Name: Joseph McGuire Class: Math 561(Fall 2021)

Category Theory

Definition 1

A category $\mathcal{C}$ consists of two classes, one of objects and the other of morphisms. The class of objects is written $\mathbf{Obj}(\mathcal{C})$ and often abbreviated to $\mathcal{C}$, and the class of morphisms is written $\mathbf{Mor}(\mathcal{C})$. There are two objects that are associated to every morphism, the source and the target. A *morphism* f with source X and target Y is written $f : X \to Y$. The class of morphisms with source X and target Y is written $\mathbf{Hom}_{\mathcal{C}}(X, Y)$.
The operation that comes with the morphisms are called compositions. The composition of f and g are defined if and only if:

1. The target of f is the source of g

And is denoted $g \circ f$ (or sometimes, simply gf). The source of $g \circ f$ is the source of f and the target of $g \circ f$ is the target of g. These must satisfy:

1. For every object X, there exists a morphism $\mathrm{id}_X : X \to X$ called the identity morphism on X, such that for every morphism $f : X \to Y$ we have $id_Y \circ f = f = f \circ id_X$.
2. $h \circ (g \circ f) = (h \circ g) \circ f$ whenever the operations are defined, that is, when the target of f is the source of g, and the target of g is the source of h.

Example 1. *Concrete Categories*

Set: *Sets and set maps*

2. ***Grp***: *Groups and group homomorphisms*
3. ***Ab***: *Abelian groups and abelian group homomorphisms. This is a subcategory of* ***Grp***.
4. ***Ring***: *Rings with* 1 *and ring homomorphisms*
5. ***Vec***$_k$: *Vector spaces over a field* k *and linear transformations.*
6. ***R-Mod***: *R-modules and R-module homomorphisms.*

HW 2: Group Conjugation

$$\begin{tikzcd} & G/N \arrow[dr, dashed, "\bar{\phi}"] & \\ G \arrow[ur, "\pi"] \arrow[rr, "\phi"'] & & H \end{tikzcd}$$

Figure 1: First Isomorphism Theorem

1 Group Conjugation (Brusell)

1.1 Homomorphisms and the First Isomorphism Theorem

Definition 2: Homomorphisms

A homomorphism $\phi : G \to H$ satisfies $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.
The kernel is a subgroup $N = \ker(\phi) \leq G$ and if $a \in N$ and $b \in G$, then the homomorphism property gives us

$$\phi(bab^{-1}) = \phi(b)e_H\phi(b)^{-1} = e_H.$$

Therefore $a \in N$ implies $bab^{-1} \in N$ for all $b \in G$.
So that $G/N = \{aN : a \in G\}$ form a group called the *quotient group* of G by N.
Any subgroup with this property is called a *normal subgroup*. The canonical map $\pi : G \to G/N$ sending $a \mapsto aN$ is a homomorphism with kernel N and it factors ϕ: Figure 1
The induced map $\overline{\phi} : G/N \to H$, given by $\overline{\phi}(aN) = \phi(a)$, is injective, and so we have an isomorphism

$$\overline{\phi} : G/N \to \phi(G)$$

This is the First Isomorphism Theorem.

Note 2. *The quotient group G/N retains some stucutre of G but is generally a kind of projection of G onto G/N. The quotient group of G/N is isomorphic to some subgroup of $H \leq G$ by the map $\overline{\phi}$, so we can think of a homomorphism as a relation between G and H.*

HW 2: Group Conjugation

Definition 3

1. A homomorphism that is *injective* if it's one-to-one and its kernel is $\{e\}$. An injective homomorphism is called a *monomorphism*.
2. A homomorphism that is surjective if its onto, and is called *epimorphism*.
3. A homomorphism is an isomorphism that is $1-1$ and onto.
4. A homomorphism from G to itself is an *endomorphism*. The set of all such is $\mathrm{End}(G)$.
5. An isomorphism from G to itself is an automorphism. The group of all such is $\mathrm{Aut}(G)$.

1.2 Conjugation

Note 3. *Automorphism on G are a kind of permutation of G that preserves G's group structure, we think of $Aut(G)$ as the symmetry group of G. Conjugation is a kind of symmetry on G.*

Definition 4

Suppose $a \in G$ is an element of G. Conjugation by a is an automorphism on G

$$\begin{aligned}\gamma_a : G &\to G \\ b &\mapsto \gamma_a(b) = aba^{-1}\end{aligned}$$

We'll use the notation

$$\gamma_c \circ \gamma_a = \gamma_{ca} \qquad \gamma_{a^{-1}} = \gamma_a^{-1}$$

Since conjugation is closed under composition and inversion, making the set of conjugation automorphisms into a subgroup of $\mathrm{Aut}(G)$, we'll call these *inner automorphisms* and we have $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

$$\begin{aligned}\gamma : G &\to \mathrm{Aut}(G) \\ a &\mapsto \gamma_a\end{aligned}$$

whose image is $\mathrm{Inn}(G)$ and whose kernel is $Z(G)$ so that $G/Z(G) \simeq \mathrm{Inn}(G)$ by the First Isomorphism Theorem.

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 2: Group Conjugation

1.2.1 Conjugate Elements

Definition 5

Two elements b and c in G are *conjugate* if there's an $a \in G$ such that $c = aba^{-1}$. The elements c in G conjugate to a given b form the conjugacy class $[b] = \{c \in G : c = aba^{-1},\ \text{some } a \in G\}$.

Remark 4. *'Conjugate' is an equivalence relation on G. Thus G is partitioned into conjugacy classes, i.e., G is a disjoint union of conjugacy classes.*

Example 5. *In S_4 the elements $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ are all conjugate, and form the conjugacy class $[(1\ 2)(3\ 4)]$. The partition of S_4 into conjugacy classes is*

$$S_4 = [e]\ \sqcup\ [(1\ 2)]\ \sqcup\ [(1\ 2\ 3)]\ \sqcup\ [(1\ 2)(3\ 4)]\ \sqcup\ [(1\ 2\ 3\ 4)]$$

1.2.2 Conjugate Subgroups

Note 6. *Conjugation is an isomorphism on any group G to itself, it takes subgroups to subgroups. Those subgroups are then isomorphic. We should name those.*

Definition 6

Two subgroups $H, K \leq G$ are *conjugate* if there's an $a \in G$ such that

$$K = aHa^{-1}$$

where $aHa^{-1} = \{aha^{-1} : h \in H\}$.

Example 7. *In S_4 the subgroups $H = \langle(1\ 2\ 3)\rangle$ and $K = \langle(2\ 3\ 4)\rangle$ are conjugate, since, taking $a = (1\ 2\ 3\ 4)$, we compute*

$$(1\ 2\ 3\ 4)H(1\ 2\ 3\ 4)^{-1} = \{e, (2\ 3\ 4), (2\ 4\ 3)\} = K\checkmark$$

Use the conjugation trick in S_4 to simplify these computations.

Example 8. *In D_6 the subgroups $H = \langle r^3, s\rangle = \{e, r^3, s, r^3s\}$ and $K = \langle r^3, r^2s\rangle = \{e, r^3, r^2s, r^5s\}$ are conjugate, since*

$$rHr^{-1} = \{e, r^3, rsr^{-1}, rr^3sr^{-1}\} = \{e, r^3, r^2s, r^5s\} = K\checkmark$$

1.2.3 Normal Subgroups

Note 9. *Conjugation being an automorphism on G means conjugate subgroups of G are isomorphic.*

Definition 7

A subgroup $H \leq G$ is *normal* if $aHa^{-1} = H$ for all $a \in G$. Equivalently, $H \leq G$ is normal if $aH = Ha$ for all $a \in G$. We write $H \lhd G$.

Example 10. *If G is Abelian then any subgroup is normal, because $aHa^{-1} = H$ is guaranteed by the commutativity of the composition law.*

Example 11. *The subgroup $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is normal in S_4. The reason is that we have corralled all of the $(2, 2)$-cycles into one subgroup, and since conjugation preserves cycle type, $K \lhd S_4$.*

Example 12. *The subgroup $N = \langle r^2, s\rangle$ is normal in D_6. This can be checked by laboriously going through the different elements $a \in D_6$ and computing aNa^{-1}, but we'll learn a quicker way later, having to do with the fact that $[D_6 : N] = 2$.*

HW 2: Group Conjugation

1.3 Application to Symmetry

Note 13. *Conjugacy is important in understanding the symmetry of groups, and in particular their internal structure.*

We have that conjugation gives us a map from G to S_X of a structured set X. Then we may define an action

$$G \times X \to X$$

A substructure of X is a structure subset. Structured subsets Y of X have their own orbits inside of X, so that we have induced action:

$$G \times \boldsymbol{orb}(Y) \to \boldsymbol{orb}(Y)$$

Definition 8

Let X be a structured set with symmetry group $G = S_X$. Substructures Y and Z of X are conjugate if they have the same orbit; $Z = a(Y)$ for some $a \in G$.

1.3.1 Stabilizer Subgroups

Definition 9

Let $G = S_X$ as above, and let Y be a substructure of X. The *stabilizer* of Y is the subgroup $G_Y := \{a \in G : a(Y) = Y\}$.

Theorem 14. 1. *We have a $1-1$ correspondence*

$$\begin{aligned} \boldsymbol{orb}(Y) &\iff G/G_Y \qquad \text{(left cosets of } G_Y) \\ a(Y) &\iff aG_Y \end{aligned}$$

In particular, the cardinality of the set of conjugate substructures is $[G : G_Y]$.

2. *The stabilizer of $Z = a(Y)$ is exactly $G_Z = aG_Ya^{-1}$:*

$$\begin{tikzcd} Y \arrow[r, "G_Y"] & Y \arrow[d, "a"] \\ Z \arrow[u, "a^{-1}"] \arrow[r, "G_Z"'] & Z \end{tikzcd}$$

This says that conjugate substructures have conjugate stabilizers and vice versa.

1.3.2 Examples

Example 15. *Let X be the oriented tetrahedron, and label the vertices as $\{Y_1, Y_2, Y_3, Y_4\}$. These vertices are conjugate substructures under the action of S_4 on indices and the rotation group of the sub-structured set X is the group A_4.*

Then by inspection $G_{Y_1} = \langle(2\ 3\ 4)\rangle$. The above theorem says the cosets of G_{Y_1} consists of elements of identical actions on the vertex Y_1. Let's check

$$G_{Y_1} = \{e, (2\ 3\ 4), (2\ 4\ 3)\}(1\ 2\ 3) \qquad G_{Y_1} = \{(1\ 2\ 3), (1\ 2\ 3)(2\ 3\ 4), (1\ 2\ 3)(2\ 4\ 3)\}$$
$$= \{(1\ 2\ 3), (1\ 2)(3\ 4), (1\ 2\ 4)\}$$
$$(1\ 3\ 2)G_{Y_1} = \{(1\ 3\ 2), (1\ 3\ 4), (1\ 3)(2\ 4)\} \quad (1\ 4\ 2)G_{Y_1} = \{(1\ 4\ 2), (1\ 4)(2\ 3), (1\ 4\ 3)\}$$

We see here how every element in a given coset sends Y_1 to the same Y_i. Four cosets, four conjugate substructures. Using the above theorem II, we can also predict the conjugate subgroups of G_{Y_1}. For example $(1\,3\,4)G_{Y_1}(1\,3\,4)^{-1} = G_{(1\ 3\ 4)Y_1(1\ 3\ 4)^{-1}} = G_{Y_3} = \langle(1\,2\,4)\rangle$.

Example 16. *Let X be the non-oriented hexagon, so $G = D_6$ and let $Y = Y_1$ be the horizontal vertex-vertex diagonal. The conjugate substructures are then the other vertex-vertex diagonals, and there are three: $\{Y_1, Y_2, Y_3\}$ (in counterclockwise order). The subgroup preserving Y_1 is $H = \langle r^3, s\rangle = \{e, r^3, s, r^3 s\}$. The corresponding cosets of H are $\{H, rH, r^2 H\}$. Three cosets, three conjugate substructures.*

Notice $H = \langle r^3, s\rangle$ has the conjugate subgroup

$$K = rHr^{-1} = \langle r^3, r^2 s\rangle$$

Check it out, $K = rHr^{-1}$ is the subgroup preserving $Y_2 = r(Y_1)$. This makes sense, because for each $h \in H$ we have $(rhr^{-1})(r(Y_1)) = rh(Y_1) = r(Y_1)$.

HW 2: Group Conjugation

Example 17. *Let X be oriented tetrahedron, $Y = \{Y_1, Y_2, Y_3, Y_4\}$ the vertices, which are all conjugate. Then $G = A_4$ is the symmetry group. Let H_i be the subgroup stabilizing Y_i. Then $H_1 = \langle(2\ 3\ 4)\rangle, [G : H_1] = 4, H_2 = \langle(1\ 2\ 4)\rangle$ and $H_4 = \langle(1\ 2\ 3)\rangle$. For example, since $Y_2 = (1\ 2\ 3)Y_1$, we expect $H_2 = (1\ 2\ 3)H_1(1\ 2\ 3)^{-1}$. Let's check it:*

$$(1\ 2\ 3)H_1(1\ 2\ 3)^{-1} = \{e, (1\ 4\ 3), (1\ 3\ 4)\} = H_2 \checkmark$$

HW 3 Notes: Semidirect Products

2 Semi-direct Products (Brussell)

2.1 Direct Products

Theorem 18 (Direct Products). *Suppose H and K are subgroups of G. Then the map*

$$\mu : H \times K \to G$$

$$(a, b) \mapsto ab$$

is an isomorphism if and only if $H \cap K = \{e\}, HK = G$, and $H, K \lhd G$.

Proof. Suppose μ is an isomorphism. If $a \in H \cap K$ then $(a, a^{-1}) \mapsto e$ and since $(e, e) \mapsto e$ and μ is injective, we must have $a = e$, hence $H \cap K = \{e\}$. Since μ is surjective, $HK = G$. Since isomorphism preserves normality and $H \times \{e\}$ and $\{e\} \times K$ are normal in $H \times K$, H and K are normal in G. For the converse, suppose $H \cap K = \{e\}$, $HK = G$ and $H, K \lhd G$. Since $H, K \lhd G$, the commutator $aba^{-1}b^{-1}$, with $a \in H, b \in K$, is in $H \cap K$, and since $H \cap K = \{e\}$, $ab = ba$. Therefore the elements of H and K commute elementwise, hence $\mu(aa', bb') = aa'bb' = aba'b' = \mu(a, b)\mu(a', b')$, which shows μ is a homomorphism. If $(a, b) \in \ker(\mu)$ then $ab = e$, so $b = a^{-1}$ by uniqueness of inverses, and since a is then in $H \cap K$, we have $a = b = e$. Therefore μ is injective. Since $HK = G$, each $g \in G$ has form $g = ab = \mu(a, b)$ with $a \in H, b \in K$, so μ is surjective, hence an isomorphism. □

Example 19. *Let O_3 be the orthogonal group: 3×3 matrices satisfying $AA^T = I_3$. This condition says that the columns are mutually perpendicular unit vectors. Since an orthogonal matrix takes one orthonormal basis to another, it represented a metric-preserving linear transformation of $\mathbb{R}^3$. Since $\det(AA^T) = (\det(A))^2 = \det(I) = 1, \det(A) = \pm 1$. Thus we have a homomorphism*

$$\det : O_3 \to \{\pm 1\}$$

whose kernel is $SO_3 \lhd O_3$, the group of rotations. The map is onto, so $[O_3 : SO_3] = 2$. We claim:

$$O_3 \simeq SO_3 \times < -I_3 >$$

The reflection $-I_3$ is in $Z(O_3)$, so $< -I_3 > \lhd O_3$. Since $\det(-I_3) = -1$, $SO_3 \cap < -I_3 >= \{I_3\}$. Since $O_3 = SO_3 \sqcup -SO_3$, $O_3 = SO_3 \cdot < -I_3 >$. This proves the claim by our proposition. More generally, if n is odd then $O_n = SO_n \times < -I_n >$. If n is even, this doesn't work!

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 3 Notes: Semidirect Products

2.2 Semi-Direct Products

Definition 10: External Semidirect Product

Suppose N and K are groups, and $\gamma : K \to \mathrm{Aut}(N)$ is a homomorphism, i.e., an action of K on N. The (external) semidirect product $N \rtimes_\gamma K$ of N and K (determined by γ) is the group $(N \times K, *)$, where $(a, b) * (c, d) \equiv (a\gamma_b(c), bd)$.
We say a group G is a *semidirect product* if it is isomorphic to an external semidirect product. We say G is an *internal semidirect product* of N, K if $N \lhd G, K \leq G$ and $G \simeq N \rtimes_\gamma K$, where the action γ is conjugation inside G.

Proposition 20. *$N \rtimes_\gamma K$ is a group with identity (e_N, e_K) and inverses $(a, b)^{-1} = (\gamma_{b^{-1}}(a^{-1}), b^{-1})$.*

Remark 21. *Let $\phi : G \to N \rtimes_\gamma K$. Then G contains subgroups $N' = \phi^{-1}(N \times \{e\})$ and $K' = \phi^{-1}(\{e\} \times K)$ and*

$$\phi(bab^{-1}) = (e, b) * (a, e) * (e, b)^{-1} = (\gamma_b(a), e) = \gamma_b(a)$$

so γ_b becomes conjugation by b in G, whereby G is an internal semidirect product of N' and K'.

Theorem 22. *Suppose $N, K \leq G$ are subgroups such that $N \cap K = \{e\}$, $NK = G$ and $N \lhd G$. Then $G \simeq N \rtimes_\gamma K$ where $\gamma : K \to Aut(N)$ is conjugation inside G.*

Example 23. *The abelian groups of order 8 are C_8, $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$. Determine all nonabelain groups of order 8. We have seen D_4, Q_8, any more? No: Suppose G is nonabelian and $|G| = 8$. Then G has an element ρ of order 4, since all order 2 implies abelian ($(ab)^2 = e \ldots$). Therefore we have a $C_4 \simeq < \rho > \lhd G$. We have $Aut(C_4) = U(4) = \{\pm 1\}$. If G has an element τ of order 2 not in C_4, then there's a map $\gamma : < \tau > \to U(4)$ sending τ to -1, and since $< \rho > \cap < \tau > = \{e\}$, we get*

$$G = C_4 \rtimes_\gamma C_2 = D_4.$$

If G doesn't have such an element, then it has an element σ of order 4 not in $C_4 = < \rho >$, and the map $< \sigma > \to U(4)$ must take σ to -1, since G is nonabelian. Thus $\sigma\rho\sigma^{-1} = \rho^{-1}$, *hence* $G =< \rho, \sigma : |\rho| = |\sigma| = 4, \sigma\rho\sigma^{-1} = \rho^{-1} >= Q_8$. *Note:* Q_8 *isn't a semidirect product!*

2.3 Automorphisms of D_n

Proposition 24. *Suppose* $n \geq 3$. *Then* $\phi \in Aut(D_n)$ *if and only if* $\phi(r) = r^a$ *and* $\phi(s) = r^b s$ *for* $a : \gcd(a, n) = 1$, *and any* b. *The group* $Inn(D_n)$ *is defined by* $(a, b) \in \{(\pm 1, 2i) : 0 \leq i \leq n-1\}$

Proof. Suppose $\phi \in \mathrm{Aut}(D_n)$. Since $n \geq 3$, $< r >$ is the unique cyclic subgroup of D_n of order n, therefore it's characteristic, hence $\phi(r) = r^a$ for some a, and since $|\phi(r)| = n$ we have $\gcd(a, n) = 1$. Since ϕ is a bijection, $\phi(s)$ must be a reflection, hence $\phi(s) = r^b s$ for some b. Conversely, it's not hard to check that such a function defines an automorphism. It's also not hard to see that ϕ_{r^i} by r is defined by $a = 1$ and $b = 2i$ and $\phi_{r^i s}$ is defined by $a = -1$ and $b = 2i$. ☐

3 IV.1. Groups, Second Encounter: The Conjugation Action (Aluffi)

3.1 Actions of Groups on Sets, Reminder

Proposition 25 (Proposition II.9.9)**.** *Every transitive (left-)action of a group* G *on a set* S *is, up to a natural notion of isomorphism, 'left-multiplication on the set of left-cosets* G/H*'. Where* $H = Stab_G(a)$ *of any* $a \in S$.

Corollary 26. *The number of elements in a finite orbit* $O = [G : Stab_a(G)]$ *for any* $a \in O$.

In particular, $|O|$ *divides* $|G|$.

Remark 27 (Fixed Points)**.** *Let* $Z = \{a \in S | (\forall g \in G) : ga = a\}$.

That is $a \in Z \iff G_a = G$; *that is,* $a \in Z$ *if and only if the orbit of* a *is 'trivial'.*

HW 3 Notes: Semidirect Products

Proposition 28 (Proposition 1.1)**.** *Let S be a finite set and let G be a group acting on S. With notation as above,*

$$|S| = |Z| + \sum_{a\in A}[G : G_a],$$

where $A \subseteq S$ has exactly one element for each nontrivial orbit of the action.

Proof. The orbits form a partition of S, and Z collects the trivial orbits; hence:

$$|S| = |Z| + \sum_{a\in A}|O_a|,$$

where O_a denotes the orbit of a. By Proposition II.9.9, the order $|O_a|$ equals the index of the stabilizer of a, yielding the statement. □

Definition 11: Definition 1.2.

A $p-$group is a finite group whose order is a power of a prime integer p.

Corollary 29 (Corollary 1.3.)**.** *Let G be a $p-$Group acting on a finite set S, and let Z be the fixed point set of the action. Then*

$$|Z| \equiv |S| \mod p.$$

Proof. Indeed, each summand $[G : G_a]$ in proposition 1.1 is a power of p larger than 1; hence it's $0 \mod p$. □

3.2 Center, Centralizer, Conjugacy Classes

Remark 30. *Recall that a group G has 2 actions on itself, left multiplication and conjugation. With conjugation being defined:*

$$\rho : G \times G \to G$$

$$\rho(g, a) = gag^{-1}.$$

This is equivalent to a homomorphism:

$$\sigma : G \to S_G$$

from G to the permutation group of G.

Definition 12

The center of G, denoted $Z(G)$, is the subgroup $\ker(\sigma)$ of G.

$$Z(G) = \{g \in G | (\forall a \in G) : ga = ag\}$$

Theorem 31. *Suppose $Z(G)$ is the center of G. Then*

1. $Z(G) \lhd G$
2. *G is commutative if and only if $Z(G) = G$*
3. *G is commutative if and only if conjugation is the trivial action on G.*

Lemma 32 (Lemma 1.5.)**.** *Let G be a finite group, and assume $G/Z(G)$ is cyclic. Then G is commutative (and hence $G/Z(G) = \{e\}$).*

Proof. As $G/Z(G)$ is cyclic, there exists an element $g \in G$ such that the class $gZ(G)$ generates $G/Z(G)$. Then $\forall a \in G$:

$$aZ(G) = (gZ(G))^r,$$

for some $r \in \mathbb{Z}$; that is, there's an element $z \in Z(G)$ of the center such that $a = g^r z$.
If now $a, b \in G$, use this fact to write

$$a = g^r z \qquad b = g^s w$$

for some $s \in \mathbb{Z}$ and $w \in Z(G)$; but then

$$ab = (g^r z)(g^s w) = g^{r+s} zw = (g^s w)(g^r z) = ba,$$

where we have used the fact that z and w commute with every element of G. As a and b are arbitrary, this proves that G is commutative. □

Definition 13: Centralizer

The **centralizer** (or **normalizer**) $Z_G(a)$ of $a \in G$ is its stabilizer under conjugation.

HW 3 Notes: Semidirect Products

Corollary 33.

$$Z(G) = \bigcap_{a \in G} Z_G(a).$$

Definition 14: The Conjugacy Class

The conjugacy class of $a \in G$ is the orbit $[a]$ of a under the conjugation action. Two elements, $a, b \in G$ are conjugate if they belong to the same conjugacy class.

Note 34. $[a] = \{a\}$ *if and only if* $gag^{-1} = a$ *for all* $g \in G$*; that is, if and only if* $ga = ag$ *for all* $g \in G$*; that is, if and only if* $a \in Z(G)$

3.3 The Class Formula

Proposition 35 (Class Formula)**.** *Let* G *be a finite group. Then*

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z(a)],$$

where $A \subseteq G$ *is a set containing one representative for each nontrivial conjugacy class in* G*.*

Proof. The set of fixed points is $Z(G)$, and the stabilizer of a is the centralizer $Z(a)$; apply Proposition 1.1. $\square$

Corollary 36 (1.9)**.** *Let* G *be a nontrivial* $p-$*group. Then* G *has a nontrivial center.*

Proof. Since $|Z(G)| \equiv |G| \mod p$ and $|G| > 1$ is a power of p, necessarily $|Z(G)|$ is a multiple of p. As $Z(G) \neq \emptyset$ (since $e_G \in Z(G)$), this implies $|Z(G)| \geq p$. $\square$

Remark 37. *It follows immediately from Corollary 1.9 and Lemma 1.5 that if* p *is prime, then every group of order* p^2 *is commutative.*

HW 3 Notes: Semidirect Products

Example 38. *Consider a group G of order 6; what are the possibilities for its class formula?*

Solution. If G is commutative, then the class formula will tell us very little:

$$6 = 6.$$

If G is not commutative, then its center must be trivial (by Lagrange's Theorem and Lemma 1.5); so the class formula is $6 = 1 + \dots$, where $\dots$ collects the sizes of the nontrivial conjugacy classes. But each of these summands must be larger than 1, smaller than 6, and must divide 6; that is, there are no choices:

$$6 = 1 + 2 + 3,$$

is the only possibility. The reader should check that this is the class formula for S_3; and in fact, S_3 is the only non-commutative group of order 6 up to isomorphism. □

Remark 39. *Another application of this is that normal subgroups must be unions of conjugacy classes: because if H is a normal subgroup, $a \in H$ and $b = gag^{-1}$ is conjugate to a then:*

$$b \in gHg^{-1} = H.$$

To apply this to $|G| = 6$, every subgroup of a group must contain the identity and its size must divide the order of the group; it follows that a normal subgroup of a non-commutative group of order 6 cannot have order 2, since 2 cannot be written as sums of orders of conjugacy classes (including the class of the identity).

