

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 , $GL(V)$ 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

$$Z(G) = \{g \in G : xg = gx \forall x \in G\}$$

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 $H \rightarrow gH$)

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

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”

Notation: S^G is the set of points in S fixed under the group action. ($gs = s \forall g \in G$)

Let G act on itself by conjugation ($S = G$). Then $S^G = Z(G)$.

For $s \in S (= G)$, G_s is a subgroup, and its order divides the order of the group, p^n .

Either $O(s)$ is trivial, and $s \in S^G = Z(G)$, otherwise $\#(O(s)) = p^k$ for $k > 0$

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

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

$Z(G)$ cannot be 1, since the identity of the group is in the center.

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 , $G_H = \{x \in G | xH = H\}$, hence $G_H = H$.

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 .

For each coset gH , K stabilizes that coset, hence K is the kernel of φ .

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 $s = e$), so an injection \rightarrow 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 $GL(n, \mathbb{Z}) = \{\phi : V \rightarrow V\}$

Can think of this as an action on $\mathbb{Z}^n \cong V$, whose permutation group is simply $GL(n, \mathbb{Z})$.

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.

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

$g \mapsto L_g$ 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

Lagrange: If $H \leq G$ then $\#(H) \mid \#(G)$.

A_4 with $n = 6$: a counterexample to the converse.

If $|G| = p^k \cdot r$, $(p, r) = 1$, a p -Sylow subgroup of G is an $H \leq G$ such that $|H| = p^k$

\mathbb{Z}_{12} has 2-sylow subgroup $\{0, 3, 6, 9\}$ and 3-sylow subgroup $\{0, 4, 8\}$

D_6 generated by r, s subject to $rs = sr^{-1}$, $r^6 = e$, $s^2 = e$

$\#(D_6) = 12$ so has 3-sylow subgroup $\{1, r^2, r^4\}$

Also has 2-sylow subgroups $\{1, r^3, s, r^3s\}$, $\{1, r^3, rs, r^4s\}$, $\{1, r^3, r^2s, r^5s\}$

$G = GL_n(\mathbb{F}_p)$, $n \times n$ linear transformations in \mathbb{F}_p , equal to $Aut(\mathbb{F}_p^n)$

Approximating 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.

Will use this fact in the subsequent proof.

Theorem: (Sylow I) For $|H| = p^k \cdot r$, $(p, r) = 1$, H has a p -Sylow subgroup.

Proof Sketch:

Show $\exists G, H \leq G$, such that 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:

Cayley's theorem, can embed H (of order n) in S_n by acting on itself by translation.

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 the action $g \in H \mapsto$ automorphism taking $\varphi(x)$ to $\varphi(xg)$.

$GL_n(\mathbb{F}_p)$ has p -Sylow subgroups. (upper triangular matrices with 1s on diag)

Let P be a p -Sylow subgroup of $G = GL_n(\mathbb{F}_p)$. Let G act on the cosets of P .

Now, $G_gP = gPg^{-1}$. Similarly, when H acts on G/P , $G_gP = (gPg^{-1} \cap H)$

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 .

The stabilizer of this orbit $gPg^{-1} \cap H$ is a p -Sylow subgroup H_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 $g \in G$.

A p -group can't contain a proper p -Sylow subgroup, so $J \cap gPg^{-1} = J$ and $J \subset gPg^{-1}$.

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

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

By the preceding corollary ($G \leq G$, $H \leq G$, $P \leq G$), $H \subset gPg^{-1}$ 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 $G/N(P) \leftrightarrow$ set of p -Sylows in G .

$N(P)$ the normalizer of P

There are $n_p = (G : N(P))$ 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:

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

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

Let $\text{Syl}_p(G)$ 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 $n_p \equiv_{\text{mod } p} 1$. Further, $n_p | r$.

Proof:

Let P act on $\text{Syl}_p(G)$ by conjugation.

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

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 $(\text{Syl}_p(G))^P \equiv_{\text{mod } p} 1$.
 G acts on $\text{Syl}_p(G)$ 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

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 ($H \subset N(K)$)

A simple group is a non-trivial group with no non-trivial proper normal subgroups

A finite abelian group G is simple $\leftrightarrow G$ is cyclic of prime order

show this

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. $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset SL(2, \mathbb{Z}|p\mathbb{Z})$

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).

G finite non-trivial.

If G is simple, $\{e\} \subset G$, $G/\{e\}$ simple.

If G is not simple $G \supset G_1 \supset (e)$, $G_1 \trianglelefteq G$, G_1 , G/G_1 smaller than G .

Use principle of strong induction for a full decomposition.

Obtain a successive extension of simple groups.

Given G , such a tower, let $G_i/G_{i+1} = Q_i$ and consider the multiset $\{Q_0, \dots, Q_{n-1}\}$.

In multiset, order does not matter, and multiplicity does matter.

Jordan-Hölder Theorem: Each composition yields the same multiset up to isomorphism.

9/10

Proposition: Given G , $\exists G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n$, $G = G_0$, $G_{i+1} \trianglelefteq G_i$, G_i/G_{i+1} simple.

