Algebraic curves from function fields

Douglas A. Leonard
Auburn University
Department of Mathematics and Statistics
Auburn, AL, 36849

October 10, 2015

Chapter 1

Introduction

There is no reason for me to rehash the existing theory of the topics in commutative algebra and algebraic curves which are discussed below. While many of the topics should necessarily be familiar, the perspective here is definitely not. This is a purely algebraic approach to algebraic curves; and, as the title suggests, an algebraic curve is to be treated as a byproduct of a function field, rather than an algebraic variety of some sort that happens to have a function field that may or may not be useful related to it.

This is to be an example-driven text, with the underlying principle that a well-chosen example can lead to correct and insightful self-evident theory, whereas as example-free theory doesn't necessarily suggest the context from which it was derived. To reinforce this, this is structured as a cross-referenced .pdf file that can be read one example at a time, with clickable definitions, algorithms, and computer algebra (input, output, and/or code). This allows examples to precede definitions and suggest theory, rather than having unmotivated definitions, theorems, and proofs to precede the examples from which they were derived or with which they were meant to deal.

An active interplay with various computer algebra systems (CASs), such as Magma, Macaulay2, and Singular used here, can be extremely enlightening, and can be a means of testing ideas before they are written as theory.

Also it is important to make sure that the theory works best on simple examples before trying to generalize it. In fact the generalization process should require revisiting simpler examples at each step to see what needs to be revised and improved. Little should be taken for granted. Just because some notation and theory is set in stone as a result of decades of use doesn't make it the right way to view a subject. As with the motto that any computer program can be written better, so it should be with mathematical theory.

At this point it is possible to proceed through the commutative algebra or to skip directly to the new perspective on algebraic curves (12). What is appropriate depends on the background of the reader, but there should be sufficient cross-references to go back and forth between the two.

It should be noted however that the rings seriously considered herein are not just multivariate polynomial rings, but more specifically multivariate polynomial rings with a monomial ordering, so that elements can actually be written down in some predictable canonical form that is not just some generic name. That is, SINGULAR requires a monomial ordering in the definition of a polynomial ring, MACAULAY2 has a default grevlex monomial ordering, and MAGMA has a default lex monomial ordering, so that while input may not have to be canonical in form, probably the internal form and definitely output are necessarily canonical.

```
ring R=0,(x,y),lp;
```

```
R=QQ[x,y,MonomialOrder=>Lex];
```

```
R<x,y>:=PolynomialRing(Rationals(),2);
```

are examples of ring definitions in SINGULAR, MACAULAY2, and MAGMA respectively, for $R := \mathbf{Q}[x, y]$ with a lexicographical monomial ordering having $x \succ y$ (whether explicit or implicit) that must be made before typing input such as $2y^2x - x^2$. The resulting output will then have a canonical form $-x^2 + 2xy^2$ That is, variables such as x and y must live somewhere (and combinations of them must have a predictable canonical form for some functions on them to make sense).

```
ring R=0,(x,y),dp;
```

```
R=QQ[x,y];
```

```
R<x,y>:=PolynomialRing(Rationals(),2,"grevlex");
```

are examples of ring definitions in SINGULAR, MACAULAY2, and MAGMA respectively, for $R := \mathbf{Q}[x, y]$ with a graded reverse lexicographical monomial ordering having $x \succ y$ (whether explicit or implicit) that must be made before typing input such as $-x^2 + 2y^2x$. The resulting output will then have a canonical form $2xy^2 - x^2$ Here the canonical form is different because it is based on a different monomial ordering.

SINGULAR in particular is meant to handle the same multivariate polynomial ring with several different monomial orderings using built-in map `imap` and `fetch` to move ideals from one ordered version to another, while never allowing an unordered version of the ring.

So while it might be tempting to say some things about a polynomial ring that are (or seem to be) independent of the monomial ordering, they will be viewed here as statements about polynomial rings with monomial orderings that don't use the monomial ordering. In particular they are independent of being able to write down the elements in some prescribed canonical way.

