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 $\alpha(g_1 G_s) = g_1 \cdot s = g_2 g s = g_2 s = \alpha(g_2 G_s)$

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 $g_1 G_s = g_2 G_s$

9/1

Group Actions $\to$ 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, $(G : H) = \frac{\#G}{\#H}$.

The kernel of the action

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

This is just the kernel of $G \xrightarrow{\phi} Perm(S)$.
We can relate the stabilizers of points in the same orbit.
Let $s' = gs$.
Assume $x \in G_s$.
Since $x \in G_s$, $(gxg^{-1})gs = g(xs) = gs$.
Hence $gxg^{-1} \in G_{gs}$, so $gG_sg^{-1} \subset G_{gs}$.
Apply this relation with $g \to g^{-1}$ and $s \to gs$:
Assume $x \in G_{gs}$.
Then $(g^{-1}xg)(s) = (g^{-1})(xgs) = (g^{-1}gs) = s$.
So $g^{-1}G_{gs}g \subset G_s \to G_{gs} \subset gG_sg^{-1}$
Thus, $gG_sg^{-1} = G_{gs} = G_{s'}$.
The stabilizer of $s' = gs$ is a conjugate of the stabilizer of s.

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 $gs = sg \to s = gsg^{-1}$, 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 $S^G = Z(G)$.
$\#Z(G) \equiv_{mod p} \#(S^G) \equiv_{mod p} \#S = \#G = p^n \equiv_{mod p} 0$.
Thus, the order of the center is divisible by p, and must be non-trivial.

$H \leq G$ a finite group, $(G : H) = p$, the smallest prime dividing #G $\to H \trianglelefteq G$
Let $S = G/H$; $\#(S) = (G : H) = p$, and let G act on S by left translation.
This induces $\varphi : G \to S_P$; 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 $V \to V$ correspond to $n \times n$ matrices over $\mathbb{Z}$: $GL(V) \approx GL(n, \mathbb{Z})$.
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 $L_g \mapsto \phi$ where $\phi(f(x)) = f(xg)$
$L_{gg'} = L_{g'} \circ L_g$ as desired? Verify for yourself.
Check this over.
$L_{gg'}(\varphi(x)) = \varphi(xgg') = L_{g'}(\varphi(xg)) = L_{g'} \circ L_g(\varphi(x))$
$g \mapsto L_g$ 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 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 $\{1, r^3, s, r^3 s\}$, $\{1, r^3, rs, r^4 s\}$, $\{1, r^3, r^2 s, r^5 s\}$
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 $n \times n$ upper triangular matrices with 1's on the diagonal.
Then $|P| = p^{1+2+3+\cdots+n-1} = p^{\frac{n^2-n}{2}}$, and P is a p-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.

Alternatively, consider $V \cong \mathbb{F}_p^n$, the vector space of functions $\varphi : G \to \mathbb{F}_p$.

Embed H into $GL(V)$ by this action: $g \in H \mapsto$ automorphism taking $\varphi(x)$ to $\varphi(xg)$.

(Recall end of previous lecture).

We know that $GL_n(\mathbb{F}_p)$ has p-Sylow subgroups. (from the lower triangular matrices)

Let $G = GL_n(\mathbb{F}_p)$.

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

Now, $Stab(gP) = gPg^{-1}$. (guest lecturer notation for stabilizer)

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

Note this is an orbit of G/P induced by the action of the group H.

Since P is a p-Sylow subgroup of G, $|G/P| \not\equiv_{modp} 0$.

The sum of the orbits is $|G/P|$.

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

Corollary: All p-subgroups of H are contained in a conjugate of P.

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

So since J is a p-group $J \cap gPg^{-1} = J$, i.e. $J \subset gPg^{-1}$.

(since a p-group can't contain a proper p-Sylow subgroup by definition)

Corollary: (Sylow II) All p-Sylow groups are conjugate.

Proof:

Let $H \leq G$ and $P \leq G$ be p-Sylow subgroups.

By the preceding corollary, $H \subset gPg^{-1}$ for some $g \in G$.

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

Corollary: Every p-subgroup of G is contained in a p-Sylow of G.

By the above, each is contained in a conjugate of P, said conjugate being a p-Sylow.

The p-Sylow subgroups in G are all conjugate, so that:

If P is a p-Sylow of G then $G/N(P)$ is the set of p-Sylows in G.

Where $N(P)$ is the normalizer of P.

So there are $(G : N(P))$ p-Sylows in total.

Lemma: If a finite p-group Γ acts on a set X, then $\#(X) \equiv_{modp} \#(X^\Gamma)$
(X^Γ the fixed points of X under Γ).
Proof:
$\#X = \sum_i \#Orb(x_i) = \sum_i \frac{|\Gamma|}{|Stab(x_i)|} \equiv_{modp} \#X^\Gamma$
Each $\frac{|\Gamma|}{|Stab(x_i)|} \equiv_{modp} 1$ if x_i fixed, else $\frac{|\Gamma|}{|Stab(x_i)|} \equiv_{modp} 0$.

