Math 250A

Fall 2015

8/27

Group Action

A group G acts on a set S:
$G \times S \to S$
$(g, s) \mapsto g \cdot s$
$e \cdot s = s$
$(gg') \cdot s = g \cdot (g' \cdot s)$
Alternatively,
$\phi : G \to Perm(S)$
ϕ is a homomorphism (gives the corresponding properties)
$(\phi(g))(s) = g \cdot s$

Examples of Group Actions

The trivial action:
$G \to Perm(S)$ where $g \mapsto e_{Perm(S)}$
G acting on self by left/right translation, conjugation
G acting on the set of subgroups of G by conjugation:
$g \cdot H = gHg^{-1} = \{ghg^{-1} | h \in H\}$
Normal subgroup $N \trianglelefteq G$
G acting on N, $g \cdot n := gng^{-1} \in N$
$G = S_3$ where S is the set of subgroups of G of order 2.
S = {{1, (1 2)}, {1, (1 3)}, {1, (2 3)}}
recall $\sigma(a_1, a_2, a_3, ...a_k)\sigma^{-1} = (\sigma a_1, \sigma a_2, \sigma a_3, ...\sigma a_k)$
V vector space over a field K
G = GL(V) = group of invertible linear maps $V \to V$
e.g. if $V = K^n$ then G = GL(n, K)
G acts on V (rather simply) by $L \cdot v = L(v)$

Orbits and Stabilizers

Given G acting on S by $G \times S \to S$ there is an obvious relation on S:
 s, s′: $s \sim s' \leftrightarrow \exists g \in G, s' = gs$
 the orbit of s is just the equivalence class of s under this relation
 i.e., $G \cdot s = \{g \cdot s | g \in G\}$
The conjugacy classes of s are the orbits of S under the group action of G by conjugation
 the orbit of s, $O(s) = \{s\} \leftrightarrow s = gsg^{-1} \forall g$
 $\leftrightarrow (\forall g) gs = sg$
 $\leftrightarrow s \in Z(G)$ the center of the group
Example, for $G = S_3$
 the orbit of 1 is $\{1\}$
 the orbit of (1 2) = $\{$(1 2), (1 3), (2 3)$\}$
 the orbit of (1 2 3) = $\{$(1 2 3), (1 3 2)$\}$
Stabilizer (isotropy group) of a given element $s \in S := G_s$
 $G_s = \{g \in G | g \cdot s = s\}$
 stabilizer is closed under inverses: $g \in G_s \to g \cdot s = s \to g^{-1} gs = g^{-1} s \to s = g^{-1} s$

large stabilizer$\leftrightarrow$ small orbit

there exists a natural bijection $\alpha : G/G_s \to O(s)$ defined $gG_s \mapsto g \cdot s$
well-definition:
 if $g_1 G_s = g_2 G_s$ then $\exists g \in G_s, g_1 = g_2 g$ and $\alpha(g_1 G_s) = g_1 \cdot s = g_2 gs = g_2 s = \alpha(g_2 G_s)$
injectivity:
 if $\alpha(g_1 G_s) = g_1 \cdot s = g_2 \cdot s = \alpha(g_2 G_s)$ then $g_2^{-1} g_1 \cdot s = s$, $g_2^{-1} g_1 \in G_s$ and $g_1 G_s = g_2 G_s$

Lang 1.1-1.4

1.1: Monoids

A *monoid* is a set with associative binary operation and unit element.
 Abelian $\leftrightarrow$ commutative
A *submonoid* is a subset of a monoid with identity and closure under the operation
 Such a submonoid is, itself, a monoid

1.2: Groups

A *group* is a monoid with inverses for each element
The *permutation group* of S is the set of all bijections $S \to S$ (with composition as product)
A direct product of groups has product defined componentwise
A *subgroup* of a group is a subset closed under composition and inverse
$S \subset G$ *generates* G if $\forall g \in G, g = \prod s_i$, where $s_i \in S$ or $s_i^{-1} \in S$
 $G = \langle S \rangle$
The *group of symmetries of the square* is a non-abelian group of order 8

generated by σ, τ such that $\sigma^4 = \tau^2 = e$ and $\tau\sigma\tau^{-1} = \sigma^3$