3.4 Conjugation of Subsets and Subgroups

Remark 40. *We can use conjugation to act on the power set of a group G : If $A \subseteq G$ is a subset and $g \in G$, the conjugate of A is a subset gAg^{-1}. By cancellation, the conjugation map $a \mapsto gag^{-1}$ is a bijection between A and gAg^{-1}.*

HW 3 Notes: Semidirect Products

Definition 15: Normalizer

The *normalizer* $N_G(A)$ of A is its stabilizer under conjugation. The *centralizer* of A is the subgroup $Z_G(A) \subseteq N_G(A)$ fixing each element of A.

$$g \in N_G(A) \iff gAg^{-1} = A \text{ and } g \in Z_G(A) \iff \forall a \in A, gag^{-1} = a.$$

If H is a subgroup of G, every conjugate gHg^{-1} of H is also a subgroup of G; conjugate subgroups have the same order.

Remark 41 (1.12)**.** *The definition implies immediately that $H \subseteq N_G(H)$ and that H is normal in G if and only if $N_G(H) = G$. More generally, the normalizer $N_G(H)$ of H in G is (clearly) the largest subgroup of G in which H is normal.*

Lemma 42 (1.13)**.** *Let $H \subseteq G$ be a subgroup. Then (if finite) the number of subgroups conjugate to H equals the index $[G : N_G(H)]$ of the normalizer of H in G.*

Proof. This again is an immediate consequence of Prop II.9.9. □

Corollary 43 (1.14)**.** *If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite and divides $[G : H]$.*

Proof.

$$[G : H] = [G : N_G(H)] \cdot [N_G(H) : H],$$

by $II.8.5$. □

Note 44. *Conjugation forms an automorphism of K; that is conjugation is a bijection and a homomorphism:*

$$(gk_1g^{-1})(gk_2g^{-1}) = gk_1k_2g^{-1}.$$

This gives us a set function;

$$\gamma : H \to Aut_{Grp}(K).$$

HW 3 Notes: Semidirect Products

4 IV.5. Products of Groups

4.1 The Direct Product

Definition 16

The direct product of two groups H, K is the group supported on the set $H \times K$, with operations defined by component-wise.
You can check that the direct product satisfies the universal property defining products in the category **Grp**.

Note 45. *Occasionally, we can realize $N \times H$ as a subgroup of G. Recall that if one of the subgroups is normal, then the subset NH of G is in fact a subgroup of G. The relation NH and $N \times H$ depends on how N and H intersect in G, so we look at this intersection.*

The 'commutator' $[A, B]$ of two subsets A, B of G is the subgroup generated by all the commutators $[a, b] = aba^{-1}b^{-1}$ with $a \in A, b \in B$.

Lemma 46 (5.1)**.** *Let N, H be normal subgroups of a group G. Then*

$$[N, H] \subseteq N \cap H.$$

Proof. It suffices to verify this on generators; that is, it suffices to check that:

$$[n, h] = b(hn^{-1}h^{-1}) = (nhn^{-1})h^{-1} \in N \cap H$$

for all $n \in N, h \in H$. But this first expression and the normality of N shows that $[n, h] \in N$; the second expression and the normality of H shows that $[n, H] \in H$. $\square$

Corollary 47 (5.2)**.** *Let N, H be normal subgroups of a group G. Assume $N \cap H = \{e\}$. Then N, H commute with each other:*

$$(\forall n \in N)(\forall h \in H) \qquad nh = hn.$$

Proof. By Lemma 5.1, $[N, H] = \{e\}$ if $N \cap H = \{e\}$; the result follows immediately. $\square$

Name: Joseph McGuire

HW 3 Notes: Semidirect Products

Proposition 48 (5.3)**.** *Let N, H be normal subgroups of a group G, such that $N \cap H = \{e\}$. Then $NH \simeq N \times H$.*

Proof. Consider the function
$$\phi : N \times H \to NH$$
defined by $\phi(n, h) = nh$. Under the stated hypothesis, ϕ is a group homomorphism: indeed
$$\begin{aligned}\phi((n_1, h_1) \cdot (n_2, h_2)) &= \phi((n_1 n_2, h_1 h_2)) \\ &= n_1 n_2 h_1 h_2 \\ &= n_1 h_1 n_2 h_2\end{aligned}$$
since N, H commute by Corollary 5.2
$$= \phi((n_1, h_1)) \cdot \phi((n_2, h_2)).$$
The homomorphism ϕ is surjective by definition of NH. To verify it's injective, consider its kernel:
$$\ker(\phi) = \{(n, h) \in N \times H | nh = e\}.$$
If $nh = e$, then $n \in N$ and $n = h^{-1} \in H$; thus $n = e$ since $N \cap H = \{e\}$. Using the same token for h, we conclude that $h = e$; hence $(n, h) =$ the identity in $N \times H$, proving ϕ is injective.

Thus ϕ is an isomorphism, as needed. □

Remark 49 (5.4)**.** *This result gives an alternative argument for the proof of Claim 2.16: if $|G| = pq$, with $p < q$ prime integers, and G contains normal subgroups H and K of order p and q, respectively (as is the case if $q \equiv 1 \mod p$, by Sylow), then $H \cap K = \{e\}$ necessarily, and then Prop.5.3. shows $HK \simeq H \times K$. As $|HK| = |G| = pq$, this proves $G \simeq H \times K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Finally, $(1, 1)$ has order pq in this group so G is cyclic, with the same conclusion we have in Claim 2.16. (Claim 2.16: Assume $p < q$ are prime integers and $q \equiv 1 \mod p$. Let G be a group of order pq. Then G is cyclic.)*

4.2 Exact Sequences of Groups; Extension Problem

Note 50. *The condition that $H \lhd G$ is necessary for Prop 5.3. An example of why it's necessary is $N = \langle(1\ 2\ 3)\rangle$ and $H = \langle(1\ 2)\rangle$, where $N \lhd S_3$ and $NH = S_3$ and $N \cap H = \{(1)\}$, but $NH \not\simeq N \times H$.*

HW 3 Notes: Semidirect Products

That is, we want weaker conditions on H.

Definition 17: Short Exact Sequence

In a sequence of groups and group homomorphisms, a *short exact sequence*:

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1,$$

where ψ is surjective and φ identifies N with $\ker \psi$. In other words (by the first isomorphism theorem), use φ to identify N with a subgroup of G; then the sequence is exact if $N \lhd G$ and ψ induces an isomorphism $G/N \to H$.

Note 51. *If G, N, H are abelian, then this notion (of short exact sequences) matches precisely the notion of short exact sequences of abelian group from III.7.1; a notational difference is that here the trivial group is denote 1 rather than $'0'$.*

There's always an exact sequence

$$1 \longrightarrow N \longrightarrow N \times H \longrightarrow H \longrightarrow 1:$$

maps $n \in N$ to (n, e_H) and $(n, h) \in N \times H$ to h. However, in the special case of:

$$1 \longrightarrow C_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1,$$

yet $S_3 \not\simeq C_3 \times C_2$.

Definition 18

Let N, H be groups. A group G is an *extension* of H by N if there's an exact sequence of groups

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1.$$

Note 52. *The extension problem aims to describe all extension of two given groups, up to isomorphism. For example, there are two extensions of C_2 by C_3: namely $C_6 \simeq C_3 \times C_2$ and S_3; we'll see that there are no other extensions.*

The extension problem is the 'second half' of the classification problem: the first half being to determine all simple groups, and the second half consists of figuring out how these can be put together to construct any group.

HW 3 Notes: Semidirect Products

Example 53. *For example, if*

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq G_3 \supsetneq G_4 = \{e\}$$

is a composition series, with (simple) quotients $H_i = G_i/G_{i+1}$, then G is an extension of H_0 by an extension of H_1 by an extension of H_2 by H_3: knowing the composition factors of G and the extension process, it should in principle by possible to reconstruct G.

Definition 19: Split

An exact sequence of groups

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

(or corresponding extension) is said to *split* if H may be identified with a subgroup of G, so that $N \cap H = \{e\}$.

Note 54. *For Abelian groups, every split extension (according to Definition 5.6) is in fact a direct product.*

Lemma 55 (5.7)**.** *Let N be a normal subgroup of a group G, and let H be a subgroup of G such that $G = NH$ and $N \cap H = \{e\}$.*

Then G is a split extension of H and N.

Proof. We have to construct an exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1;$$

we let $N \to G$ be the inclusion map, and we prove that $G/N \simeq H$. For this, consider the composition

$$\alpha : H \to G \to G/N.$$

Then α is surjective: indeed, since $G = NH$, $\forall g \in G$ we have $g = nh$ for some $n \in N$ and $h \in H$, and then

$$gN = nhN = h(h^{-1}nh)N = hN = \alpha(h).$$

Further, $\ker \alpha = \{h \in H | hN = N\} = N \cap H = \{e\}$; therefore α is also injective, as needed. $\square$

HW 3 Notes: Semidirect Products

4.3 Internal / Semidirect Products

Note 56. *If both N and H are normal and $N \cap H = \{e\}$, then N and H commute with each other (by 5.2/5.3).*

This causes the extension NH to be trivial.

Now if N is normal, then every subgroup $H \leq G$ acts on N by conjugation and conjugation determines a homomorphism

$$\gamma : H \to Aut_{\mathbf{Grp}}(N), \qquad h \mapsto \gamma_h.$$

(That is, $h \in H$ the automorphism γ_h is defined by $\gamma_h(n) := hnh^{-1}$.) N and H commute and $N \cap H = \{e\}$ if and only if γ is trivial.

That is, if $N \lhd G$ and $H \leq G$, $N \cap H = \{e\}$ and $G = NH$, then the extension G of H by N may be reconstructed from the conjugation action $\gamma : H \to Aut_{\mathbf{Grp}}(N)$. Note that:

$$(\forall n_1, n_2 \in N), (\forall h_1, h_2 \in H) \qquad n_1 h_1 n_2 h_2 = (n_1(h_1 n_2 h_1^{-1}))(h_1 h_2).$$

We say that the conjugation action of H on N, then we can recover the operation in G from this information and from the operations in N and H.

We'll use this to define an arbitrary homomorphism between any two groups N, H and an arbitrary homomorphism

$$\theta : H \to Aut_{\mathbf{Grp}}(N), \qquad h \mapsto \theta_h.$$

Define $\bullet_\theta$ on the set $N \times H$ as follows: for $n_1, n_2 \in N$ and $h_1, h_2 \in H$, let

$$(n_1, h_1) \bullet_\theta (n_2, h_2) := (n_1 \theta_{h_1}(n_2), h_1 h_2).$$

Lemma 57 (5.8)**.** *The resulting structure $(N \times H, \bullet_\theta)$ is a group, with identity (e_N, e_H).*

Proof. Do it yourself. Inverses exists because:

$$(n_1, h_1) \bullet_\theta (\theta_{h_1^{-1}}(n_1^{-1}, h_1^{-1}) = (n_1 \theta_{h_1}(\theta_{h_1^{-1}}(n_1^{-1}), h_1 h_1^{-1}) = (n_1 n_1^{-1}, e_H) = (e_N, e_H)$$

and similarly in the reverse order. □

Definition 20: 5.9

The group $(N \times H, \bullet_\theta)$ is a semidirect product of N and H and is denoted by $N \rtimes_\theta H$.

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 3 Notes: Semidirect Products

Proposition 58 (5.10)**.** *Let N, H be groups and let $\theta : H \to Aut_{\mathbf{Grp}}(N)$ be a homomorphism; let $G = N \rtimes_\theta H$ be the corresponding semidirect product. Then*

- *G contains isomorphic copies of N and H;*
- *The natural projection $G \to H$ is a surjective homomorphism, with kernel N; thus $N \lhd G$ and the sequence*

$$1 \longrightarrow N \longrightarrow N \rtimes_\theta H \longrightarrow H \longrightarrow 1$$

  is (split) exact;
- *$N \cap H = \{e_G\}$;*
- *$G = NH$;*
- *the homomorphism θ is realized by conjugation in G: that is, for $h \in H$ and $n \in N$ we have*

$$\theta_h(n) = hnh^{-1}$$

  in G

Proof. The functions $N \to G, H \to G$ defined for $n \in N$, $h \in H$ by

$$n \mapsto (n, e_H) \qquad h \mapsto (e_N, h)$$

are manifestly injective homomorphisms, allowing us to identify N, H with corresponding subgroups of G. It's clear that $N \cap H = \{(e_N, e_H)\} = \{e_G\}$, and

$$(n, e_H) \bullet_\theta (e_N, h) = (n, h)$$

shows that $G = NH$.

The projection $G \to H$ defined by

$$(n, h) \mapsto h$$

is a surjective homomorphism, with kernel N; therefore $N \lhd G$. Finally,

$$(e_N, h) \bullet_\theta (n, e_H) \bullet_\theta (e_N, h)^{-1} = (\theta_h(n), h) \bullet_\theta (e_N, h^{-1}) = (\theta_h(n), e_H),$$

as claimed in the last point. $\square$

HW 3 Notes: Semidirect Products

Proposition 59 (5.11)**.** *Let N, H be subgroups of a group G, with N normal in G. Assume that $N \cap H = \{e\}$, and $G = NH$. Let $\gamma : H \to Aut_{\mathbf{Grp}}(N)$ be defined by conjugation: for $h \in H, n \in N$,*

$$\gamma_h(n) = hnh^{-1}.$$

Then $G \simeq N \rtimes_\gamma H$.

Proof. Define a function

$$\gamma : N \rtimes_\gamma H \to G$$

by $\varphi(n, h) = nh$; this is clearly a bijection. We need to verify that φ is a homomorphism, and indeed $(\forall n \in N), (\forall h \in H)$:

$$\begin{aligned}\varphi((n_1, h_1) \bullet_\gamma (n_2, h_2)) &= \varphi((n_1\gamma_{h_1}(n_2), h_1h_2)) \\ &= \varphi((n_1(h_1n_2h_1^{-1}), h_1h_2)) \\ &= n_1h_1n_2(h_1^{-1}h_1h_2) = (n_1h_1)(n_2h_2) \\ &= \varphi((n_1, h_1))\varphi((n_2, h_2))\end{aligned}$$

as needed. □

Remark 60 (5.12)**.** *If N and H commute, then the conjugation action of H on H is trivial; therefore, γ is the trivial map, and the semidirect product $N \rtimes_\gamma H$ is the direct product $N \times H$. Thus Prop 5.11. recovers the result of Prop 5.3 in this case.*

Example 61 (5.13)**.** *The automorphism group of C_3 is isomorphic to the cyclic group C_2: If $C_3 = \{e, y, y^2\}$, then the two automorphisms of C_3 are:*

$$id : \begin{cases} e \mapsto e, \\ y \mapsto y, \\ y^2 \mapsto y^2, \end{cases} \qquad \sigma : \begin{cases} e \mapsto e, \\ y \mapsto y^2, \\ y^2 \mapsto y. \end{cases}$$

Therefore, there are two homomorphisms $C_2 \to Aut_{\mathbf{Grp}}(C_3)$: the trivial map and the isomorphism sending the identity to id and the non-identity element to σ. The semidirect product corresponding to the trivial map is the direct product $C_3 \times C_2 \simeq C_6$; the other semidirect product $C_3 \rtimes C_2$ is isomorphic to S_3. This can of course be checked by hand; but it also follows immediately from Prop 5.11, since $N = \langle(1\ 2\ 3)\rangle, H = \langle(1\ 2)\rangle \subseteq S_3$ satisfying the hypotheses of this result.

HW 3 Notes: Semidirect Products

Note 62. *Using this all groups of order pq, for $p < q$ primes; the reader should show that if $q \equiv 1 \mod p$, then there's exactly one such non-commutative group up to isomorphism.*

Using semidirect products to classify groups of small order: if a nontrivial normal subgroup N is found (usually by Sylow's theorems), with some luck the classification is reduced to the study of possible homomorphisms from known groups to $Aut_{\mathbf{Grp}}(N)$ and can be carried out.

HW 4 Notes: Sylow Theorems

5 Arithmetic Structure of Groups: Handout

5.1 Class Equation

Theorem 63 (Basic Group Theorem). *If G is a finite group and $a \in G$ such that $|a| = n$, where n is a natural number, then $n \Big| |G|$.*

Theorem 64 (Class Equation). *Let G be a group. Then*

$$|G| = \sum_{[x]:x\in G} [G : C(x)] = |Z(G)| + \sum_{[x]\neq 1} [G : C(x)].$$

Example 65 (Class Equations).

1. *If G is abelian of order n, then $G = Z(G)$, so that the class equation of G is $|G| = n$.*
2. *For D_4 we get $|D_4| = 2 + 2 + 2 + 2$.*
3. *For A_4 we get $|A_4| = 1 + 3 + 4 + 4$.*

5.2 Application to p-Groups

Definition 21: Solvable Groups

A group G is *solvable* if it admits a chain of subgroups, each normal in the next, and such that the successive quotient groups are abelian.
Thus G is solvable there is a ”normal series”

$$(e) = N_{d+1} \lhd N_d \lhd N_{d-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G,$$

such that each N_i/N_{i+1} is abelian for each i.

Proposition 66 (Solvable Criterion). *If $N \leq G$ is a normal subgroup, then G is solvable if and only if N and G/N are both solvable.*

HW 4 Notes: Sylow Theorems

Definition 22: The Derived Series

Since the commutator subgroup of any group is normal and produces the largest abelian quotient, $G^{(1)} \leq N_1, G^{(2)} \leq N_1^{(1)} \leq N_2$, and in general $G^{(i)} \leq N_i$.
It follows that G is solvable if and only if $G^{(n)} = (e)$ for some n. The series of derived subgroups of $G^{(i)}$ is called the *derived series.*

Theorem 67 (Prime Power $\implies$ Solvable Groups). *Suppose p is prime and G is a $p-$group; that is, $|G| = p^n$ for some $n \geq 1$. Then:*

1. *$Z(G) \neq \{e\}$. In particular, G has a nontrivial normal subgroup.*
2. *G is solvable.*

Proof. To prove (1) we use the class equation. [We have that $Z(G) \lhd G$ always and any normal subgroup is the union of conjugacy classes in G. Not clear how this follows, ask Brussell about this...]

To prove (2), induct on the exponent n ($n = 1$ is trivial, that's your base case), using that G is solvable if and only if N and G/N are solvable. Since $(e) \neq Z(G) \lhd G$, $G/Z(G)$ is solvable by induction. Since $Z(G)$ is also solvable, since it's abelian, G is solvable. □

Lemma 68 (Fixed Point Lemma). *Suppose G is a finite $p-$group, and G acts on a finite set X. Then $|X| = |X^G|(\mod p)$. [Note that X^G are the fixed points of X under all the actions of G.]*

Proof. We have

$$|X| = \sum_{X/G} |\mathbf{orb}(x)| = \sum_{X/G} [G : G_x] = |X^G| + \sum_{\mathbf{orb}(x) \neq \{x\}} [G : G_x],$$

[where the first equality comes from ??, the second from coset correspondence theorem, the last just from the definition of $[G : G_x]$.] and the last sum is $0 \mod p$. [Because] □

Proposition 69. *If G is a $p-$group and $(e) \neq H \leq G$, then $H \cap Z(G) \neq (e)$.*

Proof. Let G be a $p-$group and $(e) \neq H \leq G$; that is, for some prime p and $n \geq 1$, we have $|G| = p^n$.

HW 4 Notes: Sylow Theorems

Since $(e) \neq H \leq G$, we have that $|H| = p^m$ for some $1 \leq m \leq n$. Since H and $Z(G)$ are both subgroups of G, $H \cap Z(G)$ is a subgroup of G. Such that $|H \cap Z(G)|$ divides both $|H| = p^m$ and $|Z(G)|$.

□

5.3 Cauchy's Theorem

Theorem 70 (Cauchy's Theorem)**.** *Suppose G is a finite group of order n and p is a prime that divides n. Then G contains an element of order p.*

Proof. We follow McKay's proof. Let $X = \{(a_1, \dots, a_p) : a_i \in G, a_1 \dots a_p = e\}$. Then $|X| = n^{p-1}$ (we can pick the 1st $p-1$ elements arbitrarily), so $|X| = 0 \mod p$. The cyclic group $C_p =< (1\ 2\ \dots\ p) >\leq S_p$ acts on X by permuting the entries. Well defined: If $a_1 \dots a_p = e$ then $(a_2 \dots a_p)a_1 = e$, since $a_1 = (a_2 \dots a_p)^{-1}$. Look:

$$X^{C_p} = \{(a, a, \dots, a) : a^p = e\}.$$

By Lemma 68, $|X| = |X^{C_p}|(\mod p)$, hence $|X^{C_p}| = 0(\mod p)$. Look:

$$X^{C_p} \neq,$$

since it contains $(e, \dots, e)$. Therefore there exists $a \neq e$ in G such that $a^p = e$, hence $|a| = p$ (since $a^p = e \implies |a|$ divides p). □

Example 71 (Applications of Cauchy's Theorem)**.**

1. *Groups of order* 15.
2. *Groups of order pq. Suppose p, q are primes and G is a group of order pq. Then we have cyclic groups C_p and C_q by Cauchy's Theorem, which are the same if $p = q$. We can show that if G is abelian, then $G \simeq C_p \times C_p$ or C_{pq}, and if G is nonabelian then there's a group of order pq if and only if $p \Big| (q-1)$, and that group is unique (up to isomorphism).*

5.4 Sylow Theorems

Lemma 72. *If H is a p-subgroup of a finite group G, then $[N_G(H) : H] = [G : H]$* $\mod p$. *In particular, if p divides $[G : H]$, then p divides $[N_G(H) : H]$.*

HW 4 Notes: Sylow Theorems

Proof. We use left multiplication action $H \times K \to X$, where $X = G/H$ (left cosets). Compute $X^H = \{sH : asH = sH \ \forall a \in H\} = \{sH : s \in N_G(H)\}$. Therefore $|X^H| = [N_G(H) : H]$. By Lemma 68, $[N_G(H) : H] = [G : H] \mod p$. The last statement is immediate. □

Theorem 73 (Sylow 1)**.** *Suppose G is a group of order $p^n m$, where p doesn't divide m, and $n \geq 1$. Then G has a subgroup of order p^n, and every $p-$subgroup of G is contained in a subgroup of order p^n.*

Proof. (Base Case) The case of $n = 1$ is Cauchy's theorem. [That is $|G| = pm$, and $p \not| m$. Then G contains an element of order p. In other words, G contains the subgroup $< a > \leq G$ where $|a| = p$. (Second part is unclear)]

(Inductive Hypothesis) Assume the statement is true for $n - 1$, $n > 1$, and let H be a $p-$subgroup, which exists by Cauchy. If p doesn't divide $[G : H]$ we are done. Otherwise p divides $[N_G(H) : H]$ by Lemma 72. Since $H \lhd N_G(H)$, $N_G(H)/H$ is a group whose order has $p-$value at most $n - 1$. By induction and Homomorphism Correspondence, we have $H \leq K \leq N_G(H)$, with K a (nontrivial) $p-$subgroup of G, and $p \not| [N_G(H) : K]$. If $p \not| [G : K]$, then we are done. Otherwise replace H with K and repeat. Since G is finite, the argument must terminate, and we obtain a subgroup P of order p^n containing H. □

Definition 23: Sylow p-Subgroups

We call these subgroups of order p^n the Sylow $p-$subgroups of G, and denote the set of all such $Syl_p(G)$. The 1st Sylow theorem says that $Syl_p(G)$ is nonempty.

Proposition 74 (p-groups are Solvable)**.** *If a $p-$group P has order p^n then P has a solvable series*

$$(e) = P_0 \lhd P_1 \lhd \ldots \lhd P_n = P,$$

with P_{i+1}/P_i cyclic of order p.

