another group by conjugation group action $\phi(g, H) : ghg^{-1}$. Though the whole group gets mapped to another group, the elements inside get mapped to **conjugacy classes**.

- To get the conjugacy class that h is in by hand, compute $ghg^{-1}, g \in G$. You'll find all its co-members. Repeat.
- Within group G, elements h, h' in conjugacy class H have some $g \in G$ such that $h' = ghg^{-1}$ (and therefore, $g^{-1}h'g = h$). So, it's an equivalence relation, thus a partition.
- Note: if the group G is abelian, $h' = ghg^{-1} \to gg^{-1}h = h$, so all conjugacy classes there are of size one ($ghg^{-1} = gg^{-1}h = h$)
- Each one of these classes corresponds to the orbit of that element h under conjugation.
- Why useful? They can be used to show structure (and thus classify, look at isomorphisms, etc.) of groups.
- Example: In $GL_n(\mathbb{R}), A = PBP^{-1}$ is matrix similarity. B represents A under a change of bases.
- Example: In S_3, there are three conjugacy classes: $\{()\}, \{(abc), (bac)\}, \{(ab), (bc), (ac)\}$. Easy to think about with permutations - this is just relabeling the members going in, doing the permutation, then reversing the labels.
- Example: $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$ which is Abelian, so 5 classes (one for each element).

17.2 A_5 example and the class equation

- Examples: In A_5, types are repped by $(), (12)(34), (12)(23) = (123)$, and $(12)(23)(34)(45) = (12345)$.
- **Gotcha**: Note that There are $5!/5 = 24$ 5-cycles, and that subgroup order has to divide 60, so there must be two conjugacy classes of 5-cycles. Makes sense that (12345) and (21345) can't be same class, since there's nowhere to "stash" during the relabeling.
- Theorem: Sum of conjugacy class orbits is size of group, or, for arbitrary class reps $g_1 ... g_k, |G| = \sum_{i=1}^{k} [G : C_G(g_i)]$. Note that $|Z(G)|$ is all of the reps and classes of size one. Why does this work? Orbit-stabilizer says that $C_G(g_i)$ is the stabilizer, and the conjugacy classes form a partition.
- **Class Equation**: Just writing down the size of the equivalence classes. In A_5, this would be $60 = 1 + 15 + 20 + 12 + 12$ (second set of 5-cycles).
- Note that any *normal* subgroup in A_5 has to be union of those since conjugation by A_5 elements maps to the whole conjugacy class. BUT - there are no sums that divide 60. So A_5 has no normal subgroups, so it is simple!

18 4.3 Conjugacy class section

- Reminder of orbit-stabilizer theorem: **Number of conjugates of g is the index** (more generally, orbit, here under conjugation group action) of the **centralizer** (more generally, stabilizer, here under conjugation group action) of g. This reminds me: for elements h commutes with, conjugation preserves h: $ghg^{-1} = h \leftrightarrow gh = hg$.
- Example: If $|G| = 60, g \neq 1, g^5 = 1$ then size of conjugacy class is at most 12 since at least e, g, g^2, g^3, g^4 are in its centralizer $C_g(G)$.
- Example: Class equation of Q_8:
  - $\{1\}$ commute with everything = 8 / 8 = orbit of 1 under $g * 1 * g^{-1}$
  - $\{-1\}$ commutes with everything = 8 / 8 = orbit of 1 under $g * -1 * g^{-1}$
  - i commutes with $1, -1, i, -i$ = 8 / 4 = orbit of 2 under $g * i * g^{-1}$, which is $\{i, -i\}$. Similar for j, k.
  - Thus, 8 = 1 + 1 + 2 + 2 + 2.
- Example: Class equation of D_5, with σ as a clockwise rotation, τ as a flip:
  - $\{e\}$ commutes with everything = 10 / 10 = 1
  - $\{\sigma\}$ commutes with only rotations = 10 / 5 = 2, and conjugates to $\tau\sigma\tau = \sigma^4$.
  - $\{\sigma^2\}$ commutes only with rotations = 10 / 5 = 2, and conjugates to $\tau\sigma^2\tau = \sigma^3$.
  - $\{\tau\}$ commutes only with τ, em and conjugates to all five flipped actions $\sigma^k\tau$.
  - Thus, 10 = 1 + 2 + 2 + 5
- Weird **gotcha**: Note that the abelian $\mathbb{Z}_5$ has 5 conjugacy classes, and D_5 has four, and there's an injective homomorphism $z \to \sigma^z$. So even though $\mathbb{Z}_5$ is a subgroup of D_5, it has more conjugacy classes.
- D_n has n reflections. If n is odd, there is only one conjugacy class of reflections, since $(\sigma^i\tau)\tau = \sigma^i$ and $(\tau\sigma^i)\tau = \tau\tau\sigma^{-i}$, so if the paranthesized items are equal (i.e. if σ^i commutes with τ), then $\sigma^i = \sigma^{-i}$. $i = 0$ works, but only in even groups does $i = \frac{n}{2}$ work. Therefore centralizer has size 2 for n odd, 4 for n even, and for these n/2 elements, there is one conjugacy class if n odd, 2 if even.
- *Theorem*: If there's a homomorphism $\pi : G \to K$, then count of conjugacy classes $c(G) \geq c(K)$. Homomorphism maps conjugacy classes to conjugacy classes $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}$, so if there's a nonzero kernel with k in it, $\pi(1) = \pi(k)$, but 1 and k could be different conjugacy classes in the domain.

