Advanced Linear Algebra

Def. Let R be a communicative ring with identity, whose elements are called scalars. An *R-module* is a non-empty set M where

1. $(M, +)$ is an abelian group
2. For all $r, s \in R$, and $u, v \in M$:

$r(u+v) = ru + rv$; $(s+r)v = sv + rv$; $(rs)u = r(su)$; $1u = u$

The ring R is called the base ring of M

Def. A submodule of an R-module M is a non-empty subset of M where S is also an R-module, denoted $S \leq M$

Thm. A non-empty subset S of R-module M is a submodule if and only if it is closed under taking linear combinations.

Def. The submodule spanned by a subset S of a module M is the set of all linear combinations of elements in S:

$\langle\langle S \rangle\rangle = \{r_1 v_1 + \cdots + r_n v_n \mid r_i \in R, v_i \in S, n \geq 1\}$

S is said to span M if $M = \langle\langle S \rangle\rangle$

Def. An R-module M is said to be finitely generated if it contains a finite set that generates M. M is *n-generated* if $|S| = n$

Def. A subset S of an R-module M is linearly in

$v_1, \cdots, v_n \in S$, $r_1, \cdots, r_n \in R$, $r_1 v_1 + \cdots + r_n v_n = 0 \Rightarrow r_1, \cdots r_n = 0$

Def. Let V be a vector space, $S \subseteq V$ be a subset

(i) A linear combination of S is
$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$ $(a_i \in \mathbb{F},\ v_i \in S)$ which is a finite sum.

(ii) The span of S is
$\operatorname{span}(S) = \{a_1 v_1 + \cdots + a_k v_k \mid a_i \in \mathbb{F},\ v_i \in S\}$

(iii) We say S spans V is $\operatorname{span}(S) = V$

Def. We say a subset $S \subseteq V$ is said to be linearly independent if for any finite subsets
$\{s_1, s_2, \cdots, s_t\} \subseteq S$, $a_1 s_1 + \cdots + a_t s_t = 0 \Rightarrow a_1 = \cdots = a_t = 0$

Example. $S = \{1, x, x^2, \cdots, x^n, \cdots\}$ is a linearly independent set of $C^\infty(\mathbb{R})$
Take a finite subset $\{x^{\alpha_1}, x^{\alpha_2}, \cdots, x^{\alpha_k}\} \subseteq S$, suppose $\alpha_1 < \alpha_2 < \cdots < \alpha_k$
$c_1 x^{\alpha_1} + \cdots + c_k x^{\alpha_k} = 0$
Differentiate for α_1 times, then $c_1 \cdot (\alpha_1!) = 0$, $c_1 = 0$
...
so $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$

(iv) S is a basis of V if $\operatorname{span}(S) = V$ and S is linearly independent.

Thm. Every vector field has a basis.
Check the proof from <<Abstract Algebra>>

Lec 3.

Thm. $\mathcal{B}$ is a basis of $V \iff$ All $v \in V$ can be uniquely expressed can be uniquely expressed in terms of linear combination of $\mathcal{B}$

proof: Suppose $\exists\, v \in V \setminus \{0\}$. v can't be uniquely expressed by a linear combination of $\mathcal{B}$, then $\exists \{v_1, v_2, \cdots, v_n\} \subseteq \mathcal{B}$ & $\{v_1', v_2', \cdots, v_m'\} \subseteq \mathcal{B}$
s.t. $v = a_1 v_1 + \cdots + a_n v_n = a_1' v_1' + \cdots + a_n' v_m'$, w.l.o.g $a_1 \neq 0$
then $v_1 = -\frac{a_2}{a_1} v_2 - \cdots - \frac{a_n}{a_1} v_n + \frac{a_1'}{a_1} v_1' + \cdots + \frac{a_m'}{a_1} v_m'$, this implies that
$\{v_1, \cdots, v_n, v_1', \cdots, v_m'\}$ is linearly dependent
However, $\{v_1, \cdots, v_n, v_1', \cdots, v_m'\} \subseteq \mathcal{B}$, this contradicts

($\Leftarrow$) Clearly we see that $\text{span}(\mathcal{B}) = V$
Suppose $\mathcal{B}$ is not a basis, then $\exists$ a finite subset of $\mathcal{B}$
$\{v_1, v_2, \cdots, v_n\} \subseteq \mathcal{B}$. s.t. $c_1 v_1 + \cdots + c_n v_n = 0$, where $\exists\, i$ s.t. $c_i \neq 0$
w.l.o.g. suppose $c_1 \neq 0$, we see $v_1 = -\frac{c_2}{c_1} v_2 - \cdots - \frac{c_n}{c_1} v_n$
let $x = v_1$, so we has two ways to express x in terms of linear combination of $\mathcal{B}$, which contradicts ⚡

Thm.
(1) If $\mathcal{L} \subseteq V$ is linearly independent, then we can extend $\mathcal{L}$ into $\mathcal{L} \amalg \mathcal{L}' = \mathcal{B}$ is a basis for V

(2) If $\mathcal{O} \subseteq V$ is a spanning set, then there is a spanning set $\mathcal{B} \subseteq \mathcal{O}$ s.t. $\mathcal{B}$ is a basis for V

(3) All bases for V have the same cardinality

Def. The dimension of V is the cardinality of its bases.

E.g. $\dim_{\mathbb{F}}(\mathbb{F}^n) = n$

$\dim_{\mathbb{F}}(V_3) = \infty\ (= \aleph_0)$
$\dim_{\mathbb{F}}(V_1) = \infty\ (= \aleph_1)$

Def. Let V be a vector space, $W_i \leq V$, $i \in I$
The internal sum of W_i is defined as
$\sum_{i\in I} W_i := \{w_{i_1} + \cdots + w_{i_k} : w_{ij} \in W_i, j \in \mathbb{N}\}$
Note that this is a finite sum

Clearly we see that $\sum_{i\in I} W_i \leq V$

Def. Let V and $W_i \leq V$ as defined before, then
we say $\sum_{i\in I} W_i := \bigoplus_{i\in I} W_i$ is an internal direct sum if for any finite collection of subspaces $W_{i_1}, \cdots, W_{i_n} \leq V$.
$w_{i_1} + \cdots + w_{i_n} = 0_V \Leftrightarrow w_{i_1} = \cdots = w_{i_n} = 0_V$ (where $w_{ij} \in W_{ij}$)

Thm. Let $W_i \subseteq V$ be subspaces such that $\bigoplus_{i\in I} W_i$ is direct.
Suppose $B_i \subseteq W_i$ is a basis of W_i, then
$\coprod_{i\in I} B_i$ is a basis of $\bigoplus_{i\in I} W_i$

Consequencely, $\dim(\bigoplus_{i\in I} W_i) = \sum_{i\in I} \dim(W_i)$

Proof: Let $v \in V$ be given
Step 1. v can be uniquely expressed by $v = w_{i_1} + \cdots + w_{i_k}$ for $w_{ij} \in W_j$
Suppose $w_{i_1} + \cdots + w_{i_k} = w_{i_1}' + \cdots + w_{i_k}'$, so $(w_{i_1} - w_{i_1}') + \cdots + (w_{i_k} - w_{i_k}') = 0_V$
Since $W_{i_1}, \cdots, W_{i_k}$ are disjoint spaces, then $w_{ij} = w_{ij}'$

Step 2. Every $w_{ij} \in W_{ij}$ is uniquely expressed by linear combination of B_i
Therefor $v \in \bigoplus_{i\in I} W_i$ is uniquely expressed by $B_{i_1} \amalg \cdots \amalg B_{i_k} \subseteq \coprod_{i\in I} B_i$

Lec 4.

Let $\{V_i : i \in I\}$ be vector spaces over $\mathbb{F}$

Def. The external direct sum V_i is

$$\bigoplus_{i\in I} V_i := \left\{ f : I \to \bigcup_{i\in I} V_i \;\middle|\; f(i) \in V_i,\ f(i) \neq 0_{V_i} \text{ for finitely many } i\text{'s} \right\}$$

Remark. Any element $f \in \bigoplus_{i\in I} V_i$ is determined by $f(i)$ for all $i \in I$

For example, if $I = \mathbb{N}$, then f is determined by

$f \leftrightarrow (f(1), f(2), \cdots)$

$f(1) \in V_1$, $f(2) \in V_2$

Example. An element $f \in \bigoplus_{i\in\mathbb{N}} \mathbb{R}$ $(V_i = \mathbb{R})$ is given by $(f(1), f(2), \cdots)$ where $f(i) \neq 0$ for finite $i \in \mathbb{N}$

An element $f \in \bigoplus_{i\in\mathbb{R}} \mathbb{R}$ is given by $(\cdots, f(x), \cdots)$

Therefore $\bigoplus_{i\in\mathbb{R}} \mathbb{R} = \{ f : \mathbb{R} \to \mathbb{R} \mid f(x) \neq 0 \text{ for finitely many } x\text{'s} \}$

Addition & Scalar Multiplication in $\bigoplus_{i\in I} V_i$ for $f, g \in \bigoplus_{i\in I} V_i$

$(f+g)(i) := f(i) + g(i)$

$(\alpha f)(i) := \alpha f(i)$

Thm. Let $B_i = \{ b_i^j \mid j \in J_i \}$ be a basis of V_i, then the basis of $\bigoplus_{i\in I} V_i$ is given by $\bigcup_{i\in I} J_i$, where $J_i := \{ f_i^j : I \to \bigcup_{i\in I} V_i \mid f_i^j(i) = b_i^j \ \&\ f_i^j(x) = 0 \text{ if } x \neq i \}$

Consequencely (since $|J_i| = |B_i|$)

proof: **Check 1**: Every $v \in \bigoplus_{i\in I} V_i$ is uniquely expressed by linear combination of $\bigcup_{i\in I} J_i$

Let $f \in \bigoplus_{i\in I} V_i$, by hypothesis, only $f(i_1) = v_{i_1}, f(i_2) = v_{i_2}, \cdots, f(i_k) = v_{i_k} \neq 0$

so $f \leftrightarrow (\cdots, v_{i_1}, \cdots, v_{i_2}, \cdots, \cdots, v_{i_k}, \cdots)$

For each $v_{i_l} \in V_{i_l} = \mathrm{span}(B_{i_l})$, $v_{i_l} = \alpha_{i_l}^1 b_{i_l}^{a_1} + \cdots + \alpha_{i_l}^k b_{i_l}^{a_k}$ $(\alpha_{i_l}^{\cdot} \in \mathbb{F})$

Therefore,

$$f = (\alpha_{i_1}^1 f_{i_1}^{a_1} + \cdots + \alpha_{i_1}^{k_1} f_{i_1}^{a_k}) + \cdots + (\alpha_{i_k}^{n_1} f_{i_k}^{a_n} + \cdots + \alpha_{i_k}^{n_k} f_{i_k})$$

Def. The external direct product of V_i is given by
$\prod_{i\in I} V_i := \{f: I \to \bigcup_{i\in I} V_i \mid f(i)\in V_i, \forall i\in I\}$

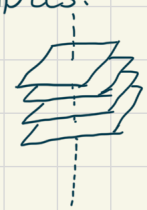
with addition and scalar multiplication defined identically as the external direct sum.

Example. $\prod_{i\in\mathbb{N}} \mathbb{R} \hookrightarrow \{(a_1^{\in\mathbb{R}}, a_2^{\in\mathbb{R}}, \cdots)\} = V_1$
and $\prod_{i\in\mathbb{R}} \mathbb{R} = \{f: \mathbb{R}\to\mathbb{R}\}$

Quotient Space

Goal: Let $W\leq V$. Devide V into "slices" of W

Examples. $V=\mathbb{R}^3$, $W=$ 

$V=$ 

Def. Let $W\leq V$ be v. subspace. We say two vectors, $x, y\in V$ are equivalent if $x-y\in W$, denoted $x\sim y$

Def. The (left) coset (陪集) of W (with representative $v\in V$) is defined as $v+W=\{v' \mid v'\sim v\} = \{v+w \mid w\in W\}$

Prop. (1) for $v, u\in V$, $(v+W=u+W) \Leftrightarrow v-u\in W$
(2) If $v+W\neq u+W$, then $(v+W)\cap(u+W)=\emptyset$

(1): If $v-u=w\in W$, then $v+W=u+w+W=u+W$

(2): Just check the properties of equivalent relationship.

Lec 5

Def. Let $W \leq V$ be given. The quotient space V/W is given by
$V/W = \{v+W \mid v \in V\}$, with $+, \cdot$ given by
$(v+W)+(u+W) := (v+u)+W$
$\alpha(v+W) := \alpha v + W$

Examples.
$V = \mathbb{F}_3[x]$, $W := \{p(x) \in V : (x^3+2x^2+1) \mid p(x)\}$

Check. $W \leq V$
$(x^3+2x^2+1)q(x) + (x^3+2x^2+1)r(x) = (x^3+2x^2+1)(q(x)+r(x))$
$V/W := \{p(x)+W \mid p(x) \in V\}$
we see that W is a subspace of V. then $\forall p(x) \in V$
$p(x) = q(x)(x^3+2x^2+1) + r(x)$, where $\deg r < 3$
so $p(x) = q(x)(x^3+2x^2+1) + (\alpha x^2 + \beta x + \gamma)$
$V/W = \{q(x)(x^3+2x^2+1) + (\alpha x^2+\beta x+\gamma) + W \mid q(x) \in \mathbb{F}_3[x]\} = \{\alpha x^2+\beta x+\gamma+W \mid \alpha, \beta, \gamma \in \mathbb{F}_3\}$
see that $|V/W| = 3^3 = 27$

Remark. In V/W, we have different expressions,
$v+W = v'+W$ for the same "vector"
So we need to check that
(1) If $\begin{cases} v+W = v'+W \\ u+W = u'+W \end{cases}$, then $(v+W)+(u+W) = (v'+W)+(u'+W)$
(2) $\alpha(v+W) = \alpha(v'+W)$ is well defined.