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 $n_p \equiv_{modp} 1$. Further, $n_p | r$.
Proof:
Let P act on $Syl_p(G)$ by conjugation.
By the lemma, $\#Syl_p(G) = n_p \equiv_{modp} (Syl_p(G))^P$.
Suppose Q is fixed under the group action. 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 Q is equal to all its conjugates in N(Q), and $P = Q$.
Hence P is the only fixed Sylow-p subgroup so $(Syl_P(G))^P \equiv_{modp} 1$.
G acts on $Syl_p(G)$ as only one orbit since all p-Sylows in G are conjugate.
$(G : P) = n_p$, $n_p = |G| = p^k \cdot r$, $n_p | p^k \cdot r$, but $n_p \nmid p$, 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 $n_p \equiv_{modp} 1$
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 no non-abelian simple groups of order < 60

(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, $n_5 \equiv_{mod 5} 1$.

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. (would make $P \cap Q$ normal)
$N(P \cap Q)$ contains P and Q since both are abelian.
Each are normal subgroups of $N(P \cap Q)$, so its order is divisible by 4.
Hence could have order 12, 20, or 60 (divisible by 4, divides 60).
Its index cannot be 1 (G is simple) cannot be 3 (A_n too small), = 5.
QED (**revisit why**).

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

Jordan-Hölder Theorem.

$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n$
    $G_{i+1} \trianglelefteq G_i$, $G_i/G_{i+1} = Q_i$ simple.
Statement of the theorem:
    The "set" (multiplicity matters) $\{Q_0, \cdots, Q_{n-1}\}$ is independent of the filtration.
    Order doesn't count, Q_i up to isomorphism.
Proof strategy: by induction.
    If G has a filtration with n quotients, then all filtrations have n quotients.
    And all filters have the same set of quotients.
Question, can two different groups have the same reduction?
    Answer: yes. $S_3 \supset A_3 \supset \{e\}$. Quotients $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.
    Also $\mathbb{Z}/6\mathbb{Z} \supset 3\mathbb{Z}/6\mathbb{Z} \supset 6\mathbb{Z}/6\mathbb{Z}$, same quotients but radically different structure.
    "Knowing the building blocks does not confer knowledge of the building".
Demonstrating the existence of such a filtration for a group $G \neq \{e\}$.
    Similar to the proof of prime decompositions.
    If it is simple, then the filtration is $G \supset \{e\}$, done.
    If G is not simple, $G \supset N \supset \{e\}$, and $G/N, N$ smaller than G.
    Strong induction. $\overline{G} = G/N$, then $\overline{G} \supset \overline{G_1} \supset \cdots$ and similarly for $N \supset H_1 \supset \cdots$
    Note there is a correspondence b/t subgroups of G con't N and subgroups of G/N
    $G \supset L \supset N$, $L/N \subset G/N$ and $\pi : G \to G/N$, $\pi^{-1}(K) \subset G$ and $K \subset G/N$.
Base case $n = 1$, $G \supset \{e\}$, $G/\{e\}$ simple and G simple.
Supposing $G \supset G_1 \supset \cdots \supset G_n \supset \{e\} = G_{n+1}$ and $G \supset G_1' \supset \cdots \supset G_m' \supset \{e\} = G_{m+1}'$.
    ? $m = n$, $\{G_i/G_{i+1}\} = \{G_j'/G_{j+1}'\}$ ... If $G_1' = G_1$, then done by induction.
    Assume G_1, G_1' are distinct. Then $G_1 \cap G_1'$ is smaller than G_1 or G_1'.
    Also, $G_1 G_1'$ is a subgroup since its factors are normal by hypothesis.
    Indeed, it is also a normal subgroup since G_1 and G_1' are invariant under conjugation.
    Additionally, $G_1 G_1'$ is of size larger than G_1 and G_1'. Thus it must be equal to G.
    Can map $G_1'/(G_1 \cap G_1') \to G_1 G_1'/G_1$. Kernel is exactly $G_1 \cap G_1'$, hence injection.
    This defines $G_1'/(G_1 \cap G_1') \hookrightarrow G/G_1$. Symmetrically, $G_1/(G_1 \cap G_1') = G/G_1'$.
    Have $G_1 \supset \cdots \supset G_n \supset \{e\} = G_{n+1}$.
    Take $G_1 \supset G_1 \cap G_1' = H \supset H_1 \supset H_2 \supset \cdots \supset H_k \supset \{e\}$, a Jordan-Hölder filtration of G_1.
    Obtained by induction.
    Note $G_1/H = G/G_1'$ is the first quotient of this filtration.
    By induction, these two filtrations have the same length.
    The constituents of G_1 are the constituents of H, with $G_1/H = G/G_1'$ appended.
    Constituents: G/G_1 + constituents of G_1 = G/G_1 + G/G_1' + constituents of H.
    Have $G \supset G_1' \supset H \supset H_1 \supset \cdots \supset H_k = \{e\}$, same length as $G_1' \supset G_2' \supset \cdots \supset G_m' = \{e\}$.
    Have related two different filtrations that have are unrelated, by a common filtration, which depends on the intersection of these two filtrations.