[A similar thing happens with vector spaces, wherein certain definitions and maybe theorems can be stated in terms of generic names for vectors, whereas actual computations generally require some explicit canonical form for each vector to even be able to write a vector down in any meaningful way. That is, it is possible to define what a basis for a subspace is by using only generic names for vectors, but in order to apply that to a specific set of vectors, it is probably necessary to have some explicit description of those vectors written in some canonical way.]

Chapter 2

Canonical forms

How can this not be the most fundamental idea in this area? It should be the driving force behind everything.

2.1 The integers mod p

Is $(-1035, 3021, -1343, 1343, -11)$ an ordered list of canonical representatives for the cosets $i + 5\mathbf{Z}$ of the ideal $5\mathbf{Z}$ of the ring of integers $\mathbf{Z}$? Well, ordered list of representatives, yes; but calling them canonical would seem to imply an algorithm to reduce $z \in \mathbf{Z}$ directly to one of them.

Likewise, there is nothing mathematically incorrect with statements such as

$$(i + p\mathbf{Z}) + (j + p\mathbf{Z}) = (i + j) + p\mathbf{Z}$$

or

$$(i + p\mathbf{Z}) * (j + p\mathbf{Z}) = (i \cdot j) + p\mathbf{Z}.$$

But there isn't even an implicit suggestion that there are reasonable choices for canonical representatives for the cosets of $p\mathbf{Z}$, let alone a straightforward algorithm to reduce elements of a coset to a canonical representative; whereas this is of paramount consideration computationally. However, the notation:

$$(i + p\mathbf{Z}) + (j + p\mathbf{Z}) = f(i + j) + p\mathbf{Z}$$

or

$$(i + p\mathbf{Z}) * (j + p\mathbf{Z}) = f(i \cdot j) + p\mathbf{Z},$$

with f an implicit reduction algorithm, is not so theoretically pleasing.

Such questions as what coset $j + 143\mathbf{Z}$ contains 301295 are trivial, absent the intent that j be a canonical representative, and not 301295 itself. What's the big deal? Well, try asking other questions, such as whether $301295 + 143\mathbf{Z}$ and $-12763902 + 143\mathbf{Z}$ are the same coset? Here the answer is not quite so trivial; but at least there is the existence of some algorithm implicit in the question itself.

This example is meant to motivate interest in questions of membership, hence isomorphism (6.2), which may not even register at a purely theoretical level, but which may be fundamental at the computational level. It is probably more common theoretically to look for invariants that show that objects are different, rather than showing how to reduce various objects to canonical form to show whether they are the same. That is not to say that the latter is not done routinely; reduction of a matrix to reduced row-echelon form being an obvious example.

To see what membership and isomorphism mean in practice, jump to the outputs of the various CASs for the normalization of the Klein quartic (13.1), ask yourself if these are the same answers in any sense, and decide how you would convince someone else of that.

Also go to (3) to see that it is not possible to blindly expect CASs to produce canonical results.

2.2 Subspaces, modules, and ideals

Just as linear algebra deals with linear relations among all types of objects, commutative algebra deals with polynomial relations among all types of objects. That is, the objects satisfy polynomial equations, not that they are polynomials themselves. The best example of this is that $c := \cos(\theta)$ and $s := \sin(\theta)$ satisfy the polynomial equation $c^2 + s^2 = 1$.

So this area of mathematics could be viewed as a natural generalization of at least some parts of linear algebra. Maybe a good starting point would then be to consider how what is known about finite-dimensional vector spaces over a field carries over to knowledge about modules over a polynomial ring.

Consider the subspace $U \subset \mathbf{Q}^4$ spanned by the vectors $(0,1,1,1)$, $(2,3,-1,5)$, and $(4,3,-5,7)$, with U by definition closed under taking $\mathbf{Q}$-linear combinations. Is $(4,7,-5,10) \in U$?

It is possible to row-reduce the matrix

$$A := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 3 & -1 & 5 \\ 4 & 3 & -5 & 7 \end{pmatrix}$$

to get

$$RREF(A) = \begin{pmatrix} 1 & 0 & -2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

then compute

$$(4,7,-5,10) - 4(1,0,-2,1) - 7(0,1,1,1) = (0,0,-4,-1) \neq (0,0,0,0)$$

to see that it isn't.