(1) $(v+W)+(u+W) = (v+u)+W = (v'+w_1+u'+w_2)+W = (v'+u')+W = (v'+W)+(u'+W)$
(2) $\alpha(v+W) = \alpha(v'+w_1+W) = \alpha v' + \alpha(w_1+W) = \alpha(v'+W)$

Linear Transformations

Def. $T: V \to W$ is a linear transformation if V, W are vector spaces and $T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$
$\forall \alpha, \beta \in \mathbb{F}$, $v_1, v_2 \in V$

Def. $\mathcal{L}(V,W) = \{T: V \to W \mid T \text{ is linear}\}$ is the collection of all linear transformations from V to W

We see that $\mathcal{L}(V,W)$ itself is also a vector space

Check. $(T+S)(v) = T(v)+S(v)$

$(\alpha T)(v) = \alpha T(v)$

In particular $0_{\mathcal{L}(V,W)}: V \to W$, where $0_{\mathcal{L}(V,W)}(v) := 0_W$ for all $v \in V$

Def (1) If $W = V$, then $\mathcal{L}(V) := \mathcal{L}(V,V)$ is called the space of linear operators.

(2) If $W = \mathbb{F}$ $(= \mathbb{F}^1)$, then $V^* := \mathcal{L}(V,\mathbb{F})$ is the dual space of V and $\alpha \in V^*$ is called a linear functional.

Thm. Let $T: V \to W$, $S: W \to U$ be linear transformations.

(1) $T(0_V) = 0_W$

(2) $S \circ T: V \to U$ is also a linear transformation.

(3) If T is bijective, then $T^{-1}: W \to V$ is also a linear transformation.

(1) $T(0_V) = T(v - v) = T(v) - T(v) = 0_W$

(2) $S(T(\alpha v_1 + \beta v_2)) = S(\alpha T(v_1) + \beta T(v_2)) = \alpha S \circ T(v_1) + \beta S \circ T(v_2)$

(3) T is 1-1 and onto, so $\forall\, w \in W, \exists!\, v$ s.t. $T(v) = w$

$aw_1 + bw_2 = aT(v_1) + bT(v_2) = T(av_1 + bv_2)$

$T^{-1}(aw_1 + bw_2) = av_1 + bv_2 = aT^{-1}(w_1) + bT^{-1}(w_2)$

(linear trans.)

Recall. $T: V \to W$ is called an isomorphism if T is bijective

e.g. (1) $V_3 := \{(a_1, a_2, \cdots) \mid \text{only finitely many } a_i \neq 0\}$

Then $V_3 \cong \bigoplus_{n=1}^{\infty} \mathbb{F} \cong \mathbb{F}[x]$

(2) $V_1 := \{(a_1, a_2, \cdots) \mid a_i \in \mathbb{F}\}$

Then $V_1 \cong \prod_{n=1}^{\infty} \mathbb{F} \simeq \mathbb{F}[[x]]$ (formal power series)

(3) $M_{m\times n}(\mathbb{F}) \cong \mathbb{F}^{mn}$

Lec 6.

Remark. $T: V \to W$ is a linear transformation, and $\{b_i \mid i \in I\}$ is a basis, then T is uniquely determined by the values of $\{T(b_i) \mid i \in I\}$ in W

Conversely, given any subset $\{w_i \mid i \in I\} \subseteq W$
we can define $T: V \to W$ uniquely by $T(a_1 b_{i_1} + \cdots + a_k b_{i_k}) = a_1 w_{i_1} + \cdots + a_k w_{i_k}$

Examples of linear transformations on quotient spaces.

Prop. 1 Let $V' \leq V$ be a subspace, then the map
$\pi_{V'}: V \to V/V'$, $\pi_{V'}(v) := v + V'$ is a surjective linear transformation.

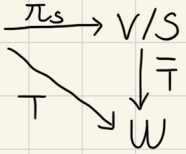
Def. $\ker(T) := \{v \in V : T(v) = 0_W\}$ where $T: V \to W$ is a linear transformation.

Prop. 2 Suppose $S \leq V$ is a subspace satisfying $S \leq \ker(T)$
then there is a linear transformation $\bar{T}: V/S \to W$
defined by $\bar{T}(v+S) := T(v)$ $(\forall v \in V)$

proof:) (well-defineness), i.e. If $v+S = v'+S$, then $T(v+S) = T(v'+S)$
If $v+S = v'+S$, then $v - v' \in S$, since $S \leq \ker(T)$, then $T(v-v') = 0$
$T(v) = T(v')$

Check. $\bar{T}$ is a linear transformation
$\bar{T}(a(v+S)) = \bar{T}(av+S) = T(av) = aT(v) = a\bar{T}(v+S)$
$\bar{T}((v+S)+(u+S)) = \bar{T}(v+u+S) = T(v+u) = T(v) + T(u) = \bar{T}(v+S) + \bar{T}(u+S)$

Remark. $\bar{T}: V/S \to W$ satisfies the following communicative diagram:



Recall. For $T: V \to W$ linear
- $\text{im}(T) := \{T(v) \mid v \in V\}$
- $\ker(T) := \{v \mid T(v) = 0\}$
- T is injective $\iff \ker(T) = \{0\}$
- T is surjective $\iff \text{im}(T) = W$
- $\text{rank}(T) = \dim(\text{im}(T))$
- $\text{nullity}(T) = \dim(\ker(T))$

Rank-Nullity Theorem

Let $T: V \to W$ linear, with $\dim(V) < \infty$, then $\text{rank}(T) + \text{nullity}(T) = \dim(V)$

proof: We see that there is a linear transformation $\bar{T}: V/\ker(T) \to \text{im}(T)$

This is because $T: V \to \text{im}(T)$ is linear

Claim. $\bar{T}$ is a bijection, i.e. isomorphism

Check 1. $\bar{T}$ is surjective, this is clear from the property

Check 2. $\bar{T}$ is injective

let $v + \ker(T) \in V/\ker(T)$, if $\bar{T}(v+\ker(T)) = 0_W = T(v)$

$\Rightarrow T(v) = 0 \Rightarrow v \in \ker(T)$, so $v + \ker(T) = \ker(T)$

so $v + \ker(T) = 0_{V/\ker(T)}$, i.e. $\bar{T}$ is injective

And we see that $V/\ker(T) \cong \text{im}(T)$ (1st isomorphism theorem)

$\dim(V/\ker(T)) = \dim(\text{im}(T)) \Rightarrow \dim(V) = \text{rank}(T) + \text{nullity}(T)$

Now we go back to Dual Space V^*

Recall. $V^* = \mathcal{L}(V, \mathbb{F}) = \{\alpha: V \to \mathbb{F} \text{ linear}\}$ Goal. Compare V and V^*

Let $B := \{b_i \mid i \in I\}$ be a basis of V

Define a subset $B^* := \{f_i : i \in I\}$ of V^* by: $f_i(b_j) = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$

($f_i: V \to \mathbb{F}$ linear transformation, so it's uniquely defined by values $\{f_i(b_j) \mid j \in I\}$)

E.g. $V := \{a_0 + a_1 x + a_2 x^2 \mid a_i \in \mathbb{R}\} (\cong \mathbb{R}^2)$ with $B = \{1, x, x^2\}$ (b_0, b_1, b_2)

Then $f_0(b_0) = 1$, $f_0(b_1) = 0$, $f_0(b_2) = 0$

i.e. $f_0(a_0 + a_1 x + a_2 x^2) = a_0$

Similarly, $f_1(a_0 + a_1 x + a_2 x^2) = a_1$, $f_2(a_0 + a_1 x + a_2 x^2) = a_2$

Consider $\alpha: V \to \mathbb{F}$ given by $\alpha(p(x)) = p'(3)$

Then $\alpha \in V^*$ with $\alpha(a_0 + a_1 x + a_2 x^2) = a_1 + 6a_2$, i.e. $\alpha = f_1 + 6f_2$

Question. Are all $\alpha \in V^*$ uniquely given by linear transformation of B^*?

In other word, is B^* a basis of V^*?

Proposition $\mathcal{B}^*$ is linearly independent in V^*

proof: Let $\{f_{i_1}, \cdots, f_{i_k}\} \subseteq \mathcal{B}^*$ be an arbitary subset of $\mathcal{B}^*$

Consider $a_1 f_{i_1} + \cdots + a_k f_{i_k} = 0_{V^*}$

so $(a_1 f_{i_1} + \cdots + a_k f_{i_k})(b_{i_j}) = a_j = 0$

so $a_1 = a_2 = \cdots = a_k = 0$

Thm. Suppose $\dim(V) \overset{=m}{}, \dim(W) \overset{=n}{} < \infty$, then $\dim(\mathcal{L}(V,W)) = \dim(V)\dim(W)$

proof: Clearly $\mathcal{L}(V,W) \cong M_{m\times n}(\mathbb{F})$

so $\dim(\mathcal{L}(V,W)) = mn$

Coltary. If $\dim(V) = n < \infty$, then $\mathcal{B}^*$ is a basis of V^*

proof: $\dim(V^*) = \dim(\mathcal{L}(V,\mathbb{F})) = \dim(V)$

Also $\mathcal{B}^*$ is linearly independent, $|\mathcal{B}^*| = |\mathcal{B}| = n$

so $\mathcal{B}^*$ is a basis of V^*

Def. Let V be a vector space. Given $S \subset V$, we define the annihilator of S in V^* as

$$\mathrm{Ann}(S) := \{f \in V^* \mid f(s) = 0 \text{ for all } s \in S\}$$

Also written as S°

Thm. Suppose $W \leq V$, then $\dim(W) + \dim(W^\circ) = \dim(V) < \infty$

proof: Take $\mathcal{B}_W = \{v_1, \cdots, v_m\}$ as a basis for W. then we can extend it to be a basis for V, $\mathcal{B}_V = \{v_1, \cdots, v_m, v_{m+1}, \cdots, v_n\}$

Since $\dim V < \infty$, we take $\mathcal{B}^* = \{f_1, \cdots, f_n\}$, where $f_i(v_j) = \delta_{ij}$

Then we can see that $\{f_{m+1}, \cdots, f_n\}$ forms a spanning set of W°

Also it is linearly independent, so $\dim(W^\circ) = n - m$

Therefore $\dim(W) + \dim(W^\circ) = \dim(V)$

Lec. 7

Thm. (1) $\mathrm{Ann}(S) \leq V^*$ is a vector subspace of V^*

(2) If W_1, W_2 are subspaces of V, then

$\mathrm{Ann}(W_1+W_2) = \mathrm{Ann}(W_1) \cap \mathrm{Ann}(W_2)$, $\mathrm{Ann}(W_1 \cap W_2) = \mathrm{Ann}(W_1) + \mathrm{Ann}(W_2)$

(3) If $\dim(V) < \infty$, then for any $W \leq V$, $\dim(\mathrm{Ann}(W)) + \dim(W) = \dim(V)$

Observation. For $\dim(V) < \infty$, $\dim(\mathrm{Ann}(W)) = \dim(V/W)$, then we can find an isomorphism between V/W and $\mathrm{Ann}(W)$

$T: \mathrm{Ann}(W) \xrightarrow{\cong} V/W$

defined by $\{g_{k+1}, \cdots, g_n\}$ (basis for $\mathrm{Ann}(W)$) $\{v_{k+1}+W, \cdots, v_n+W\}$

$T(g_j) := v_j + W$

Question. Is it still true if $\dim(V) = \infty$?

Can we define T without using basis of $\mathrm{Ann}(W)$ and V/W?

Thm. There is a natural isomorphism between $\mathrm{Ann}(W) \cong (V/W)^*$

Construct $\Phi: \mathrm{Ann}(W) \to (V/W)^*$, $\Psi: (V/W)^* \to \mathrm{Ann}(W)$

s.t. $\Phi \circ \Psi = id_{(V/W)^*}$, $\Psi \circ \Phi = id_{\mathrm{Ann}(W)}$

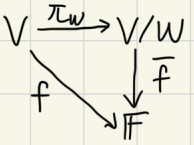
Take $f \in \mathrm{Ann}(W)$, then $f: V \to \mathbb{F}$ s.t. $W \leq \ker(f)$

By a theorem in quotient space, we have linear transformation

$\bar{f}: V/W \to \mathbb{F}$ such that $\bar{f}(v+W) := f(v) \in \mathbb{F}$

Then we can define $\Phi: \mathrm{Ann}(W) \to (V/W)^*$ by

$f \longmapsto \bar{f}$



Claim. Φ is a linear transformation.