Free Groups

S a set, define the free abelian group on S, $\mathbb{Z}^S = \mathbb{Z}\langle S\rangle = \{\sum_{s\in S} n_s \cdot s | n_s \in \mathbb{Z}\}$.

Where all but finitely many of the n_s are 0.

$S = \{1, \cdots, n\}$, $\mathbb{Z}^S = \mathbb{Z}^n = \{(c_1, \cdots, c_n) | c_i \in \mathbb{Z}\}$

$$\sum_{i=0}^{\infty} n_i x^i = \sum_{i=0}^{\infty} n_i \cdot i \in \mathbb{Z}\langle S\rangle$$

where $n_i = 0$ for $i >> 0$.

"To map $\mathbb{Z}\langle X\rangle$ to A in the world of abelian groups is to map S to A in the world of sets."

$S \to \mathbb{Z}\langle S\rangle$ a set map, $s \in S \mapsto 1 \cdot s$.

Given $f : \mathbb{Z}\langle S\rangle A$ homomorphism.

And in fact, $F : Hom(\mathbb{Z}\langle X\rangle, A) \to Maps(S, A)$, F is a bijection.

These elements of the free abelian group are "formal sums".

That is, an $f : S \to \mathbb{Z}$.

Let $f : \mathbb{Z}\langle S\rangle \to A$, $f(\sum n_s s) = \sum_{s\in S} n_s f(s)$

An abelian group A is free of finite rank if $A \cong \mathbb{Z}^n$ for some $n \geq 0$ ($\mathbb{Z} = \mathbb{Z}\langle \emptyset \rangle = 0$).

Define $rank(A) = n$. If $\mathbb{Z}^m \cong A \cong \mathbb{Z}^n$ then n = m.

Why? Take positive integer > 1, e.g. 2. Then $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}^m/2\mathbb{Z}^m$.

LHS has 2^n elts and RHS has 2^m elts so $n = m$.

A subgroup of a free abelian group of rank n is a free abelian group of rank $\leq n$.

Proof: by induction on n.

$n = 0$: $A = (0) = B$.

$n = 1$: $A = \mathbb{Z} \supset B$. What are the subgroups of $\mathbb{Z}$? $(0), (t) = t\mathbb{Z}, t \geq 1$.

Proof by division algorithm: $\mathbb{Z} \supset B \neq 0$, $t =$smallest positive integer in B.

Division algorithm ensures that all elements are multiples of t.

$B \subset \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z}$.

$\pi : (c_1, \cdots, c_n) \mapsto c_n \in \mathbb{Z}$.

Cases:

(1) $\pi(B) = (0), B \subset \mathbb{Z}^{n-1}$, free of rank $\leq n - 1$

(2) $\pi(B) = t\mathbb{Z}, t \geq 1$

$B \xrightarrow{\pi|_B} t\mathbb{Z} \xrightarrow{surj.} 0$

$ker(\pi)|_B = C$ free of rank $\leq n - 1$.

Choose $b \in B$ such that $\pi(b) = t$.

$C \subset \mathbb{Z}^{n-1} : C = ker(\pi)|_B$, free of rank $\leq n - 1$.

$C = B \cap \mathbb{Z}^{n-1}$

$C \subset B, \mathbb{Z} \cdot b \subset B$

Missing (pf in Lang)

Simple linear algebra.

$a_1, \cdots, a_n \in A$ corresponds to a homomorphism $\mathbb{Z}^n \to A$, $(c_1, \cdots, c_n) \mapsto \sum_{i=1}^n c_i a_i$.

These are linearly independent if f is 1-to-1, and these span/generate A if f is onto.

A is finitely generated if A is spanned by $a_1, \cdots, a_n$ for some $n \geq 0$, $a_i \in A$

A is finitely generated iff A is a quotient of $\mathbb{Z}^n$ for some n.

Corollary: a subgroup of a finitely generated abelian group is again finitely generated.

$\mathbb{Z}^n \xrightarrow{f} A$ finitely generated, have $B \subset A$, $f^{-1}(B) \leq \mathbb{Z}^n$, and $f^{-1}(B) \cong \mathbb{Z}^k$, $k \leq n$.

A finitely generated, torsion-free.

I.e. given $a \in A$ and $n \cdot a = 0$, $n \geq 1$, then $a = 0$.

Statement: A is free and of finite rank.

Proof: Take a finite set of generators S in which take T lin indep and large as possible.

take $T = a_1, \cdots, a_k$ and $S = a_1, \cdots, a_k, \cdots, a_m$

$\sum_1^{k+1} c_k a_k = 0$, $c_{k+1} \neq 0$

$B = span\{a_1, \cdots, a_k\} \cong \mathbb{Z}^k$.

$a_{k+1}, \cdots, a_m$: some multiple lies on B.

$N \geq 1$; $N \cdot A \subset B$.

Th: NA free, $N : A \to NA$ A torsion free.

Multiplication on A by a positive integer is injective.

A is isomorphic to NA by the mutliplication by n, since NA is free, A is free.

9/15