This gives a canonical coset representative for the coset $(4,7,-5,10) + U$ of the subspace U. While this coset representative $(0,0,-4,-1)$ may not necessarily be useful, the fact that there is a presentation of the subspace U and a straightforward algorithm for testing membership is. Maybe testing equality or isomorphism is a more compelling mathematical formulation than testing membership, but there is no real difference.

A possibly more interesting use of canonical representatives here might have been to compute an orthogonal basis such as

$$\{(0,1,1,1),\ (4,1,-5,4)\}$$

and subtract projections to get

$$(4,7,-5,10) - 4(0,1,1,1) - \frac{24}{19}(2,3,-1,5) = \left(\frac{-48}{19}, \frac{-15}{19}, \frac{71}{19}, \frac{-6}{19}\right)$$

to see that

$$(4,7,-5,10) - \left(\frac{-48}{19}, \frac{-15}{19}, \frac{71}{19}, \frac{-6}{19}\right) = \left(\frac{124}{19}, \frac{118}{19}, \frac{-24}{19}, \frac{184}{19}\right)$$

is the closest point of U to $(4,7,-5,10)$. While this may be much more useful information in context, it is more geometric than algebraic in flavor, given that it depends on properties of distance and orthogonality. The perspective here is meant to be purely algebraic.

To generalize this from a field $\mathbf{F}$ and finite-dimensional vector spaces $V := \mathbf{F}^n$ to a multivariate polynomial ring $R := \mathbf{F}[x_m, \ldots, x_1]$ and the R-modules R^n, it is possible to to start with a finite set of generators and produce a basis, from which it may be possible to determine a canonical representative for the coset of the module containing a given $f \in R$. This also works for ideals I, that is subsets of R closed under R-linear combinations and necessarily finitely-generated. But even for subspaces, the bases probably need to be in

row-echelon form (or possibly orthogonal) to have an obvious algorithm for computing a canonical form. For $R := \mathbf{F}[x]$, the division algorithm suffices, since all ideals are principal (that is, generated by a single element); and canonical forms are remainders after division by that single element. As an example, the ideal $I := \langle x^6 - 1, x^9 - 1 \rangle \subset R := \mathbf{Q}[x]$ has basis $(x^3 - 1)$. The R-module $\langle (1, 0, x^9 - 1),\ (0, 1, x^6 - 1) \rangle$ has basis

$$((-x^3 - 1, x^6 + x^3 + 1, 0), (1, -x^3, x^3 - 1)).$$

Both are gotten using variants of the Euclidean algorithm and appropriate orderings.

2.3 The extended Euclidean algorithm

Definition 1. *The division algorithm (for either* $\mathbf{Z}$ *or* $\mathbf{F}[x_1]$*) has input* a *and* $b \neq 0$*, with output* q *and* r *such that* $a = qb + r$ *and* $r \prec |b|$ *(or* $r = 0$*).*

Definition 2. *The Euclidean algorithm is just a recursive form of the division algorithm:*

$$r_i := r_{i-2} - q_i r_{i-1},\ r_i \prec r_{i-1}$$

with input r_{-1} *and* r_0 *stopping when* $r_n = 0$*. The output can be just* r_{n-1} *or all of the* r_i *and* q_i*.*

Definition 3. *The extended Euclidean algorithm is the Euclidean algorithm, together with the additional recursions*

$$u_{-1} := 0,\ u_0 := 1,\ u_i := q_i u_{i-1} + u_{i-2};$$

$$v_{-1} := 1,\ v_0 := 0,\ v_i := q_i v_{i-1} + v_{i-2}.$$

This can be applied to either the ring of integers, $\mathbf{Z}$, with the normal ordering or to a univariate polyonomial ring $\mathbf{F}[x]$ with the degree ordering. [While this can be found in the literature in some form, it is surprising that it is not to be found everywhere, given its usefulness. Most computer algebra packages stop short, computing only the gcd of the input or possibly the gcd explicitly as a linear combination of the input.]