This is a normal tower or composition series; the simple quotients are the constituents.

If it is simple, then the filtration is $G \supset \{e\}$.

If G is not simple, $G \supset N \supset \{e\}$, where $G/N, N$ proper in G .

By strong induction, have filtrations for each. To conclude, use:

\exists natural correspondence between subgroups of G/N and subgroups H of G , $N \leq H$

$G \supset L \supset N$, $L/N \subset G/N$

$\pi: G \rightarrow G/N$, $K \subset G/N$, $\rightarrow \pi^{-1}(K) \leq G$

Jordan-Hölder Theorem:

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

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

The “multiplicity set” $\{Q_0, \dots, Q_{n-1}\}$ is independent of the filtration.

Where order doesn't count, multiplicity does, and Q_i up to isomorphism.

Related question: can two different groups have the same reduction?

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”.

Jordan-Hölder Theorem: Proof.

Base case $n = 1$, $G \supset \{e\}$, $G/\{e\}$ simple and G simple.

Supposing $G \supset G_1 \supset \dots \supset G_n \supset \{e\} = G_{n+1}$ and $G \supset G'_1 \supset \dots \supset G'_m \supset \{e\} = G'_{m+1}$.

? $m = n$, $\{G_i/G_{i+1}\} = \{G'_j/G'_{j+1}\}$... 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 $G_1 \supset \dots \supset G_n \supset \{e\} = G_{n+1}$.

Take $G_1 \supset G_1 \cap G'_1 = H \supset H_1 \supset H_2 \supset \dots \supset H_k \supset \{e\}$, 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: $G/G_1 + \text{constituents of } G_1 = G/G_1 + G/G'_1 + \text{constituents of } H$.
 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

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

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

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

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

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

$\text{Mor}(?, B) = \prod \text{Mor}(A_i, B)$? = 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 $Y \rightarrow A/X$.

$\pi|_Y$ 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 $i = 1, \dots, r$

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

$\pi \circ s = id_{A/X}$

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

$\pi|_Y$ 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

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

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

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

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

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

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

$B_p \subset B$.

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

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

Proof essence:

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
 $A = \mathbb{Z}^r \oplus (\bigoplus_p B_p)$
 $\mathbb{Z}^n \xrightarrow{\varphi} A$ A finitely generated (by n 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 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 $\mu \in \text{Hom}(\mathbb{Z}^n, \mathbb{Z})$

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

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

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

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 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 .
 $z \in X$, $\lambda(z) = m\lambda(y) = ma\lambda(y)$.
 $z = z - \lambda(z)y + \lambda(z)y$
 $\lambda(z)y = m \cdot a \cdot y = mx$
 $(z - \lambda(z)y) \in \ker(\lambda) \cap X = \ker(\lambda|_X)$
 $\mathbb{Z}^n = Y = \ker(\lambda) \oplus \mathbb{Z}y$
 $Y \supset X = \ker(\lambda|_X) \oplus \mathbb{Z}ay$
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 .

$$\begin{aligned}
Y &= \mathbb{Z} \cdot y \oplus \ker(\lambda) \\
y &= x/a = x, \ker(\lambda) = \{(u, v) : u = v\} = \mathbb{Z} \cdot (1, 1) \\
Y &= \mathbb{Z} \cdot (2, 3) \oplus \mathbb{Z} \cdot (1, 1) = \mathbb{Z}^2 \\
X &= \mathbb{Z} \cdot (2, 3) \oplus \mathbb{Z} \cdot (1, 1) \cap (2\mathbb{Z} \oplus 3\mathbb{Z}) \\
\text{so } X &= \mathbb{Z} \cdot (2, 3) \oplus 6 \cdot \mathbb{Z}(1, 1) \\
Y/X &= \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

9/22

Rings R , A (= 'anneau')

definition: whether or not $1 \in R$ can vary

Lang: $1 \in R$, Hungerford: $1 \notin R$

In the former, $2\mathbb{Z}$ is not a ring, in the latter, it is

Ring:

under $+$, an abelian group with distinguished element 0

under \cdot , associative (not necessarily commutative) with distinguished element 1

distributive laws $(x + y)z = \dots$ and $z(x + y) = zx + zy$

Integral domain:

Field: under \cdot , commutative, and non-zero elements have inverses

Examples

For A an abelian group, the ring of endomorphisms.

$$R = \text{End}(A) = \text{Hom}(A, A), (f + g)(a) = f(a) + g(a), fg = f \circ g$$

If $A = \mathbb{Z}^n$ $\text{End}(A)$ can be viewed as a ring of matrices

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$ are fields.