Proof Sketch. To prove it, use nontrivality of center plus induction (type II) on n. $Z(P) \neq \{e\}$ since P is a $p-$group, and $Z(P)$ has such a series: Choose $a \in Z(P)$ of order p, set $P_0 =< a >$, then $P_0 \lhd Z(P)$ since $Z(P)$ is abelian. By induction $Z(P)$ has the desired series. By induction $P/Z(P)$ has the desired series. Patching together by applying 3rd Isomorphism Theorem. □

HW 4 Notes: Sylow Theorems

Example 75 (Example of Sylow p-Subgroups)**.** *Let $G = A_5$, and write out the Sylow $p-$subgroups for $p = 2, 3, 5$. For $G = S_5$, find a Sylow 2-subgroup (how many groups of order 8?)*

Theorem 76 (Sylow 2)**.** *Let G be a group of order n divisible by a prime p. Then all Sylow $p-$subgroups are conjugate.*

Proof. Suppose $P \in Syl_p(G)$, which is nonempty by 73, and let $X = G/P$ (left cosets). If $P' \in Syl_p(G)$ then we have left multiplication action $P' \times X \to X$, and $sP \in X^{P'}$ if and only if $s^{-1}P's = P$ (compute directly). But $|X^{P'}| \neq 0 \mod p$ by Lemma 68. Therefore $X^{P'} \neq$, hence P' and P are conjugate. □

Theorem 77 (Sylow 3)**.** *Let G be a group of order n divisible by a prime p, $P \in Syl_p(G)$, and let $n_p = |Syl_p(G)|$. Then*

1. *$n_p = [G : N_G(P)]$. In particular, n_p divides $[G : P]$.*
2. *$n_p \equiv 1 \mod p$.*

Proof. The 1st statement follows from the orbit-stabilizer theorem, in light of 2nd Sylow. For the 2nd statement, let $X = Syl_p(G)$. We have conjugation action $P \times X \to X$ and $P' \in X^P$ if and only if $P \leq N_G(P')$. But if $P \leq N_G(P')$, then both P and P' are Sylow $p-$subgroups of $N_G(P')$, hence they are conjugate inside $N_G(P')$, by the 2nd Sylow. But $P' \lhd N_G(P')$! So $P' = P$, hence $|X^P = 1$. By Lemma 68, $|X| = 1 \mod p$, as desired. □

Proposition 78 (Corollaries to Sylow Theorems)**.**

1. *For each n_p we have a homomorphism $\phi_p : G \to S_{n_p}$, which is nontrivial by 76. This is used to investigate the normal subgroups of G, and classify simple groups of small order.*
2. *Use 73 in number theory to scalar extend by prime-to-p degree.*

Proposition 79. *Determine all groups of order 12.*

HW 4 Notes: Sylow Theorems

6 The Sylow Theorems (Aluffi)

6.1 Cauchy's Theorem

Theorem 80 (Lagrange's Theorem). *If p is a prime and p^k divides $|G|$, then G contains a subgroup of order p^k.*

Theorem 81 (Cauchy's Theorem). *Let G be a finite group, and let p be a prime divisor of $|G|$. Then G contains an element of order p.*

Proof. Consider the set S of $p-$tuples of elements of G:

$$\{a_1, \dots, a_p\},$$

such that $a_1 \dots a_p = e$. We claim that $|S = |G|^{p-1}$: indeed, once $a_1, \dots, a_{p-1}$ are chosen (arbitrarily), then a_p is determined as it's the inverse of $a_1 \dots a_{p-1}$.

Therefore, p divides the order of S as it divides the order of G.

Also note that if $a_1 \dots a_p = e$,then

$$a_2 \dots a_p a_1 = e,$$

(even if G is noncommutative): because if a_1 is a left-inverse to $a_2 \dots a_p$, then it's also a right-inverse to it.

Therefore, we may act with the group $\mathbb{Z}/p\mathbb{Z}$ on S: given $[m] \in \mathbb{Z}/p\mathbb{Z}$, with $0 \leq m < p$, act by $[m]$ on

$$\{a_1, \dots, a_p\}$$

by sending it to

$$\{a_{m+1}, \dots, a_p, a_1, \dots, a_m\} :$$

as we just observed, this is still an element of S.

Now Corollary 1.3 implies

$$|Z| \equiv |S| \equiv 0 \mod p,$$

where Z is the set of fixed poins of this action. Fixed points are $p-$tuples of the form

$$\{a, \dots, a\}; \tag{1}$$

and note that $Z \neq$, since $\{e, \dots, e\} \in Z$. Since $p \geq 2$ and p divides $|Z|$, we conclude that $|Z| > 1$; therefore there exists some elements in Z of the form (1), with $a \neq e$.

This says that there exists an element $a \in G$, $a \neq e$, such that $a^p = e$, proving the statement. $\square$

HW 4 Notes: Sylow Theorems

Proposition 82. *Let G be a finite group, let p be a prime divisor of $|G|$, and let N be the number of cyclic subgroups of G of order p. Then $N \equiv 1 \mod p$.*

Remark 83. *82 implies that if there's only 1 cyclic subgroup H of order p, then that subgroup H must be normal.*

Definition 24

A group G is *simple* if its only normal subgroups are $\{e\}$ and G itself.

Remark 84. *Simple groups are an important tool in group theory, because they allow us to break larger groups down into their constituent simple group parts.*

Example 85. *Let p be a positive prime integer. If $|G| = mp$ with $1 < m < p$, then G is not simple.*

Indeed, consider any subgroup of G with p elements. By 82, the number of such subgroups is 1 modulo p. Thus, if there exists more than 1 subgroup, then it must be at least $p+1$.

That is, any two distinct subgroups of prime order p can only meet at the identity; therefore this would account for at least

$$1 + (p+1)(p-1) = p^2$$

elements in G. Since $|G| = mp < p^2$, this would be an impossibility. Therefore, there's only one cyclic subgroup of order p in G, which is normal, proving that G is not simple.

6.2 Sylow I.

Theorem 86 (Sylow I.). *Let p be a prime integer. A p-Sylow subgroup of a finite group G is a subgroup of order p^r, where $|G| = p^r m$ and $\gcd(p, m) = 1$. That is, $P \subseteq G$ is a $p-$Sylow subgroup if it's a $p-$group and p doesn't divide $[G : P]$.*

If p doesn't divide the order of $|G|$, then G contains a $p-$Sylow subgroup: namely, $\{e\}$. This isn't very interesting; what is interesting is that G contains a $p-$Sylow subgroup even when p does divide the order of G

HW 4 Notes: Sylow Theorems

Proposition 87 (Sylow I Lemma). *If p^k divides the order of G, then G has a subgroup of order p^k.*

Proof. If $k = 0$, there's nothing to prove, so we may assume that $k \geq 1$ and in particular that $|G|$ is a multiple of p.

Argue by induction on $|G|$: if $|G| = p$, again there's nothing to prove; if $|G| > p$ and G contains a proposer subgroup H such that $[G : H]$ is relatively prime to p, then p^k divides the order of H, and hence H contains a subgroup of order p^k by the inductive hypothesis, and thus so does G.

Therefore, we may assume that all proper subgroups of G have index divisible by p. By the class formula, p divides the order of the center of $Z(G)$. By Cauchy's theorem, there exists $a \in Z(G)$ such that $|a| = p$. The cyclic subgroup $N =< a >$ is contained within $Z(G)$, and hence it's normal in G. Therefore we can consider the quotient group G/N.

Since $|G/N| = |G|/p$ and p^k divides $|G|$ by hypothesis, we have that p^{k-1} divides the order of G/N. By the induction hypothesis, we may conclude that G/N contains a subgroup of order p^{k-1}. By the structure of the subgroups of a quotient, this subgroup must be of the form P/N, for a subgroup of G.

But then $|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k$, as needed. □

6.3 Sylow II.

Remark 88 (Sylow II). *Theorem* 2.5 *tells us that some maximal $p-$group in G attains the largest size allowed by Lagrange's theorem, that is, the maximal power of the prime p dividing $|G|$.*

Sylow II tells us that all $p-$Sylow subgroups are conjugates of each other. Moreover, even better than this, every $p-$group inside G must be contained in a conjugate of any fixed $p-$Sylow subgroup.

Theorem 89 (Sylow II). *Let G be a finite group, let P be a $p-$Sylow subgroup and let $H \subseteq G$ be a $p-$group. Then H is contained in a conjugate of $P0$: there exists a $g \in G$ such that $H \subseteq gPg^{-1}$.*

Proof. Act with H on the set of left-cosets of P, by left-multiplication. Since there are $[G : P]$ cosets and p doesn't divide $[G : P]$, we know this action must have fixed points: let gP be one of them. This means for all $h \in H$:

$$hgP = gP;$$

that is, $g^{-1}hgP = P$ for all $h \in H$; that is $g^{-1}Hp \subseteq P$; that is, $H \subseteq gPg^{-1}$ as needed. $\square$

Lemma 90. *Let H be a $p-$group contained in a finite group G. Then*

$$|N_G(H) : H| \equiv [G : H] \mod p.$$

Proof. If H is trivial, then $N_G(H) = G$ and the two numbers are equal.

Assume then that H is nontrivial, and act with H on the set of left-cosets of H in G, with left-multiplication. The fixed points of this action are the cosets gH such that for all $h \in H$:

$$hgH = gH,$$

that is, such that $g^{-1}hg \in H$ for all $h \in H$; in other words, $H \subseteq gHg^{-1}$, and hence (by order considerations) $gHg^{-1} = H$. This means precisely that $g \in N_G(H)$. Therefore, the set of fixed points of the action consists of the set of cosets of H in $N_G(H)$.

The statement then follows immediately from Corollary 1.3 $\square$

Proposition 91. *Let H be a $p-$subgroup of a finite group G, and assume that H isn't a $p-$Sylow subgroup. Then there exists a $p-$subgroup H' of G containing H, such that $[H' : H] = p$ and H is normal in H'.*

Proof. Since H isn't a $p-$Sylow subgroup of G, p divides $[N_G(H) : H]$, by Lemma 2.9. Since H is normal in $N_G(H)$, we may consider the quotient group $N_G(H)/H$ and p divides the order of this group. By Theorem 2.1, $N_G(H)/H$ has an element of order p; this generates a subgroup of order p of $N_G(H)/H$, which must be in the form of H'/H for a subgroup H' of $N_G(H)$.

It's straightforward to verify that H' satisfies the stated requirements. $\square$

6.4 Sylow III.

Remark 92. *This last theorem will give us a good handle on the number of $p-$Sylow subgroups of a given finite group G. This is especially true for establishing the existence of normal subgroups of G: since all $p-$Sylow subgroups of a group are conjugates of each other, if there is only one $p-$Sylow subgroup, then that subgroup must be normal.*

HW 4 Notes: Sylow Theorems

Theorem 93. *Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p doesn't divide m. Then the number of $p-$Sylow subgroups of G divides m and is congruent to 1 modulo p.*

Proof. Let N_p denote the number of $p-$Sylow subgroups of G.

By Theorem 2.8, the $p-$Sylow subgroups of G are the conjugates of any given $p-$Sylow subgroup P. By Lemma 1.13, N_p is the index of the normalizer $N_G(P)$ of P; thus (Corollary 1.14) it divides the index m of P. In fact,

$$m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P] = N_P \cdot [N_G(P) : P].$$

Now by Lemma 2.9 we have

$$m = [G : P] \equiv [N_G(P) : P] \mod p;$$

multiplying by N_p we get

$$mN_p \equiv m \mod p.$$

Since $m \not\equiv 0 \mod p$ and p is prime, this implies

$$N_p \equiv 1 \mod p,$$

as needed. □

6.5 Applications.

6.5.1 More Nonsimple Groups

Proposition 94. *Let G be a group of order mp^r, where p is a prime integer and $1 < m < p$. Then G isn't simple.*

Proof. By the third Sylow theorem, the number N_p of $p-$Sylow subgroups divides m and is in the form $1 + kp$. Since $m < p$, this forces $k = 0$, $N_p = 1$. Therefore G has a normal subgroup of order p^r; hence it's not simple. □

Example 95. *There are no simple groups of order* 2002. *Indeed,*

$$2002 = 2 \cdot 7 \cdot 11 \cdot 13;$$

the divisors of $2 \cdot 7 \cdot 13$ *are:*

$$1, 2, 7, 13, 14, 26, 91, 182 :$$

of these, only 1 *is congruent to* $1 \mod 11$. *Thus there's a normal subgroup of order* 11 *in every group of order* 2002.

Example 96 (Non-example)**.** *There are no simple groups of order* 12.

Note that $3 \equiv 1 \mod 2$ *and* $4 \equiv 1 \mod 3$; *thus the argument used above doesn't guarantee the existence of either a normal* $2-$*Sylow subgroup or a normal* $3-$*Sylow subgroup.*

However, suppose that there's more than one $3-$*Sylow subgroup. Then there must be* 4, *by the third Sylow theorem. Since any two such subgroups must intersect in the identity, this accounts for exactly* 8 *elements of order* 3. *Excluding these leaves us with the identity and* 3 *elements of order* 2 *or* 4*; that is just enough room to fit one* $2-$*Sylow subgroup. This subgroup will then have to be normal.*

Thus, either there's a $3-$*Sylow normal subgroup or there's a* $2-$*Sylow normal subgroup - either way, the group isn't simple.*

Example 97. *There are no simple groups of order* 24.

Indeed, let G *be a group of order* 24 *and consider its* $2-$*Sylow subgroups; by the third Sylow theorem, there are either* 1 *or* 3 *such subgroups. If there's* 1, *the* 2*-Sylow subgroup is normal and* G *isn't simple. Otherwise,* G *acts (non-trivially) by conjugation on this set of three* $2-$*Sylow subgroups; this action gives a nontrivial homomorphism* $G \to S_3$, *whose kernel is a proper, nontrivial normal subgroup of* G *- thus again* G *isn't simple.*

6.5.2 Groups of order pq, $p < q$ are prime

Proposition 98. *Assume* $p < q$ *are prime integers and* $q \not\equiv 1 \mod p$. *Let* G *be a group of order* pq. *Then* G *is cyclic.*

Proof. By the third Sylow theorem, G has a unique (hence normal) subgroup H of order p. Indeed, the number N_p of $p-$Sylow subgroups must divide q, and q is prime, so $N_p = 1$ or q. Necessarily $N_p \equiv 1 \mod p$ and $q \not\equiv 1 \mod p$ by hypothesis; therefore $N_p = 1$.

Since H is normal, conjugation gives an action of G on H, hence a homomorphism $\gamma : G \to \mathrm{Aut}(H)$. Now H is cyclic of order p, so $|\mathrm{Aut}(H)| = p - 1$; the order of $\gamma(G)$ must divide both pq and $p - 1$, and it follows that γ is the trivial map.

Therefore, conjugation is *trivial* in H: that is, $H \subseteq Z(G)$. Lemma 1.5 implies that G is abelian.

Finally, an abelian group of order pq, with $p < q$ primes, is necessarily cyclic: indeed it must contain elements g, h of order p, q, respectively (for example by Cauchy's Theorem), and then $|gh| = pq$. □

Proposition 99. *Let q be an odd prime, and let G be a non-commutative group of order $2q$. Then $G \simeq D_{2q}$, the dihedral group.*

Proof. By Cauchy's Theorem, there exists $y \in G$ such that y has order q. By the third Sylow theorem, $< y >$ is the unique subgroup of order q in G (and is therefore normal). Since G is not commutative and in particular it's not cyclic, it has no elements of order $2q$; therefore, every element in the complement of $< y >$ has order 2; let x be any such element.

The conjugate xyx^{-1} of y by x is an element of order q, so $xyx^{-1} \in < y >$. Thus, $xyx^{-1} = y^r$ for some r between 0 and $q - 1$.

Now observe that

$$(y^r)^r = (xyx^{-1})^r = xy^r x^{-1} = x^2 y x^{-2} = y,$$

since $|x| = 2$. Therefore, $y^{r^2-1} = e$, which implies

$$q|(r^2 - 1) = (r - 1)(r + 1)$$

by Corollary $II.1.11$. Since q is prime, this says that $q|(r-1)$ or $q|(r+1)$; since $0 \leq r \leq q-1$, it follows that $r = 1$ or $r = q - 1$.

If $r = 1$, then $xyx^{-1} = y$; that is, $xy = yx$. But then the order of xy is $2q$ (by Exercise $II.1.14$), and G is cyclic, a contradiction.

Therefore, $r = q - 1$, and we have established the relations:

$$\begin{cases} x^2 = e, \\ y^q = e, \\ yx = xy^{q-1}. \end{cases}$$

These are relations satisfied by generators x, y of D_{2q}, as the reader hopefully verified in Exercise $II.2.5$; the statement follows. □

7 Sylow Theorems (Gallian)

HW 4 Notes: Sylow Theorems

Theorem 100. *If G is a group of order pq, where p and q are primes, $p < q$, and p doesn't divide $q-1$, then G is cyclic. In particular $G \simeq \mathbb{Z}_{pq}$.*

Proof. Let H be a Sylow $p-$subgroup of G and let K be a Sylow $q-$subgroup of G. Sylow's Third Theorem states the number of Sylow $p-$subgroups of G is of the form $1+kp$ and pq. So $1+kp = 1, p, q$, or qp. From this and the fact that $p \not| q-1$, it follows that $k = 0$, and, therefore, H is the only $p-$subgroup of G.

Similarly, there's only one Sylow $q-$subgroup of G. Thus, by the corollary to Theorem 24.5, H and K are normal subgroups of G. Let $H =< x >$ and $K =< y >$. To show that G is cyclic, it suffices to show that x and y commute, for then $|xy| = |x||y| = pq$. But observe that, since H and K are normal, we have

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Ky^{-1} = K$$

and

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in xH = H.$$

Thus, $xyx^{-1}y^{-1} \in K \cap H = \{e\}$, and hence $xy = yx$. $\square$

Example 101 (Determination of Groups of Order 99)**.** *Suppose that G is a group of order 99. Let H be a Sylow $3-$subgroup if G and K be a Sylow-11 subgroup of G. Since 1 is the only positive divisor of 99 that is equal to $1 \mod 11$, we know from Sylow's Third Theorem and its corollary that K is normal in G. Similarly, H is normal in G. If follows, by the argument used in the proof of Theorem 24.6 that elements from H and K commute, and therefore, $G = H \times K$. Since both H and K are Abelian, G is also Abelian. Thus $G \simeq$ either $\mathbb{Z}_{99}$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_{33}$.*

Example 102 (Determination of Groups of Order 66)**.** *Suppose that G is a group of order 66. Let H be a Sylow $3-$subgroup of G and let K be a Sylow 11-subgroup of G. Since 1 is the only positive divisor of 66 that is equal to $1 \mod 11$, we know that K is normal in G. Thus HK is a subgroup of G of order 33. Since any group of order 33 is cyclic (Theorem 24.6), we may write $HK =< x >$. Next, let $y \in G$ and $|y| = 2$. Since $< x >$ has index 2 in G, we know that it is normal. So $yxy^{-1} = x^i$ for some i from 1 to 32. Then, $yx = x^iy$ and since every member of G is of the from x^sy^t, the structure of G is completely determined by the value of i. We claim that there's only four possibilities for i. To prove this, observe that $|x^i| = |x|$. Thus, i and 33 are relatively prime. But*

HW 4 Notes: Sylow Theorems

also, since y *has order* 2,

$$x = y^{-1}(yxy^{-1})y = y^{-1}x^iy = yx^iy^{-1} = (yxy^{-1})^i = (x^i)^i = x^{i^2}.$$

So $x^{i^2-1} = e$ *and therefore* 33 *divides* $i^2 - 1$. *From this it follows that* 11 *divides* $i \pm 1$, *and, therefore,* $i = 0 \pm 1, i = 11 \pm i, i = 22 \pm 1$, *or* $i = 33 \pm 1$. *Putting this together with the other information we have about* i, *we see that* $i = 1, 10, 23, 32$. *This proves that there are four groups of order* 66.

To prove there are exactly four, we simply observe that $\mathbb{Z}_{66}$, $D_{33}, D_{11} \oplus \mathbb{Z}_3, D_3 \oplus \mathbb{Z}_{11}$ *each has order* 66 *and that no two are isomorphic. For example,* $D_{11} \oplus \mathbb{Z}_3$ *has* 11 *elements of order* 2, *where as* $D_3 \oplus \mathbb{Z}_{11}$ *has only three elements of order* 2.

HW 5 Notes: Category Theory Revisited

8 Class Notes (Brussel)

Definition 25

Let C be a category.
C consists of a class of objects and a class of morphisms.

Example 103. *The category of: Set, Ring, $k-$Vector Space, Top, $r-$Module*

Remark 104. *When are the two objects the 'same'?*
When are they are isomorphic.

Definition 26

$f : A \to B$ is an **isomorphism** if: there exists a:

$$g : B \to A$$

such that $f \circ g = id_B$ and $g \circ f = id_A$.

Note 105. *That is f and g are general morphisms, not set maps, necessarily.*

Example 106.

- *In Set, $A \simeq B \iff |A| = |B|$, so the morphism is a bijection.*
- *In Group and In Ring, these are just isomorphisms as we know them.*
- *In Top, $A \simeq B \iff A$ and B are homeomorphic.*

Note 107. *Idea of a universal objects, is that it's a special object defined uniquely by their relations to other objects.*

HW 5 Notes: Category Theory Revisited

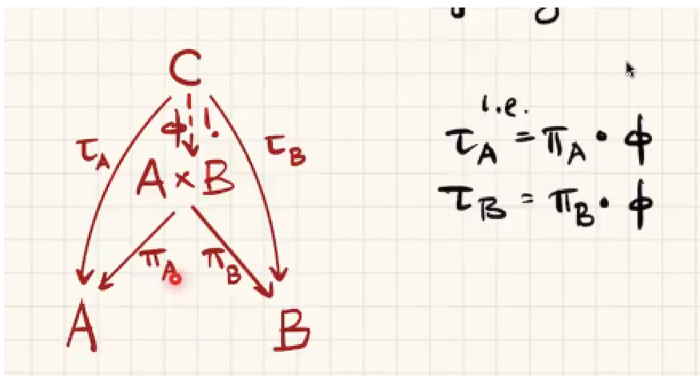


Figure 2: Products

Example 108. *$A \times B$ (we're defining an arbitrary product, not a set) A, B. Have 2 morphisms*

- $\pi_A : A \times B \to A$
- $\pi_B : A \times B \to B$

Definition 27

If C is an object and there are morphisms $\tau_A : C \to A$ and $\tau_B : C \to B$, then there's a unique morphism:

$$\phi : C \to A \times B$$

such that the following diagram commutes:

Note 109. *We have familiar intuition for this with component-wise multiplication/addition in rings, groups, etc.*

HW 5 Notes: Category Theory Revisited

Definition 28: Coproducts

$A \amalg B$, objects A, B have morphisms:

$$i_A : A \to A \coprod B$$

$$i_B : B \to A \coprod B$$

Universal Property if D is an object and there are morphisms $\delta_A : A \to D$ and $\delta_B : B \to D$ then there's a unique morphism

$$\psi : A \coprod B \to D$$

such that the following diagram commutes:

Note 110. *Sometimes these are isomorphic, products are isomorphic to co-products, such as in groups where Direct Products are the same as co-products.*

Extend to arbitrary families of objects

$$\{A_i\}_{i \in I}$$

Get

$$\prod_I A_i \qquad \text{and} \qquad \coprod_I A_i$$

with analogous universal properties.

Remark 111. *These may not be isomorphic*

In Set, $A \times B \not\simeq A \coprod B$ *in general*

In Group, $A \times B \simeq A \coprod B \equiv A \oplus B$

In Ab, $\prod_{n \in \mathbb{N}} \mathbb{Z}/n \not\simeq \coprod_{n \in \mathbb{N}} \mathbb{Z}/n$*, you need to have a finite number of non-zero entries for the co-product, but you can have an infinite number of non-zero numbers in the product.*

9 I.3(Aluffi) Categories

9.1 Definition

<u>Example</u> $\boxed{\text{Coproducts}}$ $A \amalg B$, objects A, B

Have morphisms $i_A : A \longrightarrow A \amalg B$
$i_B : B \longrightarrow A \amalg B$.

<u>universal property</u> If D is an object, and there are morphisms $j_A : A \longrightarrow D$
$j_B : B \longrightarrow D$

then there is a <u>unique</u> morphism

$$\psi : A \amalg B \longrightarrow D$$

such that the following diagram commutes:

$$\begin{tikzcd}
 & D & \\
 & A \amalg B \arrow[u, dashed, "\psi\,!"] & \\
A \arrow[ur, "i_A"] \arrow[uur, bend left, "j_A"] & & B \arrow[ul, "i_B"'] \arrow[uul, bend right, "j_B"']
\end{tikzcd}$$

i.e.

$$j_A = \psi \circ i_A$$
$$j_B = \psi \circ i_B$$

Figure 3: Co-products

HW 5 Notes: Category Theory Revisited

Note 112. *There is a class of all sets.*

Definition 29: Category

A category C consists of

1. A class $Obj(C)$ of objects of the category; and
2. For every two objects A, B of $\mathcal{C}$, a set $\mathbf{Hom}_{\mathcal{C}}(A, B)$ of morphisms, with the properties:
   (a) For every object A of $\mathcal{C}$, there exists (at least) one morphism $1_A \in \mathbf{Hom}_{\mathcal{C}}(A, A)$, the 'identity' of A.
   (b) One can compose morphisms: two morphisms $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$ and $g \in \mathbf{Hom}_{\mathcal{C}}(B, C)$ determine a morphism $gf \in \mathbf{Hom}_{\mathcal{C}}(A, C)$. That is, for every triple of objects A, B, C of $\mathcal{C}$ there is a function (of sets)

   $$\mathbf{Hom}_{\mathcal{C}}(A, B) \times \mathbf{Hom}_{\mathcal{C}}(B, C) \to \mathbf{Hom}_{\mathcal{C}}(A, C),$$

   the image of the pair (f, g) is denoted gf.
   (c) 'The composition law' is associative: if $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$, $g \in \mathbf{Hom}_{\mathcal{C}}(B, C)$, and $h \in \mathbf{Hom}_{\mathcal{C}}(C, D)$, then:

   $$(hg)f = h(gh).$$

   (d) The identity morphisms are identities with respect to composition: that is, for all $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$ we have

   $$f1_A = f \qquad 1_B f = f$$

   (e) One further requirement is that

   $$\mathbf{Hom}_{\mathcal{C}}(A, B) \qquad \mathbf{Hom}_{\mathcal{C}}(C, D)$$

   are disjoint unless $A = C, B = D$.

