Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today topic are associated primes of modules. This concept allows to prove that over a noetherian ring R any finitely generated R-module M is built from modules of the type $R/\mathfrak{p}_j$ for various primes $\mathfrak{p}_j$.

1. Associated primes
2. The 1^{st} uniqueness theorem
3. Filtration with prime ideals
4. Exactness of localization

Associated primes

Definition. Let M be an R-module. An **associated prime** of M is a prime ideal $\mathfrak{p}$ of the form

$$\mathfrak{p} = \operatorname{ann}(m) = \{r \in R \mid rm = 0\}$$

for some non-zero element $m \in M$.

Proposition. *The maximal elements with respect to inclusion of the set*

$$\mathcal{M} = \{\operatorname{ann}(m) \mid m \in M, m \neq 0\}$$

are associated primes of M.

Proof. Let $\operatorname{ann}(m) \in \mathcal{M}$ be maximal and $f, g \in R$ elements with

$$fg \in \operatorname{ann}(m).$$

Suppose $g \notin \operatorname{ann}(m)$. Then $gm \neq 0$ and $\operatorname{ann}(m) \subset \operatorname{ann}(gm)$. Since $\operatorname{ann}(m) \in \mathcal{M}$ is maximal we have $\operatorname{ann}(m) = \operatorname{ann}(gm)$ and $f \in \operatorname{ann}(gm) = \operatorname{ann}(m)$. Thus $\operatorname{ann}(m)$ is a prime ideal. □

Ass(M)

Definition. Let M be an R-module. Then

$$\mathrm{Ass}(M) = \{\mathfrak{p} \mid \mathfrak{p} \text{ is an associated prime of } M\}$$

denotes the set of associated primes of M. Over a noetherian ring $\mathrm{Ass}(M)$ is non-empty, since the set $\mathcal{M}$ above is non-empty.

Definition. A **short exact sequence** of R-modules is a sequence

$$0 \longrightarrow M' \xrightarrow{\psi} M \xrightarrow{\varphi} M'' \longrightarrow 0$$

which consists of an injective R-module homomorphism ψ and a surjective R-module homomorphism φ such that

$$\ker(\varphi) = \mathrm{im}(\psi).$$

If we identify M' with a submodule of M via ψ, then M'' is isomorphic to the quotient module M/M':

$$M'' \cong M/\ker(\varphi) = M/M'.$$

Ass(M) in short exact sequences

Proposition. *Let*

$$0 \longrightarrow M' \xrightarrow{\psi} M \xrightarrow{\varphi} M'' \longrightarrow 0$$

be a short exact sequence of R-modules. Then

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'').$$

If $M = M' \oplus M''$, then $\mathrm{Ass}(M) = \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

Proof. The first inclusion is clear. For the second consider an $\mathfrak{p} \in \mathrm{Ass}(M) \setminus \mathrm{Ass}(M')$ and an element $m \in M$ such that $\mathfrak{p} = \mathrm{ann}(m)$. Then

$$Rm \cong R/\mathfrak{p}$$

Since $\mathfrak{p}$ is prime, every non-zero element of $gm \in Rm$ has annihilator $\mathrm{ann}(gm) = \mathfrak{p}$ as well: $f \in \mathrm{ann}(gm) = 0 \Rightarrow fg \in \mathrm{ann}(m) = \mathfrak{p} \Rightarrow f \in \mathfrak{p}$ since $g \notin \mathrm{ann}(m)$.
Since $\mathfrak{p} \notin \mathrm{Ass}(M')$ it follows that $Rm \cap M' = 0$.
Thus Rm is isomorphic to its image $\varphi(Rm)$ in M'' and

$$\mathfrak{p} = \mathrm{ann}(\varphi(m)) \in Ass(M'').$$

Associated primes of a direct sum

Corollary. $\mathrm{Ass}(M' \oplus M'') = \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$

Proof. For $M = M' \oplus M''$ we have two short exact sequences

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

and

$$0 \longrightarrow M'' \longrightarrow M \longrightarrow M' \longrightarrow 0.$$

Hence

$$\mathrm{Ass}(M') \cup \mathrm{Ass}(M'') \subset \mathrm{Ass}(M' \oplus M'') \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

follows from the proposition.

