Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topic are fractions. This is an important technique in commutative algebra.

1. Multiplicative sets and localization
2. Primary decomposition and localization
3. Proof of the second uniqueness theorem

Multiplicative sets and fractions

If we want to add or multiply two fractions, we have to be able to multiply the denominators:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

Definition. A **multiplicative** subset $U \subset R$ of a ring R is a subset which satisfies

a) $1 \in U$

b) $s, t \in U \implies st \in U$.

Example. The most important multiplicative sets are:

1. $U = \{f^k \mid k \in \mathbb{N}\}$ powers of an element $f \in R$,
2. $U = R \setminus \mathfrak{p}$ the complement of a prime ideal,
3. $U = \{r \in R \mid rs \neq 0 \ \forall s \neq 0\}$ the set of non-zero divisors.

If R is an integral domain, then (0) is a prime ideal and the set of non-zero divisors coincides with the complement of (0).

Localization in U

Let $U \subset R$ be a multiplicative subset of a ring. We will define a ring of fractions

$$R[U^{-1}] = \{\frac{a}{s} \mid a \in R \text{ and } s \in U\}$$

as follows: Consider on $R \times U$ the following equivalence relation:

$$(a_1, s_1) \sim (a_2, s_2) \text{ iff } \exists u \in U \text{ such that } u(s_2 a_1 - s_1 a_2) = 0 \in R.$$

The factor u is needed for the transitivity, since R might not be an integral domain.

$$\begin{aligned}
& (a_1, s_1) \sim (a_2, s_2) \text{ and } (a_2, s_2) \sim (a_3, s_3) \\
\Rightarrow \quad & \exists u, v \in U \text{ such that } u(s_2 a_1 - s_1 a_2) = 0 \text{ and } v(s_3 a_2 - s_2 a_3) = 0 \\
\Rightarrow \quad & 0 = v s_3 u(s_2 a_1 - s_1 a_2) - u s_1 v(s_3 a_2 - s_2 a_3) = uvs_2(s_3 a_1 - s_1 a_3) \\
\Rightarrow \quad & (a_1, s_1) \sim (a_3, s_3) \text{ since } uvs_2 \in U.
\end{aligned}$$

The fraction $\frac{a}{s} = \{(b, t) \in R \times U \mid (a, s) \sim (b, t)\}$ denotes the equvalence class of (a, s).

Localization in U continued

Then

$$R[U^{-1}] = (R \times U)/\sim$$

defines the localization as a set. It is a subset of $2^{R \times U}$. The usual formulas give $R[U^{-1}]$ the structure of a commutative ring with $1 = \frac{1}{1}$. Of course, one has to verify that addition and multiplication are well defined. For example, if $(a_1, s_1) \sim (a_2, s_2)$, then

$$\frac{a_1}{s_1} + \frac{b}{t} = \frac{a_1 t + s_1 b}{s_1 t} = \frac{a_2 t + s_2 b}{s_2 t} = \frac{a_2}{s_2} + \frac{b}{t}$$

because $u(s_2 a_1 - s_1 a_2) = 0$ implies
$u(s_2 t(t a_1 + s_1 b) - s_1 t(a_2 t + s_2 b)) = t^2 u(s_2 a_1 - s_1 a_2) = 0.$
The map

$$\iota : R \to R[U^{-1}], r \mapsto \frac{r}{1}$$

is a ring homomorphism, which might be not injective:

$$\ker(\iota) = \{r \in R \mid \exists u \in U \text{ with } ur = 0\}.$$

Notice that the elements $\iota(u)$ are units in $R[U^{-1}]$: $\frac{u}{1}\frac{1}{u} = 1$.

