Comm & Hom

September 18, 2023

Contents

1 Intro

Theorem 1.0.1. *radical ideal is generated by a polynomial f with no multiple roots.*

Suppose $J \subset \mathbb{C}[x_1, \dots, x_n]$ is an ideal. Then $I(Z(J)) = rad(J) = \{f \mid f^n \subset J\}$

Definition 1.0.2. radical ideal is generated by a polynomial f with no multiple roots. cokernel: take the image of f and mod out by image of f.

1.1 Modules

Let R be a commutative ring. An R-module M is an abelian group $(+)$ with a map $R \times M \to M$ written $(r, m) \mapsto rm$. Satisfying

1. associativity: $r(sm) = (rs)m$ for all $r, s \in R, m \in M$.
2. distributivity: $r(m + m') = rm + rm'$ and $(r + r')m = rm + r'm$ for all $r, r' \in R, m, m' \in M$.
3. unitality: $1m = m$ for all $m \in M$.

Several things you could derive from the definition: $0m = 0, (-1)m = -m$, etc.

Example 1.1.1. *Let $R = k[x]$. A $k[x]$-module is*

- *a k-vector space M*
- *with a map $xM \to M$, where $m \mapsto xm$, a k linear transformation.*

Example 1.1.2. *What is an R-submodule of R? It's*

1. *$J \subseteq R$;*

2. *closed under addition, 0, negatives;*

3. *for any $r \in R, j \in J, r, j \in J$.*

an ideal.

Definition 1.1.3. Let M be an R-module, N a sbugroup of M. N is a *submodule* if for any $n \in N$ and $r \in R$, the product rn is in N.

Definition 1.1.4. If M is an R-module, we shall write $\operatorname{ann} M$ for the annihilator of M; that is,

$$\operatorname{ann} M = \{r \in R \mid rM = 0\},$$

which is an ideal.

Definition 1.1.5. Let $I \subseteq R$ an ideal, M an R-module. We denote

$$IM = \left\{ \sum a_i m_i \mid a_i \in I, m_i \in M \right\} \subseteq M$$

the smallest R-submodule of M containing all elements of the form am, where $a \in I, m \in M$.

Example 1.1.6. *Suppose M is an R-module. FOr $N, N' \subseteq M$ submodules,*

$$[N : N'] \subseteq R \quad x \in [N : N'] \iff xN' \subseteq N.$$

For N a submodule, I an ideal

$$[N : I] \subseteq M. \quad y \in [N : I] \iff Iy \subseteq N.$$

The point of having the above is to generalize the annihilator.

Example 1.1.7. *ann $M = [O : M]$.*

Some operations we could do. Given a sequence of modules $M_1, M_2, \ldots$.

Definition 1.1.8. We denote

$$\prod_{i \in I} M_i = \{(m_1, m_2, \ldots) \mid m_i \in M_i\}.$$

$\prod M_i$ is an R-module with componentwise addition and scalar multiplication.

Note that $\oplus M_i \subseteq \prod M_i$, a sub-$R$-module.

Also, $\oplus M_i = \{(m_i)_{i \in I} \mid$ only finitely many m_i are zero $\}$

Suppose we have an R-module homomorphism

$$f : M \to N.$$

We could construct 3 modules: $ker(f) \subseteq M, Im(f) \subseteq N, coker(f) = N/Im(f)$

Definition 1.1.9. Suppose we have R-module homomorphism

$$f : m \to N \quad g : N \to P.$$

This is exact if $\operatorname{Im} f = \ker g$.

Definition 1.1.10. If we have a sequence of maps

$$\cdots \to M_1 \to M_2 \to M_3 \to \cdots .$$

then we say it's exact iff each 2-term sequence is exact.

Saying $0 \to M \to N$ is exact is saying f is injective. And $M \to N \to 0$ is exact is saying f is surjective.