1^{st} uniqueness theorem

Theorem. *Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ be a minimal primary decompostion of an ideal $I \subset R$. Then the associated primes of R/I as an R-module is precisely the set*

$$\mathrm{Ass}(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$$

where $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$.

Proof. We first establish the special case when $I = \mathfrak{q}$ is a $\mathfrak{p}$-primary ideal:

$$\mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}.$$

Indeed suppose $g \in \mathrm{ann}(\overline{f}) = \mathfrak{p}'$ lies in an associated prime. Then $gf \in \mathfrak{q}$. Since $f \notin \mathfrak{q}$ we obtain $g^n \in \mathfrak{q}$, i.e., $\mathfrak{p}' \subset \mathrm{rad}(\mathfrak{q})$. Since $\mathfrak{q} \subset \mathfrak{p}'$ we deduce

$$\mathrm{rad}(\mathfrak{q}) \subset \mathrm{rad}(\mathfrak{p}') = \mathfrak{p}' \subset \mathrm{rad}(\mathfrak{q})$$

and equality holds.

Continuation of the proof

Now consider the R-module homomorphism

$$\psi : R \to R/\mathfrak{q}_1 \oplus \ldots \oplus R/\mathfrak{q}_r, f \mapsto (f + \mathfrak{q}_1, \ldots, f + \mathfrak{q}_r)$$

Since $\ker(\psi) = I$ we obtain an inclusion

$$R/I \hookrightarrow R/\mathfrak{q}_1 \oplus \ldots \oplus R/\mathfrak{q}_r.$$

Hence we obtain $\mathrm{Ass}(R/I) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ from the propostion. To see equality we use that the primary decomposition is irredundant. Thus for each i

$$\bigcap_{j \neq i} \mathfrak{q}_j \supsetneq \bigcap_{j=1}^{r} \mathfrak{q}_j.$$

Consider an element f_i in the complement and the residue class $\overline{f}_i \in R/I$. ψ maps the submodule $R\overline{f} \subset R/I$ into the summand $R/\mathfrak{q}_i$. Thus

$$\mathrm{Ass}(R\overline{f}) \subset \mathrm{Ass}(R/\mathfrak{q}_i) = \{\mathfrak{p}_i\}$$

and equality holds. Thus $\{\mathfrak{p}_i\} = \mathrm{Ass}(R\overline{f}) \subset \mathrm{Ass}(R/I)$. □

Associated primes of an ideal

Definition. If $I \subset R$ is an ideal. Then by the associated primes of I we mean $\mathrm{Ass}(R/I)$ where we regard R/I as an R-module.

Notice that $\mathrm{Ass}(I)$ where we regard I as an R-module is not so interesting. For example if R is an integral domain, then

$$\mathrm{Ass}(I) = \mathrm{Ass}(R) = \{(0)\}.$$

Thus the associated primes of I are precisely the prime ideals which occur in a minimal primary decomposition of I.

Filtration with prime ideals

Theorem. *Let M be a finitely generated non-zero module over a noetherian ring R. Then there exists a filtration*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$$

such that all quotients

$$M_i/M_{i-1} \cong R/\mathfrak{p}_i$$

for some prime ideals $\mathfrak{p}_i$ of R.

Proof. Since R is noetherian the set of proper ideals

$$\mathcal{M} = \{\mathrm{ann}(m) \mid m \in M,\ m \neq 0\}$$

is not empty, and a maximal element of this set is a prime ideal $\mathfrak{p}_1 = \mathrm{ann}(m_1)$ such

$$Rm_1 \cong R/\mathfrak{p}_1.$$

We take $M_1 = Rm_1$.