19 4.4 Permutations / Symmetric group

- Note: Every group of size n is a subgroup of S_n, since element g induces a permutation on the elements by multiplication. I suppose then the group is the permutations of each g! Repping under S_n is called the **regular representation**.
- Conjugation is interesting in S_n; If $\sigma = (123), \alpha = (13524)$, then $\sigma(13524)\sigma^{-1} = (\sigma(1)(\sigma(3)\sigma(5)\sigma(2)\sigma(4))$. Why? (Proof)
  - Say $\alpha = (a_1 a_2 ... a_n)$
  - $\sigma^{-1}\sigma a_1 = a_1$
  - $\alpha(a_i) = (a_{i+1 mod n})$
  - So for any $a_i, \sigma\alpha\sigma^{-1}(\sigma(a_i)) = \sigma(a_{i+1 mod k})$
  - So the $\sigma\alpha\sigma^{-1}$ operation on $\sigma(a_i)$ is just like taking $\sigma(a_i)$ and mapping it to the next $\sigma(a_{i+1 mod k})$.
- S_6 has 11 conjugacy classes corresponding to partitions: $(), (12), (123), (12)(34), (1234), (12345), (123)(45)$ Think of missing elements x, y, like $(x)(y)$....
- How many permutations fix 1 in S_n ? Clearly this is just $|S_{n-1}| = (n-1)!$
- Summing total fixed counts $\sum_{\sigma \in S_n} F(\sigma)$ of every permutation is then $n*(n-1)! = n!$
- Random note: $A_4 \ncong D_6$ since A_4 since there's an element of order 6 in D_6, none in A_4.
- Tetrahedon rotations group: Isomorphic to A_4. all rotations of form $(1)(234) = (23)(34)$, $(2)(13)(34)$, etc. Four places to map a vertex, and three spin locations = order 12 (or orbit-stablizer: three rotations in vertex centralizer, four places to go with vertex in orbit).

20 Aside: Legendre symbol

https://brilliant.org/wiki/legendre-symbol/

- a is a **quadratic residue** mod m if $x^2 \equiv a$ mod m has at least one x solution. So, I suppose that 1 is always a quadratic residue. a and m need to be coprime.
- If p is an odd prime, a is an integer, Legendre symbol $\left(\frac{a}{p}\right)$ is:
  - 0 if $a \equiv 0$ mod p
  - 1 if a is a quadratic residue mod p and $a \neq 0$ mod p.

– -1 if a is a non-residue

- Sum of quadratic resides of a prime is 0. Why? There are no 0's, and every residue is repped twice, once by a and once by $p-a$. So half are non-residues, half are double-residues. Why do they pair this way? $a^2 \equiv b^2 \bmod p \Rightarrow a^2 - b^2 \equiv 0 \bmod p \Rightarrow (a-b)(a+b) \equiv 0 \bmod p \Rightarrow p|(a-b)(a+b) \Rightarrow a+b \equiv 0$ or $a-b \equiv 0$. So $a = b$ or $a+b = p$

- Property: **Euler's criterion**: If p is an odd prime, a is not divisible by p, then $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ (mod p). This follows from: (1) If $a = x^2$, then $x^{p-1} \bmod p \equiv 1$ by Fermat's Little Thereom, so take square root. (2) If not, then because $\mathbb{Z}_p$ is a group, every element x has a pal $x^{-1}a$ that multiplies to a. Product of these is $a^{\frac{p-1}{2}} = (p-1)! = -1$ by Wilson's Theorem.

