

8/27

A group G acts on a set S :

$$G \times S \rightarrow S$$

$$(g, s) \mapsto g \cdot s$$

$$e \cdot s = s$$

$$(gg') \cdot s = g \cdot (g' \cdot s)$$

Alternatively,

$\phi : G \rightarrow \text{Perm}(S)$ is a homomorphism

$$(\phi(g))(s) = g \cdot s$$

Examples

trivial action: $(\forall g) g \mapsto e_{\text{Perm}(S)}$

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 $N \trianglelefteq G$: all $g \in G$ fix N under conjugation

V vector space over a field K , $\text{GL}(V)$ acts on V by $L \cdot v = L(v)$

The orbit of s , $O(s) := \{g \cdot s | g \in G\}$

constitutes an equivalence relation on S

The stabilizer (isotropy group) of $s \in S$, $G_s := \{g \in G | g \cdot s = s\}$

G_s is closed under inverses: $g \in G_s \rightarrow g \cdot s = s \rightarrow g^{-1}gs = g^{-1}s \rightarrow s = g^{-1}s$

There exists a natural bijection $\alpha : G/G_s \rightarrow O(s)$, $gG_s \mapsto g \cdot s$

well-defined: $g_1G_s = g_2G_s \rightarrow \exists g \in G_s, g_1 = g_2g, \alpha(g_1G_s) = g_1s = g_2gs = g_2s = \alpha(g_2G_s)$

injective: $\alpha(g_1G_s) = g_1 \cdot s = g_2 \cdot s = \alpha(g_2G_s) \rightarrow g_2^{-1}g_1 \cdot s = s, g_2^{-1}g_1 \in G_s$, so $g_1G_s = g_2G_s$

Action under conjugation:

the conjugacy classes of a set are the orbits of the action

$O(g) = \{g\} \leftrightarrow g \in Z(G)$ the center of the group

in a permutation group, $\sigma(a_1, a_2, a_3, \dots, a_k)\sigma^{-1} = (\sigma a_1, \sigma a_2, \sigma a_3, \dots, \sigma a_k)$

9/1

Let Σ be a set of representative elements of the orbits of S .

The index of a subgroup H is $(G : H) = \#(G/H)$

For finite G , $(G : H) = \frac{\#G}{\#H}$ ($g \notin H, \exists$ natural bijection $H \rightarrow gH$ (check text))

$$\#S = \sum_{s \in \Sigma} \#O(s) = \sum_s (G : G_s)$$

defines a 'mass formula' $\#S = (\sum_s \frac{1}{\#(G_s)}) (\#G)$

Let G act on a subgroup H by left translation.

$$\#H_s = \#H \text{ and from the above } \#G = (G : H) \cdot \#H.$$

this is a statement of Lagrange's Theorem, $(G : H) = \frac{\#G}{\#H}$.

The kernel of the action $K = \bigcap_{s \in S} G_s$, which is just the kernel of $G \xrightarrow{\phi} \text{Perm}(S)$.
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 $g \rightarrow g^{-1}$ and $s \rightarrow gs$:

Assume $x \in G_{gs}$.

Then $(g^{-1}xg)(s) = (g^{-1})(xgs) = (g^{-1}gs) = s$.

So $g^{-1}G_{gs}g \subset G_s \rightarrow G_{gs} \subset gG_sg^{-1}$

Thus, $gG_sg^{-1} = G_{gs} = G_{s'}$.

The stabilizer of $s' = gs$ is a conjugate of the stabilizer of s .

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 .

$\#S = \text{sum of } \# \text{ of elements in the orbits} \equiv_{\text{mod } p} \# \text{ of orbits of size } 1 = \#(S^G)$.

Take $S = G$, with action $g : s \mapsto gsg^{-1}$. Then $S^G = Z(G)$.

$\#Z(G) \equiv_{\text{mod } p} \#(S^G) \equiv_{\text{mod } p} \#S = \#G = p^n \equiv_{\text{mod } p} 0$.

