Math 122 – Lecture 22 Notes

1 Last Time

Recall that R is a ring and M is a module over R, where R acts on M. M is a set together with two operations:
1) $+ : M \times M \to M$ and
2) $\cdot : R \times M \to M$ is the action such that $(M, +)$ is an abelian group, and $1 \cdot m = m$, the action of 1 is trivial. $(r \cdot s) \cdot m = r \cdot (s \cdot m)$, for all $r, s \in R$ and $m \in M$. Also $(r + s) \cdot m = r \cdot m + s \cdot m$ and $r \cdot (m + n) = r \cdot m + r \cdot n$ is the distributive law.

Definition: $N \subset M$ is a submodule if it is closed under $+$ and $\cdot$.
Comment: Definition of module is quite natural.

Claim: $R = M$ with an action;

$$r \cdot m = rm; (r \in R, m \in M = R)$$

is multiplication in R. This is an example of R-module.
We have that $(M, +)$ (module axioms) is an abelian group $\iff$ $(R, +)$ (ring axioms) is an abelian group. See they are completely parallel and coincide for $M = R$ as above.

$1 \cdot m = m, (r \cdot s) \cdot m = r \cdot (s \cdot m) \iff (R, \cdot)$ is a module.

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

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

2 Examples of Modules

2.1 $R = \mathbb{Z}$.

Theorem:

$$\{\mathbb{Z} - \text{modules}\} = \{\text{Commutative Groups}\}$$

Proof: Start with abelian group $(S, +)$, want to define $\mathbb{Z}$-module structure on it $M = S$. Need to define $+ : S \times S \to S$ (which we already have) as well as $\cdot : \mathbb{Z} \times S \to S$. In other words, need to define;

$$n \cdot s \in S$$

where $n \in \mathbb{Z}$ and $s \in S$.
1. $n > 0 \implies n = \underbrace{1 + 1 + \cdot + 1}_{n}$ s;

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

Which is exactly the definition of $n \cdot s$.
2. $n = 0 \implies 0 \cdot s = 0$
3. $n < 0 \implies n \cdot s = \underbrace{(-s) + (-s) + \cdot + (-s)}_{n}$

Exercise: S with an action of $\mathbb{Z}$ as above indeed becomes a $\mathbb{Z}$-module.
For example, associativity;

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

If $a, b > 0 \implies b \cdot s = \underbrace{s + \cdots + s}_{b}$. This implies that;

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

We just discussed that if $(S, +)$ is an abelian group, then $\exists ! \mathbb{Z}$-module structure on S (extending $(S, +)$). In the opposite direction:
if $(M, +, \cdot)$ is a $\mathbb{Z}$-module, then it defines abelian group $(M, +)$.
So indeed:

$$\{\mathbb{Z} - \text{modules}\} = \{\text{Abelian Groups}\}$$

For example, consider the action of $\mathbb{Z}$ on $\mathbb{Z}/4\mathbb{Z}$, with $2 \cdot 3 = 2, 2 \cdot 2 = 0, 5 \cdot 3 = 1, 5 \cdot 2 = 2$.

If S is an abelian group, then;

$$\{\text{Submodules of } S\} = \{\text{Subgroups of } S\}$$

2.2 $R = \mathbb{F}$, a field (or more generally a Division Ring)

$\mathbb{F}$-module $V \iff$ vector space over $\mathbb{F}$. We can treat this as a definition of a vector space (will denote $V/\mathbb{F}$ as vector space over field).

For example, consider $V = \mathbb{C}/\mathbb{R}$, where $a, b \in \mathbb{C}$ have ordinary addition $a+b$ and for $r \in \mathbb{R}$, $r \cdot a = ra$ is ordinary multiplication. Alternatively, every element of $\mathbb{C}$ is $x + iy$ where $x, y \in \mathbb{R}$'

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

is a vector space over $\mathbb{R}$, and we can write $x+iy \to (x, y)$, where we have $(x_1, y_1)+(x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and $r \cdot (x, y) = (rx, ry)$. Same formula work for arbitrary field $\mathbb{F}$ to define the action $\mathbb{F}$ on $\underbrace{\mathbb{F} \times \cdots \times \mathbb{F}}_{n}$ for $n \in \mathbb{Z}_{>0}$.

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

$V/\mathbb{F}$ is finitely generated if $\exists v_1, \cdots v_n \in V$ a finite set such that $\forall v \in V, \exists a_1, \cdots a_n \in \mathbb{F}$ such that;

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

Two vector spaces V, V' are isomorphic if $\exists \varphi : V \xrightarrow{\sim} V$ is bijective such that;

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

$$\varphi(a \cdot v) = a \cdot \varphi(v) \forall a \in \mathbb{F}$$

More examples of vector spaces:

$\mathbb{H}/\mathbb{R}$ with $+$ being a sum of matrices and $\cdot$ being multiplication by a number, where;

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

Exercise: $\mathbb{H} \cong \mathbb{R}^4$; every element can be written as;

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

coordinates in $\mathbb{R}^4$ where (from pset 8);

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

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

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

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

Now consider $\mathbb{H}/\mathbb{C}, \mathbb{C} \subset \mathbb{H} \implies \mathbb{C}$ acts on $\mathbb{H}$ by multiplication, where an element $\{a+bi\} \in \mathbb{C}$ is given by the matrix $\begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix}$
In general, if R is a ring that contains a field $\mathbb{F}$ as a subring, then $\mathbb{F}$ acting on R becomes a vector space with $+$ being addition in R and $\cdot$ being multiplication in R, where for $a \in \mathbb{F}, r \in R$ we have;

$$a \cdot r = ar \in R$$

Another example: Consider $\mathbb{F}[x]/\mathbb{F}$.
$\mathbb{F} \subset \mathbb{F}[x]$ is a subring (polynomials of deg $= 0$. Indeed, $\mathbb{F}$ acts on $\mathbb{F}[x]$. Note that $\mathbb{F}[x]$ is NOT finitely generated. Only $1, x, x^2, x^3, \cdots$ generate $\mathbb{F}[x]$ over $\mathbb{F}$.

If G is a monoid and $\mathbb{F}$ is a field, then modules over $\mathbb{F}G \iff$ representations of G over $\mathbb{F}$. (vector space V over $\mathbb{F}$ plus action of G on it).

Example: Modules over $\mathbb{F}[x]$.
$\mathbb{F}[x]$ acting on V implies 1) $\mathbb{F}$ acts on V ($V-$ vector space $\mathbb{F}$).
2) $(X, \cdot) : V \to V$ by $v \to xv$, the action of X defines a map $f : V \to V$.
Properties of f:

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

For $a \in \mathbb{F}$, we have;

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

So we see that f is a linear transformation;

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

See: $\mathbb{F}[x]$-module V, we have $(V, f : V \to V)$ where V is a vector space and f is a linear transformation.

Claim: Pair (V, f) as above always defines $\mathbb{F}[x]$ acting on V (will do this next time).