- Property: If $a \equiv b$ (mod p), $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Just reduce mod p.

- Property $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Follows from Euler's criterion ands exponents.

- Property: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, by Euler's criterion, so it is 1 iff $p \equiv 1 \bmod 4$.

- Property: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, by **TODO** something called quadratic reciprocity.

- Property: If p, q distinct odd primes, then $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, by **TODO** something called quadratic reciprocity.

21 4.5 Signs of Permutations

- Note: Look at cycle structure of $\sigma_3(x) = 3x \bmod 11$. $3^5 = 1$, and $2 * 3^5 = 2$. Observe these two disjoint 5-cycles.

- If $a^k = 1 \bmod p$ and is the smallest k to do so, cycle structure of $\sigma_a(x) = ax \bmod p$ is all disjoint k-cycles. *Proof*: (1) σ_a will have no fixed points, as $ax = x$ means $a = 1$ (mod p). (2) $\sigma_{a^k} = \sigma_a^k =$ identity. And (3) if $j < k$, j can't be identity. So σ_a is the product of $\frac{p-1}{k}$ disjoint k-cycles.

- Also implies that σ_a is odd if and only if k is an even number (thus odd cycle) and $\frac{p-1}{k}$ is odd.

- **Theorem**: $\left(\frac{a}{p}\right) = -1$ iff k is even, and $\frac{p-1}{k}$ is odd, or $sgn(\sigma_a) = \left(\frac{a}{p}\right)$. Why? Suppose for some a, the primitive root g taken to x is $a : g^x = a$. The order of g^x is

$\frac{p-1}{gcd(p-1,x)}$. Then flip the denoms: $\frac{p-1}{k} = gcd(p-1,x)$, which is odd iff x is odd, or NOT A SQUARE. Therrefore, $sgn(\sigma_a) = \left(\frac{a}{p}\right)$!

- An **inverison** in a permutation is where a pair $a < b$, $\sigma(a) > \sigma(b)$.
- Number of inversions in σ_2 is straightforward, as for prime p, $\sigma(1,2,3...p-1/2, p+1/2....p-1) \to (2,4,6...p-1,1,....p-2)$ ends up as $1+2+...+\frac{p-1}{2} = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{p^2-1}{8}$
- The sign of a permutation is also $(-1)^r$, where r is number of inversions.
- Putting all this together yields $\left(\frac{2}{p}\right) = sgn(\sigma_2)$ by **theorem** above, $= (-1)^r = (-1)^{\frac{p^2-1}{8}}$, property 5 in the last section.

22 5.1 Group actions

22.1 Orbit-stabilizer

- Canonical: Group S_n acts on elements $X = 1,2,3..n$. $G \times X \to X$
- Also canonical: Any group acts on its own elements with left-multiplication, always. Straightforward action $G \times G \to G$.
- **orbit** O_x of element x is all the places x could go. Note that in a group there is only one orbit (such an action is called **transitive**).
- **Orbit-stabilizer theorem** says, for any $x \in G$, $|G| = |O_x||G_x|$.
- item **stabilizer** G_x of element x are the elements mapping x to itself. Note that in a group this is necessarily $G_x = e$ since $g \cdot x = x \to g \cdot x \cdot x^{-1} = x \cdot x^{-1} \to g = e$.
- Example: $2n = |D_n|$, and since every *vertex* element x can be rotated to any other (orbit is size X), stabilizer must be of size 2 (identity, 180 flip)
- Example: Rotations of a dodecahedron: Think of the faces - there are five rotations that fix the face, and the face can go to 12 different spots,so size of the group is 60. Turns out, also isomorphic to A_5.

22.2 Action of $GL_2(F)$ on F^2

- Action is on left-multiply: $A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$
- How many orbits in $\mathbb{R}^2$ under this action? Answer: *two*

- *One orbit*: The point $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ can only map to itself, and no non-zero determ can map to it ($A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \to \begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, which only works for zero x,y or a zero-deteminant matrix.
- *The other orbit*: There's some invertible A to match any $\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, either $\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}$ if $y \neq 0$ or $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ if $y = 0$.
- Example: $GL_2(\mathbb{Z}_p)$ acts on $\mathbb{Z}_p{}^2$, just on integers modulo prime pp.
- Orbit of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is every non-zero element, so size $p^2 - 1$. Stabilizer is anything $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $d \neq 0$, so $p^2 - p$ elements.