$\Phi(\alpha f + \beta g) := \overline{\alpha f + \beta g} \in (V/W)^*$, $f, g \in \mathrm{Ann}(W)$

$\Phi(\alpha f + \beta g)(v+W) = \overline{\alpha f + \beta g}(v+W)$

fact: $f, g \in (V/W)^*$ are equal $\Leftrightarrow f(v+W) = g(v+W)$ $\forall v+W \in V/W$

For any $v+W \in V/W$, $\Phi(\alpha f + \beta g)(v+W) := \overline{\alpha f + \beta g}(v+W) := (\alpha f + \beta g)(v) = \alpha f(v) + \beta f(v)$ ($\in \mathbb{F}$)

$= \alpha \bar{f}(v+W) + \beta \bar{g}(v+W) = \alpha \Phi(f)(v+W) + \beta \Phi(g)(v+W)$

Construct Ψ $\Psi: (V/W)^* \to \mathrm{Ann}(W)$

Step1. (Complementation) For any $W \leq V$, there is a $U \leq V$, s.t. $V = W \oplus U$

Step2. $U \cong V/W$

$\forall v \in V$, $v = u + w$ uniquely, then $v + W = u + W$

Thus we define $\bar{T}$ by $\bar{T}(v+W) = \bar{T}(u+W) := u$, see that $\bar{T}$ is an isomorphism.

Step3. $U^* \cong (V/W)^*$, define $\sigma: (V/W)^* \to U^*$ by $\sigma(f) := f \circ \bar{T}$

Step4. $U^* \xrightarrow{\cong} \mathrm{Ann}(W)$

Lec. 8

Def. Let $W \leq V$ be fixed, then we define.

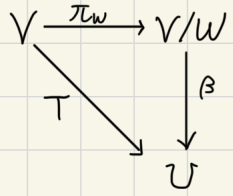
$\mathcal{C}_{eqs} := \{(X, \Phi) \mid \Phi : V \to X \text{ linear, s.t. } W \leq \ker(\Phi)\}$

$(V/W, \pi_W : V \to V/W) \in \mathcal{C}_{eqs}$

Take any $(U, T : V \to U)$, we have $\beta := \bar{T} : V/W \to U$

s.t. $\beta(v+W) := T(v)$, i.e. $\beta(\pi_W(v)) = T(v)$

↳ This is well defined since $W \leq \ker(T)$



Direct Sum $\bigoplus_{i\in I} V_i$, let V_i be fixed

Define:

$\mathcal{C}_{ds} := \{(X, \{\Phi_j\}_{j\in I}) \mid \Phi_j : V_j \to X \text{ linear}\}$

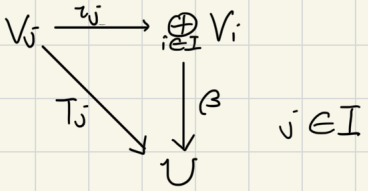
$(\bigoplus_{i\in I} V_i, \{i_j : V_j \to \bigoplus_{i\in I} V_i\}) \in \mathcal{C}_{ds}$

$i_j : V_j \to \bigoplus_{i\in I} V_i$ is given by $i_j(v_j) = (\cdots, 0, v_j, 0, \cdots)$

Take any $(U, \{T_j : V_j \to U\}) \in \mathcal{C}_{ds}$

define $\beta : \bigoplus_{i\in I} V_i \to U$ by $\beta(\cdots, v_j, \cdots) := \sum_{j\in I} T_j(v_j)$

Also, $\beta(\cdots, 0, v_j, 0, \cdots) = T_j(v_j)$, so $\beta(i_j(v_j)) = T_j(v_j)$



Direct Product $\prod_{i\in I} V_i$ (V_i fixed)

Define $\mathcal{C}_{dp} := \{(X, \{\Psi_j\}_{j\in I} \mid \Psi_j : X \to V_j\}$

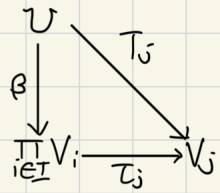
let $\tau_j : \prod_{i\in I} V_i \to V_j$, then $(V_j, \{\tau_j\}_{j\in I}) \in \mathcal{C}_{dp}$

$\tau_j(\cdots, v_j, \cdots) = v_j$

For any $(U, \{T_j : U \to V_j\}) \in \mathcal{C}_{dp}$

let $\beta : U \to \prod_{i\in I} V_i$ be given by $\beta(u) := (\cdots, T_j(u), \cdots)$, then

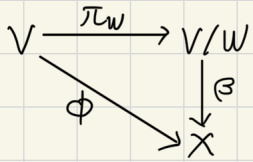
so $\tau_j \circ \beta = T_j$



Def. A category $\mathcal{C}$ consists of:

① A set of objects

② For the objects $X, Y \in Obj(\mathcal{C})$ a set of morphism.
$Hom(X,Y)$ (or $X \to Y$)



Let $W \leq V$ be fixed

$\mathcal{C}_{qs}$: { Objects: $\mathcal{C}_{qs} := \{(U, T: V \to U) \mid W \leq \ker(T)\}$

Morphism: $Hom((U,T),(X,\phi)) := \{\beta : U \to X \mid \beta \circ T = \phi\}$

Remark. For any $(X,\phi) \in \mathcal{C}_{qs}$, $Hom((V/W, \pi_W),(X,\phi)) = \{\beta : V/W \to X \mid \beta \circ \pi_W = \phi\}$
$= \{\bar{\Phi}\}$, where $\bar{\Phi}(v+W) := \phi(v)$

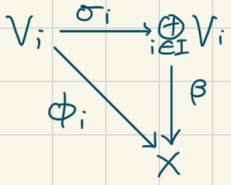
Def. Let $\mathcal{C}$ be a category. An object $I \in Obj(\mathcal{C})$ is called an initial if for $\forall\, X \in Obj(\mathcal{C})$, $Hom(I,X) = \{i_X\}$

Example.

(1) $\mathcal{C}$ = Vector spaces, $I = \{0\}$ is an initial object
Then for $\forall\, V \in \mathcal{C}$, $T(0) = 0_V$

(2) $\mathcal{C}_{qs}$, then $I = (V/W, \pi_W)$ is an initial object

(3) (Category for direct sum) Let V_i $(i \in I)$ be vector spaces over $\mathbb{F}$
Consider the category $\mathcal{C}_{ds} := \{(U, \{T_i : V_i \to U\}) \mid i \in I\}$
$Hom((U,\{T_i\}),(X,\{\phi_i\})) = \{\beta : U \to X \mid \beta \circ T_i = \phi_i \text{ for } \forall\, i \in I\}$
Then $I := (\bigoplus_{i\in I} V_i, \{\sigma_i : V_i \to \bigoplus_{i\in I} V_i\})$ is an initial object since
$Hom(I,(X,\{\phi_i\})) = \{\beta : \bigoplus_{i\in I} V_i \to X \mid \beta \circ \sigma_i = \phi_i \text{ for } \forall\, i \in I\} =$



Some MAT3040

Def. Suppose V is a vector space over $\mathbb{F}$ with $\dim(V)<\infty$ then given $B=\{v_1,\cdots,v_n\}$, $B'=\{v_1',\cdots,v_n'\}$ which are two bases $C_{B,B'}=(a_{ij})_{ij}$, where $v_i=\sum_{j=1}^{n} a_{ij}v_j'$ is called a change of basis

Def. Given $\dim(V), \dim(W)<\infty$, linear transformation $T: V\to W$, a ordered basis $A=\{v_1,\cdots,v_n\}$ for V and an ordered basis $B=\{w_1,\cdots,w_n\}$ for W, then $T(v_1,\cdots,v_n)=(w_1,\cdots,w_m)\,T_{B,A}$
Matrix $T_{B,A}$ is called a matrix representation of T

Def. Let $T: V\to W$ be an $\mathbb{F}$-linear map, then $T^*: W^*\to V^*$ defined by $T^*(f)(v):=f(T(v))$ for any $v\in V$ is called the adjoint of T

Prop. (1) T is surjective $\Leftrightarrow$ T^* is injective, vice versa
(2) $\ker(T^*)\simeq(W/\mathrm{Im}(T))^*$, $\ker(T)\simeq(W^*/\mathrm{Im}(T^*))^*$
proof: (1) Suppose T is surjective, let $f\in\ker(T^*)$, then $T^*(f)(v)=0$ for $\forall\, v\in V$
i.e. $f(T(v))=0$ for any $v\in V$, since T is surjective, $f(w)=0$ for $\forall\, w\in W$
therefore $f=0_{W^*}$
Conversely, if T^* is injective, suppose T is not surjective, then $\mathrm{im}(T)\subsetneq W$
(2) proof: $\psi\in\ker(T^*)$, $T^*(\psi)(v)=\psi(T(v))\equiv 0$ for all $v\in V$

Thm. Primary Decomposition Theorem.

Let $T: V \to V$ be a linear operator with $\dim(V) < \infty$

$m_T(x) = [p_1(x)]^{e_1} \cdots [p_k(x)]^{e_k}$

where p_i's are distinct monic, irreducible polynomials.

Let $V_i = \ker(p_i(T)^{e_i})$, then

(1) each V_i is T-invariant

(2) $V = V_1 \oplus \cdots \oplus V_k$

(3) $T|_{V_i}$ has the minimal polynomial $p_i(x)^{e_i}$

proof: if $p_i(T)^{e_i}(v) = 0$, $p_i(T)^{e_i}(T(v)) = T\,p_i(T)^{e_i}(v) = 0$

So each V_i is T-invariant

(2) See that each $p_i(x)^{e_i}$ are coprime

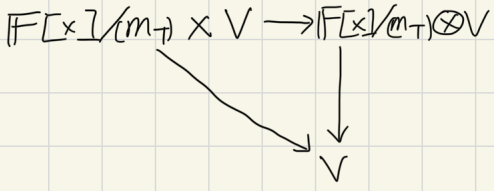
Then view V as $\mathbb{F}[x]$-module, $f \cdot v := f(T)(v)$

By CRT, $\mathbb{F}[x]/(m_T(x)) \cong \bigoplus_{i=1}^{k} \mathbb{F}[x]/(p_i^{e_i})$

Take tensor product for both side

$(\mathbb{F}[x]/(m_T)) \otimes V \cong \bigoplus_{i=1}^{k} (\mathbb{F}[x]/(p_i^{e_i})) \otimes V$

And thus $V \cong \bigoplus_{i=1}^{k} V/p_i(T)^{e_i} V$



WTS. $V/p_i(T)^{e_i} \cong \ker(p_i(T)^{e_i})$

Define $\phi: V \to \ker(p_i(T)^{e_i})$ by $\phi(v) = q_i(T)v$, wher $p_i^{e_i} q_i = m_T$

Then $\ker(\phi) = p_i(T)^{e_i} V$, Since $\gcd(p_i^{e_i}, q_i) = 1$, $\exists\, a, b \in \mathbb{F}[x]$

s.t. $a(x)q_i(x) + b(x)p_i(x)^{e_i} = 1$

For $y \in \ker(p_i(T)^{e_i})$, $y = (a(T)q_i(T) + b(T)p_i(T)^{e_i})(y) = a(T)q_i(T)y$

Therefore $y = q_i(T)(a(T)y)$, so ϕ is surjective

This implies that $V/p_i(T)^{e_i} \cong \ker(p_i(T)^{e_i})$

Therefore $V \cong V_1 \oplus \cdots \oplus V_k$, i.e. $V = V_1 \oplus \cdots \oplus V_k$

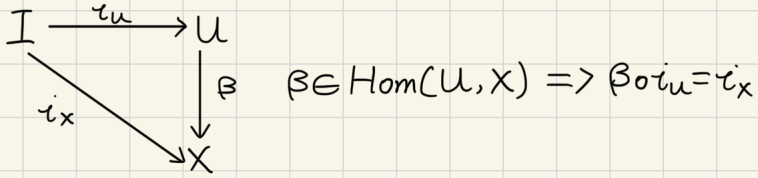
Lec 9.

Properties of initial objects:

(1) The initial object may not exist in a category

(2) In the case I exists in $\mathcal{C}$.

① For any $U, X \in \mathcal{C}$, suppose $\beta \in Hom(U, X)$, and $\{i_U\} = Hom(I, U)$ $\{i_X\} = Hom(I, X)$, then we have



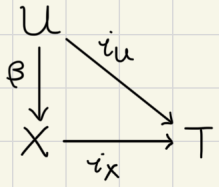
$\beta \in Hom(U, X) \Rightarrow \beta \circ i_U = i_X$

② If an initial object $I \in \mathcal{C}$ exists, then I is unique up to unique isomorphism, i.e. if $\exists J \in \mathcal{C}$ such that J is initial, then there is an unique isomorphism $\Phi: I \xrightarrow{\cong} J$ for $\Phi \in Hom(I, J)$

Def. An object $T \in Obj(\mathcal{C})$ is called terminal if for all $X \in Obj(\mathcal{C})$ $Hom(X, T) = \{i_X\}$ has exactly one element.

i.e. for any $U, X \in \mathcal{C}$, we have $\beta: U \to X$

where $i_X \circ \beta = i_U$



Examples. Let V_i $(i \in I)$ be fixed vector fields.

$\mathcal{C}_{ap} := \{(U, \{T_i: U \to V_i\}) \mid i \in I\}$

$Hom((U, \{T_i\}), (X, \{\Psi_i\})) := \{\beta: U \to X \mid \Psi_i \circ \beta = T_i \text{ for all } i \in I\}$

Then $(\prod_{i \in I} V_i, \{\tau_j: \prod_{i \in I} V_i \to V_j\})$ is a terminal element

$Hom((U, \{\sigma_i\}), (\prod_{i \in I} V_i, \{\tau_i\})) = \{\beta: U \to \prod_{i \in I} V_i \mid \sigma_i \circ \beta = \tau_i\} =$

Tensor Products

Motivation: Studying k-linear maps.