The *quaternions* are a non-abelian group of order 8

generated by i, j where defining $k = ij$, $m = i^2$

$i^4 = j^4 = k^4 = e$, $i^2 = j^2 = k^2 = m$, and $ij = mji$

A *monoid-homomorphism* $f : G \to G'$ satisfies $f(xy) = f(x)f(y)$ and $f(e_G) = e_{G'}$

If G and G′ are groups, f is a group homomorphism ($f(x^{-1}) = f(x)^{-1}$ is implied)

An *isomorphism* is a bijective homomorphism.

An *automorphism* or *endomorphism* of G is an isomorphism $\varphi : G \to G$

The group *Aut(G)* is the set of all automorphisms of G

The *kernel* of a homomorphism $f : G \to G'$ is $\{g \in G : f(g) = e_{G'}\}$

the kernel and the image f are subgroups of their respective groups

An *embedding* is a homomorphism $f : G \to G'$ where $G \cong Im(f)$.

Fact: A homomorphism with trivial kernel is injective.

Forward is obvious.

Supposing trivial kernel: $f(x) = f(y) \leftrightarrow f(x)[f(y)]^{-1} = e \leftrightarrow f(xy^{-1}) = e \leftrightarrow xy^{-1} = e$

For G a group, and $H,K \leq G$ such that $H \cap K = e$, $HK = G$, and $xy = yx\ \forall x \in H\ \forall y \in K$

The map $H \times K \to G$ defined $(x,y) \mapsto xy$ is an isomorphism

This generalizes to finitely many such subgroups by induction

A *left coset* of H in G ($H \leq G$) is $aH = \{ax : x \in H\} \leq G$

$x \mapsto ax$ gives bijection between cosets of H, are all of equal cardinality

The *index* of H in G (G : H) is the number of cosets of H in G (right or left)

The *order* of G is the index (G : 1) of its trivial subgroup

For any subgroup H of G, G is the disjoint union of its cosets in H

For $H \leq G$, $(G : H)(H : 1) = (G : 1)$, holding if at least two are finite

If (G : 1) is finite, the order of H divides the order of G.

Given:

$H,K \leq G$, $K \subset H$

$\{x_i\}$ a set of coset representatives of K in H

$\{y_i\}$ a set of coset representatives of H in G

Then:

$\{y_j x_i\}$ is a set of coset representatives of K in G.

Therefore the above can be generalized to $(G : K) = (G : H)(H : K)$

Conclusion: groups of prime order are cyclic.

$J_n = \{1,...,n\}$, $S_n = Perm(J_n)$

$\tau \in s_n$ is a *transposition* if $\exists r \neq s \in J_n$, $\tau(r) = s$, $\tau(s) = r$, $\tau(k) = k\ \forall k \neq r,s$

The set of transpositions generate S_n

Consider $H \leq S_n$ those which leave n fixed. Then $H \cong S_{n-1}$.

Now if $\sigma_i \in S_n$ for $1 \leq i \leq n$ are defined with $\sigma_i(n) = i$, $\{\sigma_i\}$ are coset reps for H

Hence $(S_n : 1) = n(H : 1) = n!$.

1.3: Normal subgroups

For H the kernel of $f : G \to G'$ a group-homomorphism, $xH = f^{-1}(f(x)) = Hx$

