1 September 19

Recall from last time: $D_n = \{\text{rotations/reflections of n-gon}\}$, where the n rotation by $\frac{2\pi a}{n}$, $0 \leq a \leq n-1$, and the n reflections in axes of symmetry.

Claim: these are all distinct, $2n$ in total. Obviously: reflections are distinct and rotations are distinct between each other. But can we have rotation = reflection?

The answer is no: linear algebra.

- The rotation of $\mathbb{R}^2$: matrix $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Has det $= 1$.
- Reflection in $\mathbb{R}^2$ has eigenvalues ± 1, and det $= -1$.

Then he draws a picture idk ff.

Abstract version of D_n

Let $\sigma =$ rotation through $2\pi/n$, so $\sigma^a =$ rotation through $2\pi/n$. Rotations are $\sigma, \sigma^2, \ldots, \sigma^n = I$ and $I = \{1, \sigma, \ldots, \sigma^{n-1}\}$.

Now let $\tau =$ reflection in x-axis. Claim: Reflections $= \{\tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$.

Proof. D_n =group $\Rightarrow \tau\sigma^j =$ either a rotation or a reflection.

Case 1: $\tau\sigma^j$ is a reflection

Case 2: $\tau\sigma^j$ is a rotation, or σ^k for some k. But then $\tau\sigma^j = \sigma^k \Rightarrow \tau(\sigma^j)(\sigma^j)^{j-1} = \sigma^k(\sigma^j)^{-1} \Rightarrow \tau = \sigma^k\sigma^{n-j} = \sigma^{k+n-j}$. And this is impossible because LHS $= \tau =$ nontrivial reflection, but RHS = rotation, which we know can't beequal.

Thus, it has to be case 1, so $\tau\sigma^j$ =reflection $\forall j$. But $\tau\sigma^j = \tau\sigma^{j'} \Rightarrow j = j'$, $0 \leq j, j' \leq n-1$. Same argument: $\tau\sigma^j = \tau\sigma^{j'} \Rightarrow \tau^{-1}\tau\sigma^j = \tau^{-1}\tau\sigma^{j'} = \sigma^j = \sigma^{j'} \Rightarrow j = j'$. Thus, $\tau, \tau\sigma, \ldots, \tau\sigma^{n-1}$ are all different, and all reflections, so we get them all. □

Thus, we get some idea of what D_n looks like. $D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}\}$ where *sigma* is a rotation through $\frac{2\pi}{n}$ and τ is a reflection ff

ff end of page 3 and start of page 4 by closure, but what are i, j? What is the algebra rule that does this? Answer: $\tau\sigma^j = \sigma^{n-j}\tau = \sigma^{-1}\tau$. Supposedly a homework question, nominally due today, but didn't release. Anyway, we know how τ and σ interact through linear algebra, so $\tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ when it is a reflection in the y axis, and the rotation $\sigma = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Then

$$\begin{aligned} \tau\sigma &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} -\cos\theta & -\sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= ff \end{aligned}$$

So to simplify $\sigma^2\tau\sigma^3 = (\sigma^2\tau)\sigma^3 = \tau(\sigma^2)^{-1}\sigma^3 = \tau\sigma^{n-2+3} = tau\sigma^{n+1} = \tau\sigma \in D_n$.

The third way to write D_n is $\{1, \sigma, \ldots, \sigma^{n+1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}\}$ with the rules $\tau^2 = 1$ (reflection), $\tau\sigma = \sigma^{-1}\tau$, and $\sigma^n = 1$.

Remark 1. These rules imply all the others

Let's see with $(\tau\sigma^i)^2 = \tau\sigma^i\tau\sigma^i = \sigma^{-i}\tau\tau\sigma^i = 1$ (where we have used $\tau\sigma^i = \sigma^{-i}\tau$, which can be found with induction and the given rules). This is an *algebraic* way of describing D_n.

In a crude form, a group is set of elements with some rules how they interact. This wraps up our beginning bit of groups, but keep in mind S_n and D_n: they're the simplest nonabelian groups, and we can actually write down all the elements.

Ch. 1.3 Isomorphism, Homomorphism

These are going to be our version of linear transformations from linear algebra, but for groups.

Definition 1 (Homomorphism). Let G_1, G_2 be groups. A *homomorphism* from $G_1 \to G_2$ is a function $\phi\colon G_1 \to G_2$ such that $\forall g_1, g_2 \in G_1$, $\underbrace{\phi(g_1g_2)}_{\text{multiplication in } G_1} = \underbrace{\phi(g_1)\phi(g_2)}_{\text{multiplication in } G_2}$.

We must have $\phi(1_{G_1}) = 1_{G_2}$.

Isomorphism ϕ is a bijection, so it matches both sets and the multiplication, while *Homomorphism*only matches multiplication (need not be injective or surjective).

Some examples

- $\exp\colon x \mapsto e^x$, which matches $(R, +) \to \mathbb{R}^*_+$ (positive reals, with multiplication). This is a isomorphism.
- $\phi\colon \mathbb{R} \to \mathbb{C}^*$ such that $x \mapsto e^{2\pi ix}$, which sends $\mathbb{R}$ to the complex numbers of modulus 1. This is surjective, but it is not innjective, since $e^{2\pi ix} = 1, \forall x \in \mathbb{Z}$. So this is only a homomorphism.
- Let $G = n \times n$ invertible real matrices, and $\phi(g) = \det(G) \in \mathbb{R}^*$. This is only a homomorphism, since $G \to \mathbb{R}^*$ (multiplication) since $\det(AB) = \det(A)\det(B)$, but it is not injective. Also have the identity map (maps to itself).
- Let G be any group, and $\phi(G) = 1 \in G_2, \forall g \in G_1$ and any G_2. This is a homomorphism from $G_1 \to G_2$, called the "trivial" homomorphism.

Definition 2 (Subgroups). $G =$group, a subset of it is ff (bottom of page 7)

Theorem 1 (Cayley's Theorem)**.** *Let G be any finnite group. Then G is isomorphic to a subgroup of S_n (permutation on n letters) for some n.*

Concretely, this means $\exists n \geq 1$ and a hommomorphism $\phi\colon G \to S_n$ that is injective.

Proof. Let $n = \#G =$ number of elements in G. So the set of n objects = elements of G. (How do objects in G move around? When you multiply two by each other, you get another element in G.) So $forallg \in G$, consider the function L_g, R_g, where $L_g, R_g\colon G \to G$, where $L_g(x) = gx$ (fixed g, $\forall x \in G$) and $R_g(x) = xg$ (fixed g, $\forall x \in G$).

Claim: L_g, R_g are permutations of G.

Check: we need to show they are bijections (could show that they are injective and surjective, or that they have an inverse, the second is easier). So $(Lg^{-1}) \circ L_g(x) = g^{-1}(gx) = x \Rightarrow L_{g^{-1}} = (L_g)^{-1}$ is a function. Similarily, $R_{g^{-1}} = (R_g)^{-1}$. Thus $g \mapsto L_g$ and $g \mapsto R_g$ so $G \to S_n$ something something.

Check: we need to show that the homomorphism respects the multiplication. Let $\phi(g) = L_g$ and $\phi(g) = R_g$. We want $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ and $\psi(g_1g_2) = \psi(g_1)\psi(g_2)$. Looking at the first, we have LHS $= L_{g_1g_2} = x \mapsto (g_1g_2)x$ and RHS $= L_{g_1} \circ L_{g_2}(x) = g_1(g_2x) =)(g_1g_2)x$. Thus ϕ is a homomorphism. Now looking at the second, note that ψ is not a homomorphism in general. We see LHS $= R_{g_1g_2} = x \mapsto xg_1g_2$ and RHS $= R_{g_1} \circ R_{g_2}(x) = (xg_2)g_1 = xg_2g_1 \neq xg_1g_2$. Just so happens that left multiplication is the homomorphism. So we get the homomorphism $\phi\colon G \to S_n$ where $g \mapsto L_g$.

Finally, to show that this is an isomorphism, need to check that ϕ is injective.

ff (page 10 and 11)

Conclusion $\phi\colon G \to S_n$ where $g \mapsto L_g$ is an injective hommmorphism $G \to S_n$. □

Going to sort out homework, probably compressed deadline but has given some answers already.

2 September 21

Last time, we started proving (proved?) Cayley's theorem. That is, for a finite group G, there exists $\phi\colon G \to S_n$ that is an injective homorphism ($n = \#G$).

Remark 2. $\#S_n = n! > n = \#G$. G is a very small subgroup of S_n.