Def. Let $V_1, \cdots, V_k, W$ be vector spaces over $\mathbb{F}$. A map $f: V_1 \times \cdots \times V_k \to W$ is k-linear if $f(\cdots, \alpha v_i, \cdots, \beta v_j, \cdots) = \alpha f(\cdots, v_i, \cdots) + \beta f(\cdots, v_j, \cdots)$

Example.

① inner product spaces over $\mathbb{R}$ $\langle \cdot, \cdot \rangle$

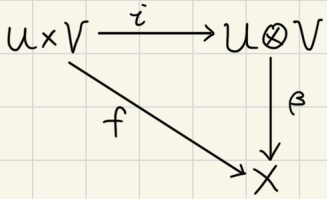
② determinant, $\det: \underbrace{\mathbb{F}^n \times \cdots \times \mathbb{F}^n}_{n \text{ times}} \to \mathbb{F}$ is n-linear

③ cross-product $\times: \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ $\quad (u, v) \mapsto u \times v$

Goal. Define category $\mathcal{C}_{tp} := \{(X, f: U \times V \to X) \mid f \text{ is bilinear}\}$ and an intitial object $(U \otimes V, i) \in \mathcal{C}_{tp}$ s.t.

$\beta: U \otimes V \to X$ is a linear transformation such that

$f = \beta \circ i$, where β is linear



For any given V and W, define

$\mathcal{A} := \{[v, w] \mid v \in V, w \in W\}$

$\mathcal{X} := \text{span}(\mathcal{A})$

Remark. The vectors $[v, w]$ are all linearly independent in $\mathcal{A}$

Let $\mathcal{Y} \leq \mathcal{X}$ be a vector subspace defined by subspace spanned by all the vectors of the form:

$[v+v', w] - [v, w] - [v', w]$

$[v, w+w'] - [v, w] - [v, w']$

$[\alpha v, w] - \alpha [v, w]$

$[v, \alpha w] - \alpha [v, w]$ for all $v, v' \in V$, $w, w' \in W$

Lec 10.

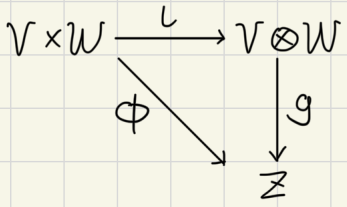
Def. The quotient space $\mathcal{X}/\mathcal{Y}$ (defined on the last page) is the tensor product space
i.e. $V\otimes W := \mathcal{X}/\mathcal{Y}$

For any $v\in V$, $w\in W$, we define $v\otimes w := [v,w]+\mathcal{Y} \in \mathcal{X}/\mathcal{Y}$
and define $\iota: V\times W \to V\otimes W$ by $\iota(v,w) := v\otimes w$

Arithmetic on $V\otimes W$:
$(v+v')\otimes w := [v+v',w]+\mathcal{Y} = [v+v',w]-\{[v+v',w]-[v',w]-[v,w]\}+\mathcal{Y}$
$=\{[v,w]+\mathcal{Y}\}+\{[v',w]+\mathcal{Y}\} = v\otimes w + v'\otimes w$
$(\alpha v)\otimes w = [\alpha v,w]+\mathcal{Y} = [\alpha v,w]-\{[\alpha v,w]-\alpha[v,w]\}+\mathcal{Y} = \alpha[v,w]+\mathcal{Y} = \alpha(v\otimes w)$

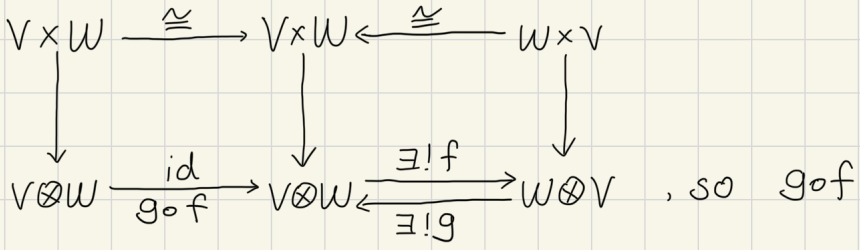
Lemma. $\iota: V\times W \to V\otimes W$ defined before is a bilinear map and $(V\otimes W,\iota)\in \mathcal{C}_{vp}$

Thm. $(V\otimes W, \iota: V\times W\to V\otimes W)$ is an initial subject.
proof: Let $(Z, g: V\times W\to Z)\in \mathcal{C}_{vp}$
* Define a linear transformation.
$\Phi: \mathcal{X}=\text{span}(\mathcal{S})\to Z$ by: for all $[v,w]\in\mathcal{S}$
$\Phi([v,w]) := g(v,w)$
Claim. $\mathcal{Y}\leq \ker(\Phi)$
Take $[v+v',w]-[v,w]-[v',w]\in\mathcal{Y}$
Then $\Phi([v+v',w]-[v,w]-[v',w]) = g(v+v',w)-g(v,w)-g(v',w) = g(0,w) = 0_Z$
Check for other vector in $\mathcal{Y}$
Then by universal property of quotient space, we have
$\beta: \mathcal{X}/\mathcal{Y}\to Z$ satisfying $\beta([v,w]+\mathcal{Y}) = \Phi([v,w]) = g(v,w)$



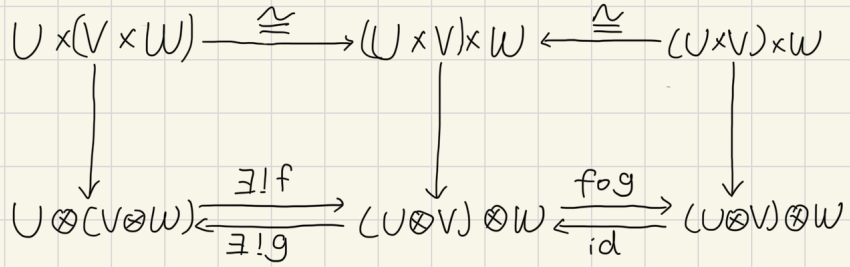
$\mathcal{Y}\leq \ker(\phi)$ (for each fixed w)

$V \otimes W \cong W \otimes V$



, so $g \circ f$

$(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$



Thm. Let $\{v_i \mid i \in I\}$ be a basis of V, $\{w_j \mid j \in J\}$ be a basis of W
Then $\{v_i \otimes w_j \mid i \in I, j \in J\}$ is a basis of $V \otimes W$

proof: Spanning set: A general vector in $V \otimes W$ is in the form

$v^{(1)} \otimes w^{(1)} + \cdots + v^{(k)} \otimes w^{(k)}$

$v^{(1)} \otimes w^{(1)} = (\alpha_1 v_{i_1} + \cdots + \alpha_p v_{i_p}) \otimes (\beta_1 w_{j_1} + \cdots + \beta_q w_{j_q}) = \sum_{m,n} \alpha_m \beta_n (v_m \otimes w_n) \in \operatorname{span}\{v_i \otimes w_j\}$

Linear independence.

For an arbitary finite subset $\{v_{i_1} \otimes w_{j_1}, \cdots, v_{i_k} \otimes w_{j_k}\}$

Consider $\alpha_1 (v_{i_1} \otimes w_{i_1}) + \cdots + \alpha_k (v_{i_k} \otimes w_{i_k}) = 0$

WTS. $\alpha_1 = \cdots = \alpha_k = 0$

Recall $\{\sigma_i \mid i \in J\} \subseteq V^*$, $\{\tau_j \mid j \in J\} \subseteq W^*$

where $\sigma_i(v_s) = \delta_{is}$, $\tau_j(w_t) = \delta_{jt}$

are linearly independent, then consider the map

$\Phi : V \times W \to \mathbb{F}$, Then $\Phi(v+v', w) = \sigma_{i_1}(v+v')\tau_{j_1}(w)$

$(v, w) \mapsto \sigma_{i_1}(v)\tau_{j_1}(w) = \sigma_{i_1}(v)\tau_{j_1}(w) + \sigma_{i_1}(v')\tau_{j_1}(w) = \Phi(v, w) + \Phi(v', w)$

So consider the linear map $\psi : V \otimes W \to \mathbb{F}$

(This is from the universal property of $\otimes$)

satisfying $\psi(v \otimes w) := \sigma_{i_1}(v)\tau_{j_1}(w)$

Therefore $\alpha_1(\sigma_{i_1}(v_{i_1})\tau_{j_1}(w_{j_1})) + \cdots + \alpha_k(\sigma_{i_1}(v_{i_k})\tau_{i_1}(w_{i_k})) = \alpha_1 = 0$

Similary, check that $\alpha_2 = \cdots = \alpha_k = 0$

Prop. Let $T : V \to V'$, $S : W \to W'$ be two linear transformations
Then there exist $T \otimes S : V \otimes W \to V' \otimes W'$ (which is unique)
satisfying $(T \otimes S)(v \otimes w) = T(v) \otimes S(w)$

proof: Using universal property of $\otimes$

Consider $\Phi : V \times W \to V' \otimes W'$, $\Phi(v, w) = T(v) \otimes T(w)$

Claim. Φ is a bilinear map

$\Phi(v+v', w) = T(v+v') \otimes S(w) = T(v) \otimes S(w) + T(v') \otimes S(w) = \Phi(v, w) + \Phi(v', w)$

$\Phi(v, w+w') = T(v) \otimes S(w+w') = T(v) \otimes S(w) + T(v) \otimes S(w') = \Phi(v, w) + \Phi(v, w')$

Therefore $\exists!\ T \otimes S : V \otimes W \to V' \otimes W'$ given by $(T \otimes S)(v \otimes w) := T(v) \otimes T(w)$

Def. Let $f: \underbrace{V\times\cdots\times V}_{k \text{ terms}} \to U$ be a k-linear map, we say f is k-alternative if $f(\cdots, \overset{i\text{-th}}{\underset{\downarrow}{v}}, \cdots, \overset{j\text{-th}}{\underset{\downarrow}{v}}, \cdots) = 0_U$ for $\forall\, v\in V$ and $i\neq j$

Example. $\times : \mathbb{R}^3\times\mathbb{R}^3 \to \mathbb{R}^3$ cross product

$\det: \underbrace{\mathbb{F}^n\times\cdots\times\mathbb{F}^n}_{n \text{ terms}} \to \mathbb{F}$

Lemma. If $f: V\times\cdots\times V \to U$ is k-alternative, then
$f(\cdots, v, \cdots, u, \cdots) = -f(\cdots, u, \cdots, v, \cdots)$
proof: $f(\cdots, v+u, \cdots, v+u, \cdots) = 0_U = f(\cdots, v, \cdots, v+u, \cdots) + f(\cdots, u, \cdots, v+u, \cdots)$
$= f(\cdots, v, \cdots, u, \cdots) + f(\cdots, u, \cdots, v, \cdots)$

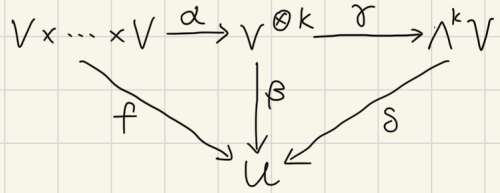
Def. Define the category $\mathcal{C}_{ep}$ by (fixed a vector space V)
Objects: $\{(U, f: V\times\cdots\times V\to U \text{ } k\text{-alternative})\}$
Morphisms: $\mathrm{Hom}((U,f),(W,g)) = \{\gamma: U\to W \text{ linear} \mid g = \gamma\circ f\}$

Then define $(\Lambda^k V, \iota: V\times\cdots\times V\to\Lambda^k V)$ in $\mathcal{C}_{ep}$, so that for $\forall$ $(U,f)\in \mathrm{Obj}(\mathcal{C}_{ep})$, $\exists!\ \beta\in\mathrm{Hom}((U,f),(\Lambda^k V,\iota))$

Consider $V^{\otimes k} := V\otimes\cdots\otimes V$ and $\mathcal{A}\leq V^{\otimes k}$, where
$\mathcal{A} := \mathrm{Span}\{\cdots\otimes v\otimes\cdots\otimes v\otimes\cdots \mid v\in V\}$
Then $\Lambda^k V := V^{\otimes k}/\mathcal{A}$, which is called the k^{th}-exterior power of V
write $v_1\wedge v_2\wedge\cdots\wedge v_k := v_1\otimes v_2\otimes\cdots\otimes v_k + \mathcal{A} \in V^{\otimes k}/\mathcal{A} = \Lambda^k V$
and define $\iota: V\times\cdots\times V\to\Lambda^k V$ by $\iota(v_1,\cdots,v_k) := v_1\wedge\cdots\wedge v_k$

Prop. $\iota: V\times\cdots\times V\to\Lambda^k V$ is k-alternative
proof: $\iota(v_1,\cdots,v,\cdots,v,\cdots,v_k) = v_1\wedge\cdots\wedge v\wedge\cdots\wedge v\wedge\cdots\wedge v_k$
$= v_1\otimes\cdots\otimes v\otimes\cdots\otimes v\otimes\cdots\otimes v_k + \mathcal{A} = \mathcal{A} = 0_{\Lambda^k V}$