The "skew field" of Hamilton quaternions over $\mathbb{R}, \mathbb{Q}, a + bi + cj + dk (= (\frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2})^{-1})$

Group G (written multiplicatively), $\mathbb{Z}[G] = \mathbb{Z}\langle G \rangle$ the free abelian group on G

elements $\sum n_g \cdot g, n_g \in \mathbb{Z}$ the sum finite

can multiply

$$(\sum n_g \cdot g)(\sum m_h \cdot h) = \sum_{x \in G} (\sum_{g, h, gh=x} n_g m_h) x$$

The term $c_x = \sum_g n_g m_{g^{-1}x}$ represents a convolution product

Ring Homomorphism

a homomorphism of abelian groups respecting multiplication

$$\varphi(xy) = \varphi(x)\varphi(y)$$

$\varphi(1) \neq 1$ is possible

$\ker(\varphi) = \{r \in R | \varphi(r) = 0\}$ is an ideal: $x \in R, r \in \ker(\varphi) \rightarrow xr, rx \in \ker(\varphi)$

Ideals

additive subgroup with ideal property:

$xI \subset I$ left-sided, $Ix \subset I$ right-sided, both \rightarrow 2-sided (bilateral)

exact analogues of normal subgroups

two-sided ideal: well-defined quotient multiplication

$$(r + I) \cdot (s + I) := rs + I$$

$$(r + I)(s + I) = r(s + i) + I = rs + ri + I \text{ and similarly}$$

$$(r + I)(s + I) = (r + i)s + I = rs + is + I$$

therefore ideals are kernels of ring homomorphisms

Principal Ideal (a) is the minimal ideal containing a

is all multiples of a in R : $I = Ra$, said to be generated by a

Ideal generated by a subset X is the intersection of all ideals containing X

if $X = \{a_1, \dots, a_t\}$, is written (a_1, \dots, a_t)

Prime ideal $P \subset R$

proper

if $rs \in P$ then $r \in P$ or $s \in P$

Examples

\mathbb{Z} has as ideals the additive subgroups $a\mathbb{Z}$, $a \geq 0 = (a)$; if $a = 0$ or a is prime, (a) is prime

$R = K[x]$ where K is a field: by Euclidean division, all ideals are principal

$R = K[x, y]$

$R \xrightarrow{\varphi} K, f(x, y) \mapsto f(0, 0) \in K, \ker(\varphi) = \{\text{polynomials with constant term of } 0\}$

this is *not* principal

elements $0 + ax + by + cx^2 + \dots$

$\varphi : R \rightarrow S$ a ring homomorphism and P a prime ideal of S

$\varphi^{-1}(P)$ is a prime ideal of R

Proof:

Let $x, y \in R$ and suppose $xy \in \varphi^{-1}(P) = P'$

then $\varphi(x)\varphi(y) = \varphi(xy) \in P \rightarrow \varphi(x) \in P$ or $\varphi(y) \in P \square$

Corollary: $\varphi : R \rightarrow S$ a non-trivial homomorphism of rings and (0) prime in S

the kernel of φ is prime

S is called an integral domain if

$$(0) \neq S$$

if $xy = 0$ then $x = 0$ or $y = 0$

Proposition: $P \subset R$ is a prime ideal $\leftrightarrow R/P$ is an integral domain

Maximal ideal $M \subset R$

$$M \neq R$$

$$M \subset M' \rightarrow M = M' \text{ or } M' = R$$

Proposition: M is maximal $\leftrightarrow R/M$ is a field

Example: $\mathbb{Z} \supset a\mathbb{Z}$ maximal $\leftrightarrow a$ is prime

Corollary: Maximal ideals are prime

Pf: Fields are integral domains.

9/24: Midterm

9/29

(Charlie)

A a ring, I an ideal in A

have a correspondence between ideals $J, I \subset J \subset A$ and the ideals of A/I

$\pi : A \rightarrow A/I$ and $\pi(J) = J/I \subset A/I$

for K ideal of A/I , consider $\pi^{-1}(K) \subset A$

$I \subset \pi^{-1}(K)$, show that is an ideal

A a ring, its group of units $A^* = \{u \in A \mid \exists v \in A, uv = 1\}$

$\mathbb{Z}[i]^* = \{1, -1, i, -i\} \cong \mathbb{Z}/4\mathbb{Z}$

$\mathbb{R}[x]^* = \mathbb{R}^*$

$\mathbb{Z}[\sqrt{5}] \ni 1, -1, 2 + \sqrt{5}, 2 - \sqrt{5}$

A a field $\leftrightarrow A^* = A - \{0\}$ and $A \neq \{0\}$

a field is an integral domain

the ideal $\{0\}$ is maximal in a field

Every proper ideal of A is contained in a maximal ideal.

Proof by Zorn's Lemma.

Chinese Remainder Theorem

a ring A with ideals $I_1, \dots, I_k, k \geq 2$

the ideals coprime: that is, $I_i + I_j = A$.

then there exists a surjective map $A \rightarrow A/I_1 \times \dots \times A/I_k$

example

$r\mathbb{Z} + s\mathbb{Z} = \gcd(r, s)\mathbb{Z}$

$(r\mathbb{Z})(s\mathbb{Z}) = r \cdot s\mathbb{Z}$

$r\mathbb{Z} \cap s\mathbb{Z} = \text{lcm}(r, s)\mathbb{Z}$

$(\text{lcm})(\gcd) = rs$

for two: $IJ, A/(IJ) \leftrightarrow (A/I) \times (A/J)$

$(IJ = I \cap J)$

Proof:

Assume $I, J \subset A, I + J = A$

$A \rightarrow A/I \times A/J$

let $x + y = 1$

$x \rightarrow (0, 1)$ and $y \rightarrow (1, 0), cx + dy \rightarrow (c, d)$

Quotient Fields

e.g. $\mathbb{Z} \rightarrow \mathbb{Q}$

A an integral domain and S a "multiplicative subset" of A

$1 \in S, x, y \in S \rightarrow xy \in S$

$S^{-1}A =$ equivalence class

10/1

Commutative centre = integral domain.