Such a relation is equivalent to e.g. $xH \subset Hx$ and $H \subset xHx^{-1}$

A subgroup $H \trianglelefteq G$ (satisfying $xHx^{-1} = H \; \forall x \in G$) is termed *normal*
H is normal $\leftrightarrow$ H is the kernel of some homomorphism
The *factor group* of G by $H \trianglelefteq G$ is the group of cosets, denoted G/H
$f : G \to G/H$ defined $x \mapsto xH$ is the canonical map for H
The *normalizer* N_S of $S \subset G$ is $\{x \in G | xSx^{-1} = S\}$
The normalizer of H is the largest subgroup of G in which H is normal
The *centralizer* Z_S of S is $\{x \in G | xyx^{-1} = y \; \forall y \in S\}$
The centralizer of G is called its *center*; its elements commute with all others in G
The *special linear group* is the kernel of the determinant (a homomorphism)
G is the *semidirect product* of N and H if $G = NH$ and $H \cap N = \{e\}$
An *exact* sequence $G' \xrightarrow{f} G \xrightarrow{g} G''$ satisfies $Im(f) = Ker(g)$.
Can extend to larger sequences as long as each triple satisfies the above
Some canonical homomorphisms, given $f : G \to G'$
$H = ker(f) \to \exists! f' : G/H \to G'$ injective $\to \exists \lambda : G/H \to Im(f)$ an isomorphism
$H \leq G$, N the minimal $N \trianglelefteq G$ s.t. $H \leq N$, $H \subset ker(f)$, then $N \subset ker(f)$, $\exists! f' : G/N \to G'$
$H, K \trianglelefteq G$, $K \subset H$, then $K \trianglelefteq H \to (G/K)/(H/K) \cong G/H$
$H, K \leq G$, $H \subset N_K \to H \cap K \trianglelefteq H$, $HK = KH \leq G$, $\to H/(H \cap K) \cong HK/K$
$H' \trianglelefteq G'$, $H = f^{-1}(H') \to H \trianglelefteq G \to \overline{f} : G/H \to G'/H'$ injective
A *tower* of subgroups of G is a sequence $G = G_0 \supseteq G_1 \supseteq G_2 ... \supseteq G_m$
Such a tower is normal if each $G_{i+1} \trianglelefteq G_i$ and abelian if each factor group is abelian
The preimage of a normal tower under a homomorphism is itself a normal tower
And similarly with the preimage of an abelian tower
Inserting finitely many subgroups into a tower yields a *refinement* of that tower
A *solvable* group has an abelian tower with $G_m = \{e\}$
An abelian tower of finite G admits a cyclic refinement.
$H \trianglelefteq G \to$ G is solvable $\leftrightarrow$ H and G/H are solvable
A *commutator* in G is an element of the form $xyx^{-1}y^{-1}$
The *commutator subgroup* of G is the subgroup generated by its commutators
A *simple* group is a non-trivial group whose only normal subgroups are {e} and itself
An abelian group G is simple $\leftrightarrow$ G is cyclic and of prime order
$U, V \leq G$, $u \trianglelefteq U$, $v \trianglelefteq V$, then we have the following:
$u(U \cap v \trianglelefteq u(U \cap V)$ and $(u \cap V)v \trianglelefteq (U \cap V)v$ with isomorphic factor groups, that is,
$u(U \cap V)/u(U \cap v) \cong (U \cap v)v/(u \cap V)v$
Two towers $G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r$, $G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_s$ are *equivalent* if:
$r = s$ and $\exists i \mapsto i'$ such that $G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$
Theorem (Schreier): Given a group G and two towers of that group.
If they are normal and end with the trivial group they have equivalent refinements
$G = G_1 \supseteq G_2 \supseteq \cdots \subseteq G_r = \{e\}$ normal, each G_i/G_{i+1} simple, $G_i \neq G_{i+1}$ for $1 \leq i \leq r-1$
Then any normal tower of G with these properties is equivalent to this tower.

1.4: Cyclic groups

A group G is *cyclic* if $\exists a \in G$ such that $\forall x \in G$, $x = a^n$ for some $n \in \mathbb{Z}$
Such an a is the *generator* of G.

If $a^m = e$ and $m > 0$ m is an *exponent* of a.

Such is an *exponent of* G if it is an exponent of a $\forall a \in G$.

Let G be a group, $a \in G$, $f : \mathbb{Z} \to G$ defined $f(n) = a^n$ and $H = ker(f)$

If the kernel is trivial, a has *infinite period* and generates an infinite cyclic subgroup

With a nontrivial kernel, its *period* d is the smallest positive element of the kernel

G a finite group, order > 1, $a \in G$, $a \neq e$, then the period of a divides n.