Something we we will see again later: $\exists m \neq n$ with $G \to S_m$ injectively (usually) m could be much smaller.

2.1 1.4 Commutativity, general associativity

The usual associative law is $(ab)c = a(bc)$: can put brackets anywhere to simplify (don't rearrange terms). Usual law of commutativity is $ab = ba$. Not going to to spend much time on this, kinda boring, can figure it out for yourself.

2.2 1.5 ff

We'll be looking at cyclic groups, and subgroupos generated by a subset.

Let G be a group, and $S \subseteq G$ any subset.

Definition 3 (Subgroup Generated by $\langle S\rangle$). $\langle S\rangle$ =smallest subgroup of G containing S. $\langle S\rangle$ is a subgroup containing S, and if H is any subgroup which contains S. Then $\langle S\rangle \subseteq H$.??? idk We all $\langle S\rangle$ the subgroup generated by S.

Existence of $\langle S\rangle$: X = set of subgroups of G containing S. Then $G \in X$, $X \neq \emptyset$. $\langle S\rangle$ is a minimal element of X. Arbitrary intersections of subgroups are subgroups (exercise), thus take the intersection of all elemments of X to get $\langle S\rangle$. Concretely, $\langle S\rangle$ is the arbitrary finite products of elements of S and their inverses.

$$\langle S\rangle = \{\prod_{i=1}^{r} S_i^{\varepsilon_i} \mid S_i \in S, \varepsilon_i = \pm 1, r = \text{ any positive integer }\}$$

You can think of this as the "span" of S (but not commutative).

Remark 3. $\langle S\rangle$ is very hard to describe in terms of S (expressions as products are usually not unique).

For example, if $G = S_n$ and $S = \{\sigma, \tau\}$ from D_n, so $\sigma = 1 \to 2, 2 \to 1$ (fixes all others) and $\tau = 1 \to 2 \to \cdots \to n \to 1$. Actually, $\langle s\rangle = S_n$. This means that we can get any permutation

Special case: $S = \{g\}$ = single element. Then $\langle S\rangle = \{g^i \mid i \in \mathbb{Z}\}$. We have $1 = g^0$ (conventiion from law of exponents) and $g^i g^j = g^{i+j}$. Our subgroup generated by S is $\langle S\rangle = \text{ group}, g \in S \subseteq \langle S\rangle \iff g^i \in \langle S\rangle \forall i$.

There exists a homomorphism $\phi\colon (Z, +) \to \langle S\rangle \subseteq G$ defined by $i \mapsto g^i$. 2 cases: ϕ is inejctive or ϕ is not injective.

Remark 4. $\phi\colon \mathbb{Z} \to \langle S\rangle$ is always onto. If ϕ is injective, then $\phi\colon \mathbb{Z} \to \langle S\rangle$ is an isomorphism, $\langle S\rangle$ and $\mathbb{Z}$ are the same.

Some notation: we would say $\mathbb{Z} \cong \langle S\rangle$ (isomorphic) (isomorphic)

Some more notation (additive notation): $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$. In this case $\langle S\rangle$ is called an *infinite* cyclic group (cyclic because it is generated by one element). We have $n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$, $-n = \underbrace{(-1) + (-1) + \cdots + (-1)}_{n \text{ times}} = -(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}})$.

Some more notation: if $S = \{g\}$, then $\langle S\rangle = \langle g\rangle$ = cyclic group generted by g. Can see that different elements g can generate the same group.

Something with matrices ff (page 5).

$\phi \to \langle g\rangle$ is not injective. This means there are repeats $g^i = g^j i \neq j$. WLOG $i > j \Rightarrow g^{i-j} = 1$ and $i - j > 0$. Define d to be the smallest positive integer with $g^d = 1$. We call d the order of g. Claim: $\langle S\rangle = \{1, g, g^2, \ldots, g^{d-1}\}$

Proof. Fix any $n \in \mathbb{Z}$. ff$n = qd + r$ where $0 \leq r \leq d - 1$. We have

$$\begin{aligned} g^n = g^{qd+r} &= (g^{qd})q^r \\ &= (g^d)^q = g^r \\ &= (1)^q g^r \\ &= ff(page6) \end{aligned}$$

If $0 \leq r_1, r_2 \leq d - 1$, let $r_2 \geq r_1$ (WLOG) and $g^{r_1} \neq g^{r_2}$ since $g^{r_1} = g^{r_2} \iff g^{r_2 - r_1} = 1$, if $r_1 \neq r_2$. But d is the smallest positive integer with $g^d = 1$. So $\{1, g, g^2, \ldots g^{d-1}\}$ represent all powers of g, with no repeats. □

Multiplication rule: $g^i g^j = g^{i+j}$. Read exponents mod d (replace by remainder). Algebra rule $g^d = 1, g^{-1} = g^{d-1}$. On this case $\langle g \rangle = \{0, 1, 2, \ldots, d-1\}$ and all additions are taken mod d. All such groups with the same d are isomorphic.

In summary, if G is a group and $g \in S$, the cyclic subgroup generated by g is $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\} \subseteq G$. There are 2 cases: $\langle g \rangle$ is infinite, $\cong \mathbb{Z}$, or $\langle g \rangle$ is finite, $\#\langle g \rangle = d$, and is equal to $\{1, g, g^2, \ldots, g^{d-1}\}$, $\cong$ integers mod d. This is commutative.

This was the simplest case, when only generated by 1 element. But what about when we generate from more than one element. Two generators can make something that is much more complex. For example, σ, τ for D_n, and no longer commutative and no longer can just be represented as powers of a single element (doesn't have to be cyclic?)

Remark 5. $\langle S \rangle = \langle g \rangle$ is described above. But if $S = \{g_1, g_2\}$ it is not easy to relate to $\langle g_1 \rangle$ and $\langle g_2 \rangle$ to the subgroup generated by both elements.

2.3 Structure of Cyclic Groups

(a). Describe all possible generators: when is $\langle g \rangle = \langle h \rangle$?

(b). Find all possible subgroups of $\langle g \rangle$

Consider the infinite cyclic group $\langle g \rangle \cong (\mathbb{Z}, +)$. Suppose $t \in \mathbb{Z}$ is a generator. Then any positive integer n is of the form

$$n = t + t + \cdots + t$$

so t is a multiple of t. This is supposed to hold for all $n \Rightarrow t = \pm 1$. Thus, ± 1 are the only possible generator.

Subgroups: let H be any subgroup of $(\mathbb{Z}, +)$. Pick $t \in H$ which is the smallest positive element. ($t \in H \iff -t \in H$, so positive elements exist.) Then $t\mathbb{Z} \subseteq H$ ($t\mathbb{Z} = \{t, t+t, \ldots, -t, -t-t, \ldots\}$). Our claim is that $H = t\mathbb{Z}$.

Proof. Suppose $s \in H$, then $s = qt + r, 0 \le r \le t-1$. Then $qt \in H$ (as above). Then $s - qt = r \in H$, which is impossible, since t is the smallest positive element. Then $H = t\mathbb{Z}$. □

Thus, subgroups of $\mathbb{Z}$ are the set $t\mathbb{Z}$, $t \in \mathbb{Z}$ (positve t).

Now we consider the finite case $\langle g \rangle = \{1, g, g^2, \ldots, g^{d-1}\} \cong \{0, 1, 2, \ldots, d-1\}$ with addition mod d. Fix t, $0 \le t \le d-1$ that generates, which means $\{0, t, 2t, \ldots, (d-1)t\} =_{\text{mod } d} \{0, 1, 2, \ldots, d-1\}$.

For example, $d = 5$. Now let $t = 2$. We have $\langle 2 \rangle = \{0, 2, 4, 6, 8\} = \{0, 1, 2, 3, 4\}$ so $\langle 2 \rangle = \langle 1 \rangle$ in integers mod 5. (The fact that 5 is prime is what makes this work, makes it cyclic; can't have a cycle sit within a group.) But if $d = 6$, $\langle 2 \rangle = \{0, 2, 4, 6\} =$ ff(page 12).

Answer???: $\langle t \rangle$ generates $\iff$ $(t, d) = 1$.

Proof. Suppose $(t, d) = s > 1$. Then $c = \frac{d}{s}$ is an integer, $0 < c < d$. Then $ct = t + t + \cdots + t$ c times. $\frac{d}{s}t = d\frac{t}{s} = d$, integer is divided by d. Thus $[ct] = [0]$ (ct is a multiple of d. $0, t, 2t, \ldots, dt$ is not distinct mod d, $[ct] = [0]$, $c < d$. Thus, if there's a common factor, can't generate.