PIDs UFDs

PID: Every ideal is principal, $I = (a)$

generalization: every ideal is finitely generated $I = (a_1, \dots, a_m) = \{\sum_{i=1}^m r_i a_i \mid r_i \in A\}$

Noetherian

equivalence of 3 conditions on a ring, for which, if holds, makes the ring Noetherian

(1) each ideal is finitely generated

(2) chains become stable

(3) Every non-empty set of ideals of A contains a maximal element.

Condition (2): stability of chains

$I_1 \subset I_2 \subset I_3 \subset \dots$ increasing chain of ideals in A

$\exists N \geq 1$ so that $I_n = I_N$ for all $n \geq N$

e.g. \mathbb{Z}

$(2^{100}) \subset (2^{99}) \subset \dots$

can have arbitrarily long chains in ring of integers

but all of them terminate

(1) implies (2)

Consider a $I_1 \subset I_2 \subset \dots$

and take $I = \bigcup_{i=1}^{\infty} I_i$

I finitely generated, each a_i needs to be in some I

eventually all of them are in some I_N , so $I \subset I_N$, we are done

(2) implies (3)

Take $I_1 \in S$. If not a maximal elt of S , $I_1 \subset I_2$, $I_2 \in S$

If I_2 not max, etc., continue and construct a chain

can't go to infinity if (2) is assumed; must end, I_N is maximal

irreducible elements of A : elements that can't be factored

an element $a \in A$, $a \neq 0$ and not a unit

if $a = bc$ then b is a unit or c is a unit

(0) $\subset (a) \subset A$

maximal if A is a PID

$(a) \subset I = (b) \subset A$

$a \in (b)$, $a = bc$

b a unit then $I = A$ and if c is a unit, $I = (a)$

Proposition: If A is a PID, then every $t \in A$, $t \neq 0$, t not a unit

t can be written as a product of irreducible elements

Proof:

Consider the set of (principal) ideals (t) for which the proposition is false

If $S = \emptyset$, done. Else consider a maximum element $(m) \in S$

but if $(m) \subsetneq (m')$ then (m') can be factored

if m irreducible it can be factored, if not $m = m' m''$ where m' , m'' not units

$(m) \subsetneq (m')$, $(m) \subsetneq (m'')$

(m') , (m'') not in S , they can be factored, we are done

This proof also works for Noetherian rings generally

common tactic by maximal counterexample

prime elements of A

$a \neq 0$, not a unit, a prime $\leftrightarrow (a)$ is prime

if $a|bc$ then $a|b$ or $a|c$

Primes are irreducible:

if a is prime and $a = bc$ then $a|b$ or $a|c$

if $a|b$ then b is a multiple of a and a is a multiple of b

so $a \sim b$: $b = u \cdot a$ and $a = u^{-1} \cdot b$, differ by a unit

irreducible elements might not be prime

$A = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}$

$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$

2 is irreducible and not prime, $2|4$ but doesn't divide either on the right side

exists norm $N : z \mapsto z\bar{z}$

$a + b\sqrt{-3} \mapsto a^2 + 3b^2$

2 is irreducible

$2 = \alpha\beta$, $N(2) = N(\alpha)N(\beta)$, $4 = N(\alpha)N(\beta)$

but norms can never be 2 so one of these must be a unit ($N = 1$ implies ± 1)

In a PID, irreducible elements are prime

an irred $\rightarrow (a)$ is maximal $\rightarrow (a)$ is prime $\rightarrow a$ is prime

Unique factorization domain: every $a \neq 0$, unit has a factorization as a prod of irreducibles

this is unique up to reordering and transformation by units

$a \sim b$, a and b are associated, if $a = b \cdot u$ and $b = a \cdot u^{-1}$ for some unit u

Theorem: PIDs are UFDs

PID: $a = \pi_1 \cdots \pi_n = \sigma_1 \cdots \sigma_m$

σ_m prime so σ_m divides some π_i

can assume $\sigma_m | \pi_n$, $\pi_n = \sigma_m \cdot c$, c unit

proceed by induction on indices, end

A PID $a, b \in A$, $(a, b) = \{ax + by | x, y \in A\} = (g)$ since principal

$g = \gcd(a, b)$: $(g) = (a, b) \ni a, b$

a and b are multiples of g , g divides a, b

t can't be factored as a product of irreducibles, (t) is maximal in this property

if t irreducible $t = t$; impossible

if t not irreducible, $t = r \cdot s$, r, s non-units

$(t) \subsetneq (r)$ $(t) \subsetneq (s)$

$A = \mathbb{Z}[\dots (7)^{\frac{1}{2^N}} \dots]$

7 is not a unit in A

Lemma: every element of A is "integral"

it satisfies an equation (monic polynomial) $x^n + c_{n-1}x^{n-1} + \dots + c_0 = 0$

monic: first coefficient = 1

$c_i \in \mathbb{Z}$

integral ring

1/7 satisfies no such polynomial

7 can be factored on and on $n(7^{1/n})$; not a Noetherian ring

10/6

A-Modules (left modules)