Thm. $(\Lambda^k V, \iota)$ is the initial object in $\mathcal{C}_{ep}$



(Sketch proof) Clearly for $\mathcal{C}_{ep}$, $\exists!\ \beta: V^{\otimes k}\longrightarrow U$ linear such that $f=\beta\circ\alpha$

Here $\alpha(v_1,\cdots,v_k)=v_1\otimes\cdots\otimes v_k$, $\gamma(v_1\otimes\cdots\otimes v_k)=v_1\wedge\cdots\wedge v_k$, then $\iota=\gamma\circ\alpha$

$\beta(v_1\otimes\cdots\otimes v_k):=f(v_1,\cdots,v_k)$, therefore $\beta(\mathcal{A})=0_U$

Hence $\mathcal{A}\leq\ker(\beta)$, so use the universal property of $\mathcal{C}_{qs}$

$\exists!\ \delta:\Lambda^k V\to U$, s.t. $\beta=\delta\circ\gamma$

Hence $f=\delta\circ\gamma\circ\alpha=\delta\circ\gamma$, where δ is unique

Thm. Let $B=\{v_1,\cdots,v_n\}$ be a basis for V, then $\{v_{i_1}\wedge\cdots\wedge v_{i_k}\mid 1\leq i_1<\cdots<i_k\leq n\}$ is a basis of $\Lambda^k V$

(Sketch proof) $\{v_{j_1}\otimes\cdots\otimes v_{j_k}\mid 1\leq j_1,\cdots,j_k\leq n\}$ spans $V^{\otimes k}$

then $\{v_{j_1}\otimes\cdots\otimes v_{j_k}+\mathcal{A}\mid 1\leq j_1,\cdots,j_k\leq n\}$ spans $V^{\otimes k}/\mathcal{A}$

This is because $\pi: V^{\otimes k}\to V^{\otimes k}/\mathcal{A}$ is surjective

However, all repeated terms are 0, and if $p>q$, we have

$v_{j_1}\wedge\cdots\wedge v_{j_p}\wedge\cdots\wedge v_{j_q}\wedge\cdots v_{j_k}=-(v_{j_1}\wedge\cdots\wedge v_{j_q}\wedge\cdots v_{j_p}\wedge\cdots)$

Therefore $\{v_{j_1}\wedge\cdots\wedge v_{j_k}\mid 1\leq j_1<\cdots<j_k\leq n\}$ is a spanning set

We can check that this is linearly independent.

Prop. $\dim(\Lambda^k V)=\binom{n}{k}$ $(1\leq k\leq n)$

For $k>n$, $\Lambda^k V=\{0\}$

Observe that $\dim(\Lambda^n V)=1$, so for $\forall T: V\to V$ linear, $\exists\,\Delta_T\in\mathbb{F}$ s.t. $T(v_1)\wedge T(v_2)\wedge\cdots\wedge T(v_n)=\Delta_T(v_1\wedge v_2\wedge\cdots\wedge v_n)$

Def. The determinant of T is defined as $\det(T):=\Delta_T$

Properties of $\det(A)$

① $\det(I_n) = 1$

② $\det(\cdots | a | \cdots | a | \cdots) = 0$

③ $\det(\cdots | \alpha a_i + \beta b_i | \cdots) = \alpha \det(\cdots | a_i | \cdots) + \beta \det(\cdots | b_i | \cdots)$

<u>Prop.</u> If $S, T : V \longrightarrow V$, then

$\det(S) \cdot \det(T) = \det(S \circ T)$

proof: Take any basis of V

$(S \circ T)^{\wedge n}(v_1 \wedge \cdots \wedge v_n) = ST(v_1) \wedge \cdots \wedge ST(v_n) = S^{\wedge n}(T(v_1) \wedge \cdots \wedge T(v_n))$

$= \det(T)(S(v_1) \wedge \cdots \wedge S(v_n)) = \det(S)\det(T)(v_1 \wedge \cdots \wedge v_n)$

so $\det(S \circ T) = \det(S) \cdot \det(T)$

<u>Thm.</u> The determinant is independent of the choice of basis.

proof: let $\{e_1, \cdots, e_n\}$ & $\{f_1, \cdots, f_n\}$ be two basis

let $f_i = S(e_i)$, then $\det(S) \neq 0$

$T(f_1) \wedge \cdots \wedge T(f_n) = TS(e_1) \wedge \cdots \wedge TS(e_n) = \det(T_1)\det(S)(e_1 \wedge \cdots \wedge e_n)$

$= \det(T_2)(f_1 \wedge \cdots \wedge f_n) = \det(T_2)\det(S)(e_1 \wedge \cdots \wedge e_n)$

Therefore $\det(T_1) = \det(T_2)$

Def. Let R be a communicative ring with identity, whose elements are called scalars. An *R-module* is a non-empty set M where

1. $(M,+)$ is an abelian group
2. For all $r,s \in R$, and $u,v \in M$:

$r(u+v)=ru+rv$; $(s+r)v=sv+rv$; $(rs)u=r(su)$; $1u=u$

The ring R is called the base ring of M

Def. A submodule of an R-module M is a non-empty subset of M where S is also an R-module, denoted $S \leq M$

Thm. A non-empty subset S of R-module M is a submodule if and only if it is closed under taking linear combinations.

Def. The submodule spanned by a subset S of a module M is the set of all linear combinations of elements in S:

$\langle\langle S \rangle\rangle = \{r_1v_1+\cdots+r_nv_n \mid r_i \in R, v_i \in S, n \geq 1\}$

S is said to span M if $M=\langle\langle S \rangle\rangle$

Def. An R-module M is said to be finitely generated if it contains a finite set that generates M. M is *n-generated* if $|S|=n$

Def. A subset S of an R-module M is linearly independent if for any $v_1,\cdots,v_n \in S$, $r_1,\cdots,r_n \in R$, $r_1v_1+\cdots+r_nv_n=0 \Rightarrow r_1,\cdots r_n=0$

E.g.

Let $R=\mathbb{F}[x]=M$. Then any ideal $\langle\langle m(x) \rangle\rangle = I \lhd \mathbb{F}[x]$ is 1-generated, i.e. $\mathbb{F}[x]$ is a PID

W.T.S $\mathbb{F}[x]$ is an Euclidian domain

Define $f: \mathbb{F}[x] \to \mathbb{N}$ by $f(p)=\deg(p)$

Remark. In vector spaces, any non-zero vector $\{v\}$ is linearly independent, however this is not true in modules

e.g. $R=\mathbb{Z}$, $M=\mathbb{Z}_m$

Then $[1]\in M$ is nonzero, $m\cdot[1]=[m]=[0]$

Hence $\{[1]\}$ is linearly dependent

Recall. I is an ideal of R if $\forall a,b\in I, r\in R$

$ar\in I$, $a+b\in I$, denoted $I\lhd R$

I is a proper ideal if $I\neq R$

I is principle if $\exists a\in R$, $I=(a)=\{ar : r\in R\}$

R is a principle ideal domain (PID) if every proper of R is principle

Def. Let M be an R-module. Then torsion of M is

$M_{tor}:=\{m\in M \mid r\cdot m=0 \text{ for some } r\in R\}$

① M is torsion free if $M_{tor}=\{0_M\}$

② M is a torsion module if $M=M_{tor}$

Example. V is a vector space over $\mathbb{F}$, $T:V\to V$ is linear

$M=V$ is an $R=\mathbb{F}[x]$ module.

$M_{tor}:=\{v\in V \mid p(x)\cdot v=0 \text{ for some } p(x)\in\mathbb{F}[x]\}$

$p(x)\cdot v:=p(T)(v)$, By Hamilton-Cayley thm, $\chi_T(x):=\det(xI-T)\in R$ satisfies that $\chi_T(T)=0_{L(V)}$

Therefore $M_{tor}=M$

Prop. (1) $M_{tor}\leq M$ is a submodule

(2) If $m_1, m_2\in M_{tor}$, i.e. $r_1m_1=r_2m_2=0$ for some $r_1, r_2\neq 0$ in R then $am_1+bm_2\in M$ for all $a,b\in R$

Def. Let M be an R-module, $m\in M$

$\mathrm{Ann}(m):=\{r\in R \mid r\cdot m=0\}$

$\mathrm{Ann}(M):=\{r\in R \mid r\cdot m=0, \forall m\in M\}$

Remark.

(1) If M is torsion-free, then $\mathrm{Ann}(m)=\{0_R\}$ $\mathrm{Ann}(M)=\{0_R\}$

(2) If $M=M_{tor}$, then $\mathrm{Ann}(m)\neq\{0_R\}$

($\mathrm{Ann}(M)=\{0_R\}$ in some case)

Def. The minimal polynomial of $M=V$ $m_T(x)\in R$ is a monic polynomial satisfying

① $m_T(x)\cdot v=0$, $\forall v\in V$

② For any $f(x)\in\mathbb{F}[x]$ s.t. $f(x)\cdot v=0$, $\deg(m_T)\leq\deg(f)$

Prop. For $M=V$ as an $\mathbb{F}[x]$-module

$\mathrm{Ann}(M)=\langle\langle m_T(x)\rangle\rangle=\{m_T(x)p(x)\mid p(x)\in\mathbb{F}[x]\}$

proof: Let $g(x)\in\mathrm{Ann}(M)$. By dividing $g(x)$ with $m_T(x)$ one have $g(x)=q(x)\cdot m_T(x)+r(x)$ ($\mathbb{F}[x]$ is an Euclidean domain) where $\deg(r)<\deg(m_T)$. Then since $g(x)\in\mathrm{Ann}(M)$

So $g(x)\cdot v=(q(x)\cdot m_T(x)+r(x))\cdot v=r(x)\cdot v=0$

However, $\deg(r)<\deg(m_T)$, so $r(x)\notin\mathrm{Ann}(M)$, hence $r(x)=0$

Therefore $m_T(x)\mid g(x)$

Def. An R-module M is free if $\exists$ a linear independent subset $\mathcal{B} \subseteq M$ s.t. $\langle\langle \mathcal{B} \rangle\rangle = M$, we say $\mathcal{B}$ is a basis of M

Thm. Let M be a free module with basis $\mathcal{B}$, then
(1) All $m \in M$ is uniquely expressed in the form
$m = r_1 b_1 + \cdots + r_n b_n$ $(r_i \in R,\ b_i \in \mathcal{B})$
(2) $\mathcal{B}$ is a minimal spanning set of M
(3) $\mathcal{B}$ is a maximal linearly independent set of M

Def. Let M be an R-module and $N \leq M$. the quotient module is $M/N := \{m+N \mid m \in M\}$

Lemma. Let M be an R-module, $I \lhd R$ be a maximal ideal, then $IM := \{i_1 m_1 + \cdots + i_k m_k \mid i_\ell \in I,\ m_\ell \in M,\ k \in \mathbb{N}\}$
is a (R-)submodule of M
proof: $\forall r \in R$, $r(i_1 m_1 + \cdots + i_k m_k) \in IM$

Lemma. Consider $M/IM := \{m+IM \mid m \in M\}$
Then $\forall i \in I$, $i(m+IM) = 0_{M/MI}$ (trivial)

Therefore M/IM is an R/I module defined by
$(r+I)(m+IM) := rm+IM$

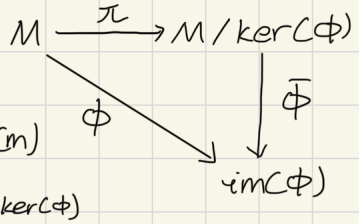
Thm. Let M be a free module with bases $\mathcal{B} = \{b_\alpha \mid \alpha \in A\}$ & $\mathcal{C} = \{c_j \mid j \in J\}$, then $|\mathcal{B}| = |\mathcal{C}|$
proof: M/IM is an $\mathbb{F} = R/I$ vector space
Claim. $\mathcal{B}' = \{b_\alpha + IM \mid \alpha \in A\}$ is a basis of M/IM
Clearly $\mathcal{B}'$ spans $M+IM$, and if $(r_1+I)(b_{\alpha_1}+IM) + \cdots + (r_n+I)(b_{\alpha_n}+IM)$
$= r_1 b_{\alpha_1} + \cdots + r_n b_{\alpha_n} + IM = IM$
so $r_1 b_{\alpha_1} + \cdots + r_n b_{\alpha_n} = i_1 m_1 + \cdots + i_n m_n = i_1(s_1^{(1)} b_{\alpha_1} + \cdots + s_1^{(n)} b_{\alpha_n}) + \cdots + i_n(s_n^{(1)} b_{\alpha_1} + \cdots + s_n^{(n)} b_{\alpha_n}) \in IM$
$[r_1 - (i_1^{(1)} + i_2^{(1)} + \cdots + i_n^{(1)})] b_{\alpha_1} + \cdots + [r_n - (i_1^{(n)} + \cdots + i_n^{(n)})] b_{\alpha_n} = 0$
Therefore $r_1, \cdots, r_n \in I$, i.e. $(r_1+I), \cdots, (r_n+I) = 0_{R/I}$
So $\mathcal{B}'$ is a basis of M/IM, and so do $\mathcal{C}$
Check. $|\mathcal{B}| = |\mathcal{B}'|$
Define $f: \mathcal{B} \to \mathcal{B}'$, $b_{\alpha_k} \to b_{\alpha_k} + IM$, clearly f is onto
if $b_{\alpha_k} - b_{\alpha_m} \in IM$, suppose $b_{\alpha_k} \neq b_{\alpha_m}$, w.l.o.g. $k=1$, $m=2$
$b_{\alpha_1} - b_{\alpha_2} = i_1^* b_{\alpha_1} + i_2^* b_{\alpha_2} + \cdots + i_n b_{\alpha_n}$, so $i_1^* - 1 = 0$, $i_2^* + 1 = 0$
However, I is proper, therefore $i_1^*, i_2^* \neq \pm 1$ ※
So f is bijective, $|\mathcal{B}| = |\mathcal{B}'| = |\mathcal{C}'| = |\mathcal{C}|$