It reamins to show that if $(t, d) = 1$, then t generates. Assume $(t, d) = 1$. Find the smallest integer s such that $[st] = [0]$. This is obviously $s = d$, because st is dividisble by d, so $d \mid s$ since $(t, d) = 1$. Thus, $0, t, 2t, \ldots, (d-1)t$ are distinct (can't have overlaps, the multiples of t are smaller than d, same argument as before).

Conclusion: possible generators in this case are the integers t, $0 \le t \le d-1$ with $(t, d) = 1$. Multiplicative rotation g^t is a generator of $\langle g \rangle \iff (t, d) = 1$. Lots of choices for generators. □

Something something this is used in a crytography scheme.

Still don't know how many open groups??? Strongly recommend reading this section before next class.

3 September 26

Last time, we were talking about cyclic groups/subgroups. G is a group, $g \in G$, then there are two cases for the subgroup generated by g $\langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$.

(a). $\langle g \rangle$ is infinite

(b). $\langle g\rangle$ finite, $\#\langle g\rangle = d$

Terminology $\#\langle g\rangle =$ the order of g (can be infinite or d). This defines the order of $g, g \in G$.

Remark 6. $\#G =$ order of G, but $\#\langle g\rangle =$ order of g (as an element). Usually context will distinguish which one we're talking about. These only coincide when $G = \langle g\rangle$ (group generated by g).

Observation: $g^m = g^l \iff g^{ml} = g^0 = 1$. Any repeat $g^m = g^l$ can be assumed to have $l = 0$. ???

Back to last class: we were trying to find all subgroups of $\langle g\rangle$ when $\#\langle g\rangle = d < \infty$. Let $G = \langle g\rangle$ and let $H \subseteq G$ be any subgroup. Let t by the samllest positive integer with $g^t \in H$. We have $0 \leq t \leq d-1$. Our claim is that $H = \langle g^t\rangle$.

Proof. The proof is the same as the infinite order case. If $h \in H$ then $h = g^s$ for some $0 \leq s \leq d-1$. We have $s = qt + r$, $0 \leq r < t$. Then $h = g^s = g^{qt+r} = (g^t)^q g^r$. But $h \in H$ and $g^t \in H$, so $g^r \in H$. But this contradicts the minimality of t unless $r = 0$ ($r < t$). Thus $s = qt \implies h = g^s = (g^t)^q \in \langle g^t\rangle$. □

Corollary 1. *Any subgroup $H \subseteq G = \langle g\rangle$ is cyclic, $H = \langle g^t\rangle$.*

We might ask what the order of $H = \langle g^t\rangle$ is. The answer is

$$\frac{\#G}{\gcd(\#G, t)} = \frac{d}{(d, t)}$$

Last time, we computed the order of $g^t = \frac{d}{(d,t)}$. Recap: the order of g^t is the smallest positive integer s such that $(g^t)^s = 1 \implies g^{ts} = 1 \implies d \mid ts$ (d is the order of g). But then s is the smallest number such that d divides ts, and then $s = \frac{d}{(d,t)}$.

After a while, people just take these kind of operations for granted, because it is quite tedious to go through details. Need to be able to prove yourself or hold in your head.

Corollary 2. order$(H) = \#H = \frac{d}{(d,t)}$ *is a divisor of $d = \#G$. Then $H \subseteq G \implies \#H \mid \#G$.*

This is a nice property of all finite groups (not just cyclic), but we will prove this later.

Corollary 3. *G is cyclic, $s \mid d \implies$ there exists a unique $H \subseteq G$ of order S.*

Proof. Existence: take $H = \langle g^t\rangle, t = \frac{d}{s}$. For uniqueness, do similar to what we showed before: given $H \subseteq G, H = \{1, g^t, g^{2t}, \ldots, g^{(r-1)t}\}$, we have r is the order of $h = g^t$. We can read off elements of G from t. The order of H determines t, since $rt = d$ ($t = \frac{d}{r}, r = \#H$). Thus H is determined by $\#H$. □

Remark 7. Thsi fails for most groups: G does not have subgroups of order r when $r \mid \#G$. This is a unique property of cyclic groups: when we pick some divisor of the order of G, we are going to get a subgroup of order of that divisor.

You have to remmber these basic facts about cyclic groups. We'll be using it a lot: we often try to understand the behaviour of a larger group by understanding cyclic subgroups of it, like with the dihedral group D_n, where we have a cyclic subgroup of order 2, and of order n.

3.1 Using our cyclic group properties for finite groups

Some terminology: the *exponent* of a group is the smallest positive integer n such that $g^n = 1, \forall g \in G$ (not typically the order).

Theorem 2. *Suppose G is commutative. Then G is cyclic $\iff$* exponent$(G) =$ order(G).

This is good for a lot of stuff that we won't actually get to in this class, but the proof is a good test of understanding. Proof requires two lemmas.

Lemma 1. *Suppose g, h are elements of a commutative group and let $m =$ order(G) and $n =$ order(G). Then $(m, n) = 1 \implies$ order$(gh) = mn$.*

Example of failing with no commutativity: take D_n, and σ is a rotation and τ is a reflection. Then $\sigma\tau$ is also a reflection, but this has order 2 (regardless of order of σ).

Proof. Suppose $(gh)^r = 1 \implies g^r h^r = 1$ (commutativity). So $g^r = h^{-r} = (h^{-1})^r$. Note that order$(g^r)$ divides order$(g) = m$ and order(h^{-r}) divides order$(h) = n$. (Using property of cyclic groups!) But since m, n were coprime, order$(g^r) =$ order$(h^{-r}) = 1$. And $\frac{m}{(m,r)} = 1$ so $m \mid r$ and $n \mid r$, thus $mn \mid r$ (coprimeness).

So $(gh)^r = 1 \implies r$ is divided by mn. It is clear that $(gh)^{mn} = (g^{mn})(h^{mn}) = 1$. Thus $n = \text{order}(h), m = \text{order}(g)$, therefore $(gh^r) = 1 \iff mn \mid r \implies gh$ has order mn. □

(proof also on page 47)

Lemma 2. *G is commutative and finite. Suppose $g \in G$ has maximal order. Then* exponent$(G) =$ order(g).

Remark 8. Suppose g_2 is any element of G. Our assumption is that order$(g_2) \leq$ order(g). Have to show $g_2^{\text{order}(g)} = 1$. (order$(g)$ is killing off every element. This is not automatic: just because order is smaller, it does not follow that being raised to the power of a larger order means it will go to 1.

Proof. Let $n =$ order(g) and $m =$ order(g_2) (random element). We have $n = \prod p_i^{e_i}$ (prime factorization) and $m = \prod p_i^{f_i}$ (using same p_i, $e_i, f_i \geq 0$). It is enough to show that $f_i \leq e_i$ $\forall i$ (then $m \mid n$). (Will show this with commutativity.)

Suppose that it is not that case, by renumbering, $f_1 > e_1$. Now g has order $n = \prod p_i^{e^i} = p_1^{e_1}\left(\prod_{i\geq 2} p_i^{e_i}\right) = p_1^{e_1} r$ and g_2 has order $m = \prod p_i^{f_i} = p_1^{f_1}\left(\prod_{i\geq 2} p_i^{f_i}\right) = p_1^{f_1} s$. Let $g_3 = g^{p_1^{e_1}}$ and $g_4 = g_2^s$. Note order$(g_3) = r = \frac{\text{order}(g)}{(\mathrm{g}, p_1^{e_1})} = \frac{n}{p_1^{e_1}}$. and order$(g_4) = p_1^{f_1}$ (for the same reason). But then by Lemma 1, order$(g_3 g_4) = p_1^{f_1} r >$ order(g) (coprime because primes are different), which is a contradiction. □

Clever, but a typical argument in group theory... reread until you get the argument. No standard proof technique in group theory, but will use a bunch of properties of specific groups, and combine the facts to get the theorem that we wanted.

Additional property of finite cyclic groups: suppose $g = \langle g \rangle$, $\#G = d$. Pick $s \mid d$, $\exists H \subseteq G$, $\#H = s$. Fact: $H = \{x \in G \mid x^s = 1\}$.

Proof. We can easily see that H is a subgroup (as defined). So it suffices (by uniqueness) to show it has order S. The elements of $G = \langle g \rangle$ are $1, g, g^2, \ldots, g^{d-1}$. The order of g^t is $\frac{d}{(d,t)}$.

$$(g^t)^s = 1 \implies d \mid ts$$

$t = 0, \frac{d}{s}, \frac{2d}{s}, \ldots$ is a list of elements satisfyin $x^s = 1$, we have S of them. □

4 September 28

ff

5 October 3

"Point-set topology has got to be one of the most boring subjects ever. After about two weeks, you get the point."