M = abelian group with an action of scalar multiplication of A (= ring)
(same axioms as for an A -vector space except that $A \neq \text{field}$)

$\text{End}(M) = \text{Hom}(M, M)$

$M = \mathbb{Z}^n, \text{End}(M) = M(n, \mathbb{Z})$

action of A on M : a homomorphism of rings $A \xrightarrow{\varphi} \text{End}(M)$

$\varphi(a) \in \text{End}(M), \varphi(a) : M \rightarrow M, (\varphi(a))(m) := a \cdot m$

$f, g \in \text{End}(M): fg = f \circ g$

Diversion: Fresh water (Chicago) algebra: $a \in A, m \in M, m^a, (m^{ab}) = (m^a)^b$

instead of $a \cdot m$ or $a(m)$

Module properties

$\varphi(ab) = \varphi(a)\varphi(b)$

$(ab) \cdot m = a \cdot (b \cdot m)$

$a \cdot (m + m') = a \cdot m + a \cdot m'$

$\varphi(a) \in \text{End}(M)$

$(a + b) \cdot m = a \cdot m + b \cdot m$

$\varphi(a + b) = \varphi(a) + \varphi(b)$

Examples:

$A = \text{field}$: an A -module is an A -vector space

Th: (uses choice) every A -vector space has a basis \leftrightarrow all A -modules are free

M free on the set of generators $\{x_i\}_{i \in I}$

if every $m \in M$ is uniquely a finite A -linear combination of the x_i

For I , the free A -module on the set I

$\{\sum_{i \in I} a_i x_i \mid a_i \in A \text{ all but finitely many are } 0\}$

could also notate $\{\sum_{i \in I} a_i i \mid a_i \in A \text{ all but finitely many are } 0\}$, just indexed by I

Direct sums $\{M_i\}_{i \in I}, \oplus_{i \in I} M_i$

set of tuples indexed by I , with the i^{th} entry in M_i , all but finitely many entries are 0

$a \cdot (\cdots m_i \cdots)_{i \in I} = (\cdots a m_i \cdots)_{i \in I}$

Homomorphisms of A -modules M, N

$M \xrightarrow{h} N$, conditions of linearity $h(x + y) = h(x) + h(y), h(a \cdot x) = ah(x)$

$A = \text{field}$: linear map

$\text{Hom}_A(M, N)$ is an A -module

A map from a direct sum to a module uniquely determined by action on the summands

$$M \hookrightarrow \oplus_{j \in I} M_j \xrightarrow{h} N$$

$$M_i \xrightarrow{h_i} N$$

$$\text{Hom}_A(\oplus M_i, N) \xrightarrow{\alpha} \prod_{i \in I} \text{Hom}_A(M_i, N), h \mapsto (\cdots, h_i, \cdots)$$

α is a bijection

To map a free module to N is to choose the images of each of the generators

Unconstrained: can choose arbitrarily the images of the generators

Examples

$A = \mathbb{Z}$, $M = \text{ab grp}$, $\mathbb{Z} \rightarrow \text{End}(M)$, $1 \mapsto \varphi(1) = id$, $2 \mapsto id + id$, $-1 \mapsto -id$

$A = A$, $I \subset A$ left ideal, $I = A$ -module, $a \cdot i = ai \in I$

ring hom $A \rightarrow A'$, $M = A'$ -module, $A \rightarrow A' \xrightarrow{\varphi} \text{End}(M)$, A' -modules $\mapsto A$ -modules

$M = \mathbb{Z}$ -module, $n \geq 1$, $M^n = \bigoplus_{i=1}^n M$

$A = M(n, \mathbb{Z})$ acts on M^n by left matrix multiplication

could replace \mathbb{Z} by some ring R , new construction

An exercise: A -modules \leftrightarrow abelian groups, leftwards, $M \mapsto M^n$, rightwards, ?