Def. Let M, N be R-modules. An (R-)homomorphism is a map $\phi: M \to N$ satisfying
$\phi(r_1 m_1 + r_2 m_2) = r_1 \phi(m_1) + r_2 \phi(m_2)$

Def. $\ker(\phi) := \{m \in M \mid \phi(m) = 0\}$, $\operatorname{im}(\phi) := \{T(m) \mid m \in M\}$

Def. The collection of all R-homomorphism
$\operatorname{Hom}_R(M, N) := \{\phi: M \to N \mid \phi \text{ is } R\text{-homomorphism}\}$
Clearly it forms a R-module

Thm. $M/\ker(\phi) \cong \operatorname{im}(\phi)$



$\pi: M \to M/\ker(\phi)$, $m \mapsto m + \ker(\phi)$
$\bar{\Phi}: M/\ker(\phi) \to \operatorname{im}(\phi)$, $m + \ker(\phi) \mapsto \phi(m)$
if $\bar{\Phi}(m) = 0$, $m \in \ker(\phi)$, so $m + \ker(\phi) = 0_{M/\ker(\phi)}$
This implies that $\bar{\Phi}$ is injective
Also $\phi: M \to \operatorname{im}(\phi)$ is surjective, $\phi = \bar{\Phi} \circ \pi$, π is surjective
Therefore $\bar{\Phi}$ is surjective, i.e. $M/\ker(\phi) \cong \operatorname{im}(\phi)$

Example. $\phi: \mathbb{Z}[x] \to \mathbb{Z}_2$ $\quad p(x) \mapsto [p(0)]$
$\ker(\phi) = \{2k + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid k, a_i \in \mathbb{Z}\} = \langle\langle 2, x, x^2, \cdots \rangle\rangle$
$\operatorname{im}(\phi) = \mathbb{Z}_2$, so $\quad \mathbb{Z}[x]/\langle\langle 2, x, x^2, \cdots \rangle\rangle \cong \mathbb{Z}_2$

Consider a finite dimensional vector space V over $\mathbb{F}$
$T: V \to V$ linear, then we have a $\mathbb{F}[x]$-module V, where
$p(x) \cdot v := p(T)(v)$
Let $\mathcal{B}$ be a basis of V, $[T]_{\mathcal{B}\mathcal{B}}$ is a matrix representation
From linear algebra, $\Phi: V \to \mathbb{F}^n$ is an isomorphism of v. spaces
$v = a_1 v_1 + \cdots + a_n v_n \mapsto (a_1, \cdots, a_n)^T$, i.e. $v \mapsto [v]_{\mathcal{B}}$
Treat $\mathbb{F}^n$ as an $\mathbb{F}[x]$-module, where $p(x) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} := p([T]_{\mathcal{B}\mathcal{B}}) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$

Claim. Φ is a isomorphism of $\mathbb{F}[x]$ module
(1) $\Phi(v + v') = \Phi(v) + \Phi(v')$
(2) $\Phi(x^n v) = \Phi(T^n(v)) = [T^n(v)]_{\mathcal{B}} = [T]_{\mathcal{B}\mathcal{B}} [T^{n-1}(v)]_{\mathcal{B}} = [T]^n_{\mathcal{B}\mathcal{B}} [v]_{\mathcal{B}} = x^n \Phi(v)$
Therefore $\Phi(p(x) v) = p(x) \Phi(v)$
And clearly $V \cong \mathbb{F}$

Cor. Let $\dim(V)<\infty$, $T: V \to V$, for any basis $\mathcal{B}$ of V
$m_T(x) = m_{T_{\mathcal{B}\mathcal{B}}}(x)$
proof: Since $V \cong F^n$ as $\mathbb{F}[x]$ modules, then $Ann(V) = Ann(\mathbb{F}^n)$
Then $\langle\langle m_T(x)\rangle\rangle = \langle\langle m_{T_{\mathcal{B}\mathcal{B}}}(x)\rangle\rangle$, $m_T(x) = m_{T_{\mathcal{B}\mathcal{B}}}(x)$

Cor. Let A, B be similary matrices, i.e. $\exists$ M invertible s.t. $A = M^{-1}BM$, then $m_A(x) = m_B(x)$

Remark. Consider $T: \mathbb{F}^n \to \mathbb{F}^n$ defined by $T(x) := Ax$
Consider $\mathcal{E} = \{e_1, \cdots, e_n\}$ as usual basis of $\mathbb{F}^n$
Then $T_{\mathcal{E}\mathcal{E}} = A$, I
If use $\mathcal{B} = \{m_1, \cdots, m_n\}$ where m_i's are colums of M
Then $T_{\mathcal{B}\mathcal{B}} = B$, here M is invertible
$T_{\mathcal{B}\mathcal{B}} = I_{\mathcal{E},\mathcal{B}} T_{\mathcal{E},\mathcal{E}} I_{\mathcal{B},\mathcal{E}}$

proof of Cor.
$A = T_{\mathcal{B}\mathcal{B}}$, $B = T_{\mathcal{E},\mathcal{E}}$, then $m_A(x) = m_T(x) = m_B(x)$

Def. Let M be an R-module. We say M is noetherian if it satisfies Ascending Chain Condition (ACC)
i.e. If for all chains of submodules of M,
$N_1 \leq N_2 \leq N_3 \leq \cdots$
then there is a k such that $N_k = N_{k+1} = \cdots$

Thm. M is noetherian $\Leftrightarrow$ for all submodule $N \leq M$
N is finitely generated.
proof: ($\Leftarrow$) Suppose all submodules of M are finitely generated
& M contains an infinite ascending sequence
$N_1 \subseteq N_2 \subseteq \cdots$ of submodules.
Then $N = \bigcup N_i$ is a submodule of M, then N is finitely generated
Say $N = \langle\langle u_1, \cdots, u_n \rangle\rangle$, since $u_i \in N$, then $\exists k_i$ s.t. $u_i \in N_{k_i}$
Therefore $\exists\, k \in \mathbb{N}$, $N \subseteq N_k \subseteq N_{k+1} \subseteq \cdots \subseteq N$
i.e. $N_k = N_{k+1} = \cdots$
($\Rightarrow$) Suppose M is noetherian, N be a submodule of M
pick $u_1 \in N$, if $N = \langle\langle u_1 \rangle\rangle$, then it's true
Otherwise, let $N_1 = \langle\langle u_1 \rangle\rangle$, then $\exists\, u_2 \in N - N_1$,
let $N_2 = \langle\langle u_1, u_2 \rangle\rangle$, if $N_2 = N$, then it's done, else, pick $u_3 \in N - N_2$
Continue by this way, $N_1 \subseteq N_2 \subseteq \cdots \subseteq N$ is an ascending chain
Then $\exists n$, $\langle\langle u_1, \cdots, u_n \rangle\rangle = N$, i.e. N is finite generated

Def. A integral domain R is said noetherian if $M = R$ is a noetherian module.

Example. $R = \mathbb{Z}[x_1, x_2, \cdots]$ is not a noetherian ring.

Prop. A PID is noetherian.
Let R be an integral domain, I be a R-submodule of R
then $\forall\, r \in R$, $a, b \in I$, $a+b \in I$, $ra \in I$
This implies that I is an ideal.
Therefore I is 1-generated. (R is a PID)

Thm. Let R be a ID, Then R is a noetherian ring $\Leftrightarrow$ all finitely generated R-module M are noetherian modules.

proof: ($\Leftarrow$) trivial

($\Rightarrow$) Suppose R is noetherian

WTS. If M is f.g., then all $N \leq M$ is f.g.

① Consider homomorphism $\Phi: R^k \to M$ defined by

$\Phi(1,0,\cdots,0) = m_1, \cdots, \Phi(0,\cdots,0,1) = m_k$

where $M = \langle\langle m_1, \cdots, m_k \rangle\rangle$

Claim. $\forall N \leq M$, $\Phi^{-1}(N) \leq R^k$, this is true since $\Phi: R^k \xrightarrow{hom} M$

then $\Phi^{-1}(N) = \langle\langle \alpha_1, \cdots, \alpha_t \rangle\rangle$ is finitely generated

NTS. R^k is noetherian.

Let $M = R^k$, $N \leq R^k$.

when $k=1$, it clearly holds since R is noetherian

Suppose $N \leq R^n$ holds for $n < k$

Then let N be a submodule of R^k

Consider $S_1 := \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a \end{pmatrix} \middle| \exists a_1, \cdots, a_{k-1} \in R \text{ s.t. } \begin{pmatrix} a_1 \\ \vdots \\ a_{k-1} \\ a \end{pmatrix} \in N \right\}$

Then $S_1 \leq \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ r \end{pmatrix} \middle| r \in R \right\} \cong R^1$, so $S_1 = \langle\langle \begin{pmatrix} 0 \\ \vdots \\ \gamma_1 \end{pmatrix}, \cdots, \begin{pmatrix} 0 \\ \vdots \\ \gamma_t \end{pmatrix} \rangle\rangle$ f.g.

↑ This will be 1-generated if R is a PID

Consider $S_2 := \left\{ \begin{pmatrix} b_1 \\ \vdots \\ b_{k-1} \\ b_k \end{pmatrix} \in N \middle| b_k = 0 \right\} \leq \left\{ \begin{pmatrix} r_1 \\ \vdots \\ r_{k-1} \\ 0 \end{pmatrix} \middle| r_j \in R \right\} \cong R^{k-1}$

Then $S_2 = \langle\langle Y_2 \rangle\rangle$ for a finite set $Y_2 \subseteq S_2$

Take $n = \begin{pmatrix} c_1 \\ \vdots \\ c_{k-1} \\ c_k \end{pmatrix} \in N$, then $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ c_k \end{pmatrix} \in S_1 \Rightarrow c_k = r_1\gamma_1 + \cdots + r_t\gamma_t$

Since $\gamma_j \in S_1$, $\exists \begin{pmatrix} d_{j,1} \\ \vdots \\ d_{j,k-1} \\ \gamma_j \end{pmatrix} \in N$

Therefore $\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} c_1 - r_1 d_{1,1} + \cdots + r_t d_{t,1} \\ \cdots \\ c_{k-1} - r_1 d_{1,k-1} + \cdots + r_t d_{t,k-1} \\ 0 \end{pmatrix} + r_1 \underbrace{\begin{pmatrix} d_{1,1} \\ \vdots \\ d_{1,k-1} \\ \gamma_1 \end{pmatrix}}_{\in S_1'} + \cdots + r_t \underbrace{\begin{pmatrix} d_{t,1} \\ \vdots \\ d_{t,k-1} \\ \gamma_t \end{pmatrix}}_{\in S_1'}$

This implies that $n \in \langle\langle Y_2, \begin{pmatrix} d_{1,1} \\ \vdots \\ d_{1,k-1} \\ \gamma_1 \end{pmatrix}, \cdots, \begin{pmatrix} d_{t,1} \\ \vdots \\ d_{t,k-1} \\ \gamma_t \end{pmatrix} \rangle\rangle$

So N is f.g.

Let M be a finite generated module over a PID R

Goal. $M = M_{free} \oplus M_{tor}$ (Moreover, $M/M_{tor} \cong M_{free}$)

Here M_{free} is a free submodule of M, $M_{tor} = \{m \in M \mid rm = 0 \text{ for some } r \in R\}$

Step. 1 M/M_{tor} is free

Step. 2. $M/M_{tor} \cong M_{free}$

Lemma. M/M_{tor} is torsion-free

Proof: Suppose $m + M_{tor}$ is a torsion element

Then $\exists s \neq 0$, s.t. $s(m + M_{tor}) = 0_{M/M_{tor}}$

So $sm \in M_{tor}$, $\Rightarrow r \neq 0$, $rsm = 0$, hence $m \in M_{tor}$

Therefor M/M_{tor} is torsion-free

Lemma. Let N be a finite generated module. Then

N is torsion-free $\Leftrightarrow$ N is free (R is PID)

($\Leftarrow$) Suppose N is free, then $N = \langle\langle b_1, \cdots, b_k \rangle\rangle$, for $B = \{b_1, \cdots, b_k\}$ basis

Suppose $n = r_1 b_1 + \cdots + r_k b_k \in N_{tor}$, then $\exists s \neq 0$ s.t.

$0_N = sr_1 b_1 + \cdots + sr_k b_k$, then $sr_1 = \cdots = sr_k = 0$

Since R is an ID, then $r_1 = \cdots = r_k = 0$, so $n = 0_N$

($\Rightarrow$) Suppose $N = \langle\langle n_1, \cdots, n_k \rangle\rangle$ is torsion-free

when $k = 1$, $N = \langle\langle n_1 \rangle\rangle$, so if $rn_1 = 0$, then $r = 0$. so $\{n_1\}$ is a basis.