As an example for $\mathbf{Z}$:

	r_{i-2}	=	$q_i r_{i-1}$	+	r_i	u_i	v_i
-1					143	0	1
0					37	1	0
1	143	=	$3 \cdot 37$	+	32	3	1
2	37	=	$1 \cdot 32$	+	5	4	1
3	32	=	$6 \cdot 5$	+	2	27	7
4	5	=	$2 \cdot 2$	+	1	58	15
5	2	=	$2 \cdot 1$	+	0	143	37

As an example over $\mathbf{Q}[x]$,

	q_i	r_i	u_i	v_i
-1		$x^7 - 1$	0	1
0		$x^3 + x + 1$	1	0
1	$x^4 - x^2 - x + 1$	$2x^2 - 2$	$x^4 - x^2 - x + 1$	1
2	$x/2$	$2x + 1$	$(x^5 - x^3 - x^2 + x + 2)/2$	$x/2$
3	$(2x - 1)/2$	$-3/2$	$(2x^6 - x^5 + 2x^4 - x^3 - x^2 - x + 2)/4$	$(2x^2 - x + 4)/4$
4	$(-4x - 2)/3$	0	$-2(x^7 - 1)/3$	$-2(x^3 + x + 1)/3$

As an example over $\mathbf{F}_2[x]$,

	q_i	r_i	u_i	v_i
-1		$x^{12}+x^8+x$	0	1
0		x^6+x+1	1	0
1	x^6+x^2+x+1	x^3+x+1	x^6+x^2+x+1	1
2	x^3+x+1	x^2+x	$x^9+x^7+x^6+x^5+x^4$	x^3+x+1
3	$x+1$	1	$x^{10}+x^9+x^8+x^6+x^4+x^2+x+1$	$x^4+x^3+x^2$
4	x^2+x	0	$x^{12}+x^8+x$	x^6+x+1

$$(x^4+x^3+x^2)(x^{12}+x^8+x)+(x^{10}+x^9+x^8+x^6+x^4+x^2+x+1)(x^6+x+1)=1\in\mathbf{F}_2[x]$$

$$(a^4+a^3+a^2)(a^{12}+a^8+a)=1(mod\ a^6+a+1)\in\mathbf{F}_2[a]$$

$$1/(a^{12}+a^8+a)=a^4+a^3+a^2\in\mathbf{F}_{64}:=\mathbf{F}_2[a]/\langle a^6+a+1\rangle$$

As an example for $(\mathbf{F}_2(x))[y]$:

	q_i	r_i	u_i	v_i
-1		$y^5+y^2(x^4+x)+yx^2+x^{12}$	0	1
0		y^4+x^2	1	0
1	y	$y^2(x^4+x)+x^{12}$	y	1
2	$\frac{y^2(x^3+1)+x^{11}}{x(x^6+1)}$	$\frac{(x^{22}+x^8+x^2)}{(x^6+1)}$	$\frac{(y^3(x^4+x)+yx^{12}+x^8+x^2)}{(x^8+x^2)}$	$\frac{(y^2(x^4+x)+x^{12})}{(x^8+x^2)}$
3	$\frac{(x^6+1)(y^2(x^4+x)+x^{12})}{(x^{22}+x^8+x^2)}$	0	$\frac{(x^6+1)(y^5+y^2(x^4+x)+yx^2+x^{12})}{(x^{22}+x^8+x^2)}$	$\frac{(x^6+1)(y^4+x^2)}{(x^{22}+x^8+x^2)}$

Exercise Prove the following about the entries in the extended Euclidean algorithm, given input $r_{-1} \succ r_0$,

1. $r_n = 0$ for some (smallest) natural number n.
2. $r_{n-1} = gcd(r_{-1}, r_0)$.
3. $u_k v_{k-1} - u_{k-1} v_k = (-1)^k$.
4. $u_{k-1} r_k + u_k r_{k-1} = r_0$.
5. $u_k v_n - u_n v_k = (-1)^k r_k$.