G cyclic: every subgroup of G is cyclic, and for f a homomorphism on G, $Im(f)$ is cyclic

Proposition:

(i) An infinite cyclic group has exactly two generators (if a is one, a^-1 is the other)

(ii) G finite cyclic of order n, x a generator; the set of generators is $\{x^v | gcd(v, n) = 1\}$

(iii) G cyclic, a and b two generators: $\exists f \in Aut(G)$, $f(a) = b$

(iii) conversely, if $f \in Aut(G)$, $f(a)$ is some generator of G

(iv) G cyclic of order n, d positive divisor of n $\to \exists! H \leq G$, $\#H = d$

(v) G_1, G_2 cyclic, $\#G_1 = m$, $\#G_2 = n$. If $gcd(m, n) = 1$, then $G_1 \times G_2$ is cyclic.

(vi) G finite abelian, noncyclic $\to \exists p$ prime and $H \leq G$, $H \cong C \times C$, C cyclic of order p

Lang 1.5-1.6

1.5: Operations of a group on a set

An *action/operation* of G on S is $\pi : G \to Perm(S)$ and S is called a G-set

Written with a product notation, this has properties $x(ys) = (xy)s$ and $es = s$

Conjugation has inverse, so action yields a homomorphism $G \to Aut(G)$

Its kernel is the *center* of G.

Elements of its image are called *inner automorphisms*.

Subsets A and B are conjugate if for some $x \in G$, $B = xAx^{-1}$

Another example of an action is left-translation.

Note that the image in $Perm(S)$ under this action does not consist of homomorphisms.

Given two G-sets and f between them, if $f(xs) = xf(s)$ then f is a *morphism* of G-sets

The $x \in G$ such that $xs = s$ for a given s is the *isotropy group* or *stabilizer* of s

This forms a subgroup of G.

9/1

Group Actions $\rightarrow$ Sylow theorems

Recall:
  the stabilizer $G_s = \{g \in G | g \cdot s = s\}$
  the orbit $O(s) = \{g \cdot s | g \in G\}$
  $G/G_s \cong O(s)$ and $\#(G/G_s) = \#O(s)$
Let $\Sigma =$ set of representatives for $s \sim s' \leftrightarrow O(s) = O(s')$
  $\#S = \sum_{s \in \Sigma} \#O(s) = \sum_s (G : G_s)$
  G finite $(G : G_s) = \frac{\#G}{\#G_s}$
  Mass formula $\#S = (\sum_s \frac{1}{\#(G_s)})(\#G)$
A subgroup H of G acted upon by G has orbits, cosets, and trivial stabilizer.
  Hence from the above $\#H_s = \#H$, and $\#G = (G : H) \cdot \#H$.
  This is a statement of Lagrange's Theorem, $(G : H) = \frac{\#G}{\#H}$.
We can relate the stabilizers of points in the same orbit.
  $G_s' = G_{g \cdot s} = gG_sg^{-1}$
  See $(gxg^{-1})s' = (gxg^{-1})gs = g(xs)$
  The stabilizer of s' is a conjugate of the stabilizer of s.
The kernel of the action

$$K = \{g \in \bigcap_{s \in S} G_s\}$$

  This is just the kernel of $G \xrightarrow{\phi} Perm(S)$.
Assume $x \in G_s$. Claim $gxg^{-1} \in G_{gs}$, showing $gG_sg^{-1} \subset G_{gs}$
  Since $x \in G_s$, $(gxg^{-1})s' = (gxg^{-1})gs = g(xs) = gs$.
  Applying this relation with $g \rightarrow g^{-1}$ and $s \rightarrow gs$, $G_{gs} \subset gG_sg^{-1}$

