Lecture 07: Module theory

Tuesday, January 23, 2018 11:56 PM

One of the best ways to understand rings is via their "actions". (as it was indicated in the case of groups.) In the case of rings, however, we are more or less forced to stick to "linear actions":

<u>Def.</u> Suppose R is a unital ring. Then M is called a (left) R-module if

① $(M,+)$ is an abelian group.

② There is a scalar multiplication: $R\times M\to M$,

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

that satisfies the following properties:

(2-a) $r_1\cdot(r_2\cdot m)=(r_1 r_2)\cdot m$

(2-b) $r\cdot\underbrace{(m_1+m_2)}_{\text{in } M}=r\cdot m_1+r\cdot m_2$

(2-c) $\underbrace{(r_1+r_2)}_{\text{in } R}\cdot m=r_1\cdot m+r_2\cdot m$

(2-d) $1\cdot m=m$

A few examples and remarks:

1. One can similarly define a right R-module. When R is

commutative, any left R-mod is a right R-mod, and vice versa. But for an arbitrary unital ring R:

($\dagger$) M is a left R-mod $\Leftrightarrow$ M is a right R^{op}-mod

where R^{op} as an abelian group is the same as R, and $x * y := yx$. One can check that $(R^{op}, +, *)$ is a ring; it is called the opposite of R. Clearly $R = R^{op}$ if R is commutative.

Going back to ($\dagger$): $m \bullet r := r \cdot m$.

$$\Rightarrow \quad (m \bullet r_1) \bullet r_2 = r_2 \cdot (m \bullet r_1) = r_2 \cdot (r_1 \cdot m)$$

$$= (r_2 r_1) \cdot m = (r_1 * r_2) \cdot m$$

$$= m \bullet (r_1 * r_2)$$

The rest of properties clearly hold.

2. If $R = F$ is a field, then M is an F-mod means M is an F-vector space. So modules are generalizations of vector spaces.

Lecture 07: Module theory

Wednesday, January 24, 2018 5:45 AM

3. Suppose R is a unital ring and I is a left ideal of R (that means $\forall r \in R, x \in I$, $r.x \in I$, but $x.r$ is not necessarily in R.) Then R/I is a left R-mod:

$\forall\ r \in R$ and $r' + I \in R/I$, $\quad r \cdot (r' + I) := rr' + I$.

well-defined. $r_1' + I = r_2' + I \Rightarrow r_1' - r_2' \in I$

$$\Rightarrow r(r_1' - r_2') \in I \Rightarrow rr_1' + I = rr_2' + I \quad \checkmark$$

Properties can be easily checked.

4. Suppose R is a unital ring. Then R^n is a left $M_n(R)$-mod. We view R^n as the set of $n \times 1$ column matrixes. And let

$\forall\ a \in M_n(R),\ v \in R^n,\quad a \cdot v =$ matrix multiplication.

5. In groups we saw that, if $H \curvearrowright X$ and $\phi: G \to H$ is a group homomorphism, then we get an induced G-action: $g \cdot x := \phi(g) \cdot x$. We have a similar property for rings and modules.

Lecture 07: Module theory

Wednesday, January 24, 2018 5:58 AM

Suppose M is an S-module, and $\phi: R \to S$ is a ring homomorphism. Then M can be viewed as an R-mod.:

$$r \bullet m := \phi(r) \cdot m.$$

In particular: • If $S \subseteq R$ is a ring extension, then any R-mod can be viewed as a S-mod.

• If $I \triangleleft R$, then any (R/I)-mod can be viewed as an R-mod.

6. (This is a particular case of the previous example which is extremely useful.)

Suppose A is a unital commutative ring, and $T \in M_n(A)$. Then we get a ring homomorphism

$$\underbrace{A[x]}_{\text{ring of polynomials}} \to \underbrace{A[T]}_{\substack{\text{subring of } M_n(A) \\ \text{which is gen. by } A \,\&\, T}} := \{\sum_{i=0}^{m} c_i T^i \mid c_i \in A\}, \quad \sum_{i=0}^{m} c_i x^i \longmapsto \sum_{i=0}^{m} c_i T^i.$$

• A^n is a $M_n(A)$-mod $\Rightarrow$ A^n can be viewed as an $A[T]$-mod

$\Rightarrow$ A^n can be viewed as an $A[x]$-mod.:

$$\left(\sum_{i=0}^{m} c_i x^i\right) \cdot v := \sum_{i=0}^{m} c_i T^i v.$$

Lecture 07: Module theory

Wednesday, January 24, 2018 6:10 AM

As always we should and will define "substructures", "homomorphisms", and try to prove isomorphism theorems.

