Lecture 22

$(R \curvearrowright M)$

Last time: R – ring, M – module over R:

M – set together with two operations:

(1) $+ : M \times M \to M$

(2) $\cdot : R \times M \to M$ – action s.t.

1) $(M, +)$ – $\underset{(= \text{abelian})}{\text{commutative}}$ group

2) $1 \cdot m = m$ – "action of 1 is trivial"

multiplication in R

$(r \cdot s) \cdot m = r \cdot (s \cdot m)$, $\forall r, s \in R$, $m \in M$

3) $(r+s) \cdot m = r \cdot m + s \cdot m$

$r \cdot (m+n) = r \cdot m + r \cdot n$

"distributive law"

Definition: $N \subset M$ – submodule if closed under $+$ and $\cdot$

Comment: definition of module is quite natural:

Claim: $R = M$ with an action:

$$r \cdot m = \underset{\text{multiplication in } R}{rm} \quad (r \in R,\ m \in M = R)$$

is an example of R-module.

See they are completely parallel and $\boxed{\text{coincide}}$ for $M = R$ as above

module axioms

ring axioms

$(M, +)$ ← abelian group $\Leftrightarrow$ $(R, +)$ ← abelian group

$1 \cdot m = m$

$(r \cdot s) \cdot m = r \cdot (s \cdot m)$ $\Leftrightarrow$ $(R, \cdot)$ ← monoid

$(r + s) \cdot m = r \cdot m + s \cdot m$

$r \cdot (m + n) = r \cdot m + r \cdot n$ $\Leftrightarrow$ $(a+b) \cdot c = a \cdot c + b \cdot c$

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

Examples of modules

① $R = \mathbb{Z}$

Thm.

quite surprising!

$$\{\mathbb{Z}\text{-modules}\} = \{\text{commutative groups}\}$$

proof.

Start with abelian group $(S, +)$, want to define $\mathbb{Z}$-module structure on it.

(i.e. $M = S$)

Need to define: $+ : S \times S \to S$ already have ✓

$\cdot\ \mathbb{Z} \times S \to S$

in other words, need to define:

$$n \cdot s \in S$$

$n \in \mathbb{Z}$ $\qquad$ $s \in S$

1) $n > 0 \Rightarrow n = \underbrace{1 + 1 + \dots + 1}_{n}$ so

$$n \cdot s = (\underbrace{1 + 1 + \dots + 1}_{n}) \cdot s = (1 \cdot s) + \dots + (1 \cdot s) =$$

$$= \underbrace{s + s + \dots + s}_{n}$$

that's the definition of $n \cdot s$

2) $n = 0 \Rightarrow 0 \cdot s = 0$

3) $n < 0 \Rightarrow n \cdot s = \underbrace{(-s) + \dots + (-s)}_{-n}$

<u>Exercise:</u> S with an action of $\mathbb{Z}$ as above indeed becomes a $\mathbb{Z}$-module.

For example associativity:

$$a \cdot (b \cdot s) \stackrel{?}{=} (ab) \cdot s \,, \quad \forall a, b \in \mathbb{Z},\ s \in S$$

if $a, b > 0 \Rightarrow b \cdot s = \underbrace{s + \dots + s}_{b}$

$$a \cdot (b \cdot s) = \underbrace{\underbrace{s + \dots + s}_{b} + \dots + \underbrace{s + \dots + s}_{b}}_{a} =$$

$$= \underbrace{s + s + \dots + s}_{ab} = (ab) \cdot s \quad \checkmark$$

We just discussed that if $(S,+)$ – abelian group

then $\exists!$ $\mathbb{Z}$-module structure on S

(extending $(S,+)$)

In the opposite direction:

if $(M,+,\cdot)$ – $\mathbb{Z}$-module, then

it defines abelian group $(M,+)$ ✓

So, indeed:

$$\{\mathbb{Z}\text{-modules}\} = \{\text{abelian groups}\}$$

Example: $\mathbb{Z} \curvearrowright \mathbb{Z}/4\mathbb{Z}$

$2\cdot 3 = 2 \qquad 5\cdot 3 = 1$

$2\cdot 2 = 0 \qquad 5\cdot 2 = 2$

If S ← abelian group, then

$$\left\{\begin{array}{c}\text{submodules}\\ \text{of } S\end{array}\right\} = \left\{\begin{array}{c}\text{subgroups}\\ \text{of } S\end{array}\right\}$$

② $R = F$ ← field

(or, more generally, <u>division ring</u>)

F-module V <=> vector space over F

can treat this as a <u>definition</u> of a vector space

(will denote $V/_F$)

vector space <u>over</u>

Example: $V = \mathbb{C}/\mathbb{R}$, $a, b \in \mathbb{C}$, $\underbrace{a+b}_{\text{ordinary addition}}$

$r \in \mathbb{R}$, $a \in \mathbb{C}$: $\underbrace{r \cdot a = ra}_{\text{ordinary multiplication}}$

Alternatively: every element of $\mathbb{C}$ is $x+iy$, $x, y \in \mathbb{R}$

i.e. $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ — vector space over $\mathbb{R}$

$x+iy \mapsto (x, y)$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$r \cdot (x, y) = (rx, ry)$$

Same formulas work for arbitrary field F to define the action $F \curvearrowright \underbrace{F \times \dots \times F}_{n}$ $(n \in \mathbb{Z}_{>0})$

Exercise (see PSet 9): every finitely generated F-module (vector space) is isomorphic to $F^{\times n}$ for some n.

Finitely generated $\Leftarrow$ V/F is finitely generated if $\exists\, v_1, \dots, v_n \in V$ such that

finite set

$\forall v \in V, \exists\, a_1, \dots, a_n \in F$ such that:

$$v = a_1 v_1 + \dots + a_n v_n$$

Two vector spaces V, V' are isomorphic

if $\exists\, \varphi : V \xrightarrow{\sim} V'$ s.t.

bijective

$$\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \quad \forall v_1, v_2 \in V$$

$$\varphi(a \cdot v) = a \cdot \varphi(v) \quad \forall a \in F$$

More examples of vector spaces

$\mathbb{H}/\mathbb{R}$ $\longleftarrow$ $+$ $\leftarrow$ sum of matrices

$\cdot$ $\leftarrow$ multiplication by number

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

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

every element can be written as:

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

coordinates on $\mathbb{R}^4$

(see PSet 8)

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

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

multiplication

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

ring

In general: if R <u>contains</u> field

F as a <u>subring</u>

$\Downarrow$

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

$+$ ← addition in R

$\cdot$ ← multiplication in R:

$a \in F$, $r \in R$ ← $a \cdot r = ar \in R$

Another example:

$F[x]/F$

$F \subset F[x]$

subring (polynomials of deg $= 0$)

$\Downarrow$

indeed $F \curvearrowright F[x]$

Note: $F[x]$ NOT finitely generated

only $1, x, x^2, x^3, \dots$ generate $F[x]$ over F

G a monoid, F a field, then

modules over FG $\Leftrightarrow$ <u>representations</u> of G over F

(vector space V over F + action of G on it)

<u>Example:</u> modules over $\underline{\underline{F[X]}}$

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

i.e. V - <u>vector space</u>$/F$

$$v \mapsto X\cdot v$$

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:

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

f o linear transformation

See:

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

vector space

linear transformation

Claim: pair (V, f) as above always defines $F[x] \curvearrowright V$

next time