Localization of modules

Let M be an R-module and $U \subset R$ a multiplicative subset. Then we can define similarly $M[U^{-1}]$:

$$(m_1, s_1) \sim (m_2, s_2) \text{ iff } \exists u \in U \text{ such that } u(s_2 m_1 - s_1 m_2) = 0 \in R$$

is an equivalence relation on $M \times U$ and the set of equivalence classes

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

becomes an $R[U^{-1}]$-module by

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}.$$

Notation

Definition. Let $\mathfrak{p} \subset R$ be a prime ideal and M and R-module. Then

$$M_{\mathfrak{p}} = M[U^{-1}]$$

where $U = R \setminus \mathfrak{p}$ is called the localization of M in $\mathfrak{p}$. For $f \in R$ the localization of M in f is

$$M_f = M[U^{-1}]$$

for $U = \{f^k \mid k \in \mathbb{N}\}$.

Example.

$$\mathbb{Z}_2 = \{\frac{a}{b} \in \mathbb{Q} \mid b \text{ is a power of } 2\}$$

and

$$\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathbb{Q} \mid b \text{ with } 2 \not| b\}$$

quite different.

A local property

Theorem. *Let M be an R-module. TFAE*

1) $M = 0$.
2) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p} \subset R$.
3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m} \subset R$.

Proof. Only the implication 3) $\implies$ 1) is non-trivial. Let $M \neq 0$ be a non-zero module and $m \in M$ a non-zero element. Then $I = \mathrm{ann}(m) \subsetneq R$ is a proper ideal since $1 \notin I$. The set of ideals $\mathcal{M} = \{J \text{ ideal in } R \mid I \subset J\}$ contains a maximal element $\mathfrak{m}$ with respect to inclusion. (This is clear for noetherian rings. For more general rings one applies Zorn's Lemma.) The ideal $\mathfrak{m}$ is a maximal ideal of R, and $M_{\mathfrak{m}} \neq 0$ because

$$\frac{m}{1} \neq 0.$$

No element of $R \setminus \mathfrak{m}$ annihilates m because $\mathfrak{m} \supset I = \mathrm{ann}(m)$. $\square$

Extended and contracted ideals

Let $\varphi : A \to B$ a ring homomorphism, $\mathfrak{a}$ an ideal in A and $\mathfrak{b}$ an ideal in B. Then

$$\mathfrak{a}^e = \mathfrak{a}B = \{\sum_i b_i\varphi(a_i) \mid b_i \in B \text{ and } a_i \in \mathfrak{a}\}$$

is called the **extended** ideal of $\mathfrak{a}$, and

$$\mathfrak{b}^c = \varphi^{-1}(\mathfrak{b})$$

is called the **contracted** ideal of $\mathfrak{b}$.

Primary decompositions behave well under contractions:

1. If $\mathfrak{b}$ is a prime ideal or primary ideal, then $\mathfrak{b}^c$ is prime respectively primary as well.
2. $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.
3. $(\mathrm{rad}(\mathfrak{b}))^c = \mathrm{rad}(\mathfrak{b}^c)$.

Extended and contracted ideals

The behavior under extension can be complicated:

Example. Consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-1}]$. Then the prime ideals $(p) \subset \mathbb{Z}$ extend as follows:

1) $(2)^e = (1 + \sqrt{-1})^2$ is a square of a prime ideal.
2) If $p \equiv 1 \mod 4$, then $(p)^e$ is the product of two distinct prime ideals, for example $(5)^e = (2 + \sqrt{-1})(2 - \sqrt{-1})$.
3) If $p \equiv 3 \mod 4$, then $(p)^e$ is a prime ideal.

Only 2) is a non-trival statement. It is equivalent to a theorem of Fermat, which says that a prime $p \equiv 1 \mod 4$ is sum of two squares: $(5 = 2^2 + 1^2, 13 = 3^2 + 2^2, \ldots, 97 = 9^2 + 4^2$, etc.)

