Last time

- vector space $\leftarrow$ module over a field
  (V/F)

- PSet 9: if $V \leftarrow$ finitely generated $/F$

then $V \underset{\text{isomorphic}}{\simeq} \underbrace{F \times \dots \times F}_{n} = F^{\times n}$ $\leftarrow$ dimension

$n \leftarrow$ for some n

- example of vector space: $\mathbb{C}/\mathbb{R}$, $\mathbb{C} \simeq \mathbb{R}^{\times 2}$

More examples of vector spaces

$+$ ← sum of matrices

$\mathbb{H} / \mathbb{R}$ ← $\cdot$ ← multiplication by (real) number

$$\left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \,\middle|\, a,b,c,d \in \mathbb{R} \right\}$$

Exercise: $\mathbb{H} \overset{\varphi}{\simeq} \mathbb{R}^{\times 4}$

every element can be

written as: $\underline{\underline{a}} \cdot \mathbb{1} + \underline{\underline{b}} \cdot \mathbb{i} + \underline{\underline{c}} \cdot \mathbb{j} + \underline{\underline{d}} \cdot \mathbb{k}$

coordinates on $\mathbb{R}^4$

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbb{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathbb{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbb{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$\mathbb{H}/\mathbb{C}$, $\quad \mathbb{C} \subset \mathbb{H} \Rightarrow \mathbb{C} \curvearrowright \mathbb{H}$

multiplication

$$\mathbb{C} = \{a+bi\} = \begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix}$$

$$\mathbb{H} \simeq \mathbb{C}^{\times 2}$$

generated by $1, j$

In general: if R – ring that <u>contains</u> a field F as a <u>subring</u>

$\Downarrow$

$F \curvearrowright R$ – becomes a vector space over F

$+$ – addition in R

$\cdot$ – multiplication in R $\left(\begin{matrix} a \in F \\ r \in R \end{matrix} \Rightarrow a \cdot r = ar \right)$

Another example

$F[x]/F \;\circ\!\!-\;\; F \subset F[x]$

<u>subring</u> $\left(\begin{array}{c}\text{polynomials} \\ \text{of } \deg = 0\end{array}\right)$

$\Downarrow$

$F \curvearrowright F[x]$

Note: $F[x] \;\circ\!\!-$ <u>NOT</u> finitely generated

only $1, x, x^2, x^3, \ldots \;\circ\!\!-$ generate $F[x]/F$

Modules over $F[x]$

$F[x] \curvearrowright V \Rightarrow$ 1) $F \curvearrowright V$

i.e. $V \leftarrow$ vector space $/F$

$$\begin{array}{ccc} v & \longmapsto & x \cdot v \\ \cap & & \cap \end{array}$$

2) $(x \cdot -) : V \to V$

action of x defines a map

$f : V \to V$

properties of f:

$$x \cdot (v_1 + v_2) = x \cdot v_1 + x \cdot v_2$$

$$\Updownarrow$$

$$f(v_1 + v_2) = f(v_1) + f(v_2)$$

$a \in F$

$$f(av) = x \cdot (av) = (xa) \cdot v = (ax) \cdot v =$$

$= a \cdot (x \cdot v) = a \cdot f(v)$

So: $\begin{cases} f(v_1 + v_2) = f(v_1) + f(v_2) \\ f(av) = a \cdot f(v) \end{cases}$

$f \to$ linear transformation

See:

$F[x]$-module $V \rightsquigarrow (V, f : V \to V)$

vector space

linear transformation

Claim: this is a bijection, i.e., any pair (V, f) as above defines $F[x] \curvearrowright V$

proof: we are given (V, f), want to define astion of $F[x] \curvearrowright V$.

Pick $p(x) \in F[x]$

$\quad = a_0 + a_1 x + \dots + a_n x^n$

Define:

$$(a_0 + a_1 x + \dots + a_n x^n) \cdot v =$$

$$= a_0 v + a_1 f(v) + a_2 f^2(v) + \dots + a_n f^n(v)$$

$$\underbrace{f(f(\dots(f}_{n}(v)\dots)$$

Exercise: this is indeed an action

In other words: $a_0 + a_1 x + \dots + a_n x^n$ acts via the matrix $a_0 \cdot id + a_1 f + \dots + a_n f^n$

Example: $V = \mathbb{R}^{\times 2}$, $f = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

matrix of this linear transform.