We are now hittinng the core stuff in the class.

5.1 Section 1.7

Let G be a group and X be a set. $S = S_X =$ group of permutations of X (saying in this way because if X is not finite, bijections, and if it is finite, just $S_X = S_n$).

Definition 4 (Group Action)*.* Suppose $\exists\phi\colon G \to S_X$ (a homomorphism). Then $\forall g \in G$, $\phi(g) \in S_X$ is a permutation, so $\forall g \in G, \forall x \in X$, $\phi(g)(x) = y \in X$. So we get a function $(g, x) \to y = \phi(g)(x) = g \cdot x$ (short-hand). We say that G *acts* on X; the elements of G move the elements of X around, according to the homomorphism ϕ.

For example, if $X = G$, $\phi(g) = Lg$, $x \mapsto gx$ (Cayley's theorem).

Definition 5 (Orbit)*.* Fix $x \in X$. Define $\text{orbit}_G(x) = \text{orb}_G(x) = \{y \in X \colon \exists g \text{ with } \phi(g)(x) = y\}$

In words: $\text{orb}_G(x) \subseteq X$, elements we can reach via permutationns from $\phi(G) \subseteq S_X$. For example (Cayley's theorem), $\text{orb}_G(1) = G$, since $\forall g \in G, Lg(1) = g \cdot 1 = g$.

X is divded up into G-orbits, these orbits carry lots of information (about G!), pretty fundamental for understanding the structure of a group (have to choose good maps ϕ and sets X). Will look at a lot later.

Today, we are only interested in one example:

$$\phi\colon G \to S_G = \text{ permutations of } X : \quad g \to Lg$$

and

$$\psi\colon G \to S_G = \text{ permutations of } X : \quad g \to Rg^{-1}$$

(where we've put the inverse to make it a homormorphism). ϕ, ψ give injective maps $G \hookrightarrow S$ (hook is injection).

Definition 6 (Left Coset)*.* $H \subseteq G$ be any subgroup, can restrict ϕ, ψ to H and get $H \hookrightarrow S = S_G$ (permutations of G). Consider $g \in G$, $\text{orb}_H(g)$ under ϕ. Define $Hg = \{L_h(g), h \in H\} = \{hg \mid h \in H\}$. This is called a coset of g with respect to H (or a coset of H with respect to g).

(naming depends on g wrt H or the other way ff)

Definition 7 (Right Coset)*.* Take ψ instead; $gH = \text{orb}_H(g) = \{gh^{-1} \mid h \in H\} = \{gh \mid h \in H\}$. This is the right coset of H.

Warning: sometimes left/right get swapped.

Remark 9*.* $gH \neq Hg$ in general

Lemma 3. *The function $h \mapsto gh$ and $h \mapsto hg$ give bijections $H \to gH$ and $H \to Hg$.*

Proof. $gh = gh' \implies h = h'$ (multiplication by g^{-1} on left). Onto is obvious. (or if H is finite $\#H - \#gH\#Hg$ $\forall g$). □

Lemma 4. $G = \sqcup_{g_i} g_i H = \sqcup_{g_i'} H g_i' =$ *disjoint union of cosets. (what is g' ?fff)*

Proof. $\forall g \in G$, $g \in gH$ and $g \in Hg$. So $G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg$.

Observation: $g_1, g_2 \in G$, either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \emptyset$. If we assume this observation, we are done. This is because $G =$ disjoint union of distinct cosets. If we prove this observation, we prove the lemma.

Suppose $g_1 H \cap g_2 H \neq \emptyset$. $\exists h_1, h_2 \in H$ with $g_1 h_1 = g_2 h_2$. Then $g_1 = g_2 h_2 h_1^{-1} \in g_2 H$. Then $\forall h \in H$, $g_1, h \in g_2 H$ (H is closed). But then $g_1 H \subseteq g)2H$, and by summetry, $g_2 H \subseteq g_1 H$. thus $g_1 H = g_2 H$. □

Corollary 4. $G = \bigsqcup_{g_i} g_i H = \bigsqcup_{g_i'} H g_i'$*, and each coset has the same cardinality. This means that if G is finite, $\#G = r \cdot \#H$ (where r is the number of cosets). In particular, $\#H \mid \#G$ and r is the index of H in G (number of distinct cosets).*

This gives us the following theorem.

Theorem 3 (Lagrange's theorem)**.** *If G is finite and H is a subgroup $\implies \#H \mid \#G$.*

This means that orders of subgroups can't be random. They have to divide the order of the original group. (Evan Chen: any element's order must divide the order of G).

Remark 10*.* The converse if false: if $d \mid \#G$, there need not be a subgroup of order d. Examples are hard to come by, but can find.

Notation: $[G\colon H]$ = index of H in G = the number of distinct cosets of H (left or right, depending on what we're looking at). These values are the same for finite gruops because $[G\colon H] \cdot \#H = \#G$ ($\#H$ is the seize of a coset, which is the same whether it's a left coset or right coset).

Coset representatives: set of elements of G, one from each distinct coset. Example: $G = \mathbb{Z}$, $H = n\mathbb{Z}$, $n > 1$. Then the coset representatives are just the remainder classes, $\{0, 1, 2, \dots, n-1\}$, because the cosets are just $x + kn, k \in \mathbb{Z} = x + H$ (additive notation).

We're taking a group, and we're cutting it up into pieces. All these pieces are of the same size, and they're all of size H.

Example: $G = (\mathbb{Q}, +)$, $H = \mathbb{Z}$. Coset of $x = \{x + k \mid k \in \mathbb{Z}\}$. contains a unique $r \in \mathbb{Q}, 0 \leq r < 1$. Cosets represented by $\{r \in \mathbb{Q}, 0 \leq r < 1\}$.

$$\mathbb{Q} = \bigsqcup_{\substack{0 \leq r < 1 \\ r \in \mathbb{Q}}} \{r + k \mid k \in \mathbb{Z}\}$$

Cosets are a special case of equavalence classes: given $G \supseteq H$, define $x \sim y$ to mean $(x, y \in G) \iff \exists h \in H$ such that $xh = y$. Equivalence class $[x] = xH$. Can also define $x \sim y \iff \exists h \in H, hx = y$, $[x] = Hx$.

Definition 8 (Quotient Map). G/H = set of cosets $gH, g \in H$, and $H\backslash G$ = set of cosets $Hg, g \in G$. There exists unique functions $\pi\colon G \to G/H$ or $G \to H\backslash G$, where $g \mapsto gH$, $g \mapsto Hg$.

Start with any G finite, $H \subseteq G$ where $H = \langle g \rangle, g \in G$. $\#H = \text{order}(g) < \infty$. Lagrange's tells us that $\#H \mid \#G \implies \text{order}(g) \mid \#G\ \forall g \in G$, thus $g^{\#G} = 1$ for all $g \in G$. Thus the $\exp(G)$ is $\leq \#G$. This implies Lagrange's for cyclic groups, but not otherwise. (really?)

5.2 1.8

Is G/H (or $H\backslash G$) a group in a natural way? "natural" means $\pi\colon G \to G/H$ should be a homormophism. The answer in general is no. This only works for special H, called a *normal* subgruops of G.

Reason: fix $g_1, g_2 \in G$.

$$\begin{aligned} \pi(g_1 &= g_1 H \in G/H \\ \pi(g_2) &= g_2 H \\ \pi(g_1 g_2) &= (g_1 g_2) H \end{aligned}$$

If it is a homomorphism, we have to have

$$\pi(g_1 g_2) = \pi(g_1)\pi(g_2)$$

but

$$\pi(g_1 g_2) = g_1 g_2 H = (g_1 H) \cdot (g_2 H)$$

where this multiplication (if it exists) is in G/H. Problem: this is not a well-defined multiplication of cosets. Explitictly: the rule is given 2 cosets $X, Y \in G/H$, $X \cdot Y = Z$ is defined by choosing representatives $g_1 \in X_1, g_2 \in Y$, setting $Z = [g_1 g_2]$. Point: different choices of g_1, g_2 in X, Y will produce different Z's!