Applications

p : prime
p-group: a finite group G, $\#G = p^n, n \geq 1$
"A p-group has a non-trivial center."
  (Recall: the center $Z(G) = Z = \{g \in G | gs = sg \forall s \in G\}$).
  Since $gs = sg \rightarrow s = gsg^{-1}$, will be useful to consider action on self by conjugation.
  G a p-group, S a finite set. Then $\#O(s) = \frac{\#G}{\#G_s} = \frac{p^n}{p^k}$.
  Two cases: 1) $\#O(s) = 1$ s is fixed by G, $s \in S^G$ (set of fixed points of S)
  2) $(k < n)$, thus $\#O(s)$ is divisible by p.
  $\#S =$ sum of # of elements in the orbits $\equiv_{mod p}$ # of orbits of size $1 = \#(S^G)$.
  Take S = G, with action $g : s \mapsto gsg^{-1}$. Then $S^G = Z(G)$.
  Thus, $\#Z(G) \equiv_{mod p} p^n \equiv_{mod p} 0$. Center has order divisible by p.
$H \leq G$ a finite group, $(G : H) = p$, p the smallest prime dividing #G $\rightarrow H \trianglelefteq G$
  Let $S = G/H$; $\#(S) = (G : H) = p$, and let G act on S by left translation.
  This induces $\varphi : G \rightarrow S_P$; recall $\#S_p = p!$

The stabillizer of H, $G_H = \{x \in G | xH = H\} = H$.
By inspection, we can see that $G_{gH} = gHg^{-1}$.
Let $K = \bigcap_{g \in G} gHg^{-1}$, the largest normal subgroup contained in H.
Note that $K = ker(\varphi)$ induced above; by the First Isomorphism Theorem $\varphi(G) \leq S_p$.
$(G:K) = \#(G/K) = \#(\varphi(G))$, which divides $\#(S_p) = p!$
Further, since $K \leq H \leq G$, $(G:K) = (G:H)(H:K)$.
Since $(G:K)$ divides $p!$ and $(G:H)$ divides p, $(H:K)$ divides $(p-1)!$.
But p is the smallest prime dividing $\#G$, so $(H:K)$ = 1, $K = H$ and H is normal.

A familiar embedding of a group into a larger group; "Cauchy's Theorem"
$G \hookrightarrow Perm(G)$ by letting G act on itself by left-translation.
Its kernel $K = \{g \in G | gs = s \forall s\} = \{e\}$ (consider $s = e$), hence is an injection.
Since an injection, an embedding.

Recall $S_n \subset$ group of $n \times n$ invertible matrices. $\sigma \mapsto M(\sigma)$ a permutation matrix.
Need to be careful in the construction to ensure $M(\sigma\tau) = M(\sigma)M(\tau)$!
E.g. $\sigma = (132)$ does $M(\sigma)$ have 1 in the 1st column, 3rd row?
Or in the 1st row, 3rd column? One of these yields $M(\sigma\tau) = M(\tau)M(\sigma)$.

G finite of order n; V the vector space of functions $G \xrightarrow{f} \mathbb{Z}$; note $V \cong \mathbb{Z}^n$
Linear maps $V \to V \leftrightarrow n \times n$ matrices over $\mathbb{Z}$; this is $GL(V) \approx GL(n, \mathbb{Z})$.
Similarly, invertible linear maps correspond to $n \times n$ invertible matrices over $\mathbb{Z}$.
We can embed G in $GL(n, \mathbb{Z})$ by using a left action of G on $GL(n, \mathbb{Z}) = \{\phi : V \to V\}$
Recall that $V = \{f : G \to \mathbb{Z}\}$.
This left action takes the form $L_g : f(x) \mapsto f(xg)$
Verify for yourself that $L_{gg'} = L_g \circ L_{g'}$ and $g \mapsto L_g$ is a homomorphism $G \to GL(V)$
Using $\mathbb{F}_p$ instead of $\mathbb{Z}$, get $G \hookrightarrow GL(n, \mathbb{F}_p)$, an embedding into a finite group