22.3 General group action properties

- Action is **regular** if $x, y \in X$ have exactly one $g \in G$ so $g \cdot x = y$. So, this means
  - There's one orbit, since any x can get to any y.
  - Every element's stabilizer is just the identity (uniqueness).
  - $|G| = |X|$ since $|G| = |O_x||G_X| = |X| * 1$
  - Really, any such regular action is isomorphic to (G, G) by left-multiplication.
- If x, y in the same orbit in G ($g \cdot x = y$ for some $g \in G$) for finite G, then $|G_x| = |G_y|$. Why? First, because of the orbit-stabilizer theorem (same orbit size, same group size). But also the "conjugating" bijection $f(h) = ghg^{-1}$, since $f(y) = ghg^{-1}(y) = gh(x)$ (since $h \in G_x$), $= gx = y$. Can reverse it too.

23 Burnside's Lemma

- The number of orbits under a group action is the average, across all group elements, of the fixed point set sizes $|X^g|$. Another way: set of orbits is called $|X/G|$, so $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$.
- How to use this to count stuff?
  - Group the "same elements" of an object under the action as orbits. So, think of configs of a cube indistinct under rotation to be in the same orbit.
  - Count the fixed points under each action $g \in G$.

- Divide by $|G|$.

- Colorings of hexagon edges, coincident by each rotation action: $R_0 = n^6, R_1 = R_5 = n, R_2 = R_4 = n^2, R_3 = n^3$, so sum is $\frac{1}{12}(n^6 + 2n + 2n^2 + n^3)$

- Colorings of hexagon edges coincident by reflection OR rotation: across central vertex line $= n^3$, across central edge line $= n^4$, so adding to previous gives total is $\frac{1}{12}(n^6 + 2n + 2n^2 + 4n^3 + 3n^4)$

- Example: Tetrahedron (n vertex colors, m edge colors): Vertex plus center opposite face: n^2m^2

- Example: Tetrahedron (n vertex colors, m edge colors): Midpoints of opposite edges (think (12)(34)) is n^4m^2

- Example: So in total, tetrahedron is identity (n^6m^4) plus the previous two: $\frac{1}{12}(n^6m^4 + 3n^4m^2 + 8n^2m^2)$

24 Aside: Semidirect products: videos

24.1 Semidirect products (inner and outer)

https://www.youtube.com/watch?v=Pat5Qsmrdaw

- **inner semidirect product** $H \rtimes K = G$ decomposes G into two subgroups H and K, with a few rules
  - H and K are **complements** in G: $HK = G, H \cap K = \{e\}$
  - $H \triangleleft G$ (H is normal in G)
  - $K \subset G$ (K is a subgroup of G)

- Note that a general product of groups HK isn't necessarily a group. But if H is normal, we can guarantee inclusion in HK under the group operation $h_1k_1 \cdot h_2k_2$
  - $h_1k_1h_2k_2 = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})(k_1k_2) = (h_1h_3)(k_1k_2) \in HK$ since $k_1h_2k_1^{-1} = h_3$ for some h_3 since $H \triangleleft G$
  - $(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}(kk^{-1}) = (k^{-1}h^{-1}k)k^{-1} \in HK$ similarly.
  - Group $H_G = (h, 1) \in H \rtimes K$ is a subgroup isomorphic to H. Same with K.

- A general semidirect product uses this conjugation $\psi_{k_1}(h) = k_1h_2k_1^{-1}$ to allow us to combine elements of H together and elements of K together almost separately. Instead of multipiying $(h_1, k_1)(h_2, k_2)$ directly, we use:
  - $(h_1, k_1)(h_2, k_2) = (h_1\psi_{k_1}(h_2), k_1k_2)$