The uses for this here, beyond computing a gcd, will be for computing inverses, reconstructing rational numbers from their cosets $\mod(n)$, and finding a better alternative to the resultant of two polynomials.

	r_{i-2}	=	$q_i r_{i-1}$	+	r_i	u_i	v_i
-1					149	0	1
0					17	1	0
1	149	=	$8 \cdot 17$	+	13	8	1
2	17	=	$1 \cdot 13$	+	4	9	1
3	13	=	$3 \cdot 4$	+	1	35	4
4	4	=	$4 \cdot 1$	+	0	149	17

can be used to produce $4 \cdot 149 - 35 \cdot 17 = 1 = gcd(149, 17)$ or $1/17 = -35 = 114$ in $\mathbf{Z}_{149}$, or $17/1 \equiv 4/9 \ mod(149)$.

From the above, $\frac{1}{37} = 58$ in $\mathbf{Z_{143}}$ even though 143 is not a prime; and $\frac{5}{4} \equiv 37 \ mod \ 143$ gives a best rational equivalent in the sense that the sum of the squares of the numerator and denominator is smallest. The resultant of $y^5 + y^2(x^4 + x) + yx^2 + x^{12}$ and $y^4 + x^2$ with respect to y (also the discriminant of $y^5 + y^2(x^4 + x) + yx^2 + x^{12}$ with respect to y) in $R := \mathbf{F}_2[y, x]$ is $x \cdot x \cdot (x^{23} + x^9 + x^3) \cdot (x^{23} + x^9 + x^3)$, whereas the gcd with respect to y is merely $x^{22} + x^8 + x^2$.

The remainder of a after division by b can also be viewed as a canonical form for $a \ mod \ b$, a canonical representative for the coset $a + \langle b \rangle$.

The division algorithm itself should probably be viewed as a summary of several individual divisions, especially in the polynomial form. Each division is really of the form

$$f - \frac{LeadTerm(f)}{LeadTerm(g)} g$$

having smaller degree than that of f, with the whole division finished when the result has degree smaller than that of g as well. This is what generalizes to canonical division (by an ordered set of divisors) in multivariate polynomial rings.

The use of LeadTerm implicitly suggests that there is an ordering on the terms in a polynomial, and that it is possible to determine which is the leading (that is largest) one in that ordering. Does it make sense to write something such as $9x^2 - 3x + 7x^6$ intended to be an element of the univariate polynomial ring $\mathbf{F}[x]$? Well, yes and no. Computer algebra systems will generally accept this as an input, but most will output a more useful form, such as $7x^6 + 9x^2 - 3x$, so that the generally most useful piece of information, the leading term, is explicit and the output is in a predictable, canonical form.

2.4 Multivariable polynomial division

Consider $I := \langle yx^3 - x,\ y^3x - y\rangle$ and a possible canonical form for $f := y^4x^3 - 3y^2x^6$ modulo I.

Possible reductions by division by elements of I include:

$$f - y^3(yx^3 - x) + 3yx^3(yx^3 - x) + 3x(yx^3 - x) - 1(y^3x - y) = y - 3x^2$$

$$f + 3yx^3(yx^3 - x) - y^3(yx^3 - x) + 3x(yx^3 - x) - 1(y^3x - y) = -3x^2 + y$$

and

$$f - yx^2(y^3x - y) + 3yx^3(yx^3 - x) + 3x(yx^3 - x) = y^2x^2 - 3x^2.$$

In the form $I := \langle y - x,\ x^4 - x\rangle$,

$$f - y^3x^3(y - x) - y^2x^4(y - x) - yx^5(y - x) - x^6(y - x) + 3yx^6(y - x)$$
$$+3x^7(y - x) + 3x^4(x^4 - x) - x^3(x^4 - x) + 3x(x^4 - x) - 1(x^4 - x) = -3x^2 + x$$

or

$$f + 3y^2x^2(x^4 - x) - y^3x^3(y - x) - y^3(x^4 - x) + 3yx^3(y - x) + 3y(x^4 - x)$$
$$-y^2x(y - x) - yx^2(y - x) - x^3(y - x) - 1(x^4 - x) + 3x(y - x) = -3x^2 + x.$$

This should be enough evidence to suggest at least that the computation at each step is based on

- what the current leading term is;
- in which order the generators should be tried as divisors;
- and which set of generators should be used as divisors.