Morita equivalence

Exact sequence $X \xrightarrow{h} Y \xrightarrow{g} Z$; $\text{Im}(h) = \text{Ker}(g)$ (implies $g \circ h = 0$, but even stronger)

can make these as long as we like $\cdots X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} \cdots$

exact if exact at each place X_i , i.e. $\text{Ker}(f_{i+1}) = \text{Im}(f_i)$ for all i

Examples

$Y \xrightarrow{g} Z \xrightarrow{0} 0$, exact. g is surjective (epimorphism)

$0 \rightarrow X \xrightarrow{h} Y$, exact. h is injective (monomorphism)

$0 \rightarrow X \xrightarrow{h} Y \xrightarrow{g} Z \rightarrow 0$ is called a short exact sequence. $Y/h(X) \cong Z$

$X \xrightarrow{h} Y$, $0 \rightarrow \text{Ker}(h) \rightarrow X \xrightarrow{h} \text{Im}(h) \rightarrow 0$, exact, $X/\text{Ker}(h) \cong \text{Im}(h)$

$0 \rightarrow \text{Im}(h) \rightarrow Y \rightarrow \text{Coker}(h) \rightarrow 0$

$0 \hookrightarrow \text{Ker}(h) \hookrightarrow X \xrightarrow{h} Y \rightarrow Y/\text{Im}(h) = \text{Coker}(h) \rightarrow 0$

$N \rightarrow X \rightarrow Y \rightarrow 0$, $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$ exact. $\text{Hom}_A(N, X) \rightarrow \text{Hom}_A(N, Y)$

use a functor, get a $0 \rightarrow \text{Hom}(N, X) \rightarrow \text{Hom}(N, Y) \rightarrow \text{Hom}(N, Z) \rightarrow 0$

have exactness at $\text{Hom}(N, X)$, $\text{Hom}(N, Y)$

what about exactness at $\text{Hom}(N, Z)$?

equivalent statement: every homomorphism $N \rightarrow Z$ lifts to a homomorphism $N \rightarrow Y$

the entering map not necessarily surjective

e.g. $A = \mathbb{Z}$, $X = 2\mathbb{Z}$, $Y = \mathbb{Z}$ and $Z = Y/X = \mathbb{Z}/2\mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$, lift does not exist

go from left to right using functor/construction $\text{Hom}_A(N, \cdot)$

this functor/construction is "left exact" but not "right exact/fully exact"

the class of modules with full exactness are the projective modules

10/8

(Tal)

A a ring and M, N modules

$\text{Hom}_A(M, N)$ is an abelian (group?/ring?)

if A is commutative, then it is an A -module

$0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \rightarrow 0$ (exact?)

$0 \rightarrow \text{Hom}_A(N, X) \rightarrow \text{Hom}_A(N, Y) \rightarrow \text{Hom}_A(N, Z) \rightarrow 0$

this sequence is left exact and exact at the center

surjectivity of the map $\text{Hom}_A(N, Y) \rightarrow \text{Hom}_A(N, Z)$

$Y \twoheadrightarrow Z$ via $G, h : N \rightarrow Z$

does H exist such that $g \circ H = h$?

the same question, rephrased:

suppose we map $\text{Hom}_A(N, Y) \rightarrow \text{Hom}_A(N, Z)$, taking H to h

is this map surjective?

an example of a case where it does not lift

take $h > 1$

$\mathbb{Z} \rightarrow \mathbb{Z}/h\mathbb{Z}$ surjective

identity $\mathbb{Z}/h\mathbb{Z}$, look for map $\mathbb{Z}/h\mathbb{Z} \rightarrow \mathbb{Z}$

map doesn't exist, no lifting

(1) Suppose $y \xrightarrow{g} Z$ is surjective.

If $\text{Hom}_A(N, Y) \xrightarrow{g^*} \text{Hom}_A(N, Z)$ is also surjective, we say N is projective

an equivalent statement: the functor $\text{Hom}_A(N, \cdot)$ is right exact

another equivalent statement: for all g, h there is a lifting H

$g : y \twoheadrightarrow Z, h : N \rightarrow Z, H : N \rightarrow y$

(2) given a sequence $0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} N \rightarrow 0$

if $\exists s$ such that $g \circ s = \text{id}_N$ we say that the sequence splits

all exact sequences split (misreading notes?)

given $y \xrightarrow{g} N \rightarrow 0$, we can find s such that $g \circ s = \text{id}$

(1) implies (2)

if N is projective, then the exact sequence $0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} N \rightarrow 0$ splits

take $h = \text{id} \rightarrow Z = N$

$y \xrightarrow{g} N, \text{id} : N \rightarrow N, N \rightarrow Y$

(3) the module N is a direct summand of a free module:

$\exists M$ such that $N \oplus M \cong F$ where $F = A\langle S \rangle$

(2) implies (3)

choose a set of generators of N , call it S . You can have $N \subset S$

induces $A\langle S \rangle \rightarrow N$ surjective

we have $f : N \rightarrow A\langle S \rangle$ by hypothesis

so $A\langle S \rangle = \text{Ker}(g) \oplus f(N)$

(3) implies (1)

$F = M \oplus N$ where F is free

want to show that if $g : Y \twoheadrightarrow Z$ then $\text{Hom}_A(N, Y) \xrightarrow{g^*} \text{Hom}_A(N, Z)$ is surjective

$F = A\langle S \rangle$ same as $\text{Hom}_A(F, X) = \text{Maps}(S, X)$

S generates F , so a map $F \rightarrow X$ is determined by S

$\text{Hom}_A(F, Y) = \text{Maps}(S, Y)$ and $\text{Hom}_A(F, Z) = \text{Maps}(S, Z)$

$\text{Maps}(S, Y) \rightarrow \text{Maps}(S, Z)$ obviously surjects, $\text{Hom}_A(F, y) \rightarrow \text{Hom}_A(F, Z)$ surjects