- Every inner semidirect product uses $\psi_k(h) = khk^{-1}$.
- In general, the ψ is a member of $K \to Aut(H)$, or an isomorphism that translates H to H. So can keep the multiplication of the h elements clean.
- Note that if $\psi = \psi_{id}$, then you *end up with a direct product*, or $G = H \times X$.
- Note also that if $H, K \triangleleft G$, then $hkh^{-1}k^{-1} \in H, K \to hkh^{-1}k^{-1} = e \to hk = kh$, so the subgroups commute among each other (pass through). Then, the direct product falls out of using $\psi_k = id$, so $h_1k_1h_2k_2 = h_1\psi_{id}(h_2)k_1k_2 = h_1h_2k_1k_2 \in HK$. So in this case, $H \times K \cong G$

- Even if G is abelian, $H \rtimes K$ need not be!
- Note that every group G that satisfies the rules above (H is normal in G, K a subgroup, and HK=G) admits a semidirect product under the conjugation action.
- An **outer semidirect product** doesn't start with $H, K \in G$. H and K could be unrelated and with totally separate shapes, as long as $H \cap K = \{e\}$. Then, combining H and K with action ψ can create a new group within $H \times K$ called $H \rtimes_\psi K = G$. There can be many distinct choices of ψ, leading to many different products.

24.2 Semidirect products: D_{2n}

https://www.youtube.com/watch?v=DvclxOaWbJM

- $D_{2n} =< r > \times < s >$, with r being rotations, s the group of $\{e, s\}$. S is the flip.
- Use the natural inner semidirect product action (conjugation) for ψ.
  - Take $\psi_e(r^k) = er^ke^{-1} = r^k$.
  - Take $\psi_e(r^k) = sr^ks^{-1} = r^{-k}ss^{-1} = r^{-k}$.
  - Then, $D_2n =< r > \rtimes < s >$
  - Example: $(r^4s)(r^3e) = (r^4\psi_s(r^3), s \cdot e) = (r^4r^{-3}, s) = (r, s)$. Just like the elements would multuply to rs.
- But semidirect products can make things simpler if we use *isomorphism* to cleaner groups, like $\mathbb{Z}_n \times_\psi \mathbb{Z}_2$, which are isomorphic to $< r >, < s >$ respectively.
  - Then, in $\mathbb{Z}_n \rtimes_\psi \mathbb{Z}_2$, we use $\psi_0(a) = a, \psi_1(a) = -a$.
  - Then, with the same example abve, $(4, 1)(3, 0) = (4+\psi_1(3), 1+0) = (4-3, 1) = (1, 1)$. Same!

25 5.3 Semidirect products

- Exercise: If $G = N \rtimes H$, and H has a_h elements of order two, similar for N and a_n, then G has at least $a_n + a_h$ elements of order two: $(n \in N_2, 1)$, $(1, h \in H_2)$, and possible combinations like $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$
- Exercise:Therefore Q_8 can't be a semidirect product of $\mathbb{Z}_2$ and $\mathbb{Z}_4$ (or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$) since it only has one element of order two: -1.
- Exercise: Heisenberg matrix group

  $H_p = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ with $a, b, c \in \mathbb{Z}_p$ ends up being $N \rtimes H$, where $N = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, $H = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

  because

  - N is normal (how to prove?) in $GL_3(\mathbb{Z}_3)$
  - H is a subgroup as well
  - $NH = G$ (just multiply)
  - $N \cap H = \{e\}$
- Exercise: Constructing a group using outer semidirect product.
  - Order of $\psi(a) = 2a$ in $\mathbb{Z}_7$ is 3, since $\psi(\psi(\psi(a))) = a$. So $\psi \in Aut(\mathbb{Z}_7)$.
  - So constructing group $G = \mathbb{Z}_7 \rtimes_\psi \mathbb{Z}_3$, with $\psi_1(a) = 2a, \psi_b(a) = \psi_1^b(a)$ makes a (nonabelian) group of size 21.
  - $(a, b)(a', b') = (a + \psi_b(a'), b + b') = (a + 2^b a', b + b')$ is the rule.