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 $\#G \rightarrow H \trianglelefteq G$

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 stabilizer 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”

$G \hookrightarrow \text{Perm}(G)$ 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 $V \rightarrow V$ 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 $GL(n, \mathbb{Z}) = \{\phi : V \rightarrow V\}$

Recall that $V = \{f : G \rightarrow \mathbb{Z}\}$.

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.

$L_{gg'}(\phi(x)) = \phi(xgg') = L_{g'}(\phi(xg)) = L_{g'} \circ L_g(\phi(x))$

$g \mapsto L_g$ is a homomorphism $G \rightarrow GL(V)$

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 $\#(H) \mid \#(G)$.

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 $\{1, r^3, s, r^3s\}$, $\{1, r^3, rs, r^4s\}$, $\{1, r^3, r^2s, r^5s\}$

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 $n \times n$ 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 $\varphi : G \rightarrow \mathbb{F}_p$.

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 , $|G/P| \not\equiv_{\text{mod } p} 0$.

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 $\#(X) \equiv_{\text{mod } p} \#(X^\Gamma)$

(X^Γ the fixed points of X under Γ).

Proof:

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

$$\text{Each } \frac{|\Gamma|}{|Stab(x_i)|} \equiv_{mod p} 1 \text{ if } x_i \text{ fixed, else } \frac{|\Gamma|}{|Stab(x_i)|} \equiv_{mod p} 0.$$

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 $n_p \equiv_{mod p} 1$. Further, $n_p | r$.

Proof:

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

By the lemma, $\#Syl_p(G) = n_p \equiv_{mod p} (\#Syl_p(G))^P$.

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 $(\#Syl_p(G))^P \equiv_{mod p} 1$.

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 $n_p \equiv_{mod p} 1$

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 $\{1, \dots, n\}$

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.

$\pi : G \rightarrow \text{Perm}(G/H) = S_n$

$\ker(\pi) \neq G$ and is a normal subgroup \rightarrow 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 $G \rightarrow S_n/A_n = \{\pm 1\}$ by the sign map, kernel is $G \cap A_n$.

Recall $\text{sgn} : S_n \rightarrow \{\pm 1\}$ $\text{sgn}(\sigma) = (-1)^t$ 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 \rightarrow 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, $n_5 \equiv_{\text{mod } 5} 1$.

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 \rightarrow done.

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

Eliminate 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.

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n$$

$$G_{i+1} \trianglelefteq G_i, G_i/G_{i+1} = Q_i \text{ simple.}$$

Statement of the theorem:

The “set” (multiplicity matters) $\{Q_0, \dots, Q_{n-1}\}$ 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. $\bar{G} = G/N$, then $\bar{G} \supset \bar{G}_1 \supset \cdots$ 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

$$G \supset L \supset N, L/N \subset G/N \text{ and } \pi : G \rightarrow G/N, \pi^{-1}(K) \subset G \text{ and } K \subset G/N.$$

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 $G'_1/(G_1 \cap G'_1) \rightarrow G_1 G'_1/G_1$. 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

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

Where all but finitely many of the n_s are 0.

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

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

where $n_i = 0$ for $i \gg 0$.

“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.”

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

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

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

These elements of the free abelian group are “formal sums”.

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

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

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 $\text{rank}(A) = n$. 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: $\mathbb{Z} \supset B \neq 0$, $t = \text{smallest positive integer in } B$.

Division algorithm ensures that all elements are multiples of t .

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

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

Cases:

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

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

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

$\ker(\pi)|_B = C$ 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.

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

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, \dots, 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 $T = a_1, \dots, a_k$ and $S = a_1, \dots, a_k, \dots, a_m$

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

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

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

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

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

Multiplication on A by a positive integer is injective.

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

9/15

Abelian group, finitely generated.