2.5 Moving beyond linear algebra

Similar methods to those for vector spaces can be used for finitely-generated modules over $\mathbf{Z}$ or even $\mathbf{F}[x]$. The ring $\mathbf{R}$ has an integral extension

$$\mathbf{R}[i]/\langle i^2+1\rangle.$$

If elements of the polynomial ring $\mathbf{R}[i]$ are written with highest degree on the left, as they would given a global monomial ordering (7), then the canonical representatives for elements of this quotient ring will be written as $bi+a$ rather than $a+bi$, and computed by division by i^2+1 to get a canonical remainder of degree less than 2. [The latter (that is, $a+bi$) would be the default when dealing with polynomials written as power series; but then there are issues with using a local monomial ordering (8), and expecting to reduce power series in i to this canonical form.]

The intent of having such a quotient ring is to view the defining relation $i^2+1=0$ in the form $i^2=-1$, meaning that computationally there is a reduction rule $i^2 \mapsto -1$ to reduce elements of $R[i]$ to canonical form modulo the ideal defining the quotient ring.

Modules over the multivariate polynomial ring $R := \mathbf{F}[x,y]$ or even ideals of R present new problems before they can be viewed this same way. Even writing elements of R takes thought. It is probably never correct to write x^3y+y^3x, in the sense that a CAS that produces canonical output would never be able to produce this relative to any monomial ordering placed on the ring. It might be correct to write either x^3y+xy^3 or y^3x+yx^3, as there are monomial orderings that would produce one or the other. In $\mathbf{F}[x,y,z]$ it could be correct to write $xz+y^2$, $zx+y^2$, y^2+xz or y^2+zx, though the two of these are less likely to be consistent with writing the variables in the order x,y,z implicit in the description of the ring.

It is possible to argue whether a ring such as $\mathbf{F}[x,y,z]$ must have a monomial ordering as part of its definition. There is no ambiguity for the CASs in use here. That is,

```
ring r=0,(x,y,z),dp;
```

defines a different ring from

```
ring r=0,(x,y,z),lp;
```

in SINGULAR, in that there must be a canonical way to write output, decide on leading terms, and the like. In fact, there is no default monomial ordering, so one must be part of the definition.

```
R=QQ[x,y,z];
```

in MACAULAY2 looks independent of a monomial ordering, but has a default grevlex one applied; whereas

```
R=QQ[x,y,z,MonomialOrder=>Lex];
```

would be a ring with a lex monomial ordering.

And similarly in MAGMA

```
R<x,y,z>:=PolynomialRing(Rationals(),3);
```

has a default lex monomial ordering, whereas

```
R<x,y,z>:=PolynomialRing(Rationals(),3,"grevlex")
```

has a grevlex one.

But once elements of a multivariate polynomial ring R have been consistently written, it is possible to start with a finite generating set for either an ideal I of R or a module M over R and produce a basis (for that ideal or module) that has the property that it is straightforward to determine whether elements of R

or R^n respectively are in the ideal I or submodule $U \in R^n$ by obvious reductions modulo the basis elements to see whether the canonical remainder is 0 or not.

As a simple example, $I := \langle\ x^3y - x,\ xy^3 - y\ \rangle$ has a Gröbner basis (14) $B := (x - y,\ y^4 - y)$.

$$f := y^5 - x^2y + xy^2 - x^2 \mapsto -x^2y + xy^2 - x^2 + y^2 \mapsto -x^2 + y^2 \mapsto -xy + y^2 \mapsto 0$$

shows that $f = y(y^4 - y) - xy(x - y) - x(x - y) - y(x - y) \in I$, whereas reduction of f to 0 relative to the given generators would not have been this straightforward.

Chapter 3

Ideals and quotient rings

Think of commutative algebra as a generalization of linear algebra in the sense that it is possible to view the latter in terms of objects of various sorts satisfying linear relations and the former in terms of objects of various sorts satisfying polynomial relations.