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 5 Notes: Category Theory Revisited

Definition 30: Endomorphism

A morphism of an object A of a category $\mathcal{C}$ to itself is called an **endomorphism**; $\mathbf{Hom}_{\mathcal{C}}(A, A)$ is denoted $\mathbf{End}_{\mathcal{C}}(A)$.
Note that composition is an operation on $\mathbf{End}_{\mathcal{C}}(A)$.

Definition 31: T

is allows us to draw *diagrams* of morphisms in any category; a diagram is said to 'commute' (or to be a 'commutative diagram') if all ways traverse it lead to the same results of composing morphisms along the way.

9.2 Examples

Example 113. *Sets form a category*

1. *Obj*(Set) *= the class of all sets;*
2. *For* A, B *in Obj*(Set) *(that is, for* A, B *sets)* $\mathrm{Hom}_{\mathrm{Set}}(A, B) = B^A$.

Example 114. *Suppose* S *is a set and* $\sim$ *is a relation on* S *satisfying the reflexive and transitive properties. Then we can encode this data into a category:*

1. *objects: the elements of* S*;*
2. *morphisms: if* a, b *are objects (that is, if* $a, b \in S$*), then let* $\mathrm{Hom}(a, b)$ *be the set consisting of the element* $(a, b) \in S \times S$ *if* $a \sim b$*, and let* $\mathrm{Hom}(a, b) = \emptyset$ *otherwise.*

   We have to show this is a category that is: Show the composition of morphisms is defined and verify the conditions provided earlier.

   (a) *(Identities) If* a *is an object, we need to find an element*

   $$1_a \in \mathrm{Hom}(a, a).$$

   That is why we have to assume that $\sim$ *is reflexive: that tells us that we have no choice but to let:*

   $$1_a = (a, a) \in \mathrm{Hom}(a, a).$$

HW 5 Notes: Category Theory Revisited

(b) *(Composition) Let a, b, c be objects and*

$$f \in \mathrm{Hom}(a, b) \qquad g \in \mathrm{Hom}(b, c);$$

we define a corresponding morphism $gf \in \mathrm{Hom}(a, c)$. Now

$$f \in \mathrm{Hom}(a, b)$$

is nonempty, and by the definition of morphisms in this category $a \sim b$ and hence $f = (a, b) \in A \times B$. Similarly, $g \in \mathrm{Hom}(b, c)$ tells us that $b \sim c$ and $g = (b, c)$. Now we have

$$a \sim b \qquad and \qquad b \sim c \implies a \sim c$$

since we are assuming that $\sim$ is transitive. This tells us that $\mathrm{Hom}(a, c)$ consists of a single element (a, c). Thus we again have no choic, so we must let:

$$gf := (a, c) \in \mathrm{Hom}(A, C)$$

Is this associative? If $f \in \mathrm{Hom}(a, b), g \in \mathrm{Hom}(b, c)$ and $h \in \mathrm{Hom}(c, d)$, then necessarily

$$f = (a, b) \qquad g = (b, c) \qquad h = (c, d)$$

and $gf = (a, c) \qquad hg = (b, d)$ and hence

$$h(gf) = (a, d) = (hg)f.$$

Finally we can check that 1_A is the identity with respect to composition.

That is this is a category if and only if $\sim$ is an equivalence relation.

Example 115 (Integer Poset)**.** *Consider $\mathbb{Z}$ with the $\leq$-relation, so that some commutative diagram of this is: 4*

Note that this would still be a commutative diagram if we reversed the arrow $3 \to 3$ and added one from $3 \to 4$, but that's not allowed since $4 \not\leq 3$

Example 116 (Power Set)**.** *Let S again be a set. Define a category $\hat{\mathrm{S}}$ by setting:*

1. $\mathrm{Obj}(\hat{\mathrm{S}}) = \mathcal{P}(S)$, *the power set of $\mathcal{S}$.*

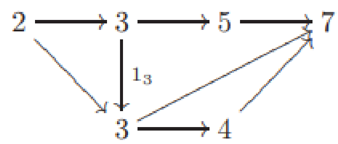


Figure 4: Commutative Diagram of $(\mathbb{Z}, \leq)$

2. *For A, B objects of $\hat{\mathcal{S}}$ (that is, $A \subseteq S$ and $B \subseteq S$) let $\mathrm{Hom}_{\hat{S}}(A, B)$ be the pair (A, B) if $A \subseteq B$ and let $\mathrm{Hom}_{\hat{S}}(A, B) = \emptyset$ otherwise.*

The identity 1_A consists of the pair (A, A) (which is one, and only one, morphism from A to A since $A \subseteq A$).
Composition is obtained by stringing together inclusions: if there are morphisms

$$A \to B \qquad B \to C$$

in $\hat{S}$, then $A \subseteq B$ and $B \subseteq C$; hence $A \subseteq C$ and there's a morphism $A \to C$.

Example 117. *Let $\mathcal{C}$ be a category, and let A be an object of $\mathcal{C}$. We are going to define a category $\mathcal{C}_A$ whose objects are certain morphisms in $\mathcal{C}$ and whose morphisms are certain diagrams of $\mathcal{C}$ (surprise!).*

1. $\mathrm{Obj}(C_A)$ *= All Morphisms from any object of* C *to A; thus, an object of* C_A *is a morphism* $f \in \mathrm{Hom}_{\mathcal{C}}(Z, A)$ *for some object Z of* C*. Pictorially, an object of* C_A *is an arrow* $Z \xrightarrow{f} A$ *in* C*:* **??**

What are the morphisms on C_A going to be?

- *Let f_1, f_2 be objects of C_A, that is, two arrows 5 in $\mathcal{C}$. Morphisms $f_1 \to f_2$ are defined to be commutative diagrams 7*

in the 'ambient' category C.
That is, morphsisms $f \to g$ correspond precisely to those morphisms $\sigma : Z_1 \to Z_2$ in C such that $f_1 = f_2\sigma$. The identities are inherited from the identities in C: for $f : Z \to A$ in C_A the identity 1_f corresponds to the diagram:

$$\begin{tikzcd} Z_1 \arrow[d, "f_1"'] & Z_2 \arrow[d, "f_2"] \\ A & A \end{tikzcd}$$

Figure 5: Two Arrows

$$\begin{tikzcd} Z \arrow[d, "f"'] \\ A \end{tikzcd}$$

Figure 6: Morphisms

$$\begin{tikzcd} Z \arrow[rr, "1_Z"] \arrow[dr, "f"'] & & Z \arrow[dl, "f"] \\ & A & \end{tikzcd}$$

which commutes by virtue of the the fact that C is a category. Composition is also a sub-product of composition in C. Two morphisms $f_1 \to f_2 \to f_3$ in C_A correspond to putting commutative diagrams side-by-side:

$$\begin{tikzcd} Z_1 \arrow[r, "\sigma"] \arrow[dr, "f_1"'] & Z_2 \arrow[r, "\tau"] \arrow[d, "f_2"] & Z_3 \arrow[dl, "f_3"] \\ & A & \end{tikzcd}$$

Then it follows again that C is a category. Since I can use composition to 'get rid' of the middle arrow:

$$\begin{tikzcd} Z_1 \arrow[rr, "\tau\sigma"] \arrow[dr, "f_1"'] & & Z_3 \arrow[dl, "f_3"] \\ & A & \end{tikzcd}$$

also commutes. Categories constructed in this fashion are called slice categories or comma categories (in particular cases).

$$\begin{tikzcd} Z_1 \arrow[rr, "\sigma"] \arrow[dr, "f_1"'] & & Z_2 \arrow[dl, "f_2"] \\ & A & \end{tikzcd}$$

Figure 7: Commutative Diagram

Example 118. *For sake of concreteness, let's apply the construction of the previous example to the category $\mathbb{Z}$ along with $\leq$. Call this category $\mathcal{C}$, and choose an object A of $\mathcal{C}$ - that is an integer, $A = 3$. Then the objects of C_A are morphisms in C with target 3, that is, pairs $(n, 3) \in \mathbb{Z} \times \mathbb{Z}$ with $n \leq 3$. There's a morphism*

$$(m, 3) \to (n, 3) \iff m \leq n.$$

In this case C_A may be harmlessly identified with the subcategory of integers ≤ 3, with the 'same' morphisms as in $\mathcal{C}$.

Example 119. *An entirely similar example to the one explored in the general example may be obtained by considering morphisms in a category C from a fixed object A to all objects in C, again with morphisms defined by suitable commutative diagrams. This leads to coslice categories.*

Example 120. *As a 'concrete' instance of a category as in Example above, let $C =$ Set and $A =$ a fixed singleton $\{*\}$. Call the resulting category* Set^*.

An object in Set^* is a morphism $f : \{*\} \to S$ in Set, where S is any set. The information of an object in Set^* consists therefore of the choice of a nonempty set S and an element $s \in S$ - that is, the element $f(*)$: the element determines and is determined by f.

Thus we may denote objects of Set^* as pairs (S, s) where S is any set and $s \in S$ is any element of S.

A morphism between two such objects $(S, s) \to (T, t)$ corresponds to a set function $\sigma : S \to T$ such that $\sigma(s) = t$.

Objects of Set^* are called 'pointed sets'. Many of the structures we will study in this book are pointed sets. For example a 'group' is a set G with , among other requirements, a distinguished element e_G; 'group homomorphisms' will be functions which (among other *properties) send identities to identities; thus they are morphisms of pointed sets in the sense above.*

Example 121. *It's useful to consider more 'abstract' examples. Start with a category* C *and two objects* A, B *of* C. *We define a new category* $\mathrm{C}_{A,B}$ *by essentially the same procedure that we used in order to define* C_A.

- $\mathrm{Obj}(\mathsf{C}_{A,B})$ = diagrams

$$\begin{tikzcd} & A \\ Z \arrow[ur, "f"] \arrow[dr, "g"'] & \\ & B \end{tikzcd}$$

  in C; and

- morphisms

$$\begin{tikzcd} & A & & & & A \\ Z_1 \arrow[ur, "f_1"] \arrow[dr, "g_1"'] & & \arrow[r] & & Z_2 \arrow[ur, "f_2"] \arrow[dr, "g_2"'] & \\ & B & & & & B \end{tikzcd}$$

  are *commutative* diagrams

$$\begin{tikzcd} & & A \\ Z_1 \arrow[r, "\sigma"] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "g_1"'] & Z_2 \arrow[ur, "f_2"] \arrow[dr, "g_2"'] & \\ & & B \end{tikzcd}$$

This example is really nothing more than a mixture of C_A *and* C_B *where the two structures interact because of the stringent requirements that the same* σ *must make both sides of the diagrams commute:*

$$f_1 = f_2\sigma \qquad \text{and} \qquad g_1 = g_2\sigma$$

Example 122. *A final variation on these examples conclude with a fibered version of* $C_{A,B}$. *Take this as a test o see if we have really understood* $C_{A,B}$ *Start with a given category* $\mathcal{C}$, *and this time choose two fixed morphisms* $\alpha : A \to C, \beta : B \to C$ *in* C *with the same target* C. *We can then consider a category* $C_{\alpha,\beta}$ *as follows:*

- $\mathrm{Obj}(\mathsf{C}_{\alpha,\beta})$ = *commutative diagrams*

$$\begin{tikzcd} & A \arrow[dr, "\alpha"] & \\ Z \arrow[ur, "f"] \arrow[dr, "g"'] & & C \\ & B \arrow[ur, "\beta"'] & \end{tikzcd}$$

in C, and

- morphisms correspond to commutative diagrams

$$\begin{tikzcd} & & A \arrow[dr, "\alpha"] & \\ Z_1 \arrow[r, "\sigma"] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "g_1"'] & Z_2 \arrow[ur, "f_2"] \arrow[dr, "g_2"'] & & C \\ & & B \arrow[ur, "\beta"'] & \end{tikzcd}$$

There's a mirror example of $\mathcal{C}^{\alpha,\beta}$ starting with two morphisms $\alpha : C \to A, \beta : C \to B$ with common source.

10 I.4(Aluffi) Morphisms

10.1 Isomorphisms

Let C

Definition 32: Isomorphism

A morphism $f \in \mathrm{Hom}_C(A, B)$ is an **isomorphism** if it has a (two-sided) inverse under composition: that is $\exists g \in \mathrm{Hom}_C(B, A)$ such that

$$gf = 1_A \qquad fg = 1_B$$

Proposition 123 (Inverse are Unique)**.** *The inverse of an isomorphism is unique.*

Proof. We have to verify that if both g_1 and $g_2 : B \to A$ act as inverses of a given isomorphism $f : A \to B$, then $g_1 = g_2$. The standard trick for this kind of verification is to compose f on the left by one of the morphisms, and on the right by ht other one; then apply associativity. The whole argument can be compressed into one line:

$$g_1 = g_1 1_B = g_1(fg_2) = (g_1 f)g_2 = 1_A g_2 = g_2,$$

as needed. □

Proposition 124 (Inverse Properties). *With notation f^{-1} being the inverse of f:*

1. *Each identity 1_A is an isomorphism and is its own inverse.*
2. *If f is an isomorphism, then f^{-1} is an isomorphism and further $(f^{-1})^{-1} = f$.*
3. *If $f \in \mathrm{Hom}_C(A, B), g \in \mathrm{Hom}_C(B, C)$ are isomorphisms, then the composition gf is an isomorphism and $(gf)^{-1} = f^{-1}g^{-1}$*

Proof. These all 'prove themselves'. For example, it's immediate to verify that $f^{-1}g^{-1}$ is a left-inverse of gf: Indeed

$$(f^{-1}g^{-1})(gf) = f^{-1}((g^{-1}g)f) = f^{-1}(1_B) = f^{-1}f = 1_A.$$

The verification that $f^{-1}g^{-1}$ is also a right-inverse of gf is analogous. □

Note 125. *Two objects A, B are isomorphic if there's an isomorphism $f : A \to B$. The 'isomorphism' defines an equivalence relation. Write $A \simeq B$.*

Example 126. *Of course, the isomorphisms in* Set *are precisely the bijections.*

Example 127. *As noted in previously in 124, identities are isomorphisms. They may be only isomorphisms in a category: for example, this is the case in the category $\mathcal{C}$ obtained from the relation $\leq$ on $\mathbb{Z}$, as in Example 3.3. Indeed, for a, b objects of* C *(that is, $a, b \in \mathbb{Z}$), there's a morphism $f : a \to b$ and a morphism $g : b \to a$ only if $a \leq b$ and $b \leq a$; that is if $a = b$. So an isomorphism in* C *necessarily acts from an object a to itself; but in* C *there's only one such morphism, that is, 1_a.*

HW 5 Notes: Category Theory Revisited

Example 128. *There are categories in which every morphism is an isomorphism; such categories are called groupoids. The reader 'already knows' many examples of 'groupoids'.*

Definition 33

An **automorphism** of an object of a category C is an isomorphism from A to itself. The set of automorphisms of A is denoted $\mathrm{Aut}_C(A)$; it's a subset of $\mathrm{End}_C(A)$. By prop 4.3, composition confers on $\mathrm{Aut}_C(A)$ a remarkable structure:

1. The composition of two elements $f, g \in \mathrm{Aut}_C(A)$ is an element $gf \in \mathrm{Aut}_C(A)$;
2. composition is associative;
3. $\mathrm{Aut}_C(A)$ contains the element 1_A, which is an identity for composition;
4. every element $f \in \mathrm{Aut}_C(A)$ has an inverse $f^{-1} \in \mathrm{Aut}_C(A)$.

That is every category, C, has an associated group $\mathrm{Aut}_C(A)$ for any object A in C

10.2 Monomorphisms and Epimorphisms

Definition 34: Monomorphisms

Let C be a category. A morphism $f \in \mathrm{Hom}_C(A, B)$ is a *monomorphism* if the following holds:

$$\text{for all objects Z of C and all morphisms } \alpha', \alpha'' \in \mathrm{Hom}_C(Z, A),$$
$$f \circ \alpha' = f \circ \alpha'' \implies \alpha' = \alpha''.$$

Definition 35

Let C be a category. A morphism $f \in \mathrm{Hom}_C(A, B)$ is an epimorphism if the following holds:

$$\text{for all objects Z of C and all morphisms } \beta', \beta'' \in \mathrm{Hom}_C(B, Z),$$
$$\beta' \circ f = \beta'' \circ f \implies \beta' = \beta''.$$

Example 129. *As proven in Prop 2.3, in the category of* Set *the monomorphisms are precisely the injective functions. The reader should have by now checked that, likewise, in* Set *the epimorphisms are precisely the surjective functions. Thus while the definitions* *given in 2.6 may have looked counterintuitve at first, they work as natural 'categorical counterparts' of the ordinary notions of injective/surjective functions.*

Example 130. *In the categories of 3.3, every morphism is both a monomorphism and an epimorphism. Indeed, recall that there's always at most one morphism between any two objects in this category; hence the conditions defining monomorphisms and epimorphisms are vacuous.*

11 I.5 (Aluffi) Universal Properties

11.1 Initial and Final Objects

Definition 36: Final and Initial Objects

Let C be a category. We say that an object I of C is **initial** in C if for every object A of C there exists exactly one morphism $I \to A$ in C :

$$\forall A \in \mathrm{Obj}(C): \qquad \mathrm{Hom}_C(I, A) \text{ is a singleton.}$$

We say that an object F of C is **final** in C if for every object A of C there exists exactly one morphism $A \to F$ in C:

$$\forall A \in \mathrm{Obj}(C): \qquad \mathrm{Hom}_C(A, F) \text{is a singleton.}$$

Example 131. *The category obtained by endowing $\mathbb{Z}$ with the relations $\leq$ has no initial or final object. Indeed, an initial object in this category would be an integer i such that for all $a \in \mathbb{Z}$, $i \leq a$. Similarly, a final object would be an integer f larger than every integer, and there's no such integer.*

That contrasts with the category considered in Example 3.6 which does have a final object $(3, 3)$ but no initial.

Example 132. *In* Set*, the empty set $\emptyset$ is initial (the 'empty graph' defined the unique function from $\emptyset$ to every object), and clearly is the unique set that first this requirement.*

Set *also has final objects: for every set A, there's a unique function from A to a singleton*

$\{p\}$ *(that is, the constant function). Every singleton is final in* Set; *thus, final objects are not unique in this category.*

Proposition 133. *Let C be a category.*

- *If I_1, I_2 are both initial objects in C, then $I_1 \simeq I_2$.*
- *If F_1, F_2 are both final objects in C, then $F_1 \simeq F_2$.*

Further, these isomorphisms are uniquely determined.

Proof. Recall that for every object A of C there's at least one element in $\mathrm{Hom}_C(A, A)$ namely the identity 1_A. If I is initial, then there's a unique morphism $I \to I$, which therefore must be the identity 1_I.

Now assume I_1 and I_2 are both initial in C. Since I_1 is initial, there's a unique morphism $f : I_1 \to I_2$ in C; we have to show that f is an isomorphism. Since I_2 is initial, there's a unique morphism $g : I_2 \to I_1$ in C. Consider $gf : I_1 \to I_1$; as observed, necessarily

$$gf = 1_{I_1}$$

since I_1 is initial. By the same token

$$fg = 1_{I_2}$$

since I_2 is initial. This proves that $f : I_1 \to I_2$ is an isomorphism, as need. The proof for final objects is entirely analogous. □

11.2 Quotients

Example 134. *Let $\sim$ be an equivalence relation defined on a set A. Let's parse the assertion:*

'The quotient $A/\sim$ universal with respect to the property of mapping A to a set in such a way that equivalent elements have the same image.'

What can this possibly mean, and is it true? The assertion is talking about functions

$$A \xrightarrow{\varphi} Z$$

with any set Z, satisfying the property

$$a' \sim a'' \implies \varphi(a') = \varphi(a'').$$

The morphisms are objects of a category; for convenience, let's denote such an object by (φ, Z)*. The only reasonable way to define morphisms* $(\varphi_1, Z_1) \to (\varphi_2, Z_2)$ *is as commutative diagrams:*

$$\begin{tikzcd} Z_1 \arrow[rr, "\sigma"] & & Z_2 \\ & A \arrow[ul, "\varphi_1"] \arrow[ur, "\varphi_2"'] & \end{tikzcd}$$

This is the same definition as in Example 3.7. Does this thing have initial objects?

Proposition 135 (5.5)**.** *Denoting by* π *the 'canonical projection' defined in Example* 2.6*, the pair* $(\pi, A/\sim)$ *is an initial object of this category.*

Proof. Consider any (φ, Z) as above. We have to prove that there exists a unique morphism $(\pi, A/\sim) \to (\varphi, Z)$, that is, a unique commutative diagram:

$$\begin{tikzcd} A/\sim \arrow[rr, "\overline{\varphi}"] & & Z \\ & A \arrow[ul, "\pi"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

that is, a unique function $\overline{\varphi}$ making this diagram commute.

Let $[a]_\sim$ be an arbitrary element of $A/\sim$. If the diagram is indeed going to commute, then necessarily

$$\overline{\varphi}([a]_\sim) = \varphi(a);$$

this tells us that $\overline{\varphi}$ is indeed unique, if it exists at all - that is, if this prescription does define a function $A/\sim \to Z$.

Hence, all we have to check is that $\overline{\varphi}$ is well-defined, that is, that if $[a_1]_\sim = [a_2]_\sim$, then $\varphi(a_1) = \varphi(a_2)$; and indeed

$$[a_1]_\sim = [a_2]_\sim \implies a_1 \sim a_2 \implies \varphi(a_1) = \varphi(a_2).$$

This is precisely the condition that morphisms in our category satisfy. □

11.3 Products

Example 136. *Here is a universal property. Let A, B be sets and consider the product $A \times B$, with two natural projections:*

HW 5 Notes: Category Theory Revisited

$$\begin{tikzcd} & A \\ A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & \\ & B \end{tikzcd}$$

[redacted]

$$\begin{tikzcd} & A \\ Z \arrow[ur, "f_A"] \arrow[dr, "f_B"'] & \\ & B \end{tikzcd}$$

[redacted]

$$\begin{tikzcd} & & A \\ Z \arrow[urr, bend left, "f_A"] \arrow[r, "\sigma"] \arrow[drr, bend right, "f_B"'] & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & \\ & & B \end{tikzcd}$$

Then for every set Z and morphisms above there exists a unique morphism $\sigma : Z \to A \times B$ such that the diagram above commutes.

In this situation, σ is usually denoted $f_A \times f_B$.

Proof. Define $\forall z \in Z$

$$\sigma(z) = (f_A(z), f_B(z)).$$

This function manifestly makes the diagram commute: $\forall z \in Z$

$$\pi_A \sigma(z) = \pi_A(f_A(z), f_B(z)) = f_A(z),$$

showing that $\pi_A\sigma = f_A$ and similarly $\pi_B\sigma = f_B$.

Furthermore, the definition is forced by the commutativity of the diagram; so σ is unique, as claimed. □

Note 137. *That shows that products of sets are final objects in the category $C_{A,B}$ considered in Example 3.9, for $C = \text{Set}$.*

Example 138. *Looking back at our example of $\mathbb{Z}$ with $\leq$ what are products here?*

Objects are simply $a, b \in \mathbb{Z}$ such that $a \times b$ is the categorical product. The universal property written out above becomes, in this case, for all $z \in Z$ such that $z \leq a$ and $z \leq b$, we have $z \leq a \times b$.

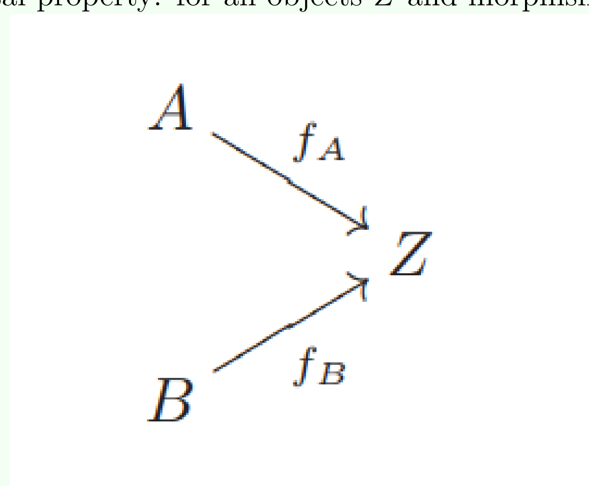
This universal problem does have a solution $\forall a, b$. Namely $a \times b = \min(a, b)$.

11.4 Coproducts

Just as products are final objects in the category $C_{A,B}$ obtained by considering morphisms in C with common source, whose targets are A and B, coproducts will be initial objects in the categories $C^{A,B}$ of morphisms with common target, whose sources are A and B.

Definition 37

Let A, B be objects of a category C. A co-product $A \coprod B$ of A and B will be an object of C, endowed with two morphisms $i_A : A \to A \coprod B$, $i_B : B \to A \coprod B$ and satisfying the following universal property: for all objects Z and morphisms:



There exists a unique morphism $\sigma : A \coprod \to Z$ such that the diagram commutes:

$$\begin{tikzcd}
A \arrow[dr, "i_A"] \arrow[drr, bend left, "f_A"] & & \\
& A \amalg B \arrow[r, "\sigma"] & Z \\
B \arrow[ur, "i_B"'] \arrow[urr, bend right, "f_B"'] & &
\end{tikzcd}$$

Proposition 139 (5.6)**.** *The disjoint union is a co-product in* Set.