Extended and contracted ideals

Proposition. *For a ring homomorphism $A \to B$ and notation as before we have*

1. $\mathfrak{a}^{ec} \supset \mathfrak{a}$ *and* $\mathfrak{b}^{ce} \subset \mathfrak{b}$.
2. $\mathfrak{a}^{e} = \mathfrak{a}^{ece}$ *and* $\mathfrak{b}^{cec} = \mathfrak{b}^{c}$.
3. *The set of contacted ideals is* $C = \{\mathfrak{a} \mid \mathfrak{a} = \mathfrak{a}^{ec}\}$, *and the set of extended ideal is* $E = \{\mathfrak{b} \mid \mathfrak{b} = \mathfrak{b}^{ce}\}$. *These sets are in bijection via* $\mathfrak{a} \mapsto \mathfrak{a}^{e}$ *and* $\mathfrak{b} \mapsto \mathfrak{b}^{c}$.

Proof. 1) is clear. 2) follows from 1): $\mathfrak{a}^{ec} \supset \mathfrak{a}$ implies $\mathfrak{a}^{ece} \supset \mathfrak{a}^{e}$, and apply $\mathfrak{b}^{ce} \subset \mathfrak{b}$ to $\mathfrak{b} = \mathfrak{a}^{e}$ gives the other inclusion. 3) follows with 2). □

The situation is better for localizations maps

$$\iota : R \to R[U^{-1}].$$

Passing from ring to a localization makes things easier at least from a theoretical point of view. For example the ideal theory of $R[U^{-1}]$ is a simplified version of the ideal theory of R.

Ideal theory of localizations

Theorem. *Let $U \subset R$ be a multiplicative subset of a ring and let $\iota : R \to R[U^{-1}], r \mapsto r/1$ denote the natural homomorphism.*

1. *If I is an ideal in R, then*
$$I^{ec} = \iota^{-1}(IR[U^{-1}] = \{a \in R \mid \exists u \in U \text{ with } ua \in I\}.$$
2. *If J is an ideal in $R[U^{-1}]$, then*
$$J^{ce} = \iota^{-1}(J)R[U^{-1}] = J$$
Thus the map $J \mapsto \iota^{-1}(J)$ is an injection of the set ideals of $R[U^{-1}]$ into the set of ideals of R.
3. *If R is noetherian, then $R[U^{-1}]$ is noetherian.*
4. *ι^{-1} induces a bijection between the set of prime ideals of $R[U^{-1}]$ and the set of prime ideals $\mathfrak{p}$ of R with $U \cap \mathfrak{p} = \emptyset$.*
5. *ι^{-1} induces a bijection between the set of primary ideals of $R[U^{-1}]$ and the set of prime ideals $\mathfrak{q}$ of R with $U \cap \mathfrak{q} = \emptyset$.*

Proof

Part 1: If $a \in R$, then $a \in \iota^{-1}(IR[U^{-1}]) \iff a/1 \in IR[U^{-1}]$
$\iff ua \in I$ for some $u \in U$.
Part 2: Let $b/u \in R[U^{-1}]$. Then $b/u \in J \iff b/1 \in J$
$\iff b \in \iota^{-1}(J) \iff b/u \in \iota^{-1}(J)R[U^{-1}]$.
Part 3 follows from part 2.
Part 5 and 4: Let $\mathfrak{q}$ be a primary ideal of $R[U^{-1}]$. Then
$\mathfrak{q}^c = \iota^{-1}(\mathfrak{q})$ is a primary ideal of R which does not intersect U
because $\mathfrak{q}$ contains no units.
Conversely, let $\mathfrak{q}$ be a primary ideal in R with $\mathfrak{q} \cap U = \emptyset$.
Then $\mathfrak{q}^e = \mathfrak{q}R[U^{-1}]$ is a proper ideal because $\mathfrak{q}^{ec} = \iota^{-1}(\mathfrak{q}^e) = \mathfrak{q}$
follows from part 1: $ua \in \mathfrak{q}$ and $u^n \notin \mathfrak{q}$ implies $a \in \mathfrak{q}$ since $\mathfrak{q}$ is
primary. It remains to prove that $\mathfrak{q}^e$ is a primary ideal. Suppose
$a/u \cdot b/v \in \mathfrak{q}^e$, then $wab \in \mathfrak{q}$ for some $w \in U$ by part 1. Hence
$wa \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some n since $\mathfrak{q}$ is primary. It follows $a/u \in \mathfrak{q}^e$
or $(b/v)^n \in \mathfrak{q}^e$ because wu and v are units in $R[U^{-1}]$.
In case of prime ideals we have $n = 1$ in the argument above.