$s \rightarrow z \in Z$ and $Y \ni y \rightarrow z \in Z$

$$\text{Hom}_A(M \oplus N, Y) = \text{Hom}_A(M, Y) \times \text{Hom}_A(N, Y)$$

have surjective $\text{Hom}_A(M \oplus N, Y) \xrightarrow{\sigma} \text{Hom}_A(M \oplus N, Z)$

$$\text{Hom}_A(M, Y) \times \text{Hom}_A(N, Y) \xrightarrow{(g_*, g_*)} \text{Hom}_A(M, Z) \times \text{Hom}_Z(N, Z)$$

since σ surjective, (g_*, g_*) surjective and g_* surjective

Thus $\text{Hom}_A(N, Y) \xrightarrow{g_*} \text{Hom}_A(N, Z)$ surjective.

Diagram

$$\text{Hom}(M \oplus N, Y) \rightarrow \text{Hom}(N, Y) \text{ by } h \mapsto h \circ i$$

$$\text{Hom}(M \oplus N, Y) \xrightarrow{g_*} \text{Hom}(M \oplus N, Z)$$

$$\text{Hom}(N, Y) \rightarrow \text{Hom}(N, Z)$$

$$\text{Hom}(M \oplus N, Z) \rightarrow \text{Hom}(N, Z)$$

$$g \circ h \mapsto (g \circ h) \circ i = g \circ (h \circ i)$$

Diagram

$$N \xrightarrow{h \circ i} Y$$

$$N \hookrightarrow M \oplus N$$

$$M \oplus N \xrightarrow{h} Y$$

Examples: free modules are projective.

Any free module is a summand of another module that generates (word unsure) a free module

If A is a field, all A -modules are free.

$$A = K \oplus K = \{(a, b) | a, b \in K\}, K \text{ a field}$$

$$F = A = N \oplus M \text{ where } N = \{(a, 0) | a \in K\} \text{ and } M = \{(0, b) | b \in K\}$$

Projective, but not free over A .

Suppose $N \cong A\langle S \rangle$, basis over $A \leftrightarrow S$

$$N \cong A^n, \dim_k N = 2h = 1 \text{ (not sure about these figures)}$$

$$n > 1, A = M(n, k), F = A$$

$$M \in A, x \in F$$

$$M_1 x \text{ matrix (not sure if right), } x = (c_1 \cdots c_n) \text{ n columns}$$

$$M \circ X = (M_{c_1}, \dots, M_{c_n})$$

$$F = K^n \oplus \cdots \oplus K^n$$

K^n projective, not free.

example (justification left for homework)

k a number field; that is, contains \mathbb{Q} (\mathbb{Q} ?) and $\dim_{\mathbb{Q}} k < \infty$

let $\alpha \in \mathbb{C}$ and α algebraic

$$k = \text{span}(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$$

k field

Diagram

$$A \subset k, \mathbb{Z} \subset \mathbb{Q}, A \text{ assoc with } \mathbb{Z}, k \text{ with } \mathbb{Q}$$

$$A = \{\beta \in k | \beta \text{ satisfies a monic polynomial with integer coefficients}\}$$

Theorem: the ring A is a Dedekind domain.

Definition of a Dedekind domain

If I is an ideal in A , then there exists $J \subset A$ (is it an ideal?) such that

$$IJ = \left\{ \sum_{r=1}^t x_r y_r \mid x_r \in I, y_r \in J, t \geq 0 \right\}$$

is principal

What is J ?

Define $I^{-1} = \{y \in k \mid yI \subset A\} \subset A$

I^{-1} is an A -submodule of k .

$II^{-1} \subset A$, in fact $II^{-1} = A$

Theorem: If I is a nonzero ideal in a Dedekind Domain A , I is a projective.

10/13

Category

notation e.g. \mathcal{A} , (sets)

objects, and $Mor(A, B)$ a set of morphisms from the object A to the object B

axioms: every object has an identity morphism

composition of which preserves morphisms, etc.

define isomorphisms in terms of the existence of inverses

in some categories, bijections are not isomorphisms

Examples

for A a ring, the category of A -modules

morphisms of which are the A -linear homomorphisms $X \rightarrow Y$, $Hom_A(X, Y)$

pointed sets (X, x) in which a morphism is an $f : (X, x) \rightarrow (Y, y)$, $f(x) = y$

A -modules X, Y, Z, W and fixed X take as objects pairs (Y, f) where $f : Y \rightarrow X$

we have created a new category relative to X

category of partially ordered sets, whose morphisms are isotone maps

Functor

takes objects to objects, and also morphisms to morphisms

Diagram (F is the functor, f is a morphism, A, A' are objects)

$$A \xrightarrow{F} F(A)$$

$$A \xrightarrow{f} A'$$

$$A \xrightarrow{F} F(A')$$

$$F(A) \xrightarrow{Ff} F(A')$$

since the arrows go in the same direction, this describes a covariant functor

if, say, $F(A') \xrightarrow{Ff} F(A)$, this would be a contravariant functor

Examples

forgetful functors from for instance (groups) \rightarrow (sets) or (A -modules \rightarrow (abelian groups)

Fix X . Functor from $A \in Ob(A) \rightarrow Mor(X, A)$ (morphisms in the category of sets)

or, contravariantly $A \in Ob(A) \rightarrow Mor(A, X)$

in A -modules, fix X and take N to $N \oplus X$

or from (sets) to (abelian groups) using the free group construction

Representable Functors

covariant $\mathcal{A} \xrightarrow{F} (\text{sets})$

Fix X . By the hom-functor $h_X, A \mapsto \text{Mor}(X, A)$.