Proof. Recall 1.4 that the disjoint union $A \coprod B$ is defined as the union of two disjoint isomorphic copies A', B' of A and B, respectively; for example, we may let $A' = \{0\} \times B, B' = \{1\} \times B$. The function i_A, i_B are defined by

$$i_A(a) = (0, a) \qquad i_B(b) = (1, b),$$

where we view these elements as elements of $(\{0\} \times A) \cup (\{1\} \times B)$.
Now let $f_A : A \to Z, f_B : B \to Z$ be arbitrary morphisms to a common target. Define

$$\sigma : A \coprod B = (\{0\} \times A) \cup (\{1\} \times B) \to Z$$

by

$$\sigma(c) = \begin{cases} f_A(a) & \text{if } c = (0, a) \in \{0\} \times A, \\ f_B(b) & \text{if } c = (1, b) \in \{1\} \times B. \end{cases}$$

This definition makes the relevant diagram commute and is in fact forced upon us by this commutativity, providing σ exists and is unique. □

Example 140. *The category obtained from $\leq$ and $\mathbb{Z}$ does have coproducts: the corpoducts of two objects (integers) a, b is simply the maximum of a and b.*

12 Class Notes (10-28-2021)

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 5 Notes: Category Theory Revisited

Note 141. *Category Theory is a generalization of the concept of a monoid. Every Category Forms a*

HW 6: Modules

13 Class Notes

13.1 Class Notes 10-26-2021

Definition 38

Let R be a ring with unity 1.
A (left) $R-$module is an abelian group $(M,+)$ together with a pairing

$$R \times M \to M$$

$$(r,m) \mapsto r \cdot m$$

such that

1. $(r+s) \cdot m = r \cdot m + s \cdot m$
2. $r \cdot (s \cdot m) = (rs) \cdot m$
3. $0 \cdot m = 0$ and $1 \cdot m = m$
4. $r \cdot (m+n) = r \cdot m + r \cdot n$

Example 142. 1. *$R = k$-Fields, $M = V, K-$Vector Spaces*

2. *$R = \mathbb{Z}$ and $\mathbb{Z} \times M \to M$, take $(n,v) \mapsto nv$. The $\mathbb{Z}$-modules are just Abelian groups; $\mathbb{Z}-$modules $=$ Abelian Groups.*

3. *$I \subset R$ is a $R-$module*
$$R \times I \to I$$

4. *R/I quotient is an R-module. That would be*

$$R \times R/I \to R/I$$

$$(a, c+I) \mapsto ac + I.$$

5. *$k[x]-$Modules is a k Field.*

Let V be a $k-$Vector Space.
$$k[x] \times V \to V$$
$$(x,v) \mapsto x \cdot v$$

If $c \in k$, $x \cdot cv = cx \cdot v$

$x \cdot (v + w) = x \cdot v + x \cdot w$

x is a linear transformation.

Definition 39:

1. A **sub-module** of a module $(N, +) \leq (M, +)$ and stable under R
2. A **quotient module** is The Abelian group quotient determined by a sub-module $N \subset M$, M/N. Here $R \times M/N \to M/N$ along

$$(r, m + N) \mapsto rm + N$$

3. A **cyclic module** contains an element m such that $M = R \cdot m$, some $m \in M$
4. An **irreducible module** A module that has no sub-modules $(0) + M$.

Example 143. *Suppose $V = \mathbb{R}^3$ and let's define $X \cdot v = T(v)$ where $T = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ Then V is an $\mathbb{R}[x]$-module.*

E.g. What does this mean: $x^2 + 1 \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = x^2 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ where we obtain x^2 be composition and 1 is just identity. So that: $\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}$

Sub-modules: $\mathbb{R}[x] \cdot e_1 =$ xy-plane and $\mathbb{R}[x] \cdot e_2$, both are (irreducible) cyclic submodules. Notice that $\mathbb{R} \cdot e_1 \subseteq \mathbb{R}[x] \cdot e_1$ is a subgroup but not submodule.

Definition 40

An $R-$module homomorphism (or just $R-$homomorphism) $f : M \to N$ is a homomorphism of the underlying groups that commutes with the R-actions: $f(rm) = rf(m)$. We write

$$\mathrm{Hom}_R(M, N)$$

it's self is an R-Module.

HW 6: Modules

13.2 Class Notes 10-28-2021

Note 144 (Last TIme). *R is a ring with unity, M is an $R-$module (that is an abelian group $+$, and scalar multiplication by R).*
The category is $R-$Modules

- *Submodules That is stable under the operation.*
- *Quotient Modules That is the quotient group formed by submodules.*
- *Cyclic Submodules*
- *Irreducible Submodules No submodules except for trivial ones.*
- *Finitely generated Modules That is, there exists a finite set $X \subseteq M : M = \{\sum rx : x \in X\}$*

Note 145. *Recall that $\mathbb{Z}$-modules are just modules with scalars in $\mathbb{Z}$. And we showed that every Abelian group is a $\mathbb{Z}$-module. And every $\mathbb{Z}$-module is an Abelian group.*
I.e

$$\mathbb{Z} - \textit{module} \iff \textit{Abelian Group}$$

Any $k-$vector space is a $k[x]$-module, x acts as a linear transformation, we saw this in 143.
In this example, the action of $X = T$ on $xy-$plane: this was a $\pi/2$ rotation. On the $z-$axis, this was multiplication by 1.
These submodules are invariant subspaces under $T = X$. In general, there's always going to be a $1-1$ correspondence between

$$\{k[x] - \textit{Modules}\} \iff \{\textit{Invariant Sub-spaces of } V\}$$

Example 146. *Consider these*

1. *$\mathbb{Z}$ is a finitely generated $\mathbb{Z}$-module*
2. *$\mathbb{Q}/\mathbb{Z}$ is not a finitely generated $\mathbb{Z}-$module.*

HW 6: Modules

Example 147. *$\mathbb{Z}_m, \mathbb{Z}_n$ are $\mathbb{Z}-$modules investigate* $\hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n)$.

Solution. We know that by Fact's of cyclic groups any $\phi \in \hom(\mathbb{Z}_m, \mathbb{Z}_n)$ is completely determined by $\phi([1]_m)$.

That is, $|\phi([1]_m)|$ divides $d = \gcd(m, n)$.

Therefore, $\hom(\mathbb{Z}_m, \mathbb{Z}_n)$ corresponds to $\langle [c]_n \rangle$, where $c = \dfrac{n}{d} \in \mathbb{Z}$.

So therefore, we have a bijection between $\hom(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_d$.

So what gets mapped to $[1]_d$?

Note: $[1]_d$ is the equivalence class in $\mathbb{Z}_n$, so $\{[0]_n, [1]_n, \ldots [n-1]_n\} = \mathbb{Z}_n$, that is $[0]_n = \{0, \pm n, \pm 2n, \ldots\}$.

So that is $\phi_0 \mapsto [1]_d$, where $\phi([1]_m) = [c]_n$, where $c = n/\gcd(m, n)$. So then $\phi_0(3[1]_m) = 3\phi_0([1]_m)$?

$$\phi([1]_m + [1]_m + [1]_m) = \phi([1]_m) + \phi([1]_m) + \phi([1]_m) \checkmark$$

So $\hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n)$ is a $\mathbb{Z}-$module, i.e an Abelian group. But how do I define $\phi + \psi$?

$$(\phi + \psi)([1]_m) = \phi([1]_m) + \psi([1]_m)$$

Claim: $\hom(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_d$ is an isomorphism

Special case: $m = n$. Then hom = end. (Ring)

Multiplication = Composition of Functions □

13.3 Class Notes 10-29-2021

Note 148 (Last Time)**.**

1. *R is a ring with 1, M is an $R-$Module (Abelian Group + Scalar Multiplication by R).*
2. $\hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \xrightarrow{\sim} \mathbb{Z}_d$
3. ***end***$_{\mathbb{Z}}(\mathbb{Z}_n) \xrightarrow{\sim} \mathbb{Z}_n$ *(Ring Isomorphism)*
4. $\{k[x] -$ *Submodules of* $V\} \iff \{$*Invariant Subspaces of* $V\}$, *under linear transformation that is* x.

One more.

HW 6: Modules

Example 149. *Let M be irreducible $R-$module.*

Recall: No nontrivial proper submodules.

$\boldsymbol{End}_R(M)$ *is an $R-$Module, also a Ring (with composition). The addition in the endomorphism ring, is the sum in the image; that is $(\phi+\psi)(m) = \phi(m)+\psi(m)$.*

An $R-$Algebra is an $R-$Module that's also a ring; that is $\boldsymbol{End}_R(M)$ *is an $R-$Algebra.*

That is $\varphi \in \boldsymbol{End}_R(M) \implies \varphi(M) \leq M$ (R-Submodule), but since M is irreducible that would imply that $\varphi(M) = (0)$ or M. If $\varphi(M) \neq 0$, implies that $\varphi(M) = M$.

This gives that $\ker(\varphi) = M$ or (0). Hence if $\varphi \neq 0$, then $\ker(\varphi) = (0)$. Hence φ is injective.

So that φ is a bijection and is in the automorphisms; $\mathbf{Aut}_R(M)$*.*

That is, it's invertible. So we have a Ring with non-zero elements all being invertible. So that's a division ring, and so a division algebra.

Theorem 150 (Schur's Lemma)**.** *Let M be an irreducible $R-$Module, then* $\mathbf{End}_R(M)$ *is an $R-$division algebra.*

Theorem 151 (1st Isomorphism Theorem for Modules)**.** *Suppose $f : M \to R$ is an $R-$module homomorphism. Then $\ker(f)$ is a submodule of M, and we have an isomorphism*

$$M/\ker(f) \to f(M) \leq N.$$

There's a $1-1$ correspondence between submodules of M containing $\ker(f)$ and submodules of $f(M)$, given by $M' = f^{-1}(N')$ for $N' \leq f(M)$.

Proof. $\ker(f) \leq (M,+)$ is an Abelian subgroup, and I claim that it's a $R-$submodule that is we have an action: $R \times \ker(f) \to \ker(f)$

$$(r,m) \mapsto rm)$$

All Module axioms hold, since they hold for M. So it remains to show that it's well-defined: $rm \in \ker(f)$.

Consider $f(m) = 0$, then $r \cdot f(m) = r \cdot 0 = 0$, but $f(rm) = 0$ (since f is R-linear). Hence $rm \in \ker(f)\checkmark$.

Consider the quotient $M/\ker(f)$, that's a group quotient since $\ker(f) \lhd M$.

Claim: $R-$Module action. $r(m+\ker(f)) = rm + \ker(f)$.

I need to show this is well-defined, suppose $m + \ker(f) = m' + \ker(f)$, is $rm + \ker(f) = rm' + \ker(f)$?

Check that:

$$r(m - m') + \ker(f) = \ker(f)$$

$$m - m' \in \ker(f) \implies r(m - m') \ker(f)$$

since $\ker(f)$ is an $R-$Module. So that $rm - rm' \in \ker(f)$, hence $rm + \ker(f) = rm' + \ker(f)$, as required.

Other module requirements are super easy to check.

E.g. $0 \cdot (m + \ker(f)) = 0 \cdot m + \ker(f) = \ker(f)$, since $0 \cdot m = m$ in M because M is an $R-$Module.

E.g. $1 \cdot (m + \ker(f)) = 1 \cdot m + \ker(f) = m + \ker(f) \checkmark$.

So along with this and the three other conditions, we have $M/\ker(f)$ is an $R-$Module.

Function $M/\ker(f) \to f(M)$, isomorphism on Abelian Groups.

Remains to show that this is $R-$Linear so then it's an $R-$Isomorphism.

$$\phi(r(m + \ker(f)) =$$

□

13.4 Class Notes 11-01-2021

Note 152. *Last Time: 1st Isomorphism Theorem in $R-$Module, by the way of kernels and images are $R-$Modules quotients by $R-$Modules are too.*

Outline

1. *Products, Free Modules, and Determinants*
2. *Smith Normal Form, and Modules over a PID. Invariant Factors and how to compute them.*
3. *Main Theorem for Finitely Generated Modules over a PID. Presentation Matrix*
4. *Applications to Linear Transformations Invariants and Similarity*
5. *Canonical Forms*

Name: Joseph McGuire

Class: Math 561(Fall 2021)

HW 6: Modules

Theorem 153 (2nd Isomorphism Theorem)**.** *Suppose A and B are submodules of an $R-$Module M. Then $(A+B)/N \simeq A/(A \cap B)$.*

Theorem 154 (3rd Isomorphism Theorem)**.** *Suppose A and B are submodules of an $R-$Module M. If $A \subset B$, then $(M/A)/(B/A) \simeq M/B$.*

Note 155. *Know how to do these for exams.*

Definition 41: Coproducts (Direct Sums)

Let $\{A_i\}_I$ be a family of Objects. Then a co-cone: $(C, \{\iota_i\})$ of the A_i is an object C together with maps into $\iota_i : A_i \to C$.
A morphism of co-cones of the A_i's is a morphism $\phi : C \to C'$ compatible with the maps from the A_i

$$\begin{tikzcd} & C \arrow[dd, "\phi"] \\ A_i \arrow[ur, "\iota_i"] \arrow[dr, "\iota_i'"'] & \\ & C' \end{tikzcd} \qquad \iota_i' = \phi \circ \iota_i$$

A **coproduct** is an initial object in the category of co-cones of the A_i.
Write: $(\coprod A_i, \{\iota_i\})$.

Remark 156. *Existence of products and co-products are not guaranteed to exist in any given category.*

Example 157.

- *Groups. Given H, G groups, usual direct sum is a coproduct of $\{H, G\}$.*

  Or '$G \oplus H$'

  Have Morphisms:

  - $G \to G \oplus H$ *and* $g \mapsto (g, e_H)$

– *$H \to G \oplus H$ and $h \mapsto (e_G, h)$*

Given any group K and maps $G \xrightarrow{\phi} K$ (co-cone) and $H \xrightarrow{\psi} K$, we get a unique map $G \oplus H \to K$ given by $(g, h) \mapsto \phi(g) \cdot \psi(h)$.

Theorem 158. *Coproducts exist in $R-$Mod.*

Proof. Let $\{M_i\}_I$ be a family of $R-$Modules.
Let $\coprod M_i = \{\sum_{i \in I} m_i\}$ (finite formal sums)
R-Module:

$$\sum m_i + \sum m_i' = \sum m_i + m_i'$$

$$r \sum m_i = \sum r m_i \qquad \text{Works since each } M_i \text{ is a } R - Module$$

Define co-cone structure

$$\iota_i : M_i \to \coprod M_i$$

$$m_i \overset{\iota_i}{\mapsto} m_i$$

Check $\iota_i(m_i + m_i') = m_i + m_i' = \iota(m_i) + \iota(m_i')$ and $\iota_i(rm_i) = rm_i = r\iota_i(m_i)$.
Therefore it's a R-Module homomorphism.
Therefore this is a co-cone over the M_i's. □

Note 159. *Suppose* $(C, \{\psi_i\})$ *is a co-cone.*

$$\begin{tikzcd} & \coprod M_i \arrow[dd, dashed, "\phi"] \\ M_i \arrow[ur, "\iota_i"] \arrow[dr, "\psi_i"'] & \\ & C \end{tikzcd}$$

How about $\phi(\sum m_i) = \sum \psi_i(m_i)$*? Check:* $\phi \circ \iota_i = \psi_i$*, so we would have:*

$$\psi \circ \iota_i(m_i) = \phi(m_i) = \psi_i(m_i)\checkmark.$$

Furthermore, we can check this is a $R-$*linear homomorphism e.g.* $\phi(\sum m_i + \sum m_i') = \phi(\sum m_i) + \phi(\sum m_i')$.

Therefore ϕ *is a map of co-cones, I need it to be uniquely determined (check this).*

Note that on each $m_i \in M_i\checkmark$

Therefore, also on $\sum m_i$*, since every element of coproduct* $\coprod M_i$ *is uniquely expressible as a formal sum.*

Therefore, $\coprod M_i$ *is a coproduct in* $R-$*Module.*

Definition 42

This is a special case
$$\{M_i\}_I = \{R_i \simeq R\}_I$$
where $R_i = R \cdot 1_i \simeq R$, where 'R as a Module over Itself'.
A **free** $R-$Module is a coproduct $R^I = \coprod R_i$. The set $\{1_i\}$ is a basis for R^I.

Definition 43: A

asis for an R-Module M is a set $\{x_i\}_I \subset M$ such that

1. It spans M
2. And is linearly independent

HW 6: Modules

Example 160.

1. $\mathbb{R}^n$ *is free*
2. *Any* $k-$*Module is free*
3. $\mathbb{Z}/n$ *is not a free* $\mathbb{Z}-$*Module*
4. $\mathbb{Q}$ *is not a free* $\mathbb{Z}-$*Module*

Theorem 161 (Universal Property of Free Modules)**.** *Let* I *be an index set,* M *an* $R-$*Module, say* $f : I \to M$ *set map,* $i \mapsto m_i$

Then there exists a unique $R-$*Map* $g : R^I \to M$ *such that* $g(1_i) = f(i) = m_i$

Note 162. *Given any* $\{m_i\}_I \subset M$*, there exists a unique* $R^I \to M$ *such that* $1_i \mapsto m_i$*.*

13.5 Class Notes 11-02-2021

Note 163 (Midterm #1)**.** *For* (b)*., we want to show* $|G| = 12 \implies G$ *is not simple.* *Sylow #1 gives us there exists a subgroup of order* 4*. So that* $[G : P_2] = 3$*. So there exists a non-trivial homomorphism:*

$$G \to S_3$$

by (a) *is non-trivial and ISH. So the Kernel is a non-trivial normal subgroup.*

Name: Joseph McGuire   Class: Math 561(Fall 2021)

HW 6: Modules

Note 164 (Last Time)**.** *Ho9.pdf posted*
Write down the universal property of a coproduct

- *Set : Disjoint Union*
- *Ab : Direct Sum*
- *Grp : not easy, Includes Free Groups*
- *R - Mod : Direct Sum*

Note 165. R^I *or* R^n *if* $|I| = n$.
The true analog of a vector space. Have

- $M_{m\times n}(R) = \hom_R(R^n, R^m)$
- $M_n(R) = \mathrm{end}_R(R^n)$
- $GL_n(R) = Aut_R(R^n)$

If R is commutative, the usual determinant

$$\det : GL_n(R) \to R^\times$$

Example 166. $GL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = \pm 1 \right\}$.
We can check that:

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

These two generate the free group on 2 generators.

Note 167. *Finitely generated modules are similar to finite-generated vector spaces, their span is finite.*

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 6: Modules

Remark 168. *If V is a $k-$Vector Space, then any $k-$Submodule is also a vector space, of at-most-equal dimension*

Therefore submodule of free $k-$Module of rank n is free of rank $m \leq n$. (i.e. Every submodule of a $k-$Module has a basis)

Philosophy: PID is close to being a field, so that

Note 169 (Basic Idea of Finitely Generated Modules over a PID)**.** *Given a finitely generated module M/PID ring. Have a surjection of R-Modules $\pi : R^n \to M$.*

If $x = \{x_1, \ldots, x_n\}$ is a generating set, send $1_i \mapsto x_i$ ($\pi(1_i) = x_i$), since M is finitely generated and x is a generating set, this has to be a surjection.

Therefore, we have $R^n/\ker(\pi) \simeq M$ (1st Isomorphism Theorem).

Theorem 170. *By diagonalizing $\ker(\pi)$, get $M \simeq \coprod R/(d_i)$.*

Where (d_i) are called invariant factors such that d_i/d_j if $i < j$

Theorem 171. *Let R be a PID. Suppose M isa free $R-$Module of rank n, and K is a submodule. Then K is free of rank $m \leq n$.*

Proof. False if R is not a PID. Examples:

$$R = \mathbb{Z}_4 \qquad M = \mathbb{Z}_4 \qquad K = \mathbb{Z}_4 \cdot 2 = \{0, 2\},$$

not free since $\{2\}$ is not linearly independent.

$k = 0$✓

Assume $k \neq 0$. $n \geq 1$.

Induct on n. $n = 1$, then $M \simeq R$ so $K \simeq I \subset R$ is an ideal. So that K is free, and rank 1, since R is a PID. Since $K = R \cdot f$, but is f linearly independent? Yes, since $a \cdot f = 0 \implies a = 0$ since we're in a PID.

$n > 1$. Say $M = R^n$ and let $M' = R^{n-1}$ first $n-1$ copies. Therefore

$$0 \longrightarrow M' \longrightarrow M \longrightarrow\xrightarrow{\pi} R \longrightarrow 0$$

short exact sequence ($R \simeq M/M'$).

So an Induced map is:

$$0 \longrightarrow K \cap M' \longrightarrow K \stackrel{\pi}{\longrightarrow} K'' \longrightarrow 0$$

$K'' \subset R$, free $rk \leq 1$ by base case. By the universal property of a Free Module, there exists a map back into K, that is:

$$K \simeq (K \cap M') \oplus K''$$

Notice:

$$0 \longrightarrow (K \cap M') \longrightarrow K \longrightarrow K'' = R \cdot f \longrightarrow 0$$

Since $K \to R \cdot f$, we have $a \mapsto f$.

Hence $R \cdot f \to K$ given by $f \mapsto a$ splits the map, which implies the result.

So $K \cap M'$ is free rank less than or equal to $n-1$ and K'' is free rank less than or equal to 1. So that K is free, and has rank less than or equal to n. $\square$

13.6 Class Notes 11-04-2021

Updated the notes since last time

Note 172. *Last Time:*

Theorem 173. *If R is a PID, M is a free $R-$Module (Has some Index Set and Rank: n); that is $R^n \simeq M$. Then any submodule N of M is free and it's rank m is less than or equal to n.*

This doesn't hold if R isn't a PID, example in homework. Analagous to the result for Vector Spaces.

Corollary 174. *If R is a PID, then $R^m \simeq R^n \iff m = n$.*

Note 175. *That is the rank is invariant for Modules over a PID. Dimension is a well-defined concept.*

HW 6: Modules

Remark 176. *True for R being commutative.*

PID is any ring where all Ideals are principal, i.e. their generated by a single element.

Proof of Corollary. If $R^m \simeq R^n$ then R^m is isomorphic to a sub module of R^n, so $m \leq n$. And vice versa, $n \leq m$, by theorem, $n = m$.

Conversely, it also follows. □

Note 177. *Co-products and products are dual concepts of each other, opposite, but similar.*

On homework $\hom(A \oplus B, M) \simeq \hom(A, M) \times \hom(B, M)$*, the "$\oplus$" here is a coproduct in some category, while "$\times$" is a product in the homomology category. Note that we'll need two maps:*

$$A \to A \oplus B$$

$$B \to A \oplus B \xrightarrow{\varphi} M$$

And we'll get a unique map:

$$B \to M.$$

This means that given a map: $\hom(A \oplus B, M) \to \hom(B, M)$ *and* $\hom(A \oplus B, M) \to \hom(A, M)$*. This is a co-cone.*

For the product, we'll get maps: $H_A \times H_B \to H_A$ and $H_A \times H_B \to H_B$ (Cone).

That is, given any maps $P \to H_A$ and $P \to H_B$, by the universal property, we get a new map:

$$P \to H_A \times H_B$$

That is exactly the universal property for products.

Take $\hom(A \oplus B, M)$ *then we have a map to* $\hom(A, M)$ *and* $\hom(B, M)$ *by the universal properties for products.*

Cones map products into their things, and co-cones map their things into co-products.

Note 178. *Homework problem 8 is a big problem, done in office hours.*

Why is irreducible mean cyclic in submodules?

Consider a ring R and module M irreducible. (Note that irreducible we'll assume non-trivial)

Claim: M cyclic. i.e. that $M \simeq R \cdot f$ for some $f \in M$. (Converse is false)

Pick $f \in M \setminus \{0\}$, then $R \cdot f \subset M$ is a submodule. (Why?) We can check that it will be a submodule, since $R \cdot f$ is an additive subgroup and f is stable under R.

So therefore $R \cdot f = 0$ or M. But we assumed that $f \neq 0$, so that $R \cdot f = M$.

If R is a matrix ring, that leads into representation theory.

Note 179. *Recall the scheme for the proof of finitely generated Modules over PID's.*

R is a PID and M is a finitely generated $R-$Module.

We want to show that $M \simeq \coprod R/(d_i) \oplus R^f$

To start: Have a map $\pi : R^n \to M \to 0$ and the kernel is a sub-module of R^n; $\ker(\pi) \subset R^n$ and it's free with rank $m \leq n$ (by Theorem).

$$R^m \xrightarrow{\iota} R^n \xrightarrow{\pi} M \to 0$$

This first R^n is the $\ker(\pi)$.

Idea: Diagonalize the map ι, that is embed R^m into R^n in a diagonal manner.

We need: ***Smith Normal Form***

Definition 44

Let R be commutative, and $A, B \in M_{m\times n}(R)$, i.e their homomorphism from R^m into R^n.
We say A, B are equivalent if there exists a $P \in GL_n(R)$ and $Q \in GL_m(R)$ such that:

$$B = QAP$$

So since $R^n \xrightarrow{A} R^m$ we can change the basis of R^n or R^m independent of A. Write $A \sim B$.

HW 6: Modules

Theorem 180 (Smith Normal Form). *Let R be a PID, $A \in M_{m\times n}(R)$, then A is equivalent to a diagonal matrix.*

$$A \sim \mathrm{Diag}\{1,\dots,1,d_1,\dots,d_r,0,\dots,0\}$$

with t-number of 1's, r-number of d_i's, and f-number of 0's. d_i divides d_j if $i<j$ and $d_i \neq 0$ for all i.

If R is a ED, then this can be done by elementary row and column operations. Meaning that I can use elementary row operations on the left and those stack to make a Q, then I use column operations on the right and those build up to make my P.

Using Gauss - Jordan operations, I make the top left element a unit and zero out the remaining column elements. Continue right-wards till you have a diagonal matrix.