9/3

Sylow Theorems

Lagrange: If $H \leq G$ then $\#(H) | \#(G)$.
A_4 with $n = 6$ gives the counterexample to the converse.
Salvaging the converse: the case where $n = p^k$, p prime.
(Sylow I): If $|G| = p^k \cdot r$, $(p, r) = 1$
$\exists H \leq G$ such that $|H| = p^k$
Such an H is called a p-Sylow (Sylow-p) subgroup of G
Generally assuming $k \neq 0$
Example : $\mathbb{Z}_{12}$
has 2-sylow subgroup $\{0, 3, 6, 9\}$ and 3-sylow subgroup $\{0, 4, 8\}$
Example: D_6 generated by r, s subject to $rs = sr^{-1}$, $r^6 = e$, $s^2 = e$, has order 12
$\#(D_6) = 12$ so has 3-sylow subgroup $\{1, r^2, r^4\}$
Also has 2-sylow subgroups $\{1, r^3, s, r^3s\}$, $\{1, r^3, rs, r^4s\}$, $\{1, r^3, r^2s, r^5s\}$
Example: G = $GL_n(\mathbb{F}_p)$, $n \times n$ linear transformations in $\mathbb{F}_p$, equal to $Aut(\mathbb{F}_p^n)$
The order of $|G|$:

Asserting linear independence in each vector of an $n \times n$ matrix

$|G| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}) = p^{1+2+3+\cdots+n-1} \cdot r = p^{\frac{n^2-n}{2}} \cdot r$

$(p,r) = 1$

Consider P the set of all lower triangular matrices in $n \times n$.

Then $|P| = p^{1+2+3+\cdots+n-1} = p^{\frac{n^2-n}{2}}$, and P is a Sylow subgroup.

Theorem: (Sylow I) p-Sylow subgroups always exist.

Proof Sketch:

Suppose $|H| = p^k \cdot r$, $(p,r) = 1, k > 0$

Show $\exists G$, $H \leq G$, where G has a p-Sylow subgroup.

Show that if G has a p-Sylow subgroup and $H \leq G$, then H has a p-Sylow subgroup

Proof:

By Cayley's theorem, if $|H| = n$, then $H \leq S_n$.

(H acts on itself by left translates. This yields an embedding into S_n.)

Additionally $S_n \leq GL_n(\mathbb{F}_p)$ mapping to permutation matrices.

We know that $GL_n(\mathbb{F}_p)$ has p-Sylow subgroups.

Let P be a p-Sylow subgroup of G. Consider G acting on the set of cosets of P.

Now, $Stab(gP) = gPg^{-1}$.

Similarly, letting H act on G/P, $Stab(gP) = (gPg^{-1} \cap H)$

This intersection is a p-group.

Want to choose $g \in G$ such that $gpg^{-1} \cap H$ is a p-Sylow subgroup.

If $(H : (gPg^{-1} \cap H))$ is coprime to p, then $gPg^{-1} \cap H$ is a p-Sylow subgroup.

By Orbit-Stabilizer, $(H : (gPg^{-1} \cap H)) = O(gP)$.

$|G/P| \not\equiv 0$ (mod p), and the sum of the orbits is $|G/P|$

Hence there must be some orbit with size coprime to p.

Corollary of proof, using fact that these have the form $gPg^{-1} \cap H$.

Statement of the corollary: (Sylow II) All p-Sylow groups are conjugate.

Proof:

Let $H \leq G$, $P \leq G$ p-Sylows. Then $H \cap gPg^{-1}$ is a p-Sylow of H for some $g \in G$.

Since H is a p-group $H \cap gPg^{-1} = H$ i.e. $H \subset gPg^{-1}$. **I don't know why this is true.**

Then $|H| = |P| = |gPg^{-1}|$, so $H \cap gPg^{-1} = H$.

Corollary of Proof of Sylow I:

If $|G| = p^k \cdot r$, then $\exists H_i \subset G$ such that $|H_i| = p^i$, for $0 \leq i \leq k$.

Proof left to student: not sure what it is.

Let $Syl_p(G)$ describe the p-Sylow subgroups of G and n_p denote its cardinality.

Theorem (Sylow III) If $|G| = p^k \cdot r$, $k > 0$ then $n_p \equiv 1(p)$ $n_p | r$.