$\Downarrow$

$2 + 3x + 4x^2$ acts via the matrix

$2 \cdot \mathrm{id} + 3 \cdot f + 4 \cdot f^2$

$\parallel$

$$2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 4 \cdot \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$$

$$(2 + 3x + 4x^2) \cdot (a, b) = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix} \begin{bmatrix} a \\ b \end{bmatrix} =$$

$$= (2a + 3b, 2b)$$

$(2,1) \longmapsto (7,2)$

$(1,1) \longmapsto (5,2)$

$\vdots$

Example $V = \mathbb{R}^{\times 2}$, $f = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$

$\big((a,b) \mapsto (2a, 3b) \big)$

$$2 + 3f + 4f^2$$

$$\|$$

$$2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} + 4 \cdot \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 24 & 0 \\ 0 & 47 \end{pmatrix}$$

$$\swarrow$$

$$(2 + 3x + 4x^2) \cdot (a,b) = (24a, 27b)$$

We see that the same vector space can have many different $F[x]$-module structures

$F[x]$-submodules of V ?

$$\left\{ \underset{F[x]\text{-submodule}}{W \subset V} \right\} \overset{\text{claim}}{\longleftrightarrow} \left\{ \begin{array}{c} W \overset{\text{vector subspace}}{\subset} V \\ f(W) \subset W \end{array} \right\}$$

i.e., W is an f-invariant vector subspace

proof (of the claim)

If $W \subset V$ $F[x]$-submodule then W is stable under the action of $F[x]$.

In particular: 1) it's F stable $\Rightarrow$
$\Rightarrow W$ a vector subspace

2) its x-stable (i.e. $x \cdot W \subset W$)

So indeed $f(W) \subset W$ (as $(X \cdot -) = f$)

In the opposite direction: if

$f(W) \subset W$ then $X \cdot W \overset{(*)}{\subset} W$

by the very definition

$(*) \Rightarrow (a_0 + a_1 X + \dots + a_n X^n) \cdot W \subset W$

indeed: $X^k \cdot W =$

$= \underbrace{f(f \dots (f}_{k}(W) \dots) \subset W$

<u>Example:</u> $f = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$; $(a,b) \mapsto (b,0)$

$\Rightarrow \{(a,0) \mid a \in \mathbb{R}\} \subset \mathbb{R}^2$

a submodule

<u>Exercise:</u> in this case only submodules of $\mathbb{R}^2$ are: $\{0\}$, $\underset{\substack{\text{is} \\ \mathbb{R}}}{\{(a,0) \mid a \in \mathbb{R}\}}$, $\mathbb{R}^2$

Another example: $f = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$; $(a,b) \xmapsto{f} (2a, 3b)$

See that: $\{(a,0) \mid a \in \mathbb{R}\}$, $\{(0,b) \mid b \in \mathbb{R}\}$

$\mathbb{R}$ ↘ ↗ $\mathbb{R}$

are submodules

Next time (Lecture 24):

<u>One more example:</u> action by multiplication

$R \curvearrowright R_R$ let's assume R ← <u>commutative</u> ring

Submodules: $I \subset R$

1) I ← abelian subgroup under $+$

I ← submodule if

2) $R \cdot I \subset I$

Another name for such $I \leftarrow$ ideals

Examples: $R = F \leftarrow$ field

only submodules are $\{0\}, F$

(if $I \subset F$ s.t. $I \neq \{0\}$)

submodule

$\Downarrow$

$\exists a \in I, a \neq 0 \Rightarrow \underbrace{a^{-1} \cdot a}_{= 1} \in I \Rightarrow \forall b \in F$

$\underbrace{b \cdot 1}_{= b} \in I$

i.e. $F = I$

$R = \mathbb{Z}$, we know that every subgroup of $(\mathbb{Z}, +)$ is $a\mathbb{Z}$ for some a.

Every $a\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

For $a \in R$, we will denote $aR = (a)$

principal ideal

We have just discussed that in $\mathbb{Z}$ every ideal is principal.

Definition R - principal ideal domain (PID)

if 1) R - commutative

2) every $I \subset R$ is (a) for some $a \in R$

3) R - has no zero divisors

Example: $R = \mathbb{Z}$ - PID

$R = F$ - PID

More examples of PIDs:

$R = F[x]$ is $\underline{\underline{\text{PID}}}$

$\underline{\text{proof.}}$ take $\underset{\text{ideal}}{I \subset R}$, assume $I \neq 0$

Let $f \in I$ nonzero of $\underline{\text{minimal}}$ possible degree

We claim that $I = (f)$.