That diagonal matrix is

$$\coprod_{i=1}^{r} R/(d_i) \oplus R^f$$

Theorem 181 (Obtaining the d_i's). *Let R be a PID. Equivalent matrices have the same d_i's.*

Moreover, suppose rank of $A = t+r$.

For i such that $1 \le i+t \le r+t$ let $\Delta_i = \gcd$ of determinants of rank $i+t$ minors of A. This is well-defined since R is a PID.

$$d_1 \sim \Delta_{1+t} \qquad d_2 \sim \Delta_{2+t}\Delta_{1+t}^{-1} \qquad \dots \qquad d_r \sim \Delta_{r+t}\Delta_{r+t-1}^{-1}.$$

13.7 Class Notes 11-05-2021

Note 182. *Last Time:*

$$M \simeq \coprod_{i=1}^{r} R/(d_i) \oplus R^f$$

where $\coprod_{i=1}^{r} R/(d_i)$ is the torsion part, and R^f is the free part.

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 6: Modules

Theorem 183. *R PID, M free rank n and $N \subset M$ submodule $\implies$ N free with rank $m \leq n$.*

Corollary 184. *R is a PID and $R^m \simeq R^n \iff m = n$. (Assuming R is a commutative ring)*

Theorem 185. *R PID, $A \in M_{m\times n}(R)$. Then $A \sim \mathrm{Diag}\{1, \ldots, 1, d_1, \ldots, d_r, 0, \ldots, 0\}$ then $d_i | d_j$ for $i < j$.*
R is a Euclidean Domain, then $D = PAQ$, $P =$ Product of elementary row operations and $Q =$ Product of elementary column operations

Note 186. *Goal is to compute the d_i's when A is small.*

Note 187. *On Homework, G is abelian group say:*

$$G \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

then $G \simeq \ker(\pi) \oplus \mathbb{Z}$.
(HW 6.8)

Theorem 188. *R is a PID, $A \in M_{m\times n}(R)$, rank $A = t + r$. For $i : 1 \leq i \leq r + t$, $\Delta_i = \gcd(\deg -(i)$Minors of $A)$.*
Then $d_1 \sim \Delta_1$, $d_2 \sim \Delta_2\Delta_1^{-1}, \ldots, d_r \sim \Delta_r\Delta_r^{-1}$.

HW 6: Modules

Example 189. *Consider:*

$$A = \begin{bmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \\ 0 & 0 & 0 \end{bmatrix}$$

so $d_1 = 3$, $\Delta_2 = \gcd(-90, -54, 108) = 2 \cdot 3^2 = 18$, $d_2 = \dfrac{18}{3} = 6, d_3 = 0, f = 1$*(number of 0's in the Smith Normal Form).*

Example 190. *Suppose* $A \sim B = QAP$.
The k_i *entry of* QA *is* $\sum_j^m q_{k_j} a_{ji}$. *Then* $R_k(QA)$ *is the* k^{th} *row of* QA *and:*

$$R_k(QA) = q_{k_1} R_1(A) + q_{k_2} R_2(A) + \ldots + q_{k_m} R_m(A),$$

that is a $R-$*Linear combination of rows of implies* $\deg(i)$ *minors of* QA *are R-linear combinations of degree* i *minors of* A.

$$\Delta_i(A) \text{ divides each } \deg -i \text{ minor of } QA$$

so that $\Delta_i(A) | \Delta_i(QA)$.
Similarly, $\Delta_i(A)|\Delta_i(AP)$. *Therefore* $\Delta_i(A)|\Delta_i(QAP) = \Delta_i(B)$ *Since* $\Delta_i(A)|\Delta_i(QA)|\Delta_i(QAP)$.

Note 191. *Determinant:* $\det : GL_2(R) \to R^\times$ *is multilinear in that:*

$$\begin{bmatrix} r_1 \\ r_2 + r_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c + c' & d + d' \end{bmatrix} \mapsto \det \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} + \det \begin{bmatrix} r_1 \\ r_2' \end{bmatrix}$$

Note 192. *Say* $A \sim \text{Diag}\{d_1, \ldots, d_{r+t}, 0, \ldots, 0\}$.
With $d_i | d_j$ *with* $i < j$, *so that* $\Delta_1 \sim d_1, \Delta_2 \sim d_1 d_2 \implies d_2 \sim \Delta_2 \Delta_1^{-1}, \ldots, \Delta_{r+t} \sim d_1 \ldots d_{r+t} \implies d_{r+t} \sim \Delta_{r+t} \Delta_{r+t-1}^{-1}$
Same Δ_i*'s implies same* d_i*'s*

14 Handout 6: Module Theory Basics

14.1 Modules and Morphisms

HW 6: Modules

14.1.1 Objects

Definition 45: A

left) $R-$module is an Abelian group $(M,+)$ together with a pairing:

$$\begin{aligned} R \times M &\to M \\ (r,m) &\mapsto r \cdot m \end{aligned}$$

such that

1. $(r+s) \cdot m = r \cdot m + s \cdot m$
2. $r \cdot (s \cdot m) = (rs) \cdot m$
3. $0 \cdot m = 0$ and $1 \cdot m = m$
4. $r \cdot (m+n) = r \cdot m + r \cdot n$

Alternatively, an $R-$Module is an Abelian group $(M,+)$ with an action of R on M.

HW 6: Modules

Definition 46: Right Modules

$R-$Module is the same, except we write $M \times R \to M$ instead. Let's note that it's immediate $r \cdot 0 = r \cdot (0+0) = r \cdot 0 + r \cdot 0$, so $r \cdot 0 = 0$ by group cancellation.

Example 193. *Examples of Modules include:*

1. *If k is a field, then a $k-$module is a $k-$Vector Space. If we have a $k-$Module is a $k-$Vector Space, then k is a Field.*
2. *A $\mathbb{Z}-$Module is an Abelian Group, and every Abelian group is a $\mathbb{Z}-$Module.*
3. *If $I \subset R$ is an ideal, then I is an $R-$Module.*
4. *If $I \subset R$ is an ideal, then R/I is an $R-$Module (e.g. $\mathbb{Z}/n$ is a $\mathbb{Z}-$Module)*
5. *If k is a field and $R = k[x]$, then an $R-$Module is a $k-$Vector Space together with a linear transformation T (note x^n will be $T \circ T \circ \ldots \circ T$, n-times). We have a $1-1$ correspondence.*

   $$\{k[x]-\textit{Modules}\} \iff \{(k \textit{ - Vector Spaces together with a linear transformation } T)\}$$

6. *Let $\rho : G \to GL(V)$ be a complex linear representation. Then V is a $\mathbf{C}[G]-$module, where $\mathbf{C}[G]$ is the **group ring**. Also have a $1-1$ correspondence.*

Example 194. *Let $R = \mathbb{Z}[x]$, $p(x) = x^2+1$, then $I = R \cdot p = \{f(x) \cdot (x^2+1) : f(x) \in \mathbb{Z}[x]\}$ is an ideal of R, hence it's an $R-$Module. In fact, the definition of ideal is precisely an abelian subgroup of $(R, +)$ that is stable under scalar left multiplication.*

Consider the ring of Gaussian Integer $\mathbb{Z}[i]$. Can you see how to make it a $\mathbb{Z}[x]-$Module?

HW 6: Modules

14.1.2 Morphisms

Definition 47: $R-$**Module Homomorphisms**

n **R-Module Homomorphism** (or just $R-$Homomorphism) $f : M \to N$ is a homomorphism of the underlying abelian groups that commute with the $R-$actions:

$$f(rm) = rf(m)$$

we write $\hom_R(M, N)$.

Definition 48: T

e **category of R-Modules,** denoted $R - \text{Mod}$, is the category whose objects are $R-$Modules, and whose morphisms are $R-$Module Homomorphisms.

Example 195. $\hom_R(M, N)$ *is an* $R-$*Module, under the operation* $(f+g)(m) = f(m)+g(m)$ *and* $(rf)(m) = f(rm)$.
When $M = N$*, composition of functions makes* $\hom_R(M, N)$ *into a ring, denoted by:*

$$\text{End}_R(M)$$

the endomorphism ring of M*.*

HW 6: Modules

Example 196. *Group homomorphisms $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ are completely determined by $\phi([1]_m)$. By Lagrange's Theorem, $|\phi([1]_m)|$ divides $d = \gcd(m, n)$, so there are as many homomorphisms as there are elements in the cyclic subgroup $\langle [c]_n \rangle$ of $\mathbb{Z}_n$, where $c = \dfrac{n}{d}$ (note $|[c]_n| = d$. Therefore we have a bijection:*

$$\hom(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_d$$

what maps to $[1]_d$?

An abelian group homomorphism is a $\mathbb{Z}-$Module homomorphism. If $\phi \in \hom(\mathbb{Z}_m, \mathbb{Z}_n)$ prove $\phi(3[1]_m) = 3\phi([1]_m)$. The set $\hom(\mathbb{Z}_m, \mathbb{Z}_n)$ is a group.

If $\phi, \psi \in \hom(\mathbb{Z}_m, \mathbb{Z} - n)$ what is $\phi + \psi$?

Is the bijection a group isomorphism?

The group $\hom(\mathbb{Z}_m, \mathbb{Z}_n)$ is a $\mathbb{Z}-$Module. If $\phi \in \hom(\mathbb{Z}_m, \mathbb{Z}_m)$, how is 3ϕ defined?

If $m = n$, then $\hom(\mathbb{Z}_m, \mathbb{Z}_n) = \mathrm{End}(\mathbb{Z}_n)$ is a ring. If $\phi \in \mathrm{End}(\mathbb{Z}_n)$, what is ϕ^2? Is $\mathrm{End}(\mathbb{Z}/n)$ ring isomorphic to $\mathbb{Z}_n$?

Definition 49: Ring Action

Suppose R is a ring with 1, and M is an Abelian group. Then $\mathrm{End}_{\mathbb{Z}}(M)$ is a ring with 1. An **action** of R with 1 on M is a ring homomorphism $\alpha : R \to \mathrm{End}_{\mathbb{Z}}(M)$. Since α is a ring homomorphism, we have

- $(r + s) \cdot m = r \cdot m + s \cdot m$, since α is a group homomorphism
- $r \cdot (s \cdot m) = (rs) \cdot m$, by definition of composition of functions
- $0 \cdot m = 0$ and $1 \cdot m = m$, by definition of the zero and identity endomorphisms
- $r \cdot (m + n) = r \cdot m + r \cdot n$, since $\alpha(r)$ is a group endomorphism

Therefore, an R-Module is an Abelian group $(M, +)$ with an $R-$Action.

Name: Joseph McGuire Class: Math 561(Fall 2021)

HW 6: Modules

14.2 Submodules, Quotient Modules, Finitely Generated Modules

Definition 50

Let M be a (left) $R-$Module

1. A **submodule** is a subgroup $(N, +) \leq (M, +)$ that is stable under R
2. A **quotient** of M is the Abelian group quotient determined by a submodule $N \subset M$, with the induced action
3. M is **generated by a set X** if $M = \{\sum rx : x \in X\}$.
4. M is **finitely generated** if there exists a finite set X such that M is generated by X.
5. M is **cyclic** if $M = R \cdot m$ for some $m \in M$
6. M is **irreducible** if it has no submodules except for (0) and M.

Example 197.

- *$\mathbb{Z}$ is a finitely generated $\mathbb{Z}-$Module.*
- *$\mathbb{Q}/\mathbb{Z}$ is not finitely generated $\mathbb{Z}-$Module (prove).*
- *Every irreducible module is cyclic*
- *The $k[x]$-Submodule, $k[x]\cdot(x^2+1)$ is cyclic, but not irreducible: It's $k[x]$-isomorphic to $k[x]$.*
- *The $\mathbb{R}[x]/(x^2+1)$ is cyclic, and irreducible. It is $\mathbb{R}[x]-$Isomorphic to* $\mathbf{C}$

Example 198. *Let*

$$R = \mathbb{R}[x], \qquad T = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad V = \mathbb{R}^3 \text{ on basis } \{e_1, e_2, e_3\}.$$

Then V is an $\mathbb{R}[x]-$Module, and $\mathbb{R}[x] \cdot e_1$ and $\mathbb{R}[x] \cdot e_3$ are (irreducible) cyclic submodules of V, then $xy-$plane and the $z-$axis, respectively. Check it out, $\mathbb{R} \cdot e_1$ is a subgroup that is not a submodule.

Geometrically, these two cyclic submodules are invariant subspaces of V. In fact, we verify easily that

$$\{k[x] - \textit{submodules of } V\} \iff \{\textit{invariant subspaces of } V\}$$

In this case, on $\mathbb{R}[x] \cdot e_1$, x acts as a $\pi/2$ rotation. On $\mathbb{R}[x] \cdot e_3$, x acts as multiplication by 1.

Example 199. *Suppose that M is an irreducible $R-$Module. Then $\operatorname{End}_R(M)$ is a ring, and also a left $R-$Module. This is called an **R-Algebra**.*

What kind of ring is it?

*Since the image of a nonzero R-Endomorphism is a nonzero $R-$Submodule, each endomorphism is bijective, hence invertible. Since there's no reason a priori why the ring should be commutative, we conclude that $\operatorname{End}_R(M)$ is an **R-Division Algebra**.*

*This result is called **Schur's Lemma***

14.3 Isomorphism Theorems

Theorem 200 (First Isomorphism Theorem)**.** *Suppose $f : M \to N$ is an $R-$Module homomorphism. Then $\ker(f)$ is a submodule of M, and we have aan isomorphism*

$$M/\ker(f) \xrightarrow{\sim} f(M) \leq N$$

There's a 1-1 correspondence between submodules of M containing $\ker(f)$, and submodules of $f(M)$ given by $M' = f^{-1}(N')$ for $N' \leq f(M)$

Proof. First we show that $\ker(f)$ is an $R-$Submodule. We know from group theory that $\ker(f)$ is an Abelian subgroup of M, so it remains to show $\ker(f)$ is stable under the action of R on M. But if $m \in \ker(f)$, then $f(rm) = rf(m) = 0$, since f is $R-$Linear, so $rm \in \ker(f)$. This proces the first statement.

Next we show that $M/\ker(f)$ is an $R-$Module, with action $r(m + \ker(f)) = rm + \ker(f)$. This is well-defined since $\ker(f)$ is an $R-$Module: If $m+\ker(f) = m'+\ker(f)$, then $m-m' \in \ker(f)$, so $r(m - m') \in \ker(f)$ since $\ker(f)$ is an R-module. Therefore $rm - rm' \in \ker(f)$ by the module axioms, and this shows the action is well defined. To show that the action satisfies the other module axioms is easy, and relies on the analogous axioms for M. For example, we check easily #1 :

$$(r+s)\cdot(m+\ker(f)) := (r+s)m+\ker(f) = rm+sm+\ker(f) = (rm+\ker(f))+(sm+\ker(f)) \checkmark$$

HW 6: Modules

Next we show the map $\phi : M/\ker(f) \to f(M)$ given by $\phi(m + \ker(f)) = f(m)$ is an R-Module isomorphism. We know $\phi : M/\ker(f) \to f(M)$ is a group isomorphism by group theory. Since $\phi(rm + \ker(f)) = f(rm) = r(f(m)) = r\phi(m + \ker(f))$, the map is $R-$linear. Therefore ϕ is an $R-$module isomorphism, as desired. This proves the second statement.

To finish, we have $1 - 1$ correspondence for the underlying abelian groups by group theory, and it remains to show it extends to $R-$modules, i.e., a subgroup $M' \leq M$ containing $\ker(f)$ is a submodule if and only if $f(M') \leq f(M)$ is a submodule. Suppose then that $M' \leq M$ is a submodule containing $\ker(f)$. Then $f(M') \leq f(M)$ is a subgroup, and $r \cdot f(m') = f(rm')$ since f is $R-$linear, and $f(rm') \in f(M')$ since M' is a submodule. Therefore $f(M')$ is stable under the action of R, so it's a submodule of $f(M)$. Conversely, if $f(M')$ is a submodule of $f(M)$, and $m \in M'$, then $rf(m')$ is in $f(M')$ by our hypothesis, and this is $f(rm')$ since f is $R-$linear. Since M' contains $\ker(f)$, we must have $rm' \in M'$, which shows that M' is stable under the $R-$action, hence M' is an $R-$Module. Therefore the correspondence extends to $R-$Modules. This completes the proof! $\square$

Theorem 201 (2nd and 3rd Isomorphism Theorems)**.** *Suppose A and B are submodules of an $R-$Module M.*

I Then $(A + B)/B \simeq A/(A \cap B)$

II If $A \subset B$, then $(M/A)/(B/A) \simeq M/B$.

HW 6: Modules

15 Handout 7: Products and Coproducts

15.1 Categorical Products and Coproducts

Note 202. *A product of a family of objects is the most general object of the category for which there's a morphism into each member of the family.*

Where a coproduct of a family of objects is the least specific object into which there's a morphism from each member of the family.

Definition 51: L

t C be a category and I a **discrete index category**, which is a category whose objects are in an index set I, and whose morphisms are only identity morphisms. Let $F : I \to C$ be a functor. This is just a formalism for specifying a family of objects $\{A_i\}_I$ in C.

Definition 52: A

cone to F, or a cone to $\{A_i\}_I$, is a pair $(A, \{\tau_i\}_I)$, with A an object in C, and $\tau_i : A \to A_i$ a morphism.
The cones to F form a category whose morphisms $\phi : (A', \{\tau_i'\}) \to (A, \{\tau_i\})$ are morphisms $\phi : A' \to A$ in C such that $\tau_i' = \tau_i \circ \phi$.

Definition 53: A

co-cone to F, or a **co-cone to** $\{A_i\}_I$, is a pair $(B, \{\iota_i\}_I)$, with B an object in C, and $\iota_i : A_i \to B$ a morphism.
The co-cones to F form a category whose morphisms $\psi : (B, \{\iota_i\}) \to (B', \{\iota_i'\})$ are morphisms $\psi : B \to B'$ in C such that $\iota_i' = \psi \circ \iota_i$.

HW 6: Modules

Definition 54: Categorical Products

I The **Categorical Product**, denoted:

$$\left(\prod_{i\in I} A_i, \{\pi_i\}\right)$$

is a terminal object in the category of cones to $\{A_i\}$. Thus for any cone $(A, \{\tau_i\})$ to $\{A_i\}$ there exists a unique map $\phi : A \to \prod_i A_i$ such that the follow diagram commutes for all j:

$$\begin{tikzcd} & \prod_{i\in I} A_i \\ A \arrow[ur, dashed, "\phi", "!"'] \arrow[r, "\tau_j"'] & A_j \arrow[u, "\pi_j"'] \end{tikzcd}$$

II The **categorical coproduct**, or **sum**, denoted

$$\left(\coprod_{i\in I} A_i, \{\iota_i\}\right)$$

is an initial object in the category of co-cones to $\{A_i\}$. Thus for any co-cone $(B, \{\eta_i\})$ to $\{A_i\}$. Thus for any co-cone $(B, \{\eta_i\})$ to $\{A_i\}$ there exists a unique map $\phi : \coprod_i A_i \to B$ such that the following diagram commutes for all j:

$$\begin{tikzcd} & \coprod_{i\in I} A_i \arrow[dl, dashed, "\psi"', "!"] \arrow[d, "\iota_j"] \\ B & A_j \arrow[l, "\eta_j"] \end{tikzcd}$$

Remark 203. *Being terminal and initial objects in a category entails uniqueness up to unique isomorphism. For if A and B are both terminal objects in a category C, then there exists precisely one morphism $f : A \to B$ and $g : B \to A$, hence $g \circ f : A \to A$*

is uniquely determined, hence $g \circ f = id_A$ and similarly $f \circ g = id_B$. Thus f and g are each bijections, whose inverses are morphisms, hence they are uniquely determined isomorphisms.

Note 204. *We say the above constructions are products and coproducts in a category C, usually omitting reference to the categories of cones and co-cones to a given family of objects.*

The above terminal and initial properties are codified as ***universal properties in C***. *The universal property for products : If $\prod_{i \in I} A_i$ is a product in C, and A is an object of C for which there are maps $\tau_i : A \to A_i$ for each $i \in I$, then there's a unique map $\phi : A \to \prod_i A_i$ satisfying the above commutative diagram.*

For coproducts : If $\coprod_{i \in I} A_i$ is a coproduct in C, and B is an object in C for which there are maps $\eta_i : A_i \to B$ for each i, then there's a unique map $\psi : \coprod_i A_i \to B$ satisfying the above commutative diagram.

15.2 Module Products and Coproducts

Theorem 205. *There exist products and coproducts in $R-Mod$.*

Proof. Products: Let M and N be two $R-$Modules and let $M \times N$ denote the Cartesian product with pointwise addition, 'diagonal' R-action $r(m, n) = (rm, rn)$, and $R-$linear projection maps $\pi_m : M \times N \to M$ and $\pi_n : M \times N \to N$. Similarly, for a family $\{M_i : i \in I\}$ of modules, let $\prod_{i \in I} M_i$ denote the Cartesian product, with pointwise addition, diagonal $R-$action and R-linear projection maps $\pi_j : \prod_i M_i \to M_j$ for each j. Clearly the latter generalizes the former, so we treat the latter. It's easy to check that $\prod_i M_i$ is an $R-$Module, hence $(\prod_i M_i, \{\pi_i\})$ is a cone to $\{M_i\}_I$: An $R-$module with a family of morphisms $\{\pi_i\}$ to $\{M_i\}$. Note that every element of $\prod_i M_i$ is uniquely determined by its projections. To show it's a product in $R-$Mod it remains to show it has the universal property, which in category theoretic language means it's terminal in the category of cones to $\{M_i\}_I$.

If $(P_i\{\tau_i\})$ is a cone to $\{M_i\}_I$, then we define $\tau : P \to \prod_i M_i$ by $\tau(a) = (\tau_i(a))$. This is an $R-$homomorphism, since the τ_i are $R-$linear, and the $R-$action on the product is diagonal. It is a map of cones since $\pi_i(\tau(a)) = \tau_i(a)$, and it's uniquely determined since $\tau(a)$ is uniquely determined by its projection $\tau_i(a)$ to the M_i. This completes the proof for products.

(Coproducts)

Let M and N be R-Modules and let $M \oplus N = \{m + n : m \in M, n \in N\}$ denote the set of formal sums, with pointwise addition, distributive $R-$action $r(m+n) = rm + rn$, and R-linear maps $\iota_M : M \to M \oplus N$ and $\iota_N : N \to M \oplus N$ given by $\iota_M(m) = m + 0$ and $i_N(n) = 0 + n$. Similarly for a family $\{M_i : i \in I\}$ of modules, let $\coprod_{i \in I} M_i = \{\sum_i m_i : i \in I\}$ denote the set of formal finite sums, with pointwise addition, distributive $R-$action and $R-$linear maps $\iota_i : M_i \to \coprod_{i \in I} M_i$. Note that there's no 'ambient module' containing M and N, or the M_i, and in which these sums take place; they are just formal sums, and every element is thus uniquely expressible as a sum of some $m \in M, n \in N$ or of the $m_i \in M_i$. It's easy to check that each construction is an R-Module, and $(M \oplus N, \{\iota_M, \iota_N\})$ and $(\coprod_i M_i, \{\iota_i\}_I)$ are co-cones to $\{M_i\}$. To show they are coproducts it remains to show they are initial as co-cones.

We show it for $\{M_i\}_I$. If $(Q, \{\eta_i\})$ is a co-cone, define a map $\psi : \coprod_i M_i \to Q$ by $\psi\left(\sum_i m_i\right) = \sum_i \eta_i(m_i)$. This is well defined since the sums are finite, $R-$linear since the η_i are R-linear, and it's a map of co-cones since evidently $\eta_i = \psi \circ \iota_i$. Uniqueness: ψ is determined uniquely on the $m_i \in M_i$ by the rule $\psi(m_i) = \psi \circ \iota_i(m_i) = \eta_i(m_i)$. Since every element of $\coprod_i M_i$ is uniquely a sum of the m_i, ψ is uniquely determined. This completes the proof. $\square$

Remark 206. *There's a canonical morphism $\theta : \coprod_i M_i \to \prod_i M_i$ defined by $\theta\left(\sum m_i\right) = (m_i)$, where the sum is finite, and the indices of the product that do not appear in the sum are set to zero. Note the definition of this map requires a zero element. This map is clearly injective. It therefore realizes the coproduct as a canonical submodule of the product. If the index set is finite, the map is onto, and the coproduct and product are then canonically isomorphic.*

15.3 Free Modules

Definition 55

Let R be a ring with unity. A **free module** is a coproduct:

$$R^I := \coprod_{i \in I} R_i$$

for some index set I, where $R_i = R \cdot 1_i \simeq R$ is the left R-Module. The set $\{1_i\}_I$ will be called a **basis**. A free $\mathbb{Z}-$Module is called a free Abelian group.

Remark 207. *An $R-$Module M is free if and only if it has a basis, which is a subset $\{x_i\}_I$ on an index set I, such that:*

1. *The x_i span M, i.e., $M = \sum_i R \cdot x_i$ (finite sums)*
2. *The x_i are linearly independent: $\sum_i a_i x_i$ implies $a_i = 0 \ \forall i$.*

To see this is equivalent, if M has basis $\{x_i\}_I$, define a map

$$\coprod R_i \to M$$

$$\sum a_i \cdot 1_i \mapsto \sum a_i \cdot x_i$$

using the initial property of the coproduct with respect to co-cones. This is 1-1 by linear independence, and obviously onto. Conversely, the elements $\{1_i\}$ for R^I are easily seen to be a basis.

Example 208.