Multivariate polynomial rings will be denoted here by notation $R := \mathbf{F}[x_n, \ldots, x_1]$ that describes the field and the variable names (3.1). Everything here is ultimately about multivariate polynomial rings and their ideals. A general definition of an ideal is:

Definition 4. *An ideal I of a ring R is a subset of R which is closed under addition and under multiplication by ring elements. That is, if $a, b \in I$ then $a + b \in I$ and if $r \in R$ then $ra \in I$. This can be combined in one statement*

$$a_1, \ldots, a_m \in I,\ r_1, \ldots, r_m \in R \Rightarrow \sum_{i=1}^{m} r_i a_i \in I.$$

The definition of an ideal is very much like the definition of a subspace of a vector space. The similarity extends to ideals of a multivariate polynomial ring being finitely generated (13) in the same way that finite-dimensional vector spaces (and their subspaces) are finitely generated. So it should come as no surprise that there are bases for an ideal that are more important than just sets of generators; and that some bases (14) are more useful than others.

In certain rings, namely the integers, $\mathbf{Z}$, and univariate polynomial rings, $\mathbf{F}[x_1]$, all ideals are principal, meaning they are generated by a single element. This is rarely the case in multivariate polynomial rings; though below, the function field defining an algebraic curve will generally be given in the form

$$\mathbf{K} := \overline{\mathbf{F}}(x_2, x_1)/\langle f(x_2, x_1)\rangle$$

for f an irreducible polynomial relating two defining variables x_2, x_1.

In general, the ideals in a multivariate polynomial ring can be thought of as sets of relations among the variables. The notation

$$I := \langle g_1, \ldots, g_m\rangle \in R := \mathbf{F}[x_n, \ldots, x_1].$$

will mean that I is an ideal of R with generators $g_1, \ldots, g_m$.

Definition 5. *The quotient ring of a ring R and an ideal I is $A := R/I$. Its field of fractions, $Q(A)$, is the set of all fractions a/b with $a, b \in A$, $b \neq 0$, and a and b having no non-trivial common factors (which here means $\gcd(a, b) = 1$).*

Warning: Learn how elements of a quotient ring are automatically reduced in any CAS. At this moment it is still the case that in MACAULAY2

```
Macaulay2, version 1.7
R=ZZ/2[u,v,w,x,y,z];
I=ideal(x^3+x^2*y+w*y+x*z,
        v*x+u*y,
        u*x^2+v*x^2+v*w+u*z,
        x^4+v^2*x+w*x^2+x^2*y+x^2*z+x^2+w*y+w*z,
        u*x^2+w*x+u*y+u*z,
        u*v^2+w*x^2+w^2+u*x,
        x^4+v^2*y+x^2*y+x*y+y*z+z^2,
        v*x^2+v*y+w*y+v*z,
        v^3+w*x^2+v*x+w*z);
A=R/I;
K=frac(A);
x^2/y
--       (u*x)/v
u*x/v
--       (u*w+u*x+w*x+u*y+u*z)/w
(u*w+u*x+w*x+u*y+u*z)/w
--      x^2/y
```

will produce the quotient ring $A = R/I$ and field of fractions $\mathbf{K} = Q(A)$, but uses a non-canonical method to forcibly reduce them to what it thinks is a better form. As can clearly be seen these cycle, so this cannot be canonical.

The difference between an ideal I of a ring R and the corresponding quotient ring R/I defined by it, is one of focus, not just one of comparing two different types of objects, an ideal and a quotient ring. That is, $\mathbf{Z}/\langle 7\rangle$ focuses on canonical remainders after division by 7 rather than on the multiples of 7 that are the elements of the ideal. Similarly $\mathbf{R}[i]/\langle i^2+1\rangle$ focuses on the polynomial remainders after division by i^2+1, not on the multiples of i^2+1.

[This distinction is somewhat blurred in the SINGULAR examples of integral closures in that

```
ring R=0,(y,x),dp;
ideal I=y8-y2x3+2yx6-x9;
list nor=normal(I);
```

should really have been about the normalization of the quotient ring R/I instead of I. MAGMA does the same with

```
R<y,x>:=PolynomialRing(Rationals(),2,"grevlex");
I:=ideal<R|y^8-y^2x^3+2*y*x^6-x^9>;
N:=Normalisation(I);
```

But MACAULAY2 uses

```
R=QQ[y,x];
I=ideal(y^8-y^2*x^3+2*y*x^6-x^9);
A=R/I;
G=gens gb ideal integralClosure A;
```

Also SINGULAR uses

```
ring R=0,(y,x),dp;
poly f=y8-y2x3+2yx6-x9;
qring A=f;
```

to actually define a quotient ring.]