Indeed if $g \in I$, $g \neq 0$ we can divide with remainder: $\underset{I}{g} = \underset{I}{q f} + r \Rightarrow$

$\Rightarrow r \in I$, but if $r \neq 0 \Rightarrow \deg r < \deg f$

contradiction (f has min. degree in I)

$\Leftarrow$

$r = 0 \Rightarrow g = qf \in (f)$

ideals in $\mathbb{C}[x]$ are all $((x-c_1)\dots(x-c_r))$

for some $c_i \in \mathbb{C}$

Some similarity

ideals in $\mathbb{Z}$ are $(p_1 \cdot p_2 \cdots p_r)$

for some prime p_i

<u>Def:</u> $a \in R$ a PID

is <u>irreducible</u> if a

not a unit

can not be written as: $a = bc$

non-unit elements

<u>Example:</u> in $\mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ is irreducible $\iff$ n-prime

in $\mathbb{C}[x]$, $f \in \mathbb{C}[x]$ <u>irred.</u> $\iff$ $f = (x-c) \cdot a$ $(a \neq 0)$

In $\mathbb{R}[x]$ — more irreducible elements:

$f = x^2+1$ — is irreducible

(use that x^2+1 has no roots over $\mathbb{R}$)

In PID, every ideal $I \subset R$ is:

$$I = (f_1^{k_1} \dots f_r^{k_r})$$

some irreducible elements

How ideals appear in ring theory and why irreducible elements are important:

$I \subset R \Rightarrow R/I$ — ring!

ideal

analog of normal subgroup ($R \cdot I \subset I \sim gHg^{-1} \subset H$)

$R/I \leftarrow$ set of cosets of the form $a+I$

$(a+I)+(b+I) = a+b+I$

$(a+I)\cdot(b+I) = ab+I$

Example: $I=(n)\subset\mathbb{Z} \Rightarrow \mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$

with the standard ring structure

Exercise: if $f\in R$ irreducible $\Rightarrow R/(f)$ a field

Ex: $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C} \leftarrow$ field

Ex: $(\mathbb{Z}/2\mathbb{Z})[x]\Big/(x^2+x+1) \leftarrow$ field of 4 elements!

irreducible

(no roots over $\mathbb{Z}/2\mathbb{Z}$)

Recall that for $R = F$ we had

<u>complete</u> classification of finitely generated modules over F
(vector spaces)

It turns out that for R PID one can also classify finitely generated R-modules.

The answer is more complicated!

For $R = F$, every f.g. module is $F^{\times n}$.

Already for $R = \mathbb{Z}$, have $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

as we discussed, every abelian group is a module over $\mathbb{Z}$.

Can not be isomorphic to $\mathbb{Z}^{\times ?}$

Thm: every finitely generated module over PID R is isomorphic to:

$$R^{\times n} \times \left(R/(f_1^{k_1})\right) \times \left(R/(f_2^{k_2})\right) \times \cdots \times \left(R/(f_r^{k_r})\right)$$

for some f_i ← irreducible.

Applications:

discussed

① $\mathbb{Z}$ - modules ⟷ Commutative groups

PID

$f \in \mathbb{Z}$ irreducible $\Leftrightarrow$ $f = p$ ← prime

So, every finitely generated abelian group is isomorphic to:

$$\mathbb{Z}^{\times k} \times (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})$$

Very explicit answer!

F-vector space

linear operator

② $\mathbb{C}[x]$-modules $\longleftrightarrow \{(V, f: V \to V)\}$

PID

$p \in \mathbb{C}[x]$ irreducible $\iff p = (x-c) \cdot a, \ a \neq 0$

any linear operator

Now fix $f: V \to V$

finite dimensional vector space

Thm. above implies:

$$\begin{array}{ccccc} V & \simeq & \mathbb{C}[x]/(x-c_1)^{k_1} & \times \dots \times & \mathbb{C}[x]/(x-c_r)^{k_r} \\ \circlearrowright & & \circlearrowright & & \circlearrowright \\ f & & \cdot x & & \cdot x \end{array}$$

$$\cdot x \curvearrowright \mathbb{C}[x]/(x-c_1)^{k_1}$$

has basis $1, x-c_1, (x-c_1)^2, \dots, (x-c_1)^{k_1-1}$

in this basis $\cdot x$ has matrix:

$$\begin{pmatrix} c_1 & 1 & & \\ & c_1 & 1 & \\ & & \ddots & 1 \\ & & & c_1 \end{pmatrix}$$

We see that there is some basis in V such that the matrix of f in this basis is:

$$\begin{pmatrix}
\begin{array}{|ccc|} \hline c_1 & 1 & \\ & \ddots & 1 \\ & & c_1 \\ \hline \end{array} & 0 & \cdots & 0 \\
0 & \begin{array}{|ccc|} \hline c_2 & 1 & \\ & \ddots & 1 \\ & & c_2 \\ \hline \end{array} & & 0 \\
\vdots & 0 & \ddots & \\
0 & \cdots & & \begin{array}{|ccc|} \hline c_r & 1 & \\ & \ddots & 1 \\ & & c_r \\ \hline \end{array}
\end{pmatrix}$$

this is precisely a thm. about existence Jordan normal form (JNF) of a linear transformation over $\mathbb{C}$

just discussed how to prove this thm. <u>using</u> ring theory

(note that thm. itself knows nothing about rings!)