Def.. (Submodule) Suppose M is a left R-module. We say N is a submodule of M if

① N is a subgroup of $(M,+)$

② $\forall r\in R, n\in N$, $r\cdot n\in N$.

(R-mod. homomorphism) Suppose M_1 and M_2 are R-mod. Then $\phi: M_1\to M_2$ is called an R-mod homomorphism if

- ϕ is an abelian gp homomorphism.
- $\forall r\in R, m_1\in M_1$, $\phi(r\cdot m_1) = r\cdot\phi(m_1)$.

(Image and kernel) Suppose $\phi: M_1\to M_2$ is an R-mod. homomorphism. Then

- Image of ϕ: $\mathrm{Im}(\phi) := \{\phi(m_1) \mid m_1\in M_1\}$
- kernel of ϕ: $\ker(\phi) := \{m_1\in M_1 \mid \phi(m_1)=0\}$.

Lecture 07: Image, kernel, quotient for modules

Wednesday, January 24, 2018 6:22 AM

<u>Proposition</u>. Suppose $\phi: M \to N$ is an R-mod homomorphism.

Then (a) $\mathrm{Im}(\phi)$ is a submod. of N.

(b) $\ker(\phi)$ is a submod. of M.

<u>Pf.</u> Since ϕ is an additive gp homomorphism, $\mathrm{Im}(\phi)$ and $\ker(\phi)$ are subgps. So it is enough to check that they are invariant under scalar multiplication.

- $r\cdot\phi(m) = \phi(r\cdot m) \in \mathrm{Im}\,\phi$
- $\phi(m) = 0 \Rightarrow \phi(r\cdot m) = r\cdot\phi(m) = r\cdot 0 \overset{(?)}{=} 0$

$\boxed{r\cdot 0 = r\cdot(0+0) = r\cdot 0 + r\cdot 0 \Rightarrow r\cdot 0 = 0}$ ∎

<u>Proposition</u>. Suppose M is an R-mod. and $N \subseteq M$ is a submod.

Then $r\cdot(m+N) := rm + N$ is well-defined and makes M/N into an R-module.

<u>Pf.</u> We just show it is well-defined. It is easy to check module properties: $m_1+N = m_2+N \Rightarrow m_1-m_2 \in N \Rightarrow r\cdot(m_1-m_2)\in N$
$\Rightarrow r\cdot m_1 - r\cdot m_2 \in N \Rightarrow r\cdot m_1 + N = r\cdot m_2 + N$. ∎

Lecture 07: The 1st isomorphism theorem for mod

Wednesday, January 24, 2018 6:34 AM

__Def.__ Suppose M and N are R-mod. and $\phi: M \to N$ is an R-mod. Then ϕ is called an __isomorphism__ if $\exists \psi: N \to M$ which is an R-mod homomorphism and

$$\phi \circ \psi = id_N \quad \text{and} \quad \psi \circ \phi = id_M .$$

__Theorem.__ (The fundamental isomorphism theorem)

Suppose $\phi: M \to N$ is an R-mod. homomorphism. Then

$$\overline{\phi}: M/\ker\phi \longrightarrow \operatorname{Im}\phi, \quad \overline{\phi}(m+\ker\phi) := \phi(m)$$

is an R-mod. isomorphism.

__Pf.__ From group theory we know $\overline{\phi}$ is a well-defined abelian group isomorphism.

(__R-mod__) $\overline{\phi}(r\cdot(m+\ker\phi)) = \overline{\phi}(rm+\ker\phi)$

$$= \phi(rm) = r\,\phi(m) = r\,\overline{\phi}(m+\ker\phi).$$

Since $\overline{\phi}$ is an abelian group isomorphism,

$$\psi: \operatorname{Im}\phi \longrightarrow M/\ker\phi, \quad \psi(\phi(m)) := m+\ker\phi$$

is a well-defined abelian group homomorphism. Next we check

Lecture 07: The 1st isomorphism theorem for mod

Wednesday, January 24, 2018 6:45 AM

that ψ is an R-mod homomorphism:

$$\psi(r\,\phi(m)) = \psi(\phi(rm)) = rm + \ker\phi$$

$$= r\,(m+\ker\phi) = r\,\psi(\phi(m)).$$

And, since $\psi \circ \overline{\Phi} = \mathrm{id}_{M/\ker\phi}$ and $\overline{\Phi}\circ\psi = \mathrm{id}_{\mathrm{Im}\,\phi}$, we deduce that $\overline{\Phi}$ is an R-mod. isomorphism. ■

<u>Cor.</u> A bijective R-mod. homomorphism is an R-mod. isomorphism.

<u>Remark.</u> As before $\phi: M \to N$ is injective if and only if $\ker(\phi) = 0$.