Induction hypothesis, suppose $N' = \langle\langle n_1, \cdots, n_\ell \rangle\rangle$ is free for $\ell < k$

Consider a k-generated module $N = \langle\langle n_1, \cdots, n_k \rangle\rangle$

If $\{n_1, \cdots, n_k\}$ is linearly independent, then it is done

Otherwise, $an_k = r_1 n_1 + \cdots + r_{k-1} n_{k-1}$, $a \neq 0$

Hence $aN := \{a \cdot n \mid n \in N\} = \langle\langle an_1, \cdots, an_{k-1}, an_k \rangle\rangle \leq \langle\langle n_1, \cdots, n_{k-1} \rangle\rangle$

Since R is a PID, then aN is $(k-1)$-generated

Hence aN is free

Now, consider the homomorphism $\Phi: N \to aN$, $n \mapsto an$

Clearly Φ is surjective, suppose $\Phi(n) = an = 0$

Since N is torsion-free, then Φ is injective

Hence, $N \cong aN$, so N is free.

Lemma. Let M be an R-module, $N \leq M$ s.t. M/N is free, Then $\exists\ N' \leq M$ such that

① $N' \cong M/N$

② $M = N' \oplus N$

Proof: By assumption, $M/N = \langle\langle \{b_i + N \mid i \in I\} \rangle\rangle$ where $\{b_i + N \mid i \in I\}$ is a basis of M/N

Let $N' = \langle\langle \{b_i \mid i \in I\} \rangle\rangle$. consider R-homomorphism $\psi : N' \to M/N$ where $\psi(b_i) = b_i + N$.

Check that ψ is isomorphic

② Suppose $n \in N' \cap N$, $n = r_1 b_{i_1} + \cdots + r_k b_{i_k}$

$n + N = r_1 b_{i_1} + \cdots + r_k b_{i_k} + N = r_1(b_{i_1} + N) + \cdots + r_k(b_{i_k} + N) = 0_{M/N}$

Since $\{b_i \mid i \in I\}$ is a basis of M/N, then $r_1 = \cdots = r_k = 0$

Therefore $N' \cap N = \{0\}$

Since $\{b_i \mid i \in I\}$ is a basis of M/N, then $\forall\ m \in M$ $\exists\ n' \in N'$, $n \in N$, s.t $m = n + n'$, hence $M = N \oplus N'$

Therefore, given that M is finite generated over a PID, we have M/M_{tor} is torsion-free and therefore free, hence naturally we have $M = M_{free} \oplus M_{tor}$

Thm. Moreover, if $M = F \oplus T$, $F \leq M$ is free, $T \leq M$ is a torsion module module, then $F \cong M_{free}$, $T = M_{tor}$

proof: Suppose $\tau = f + t \in M_{tor} \leq M = F \oplus T$, where $f \in F$, $t \in T$

This implies that $f = \tau - t \in M_{tor}$, then $sf = 0$ for some $s \in R \setminus \{0\}$

Since F is free (thus torsion free), then $f = 0$, i.e. $\tau = t$

so $T \subseteq M_{tor} \subseteq T$, so $T = M_{tor}$

Also, by the 2nd isomorphism theorem,

$M_{free} \cong M/M_{tor} = (F + M_{tor})/M_{tor} \cong F/\{0\} \cong F$

Consider the 1-generated torsion module $M=M_{tor}=\langle\langle v\rangle\rangle$, then $Ann(M)=Ann(v)=\{r\in R \mid rv=0\}$, we say that M is cyclic

Check. $Ann(v)$ is an ideal.

Then we assume that R is a PID, in this case $Ann(M)=Ann(v)=\langle\alpha\rangle$ for some $\alpha\in R$

Prop Let R be a PID, $M=\langle\langle v\rangle\rangle$ is cyclic with $Ann(M)=\langle\alpha\rangle$. then

1. $\langle\langle v\rangle\rangle\cong R/\langle\alpha\rangle$
2. For $\forall\, 0\neq\beta\in R$, $Ann(\beta v)=\langle\frac{\alpha}{gcd(\alpha,\beta)}\rangle$
3. $\langle\langle v\rangle\rangle=\langle\langle \beta v\rangle\rangle \iff gcd(\alpha,\beta)=1$

proof: (1) Define $\phi: R\longrightarrow\langle\langle v\rangle\rangle$ by $\phi(r)=rv$, $im(\phi)=\langle\langle v\rangle\rangle$, $\ker(\phi)=\langle\alpha\rangle$

Hence $R/\langle\alpha\rangle\cong\langle\langle v\rangle\rangle$

(2) $\forall\, r\in Ann(\beta v)$, $(r\beta)v=0$, so $\beta r=\alpha s$ for some $s\in R$

Since R is a PID, then $\exists c_1,c_2\in R$, $c_1\alpha+c_2\beta=gcd(\alpha,\beta)$,

$c_1r\beta+c_2r\alpha=(c_2r+s)\alpha$, $(c_2r+s)\alpha=gcd(\alpha,\beta)\cdot r$

Then $r\in\langle\frac{\alpha}{gcd(\alpha,\beta)}\rangle$, and clearly $\langle\frac{\alpha}{gcd(\alpha,\beta)}\rangle\subseteq Ann(\beta v)$

So $Ann(\beta v)=\langle\frac{\alpha}{gcd(\alpha,\beta)}\rangle$

(3) ($\Leftarrow$) Since $gcd(\alpha,\beta)=1$, $\exists\, x,y\in R$, s.t. $1=x\alpha+y\beta$

Then $v=(x\alpha+y\beta)v=y\beta v\in\langle\langle\beta v\rangle\rangle$, so $\langle\langle\beta v\rangle\rangle\leq\langle\langle v\rangle\rangle\leq\langle\langle\beta v\rangle\rangle$

($\Rightarrow$) $Ann(\beta v)=\langle\frac{\alpha}{gcd(\alpha,\beta)}\rangle=\langle\alpha\rangle$, so $gcd(\alpha,\beta)=1$

Thm. Let $M=\langle\langle v\rangle\rangle$ be cyclic with $Ann(v)=\langle\alpha\rangle$, $\alpha=p_1^{e_1}\cdots p_k^{e_k}$ ($p_i\in\mathcal{P}$, $e_i\in\mathbb{N}$), Then

1. $v=u_1+\cdots+u_k$, $Ann(u_i)=\langle p_i^{e_i}\rangle$
2. $\langle\langle v\rangle\rangle=\langle\langle u_1\rangle\rangle\oplus\cdots\oplus\langle\langle u_k\rangle\rangle$

proof: (1) Let $\beta_i=\frac{\alpha}{p_i^{e_i}}$, Then $gcd(\beta_1,\cdots,\beta_k)=1$

By Bezout's Th'm, $\exists\, r_1,\cdots,r_k\in R$, $r_1\beta_1+\cdots+r_k\beta_k=1$

Then $v=(r_1\beta_1+\cdots+r_k\beta_k)v=r_1\beta_1v+\cdots+r_k\beta_kv$

Let $u_i:=r_i\beta_iv$, so $v=u_1+\cdots+u_k$

$Ann(u_i)=\langle\frac{\alpha}{gcd(\alpha,r_i\beta_i)}\rangle=\langle\frac{\alpha}{\beta_i}\rangle=\langle p_i^{e_i}\rangle$

(2) Clearly, $\langle\langle v\rangle\rangle=\langle\langle u_1\rangle\rangle+\cdots+\langle\langle u_k\rangle\rangle$

Suppose $\alpha_1u_1+\cdots+\alpha_ku_k=0$, then $\beta_i(\alpha_1u_1+\cdots+\alpha_ku_k)=0 \Rightarrow \beta_i\alpha_iu_i=0$

Therefore $\alpha_i\in Ann(\beta_iu_i)=\langle\frac{p_i^{e_i}}{gcd(p_i^{e_i},\beta_i)}\rangle=\langle p_i^{e_i}\rangle=Ann(u_i)$

This implies that $\alpha_iu_i=0$, hence $\langle\langle u_i\rangle\rangle\cap\langle\langle u_j\rangle\rangle=\{0\}$

so $\langle\langle v\rangle\rangle=\langle\langle u_1\rangle\rangle\oplus\cdots\oplus\langle\langle u_k\rangle\rangle$

Cor. 中国剩余定理

Let R be a PID, $p_1, \cdots, p_k \in R$ be distinct primes, then

$R/\langle p_1^{e_1} \cdots p_k^{e_k} \rangle \cong R/\langle p_1^{e_1} \rangle \oplus \cdots \oplus R/\langle p_k^{e_k} \rangle$

proof: Consider the cyclic module M over R, $\mathrm{Ann}(M) = \langle \alpha \rangle = \langle p_1^{e_1} \cdots p_k^{e_k} \rangle$

Then $R/\langle p_1^{e_1} \cdots p_k^{e_k} \rangle \cong M = \langle\langle u_1 \rangle\rangle \oplus \cdots \oplus \langle\langle u_k \rangle\rangle \cong R/\langle p_1^{e_1} \rangle \oplus \cdots \oplus R/\langle p_k^{e_k} \rangle$

Def. A R-module M is primary if $\mathrm{Ann}(M) = \langle p^e \rangle$ for some p prime

Thm. (Primary Decomposition), Let R be a PID, M is a finitely generated torsion R-module with $\mathrm{Ann}(M) = \langle \alpha \rangle$, where $\alpha = p_1^{e_1} \cdots p_k^{e_k}$ for $p_1, \cdots, p_k$ be distinct primes and $e_i \in \mathbb{N}$, then

$M = M_1 \oplus \cdots \oplus M_k$, where with $\mathrm{Ann}(M_i) = \langle p_i^{e_i} \rangle$

proof: Let $M_i := \beta_i M = \{\beta_i m \mid m \in M\}$, clearly this is a submodule of M

Notice that $\langle p_i^{e_i} \rangle \subset \mathrm{Ann}(M_i)$, Also if $s \in \mathrm{Ann}(M_i)$, $s\beta_i m = 0$ for $\forall m \in M$

Therefore $s\beta_i \in \langle \alpha \rangle$, so $s \in \langle p_i^{e_i} \rangle$. Therefore $\mathrm{Ann}(M_i) = \langle p_i^{e_i} \rangle$

By Bezout's Thm. $r_1\beta_1 + \cdots + r_k\beta_k = 1$, $m = (r_1\beta_1 + \cdots + r_k\beta_k)m \in M_1 + \cdots + M_k$

Therefore $M = M_1 + \cdots + M_k$

if $m_1 + \cdots + m_k = 0$, then $\beta_i(m_1 + \cdots + m_k) = \beta_i m_i = 0$

Suppose $\mathrm{Ann}(m_i) = \langle u \rangle$, then $\beta_i \in \langle u \rangle$

Also, $p_i^{e_i} m_i = 0$, so $p_i^{e_i} \in \langle u \rangle$, then $u \in U$, $\langle u \rangle = R$

Hence $\mathrm{Ann}(m_i) = R$, this implies that $m_i = 0$

So $M = M_1 \oplus \cdots \oplus M_k$

Thm. Let M be a finitely generated primary module over a PID R, with $\mathrm{Ann}(M)=\langle p^e\rangle$ where p is prime

Then $M=\langle\langle v_1\rangle\rangle\oplus\cdots\oplus\langle\langle v_\ell\rangle\rangle$, where $\langle\langle v_i\rangle\rangle\cong R/\langle p^{e_i}\rangle$ for $e=e_1\geq e_2\geq\cdots\geq e_\ell$

proof: ① Since $\mathrm{Ann}(M)=\langle p^e\rangle$, $\exists\, v\in M$ s.t. $\mathrm{Ann}(v)=\langle p^e\rangle$

② Clearly $R/\langle p^e\rangle\cong\langle\langle v\rangle\rangle\leq M$, if $\langle\langle v\rangle\rangle=M$, then it's done

Otherwise, $\exists\, w\in M\setminus\langle\langle v\rangle\rangle$, set $S_1=\langle\langle w\rangle\rangle$, $M_1=S_1\oplus\langle\langle v\rangle\rangle$

Suppose we've construct such direct sum for $1\leq n\leq k$

Claim. $\exists\,\alpha\in R$ s.t. $\forall\, u\in M\setminus M_k$, $S_{k+1}:=\langle\langle S_k, u-\alpha v\rangle\rangle\supsetneq S_k$

Consider $I=\{i\in R\mid iu\in M_k\}$, clearly $I\lhd R$, also $p^e\in I$

so $I=\langle p^f\rangle$ for some $f\leq e$

$p^f u=dv+s_k'\in M_k=\langle\langle v\rangle\rangle\oplus S_k$, $p^e u=0=p^{e-f}dv+p^{e-f}s_k'$

Then $p^{e-f}dv=0$ & $p^{e-f}s_k'=0$, $p^e\mid p^{e-f}d$, so $p^f\mid d$, i.e. $d=\alpha p^f$

$p^f u=p^f\alpha v+s_k'$, so (†) $p^f(u-\alpha v)\in S_k$

Claim. $\langle\langle v\rangle\rangle\cap\langle\langle S_k, u-\alpha v\rangle\rangle=\{0\}$

Suppose $x\in\langle\langle v\rangle\rangle\cap\langle\langle S_k, u-\alpha v\rangle\rangle$, i.e. $x=rv=s_k+b(u-\alpha v)$

then $bu=(r+b\alpha)v-s_k\in\langle\langle v\rangle\rangle\oplus S_k=M_k$

Therefore $b\in\langle p^f\rangle$, $b=\delta p^f$ for some $\delta\in R$

then $x=rv=s_k+(\delta p^f)(u-\alpha v)$, (†) indicates that $x\in\langle\langle v\rangle\rangle\cap S_k=\{0\}$

Hence we have $M_1<M_2<\cdots<M_k<\cdots$ infinitely ascending if $\forall k$, $M_k\neq M$

This is impossible since M is noetherian.