Example: pick $X = [g], Y = [g^{-1}]$, $Z = [gg^{-1}] = [1] = H$. Now we change g with $gh \in gH$ (this is a different representative of the same coset). Now we get $z = [ghg^{-1}] \neq H = [1]$. In general, $ghg^{-1} \notin H$ (can't commute h and g). We need some further conditions on G to make this work out, we need $ghg^{-1} \in H$. This leads us to the definition of a normal subgroup.

Definition 9 (Normal Subgroup). $H \subseteq G$ is a *normal* subgroup if $\forall g \in G, \forall h \in H$, $ghg^{-1} \in H$.

Theorem 4. *If H is a normal subgroup, then $G/H = H\backslash G$ and the maps $G \to G/H$ and $G \to H\backslash G$ are homomorphisms.*

In this case, write $G/H = H\backslash G$ (normally only use the first), called the *quotient* group of G mod H. Example: if G is commutative, all subgroups are normal ($\mathbb{Z} \supseteq n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ = integers mod n).

Will do the proof of the theorem next time. For next time, read the relevent section in the text. The presentation is a bit more elaborate than needed, but really going through the conditions for it to be a homomorphism (what we did with the X, Y, Z).

6 October 5

Changing order a little from textbook. ff I completely missed the first page.

Question: can we make G/H or $H\backslash G$ a group such that π is a homomorphism? Answer: no, necessary condition $\forall g \in G, h \in H$, $ghg^{-1} \in H$ $(*)$. Reason: definition of π is $\pi(x_1x_2) = x_1x_2H$, $\pi(x_1) = x_1H$, $\pi(x_2) = x_2H$.

π is a homomorphism $iff\pi(x_1, x_2) = \pi(x_1)$ ff

G/H to be defined by

$$\pi(x_1)\pi(x_2) = (x_1H)(x_2H) = (x_1x_2)H = \pi(x_1x_2)$$

for all x_1, x_2 $(**)$. This is not well defined unless $(*)$ holds. E.g. $x_1H = (x_1h)H, \forall h \in H$. But $(x_1H)(x_2H) = (x_1hH)(x_2H) = (x_1hx_2)H \neq x_1x_2H$ since $x_1hx_2H = x_1x_2H \iff x)1hx_2$.

Hmm, I might just throw this lecture, I've already behind and doing piazzas.

Some notes about normal groups (end of page 6). Every group has normal subgroups, namely the identity and itself. A group that does not have any normal subgroups not these two are called simple. D_n and even permutations?? And alternating group? Galois theory says that there is a formula for the roots of an equation iff there is some condition on the normal subgroups.

This is the place where students start getting hopelessly lost, so make sure you know what everything is saying. The homomorphism theorems are like the IVT and MVT in calculus: once you introduce it, just going to use it quickly and without mention at times.

Any homomorphism will obey the picture (page 9). So knowing the kernal tells you a lot about the homomorphism. If you have a homomorphism, you can make a normal subgroup (the kernel), and if you have a normal subgroup, you make a homomorphism, kinda tricky because both direction... but saying that these are fundamentally the same thing.

Every point in the coset has exactly one image. The cosets are getting crunched into one image in the ϕ.

Nike: Understanding of group theory isn't linear, it goes from being mystical to being obvious. It's like a step function. Grades normally go up as the term goes on.

Today has mostly been 1.8 and 1.9. Really suggest reading it.

Herstein is extremely user friendly, and students tend to like it in the beginning. Dummit and Foote is good, but it's a word salad. They take complicated things... he thinks it's really hard to find anything. Jacobson is a little abstract and terse, but you will come to appreciate.

Next section is on fundamental theorem of homomorphisms, 1.10. Would suggest pre-reading it. There's a lot of notation, really need to see it a little before. Make sure you understand 1.8, 1.9, but 1.10 might be a bit rough. Midterm will be whatever we cover up to a week before.

7 October 10

Midterm 1: Thursday, next week, up to and including 1.10.

Recall last time: hommomorphisms and quotients.

$$G_1 \xrightarrow{\phi} G_2$$

$K = \text{kernel}(\phi) = \ker(\phi) = \phi^{-1}(1_{G_2})$. K is a normal subgroup, $G_1/K \cong \phi(G_1) \subseteq G_2$. We saw (draw picture ff page 1).

Corollary 5. *If ϕ is surjective, $\phi(G_1) \cong G_1/K$.*

Notation (exact sequence): G group $K \subseteq G$ normal. $1 \xrightarrow{\subseteq} K \xrightarrow{\subseteq} G \xrightarrow{\pi} G/K \xrightarrow{\text{all to 1}} 1$ means the image of each group on the left of the arrow is the kernel of the next map (arrows are homomorphisms). $1 \to K$ subset (is injective) and $K \to G$ subset (injective). (Yoo it's like the thing Sebastian drew for the de Rahm cohomology). Some clarity: can draw $G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3$, means that $\phi_1(G_1) = \ker(\phi_2(G_2))$.

The point is G is "built" from $K, G/K$. Our goal is to study G by analysing the smaller pieces $K, G/K$. Answer (partial): fundamental theorems.

The first fundamental theorem relates subgroups of G/K with certain subgroups of G. Note that this numbering is specific to Jacobson.

Theorem 5 (First Fundamental Theorem (Part a))**.** *Construction: $H \subseteq G/K$ a subgroup. $\pi^{-1}(H) = H' \subseteq G$. Then $H \leftrightarrow H'$ is a bijective correspondence between subgroups of G/K and subgroups of G which contain K.*

Proof. Note that since H is a subgroup of G/K, $\pi^{-1}(H) = H' =$ subgroup of G, contains K. Want to show bijection, so show π^{-1} has an inverse.??? If H' is a subgroup of G containing K, then $H = \pi(H')$ and is a subgroup of G/K. We are going from subgroups of G that contain K to subgroups of G/K. Note that this is the inverse of the previous function, $\phi(\phi^{-1}x)) = x, \forall x \in G/K$. Thus $H \xrightarrow{\text{preimage}} H' \xrightarrow{\pi} H$ follows. For a bijection, have to check inverse on the other side as well. So start with $H' \supset K$, subgroup of G. Send to $H = \pi(H')$, take preimage. Do we get H' back? Recall $\pi \colon G \to G/K$, $x \mapsto xK$. So $\pi^{-1}(\pi(x)) = xK \subseteq G$ (the whole coset). Thus, for any $x \in G$, $\pi(x) = xK$, $\pi^{-1}(\pi(x)) = \pi^{-1}(xK) = xK \subseteq G = \{xk \mid k \in K\}$. Thus $\pi^{-1}(\pi(H')) = \{h'k \mid k \in K, h' \in H\} =$ union of cosets coming from $H' = H'$ since $K \subseteq H'$ by assumption. □

Really important to understand this. This is only part a in theorem 1, and will use alot.

Corollary 6. *Assume that $H' \supseteq K$.*

(a). H is normal in $G/K \iff H'$ is normal in G.

(b). If so, $(G/K)/H \cong G/H'$

Intuitively, $G \supseteq H' \supseteq K$, divide by K to get G/K, divide again by $H = \pi(H')$, this is the same as dividing by H' in one step.

Modding out by K squashes kernel to identity, and we do it twice (from G to G/K and then to $(G/K)/H$, or just G/H').

Example (Abelian setting where everything is normal): $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 6\mathbb{Z}$. Here, $G = \mathbb{Z}, H' = 2\mathbb{Z}, K = 6\mathbb{Z}$. $G/H' =$ cyclic of order 2. $G/K =$ cyclic of order $6 \supseteq$ a subgroup of H of order 3. $\underbrace{(G/K)}_{\text{order 6}} / \underbrace{H}_{\text{order 3}}$ has order $2 \cong \mathbb{Z}/H'$.

Explicitly: $G/K = \mathbb{Z}/6\mathbb{Z}$ are the cosets: $\{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, \dots\}$. We have $\pi \colon x \mapsto x + 6\mathbb{Z}$. We now have $H = \pi(H') = \{0 + \mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$. So then $G/H' = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$. Again, to see this more explicitly, we have $H = \{[0], [2], [4]\}$, and $[1] \in G/K$, we have $1 + H = [1], [3], [5]$. So $G/K = H \sqcup [1] + H$. Could have just modded out by H' at the beginning (cutting group up into evens and odds).

Proof. (a). Is easy. Suppose H' is normal in G. This means that $gH'g^{-1} \subseteq H' \iff gh'g^{-1} \in H' \forall g \in G, h' \in H'$. We have to show $\pi(H') = H$ is normal in G/K. But note we have $\pi(x)\pi(h')\pi(x)^{-1} = \pi(xh'x^{-1}) \in H$, and since $xh'x^{-1} \in H'$ and $\pi(H') = H$. Thus H' normal in $G \implies H$ normal in G/K.