Lemma: If Γ acts on X, X a set, Γ a p-group (finite)

Then $\#X \equiv \#Fix_\Gamma(X)(mod p)$, where $Fix_\Gamma(X)$ is the set of elements of x fixed by all of Γ

Proof:

$\#X = \sum_i \#Orb(x_i) = \sum_i \frac{|\Gamma|}{|Stab(x_i)|} \equiv \#Fix_\Gamma(X)(mod p)$

Each $\frac{|\Gamma|}{|Stab(x_i)|} = 1$ if x_i fixed, else 0

Proof of the Theorem:

Let $Syl_p(G)$ act on itself by conjugation.

By the lemma, $\#Syl_p(G) = n_p \equiv Fix_p(Syl_p(G))(mod p)$.

Suppose Q is fixed. Then $pQp^{-1} = Q \; \forall p \in P$.
Then $P \leq N(Q)$; similarly $Q \leq N(Q)$.
P, Q are p-Sylow subgroups of N(Q); therefore P, Q are conjugate in N(Q).
However, $Q \trianglelefteq N(Q)$ so that $P = Q$.
Further, P is the only such Sylow-p subgroup that works so $Fix_p(Syl_p(G)) = 1(modp)$
G acting on $Syl_p(G)$ as only one orbit since all p-Sylows in G are conjugate.
Stab. $n_p = |G| = p^k \cdot r$, $n_p | p^k \cdot r$, but $n_p \nmid r$, so $n_p | r$.

9/8

Review of Sylow Theorems

Prove existence by showing existence in a larger known subgroup.
And then that contained subgroups must have their own Sylow p-subgroups.
$O(s) = S = \{\text{p-Sylows}\}$
$O(s) = G/G_s = G/N(P)$
The number of p-Sylows is notated $n_p = (G : N(P))$
P, Q p-Sylows and $P \subset N(Q)$ then $P = Q$
reason: $PQ \leq G$ a subgroup of G
HK not necessarily a group, but will be if one normalizes the other
ie $H \subset N(K)$
Theorem $n_p \equiv 1$ (mod p)
Consider the action of P on S by conjugation
Take $x \in P$ and $x : Q \mapsto xQx^{-1}$
The number of fixed points is 1, since P fixes only itself
A simple group has
more than one element
no non-trivial proper normal subgroups
(kind of like a prime number)
G finite abelian
G simple $\leftrightarrow$ G cyclic of prime order (simple easy exercise)

continuing...

non-sporadic finite simple groups
$A_n (n \leq 5)$
recall the alternating groups A_n are the even permutations on $\{1, \cdots, n\}$
Lie groups over finite fields, e.g. $\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} \subset SL(2, \mathbb{Z}|p\mathbb{Z})$
P = projective; $PSL(2, \mathbb{Z}|p\mathbb{Z}) = SL(2, \mathbb{Z}|p\mathbb{Z})$
Simple groups of order ≤ 60.
(a) There are none of order < 60 (HW)
(b) If G is simple of order 60, then $G \cong A_5$.
($\# A_n = \frac{n!}{2}$)

G simple of order 60.

$H < G$ simple (finite), H proper, $(G : H) = n \geq 2$

G acts on G/H by left translation.

The action is transitive (for each pair xH, yH, $\exists$ permutation taking one to the other)

Therefore, this action is non-trivial.

$\pi : G \to Perm(G/H) = S_n$

$ker(\pi) \neq G$ and is a normal subgroup $\to$ the kernel is trivial.

$\pi : G \hookrightarrow S_n$ and in fact $\pi : G \hookrightarrow A_n$ (if $\#G > 2$)

Why? because $G \cap A_n \trianglelefteq G$

If $G \subset S_n$.

Then $G \to S_n/A_n = \{\pm 1\}$ by the sign map, kernel is $G \cap A_n$.

Recall $sgn : S_n \to \{\pm 1\}$ $sgn(\sigma) = (-1)^t$ given t, num of transpositions

$G/(G \cap A_n) \hookrightarrow S_n/A_n = \{\pm 1\}$

$(G : G \cap A_n) = 1$ or 2.