26 Aside: Sylow Theorems

26.1 Sylow Theorem I

- Link: https://www.youtube.com/watch?v=xTCxmr4ISU4
- Main idea: If $|G| = p^k m, gcd(p, m) = 1$, there exists a subgroup of size p^k. So, there are one or more subgroups of size p^k if k is maximized.
- Proof:

- Main idea: for any set X of size p^k (call the totality of them Ω), the coset gX is also of that size, since $\phi(x) = gx$ is injective: $gx = gy \to g^{-1}gx = g^{-1}gy \to x = y$.
- $|\Omega| = \binom{p^k m}{p^k}$.
- There's a theorem that $\binom{p^k m}{p^k} \equiv m \bmod p$.
- So taking g as an action of each $X \in \Omega$, this itself splits $g\Omega$ into orbits. Then there has to be an orbit $O = gX$ with size *not a multiple of* p, since $|\Omega| = \binom{p^k m}{p^k} \equiv m \bmod p$.
- Pick a set $X \in$ some orbit O. So $G \cdot X = O$ since that's how orbits work.
- By orbit stabilizer, $|G_X| \cdot |G \cdot X| = p^k m$, but this $|O| = |G \cdot X|$ is not a mutliple of p. So p^k divides $|G_X|$.
- If $g \in G_X, a \in X, ga \in X$. But gX is always in X (of size p^k), so $|G_X| \leq p^k$
- So $|G_X| \leq |X| = p^k$, but also p^k divides $|G_X|$. So $p^k = |G_X|$, and this stabilizer group is such a subgroup of G.

26.2 Sylow Theorem II

- Link: https://www.youtube.com/watch?v=n8senIN0RgM
- Main idea: Any two Sylow p-subgroups H, K of G are conjugate, so $H = gKg^{-1}$ for some g
- Proof outline:
  - Consider the set Ω of all p-Sylow subgroups of G.
  - Consider the set G/K, cosets of K in G. K doesn't have to be normal. Of size $p^k m/p^k = m$.
  - The group action of some p-Sylow group H by left multiplication maps H into a number of orbits, totaling size $|H| = p^k$.
  - By orbit stabilizer theorem, H's orbits $H \cdot gK$ look like $|H| = |H \cdot gK||N_H(gK)|$, so they all divide p^k, so of size $1, p, p^2...p^k$.
  - However, since the sum of these orbit sizes is m, where $\gcd(m, p) = 1$, then there must be an orbit gK of size 1.
  - This means that for any $h \in H$, $hgK \in gK$, or $g^{-1}hgK = K$, or $g^{-1}hg \in K$.

- This means that $gHg^{-1} \in K \to g^{-1}Kg \in H$, and the two subgroups are conjugate
- So, for any two p-groups H, K, we can find a conjugation mapping one to the other.

26.3 Sylow Theorem III

- Link: https://www.youtube.com/watch?v=543-79vKJFw
- Main idea: Call the number of p-subgroups n_p. Remember that if $p^k = 2^3 = 8, p$ is still 2.
  - $n_p | m$
  - $n_p \equiv 1 \bmod p$
  - $n_p = |G|/|N_H(G)|$, where $N_H(G)$ is the size of the normalizer of H. It follows $n_p = 1$, then H is normal in G since then $|N_H(G)| = |G|$.
- Proof: $n_p | m$
  - Set: Sylow p-subgroups Ω
  - Action: G acting on $P \in \Omega$. as $g \cdot P = gPg^{-1}$
  - Then it is true that orbit $G \cdot P = \Omega$, since P and every other p-subgroup are conjugates (Sylow II).
  - By orbit stabilizer, $|G \ = |G \cdot P||G_P| = n_p|G_P|$ by definition of n_p.
  - $G_P = g \in G : gPg^{-1} = P$, which is the definition of the normalizer $N_G(P)$.
  - Note that $P \leq N_G(P) \leq G$.
  - So stabilizer $|G_P|$ under this action is the normalizer. So $|G| = n_p|N_G(P)|$. **Note: this is the third result**.
  - $|G| = p^k m$, $|P| = p^k$, $P \leq N_G(P)$, so $|N_G(P)| = p^k m'$ for some m', since P is a subgroup of $N_G(P)$.
  - Therefore, $n_p = \frac{m}{m'} \to m' n_p = m \to n_p | m$
- Proof: $n_p \equiv 1 \bmod p$
  - Set: Sylow p-subgroups Ω, size is n_p.
  - Action inputs: Take a Sylow p-subgroup $P \in \Omega$. Take element $p \in P$, p-subgroup $Q \in \Omega$.