Last week:

free group has to do with some correspondence to a \mathbb{Z}^n

subgroups of free finitely generated abelian groups are free and finitely generated

subgroups of finitely generated abelian groups are finitely generated

finitely generated, torsion free abelian group is a free abelian group

recall torsion free: for all $n \geq 1$, mult by n, $n \cdot A$ is injective

opposite A torsion: for all $a \in A$, $\exists n \geq 1$ such that $n \times a = 0$

Example of a torsion abelian group: \mathbb{Q}/\mathbb{Z}

element $p/q \mod \mathbb{Z}$, $q \geq 1$, $p \in \mathbb{Z}$; $q \times \frac{p}{q} = 0$ in \mathbb{Q}/\mathbb{Z}

finitely generated abelian groups up to isomorphism

A is a direct sum of a free part \mathbb{Z}^r and a torsion part (a direct sum of cyclic groups)

Direct product of sets A_i indexed by S:

$$\bigoplus_{i \in S} A_i = \{f : S \rightarrow \cup_{i \in S} A_i : f(i) \in A_i\}$$

where for all but finitely many i, $f(i) = 0$

this is equivalent to the direct product when S is finite

Image 1: a map from a $\bigoplus_{i \in S} A_i$ to B is determined by the mappings from the A_i

The direct sum is a coproduct.

Image 2: a map into a $\prod_{i \in S} A_i$ is determined by the mappings into the A_i

The direct product is a product (in the categorical sense).

S countably infinite, $A_i = \mathbb{Z}/2\mathbb{Z}$

$\bigoplus_{i \in S} A_i$ is countable, but $\prod_{i \in S} A_i$ is not

Categories: products, coproducts, morphisms

$\text{Mor}(?, B) = \coprod \text{Mor}(A_i, B) \Rightarrow \text{co-product}$

The coproduct of sets is disjoint union.

Abelian group A and subgroups X and Y

we have inclusions from each into A

$$X \times Y = X \oplus Y \xrightarrow{h} A, (x, y) \mapsto x + y$$

h is injective if every $a \in A$ is of the form $x + y$

h is one-to-one \Leftrightarrow you can't write $x + y = x' + y'$ unless $x = x', y = y'$

If true, say A is the direct sum of its submodules X and Y .

Suppose $A, X \subset A, A/X$ is free (f.g. free): then X has a complement Y in $A, A \cong X \oplus A/X$

$$A \xrightarrow{\pi} A/X$$

$Y \subset A, \pi|_Y$ is an isom $Y \rightarrow A/X$.

$$\pi|_Y \text{ inj} \Leftrightarrow Y \cap X = (0).$$

$\pi|_Y$ surjective: given $a + X \in A/X$ we can find $y \in Y$ s.t. $y + X = a + X$

$$x = y \cdot a \in X$$

$$a = y \cdot x, x \in X, y \in Y$$

A/X free, say $\cong \mathbb{Z}^r$

To map A/X to A is to choose images in A of the generators of A/X corresponding to the unit vectors of \mathbb{Z}^r .

There is a unique homomorphism $s : A/X \rightarrow A$ so that $s(q_i) = a_i$ for $i = 1, \dots, r$

$$(\pi \cdot s)(q_i) = \pi(a_i) = q_i$$

$$\pi \circ s = \text{id}_{A/X}$$

$Y = \text{image of } S \subset A$.

$\pi|_Y$ surjective. $\pi(s(q)) = q$ for all $q \in A/X$

$\pi|_Y$ is 1-1. $\pi(s(q_0)) = 0$ but $s(q_0) = q_0$ so equals 0.

A a finitely generated abelian group

$$X = A_{\text{tors}} = \{a \in A \mid na = 0 \text{ for some } n \geq 1\}.$$

X f.g., tors $\rightarrow X$ finite abelian group.

A/X torsion free, f.g. $\rightarrow A$ free $\approx \mathbb{Z}^r$

$$A \approx \mathbb{Z}^r \oplus A_{\text{tors}}. A_{\text{tors}} = ???$$

it is a finite abelian group, let $B = A_{\text{tors}}$

p prime, $B_p = \{b \in B \mid p^t \cdot b = 0 \text{ for some } t \geq 0\}$.

$$B_p \subset B.$$

$$\bigoplus_p B_p \xrightarrow{\iota} B$$

Proposition: ι is an isomorphism. (formal proof in Lang's book)