If G is simple then this cannot be 2 (would be normal subgroup), so =1.

And $G \hookrightarrow A_n$ for that A_n.

G simple, order 60.

H a proper subgroup of G, index n. (consider small values of n)

If $n = 2$ then H is normal in G, a contradiction.

(smallest prime dividing the order of a group)

If $n = 3$ or $n = 4$: $G \hookrightarrow A_3, A_4$ but their orders are too small (3, 12)

If $n = 5$: $G \hookrightarrow A_5$ and they are equal in cardinality $\to$ done.

Remaining case: $n = 15$.

What is n_5, the number of 5-Sylow subgroups.

$n_5 | 60/5 = 12$, $n_5 = (G : N(P))$ n_5 divides the index

Also, $n_5 \equiv 1 \pmod 5$.

Thus $n_5 = 1$ or $n_5 = 6$.

If $n_5 = 1$ then only one 5-Sylow subgroup of G, must be normal.

This is impossible since G is simple.

Then $n_5 = 6$: tells you there are lots of elements of order 5 in G.

There is no overlap (excepting at the identity) between 5-Sylows.

Hence the number of elements of order 5 is $6 \cdot 4 = 24$

Elements of order 5 in A_5 are 5-cycles (a b c d e).

Need to take all strings of length 5: 120, and divide out by rotations 5.

Thus we get $120/5 = 24$ (check).

Consider n_2 the number of 2-Sylow subgroups.

Then n_2 divides $60/4 = 15$, and $n_2 \neq 1$ because of simplicity.

Also, $n_2 = (G : N(P_2))$, and this can't be 3 since G has no subgroup of index 3.

If $n_2 = 5$ then $N(P_2)$ is the desired index-5 subgroup $\to$ done.

From divisibility $n_2 = 1, 3, 5, 15$.

Elminate 1 by simplicity, 3 since the index is too small, 5 works, consider 15.

Considering the situation where there are 15 2-Sylow subgroups (of order 4).

These are groups like the Klein 4-group (no elements of order 4).

There are 2 2-Sylow subgroups P and Q where $P \cap Q$ has order 2.

Prove by counting.

Taking intersection, must be proper else they would be the same.
Hence $P \cap Q$ has order 1 or 2.
If there is utterly no overlap, there are $15 \cdot 3 + 1 = 46$ elt's of 2-Sylows.
And these do not have order 5. But there are 24 elements of order 5. Too many.
Now we know that some of these 2-Sylow subgroups have non-trivial overlap.
Consider $N(P \cap Q)$ for some such intersection, will be a subgroup of G.
Cannot be all of G, G is simple.
Moreover, $P, Q \leq N(P \cap Q)$. Now, $N(P \cap Q)$ cannot contain P or Q.
Therefore, its index cannot be 1 (G is simple) cannot be 3, A_n too small, = 5.
Jordan-Hölder theorem
Website reference.
G finite non-trivial. Is G simple? $\{e\} \subset G$, $G/\{e\}$ simple.
Not simple $G \supset G_1 \supset (e)$, $G_1 \trianglelefteq G$, G_1, G/G_1 smaller than G.
Keep going until 'end', using principle of string induction.c
Proposition: $\exists G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n$, $G_{i+1} \trianglelefteq G_i$, G_i/G_{i+1} simple.
A *normal tower* or *composition series*, the simple quotients are the *constituents*.
Obtain a successive extension of simple groups.
Main point.
$N = p_1 \cdots p_n$
$\{p_1, p_2, \cdots, p_n\}$ a set where order doesn't count but multiplicity does.
Gauss's theorem: (FTA) each prime decomposition of N yields the same set.
Similarly, given G and $G_i/G_{i+1} = Q_i$ and $\{Q_0, \cdots, Q_{n-1}\}$.
Order not mattering, multiplicity matters, up to isomorphism.
Theorem: Each composition yields the same multiset.
Theorem of "Camille Jordan and some guy named Hölder."

9/10