- Action definition: $p \cdot Q = pQp^{-1}$. This a conjugate of Q so therefore same size, therefore a p-subgropup $\in \Omega$.
- $|P| = p^k$, and P and multiplying by P splits Ω into a bunch of orbits.
- Similarly to the earlier argument in part 1, all of the orbit sizes need to divide p^k by orbit-stabilizer, so of size $1, p, p^2 ... p^k$.
- Ignore everything bigger than one. So we're looking for number of size-one orbits.
- Take $Q \in \Omega$ where $|P \cdot Q| = 1$. Remember $P \cdot Q$ is the set $\{pQp^{-1}, p \in P\}$
- $pQp^{-1} = Q \forall_{p \in P}$ is another way of saying $P \leq N_G(Q) \leq G$.
- $Q \leq N_G(Q) \leq G$ as well.
- $|P| = |Q| = p^k, |G| = p^k m$, which means $N_G(Q)$ is (inclusive) between these two.
- But P, Q are sylow p-subgroups of $N_G(Q)$! So they're conjugate $P = gQg^{-1}, g \in N_G(Q)$
- But Q is normal in $N_G(Q)$, so $P = gQg^{-1} = Q$.
- Thus arbitrarily chosen Q has been proven to be P. So P is the only element with an orbit of 1.

27 5.4 Sylow Practice

- Remember that if H, K are normal subgroups of G, then if they're complements $HK = G, H \cap G = \{1\}$, then $(h, k) \to hk$ is an isomorphism $H \times K \cong G$.
- Therefore, inductively extending it, if evrry Sylow subgroup of G is normal, then G is isomorphic to direct prodcut of Sylow subgroups. This is true in the case of Abelian groups for example.
- Prove: Every group of order 15 is Abelian.
  - 3-subgroup $H : n_3 = 1 \bmod 3, n_3 | 5 \to n_3 = 1$
  - 5-subgroup $K : n_5 = 1 \bmod 5, n_5 | 3 \to n_5 = 1$
  - Both are normal in G (Sylow 3), so $G \cong H \times K$
  - Counterexamples from the problem:
    * $|G| = 16$: D_8 is not Abelian.

    * $|G| = 20$: D_{10} is not Abelian.
    * $|G| = 21$: The semidirect product of $\mathbb{Z}_3 \rtimes_\psi \mathbb{Z}_7$ we saw with $\psi(a) = 2a$ was not abelian.
    * $|G| = 27$: TODO Apparently any p^3 has two nonabelian groups. (maybe like D_4 and Q_8 for 2^3)

- Problem: How many elements of order 3 does a nonabelian group of order 21 have?
  - $n_3 = 1 \bmod 3, n_3|7, n_3 \in \{1, 7\}$.
  - $n_7 = 1 \bmod 7, n_7|7, n_7 = 1$.
  - If they're both 1, then they're both single normal subgroups, so they must be $\cong \mathbb{Z}_3 \times \mathbb{Z}_7$, but that's Abelian. Contradicted assumption.
  - So $n_3 = 7, n_7 = 1$. All the 7 subgroups are $\cong \mathbb{Z}_3$ and can't overlap except the identity. So $7 * 2 = 14$ distinct order-3 elements.
- Problem: How many elements of order 5 does a group of size 60 have?
  - $n_5 = 1 \bmod 5, n_5|12 \rightarrow n_5 \in \{1, 6\}$
  - If $n_5 = 1$, like in $\mathbb{Z}_{60}$, then it has 4 elements of order 5.
  - If $n_5 = 6$, like in $(abcde) \in A_5$, there are $5!/5 = 24$ elements.
  - Both are possible, so either 4 or 24.
- Problem: If G is of order 12, and n_2, n_3 are the count of those 2-, 3-subgourps, then $n_2 > 1, n_3 > 1$ are possible, but not simultaneously. Prove.
  - $n_2 = 1 \bmod 2, n_2|6 \rightarrow n_2 \in \{1, 3\}$
  - $n_3 = 1 \bmod 3, n_3|4 \rightarrow n_3 \in \{1, 4\}$
  - Can both be 1, like $\mathbb{Z}_{12}$.
  - If $n_2 = 1, n_3 = 4$, then there are $4 * 2 = 8$ elements of order 3, and in the p^2-group, two of order 4, one of 2, one of 1. This is A_4 with the 3-groups of form $< (abc) >$, and the 2-group $\{(12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
  - If $n_2 = 3, n_3 = 1$, there is the identity, 2 elements of order 3, and up to six in the 2-groups. Example would be D_6, with $n_3 =< r_2 >$, and $n_2 = \{\{< r^3, s > \}, sr\{< r^3, s >\}(sr)^{-1} = \{< r^3, sr^2 >\}, s^2r\{< r^3, s >\}(sr^2)^{-1} = \{< r^3, sr^4 >\}$
  - $n_3 = 4$ means eight elements of order 3. $n_2 = 1$ fits one 2-subgroup. No room for more! Can't be both!