Proof essence:

$$\text{suppose } 60 \cdot b = 0, 60 = 4 \cdot 3 \cdot 5 = 12 \cdot 5$$

$$(12, 5) = 1$$

$$1 = r \cdot 5 + s \cdot 12 = 25 - 24$$

$$b = r \cdot 5 \cdot b + s \cdot 12 \cdot b$$

$$12x = 0, 5y = 0$$

Every element can be written as a sum of terms killed by a power of a prime

$$A = \mathbb{Z}^r \oplus (\bigoplus_p B_p)$$

$$\mathbb{Z}^n \approx F \xrightarrow{\varphi} A \text{ } A \text{ finitely generated (by } n \text{ elements)}$$

$$\text{Ker}(\varphi) = X \subset F.$$

? understand A ! understand X inside F.

Elementary division theorem

There exists a basis of $F \approx \mathbb{Z}^n$ s.t. ... $X = \bigoplus_{i \leq r} 0 \oplus a_1 \mathbb{Z} \oplus a_2 \mathbb{Z} \oplus \cdots \oplus a_{n-r} \mathbb{Z}$, $a_i \geq 1$
 $X \subset \mathbb{Z}^n$

$a_1 | a_2 | a_3 | \cdots | a_{n-r}$, increasing multiplicatively

$A = F/X = \mathbb{Z}^r \oplus \mathbb{Z}/a_1 \mathbb{Z} \oplus \mathbb{Z}/a_2 \mathbb{Z} \oplus \cdots$, $a_i | a_{i+1}$

A finite abelian group $\rightarrow A$ is a direct sum of cyclic groups

p prime, $\#A = p^4 = a_1 a_2 a_3 \cdots$

A is direct sum of cyclic groups of p-power order.

$A \approx \mathbb{Z}/p^i \oplus \mathbb{Z}/p^j \oplus \mathbb{Z}/p^k \oplus \mathbb{Z}/p^l$ at most

$i \leq j \leq k \leq l$, $i + j + k + l = 4$, $i, j, k, l, \geq 1$

9/17

A arbitrary finitely generated group that we want to understand

Pick some generators g_1, \dots, g_n

Get a map from $Y = \mathbb{Z}^n$ to A , has some kernel

Considering $A = Y/X$, and how X lies in Y gives indication of structure of A

Can think of X, Y , as lattices

Theorem: $Y \cong \mathbb{Z}^n$ exists v_1, \dots, v_n basis of Y

such that in that basis $X = a_1 \mathbb{Z} \oplus a_2 \mathbb{Z} \oplus \cdots \oplus a_m \mathbb{Z} \oplus 0 \oplus 0 \oplus \cdots \oplus 0$.

$a_i \geq 1$, $a_1 | a_2, a_2 | a_3, \dots, a_{m-1} | a_m$.

Example: $A = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

$Y = \mathbb{Z} \oplus \mathbb{Z}$

$Y \supset X = 2\mathbb{Z} \oplus 3\mathbb{Z}$

Not at all true that the integers divide each other.

Puzzle. Not the case as in the theorem.

Need to prove to self that in some new basis, $Y = \mathbb{Z} \oplus \mathbb{Z}$,

and $X = \mathbb{Z} \oplus 6/\mathbb{Z}$, $Y/X = \mathbb{Z}/6\mathbb{Z}$.

$a_1 = 1$, and $a_2 = 6$.

$X \subset \mathbb{Z}^n$. Ask whether $X = (0)$ the zero submodule. If so, simple. So can assume nonzero.

Consider linear forms, homomorphisms $\mathbb{Z}^n \rightarrow \mathbb{Z}$.

For each λ have $\lambda(X) \subset \mathbb{Z}$. e.g., $\lambda(X) = 3\mathbb{Z}$. Some λ s are nonzero since X is nonzero.

Choose λ so that $\lambda(X)$ is maximal.

Example: $X = 2\mathbb{Z} \oplus 3\mathbb{Z}$. The first coordinate fn yields $2\mathbb{Z}$,

the second coordinate fn yields $3\mathbb{Z}$.