Definition 1.1.11. A short exact sequence is an exact sequence

$$0 \to M \to N \to P \to 0 \quad f : M \to N, g : N \to P.$$

This tells us that

1. M iso to $Im(f)$
2. P iso to $N/ker(g)$
3. $ker(g) = Im(f)$, P iso $coker(f)$

Definition 1.1.12. A free R-module is an R-module isomorphic to $\oplus_{i\in I} R$. In particular, R^n are the finitely generated free modules.

Definition 1.1.13. A module M is finitely generated if there exists $m_1, \ldots, m_n \in M$ such that every element of M is of the form $\sum_{i=1}^{n} a_i m_i$ for some $a_i \in R$.

Definition 1.1.14. A module M if finitely presented if there exists an exact sequence

$$R^n \to R^m \to M \to 0.$$

1.2 Localization

Suppose R is a ring, $U \subseteq R$ is a subset thatis closed under multiplication, and contains the unit $1 \in R$.

Definition 1.2.1. We can form the localization $R[U^{-1}]$, whose elements are

$$\{(r, s) \mid r \in R, s \in U\}.$$

We also put an equivalence relation on the elements.

$$(r, s) \equiv (r', s') \iff \exists u, v \in U, (ur, us) = (vr', vs').$$

Note that the equivalence relation is different from cross-multication as what we do in fractions.

Example 1.2.2. *Let $R = \mathbb{Z}, U = \{1, 2, 4, 6, 16, \ldots\}$. Then*

$$R[U^{-1}] = \mathbb{Z}[\frac{1}{2}] = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q = 2^k \right\}.$$

Definition 1.2.3. In $R[U^{-1}]$, we have a ring.

$$\begin{aligned}
(r,s)+(r',s') &= (rs'+r's,ss') \\
(r,s)\cdot(r',s') &= (rr',ss') \\
0 &= (0,1) \\
1 &= (1,1)
\end{aligned}$$

Example 1.2.4. *Let $R=\mathbb{Z}/6, U=\{1,3\}$. Then localization is smaller:*

$$R[U^{-1}]=\mathbb{Z}/2.$$

Example 1.2.5. *Let $R=\mathbb{C}[x], U=\{1,x,x^2,x^3,\ldots\}$. Then*

$$R[U^{-1}]=\mathbb{C}[x,x^{-1}]=\{f(x)/x^n|f(x)\text{ poly },n\in\mathbb{N}\}=\left\{\sum_{n\in\mathbb{Z}}a_nx^n\mid a_n\in\mathbb{C}\right\}.$$

Note that in the summation there should only be finitely many n. The ring is also called Laurent polynomials.

This ring is isomorphic to

$$\mathbb{C}[x,y]/(yx-1).$$

Note that there is always a ring homomorphism

$$\phi:R\to R[U^{-1}]\quad \phi(r)=\frac{r}{1}.$$

Example 1.2.6. $R=\mathbb{C}[x_1,\ldots,x_n], U=R-\{0\}$. *Note U is closed under multiplication because R is an integral domain.*

$$R[U^{-1}]=\{f(\vec{x})/g(\vec{x})\mid f,g\in\mathbb{C}[x_1,\ldots,x_n],g\neq 0\}.$$

Proposition 1.2.7. *The theory of ideals in $R[U^{-1}]$ is closely related to the theory of ideals in R. Given an ideal J in R, we could have $J\cdot R[U^{-1}]$, which is an ideal in $R[U^{-1}]$.*

The map from ideals of $R[U^{-1}]$ to ideals of R is an injection. They are sort of "ideals that don't meet the set U".

An ieal J is of the form $\phi^{-1}(L)$ iff for any a,b s.t. $a\in R,b\in U$, $ab\in J\implies a\in J$.

There is a correspondance between prime ideals of $R[U^{-1}]$ and prime ideals of R that don't contain any elements of U.

Example 1.2.8. *prime ideals of $\mathbb{Q}$; prime ideals of $\mathbb{Z}$ that don't contain any elements of the set $\{1,2,3,4,5,\ldots\}$; $\{(0)\}$.*

Definition 1.2.9. Supose R is a ring. $P\subseteq R$ is a prime ideal. We define R_P to be the localization of the set $U=R-P$.

Note that U is closed under multiplication because P is prime.