- Problem: If G is of order 56, and n_2, n_7 are the count of those 2-, 7-subgroups, then $n_2 > 1, n_7 > 1$ are possible, but not simultaneously. Prove.
  - $n_2 = 1 \bmod 2, n_2 | 7 \to n_2 \in \{1, 7\}$
  - $n_7 = 1 \bmod 7, n_7 | 8 \to n_3 \in \{1, 8\}$
  - If $n_2 = 1, n_7 = 8$, then there are $8 * 6 = 48$ elements of order 7. There is enough room for only one 2-subgroup of size $2^3 = 8$. There is a semidirect product way to do this.
  - If $n_2 = 7, n_8 = 1$, then the 2-groups require at most 49, n_2 requires 7, plus the identity is 57, so we need a little overlap in the 2-subgroups. No example provided.
- Problem: If G is of order 70, G must always contain a normal subgroup of order 35.
  - $n_5 = 1 \bmod 5, n_2 | 14 \to n_5 = 1$
  - $n_7 = 1 \bmod 7, n_7 | 10 \to n_7 = 1$
  - Therefore $1 = |G|/|N_{H_5}| \to |N_{H_5}| = |G|$, so $H_5 \triangleleft G$.
  - Therefore $1 = |G|/|N_{H_7}| \to |N_{H_7}| = |G|$, so $H_7 \triangleleft G$.
  - So the product $H_5 \times H_7 \cong G$, of size 35.
- Since any two sylow p-subgroups are conjugate, there's a homomorphism by conjugation $f : G \to S_{n_p}$, f mapping to some permutation function scrambling n_p elements.
- f isn't trivial if $n_p > 1$, since there are always elements that map one subgroup to another (Sylow II?)
- Kernel of f is normal, like any kernel.
- Example: if $n_3 = 4$, then $f : G \to S_4$ has a kernel which is a proper normal subgroup of G. If $|G|$ doesn't divide $|S_4| = 24$, then G has a proper normal subgroup since it can't be injective. We use this to prove G is not simple
- Problem: If $G = D_6$, what is n_2?
  - $n_2 = 1 \bmod 2, n_2 | 3, n_2 \in \{1, 3\}$.
  - So there's $f : D_6 \to S_3$. But 12 doesn't divide 6. So f is not injective, so it has a nontrivial kernel, which is a proper normal subgroup.
  - The 2-subgroups are given a few problems above: $\{< r^3, s >\}$ and its conjugations by sr and sr^2.

- Problem: Of those 3 2-subgroups of $G = D_6$, use the action $g \cdot H = gHg^{-1}$. This gives a homomorphism $f : D_6 \to S_3$. How many elements does ker(f) have?
  - Of the 3 2-subgroups , we're looking for an element g that doesn't change *any* of them.
  - Note that the center $Z(G) = \{e, r^3\}$ commutes with all.
  - Note also that $|G|/n_2 = 12/3 = 4$, and that every one of these groups has its own elements that conjugate H to itself.
  - Then, $\{e, r^3\}$ is the intersection of all of the normalizers. There are two elements of ker(f).
- Problem: If $|G| = 132 = 4 * 33 = 2^2 * 3 * 11$, prove it is not simple.
  - Note that $n_2 \neq 1, n_3 \neq 1, n_{11} \neq 1$ since if it did, that would provide a normal subgroup (since the normalizer is all of G).
  - Also, if for any of these $n < 11$, then $|G|$ can't divide S_n since G has a factor of 11. So this means $f : G \to S_n$ is not injective, therefore nontrivial kernel , therefore normal subgroup.
  - So if every one of them is 11 or greater:
  - $n_2 = 1 \bmod 2, n_2 | 33, n_2 \geq 11 \to n_2 \in \{11, 33\}$
  - $n_3 = 1 \bmod 3, n_3 | 44, n_3 \geq 11 \to n_3 \in \{22\}$
  - $n_{11} = 1 \bmod 11, n_{11} | 12, n_{11} \geq 11 \to n_{11} \in \{12\}$
  - But there's no way to have even $n_3, n_1 1$ in there, since $132 < 2 * 22 + 12 * 10$.