Conversely, given H normal in G/K and want $H' = \pi^{-1}(H)$ is normal in G. By definition, this means $\forall g \in G$, $h' \in H'$, $gh'g^{-1} \in H'$, which is truee if and only if $\pi(gh'g^{-1}) \in H$. But recall that $\pi(gh'g^{-1}) = \pi(g)\pi(h')\pi(g^{-1}) = (gK)(h'K)(gK)^{-1} \in H$ (elements of H are cosets). But by assumption, H is normal, so we are done.

(b). (Sketch) Consider $G \supseteq H \supseteq K$ (K, H' both normal). Then $H' \supseteq K$ means we can write $H' = \sqcup h'_i K$. Then each coset $xH' = \sqcup x h'_i K$ ($h'_i K \in H = \pi(H')$). So cosets of H' break up as cosets of K. Dividing by K and then by the image of H' turns out to be the same as first grouping according to cosets of K, then some of these cosets together to get cosets of H'.

□

8 October 17

Recall from last time: Fundamental Theorem (part 1): G is a group, K is normal, and $\phi \colon G \to G/K$ is surjective.

Theorem 6. *(a). $H \leftrightarrow \phi^{-1}(H) = H'$ is bijection between $\{$subgroups of $G/K\} \leftrightarrow \{$subgroups of G containing $K\}$.*

(b). H normal in $G/K \iff H'$ normal in G. In this case $(G/K)/H \cong G/H'$.

Last time, proved (i), but it still remains to show (ii).

Proof. H' normal in $G \iff gH'g^{-1} \subseteq H' \forall g \in G$. Apply ϕ: get $\phi(g)\phi(H')\phi(g)^{-1} \subseteq \phi(H') = H$ for all $g \in G$. Since ϕ is surjective, $G \to G/K$. $\phi(g)$ covers all of G/K as g varies, thus get that H is normal in G/K.

Other direction: if H is normal in G/K want $\phi^{-1}(H) = H'$ is normal in G. By definition of normal, we have that for all cosets $gK \in G/K$, $(gK)H(gK)^{-1} \subseteq H$. We do the algebra:

$$\begin{aligned}
(gK)(H)(gK)^{-1} \subseteq H &\implies \phi(g)H\phi(g^{-1}) \subseteq H \\
&\implies \phi(g)\phi(H')\phi(g^{-1}) \subseteq \phi(H') && \forall g \in G \\
&\implies \phi(g)\phi(h')\phi(g^{-1}) = \phi(h'') && \forall h' \in H',\ \text{some } h'' \in H' \\
&\implies \phi(gh'g^{-1}) = \phi(h'') \in H
\end{aligned}$$

This is true for all $g \in G, h' \in H'$, and for some $h'' \in H'$, thus $gh'g^{-1} \in \phi^{-1}(\phi(h'')) \subseteq H'$. □

Get used to this. We are going to be doing a lot of symbol pushing. This is why the book is called basic algebra; stuff like this should become doing arithmetic.

Now how do we get the second bit, $(G/K)/H \cong G/H'$.

Proof. Start by getting a map from one to the other. Need to remember that $\phi^{-1}(H) = H' \supseteq K$. Start with $(G/K)/H$. The element of this are of the form xH for $x \in G/K$. But $x = yK$ for some $y \in G$. Want to get form this an element on the right: $zH', z \in G$. Then we use the obvious map, $x = yK \to yH'$ (it maps to itself). There is ambiguity: different representative $y' = yk, k \in K$. Our function gives ykH' but this is equal to yH' since $K \subseteq H' \implies kH' = H'$. So we get a well defined function from $G/K \to G/H'$.

Standard: we are defining a function on cosets, not on elements, so need to show well-defined; regardless of choice of element in the set, map to the same set.

Example (aside): $G = \mathbb{Z}$ and $K = 4\mathbb{Z}$. Then G/K are the remainders modulo 4: $\{[0, [1], [2], [3]\}$. And if $H = \{[0], [2]\}$. What is pre-image of this (ϕ is a map from G to G/K??? so H is a subset of G/K?... wait yeah, obviously, otherwise how would we mod out by H)? $\phi^{-1}(H)$ = even numbers (remainders are 0 and 2) $= H' = 2\mathbb{Z} \supseteq 4\mathbb{Z} = K$. What is a map $G/H' \to (G/K)/H$. We have $\{[0], [2]\} = H$ and $\{[1] + [3]\} = [1] + H$ in $(G/K)/H$. Chinese Remainder Theorem!!! (I think... he was doing $\mathbb{Z}/6\mathbb{Z}$ example with $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$)

Back to the theorem: $G \supseteq H' \supseteq K$. Map is $G/K \to G/H'$, $xK \mapsto xH'$ (well-defined by what we said before since $K \subseteq H'$). Our claimm is this is a homomorphism when H', K is normal. We know that by the construction of quotients that $(xK)(yK) = xyK$ thus $(xH')(yH') = xyH'$ so homomorphism (multiplication is inerited from G). Now what is our theorem on homomorphisms say? It says that if ψ is onto, then image$(\psi) \cong$ domain of $\psi/\ker(\psi)$. ψ is obviously onto (because all the coset representatives are in G; all a surjective images of G). What is our kernel? Well, it's H! Because these are the elements xK such that $xH' = H$ which are just the ones in H'. Thus the kernel are the cosets $xK, x \in H' = H'$ (by definition $H = \phi(H')$). [I answered and solved this, my (equivalent) explanation: the identity of the cosets in G/H' is H', and $\phi(H) = H'$] □

8.1 Isomorphism Theorem 2

This works for any subgroup of G which contains K. What about other subgroups? Start with $G \supseteq K$ normal, H' is any subgroup of G (not necessaryily $H' \supseteq K$), $\phi \colon G \to G/K$, and define $H = \phi(H')$ as before. This is a subgroup of G/K. Our bijective correspondance isn't going to work anymore, because we don't have $H' \not\supseteq K$.

Fact: $\phi \colon H' \to H$ is onto by definition, thus $H \cong H'$. $\ker(H' \to G/K) = K' = K \cap H'$ (since these are the elements $x \in H'$ where $\phi(x) \in K = 1_{G/K}$). So

$$H \cong H'/K',\ K' = H' \cap K$$

(consistent with previous case $H' \supseteq K \implies K' = K$). Now $\phi^{-1}(H)$ = all the cosets $h'K$, where $h' \in H'$ $= \{h'k \mid h' \in H', k' \in K\}$. Nike growled because he kept getting the primes wrong lol. "When the notation is harder to keep track of than the ideas, you're in a good spot."

Point: $\phi^{-1}(\phi(H')) = H'K = \{h'k \mid h' \in H, k \in K\}$ is a group since the preimage of a group is a group (homomorphism theorems). Direct check (need to use K is normal): $(h'k)(h''k'') = h'(h'')h''^{-1}kh''k''$ and $h''^{-1}k'' \in$

K so this is $h'''k'''$ (something in H' times something in K'). Used the algebra trick:

$$\begin{aligned} x_1y_1x_2y_2 &= x_1x_2x_2^{-1}y_1x_2y_2 && \text{multiplying by } x_2x_2^{-1} \\ &= [x_1(x_2)](x_1^{-1}y_1x_2)y_2 \\ &= (x_1x_2)(y_3y_2) && \text{if normal} \end{aligned}$$

So normal is very useful, because $xy \neq yx$ typically in groups. but to compare $xyx^{-1}x = y'x$, $y' = xyx^{-1}$, $xy = y'x$ always if $y' = xyx^{-1}$.

Strongly recommend doing the 10 million problems in Herstein. Do the problems in Herstein in the early sections. You just need to get familiar with the algebra. Do all these in the beginning of chapter 2 in Herstein (his print out is page 48). Don't panic about this, just do a lot of problems.

Properties of homomorphisms are quite important. It will allows us to find out that there are only two groups of order 55, one commutative and one non commutative, etc.

Note if G finite, $\#(G/K) =$ the number of distinct cosets $=$ the number of elements in G divided by the number of elements of K, since each coset has K elements. Thus $\#K \mid \#G$ (Lagrange), so $\#G/K \mid \#G$.

9 October 24

Recall our Fundamental Theorems: If $\phi\colon G \to G/K$.