Also, R_P has one maximal ideal: PR_P.

There is a correspondance between prime ideals of R_P; prime ideals of R that don't contain any elements of U; prime ideals of R contained in P.

Example 1.2.10.

$$\mathbb{Z}_{(2)} = \left\{ \frac{n}{m} \mid m \text{ odd} \right\}.$$

This has 2 ideals: $(0), (2)$.

Definition 1.2.11. A ring R is *local* if it has a unique maximal ideal.

R_P is always local if P is prime.

If R is a ring, M is an R-module, $U \subseteq R$ is a subset closed under multiplication and 1. We can construct

$$M[U^{-1}] = \left\{ \frac{m}{s} \mid m \in M, s \in U \right\}.$$

$M[U^{-1}]$ is an abelian group and a module on $R[U^{-1}]$.

Example 1.2.12. $R = \mathbb{Z}, U = \{1, 3, 9, 27, \ldots\}, M = \mathbb{Z}/10$. *Check that* $M[U^{-1}] \cong \{0\}$.

1.3 Hom

For R-modules M, N. There is a new R-module $\mathrm{Hom}_R(M, N)$

$$\mathrm{Hom}_R(M, N) \subseteq \{f : M \to N\}.$$

Functions that are

1. group homomorphisms
2. R-linear: $f(rx) = rf(x)$

Definition 1.3.1. $\mathrm{Hom}_R(M, N)$ is an R-module in the following way.

- $f + g : (f + g)(m) = f(m) + g(m)$
- $rf : (rf)(m) = rf(m)$

There are some properties of Hom.

1. $\mathrm{Hom}_R(R, N) \cong N$, where $f \mapsto f(1), n \in N \mapsto f(r) = rn$. Basically the same as picking an element from N.
2. $$\mathrm{Hom}_R\left(\oplus_{i \in I} M_i, N\right) \cong \prod_{i \in I} \mathrm{Hom}_R(M_i, N).$$

   The RHS is choosing for each $i \in I$, a homomorphism $M_i \to N$. There's also

   $$\mathrm{Hom}_R(M, \prod N_i) \cong \prod_{i \in I} \mathrm{Hom}_R(M, N_i).$$

3. If I have R-module homomorphisms

$$\alpha : M \to M' \quad \beta : N \to N'.$$

I get a map

$$\mathrm{Hom}_R(\alpha, \beta) : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N') \quad \text{where} \quad f \mapsto \beta f \alpha.$$

Thi respects identity functions and function composition. Functorial.

4. Exactness. Hom_R is *left-exact*:

   (a) If $M' \to M \to M'' \to 0$ is an exact sequence, then for any N,

   $$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$$

   is also exact.

   (b) If $0 \to N' \to N \to N''$ is exact then

   $$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$$

   is exact.

For R-module M, N there is a tensor product $M \otimes_R N$, which we get by taking all formal sums of symbols $m \otimes n, m \in M, n \in N$, mod out by subgroup generated by elements of the form

- $(m + m') \otimes n - m \otimes n - m' \otimes n$;
- $m \otimes (n + n') - m \otimes n - m \otimes n'$;
- $(rm) \otimes n - m \otimes (rn)$.

Example 1.3.2.

$$R[x_1, \dots, x_n] \otimes_R R[y_1, \dots, y_n] \cong R[x_1, \dots, x_n, y_1, \dots, y_n].$$

Properties of $\otimes_R$.

1. $$R \otimes_R M \cong M \quad \sum r_i \otimes m_i \mapsto \sum r_i m \quad 1 \otimes m < -m.$$

2. $$(\oplus M_i) \otimes_R N \cong \oplus (M_i \otimes_R N).$$

3. Functornality. For R-module homomorphisms $\alpha : M \to M'$, $\beta : N \to N'$, we get an R-module homomorphism

$$\alpha \otimes \beta : M \otimes_R N \to M' \otimes_R N' \quad \sum m_i \otimes n_i \mapsto \sum \alpha(m_i) \otimes \beta(n_i).$$

4. Right exactness. If $M' \to M \to M''$ is exact, then

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0.$$

is exact.