Primary decomposition and localization

Corollary. *Let* U *be a multiplicative subset of a ring* R *and*

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$$

a primary decomposition of an ideal $I \subset R$*. Then*

$$I^e = \bigcap_{\mathfrak{q}_i : \mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i^e$$

is a primary decomposition of the extended ideal $I^e \subset R[U^{-1}]$ *and*

$$I^{ec} = \bigcap_{\mathfrak{q}_i : \mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i.$$

In particular the last intersection does not depend on the choice of the primary decomposition.

Proof

We need one more Lemma.
Lemma. *Let $\iota : R \to R[U^{-1}]$ be a localization, and let I and J be ideals in R. Then*

$$I^e \cap J^e = (I \cap J)^e.$$

Proof of the Lemma. $I^e \cap J^e \supset (I \cap J)^e$ is clear. Suppose

$$\frac{a}{u} = \frac{b}{v} \in I^e \cap J^e \text{ with } a \in I \text{ and } b \in J$$

Then there exists a $w \in U$ such that $wva = wub \in I \cap J$. Hence

$$\frac{a}{u} = \frac{wva}{uwv} \in (I \cap J)^e.$$

$\square$

Primary ideals $\mathfrak{q}_j$ with $\mathfrak{q}_j \cap U \neq \emptyset$ extend to $\mathfrak{q}_j^e = (1)$, since elements of U become units in $R[U^{-1}]$. Thus these can be dropped in the intersection, and

$$I^e = \bigcap_{\mathfrak{q}_i : \mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i^e$$

2^{nd} uniqueness theorem

The rest of the theorem clear, because contraction commutes with intersections and $\mathfrak{q}_i^{ec} = \mathfrak{q}_i$ for primary ideals with $\mathfrak{q}_i \cap U \neq \emptyset$. $\square$

Corollary. *Let $\mathfrak{p}_i$ be a minimal associated prime of a minimal primary decomposition*

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r.$$

Then $\mathfrak{q}_i$ is uniquely determined by I.

Proof. Consider the localization in $\mathfrak{p}_i$, i.e., with respect to $U = R \setminus \mathfrak{p}_i$. Since $\mathfrak{p}_i$ is minimal all other associated primes $\mathfrak{p}_j = \operatorname{rad}(\mathfrak{q}_j)$ intersect U:

$$(R \setminus \mathfrak{p}_i) \cap \mathfrak{p}_j = \emptyset \iff \mathfrak{p}_j \subset \mathfrak{p}_i$$

and $\mathfrak{p}_j$ would be smaller than $\mathfrak{p}_i$. Since U is multiplicative $\mathfrak{p}_j \cap U \neq \emptyset \iff \mathfrak{q}_j \cap U \neq \emptyset$ holds. Thus

$$I^{ec} = \mathfrak{q}_i$$

holds by the theorem. $\square$

Examples

1. $R = \mathbb{Z}$. The ideals of $\mathbb{Z}$ are principal and
$$(n) = (p_1^{e_1}) \cap \ldots \cap (p_r^{e_r})$$
is the primary decomposition if
$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$
is the prime factorization.
2. The polynomial ring $K[x_1, \ldots, x_n]$ for any field K is factorial. As above the primary decomposition of an principal ideal (f) corresponds factorizations: If
$$f = uf_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$$
with $u \in K^*$ a unit and f_j irreduzible then $(f) = (f_1^{e_1}) \cap \ldots \cap (f_r^{e_r})$ is the primary decomposition.