1. *If k is a field, every $k-$Module is free.*
2. *R^n is a free $R-$Module*
3. *$\mathbb{Z}/n$ is not a free $\mathbb{Z}-$Module*
4. *$\mathbb{Q}$ is not a free $\mathbb{Z}-$Module*
5. *$2\mathbb{Z}$ is a free $\mathbb{Z}$-Module*

Note 209. *Since a free module is the coproduct with respect to the indexed family $\{R_i\}_I$ and a morphism $f_i : R_i \to M$ is completely determined by $f_i(1_i)$, it has the following universal property:*

Suppose M is a module, and $f : T \to M$ is a set-map. Then there's a unique $R-$Linear map $g : R' \to M$, defined by $g(1_i) = f(i)$. For then we have $R-$Linear maps $f_i : R_i \to M$ for each i, given by $f_i(r \cdot 1_i) = rf(i)$, which makes M into a co-cone for the $\{R_i\}_I$, inducing a unique map $R^I \to M$ since R^I is initial in the category of co-cones to $\{R_i\}_I$.

15.4 Matrices and Determinants over Commutative Rings

HW 6: Modules

Theorem 210. *Let R be a commutative ring with unity. Then we have*

- $M_{m\times n} \simeq \hom_R(R^n, R^m)$
- $M_n \simeq \mathrm{End}_R(R^n)$
- $GL_n(R) \simeq \mathrm{Aut}_R(R^n)$

Definition 56: Determinant of Module

Let R be a commutative ring with 1. Suppose $A = (a_{ij}) \in M_n(R)$. The determinant of A is

$$\det(A) = \sum_{S_n} \mathrm{sgn}(\pi) a_{1\pi(1)} \ldots a_{n\pi(n)},$$

where the **cofactor** a_{ij} is $A_{ij} = (-1)^{i+j}\det(M_{ij})$, where M_{ij} is the $(n-1)\times(n-1)$ matrix obtained by striking the i-th row and j-th column.
The **adjoint** of A is the matrix $\mathrm{adj}(A) = (b_{ij})$ where $b_{ij} = A_{ji}$.

Note 211. *We have formal identities :*

$$\begin{aligned} \det(A) &= a_{i1}A_{i1} + \ldots + a_{in}A_{in} \\ &= a_{1j}A_{1j} + \ldots + a_{nj}A_{nj} \\ 0 &= a_{i1}A_{i'1} + \ldots + a_{in}A_{i'n} \qquad (i \neq i') \\ &= a_{1j}A_{1j'} + \ldots + A_{nj}A_{nj'} \qquad (j \neq j') \end{aligned}$$

hence

$$\det(A)I = A(\mathrm{Adj}(A)) = (\mathrm{Adj}(A))A$$

Remark 212. *Commutativity is important here, with noncommutative rings, no idea what the determinant is even for $n = 2$.*

Theorem 213.

$$GL_n(R) = \{A \in M_n(R) : \det(A) \in R^\times\}.$$

Proof. Formally, we have $\det(AB) = \det(A)\det(B)$ since R is commutative. If $A \in GL_n(R)$, then $\det(AA^{-1}) = \det(A)\det(A^{-1}) = 1$, so $\det(A) \in R^\times$.

Conversely, if $\Delta = \det(A) \in R^\times$, R commutative implies $(\text{Adj}(A))\Delta^{-1} = \Delta^{-1}(\text{Adj}(A))$. Therefore $A(\text{Adj}(A))\Delta^{-1} = \Delta\Delta^{-1}I = I = (\Delta\text{Adj}(A))A$. Conclude A is invertible and $A^{-1} = (\text{Adj}(A))\Delta^{-1}$. ☐

Remark 214. *If R is commutative with 1 and $A, B \in M_n(R)$, then $AB = I$ implies $BA = I$. For if $AB = I$, then since R is commutative,* $\det(A) \in R^\times$ *by multiplicativity of* $\det$*, so $A \in GL_n(R)$ by the previous Theorem. Then $A^{-1}(AB)A = I = (A^{-1}A)(BA) = BA$, by Associativity.*

That is (Left Inverse) $\iff$ (Right Inverse).

Theorem 215. *Suppose R is commutative with 1. If $R^n \simeq R^m$, then $m = n$.*

Proof. Let $\{e_i : 1 \leq i \leq m\}$ and $\{f_i : 1 \leq j \leq n\}$ be the standard bases. Then

$$f_j = \sum_{i=1}^{m} a_{ji}e_i \qquad e_i = \sum_{j=1}^{n} b_{ij}f_j$$

for $a_{ij}, b_{ij} \in R$. By substitution,

$$f_j = \sum_{i,j'}^{m,n} a_{ji}b_{ij'}f_{j'} \qquad e_i = \sum_{i',j}^{m,n} b_{ij}a_{ji'}e_{i'}$$

Applying linear independence, we obtain

$$\sum_i a_{ji}b_{ij'} = \begin{cases} 1 & \text{if } j = j' \\ 0 & \text{if } j \neq j' \end{cases}$$

$$\sum_j b_{ij}a_{ji'} = \begin{cases} 1 & \text{if } i = i' \\ 0 & \text{if } i \neq i' \end{cases}.$$

Now consider the matrices:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \qquad B = \begin{bmatrix} b_{11} & \dots & b_{1n} & 0 & \dots & 0 \\ b_{21} & \dots & b_{2n} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} & 0 & \dots & 0 \end{bmatrix}$$

Then $A, B \in M_n(R)$, $BA = I$, and since R is commutative $AB = I$ by the previous remark. But this is obviously false if $m < n$: $AB \neq I$. Similarly $BA \neq 1$ if $m > n$. We conclude that $m = n$. □

Alternative Proof. Let $m \subset R$ be maximal, then $mM = \{ax : a \in m, x \in M\} \subset M$. Then $M/mM \simeq R^m/mR^m \simeq R^n/mR^n$, but the latter two are $(R/m)^m \simeq (R/m)^n$. Now quote the vector space result. □

Definition 57

The **rank** of $M \simeq R^n$ over commutative R (with 1) is n.

Corollary 216. *Let R be a commutative ring with unity, M a free module with basis $\{e_1, \dots, e_n\}$. Suppose $A = (a_{ij}) \in M_n(R)$. Then the elements*

$$f_i = \sum_j a_{ij} e_j$$

form a basis if and only if $A \in GL_n(R)$.

Proof. We showed that if the f_i form a basis then $A \in GL_n(R)$. Conversely, if $A \in GL_n(R)$ then $m = n$ (in the proof) and we define the f_i. To show the f_i span, we use $BA = I$ to produce each e_k. If $\sum d_j f_j = 0$, then $\sum\limits_{i,j} d_j a_{ji} e_i = 0$, so $\sum\limits_j d_j a_{ji} = 0$, $\forall k$. Since $AB = I$, this shows $d_k = 0$, $\forall k$. □

16 Handout 9: Finitely Generated Modules over a PID

16.1 Submodules of Free Modules Over a PID

Theorem 217. *Let R be a PID. Suppose M is a free $R-$Module of rank n and $K \subset M$ is a submodule. Then K is a free module of rank $m \leq n$.*

HW 6: Modules

Remark 218. *False if R is not a PID. If $P = \mathbb{R}[X,Y]$, $M = R$, and $K = (X,Y)$, then K isn't free. For example, X and Y span K, but aren't linearly independent, since $Y \cdot X = X \cdot Y = 0$. In fact, any two elements $p(X,Y), q(X,Y) \in K$ are dependent, since $qp = pq = 0$.*

On the other hand, no single element spans K, since X and Y are already not $R-$Multiples of a single element of K: R is a UFD (Unique Factorization Domain) and X and Y are distinct primes, hence have no common divisor.

Or if $R = \mathbb{Z}/4$ and $M = R$, the submodule $R\cdot = \{0,2\}$ is not free, for 2 isn't linearly independent since $2 \cdot 2 = 0$, and there's no other choices for a spanning set!

Proof. If $K = 0$ we say it's free of rank zero, done, so we assume $n \geq 1$ and $K \neq 0$.

We induct on the rank n of M. If $n = 1$, then $K \simeq I$ for some nonzero ideal $I \subset R$. Since R is a domain, and R is a PID, K is free of rank 1 ✓.

Assume $n > 1$ and the result holds for modules of rank $< n$. Set $M = R^n$ and $M' = R^{n-1} \subset M$ be the first $n-1$ summands. We have an exact sequence

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{\pi} 0$$

with $M'' = M/M' \simeq R$. Then we have an exact sequence

$$0 \longrightarrow K' \longrightarrow K \xrightarrow{\pi} K'' \longrightarrow 0$$

where $K' = K \cap M'$ and $K'' = \pi(K) \subset M''$. Since K' is a submodule of M', it's free of rank $\leq n-1$, and $K'' \subset M''$ is free of rank ≤ 1, both by induction hypothesis. If $K'' = 0$, then $K' \simeq K$, and we are done. If $K'' \neq 0$, then $K' \oplus K'' \simeq K$ by Homework 6.8. Therefore K is free of rank $\leq n$. □

Corollary 219. *Let R be a PID. Then $R^m \simeq R^n$ if and only if $m = n$.*

Proof. If $m < n$, then there can't be an injection $R^n \to R^m$, by the above theorem, any submodule of R^m has rank at most m.✓ □

16.2 Smith Normal Form for Matrices Over a PID

Note 220. *Let R be a commutative ring with 1. Any R-Module Endomorphism $R^n \to R^n$ may be represented by a matrix $A \in M_n(R)$ so that*

$$M_n(R) \simeq \mathrm{End}_R(R^n)$$

As usual, we put $GL_n(R) = Aut_R(R^n) = M_n(R)^\times$.

Definition 58

We say two $m \times n$ matrices A and A' are equivalent if there exists $P \in GL_n(R)$ and $Q \in GL_m(R)$ such that $A' = QAP$. This is clearly an equivalence relation.

16.2.1 Elementary Row and Column Operations

Definition 59: Row Operations

Let $e_{i,j}$ denote the $i,j-$entry unit in $M_n(R)$, with a single 1 in the i,j-position. Check that elementary row operations are given by left-multiplication matrices:

1. $T_{i,j}(b) = I + be_{i,j}$ for $i \neq j$ $(R_i \mapsto R_i + bR_j)$
2. $D_i(u) = I + (u-1)e_{ii}$ for $u \in R^\times$ $(R_i \mapsto uR_i)$
3. $P_{ij} = I - e_{ii} - e_{jj} + e_{ij} + e_{ji}$ $(R_i \iff R_j)$

Right-Multiplication by the transpose leads to $C_i \mapsto C_i + bC_j$ and $C_i \mapsto uC_i$ and $C_i \iff C_j$, respectively.

Theorem 221 (Smith Normal Form)**.** *Suppose R is a PID and $A \in M_{m,n}(R)$. Then*

$$A \sim \mathrm{Diag}\{1, \dots, 1, d_1, \dots, d_r, 0, \dots, 0\}$$

such that $d_i \in R - \{0\}$ and d_i divides d_j if $i < j$. If R is a Euclidean domain then we can arrange so that Q and P from Definition of equivalent matrices are products of elementary row and column operations, respectively.

Proof. Assume that R is a Euclidean domain, with degree function:

$$\delta : R \to N \cup \{0\} \cup \{\infty\}$$

We may assume $A \neq \{0\}$ else done.

We claim that if a_{11} doesn't divide every entry of A, then we may replace it with an element of smaller degree, using row/column operations. If a_{11} doesn't divide some a_{1j} we have $a_{1j} = a_{11}b_j + b_{11}$, with $\delta(b_{11}) < \delta(a_{11})$, by the Euclidean property, and by committing the column operation $T_{j1}(-b_j)^t : C_j \mapsto C_j - b_j C_1$ we replace a_{1j} with b_{11} and then P^t_{1j} replaces a_{11} with b_{11} ✓.

Similarly if a_{11} doesn't divide some a_{i1}, we may replace it with an element of smaller degree using a row operation. ✓

If a_{11} divides a_{1j} and a_{i1} but not a_{ij}, then we may replace a_{i1} with zero, which replaces a_{ij} with a_{ij} plus a multiple of a_{1j} call it a'_{ij}. Then using T_{i1} we replace a_{1j} with itself plus a'_{ij}, producing an element in row 1 not divisible by a_{11}, and then we lower the degree a_{11} as before ✓. This proves the claim.

Since the degree function takes values in $\mathbb{N} \cup \{0\} \cup \{\infty\}$ and $\delta(a_{11})$ is minimal among all values in R if and only if it's a unit in R, the claim implies that we may assume a_{11} divides every element of A. Then we may use row/column operations to zero out every other entry in R_1 and C_1, so that A is equivalent to:

$$\begin{bmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & \dots & c_{mn} \end{bmatrix}$$

and b_{11} divides c_{kl}. If b_{11} is a unit, we make b_{11}, using an elementary row operation.

Continue with the $(m-1) \times (n-1)$ matrix in the southeast corner, nothing that always b_{11} will divide everything. By induction, A is equivalent via row/column operations to a diagonal matrix of form $\mathrm{Diag}\{1, \dots, 1, d_1, \dots, d_r, 0, \dots, 0\}$, with nonzero entries d_i such that d_i divides d_j for $i < j$ ✓.

If R isn't a Euclidean domain, we modify the argument as follows. Instead of δ we use the length λ, defined to be the number of primes - with multiplicity - appearing in a prime factorization, and ∞ for 0. Then $\lambda(u) = 0 \iff u \in R^\times$, and then u divides everything. We make the analogous claim, that if a_{11} doesn't divide some a_{ij}, then we may replace it with an element of smaller length. If $a_{11} \not| a_{1j}$, commit $C_2 \iff C_j$ so that $a_{11} \not| a_{12}$. Let $d = \gcd(a_{11}, a_{12})$, then $\lambda(d) < \lambda(a_{11})$. By Bezout's theorem there exists elements x, y such that:

$$a_{11}x + a_{12}y = d.$$

Note we have used the fact that R is a PID. Put $s = a_{12}d^{-1}$, $t = -a_{11}d^{-1}$, and behold:

$$\begin{bmatrix} -t & s \\ y & -x \end{bmatrix} \cdot \begin{bmatrix} x & s \\ y & t \end{bmatrix} = I_2.$$

In particular we have an invertible matrix:

$$\begin{bmatrix} x & s \\ y & t \end{bmatrix} \oplus I_{n-2}$$

Right multiplication on A gives a matrix whose first row is $\text{Diag}\{d, 0, b_{13}, \ldots, b_{1n}\}$, and $\lambda(d) < \lambda(a_{11})$. Similarly, we can lower the length if $a_{11} \not| a_{i1}$, and the rest of the proof follows the Euclidean case. □

Theorem 222. *Suppose R is a PID, $A \in M_{m\times n}(R)$ and $rk(A) = t + r$. For each $1 \le i + t \le r + t$, let $\Delta_i = \Delta_i(A)$ be a* gcd *of the degree $(t + i)$ minors of A. Suppose*

$$A \sim \text{Diag}\{1, \underset{t}{\ldots}, 1, d_1, \ldots, d_r, 0, \ldots, 0\}$$

with $d_i|d_j$ for $i < j$ as in Theorem 2.3*. Then Δ_i divides Δ_{i+1} for each i, and*

$$d_1 \sim \Delta_1, d_2 \sim \Delta_2\Delta_1^{-1}, \ldots, d_r \sim \Delta_r\Delta_{r-1}^{-1}$$

Proof. Claim: $A \sim B$ implies $\Delta_i(A) \sim \Delta_i(B)$ $(i \le r)$ (associates in R).

If $Q \in M_m(R)$, then the $ki-$entry of QA is $\sum_j q_{kj}a_{ji} \implies R_k(QA) = q_{k1}R_1(A) + q_{k2}R_2(A) + \ldots + q_{kn}R_n(A)$, i.e., the rows of QA are $R-$linear combinations of the rows of A. The determinant functions is alternating and $R-$Multilinear on rows (or columns) $\implies$ degree-i minors of QA are $R-$Linear combinations of the degree-i minors of A. (Formal properties of determinants. Try degree-2 minors for $n = 3$.) Therefore $\Delta_i(A)$ divides each degree-i minor of QA, hence $\Delta_i(A)|\Delta_i(QA)$. Similarly if $P \in M_n(R)$, then $\Delta_i(A)|\Delta_i(AP)$.

If $A \sim B$, then there exists $Q \in GL_m(R)$ and $P \in GL_n(R)$ such that $B = QAP$, $Q^{-1}BP^{-1} = A$, hence $\Delta_i(A)|\Delta_i(B)|\Delta_i(A)$.

Therefore $\Delta_i(A) \sim \Delta_i(B)$✓. Now in particular $A \sim \text{Diag}\{1, \ldots, 1, d_1, \ldots, d_r, 0, \ldots, 0\}$ by Theorem 2.3, and we compute $\Delta_i \sim 1$ for $i : 1 - t \le i \le 0$ and $\Delta_i \sim d_1 \ldots d_i$ for $i : 1 \le i \le r$, by inspection. Successive solving for the d_i yields $d_1 \sim \Delta_1, d_2 \sim \Delta_2\Delta_1^{-1}, \ldots, d_r \sim \Delta_r\Delta_{r-1}^{-1}$. □

Remark 223. *This theorem gives an important shortcut for computing the d_i, which as we will see are crucial for classifying finitely generated modules over a PID.*

Corollary 224. *Suppose $A \in M_{m,n}(k)$. Then the elements d_i in Theorem 2.3, with d_i divides d_j for $i < j$ are uniquely determined up to units.*

Proof. If $A \sim \text{Diag}\{c_1, \ldots, c_{t+r}, 0, \ldots, 0\}$ then the result applies to the c_i hence they are associate to the $1's$ and the d_i, in order. □

HW 6: Modules

Definition 60

Suppose R is a PID and $A \in M_{m,n}(R)$ has rank $t + r$. The Smith normal form of A is the matrix:

$$SNF(A) := \text{Diag}\{1, \ldots, 1, d_1, d_2, \ldots, d_r, 0, \ldots 0\}$$

of Theorem 2.3, with $t \geq 0$ and nonzero d_i satisfying $d_i | d_j$ for $i < j$.

17 (Aluffi) VI.1: Free Modules Revisted

17.1 1.1 R-Mod.

Definition 61

A module over R is an Abelian group M, endowed with an action of R.
The action of $r \in R$ on $m \in M$ is denoted rm. [We'll only be considering Commutative Modules]

- $(r_1 + r_2)m = r_1 m + r_2 m$
- $1m = m$ and $(r_1 r_2)m = r_1(r_2 m)$
- $r(m_1 + m_2) = rm_1 + rm_2$

17.2 1.2: Linear Independence and Bases.

Definition 62

$F^R(S)$ denotes an $R-$Module containing a given set S and universal with respect to the existence of a set-map from S. We proved that the module $R^{\oplus S}$ with 'one component for each element of S' gives an explicit realization of $F^R(S)$.

HW 6: Modules

Definition 63

Indexed Sets, that is, for functions:

$$i : I \to M$$

for a non-empty indexing set I to a given module M, is a labelling of the elements of M, possibly not distinct.

Theorem 225. *For all sets I there's a canonical injection $j : I \to F^R(I)$ and any function $i : I \to M$ determins a unique $R-$Module Homomorphism $\varphi : F^R(I) \to M$ making the following commute:*

$$\begin{tikzcd} F^R(I) \arrow[r, "\varphi"] & M \\ I \arrow[u, "j"] \arrow[ur, "i"'] & \end{tikzcd}$$

This is precisely the universal property satisfied by $F^R(I)$.

Definition 64

We say that the indexed set $i : I \to M$ is linearly independent if φ is injective, i is linearly dependent otherwise. We say that i generates M if φ is a surjection.
Equivalently for an indexed set $S = \{m_\alpha\}_{\alpha \in I} \subset M$ is linearly independent if and only if:

$$\sum_{\alpha \in I} r_\alpha m_\alpha = 0$$

is only obtained if choosing $r_\alpha = 0$ for all $\alpha \in I$.
Otherwise S is linearly dependent.

Note 226. *For any arbitrary sum:*

$$\sum_{\alpha \in I} m_\alpha$$

we're assuming that $m_\alpha = 0$ for all but a finite number of α.

HW 6: Modules

Lemma 227. *Let M be an $R-$Module, and let $S \subset M$ be a linearly independent subset. Then there exists a maximal linearly independent subset of M containing S.*

Proof. Consider the family $\mathcal{P}$ of linearly independent subset of M containing S, ordered by inclusion. Since S is linearly independent, $\mathcal{P} \neq \emptyset$. By Zorn's Lemma, it suffices to verify that every chain in $\mathcal{P}$ has an upper bound. Indeed, the union of a chain of linearly independent subsets containing S is also linearly independent: because any relation of linear dependence only involves finitely many elements and these elements would all belong to one subset in the chain. □

Remark 228. *This statement is in fact known to be equivalent to the axiom of choice; therefore, the use of Zorn's lemma in one form or another cannot be bypassed.*

Note that a set can be maximal and linearly independent but not a generator. For example $\{2\} \subseteq \mathbb{Z}$.

Definition 65

An indexed set $B \to M$ is a basis if it generates M and is linearly independent.

Lemma 229. *An $R-$Module M is free if and only if it admits a basis. In fact, $B \subseteq M$ is a basis if and only if the natural homomorphism $R^{\oplus B} \to M$ is an isomorphism.*

Proof. This is immediate from Definition 1.1 of linear independence, if $B \subseteq M$ is linearly independent and generates M, then the corresponding homomorphism $R^{\oplus B} \to M$ is injective and surjective. Conversely, if $\varphi : R^{\oplus B} \to M$ is an isomorphism, then B is identified with a subset of M which generates it (because φ is surjective) and is linearly independent (because φ is injective). □

Note 230. *The choice of basis is equivalent to choosing an isomorphism for:*

$$R^{\oplus B} \simeq M$$

Once that's chosen we can write for any $m \in M$, there exists $r_b \in R$ such that:

$$m = \sum_{b \in B} r_b b$$

with all but a finite number of r_b being 0.

17.3 1.3: Vector Spaces

Lemma 231. *Let $R = k$ be a field, and let V be a $k-$Vector Space. Let B be a maximal linearly independent subset of V; then B is a basis of V.*

Proof. Let $v \in V$ and $v \notin B$. Then $B \cup \{v\}$ is not linearly independent, by the maximality of B; therefore, there exists $c_0, \ldots, c_t \in k$ and (distinct) $b_1, \ldots, b_t \in B$ such that:

$$c_0 v + c_1 b_1 + \ldots + c_t b_t = 0$$

with not all $c_0, \ldots, c_t$ equal to 0. Now, $c_0 \neq 0$: otherwise we would get a linear dependence relation among elements of B. Since k is a field, c_0 is a unit; but then

$$v = (-c_0^{-1} c_1) b_1 + \ldots + (-c_0^{-1} c_t) b_t,$$

proving that v is in the span of B. It follows that B generates V, as needed. □

Proposition 232. *Let $R = k$ be a field, and let V be a $k-$Vector Space. Let S be a linearly independent set of vectors of V. Then there exists a basis B of V containing S. In particular, V is a free $k-$Module.*

Proof. Follows Lemma 1.2: There's always a maximal linearly independent subset of M, Lemma 1.6: over fields Maximal linearly independent subsets are bases of V and Lemma 1.5. □

Lemma 233. *Let $R = k$ be a field, and let V be a k-Vector Space. Let B be a minimal generating set for V; then B is a basis of V.*

For general rings this last result fails.

17.4 Recovering B from $F^R(B)$.

Proposition 234. *Let R be an integral domain and Let M be a free $R-$Module. Let B be a maximal linearly independent subset of M, and let S be a linearly independent subset. Then $|S| \leq |B|$.*

Proof. By taking fields of fractions, the general case over an integral domain is easily reduced to the case of vector spaces over a field. We may then assume that $R = k$ is a field and $M = V$ is a $k-$Vector Space.

We have to then prove there exists an injective map $j : S \hookleftarrow B$, and this can be done by an inductive process, replacing elements of B by elements of S 'one-by-one'. For this, let $\leq$ be a well-ordering on S, let $v \in S$, and assume we have defined j for all $w \in S$ with $w < v$. Let B' be the set obtained from B by replacing all $j(w)$ for w, for $w < v$, and assume (inductively) that B' is still a maximal linearly independent subset of V. Then we claim that $j(v) \in B$ may be defined so that:

- $j(v) \neq j(w)$ for all $w < v$;
- the set B'' obtained from B' by replacing $j(v)$ by v is still a maximal linearly independent subset.

(Transfinite) Induction then shows that j is injective on S, as needed.

To verify our claim, since B' is a maximal linearly independent set, $B' \cup \{v\}$ is linearly dependent((as an indexed set), so that there exists a linear dependence:

$$c_0 v + c_1 b_1 + \ldots + c_t b_t = 0$$

with not all $c_i = 0$ and the b_i distinct in B'. Necessarily $c_0 \neq 0$ (because B' is linearly independent); also, necessarily not all the b_i with $c_i \neq 0$ are elements of S (because S is linearly independent). Without loss of generality we may then assume that $c_1 \neq 0$ and $b_1 \in B' \setminus S$. This guarantees that $b_1 \neq j(w)$ for all $w < v$; we set $j(v) = b_1$.

Al that is left now is the verification that the set B'' obtained by replacing b_1 by v in B' is a maximal linearly independent subset. But by using the linear dependence relation we have that:

$$v = -c_0^{-1} c_1 b_1 - \ldots - c_0^{-1} c_t b_t,$$

this is an easy consequence of the fact that B' is a maximal linearly independent subset. Further □

Name: Joseph McGuire Class: Math 561(Fall 2021)

Homework 7: Finitely Generated Modules over a PID

18 Class Notes

18.1 Class Notes: 11-08-2021

Note 235. *The proof of the Smith-Normal form good, make sure you know the multi-linear alternating properties of the* $\det : GL_n(R) \to R^\times$.