- $H \subseteq G/K$, then $H' = \phi^{-1}(H)$ is a subgroup of G containing K and H' normal $\iff$ H normal in G/K. In this case $G/H' \cong (G/K)/H$, $G \supseteq H' \supseteq K \overset{\phi}{\rightsquigarrow} G/K \supseteq H = H'/K \supseteq 1_{G/K} = K/K$ (the squiggly arrow just means this side becomes the other side when we apply ϕ).
- If H' is any subgroup of G then $\phi(H') = H \cong H/(H' \cap K) \cong (H'K)/K$. $\phi^{-1}(H) = H'K$. We talked about last time, proof is just using the definitions.

Want to apply these to specific homomorphisms. This takes us to this business of groups acting on sets... the techinical heart of the class.

Goal (a): given $n > 1$, find all groups of order n (up to isomorphism). Goal (b): Is the converse of Lagrange's theorem true? (If $d \mid \#G$ does there exist a subgroup of order d.)

Answers:

(a). In principle known, but very complicated. We will give a (very) partial answer: only for specific kinds of n

(b). In general, the converse is false, but we still have that if p is a prime and $p \mid \#G$ then

  (a) $\exists x \in G$, $\text{ord}(x) = p$ (Cauchy's Theorem)

  (b) if $\#G = p^r \cdot s$ with $(s, p) = 1$, then there exists a subgroup of order $p^{r'}$ for all r' in $0 \leq r' \leq r$. So the converse of Lagrange's works if d is a prime power (Sylow's Theorem).

We will prove all of these before the end of the class.

9.1 Method of proof

Recall Lagrange's theorem: $\#G = n$, $H \subseteq G, \#H = d$. Divide G into cosets of H, each coset has size d. If there are t cosets, n elements are grouped into t subsets of size d. Thus $n = dt \implies d \mid n, t \mid n$. ($\implies$ if H is normal, then $\#(G/H) = t$ als divides $\#G = n$). Counting argument: we divide n elements into t equisize pieces.

The new method is just counting again, but instead of counting elements of G, we count other sets. Quite clever: the other sets can be quite random, and there is lots of choice; we have to somehow relate them to G.

How does this work: let X be a finite set. Consider a homomorphism (assume it exists) $\phi\colon G \to S_X =$ set of permutation of $X \cong S_m$, $m = \#X$. Recall $\#S_X = m!$. ϕ need not be injective or surjective. We partition X into equivalence classes X_i where the equivalence relation is $x \sim y \iff \exists g \in G$ such that $\phi(g)(x) = y$ ($\phi(g) \in S_X$ is a permutation of X). Recall that this is the definition of an orbit: the equivalence classes are just orbits of G acting via ϕ as permutations. In this situation, we say that G acts on X via ϕ. We have not told you anything about X or ϕ, so how will this help us understand G?

Counting argument: $\#X = \sum$ sizes of orbits $= \sum$ sizes of equivalence classes. This doesn't look particularly useful yet, we don't have size of X yet. Here's the miracle: the size of these orbits $\#X_i$ has to divide the order of G (will have to prove this). This counting reveals the structure of G if we choose X, ϕ clearly.

Ex. Cayley's theorem sets up an action of G on $X = G$. $g \mapsto L_g$, $L_g(x) = gx$, $x \in G$ (the left translation business). There's only one orbit, because $\forall g \in G$, $L_g(1)$ sends $1 \mapsto g \cdot 1 = g$, so $[1] = G$. (An orbit says there's one element in the group L_g??? that can get you to the element; $x, y \in X$ in the same orbit $\iff \exists$ some $g \in G$ with $\phi(g)(x) = y$, and don't care which g.) Counting doesn't say anything interesting: it just says $\#G = \#G$.

Ex. Let H be any subgroup of G (not necessarily normal) and set $X = G/H$ (quotient set of cosets). Given $g \in G$, we have to define $\phi(g)$ as a permutation of $X = G/H$. Define $\phi(g)\colon xH \mapsto gxH$. To get $\phi\colon G \to S_X$, have to check i) that ϕ is well-defined, and ii) $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$. Check i): suppose we pick a different representative x' in xH. Then $x' = xh, h \in H$, so $gx'H = (gxh)H = gxH$ since H is closed. Check ii):

$$\begin{aligned}
\phi(g_1g_2)(xH) &= g_1g_2xH \\
&= g_1(g_2xH) \\
&= \phi(g_1)(g_2xH) \\
&= \phi(g_1)\phi(g_2)(xH)
\end{aligned}$$

Oh, and this is a permutation, since inverse is just $\phi^{-1} = g^{-1}$ so bijection.

Subexample: Suppose G has order n and $H \subseteq G$ has order d. This construction produces a homomorphism $G \to S_{n/d} \cong S_X$ (where $n/d = \#(G/H) =$ the number of cosets). This is useful, because $n/d!$ because is usually much smaller than $n!$??? Consider when $n = 15$, and assume G is not cyclic. Let $H = \langle g \rangle$ for some $g \in G$, $g \neq 1$. $\#H = 3, 5$. Suppose $\#H = 3$. We get $\phi\colon G \to S_X$, which is a map from a group of order 15 ot one of order $(\#X)! = 5!$. The other case is more intersting: if $\#H = 5$, then $\#X = 3$, $\#S_X = 6 = 3!$. So $\phi\colon G \to S_X$, which is a map from a group of order 15 to one of order 6. Thus, this map cannot be injective! We have a nontrivial kernel, so there exists a normal subgruop of order 5 or 15. The reason for this is from Homomorphism theorems: $\phi(G) \subseteq S_X$, of order 6. But $\phi(G) \cong G/K$, has order dividing $15 = \#G$ has to divide $\#S_X = 6$. Thus, the only possibilities for $\#G/K$ divide $(15, 6) = 3$. So G/K has order 1 or 3, so either K has order 15 or order 5. Now we claim that $\phi(G) \neq \{1\}$. $\phi(g)(H) = gH \neq H$ unless $g \in H$, thus $\phi(g)$ is not trivial if $g \notin H$ (such that g exists since $\#H = 5$, $\#G = 15$). Thus, $phi(G)$ has order 3, and $K = \ker(\phi)$ is a normal subgroup of order 5.

Recap of example: we start with G of order 15, not cyclic. Pick $g \in G$, $H = \langle g \rangle \subsetneq G$. $X = G/H =$ cosets of H, and $\phi\colon G \to S_X$ where $g \mapsto \phi(g)\colon xH \mapsto gxH$. G is not cyclic, so $\#H = 3, 5$, and if $\#H = 3$, got nothing. But when $\#H = 5 \implies \phi$ is not injective, and has a kernel K of order 5. We have two subgruops, H, K, and actually it will turn out that $H = K$, but not true in general. Conclusion (not obvious): if $\#G = 15$ and G is not cyclic, and $g \in G$ has order 5, then $\langle g \rangle$ is normal in G!! (Did assume that we could pick an element of order 5.)

Lol goat girl just pointed out that all groups of order 15 are cyclic (all abelian). So we just throw on the condition that g is not a generator of G.

This is a very important example. Let's talk more about it. Let G be any group and H any subgroup. Let $X = G/H$ and ϕ as above. The question is, how many orbtis are there? Is $gH \sim H$ via ϕ? Yes because $\phi(g)(H) = gH$ by definition ($H = 1 \cdot H$). So there is only one orbit, of size $\#X = [G : H]$.

Definition 10 (Transitive). Consider $\phi\colon G \to S_X$. ϕ is called *transitive* if there is only one orbit.

When $X = G/H$ and ϕ is as above, ϕ is transitive. The Cayley's action is also a transitive action.

Ex (important): $X = G$, but this time, $\phi(g) = \phi(g)(x) = gxg^{-1}$ ($x \in G$). This is obviously a permutation since $\phi(g^{-1}) = \phi^{-1}(g)$, and so bijection, and $\phi(g_1g_2)(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = \phi(g_1)(\phi(g_2)(x))$, so homomorphism. So we get $\phi\colon G \to S_n$ where $n = \#G$. Now, something interesting happens. We had a similar homomorphism with Cayley's theorem, but that was injective, and had one orbit. In general ϕ is not injective, and has many orbits. What you get is that

$$\#G = \sum \#(\text{orbits})$$

(these terms can all be different). This is one of the most important equations in group theory, called a "class equation". Recall we've seen this in linear algebra: we grouped together similar matrices $A \sim B$ when $A = MBM^{-1}$. Likewise, we're grouping together elements of the group when they're "similar": $x \sim y \iff \exists g \in G$ such that $gxg^{-1} = g$ ($x, y \in G$). With matrices, the kernel of this map were the scalar matrcies (diagonal); notably, these commute with all other matrices. So $\ker(\phi) = \{g \in G \mid \phi(g) = \text{ trivial } \iff gxg^{-1} = x, \forall x\} = \{g \in G \mid gx = xg, \forall x\} =$ center of G (elements that commutie with everythinig).