But with $\lambda(u, v) = v - u$ we can get all of \mathbb{Z} .

possible to get λ s yielding images $2\mathbb{Z}, 3\mathbb{Z}$, but not to get $\lambda, \lambda(X)$ containing both?

In any case, take a maximal λ , fix that λ .

$\lambda(X) = a\mathbb{Z}$ maximal

Pick $x \in X$ so that $\lambda(x) = a$.

Claim: $\mu(x) = b$ is divisible by a for all $\mu \in \text{Hom}(\mathbb{Z}^n, \mathbb{Z})$

$\gcd(a, b) = g = ra + sb$

$$\tau := r\lambda + s\mu, \tau(x) = g$$

$$\text{Now } \tau(X) \supset \mathbb{Z}g \supset \mathbb{Z}a$$

$$\text{So } \tau(x) = \lambda(x), \mathbb{Z}g = \mathbb{Z}a$$

$a|b$ for this reason of maximality

“Executive session”

R a commutative ring

R -module: M

1) abelian group

2) endowed with a scalar multiplication $r \in R, m \in M, rm \in M$

same as a vector space definition except R is not assumed to be a field

The context in which this elementary divisor theorem works.

A a finitely generated abelian group replaced by a finitely generated R -module

And there are 2 conditions on R .

R is an integral domain: $rs = 0 \rightarrow r = 0$ or $s = 0$

Ideals of R are principal $M \subset R \rightarrow M = R \cdot a$

Digression: motivation. Killer example.

K a field, and $R = K[t]$. (very much like \mathbb{Z} , can do Euclidean division by remainders)

Have V and action of $K[t]$: (action of K and action of t)

V + action of $K \rightarrow K$ -vector space

Action of t : $T : V \rightarrow V$ multiplication by $t, v \mapsto t \cdot v, T(v) = t \cdot v$

Conversely, can form the corresponding polynomial in the linear transformation

Principal Ideal domain. Element of smallest degree, Euclidean algorithm.

Suppose we have an R -module V . This is a K -vector space V with action of t

Multiplication by t gives a linear operator $T : V \rightarrow V$ (t commutes with K)

Remark: if V is of finite dimension over K , then it is finitely generated as a K -module

In particular, it's finitely generated over the ring $R = K[t]$

A an abelian group. If A is torsion, we are especially interested.

Suppose we start with a linear operator on a finite-dimension vector space.

There is a characteristic polynomial h such that $h(T) = 0$.

Cayley-Hamilton theorem.

$h(t) \in R = K[t]$. So $h(t) \cdot v = 0$.

V is a torsion module because $h(t)$ annihilates V .

Summary of what we have so far:

$0 \neq X \subset Y = \mathbb{Z}^n, \lambda : Y \rightarrow \mathbb{Z}, \lambda(X)$ is maximal among $\mu(X)$ s, $\lambda(X) = a\mathbb{Z}$.

Have shown that $a = \lambda(x)$, then $\mu(x)$ is divisible by a for all μ .

Take μ to be the i^{th} coordinate function, $x = (x_1, \dots, x_n) \in \mathbb{Z}^n, a|x_i$ for all $i = 1, \dots, n$,

$x = a \cdot y, y \in \mathbb{Z}^n, \lambda(y) = \lambda(x)/a = 1$

Think of Y : contains two submodules (subgroups)

$Y \supset \ker(\lambda), Y \supset \mathbb{Z} \cdot y$.

Claim: $Y = \ker(\lambda) \oplus \mathbb{Z}y$

1) each $z \in Y$ is: e.g. $(z - \lambda(z) \cdot y) + \lambda(z)y$

2) if my is in $\ker(\lambda)$ then $0 = \lambda(my) = m\lambda(y) = m$ so $m = 0, my = 0$, intersection is 0

The corresponding statement for X is that $X = (\ker(\lambda|_X)) \oplus \mathbb{Z}_X$

Kind of obvious that the intersection is 0.

Each component is a submodule of the corresp. one in Y .