Filtration with prime ideals

Suppose $M_0 \subset \ldots \subset M_{k-1}$ are already constructed. If $M_{k-1} \subsetneq M$, then we consider an associated prime $\mathfrak{p}_k = \operatorname{ann}(\overline{m}_k) \in \operatorname{Ass}(M/M_{k-1})$ and define

$$M_k = \pi^{-1}(R\overline{m}_k) = Rm_k + M_{k-1}$$

where $\pi : M \to M/M_{k-1}$ is the natural projection and $\pi(m_k) = \overline{m}_k$.

$$M_k/M_{k-1} \cong Rm_k/Rm_k \cap M_{k-1} \cong Rm_k/\mathfrak{p}_k m_k \cong R\overline{m}_k \cong R/\mathfrak{p}_k.$$

The process stops with an $M_n = M$ because any ascending chain of submodules becomes stationary, because M is noetherian. $\square$

Filtration with prime ideals

Proposition. *Let M be an R-module with a filtration*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$$

such that all quotients $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i$ of R. Then

$$\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

Functoriality of localization

Let $\varphi : M \to N$ be an R-module homomorphism. Then

$$\varphi[U^{-1}] : M[U^{-1}] \to N[U^{-1}]$$

defined by

$$\varphi[U^{-1}](\frac{m}{s}) = \frac{\varphi(m)}{s}$$

is a well-defined $R[U^{-1}]$-module homomorphism. If

$M' \xrightarrow{\psi} M \xrightarrow{\varphi} M''$ are two composable morphisms with $\varphi \circ \psi = 0$, then the same holds for the localizations. More is true.

Definition. A sequence

$$M' \xrightarrow{\psi} M \xrightarrow{\varphi} M''$$

of R-module homomorphism is **exact at** M if $\ker(\varphi) = \mathrm{im}(\psi)$.

Exactness of localization

Proposition. *Let* $M' \xrightarrow{\psi} M \xrightarrow{\varphi} M''$ *be exact at* M*. Let* U *be a multiplicative subset. Then the induced sequence*

$$M'[U^{-1}] \xrightarrow{\psi[U^{-1}]} M[U^{-1}] \xrightarrow{\varphi[U^{-1}]} M''[U^{-1}]$$

is exact at $M[U^{-1}]$*.*

Proof. The inclusion $\mathrm{im}(\psi[U^{-1}]) \subset \ker(\varphi[U^{-1}])$ is clear because $\varphi \circ \psi = 0$. To prove the converse inclusion let $m/s \in \ker(\varphi[U^{-1}])$. Then $\varphi(m)/s = 0 \in M''[U^{-1}]$, i.e., $\exists\, u \in U$ such that $u\varphi(m) = 0 \in M''$. But $u\varphi(m) = \varphi(um)$ since φ is R-linear. Hence $um \in \ker(\varphi) = \mathrm{im}(\psi)$. So there exists $m' \in M'$ such that $\psi(m') = um$. Thus

$$\frac{m'}{us} \mapsto \frac{um}{us} = \frac{m}{s}.$$

□

Localization commutes with the formation of finite sums, finite intersections and quotients

If $N \subset M$ is a submodule, then by the proposition applied to the exact sequence

$$0 \to N \to M$$

we may regard $N[U^{-1}]$ as a submodule of $M[U^{-1}]$.

Corollary. *Let N, P be submodules of M. Then*

1) $(N + P)[U^{-1}] = N[U^{-1}] + P[U^{-1}]$.
2) $(N \cap P)[U^{-1}] = N[U^{-1}] \cap P[U^{-1}]$.
3) $(M/N)[U^{-1}] \cong M[U^{-1}]/N[U^{-1}]$.

Proof. 1) follows from $n/s + p/t = (tn + sp)/st$.
2): If $n/s = p/t$, then $\exists u \in U$ with $utn = usp \in N \cap P$.
3) follows from the proposition applied to the exact sequence

$$0 \to N \to M \to M/N \to 0.$$

Further local properties

Theorem. *Let $\varphi : M \to N$ be an R-module homomorphism. TFAE*

1) *φ is injective.*
2) *$\varphi_{\mathfrak{p}}$ is injective for all prime ideals $\mathfrak{p}$ of R.*
3) *$\varphi_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$ of R.*

A similar result holds for 'injective' replaced by 'surjective'.

Proof. Consider the sequence

$$0 \to \ker(\varphi) \to M \to N$$

which is exact at M and $\ker(\varphi)$. By the exactness of localization

$$\ker(\varphi_{\mathfrak{p}}) = (\ker(\varphi))_{\mathfrak{p}}.$$

Thus the result follows because being the zero-module is a local property. For the second version we consider the sequence

$$M \to N \to \operatorname{coker}(\varphi) \to 0.$$