10 November 9

10.1 Solvable Groups (Section 4.6)

The name comes from the origin of group theory.

Definition 11 (Solvable Group). G is called solvable if there exist subgroups $G_1 = G$, $G_2 \subseteq G_1$, $G_3 \subseteq G_2$ until $G_r = \{1\} \subseteq G_{r-1}$ (decreasing).

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{r-1} \supseteq G_r = \{1\}$$

such that G_{i+1} is normal inside G_i (not neccessarily in G) and G_i/G_{i+1} is abelian.

This definition looks arbitrary, but actuall goes back to Galois' study of polynomials. Motivating question: $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with rational coefficients, and $f(x) = \prod_{i=1}^n (x - \alpha_i)$ where $\alpha_i \in \mathbb{C}$ (complex roots); how do we find α_i in terms of the coefficients $a_1, a_2, \ldots, a_{n-1}$ (a formula for the roots)? We want polynomials in $a_1, a_2, \ldots$ and $\sqrt{\ }$ of some kind. Does this formula exist?

In the case of $n = 2$: $(x - \alpha_1)(x - \alpha_2) = x^2 + ax + b = 0$. Our formula is $\alpha_i = \frac{-a\pm\sqrt{a^2-4b}}{2}$ ("I don't even know the quadratic formula"). This is just found from completinng the square. Cubics: possible, messy. Quartics: possible, even worse (Jacobson exercise). deg 5 and up: no solution (due to Galois). The proof of this actually uses group theory.

The way to do this is to realize that the coefficients have a simple expression in terms of the roots. E.g.:

$$\begin{aligned} a_0 &= \prod(-\alpha_i) = (-1)^n \prod \alpha_i \\ a_1 &= \prod \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_{n-1}})\pm \\ &\vdots \\ a_{n-1} &= \pm(\alpha_1 + \cdots + \alpha_n)??? \end{aligned}$$

(where in a_1, they are the distinct $n-1$ tuples). These are all called symmetric functions: they are invariant under permutatin roots. The coefficients treat all roots the same! The problem is that these roots are different, they are not all the same; we have to somehow break the symmetry in the coefficients (otherwise we cannot determine the roots).

How do we do this when $n = 2$: $(x-\alpha)(x-\beta) = x^2-(\alpha+\beta)x+\alpha\beta = x^2-a_1x+a_0$ This is symmetric in the sense that I could switch α and β and would get the same. Functions that are not symmetric: $\alpha/\beta, \alpha^\beta, \alpha - \beta$ (we swap the two, we get a different value). So we can write $(\alpha-\beta)^2 = \alpha^2 - 2\alpha\beta + \beta^2 = (\alpha+\beta)^2 - \alpha\beta = a_1^2 - 4a_0 = a^2 - 4b$ (kind of a trick: we can write the square of this nonsymmetric expression in terms of things that were symmetric expressions). So $\alpha - \beta - \sqrt{a^2-4b}$, $\alpha = \frac{(\alpha+\beta)+(\alpha-\beta)}{2} = (a + \sqrt{a^2-4b})/2$ and $\beta = \frac{(\alpha+\beta)-(\alpha-\beta)}{2} = (a - \sqrt{a^2-4b})/2$.

For cubics, we have three roots. $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = x^3 + a_2x^2 + a_1x + a_0$. Note

$$\begin{aligned} a_2 &= -(\alpha_1 + \alpha_2 + \alpha_3) \\ a_1 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ a_0 &= -\alpha_1\alpha_2\alpha_3 \end{aligned}$$

which are all symmetric. We want expressions for $\alpha_1, \alpha_2, \alpha_3$. We have to do *a lot* of algebra to produce expressions that are not symmetric but whose powers *are* symmetric; it works out by an apparent miracle. For degree 4, similar, but worse. For degree 5, it just fails.

Galois realized if you are just doing algebra, you are just lookinng at the shape of the equations. Galois realized that the key is understanding possible symmetries and their complexity is the key. These old school math people just did algebra: just computing machines. Galois reallized algebra is not going to get you anywhere: what are the relationships between roots and their symmetries.

Theorem 7 (Galois)**.** *Given $f(x)$, a rational polynomial as above (degree n, then (1) there exists a finite group $G_f \subseteq S_n$ (permutations of roots $\alpha_1, \ldots, \alpha_n$) and (2) there is a formula for the roots $\iff$ G_f is solvable in the sense that we just defined. Furthermore, (3) for most polynomials $G_f = S_n$ (might not be Galois). (4) S_n is not solvable if $n \geq 5$*

That's why we call them solvable groups. They correspond to a solvable polynomial. Galois basically developed group theory to prove this... not with groups like we know, looking mostly at these permutations. Amazing: same age as us, but died shortly after, Nike's goat.

How to define G_f? Idea: Consider polynomials $P(x_1, x_2, \dots, x_n)$ in n-variables (where n is the degree) with rational coefficients. Say that P is a relation between the roots if the following holds: $P(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$ $(x_1 = \alpha_1, x_2 = \alpha_2, \dots, x_n = \alpha_n)$. $P_f =$ all possible P that give relations like this. $G_f =$ set of permutations that preserves all the relations, which *means* $\sigma \in G_f$ if for all(?) $P \in P_f$ we have $P(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \in P_f$.

Then $G_f \neq \{1\}$; Galois proved f is solvable $\iff$ G_f is solvable. What we get is that two polynomials that look quite similar have Galois groups that are quite different. Example (Quanta Article, Aug. 3 2021): $x^3 - 7x + 5$ and $x^3 - 7x + 7$; gives examples of relations that are quite different... one actually has Galois group S_3, and one has a cyclic Galois group. The Galois group is the key, the underlying symmetry.

10.1.1 Proof that S_5 is not solvable

Recall the definition: G is called solvable if there exists subgroups $G = G_1 \subseteq G_2 \subseteq \cdots \subseteq G_r = \{1\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian.

Condition with polynomials: taking a d-th root of a solves $x^d = a$, $x = a^{1/d}$; $f(x) = x^d - a$. These have a Galois group that is (almost) abelian ($\implies$ solvability criterion). Nike was always confused how you go from polynomials to this definition, it lies somewhere in here. (Almost abelian here means if we allow n-th roots of unity, it becomes abelian, but the point is that they are solvable: either abelian already, or abelian after throwing in some roots).

Goal: S_n is not solvable if $n \geq 5$. The only normal subgroup of $S_n, n \geq 5$ are $\{1\}, A_n, S_n$ (and A_n haas no normal subgroups except $\{1\}$).

For $n = 2$ $S_2 = \{1\}, (12)$, and two element groups are obviously solvable: $G_1 = S_2, G_2 = \{1\}$. The solution is via just $\sqrt{(\ )}$. For $n = 3$ $S_3 \supseteq \langle (123) \rangle \supseteq \{1\}$. We have that $G_1/G_2 =$ cyclic or order 2, and G_2/G_3 is cyclic of order 3. Thus this is solvable, and solution via $\sqrt[2]{(\ )}$ and $\sqrt[3]{(\ )}$ (which corresponds to our quotient groups). For $n = 4$, $S_4 \supseteq A_4 \supseteq V = \{e, (12)(34), (13)(24), (14)(32)\} \supseteq \{1\}$. In order, our quotient groups have order 2, order 3, and V is abelian, so it is solvable. The group theory actually gives a very precise way to write down these nonsymmetric expressions: for $n = 3$, we want an expression invariant under cylic permutation of order 3, but not invariant under a transposition (in $\langle (123) \rangle$ vs. in $S_3 \setminus \langle (123) \rangle$). This is very pretty: "it's what got [Nike] interested in math in the first place."

How do we deal with S_n when $n \geq 5$. Recall that G is called simple if it has no normal subgroups other than itself and the $\{1\}$. E.g. $G =$ cyclic, prime order (only abelian example).

Theorem 8 (Also due to Galois). *A_n simple when $n \geq 5$*

Strategy: consider $H \subseteq A_n$, $H \neq \{1\}$, normal. Step 1: show that H contains a 3-cycle (abc). Step 2: using the fact that H is normal, show H contains all 3-cyles. Step 3: show that the 3-cycles generate A_n. Thus, $H = A_n$. The only hard part is the first step (but not terrible).

Will end early for the Holiday, and present proof when we come back.