Hence $M=\langle\langle v_1\rangle\rangle\oplus\cdots\oplus\langle\langle v_\ell\rangle\rangle$, $\mathrm{Ann}(v_i)=\langle p^{e_i}\rangle$, $e=e_1\geq e_2\geq\cdots\geq e_\ell$

Thm. Let M, N by finitely generated modules with $\mathrm{Ann}(M)=\langle p^e\rangle$, $\mathrm{Ann}(N)=\langle q^f\rangle$,

Suppose $\begin{cases} M=M_1\oplus\cdots\oplus M_k, & M_i\cong R/\langle p^{e_i}\rangle \\ N=N_1\oplus\cdots\oplus N_\ell, & N_j\cong R/\langle q^{f_j}\rangle \end{cases}$ with $\begin{cases} e=e_1\geq\cdots\geq e_k \\ f=f_1\geq\cdots\geq f_\ell \end{cases}$

Then $M\cong N\iff p=q$, $k=\ell$, $e_i=f_i$

proof: ($\Leftarrow$) trivial

($\Rightarrow$) For any module M, $\forall\, r\in R$, let $M^{(r)}:=\{m\mid rm=0\}$

Then $M^{(r)}\leq M$, $M^{(r)}=M_1^{(r)}\oplus\cdots\oplus M_k^{(r)}$

Take $p\in R$, consider $p\in R$, $M^{(p)}=M_1^{(p)}\oplus\cdots\oplus M_k^{(p)}$

Then $M^{(p)}$ is a vector space over $\mathbb{F}=R/\langle p\rangle$ ($\langle p\rangle$ is maximal)

Defined by $(r+\langle p\rangle)\cdot m=r\cdot m$

Therefore $M^{(p)}\cong N^{(p)}$ as $\mathbb{F}$-vector spaces

Here $M_i^{(p)}=\langle\langle v_i\rangle\rangle^{(p)}$, $\phi:\langle\langle v_i\rangle\rangle\xrightarrow{\cong}R/\langle p^{e_i}\rangle$

Then $\exists\, u\in\langle\langle v_i\rangle\rangle$, s.t. $\phi(u)=p^{e_i-1}+\langle p^{e_i}\rangle$, $\phi(pu)=p^{e_i}+\langle p^{e_i}\rangle=0_{R/\langle p^{e_i}\rangle}$

Hence $pu=0$, $u\in\langle\langle v_i\rangle\rangle^{(p)}$, while if $pw=0$ ($w\in\langle\langle v_i\rangle\rangle$), then

$\phi(pu)=p\phi(u)=p(r+\langle p^{e_i}\rangle)=pr+\langle p^{e_i}\rangle$, so $p^{e_i-1}\mid r$.

Therefore $\langle\langle v_i\rangle\rangle^{(p)}=\mathrm{span}_{\mathbb{F}}(u)$

This implies that $k = \dim(M^{(p)}) = \dim(N^{(p)}) = t$

So $M = M_1 \oplus \cdots \oplus M_k$, $N = N_1 \oplus \cdots \oplus N_k$

Obviously, $\mathrm{Ann}(M) = \mathrm{Ann}(N) = \langle p^e \rangle = \langle q^f \rangle$, so $p = q$, $e_1 = f_1$

When $e_1 = f_1 = 1$, clearly it holds

Induction hypothesis, suppose $e_i = f_i$ for all i when $e_1 = f_1 < n$

Then $pM \cong R/\langle p^{n-1} \rangle \oplus R/\langle p^{e_2-1} \rangle \oplus \cdots \oplus R/\langle p^{e_k-1} \rangle$

$pN \cong R/\langle p^{n-1} \rangle \oplus R/\langle p^{f_2-1} \rangle \oplus \cdots \oplus R/\langle p^{f_k-1} \rangle$

Therefore $e_i = f_i$ for all i

Thm. Let M be a finite-generated module over a PID R, then by previous theorem we have $M = M_{free} \oplus M_{tor}$

Then

$$M \cong R^t \oplus \begin{pmatrix} R/\langle p_1^{e_{1,1}} \rangle \oplus \cdots \oplus R/\langle p_1^{e_{1,a_1}} \rangle \\ \oplus \\ \vdots \\ \oplus \\ R/\langle p_k^{e_{k,1}} \rangle \oplus \cdots \oplus R/\langle p^{e_{k,a_k}} \rangle \end{pmatrix}$$

Proof is not complicated, here M_{free} is free and thus has a basis, so $M_{free} \cong R^t$

While since R is a PID, then $\mathrm{Ann}(M_{tor}) = \langle \alpha \rangle$ for some $\alpha \in R$

then

$$M_{tor} \cong R/\langle p_1^{e_{1,1}} \rangle \oplus \cdots \oplus R/\langle p_k^{e_{k,1}} \rangle \cong \begin{pmatrix} R/\langle p_1^{e_{1,1}} \rangle \oplus \cdots \oplus R/\langle p_1^{e_{1,a_1}} \rangle \\ \oplus \\ \vdots \\ \oplus \\ R/\langle p_k^{e_{k,1}} \rangle \oplus \cdots \oplus R/\langle p_k^{e_{k,a_k}} \rangle \end{pmatrix}$$

Thm. Let $(G, +)$ be an Abelian group with $|G| = n < \infty$

then

$$G \cong \begin{pmatrix} \mathbb{Z}_{p_1^{e_{1,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{e_{1,a_1}}} \\ \oplus \\ \vdots \\ \oplus \\ \mathbb{Z}_{p_k^{e_{k,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_{k,a_k}}} \end{pmatrix}, \quad n = \prod_{j=1}^{k} \prod_{i=1}^{a_j} p_j^{e_{j,i}}$$

This is direct from the last theorem

Example. Classify all Abelian groups G with $|G| = 180$

$180 = 2^2 \times 3^2 \times 5$

$\mathbb{Z}_{2^2}$	$\mathbb{Z}_{3^2}$	$\mathbb{Z}_5$
$\mathbb{Z}_2 \ \mathbb{Z}_2$	$\mathbb{Z}_3 \ \mathbb{Z}_3$	

Therefore there are 9 such groups up to isomorphism

Linear Operators over vector spaces.

For a fixed $T \in \mathcal{L}(V)$, consider V as a $\mathbb{F}[x]$-module by
$(x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0) \cdot v := (T^k + a_{k-1}T^{k-1} + \cdots + a_1 T + a_0)(v)$
Note that $\mathbb{F}[x]$ is an Euclidian Domain and hence a PID
Claim. $\mathrm{Ann}(V) = \langle m_T(x) \rangle$, where m_T is the minimal polynomial

In this case, we can apply the classification of finitely generated modules over R.

Thm. (Primary Decomposition) Let $T: V \to V$ with $m_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$
Then $\exists\ V_1, \cdots, V_k \leq V$, s.t.
① $V = V_1 \oplus \cdots \oplus V_k$
② V_i is T-invariant
③ $\mathrm{Ann}(V_i) = \langle p_i(x)^{e_i} \rangle$, i.e. $V_i = \ker(p_i(T)^{e_i})$
proof: ①, ③ are direct from Primary Decomposition of modules
② $V_i \leq V$ as a submodule, clearly $x \cdot v_i \in V_i$

Now consider each V_i

$$V = \begin{pmatrix} V_{1,1} \oplus \cdots \oplus V_{1,a_1} \\ \oplus \\ \vdots \\ \oplus \\ V_{k,1} \oplus \cdots \oplus V_{k,a_k} \end{pmatrix} \cong \begin{pmatrix} \mathbb{F}[x]/\langle p_1^{e_{1,1}}(x) \rangle \oplus \cdots \oplus \mathbb{F}[x]/\langle p_1^{e_{1,a_1}}(x) \rangle \\ \oplus \\ \vdots \\ \oplus \\ \mathbb{F}[x]/\langle p_k^{e_{k,1}}(x) \rangle \oplus \cdots \oplus \mathbb{F}[x]/\langle p_k^{e_{k,a_k}}(x) \rangle \end{pmatrix}$$

Def. For a fixed $T \in \mathcal{L}(V)$, the characteristic polynomial of T is defined as $\chi_T(x) := \prod_{i=1}^{k} \prod_{j=1}^{a_i} p_i^{e_{i,j}}(x)$

Observe that $m_T(x) \mid \chi_T(x)$

Thm. (Cayley-Hamilton Theorem)
Let B be a basis of V, then $\chi_T(x) = \det(xI - T_{BB})$

proof: *Claim.* $\dim(V_{i,j}) = \deg(p_i^{e_{i,j}}(x))$

Suppose $p_i^{e_{i,j}}(x) = x^d + \cdots + a_1 x + a_0 := g(x)$

Then $\mathbb{F}[x]/\langle p_i^{e_{i,j}}(x)\rangle := \{p(x) + \langle g(x)\rangle \mid p(x) \in \mathbb{F}[x]\} = \{r(x) + \langle g(x)\rangle \mid \deg(r(x)) < \deg(g(x))\}$

Therefore $\deg(\chi_T(x)) = \dim(V)$

Let B be any ordered basis of V with $\dim(V) = n$. Then

$\phi: V \longrightarrow \mathbb{F}^n$, the coordinate map is an isomorphism of $\mathbb{F}[x]$-modules

$v \longmapsto [v]_B$

Where $\mathbb{F}^n$ is an $\mathbb{F}[x]$-module defined by $x^m \cdot (b_1, \cdots, b_n)^T := [T_{BB}]^m (b_1 \cdots, b_n)^T$

Hence $\chi_T(x) = \chi_{T_{BB}}(x)$

Define $\varphi : V_{i,j} \xrightarrow{\cong} \mathbb{F}[x]/\langle p_i^{e_{i,j}}\rangle$

then $\exists\, v_1, \cdots, v_{d-1} \in V_{i,j}$ s.t. $\varphi(v_0) = 1 + \langle p_i^{e_{i,j}}\rangle$, $\cdots$, $\varphi(v_{d-1}) = x^{d-1} + \langle p_i^{e_{i,j}}\rangle$

$\varphi(T(v_0)) = \varphi(x \cdot v_0) = x\,\varphi(v_0) = \varphi(v_1)$, so $v_1 = T(v_0)$

Therefore $B_{i,j} = \{v_0, T(v_0), \cdots, T^{d-1}(v_0)\}$ forms a basis of $V_{i,j}$

So $(T|_{V_{i,j}})_{B_{i,j} B_{i,j}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$. By direct computation we have

$\det([T]_{BB} - xI) = \chi_T(x)$, then it's done

Thm. (Jordan Normal Form)
Let $\mathbb{F}$ be an algebraic closed field, V be a finite dimensional vector space over $\mathbb{F}$, $T \in \mathcal{L}(V)$, $\chi_T(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_k)^{e_k}$

Then there exist a basis B s.t.

$$T_{BB} = \begin{pmatrix} J_{1,1} & & & \\ & J_{1,a_1} & & \\ & & J_{k,1} & \\ & & & J_{k,a_k} \end{pmatrix}, \quad \text{where } J_{i,j} = \begin{pmatrix} \alpha_i & 1 & & \\ & \alpha_i & \ddots & \\ & & \alpha_i & 1 \\ & & & \alpha_i \end{pmatrix}$$

proof: $V = (V_{1,1} \oplus \cdots \oplus V_{1,a_1}) \oplus \cdots \oplus (V_{k,1} \oplus \cdots \oplus V_{k,a_k})$

Then we only consider $V_{i,j}$

Let $\varphi : V_{i,j} \xrightarrow{\cong} \mathbb{F}/\langle (x-\alpha_i)^{e_{ij}}\rangle$, then $\exists \{v_{e_{ij}-1}, \cdots, v_1, v_0\}$ s.t.

$\varphi(v_\ell) = (x-\alpha_i)^\ell + \langle (x-\alpha_i)^{e_{ij}}\rangle$

$\varphi(T(v_\ell)) = \varphi(x \cdot v_\ell) = x(x-\alpha_i)^\ell + \langle (x-\alpha_i)^{e_{ij}}\rangle = (x-\alpha_i)^{\ell+1} + \alpha_i (x-\alpha_i)^\ell + \langle (x-\alpha_i)^{e_{ij}}\rangle$

$= \varphi(v_{\ell+1} + \alpha_i v_\ell)$, so $T(v_\ell) = v_{\ell+1} + \alpha_i v_\ell$

Therefore $J_{i,j} = \begin{pmatrix} \alpha_i & 1 & & \\ & \alpha_i & \ddots & \\ & & \alpha_i & 1 \\ & & & \alpha_i \end{pmatrix}$, let $B_{i,j} = \{v_{e_{ij}-1}, \cdots, v_1, v_0\}$ be a basis of $V_{i,j}$

(This is true since $\dim(V_{i,j}) = e_{ij}$)

Hence the proof is done