Different interpretations for Rings, and not a closed problem.

'Squidgy that thing'

Theorem 236. *Smith Normal Form:*

Over a PID R and $A \in M_{m\times n}(R)$.

Then

$$A \sim \{d_1, \mathrm{Diag}\ldots, d_r, 0, \ldots, 0\} = P^{-1}AQ,$$

with $d_i|d_j$ *such that* $i < j$, $P^{-1} \in GL_m(R)$ *and* $Q \in GL_n(R)$.

This Diagonal Form is the Smith Normal Form of A, or $SNF(A)$.

Example 237. *Let G be an Abelian Group. Then we'll describe it with 3 generators:* $a, b, c \in G$.

Let them obey:

$$3a + 9b + 9c = 0$$

$$9a - 3b + 9c = 0$$

Write G as a direct sum of cyclic groups.

$$\mathbb{Z}^3 \longrightarrow \mathbb{Z}^3 \longrightarrow G \longrightarrow 0$$

where

$$e_1 \mapsto a$$
$$e_2 \mapsto b$$
$$e_3 \mapsto c,$$

where $e = e_1, e_2, e_3$ *are a basis of the second copy of* $\mathbb{Z}^3$, *and* $\langle a, b, c\rangle = G$. *This is allowable since* $\mathbb{Z}^3$ *is a Free Module, and so this map is uniquely determined by this* *definition. On the first map, I'll define this via:*

$$\begin{aligned} f_1 &\mapsto 3e_1 + 9e_2 + 9e_3 \\ f_2 &\mapsto 9e_1 - 3e_2 + 9e_3 \\ f_3 &\mapsto 0, \end{aligned}$$

where $f = f_1, f_2, f_3$ are a basis over our first copy of $\mathbb{Z}^3$. So that this map is:

$$A = \begin{bmatrix} 3 & 9 & 0 \\ 9 & -3 & 0 \\ 9 & 9 & 0 \end{bmatrix}.$$

By Smith Normal form we have that the GCD of all the determinants 1×1 submodules is 3 and the 2×2 is 6 and 3×3 is 0.
So that:

$$A \sim \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix} = P^{-1}AQ,$$

for some $P, Q \in GL_3(\mathbb{Z})$.
So that:

$$Q = [id]^{f}_{f'}$$

and

$$P^{-1} = [id]^{e'}_{e}.$$

So that:

$$P^{-1}AQ = [\mathbb{Z}^3]_{f'} \xrightarrow{Q} [\mathbb{Z}^3]_f \xrightarrow{A} [\mathbb{Z}^3]_e \xrightarrow{P^{-1}} [\mathbb{Z}^3]_{e'}.$$

Behold

$$\mathbb{Z}^3 \xrightarrow{\begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}} \mathbb{Z}^3 \longrightarrow G \longrightarrow 0.$$

So that:

$$\frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}{3\mathbb{Z} \oplus 6\mathbb{Z} \oplus 0} \simeq \mathbb{Z}/3 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}.$$

Homework 7: Finitely Generated Modules over a PID

Theorem 238. *Main Theorem For a Principal Ideal Domain R, M is a finitely generated R-Module, on n generators. Have a surjection:*

$$\pi : R^n \longrightarrow M$$

Let $K = \ker(\pi)$ be free, rank $m \leq n$ (Uses the fact R is a PID, hence K is generated by a single element), by Theorem. Let

$$\overline{e} = \{e_1, \ldots, e_n\} \text{ basis for } R^n$$

$$\overline{y} = \{y_1, \ldots, y_m\} \text{ basis for } K$$

$$\overline{f} = \{f_1, \ldots, f_n\} \text{ basis for } R^n$$

Define $L : R^n \to R^n$ by :

$$f_i \mapsto \begin{cases} y_i & i \leq n \\ 0 & i > n \end{cases},$$

then $L(R^n) = K$. Let $A = [L]^{\overline{e}}_{\overline{f}} \in M_n(R)$.

Define A^t = Presentation Matrix forM (a presentation matrix, not the only one).

Remark 239. *If $P = [id]^{\overline{e}}_{\overline{e'}}, Q = [id]^{\overline{f}}_{\overline{f'}}$, then $[L]^{\overline{e'}}_{\overline{f'}} = P^{-1}AQ$.*

New presentation matrix:

$$(P^{-1}AQ)^t = Q^t A^t P^{-t}$$

Theorem 240. *Let R be a PID, M is a finitely generated R-Module, Then $M \simeq \coprod_{i=1}^{r} R/(d_i) \oplus R^f$ for nonzero non-units d_i satisfying $d_i | d_j$ for $i < j$ and non-negative integer f. (All uniquely determined by M)*

Solution. Sketch:

$$R^n \overset{A \sim P^{-1}AQ}{\longrightarrow} R^n \overset{\pi}{\longrightarrow} M \longrightarrow 0.$$

□

18.2 Class Notes: 11-09-2021

Homework 7: Finitely Generated Modules over a PID

Example 241. *Given an Abelian group $\mathbb{Z}e_1 \oplus \mathbb{Z}_2e_2/\mathbb{Z}(4e_1 + 6e_2)$, write it as a direct sum of cyclic groups.*

Geometrically, $\mathbb{Z}(4e_1 + 6e_2)$ would be the line that passes through the origin $(0, 0)$ and $(4, 6)$ on the lattice, $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, with $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2/\mathbb{Z}(4e_1 + 6e_2)$ is then the set of all parallel lines to this original line.

Note the element $2e_1 + 3e_2 + \mathbb{Z}(4e_1 + 6e_2)$ has order 2 in this quotient group, so we can show that this is:

$$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}.$$

Theorem 242. *Fundamental Theorem Let R be a PID and M be a finitely generated $R-$Module.*

Then $M \simeq \coprod_{i=1}^{r} R/(d_i) \oplus R^f$, with $d_i|d_j$ for $i < j$ and $f \geq 0$. The d_i's are uniquely determined up to multiplication by units, and f is uniquely determined.

Proof. Recall the set up:

$$R^n \longrightarrow R^n \xrightarrow{\pi} M \longrightarrow 0$$

with $L(R^n) = \ker(\pi)$.

Remark: $\overline{e}, \overline{f}$ bases for middle and left R^n's, then (think $A =$) $[L]^{\overline{e}}_{\overline{f}} \in M_n(R)$ is transpose of presentation matrix: In general A is not diagonal.

Goal: Diagonalize A by replacing $\overline{e}, \overline{f}$ by New Bases.

The presentation matrix is A^T.

By the Smith Normal Form Theorem:

$$\exists P, Q \in GL_n(R).$$

Such that:

$$P^{-1}AQ = \text{Diag}\{1, \ldots, 1, d_1, \ldots, d_r, 0, \ldots 0\}.$$

With d_i's are nonzero nonunits, the number of 1's is t and the number of 0's is f, where $d_i|d_j$ for $i < j$ uniquely determined up to units.

Define $\overline{e} \cdot \overline{f'}$ by $[id]^{\overline{e}}_{\overline{e'}} = P$ and $[id]^{\overline{f}}_{\overline{f'}} = Q$.

Now

$$[R^n]_{\overline{f'}} \overset{SNF(A)}{\longrightarrow} [R^n]_{\overline{e'}} \longrightarrow [M]_{x'} \longrightarrow 0,$$

That is surjective hence, by the embedding along the diagonal argument we have that:

$$M \simeq \coprod_{i=1}^{t} \frac{Re'_i}{1e'_i} \oplus \coprod_{i=1}^{r} \frac{Re'_{i+t}}{(d_i)e'_{i+t}} \oplus \coprod_{i=1}^{f} Re'_{i+t+r}$$

Simplified:

$$M \simeq \coprod_{i=1}^{r} R/(d_i) \oplus R^f.$$

$M_{tor} = \coprod_{i=1}^{r} R/(d_i)$, everything in this is 'killed' by a scalar, in this case d_i is the ring element. □

Lemma 243. *For the exact sequence to lead to the result above we need:*

$$\frac{Re_1 \oplus Re_2}{(d_1)e_1 \oplus (d_2)e_2} \simeq \frac{R}{(d_1)} \oplus \frac{R}{(d_2)}$$

So that we need a surjective map:

$$Re_1 \oplus Re_2 \to \frac{Re_1}{(d_1)e_1} \oplus \frac{Re_2}{(d_2)e_2}$$

and

$$e_1 \longmapsto e_1 + (d_1)e_1$$
$$e_2 \longmapsto e_2 + (d2)e_2$$

and hence the kernel of this map is:

$$\ker : \{re_1 + se_2 : d_1|r, d_2|s\} = (d_1)e_1 + (d_2)e_2.$$

That is, take $re_1 \longmapsto (d_1)e_1 = re_1 + (d_1)e_1$ *hence* $re_1 \in (d_1)e_1$ *and similarly if* $re_2 \mapsto 0$ *then* $re_2 \in (d_2)e_2$.

Remark 244. *Generators for the diagonalized* M.
Say $SNF(A) = P^{-1}AQ$ *and* $\overline{e'} = \overline{e}P$. *If* $\overline{x}$ *are the original generators of* M, *so that* $\pi(e_i) = x_i$, *then* $\overline{x'} = \overline{x}P$ *are the 'diagonalized' generators.*

18.3 Class Notes 11-12-2021

Theorem 245. *R is a PID and M is a finitely generated $R-$Module. Then*

$$M \simeq \coprod_{i=1}^{r} R/(d_i) \oplus R^f.$$

For possibly empty set of nonzero no units $d_i : d_i | d_j$ for $i < j$, that is d_i is unique upto units, f is a nonnegative integer.

Example 246. *$R = \mathbb{Z}$ is finitely generated, abelian group:*

$$G \simeq \coprod_{i=1}^{r} \mathbb{Z}/(d_i) \oplus \mathbb{Z}^f$$

Example 247. *$R = k[x]$ where k is a field, V is a $n-$dimensional $k-$Vector Space. So note that R is a PID and suppose we have $T \in \mathrm{end}_k(V)$.*
Make V into a $k-$Module 'V_T', where $V = V_T$ as $k-$Vector Space.

Theorem 248. *$k[x] \times V_T \to V_T$*
$(f(x), v) \longmapsto f(T)(v)$
Then we'll define:

$$T^i(v) = (T \circ \dots_{itimes} \circ T)(v).$$

So that

$$(aT^i + bT^j)(v) = aT^i(v) + bT^j(v).$$

By the structure theorem:

$$V_T \simeq \coprod_{i=1}^{r} \frac{k[x]}{(d_i(x))} \oplus k[x]^f$$

but that we have $\dim_k(V) < \infty$ so that $f = 0$ and we can make each $d_i(x)$ a monic polynomial.

Homework 7: Finitely Generated Modules over a PID

18.4 Class Notes 11-15-2021

Note 249.
- *Homework 8 is due Monday 9AM of Thanksgiving Break*
- *Possibly another homework due the following Friday/Saturday*

R is a PID and M is finitely generated $R-$Module, then we have $M \simeq M_{tor} \oplus R^f$.

Note 250. *Know how to show this on the final!*

In particular, M_{tor} is a submodule always for any M.
And that M/M_{tor} is torsion free (i.e contains no torsion elements).
To show this the trick is to construct an exact sequence:

$$0 \longrightarrow M_{tor} \longrightarrow M \longrightarrow M/M_{tor} \longrightarrow 0$$

and show that there exists a $R-$Linear Transformation $M/M_{tor} \longrightarrow M$ such that the sequence splits.

Note 251. *This will likely be on final!*

Example 252. *Consider the following: Let M be a finitely generated Module over some PID R, with n generators (not the same thing as having rank n), so that we have a surjective map:*
Assume without loss of generality that $\dim_k(M) = n$.

$$R^n \longrightarrow M \longrightarrow 0.$$

Now let $R = k[x]$ where k is some field.
Then x is a linear transformation $T : V \to V$ and M is finite dimensional in k.
Let $\underline{v} = \{v_1, \ldots, v_n\}$ be a $k-$Basis for M, then:

$$(k[x])^n_{\underline{e}} \longrightarrow M_{\underline{v}}. \longrightarrow 0$$

Homework 7: Finitely Generated Modules over a PID

Remark 253. *Then any eH with $m \in M$ is a $k-$linear combination of v_i.*

Therefore, m is a $k[x]-$Linear Combination of the v_i's but v_i are $k[x]-$Linearly Dependent. Since $p_T(x)v_i = 0$ for any i.

That is M cannot contain any basis in $k[x]$.

Example 254.

$$[T]_{\underline{v}} = \begin{bmatrix} 2 & 1 \\ -1 & 3 \end{bmatrix}$$

and let $M = k^2$ with basis $\underline{v} = \{v_1, v_2\} = \{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$.

So that $k[x]$-Module via $[1]_{\underline{e}}$.
So that:

- $$x \cdot v_1 = T \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ -1 \end{bmatrix} = 2v_1 - v_2.$$
- $$x \cdot v_2 = T \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}.$$
- $$x^2 v_1 = T^2 v_1 = \begin{bmatrix} 3 \\ -5 \end{bmatrix}$$
- $$(x^2 + x + 1)v_1 = \begin{bmatrix} 6 \\ -6 \end{bmatrix}$$

Finally we can compute the characteristic polynomial of T by noting that:

$$p_T(x) = \det \begin{vmatrix} 2 - x & 1 \\ -1 & 3 - x \end{vmatrix} = x^2 - 5x + 7.$$

Additionally, note that $p_T(T) = 0$.

If we wanted to calculate its structure:

$$M \simeq \coprod_{i=1}^{r} \frac{k[x]}{(d_i(x))},$$

then note that $\Delta_1 = d_1(x) = \gcd(x-2, -1, x-3, 1) = 1$ *and then* $d_2(x) = \Delta_2\Delta_1^{-1} = \Delta_2 = \gcd(x^2-5x+7) = x^2-5x+7$. *So that:*

$$M \simeq \frac{k[x]}{(1)} \oplus \frac{k[x]}{(x^2-5x+7)} \simeq \frac{k[x]}{(x^2-5x+7)}.$$

18.5 Class Notes 11-18-2021

HW 8.5: We have $V = \dfrac{k[x]}{(d(x))}$ where with is a finite dimensional k-v.s. where x acts like $T \in End_k(V)$. So that $\dim_k(V) = \deg(V)$ and furthermore we have a basis:

$$\{1, x, \dots, x^{n-1}\}.$$

We defne an eignevector v in this space such that:

$$v \in V \qquad \text{an element } f(\overline{x}) = v$$

such that $x \cdot f(\overline{x}) = \lambda f(\overline{x})$, where $\lambda \in k$, and λ is an eigenvalue of v. Where $f(\overline{x}) = f(x) + (d(x))$.

Note 255. *Canonical Forms Let k be a field, V a n-dimension $k-$v.s. and $T \in End_k(V)$. Then*

$$V_T \simeq \coprod_{i=1}^{r} \frac{k[x]}{(d_i(x))}.$$

The idea of what we want to do is use the above relationship to derive new bases for V, in particular a standard form for general matrices. So we want a decomposition above that suggest k-bases with respect to T has a 'canonical' form.

Many different kinds:

- Rational Canonical Form
- Jordan Canonical Form
- Many more...

Homework 7: Finitely Generated Modules over a PID

Note 256. *Diagonal Matrix:*

$$\mathrm{Diag}\{a_1, a_2, \ldots, a_n\}.$$

with

$$\begin{bmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & a_{n-1} & & \\ 0 & & & & a_n \end{bmatrix}$$

Easy to interpret and is a kind of canonical form.

Some stuff we know, similar matrices represent the same linear transformation possibly in different bases.

- Q: When can T be represented as a diagonal matrix?
- Q: When is $A \in M_n(k)$ similar to diagonal matrix?

Definition 66

Let V be a n-dimensional k-Vector Space, and k be a field.

1. $T \in \mathrm{End}_k(V)$ is diagonalizable if it can be represented by a diagonal matrix.
2. $A \in M_n(k)$ is diagonalizable if it is similar to a diagonal matrix

Remark 257. *Fix $\underline{e} \subset V$ as a basis, then we have $1-1$ correspondence:*

$$\mathrm{End}_k(V) \iff M_n(k)$$

$$T \longmapsto [T]_{\underline{e}}$$

So that $T(v+v') = T(v) + T(v')$ and $T(cv) = cT(v)$.

That is $\mathrm{End}_k(V)$ is just some linear transformation, possible described in words, e.g. a linear projection on a plane in $\mathbb{R}^3$.

While $M_n(k)$ explicitly describes how this linear transformation acts on basis elements of V, and gives us an exact description of that transformation.

Theorem 258. *k is a field, V is a n-dimensional k-Vector Space, $T \in \mathrm{End}_k(V)$. Then T is diagonalizable $\iff$ $m_T(x)$ splits into distinct linear factors.*

Remark 259. *$k[x]/(x-1)^2$ is non-diagonalizable but a linear transformation on V.*

Proof. Suppose T is diagonalizable, then we have a basis $\underline{e} \subset V$ k-basis, with respect to which $[T]_{\underline{e}} = \mathrm{Diag}\{a_1, \ldots, a_n\}$, by definition.
Then the presentation matrix for $k[x]$-Module V is:

$$Ix - T = \mathrm{Diag}\{x-a_1, x-a_2, \ldots, x-a_n\}.$$

So that:

$$V \simeq \coprod \frac{k[x]}{(x-a_i)} = k \cdot e_i.$$

Let $\{a_{ij}\}$ be the set of distinct a_i. Then $\coprod(x-a_j)$ kills V, and smaller polynomial will do the job. Hence $= m_T(x)$ ✓
Conversely, suppose that $m_T(x)$ splits into distinct linear factors, then so does each $d_i(x)$ since they all divide $m_T(x) = d_r(x)$.
Therefore:

$$V \simeq \coprod \frac{k[x]}{(d_i(x))} \simeq \coprod_{i=1}^{r} \coprod_{j=1}^{n_i} \frac{k[x]}{(x-a_{ij})},$$

some subset of all distinct $x - a_{ij}$. So that T is now diagonal.
Rewrite:

$$V \simeq \coprod_{i=1}^{n} \frac{k[x]}{(x-a_i)} 1_i$$

with some a_i's repeated. Then let $\underline{e} = \{1_i\}$ for this coproduct so that $[T]_{\underline{e}} = \mathrm{Diag}\{a_1, \ldots, a_n\}$. □

18.6 Class Notes 11-19-2021

Last time:

V is a finite-dimensional $k-$Vector Space with k as as field and $T \in \mathrm{End}_k(V)$. This gives us a similarity class in $M_n(k)$, the trick is to find a representative element from this group that is nice or canonical.

Homework 7: Finitely Generated Modules over a PID

With $m_T(x) =$ Smallest Polynomial such that $m_T(T) = 0$, we can find this using $p_T(x)$, since we must have $m_T(x)$ divides $p_T(x) = \det(xI - A)$ with A being any matrix representing T. With $p_T(x)$ being small we can just compute $m_T(x)$ by hand usually.

Theorem 260. *T is diagonalizable if and only if $m_T(x)$ splits into distinct linear factors over the field k.*

Example 261. *Consider $A, B \in M_3(k)$ with $k = \mathbb{R}$.*

$$A = \begin{bmatrix} 5 & 6 & 0 \\ -3 & -4 & 0 \\ -2 & 0 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 3 & -1 & 2 \\ -10 & 6 & -14 \\ -6 & 3 & -7 \end{bmatrix},$$

are these similar?

Solution. One quick trick is to check the trace, they should be equal.

Decide if they're similar find the characteristic polynomials:

$$p_A(x) = x^3 - 2x^2 - x + 2$$

We can check that $x - 1$ is a factor of this:

$$p_A(x) = (x-1)(x^2 - x - 2) = (x-1)(x+1)(x-2)$$

and similarly:

$$p_B(x) = x^3 - 2x^2 - x + 2$$

doesn't immediately imply similarity! Need to find the minimal polynomial:

$$p_A(x) = p_B(x) = (x-1)(x+1)(x-2).$$

Since $d_1(x)|d_2(x)|m_A(x)$ we must have in both:

$$m_A(x) = m_B(x) = (x-1)(x+1)(x-2)$$

So because they have the same minimal polynomial and characteristic polynomial they are similar to $\text{Diag}\{1, 2, -1\}$ and hence each other. □

18.6.1 Rational Canonical Form

Name: Joseph McGuire Class: Math 561(Fall 2021)

Homework 7: Finitely Generated Modules over a PID

Example 262. *$V = k[x]/(d(x))$, where $d(x)$ is monic and degree n. e.g. $d(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$.*
Q: $k-$basis?

$$\{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\} = \overline{e},$$

is a kronecker basis.

Multiplication by x gives us a natural linear transformation of this:

$$[X]_{\overline{e}} = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

This is the companion matrix of $d(x)$: $C(d(x))$. Where we obtain this from the kronecker basis and note that:

$$x \cdots \overline{x}^{n-1} = -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1}.$$

Theorem 263. *k is a field, V is a finite dimensional k Vector Space and $T \in \mathrm{End}_k(V)$, let $d_i(x)$ with $1 \leq i \leq r$ be the invariant factors of V_T.*
Then there exists a basis $\overline{e}$ with respect to which:

$$[T]_{\overline{e}} = \coprod_{i=1}^{r} C(d_i(x)) = \begin{bmatrix} C(d_1(x)) & 0 & \ldots & 0 \\ 0 & C(d_2(x)) & \ldots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \ldots & C(d_r(x)) \end{bmatrix}$$

Proof. Make $k[x]$-Module V_T such that:

$$V_T \simeq \coprod_{i=1}^{r} \frac{k[x]}{d_i(x)}$$

where V_i is stable under T so that: (e_i = Kronecker Basis)

$$[T|_{v_i}]_{\overline{e_i}} = C(d_i(x))$$

implies

$$[T]_{\overline{e}} = \coprod_{i=1}^{r} C(d_i(x)).$$

□

18.7 Class Notes 11-29-2021

Anytime you invoke a coproduct map, it's automagically a R-homomorphism and hence a R-Linear map.

Last Time: Diagonalizability and RCF, over any field, we have a rational canonical form. This fully classifies a linear transformation by using the coproduct correspondence theorem and invariants factors. Finally, Jordan Canonical Form. A generalization of a diagonal matrix.

First, for some setup we need background: Chinese Remainder Theorem.

Suppose we have ring R with unity 1. Say Ideal I, J are coprime if $I + J = R$. I.e, there are $a \in I$ and $b \in J$ such that $a + b = 1$, think gcd as linear combination theorem.

Theorem 264. *Suppose $I_1, I_2, \ldots, I_r$ are pairwise coprime. Let $I = \prod_{\theta=1}^{r} = I_\theta$ in R. Equivalently $I = \bigcap_{j=1}^{r} I_j$. Then*

$$R/I \longrightarrow \prod_{j=1}^{r} R/I_j \text{ isomorphism and there's an algorithm for computing the inverse.}$$

Example 265.

$$\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_{45} \simeq \mathbb{Z}_9 \times \mathbb{Z}_5 \qquad 3^2 \text{ and } 5 \text{ coprime}$$

$$R = k[x], f, g \in k[x] \qquad \text{with no common factors} \qquad \text{then: } \frac{k[x]}{fg} \simeq k[x]/f \times k[x]/g.$$

Example 266. *Suppose*

$$V = \frac{k[x]}{(x-\lambda)^n},$$

Q: What is the linear transformation here?

T = Multiplication by x, making it a $V[x]-$Module.

Q: What are the invariant factors?

Just $(x-\lambda)^n = m_x(x) = p_x(x)$.

Q: Is it a k-Vector Space?

Yes, by Kronecker's Theorem

Q: What's the k-basis?

$\{1, \overline{x}, \overline{x}^2, \dots, \overline{x}^{n-1}\}$, *where* $\overline{x} = x + (x-\lambda)^n$.

Another k-basis, is $\{1, \overline{x}-\lambda, (\overline{x}-\lambda)^2, \dots, (\overline{x}-\lambda)^{n-1}\}$, *write these as:* $e_i = (\overline{x}-\lambda)^{n-i}$.

Q: What is $[x]_{\overline{e}}$*?*

$x \cdot e_1 = x \cdot (\overline{x}-\lambda)^{n-1} = \lambda(\overline{x}-\lambda)^{n-1}$ *so that* $x \cdot e_1 = \lambda e_1$.

$(x-\lambda)(\overline{x}-\lambda)^{n-1} = 0$.

$$x \cdot e_2 = x \cdot (\overline{x}-\lambda)^{n-2} = e_1 + \lambda e_2$$

since $(x-\lambda)(\overline{x}-\lambda)^{n-2} = (\overline{x}-\lambda)^{n-1} = e_1$.

That matrix is exactly a Jordan Block

Theorem 267. *k field, V is an n−dimensional k-Vector Space and* $T \in End_k(V)$. *Suppose* $m_T(x)$ *splits into linear factors in* $k[x]$. *Then there exists* $k-$*basis* v *with respect to which:*

$$[T]_{\overline{v}} = \prod_{d=1}^{t_r} \prod_{i=s_j}^{r} J_{e_{ij}}(\lambda_j)$$

with: $\{\lambda_j : 1 \le j \le t_r\}$ *the eigenvalues of* T. *(All Distinct)*

$s_j = \inf\{i : (x-\lambda_j)\Big| d_i\}$. $e_{ij} \ge 0$ *and* $e_{ij} \le e_{i'j}$ *if* $i < i'$