5. Symmetry.

$$M \otimes_R N \cong N \otimes_R M \quad \sum m_i \otimes n_i \mapsto n_i \otimes m_i.$$

Proposition 1.3.3.

$$M[U^{-1}] \cong R[U^{-1}] \otimes_R M.$$

Proof sketch. The procedure we could do is

$$\frac{m}{u} \mapsto \frac{1}{u} \otimes m \quad \frac{rm}{u} \leftarrow\!\shortmid \frac{r}{u} \otimes m.$$

□

Definition 1.3.4. An R-module F is *flat* whenever

$$f : M \to N \quad \text{is injective,}$$

and the map

$$F \otimes_R M \to F \otimes_R N \quad \text{is injective.}$$

Alternatively,

$$0 \to M \to N \text{ exact } \implies 0 \to F \otimes_R M \to F \otimes_R N \text{ exact }.$$

Theorem 1.3.5. *$R[U^{-1}]$ is always a flat module over R.*

Proof. Suppose $f : M \to N$ is injective. We need to check $M[U^{-1}] \to N[U^{-1}]$ is also injective.

Suppose $\frac{m}{u} \in M[U^{-1}]$ which goes to 0 in $N[U^{-1}]$, then $\frac{f(m)}{u} = \frac{0}{1}$ in $N[U^{-1}]$. This means there exists $v \in U$ s.t. $vf(m) = 0$, which leads to $vf(m) = f(vm) = 0$. Since f is injective, $vm = 0$ in M. Then $\frac{m}{u} = \frac{vm}{vu} = \frac{0}{m} = \frac{0}{1}$. □

Example 1.3.6. *$\mathbb{Q}$ is a flat module over $\mathbb{Z}$. $\mathbb{Z}/2$ is a falt module over $\mathbb{Z}/6$. Both $\mathbb{C}(x)$ and $\mathbb{C}[x, x^{-1}]$ are flat over $\mathbb{C}[x]$.*

Theorem 1.3.7. *A module M over R is zero iff for every maximal ideal m, the localization M_m is zero.*

Definition 1.3.8. An R-module M is *Noetherian* is every submodule of M is finitely genereated.

Theorem 1.3.9. *If*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is exact, then M is Noetherian (resp. Artinian) iff M' and M'' are both Noetherian (resp. Artinian).

1.4 Rings and Modules of Finite Length

Definition 1.4.1. An R-module M is *simple* iff M has exactly 2 R-submodule: 0 and M.

Definition 1.4.2. A *composition series* for a module M is a chain

$$0 = M_0 < M_1 < M_2 < \cdots < M_{n-1} < M_n = M$$

of submodules (with strict inclusion) such that for all $1 \leq i \leq n$, M_i/M_{i-1} is simple.

Proposition 1.4.3. *A $\mathbb{Z}$-module M is simple iff it's of the form $\mathbb{Z}/p$ where p is prime.*

Proposition 1.4.4. *Let R be an R-module, J be an ideal. R/J is simple iff J is maximal.*

Example 1.4.5. *Let $R = \mathbb{C}[x, y]$, $M = C_z[x, y]/(x^2, xy, y^2)$.*

Proposition 1.4.6. *If k is a field, a compositions series for a vectors space V exists iff V is finite dimensional, the sequence always goes from 0 dimension to 1, 2, and grows to the entire thing V.*

Definition 1.4.7. The *length* of an R-module M is the minimal length of a compositions series, if one exists, or ∞. We denote it as $l(M)$.

Theorem 1.4.8. *Every composition series for M has the same length.*

Throughout the following, we assume all modules we work with have finite length.

Proposition 1.4.9. *If $N < M \implies l(N) < l(M)$.*

Proof. Choose a composition series for N:

$$0 < N_1 < N_2 < \cdots < N.$$

We start with a composition series for M of minimal length:

$$0 < M_0 < M_1 < \cdots < M_n = M.$$

We intersect it with N: $N_k = N_k \cap N$. Then we don't necessarily have strict containment.

$$0 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_n = N.$$

□