Given an F , can it be written as a hom-functor?

That is, for some X , is $F \cong h_X$?

Those which can be are said to be represented by X (not a complete definition)

Fully defining a representable functor F

we need an $X \in \mathcal{A}$ and a $u \in F(X)$ such that for all A have a bijection

$$\text{Mor}(X, A) \rightarrow F(A)$$

if we have an $h : X \rightarrow A$, it induces a morphism $h_* : F(X) \rightarrow F(A)$

the lower-star signifies a covariant (push-forward)

a contravariant (pull-back) would be represented by an upper-star

can associate $h \in \text{Mor}(X, A)$ with $h(u)$ and this $h \mapsto h(u)$ is a bijection

epithet: to give an element of $F(A)$ is to give a map $X \rightarrow A$

Example of a Representable Functors

Fix a set S , let \mathcal{A} be the category of abelian groups

Take $G \mapsto F(G) = \text{Maps}(S, G)$

Want an abelian group X such that $\text{Maps}(S, G) \cong \text{Hom}(X, G)$

Take X to be the free abelian group on S

The universal element u is the set map taking s to $1 \cdot s$

Diagram:

$$X = \mathbb{Z}\langle S \rangle \xrightarrow{h} G$$

$$S \xrightarrow{u} \mathbb{Z}\langle S \rangle$$

$$S \xrightarrow{h_*(u)} G$$

a set map in the category of sets is given by a group map from the free group

Another example

From \mathcal{A} the category of abelian groups to sets

Fix $M, N \in \mathcal{A}$. Define the functor $A \mapsto \text{Hom}(M, A) \times \text{Hom}(N, A)$

to give a pair of maps $M \rightarrow A, N \rightarrow A$ is to give a map from the direct sum to A

Take $X = M \oplus N$ and $u \in F(X) = \text{Hom}(M, X) \times \text{Hom}(N, X)$

u is a universal pair of inclusions

to give a map of the direct sum is to give a map of the first and a map of the second

The uniqueness of (X, u)

if they represent the same functor, they are isomorphic in a canonical sense

no choice involved in the formulation of isomorphism

say (X, u) and (X', u') represent the functor F

then $\text{Mor}(X, A) \ni h \mapsto h_*(u) \in F(A)$ and $\text{Mor}(X', A) \ni h' \mapsto h'_*(u') \in F(A)$

taking the particular cases when $A = X'$, $A = X$
not totally sure if the next two lines are totally right
I remember he said in class that these are "the same" h as those in the above line
 there is a bijection $\text{Mor}(X, X') \rightarrow F(X')$; so for some $h \in \text{Mor}(X, X')$, $h(u) = u'$
 there is a bijection $\text{Mor}(X', X) \rightarrow F(X)$ so for some $h' \in \text{Mor}(X', X)$, $h'(u') = u$
 the representing property of X and X' gives two morphisms
 their compositions are the identity on X and the identity on X' (why?)

Tensor Products

can be defined on noncommutative rings
 one must be a left-module and the other a right-module
 will be defined on a commutative ring A for simplicity
 A -modules X, Y, Z, M, N, T
 bilinear maps $\text{Bil}(X \times Y, Z)$: linear in each variable
 i.e. $\text{Bil}(X \times Y, Z) = \text{Hom}_A(X, \text{Hom}_A(Y, Z))$

two examples of bilinear maps

$X, Y = k^n$ for k a field, $f(x, y) = \det(x|y|c_1|\cdots|c_{n-2}) \in k$
 $x \in X, Y = \text{Hom}_A(X, A) \ni \varphi$ a linear form, $(x, \varphi) \mapsto \varphi(x)$

Define a functor whose representing element is T a tensor product.

Fix X, Y in the category of A -modules and have $F : Z \mapsto \text{Bil}(X \times Y, Z)$
 $F(Z) = \text{Mor}(T, Z) = \text{Hom}_A(T, Z)$
 $u \in F(T)$ gives the universal bilinear map $u : X \times Y \rightarrow T$
 A homomorphism $T \rightarrow Z$ gives a bilinear map $X \times Y \rightarrow Z$
 i.e. there is a set bijection $\text{Bil}(X \times Y, Z) \leftrightarrow \text{Mor}(T, Z)$
 How one constructs such a T : next lecture.

T has uniqueness property by canonical isomorphism.

We do some amount of work to show this construction is possible
 Then we can abstract away this work because of the universality of T
 (last line unsure; maybe ask about it again)

10/15