$z \in X, \lambda(z) = m\lambda(x) = ma\lambda(y).$
 $z = z - \lambda(z)y + \lambda(z)y$
 $\lambda(z)y = m \cdot a \cdot y = mx$
 $(z - \lambda(z)y) \in \ker(\lambda) \cap X = \ker(\lambda|_X)$
 $\mathbb{Z}^n = Y = \ker(\lambda) \oplus \mathbb{Z}y$
 $Y \supset X = \ker(\lambda|_X) \oplus \mathbb{Z}ay$
 Apply inductively to portion of lower rank, having pulled off $\mathbb{Z}a$
 $X = a_1\mathbb{Z} \oplus a_2\mathbb{Z} \oplus \cdots \oplus a_m\mathbb{Z} \oplus 0 \cdots 0 \subset Y = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$
 need to have some kind of divisibility among these a , need to be explained
 $a_1|a_2, \dots$
 $Y = \mathbb{Z} \oplus Y'$ and $X = a\mathbb{Z} + X'$, working rightward
 start thinking of various linear maps $\lambda' : Y' \rightarrow \mathbb{Z}$, and how they restrict to X
 taking a maximal one, etc., etc.
 need to understand somehow that if we take this $\lambda'(X') = a'\mathbb{Z}$
 we want $a|a'$, meaning $a'\mathbb{Z} \subset a\mathbb{Z}$, do this with some greatest common divisor argument
 Introduce $g = \gcd(a, a')$ which we want to be a , write in form $ra + sa'$
 Need to find some interesting linear map from Y to \mathbb{Z}
 Have a map $Y' \xrightarrow{\lambda'} \mathbb{Z}$ and $\mathbb{Z} \rightarrow \mathbb{Z}$ the identity
 Both of these are linear maps that give linear maps $Y \rightarrow \mathbb{Z}$.
 Choose $x' \in X'$ so that $\lambda'(x') = a'$
 Have $(a, 0)$ in X so that the second linear map (just taking the first coordinate)...
 ...applied to $(a, 0)$ gives a
 Take $Y = \mathbb{Z} \oplus Y'$
 $\mathbb{Z} \oplus Y' \xrightarrow{f} \mathbb{Z}$
 $\mathbb{Z} \oplus Y' \rightarrow Y' \rightarrow Y' \xrightarrow{\lambda'} \mathbb{Z}$, the composition of which call g
 $Y = \mathbb{Z} \oplus Y' \ni (a, x') \in X$
 $f(a, x') = a$
 $g(a, x') = \lambda(x') = a'$
 $(rf + sg)(a, x') = G, rf + sg = \mu$
 $\mu(X) \supset \mathbb{Z} \cdot G \supset \mathbb{Z}a$
 Maximality $\rightarrow G = a$.
 Tells us that a really divides a' by maximality.
 The Y and the X really divide off into two separate worlds.
 $Y = \mathbb{Z} \oplus Y'$ and $X = a\mathbb{Z} \oplus X'$
 The world which we have already considered, and the trailing-off world of Y' and X'
 New map μ defined on all of Y and X , by leaving the first coordinate alone.
 Go back to the original example of the 2 and the 3. $Y = \mathbb{Z} \oplus \mathbb{Z} \supset X = 2\mathbb{Z} \oplus 3\mathbb{Z}$
 $\lambda(u, v) = v - u$
 $x = (2, 3), \lambda(x) = 1$
 $a = 1, \lambda(X) = \mathbb{Z}$, need to see how that line splits off in \mathbb{Z} and in X .
 $Y = \mathbb{Z} \cdot y \oplus \ker(\lambda)$
 $y = x/a = x, \ker(\lambda) = \{(u, v) : u = v\} = \mathbb{Z} \cdot (1, 1)$
 $Y = \mathbb{Z} \cdot (2, 3) \oplus \mathbb{Z} \cdot (1, 1) = \mathbb{Z}^2$
 $X = \mathbb{Z} \cdot (2, 3) \oplus \mathbb{Z} \cdot (1, 1) \cap (2\mathbb{Z} \oplus 3\mathbb{Z})$

$$\text{so } X = \mathbb{Z} \cdot (2,3) \oplus 6 \cdot \mathbb{Z}(1,1)$$

$$Y/X = \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}.$$