Definition 6. *The ideal defining a quotient ring of a multivariate polynomial ring can be viewed as an ideal of relations defining a set of reduction rules on the elements of the ring of the form $LT(g_i) \mapsto LT(g_i) - g_i$ (reducing the leading term $LT(g_i)$ of a relation g_i to something smaller in the monomial ordering (4)).*

This is a key idea not emphasized well enough in the literature. That is, different monomial orderings can be used to produce different reduction rules, thus emphasizing different aspects of the quotient ring.

Consider a simple example $I := \langle x_2 - x_1,\ x_1^4 - x_1\rangle$. As relations it doesn't matter whether we write $x_2 - x_1 = 0$, $x_1 - x_2 = 0$, or even $x_2 = x_1$; similarly it doesn't matter whether we write $x_1^4 - x_1 = 0$, $x_1 - x_1^4 = 0$, or $x_1^4 = x_1$. But in terms of reduction rules, it matters whether $x_2 \mapsto x_1$ or $x_1 \mapsto x_2$, and whether $x_1^4 \mapsto x_1$ or $x_1 \mapsto x_1^4$. A monomial ordering forces a decision as to which reduction should occur, and different monomial orderings may force different reductions. The takeaway from that is that a default monomial ordering may force reductions different from those intended.

As an example, in an R-algebra the multiplication in the R-module $R\langle y_m,\ldots,y_1\rangle$ would be given by reduction rules $y_iy_j \mapsto \sum_k a_{i,j,k}y_k$. This corresponds to an ideal of relations

$$I := \left\langle y_iy_j - \sum_k a_{i,j,k}y_k \ :\ 0 \le i \le j \le m \right\rangle,$$

and the R-algebra $R[y_m,\ldots,y_1]/I$. The reduction rules emphasize that the elements of this R-algebra form an R-module with all its elements necessarily of the form $\sum_k a_{i,j,k}y_k$, since any products can be reduced.

A grevlex monomial ordering might produce these reduction rules, whereas a lex monomial ordering might not.

In a finite field such as $\mathbf{F}_{16} := \mathbf{F}_2[a]/\langle a^4 + a + 1\rangle$, the reduction rule $a^4 \mapsto a + 1$ emphasizes the fact that any element can be written canonically as a polynomial in a of degree less than 4. It is not so easy to emphasize that any non-zero element can be written as a power of a.

[If $A := \mathbf{F}[y, x]/\langle y^3 + yx + x^5\rangle$, and $z := y^2/x$ is an element of its field of fractions needed to define an overring $B := \mathbf{F}[z, y, x]/J$ for some ideal (of relations) J, should J have a monomial ordering that corresponds to the reduction rule $z \mapsto y^2/x$ or one that corresponds to the redcution rule $y^2/x \mapsto z$? Even if it is necessary to use polynomial versions of these, such as $zx \mapsto y^2$ or $y^2 \mapsto zx$, it would seem that the former would be there to replace z by the rational function y^2/x, whereas the latter would be there to let z replace the rational function y^2/x. Probably the intent of introducing a new variable was to do the latter.

This is a common problem in integral closure code, wherein a default product monomial ordering on the output implicitly produces the former, viewing $zx - y^2 = 0$ as an A-linear relation.]

3.1 Code

The MAGMA code

```
R<x2,x1>:=PolynomialRing(Rationals(),2);
I:=ideal<R|x2^3*x1-x2,x2*x1^3-x1>;
G:=GroebnerBasis(I);G;
```

sets up a multivariate polynomial ring R over $\mathbf{Q}$, with two variables and a default lex monomial ordering (9). Then it defines an ideal I of R generated by two polynomials. Finally it computes a minimal, reduced Gröbner basis for it, and outputs that.

MACAULAY2 code for this is

```
R=QQ[x2,x1, MonomialOrder=>Lex];
I=ideal(x2^3*x1-x2,x2*x1^3-x1);
G=gens gb I
```

since the default ordering is grevlex (10), not lex.

SINGULAR code for this is

```
ring R=0,(x2,x1), lp;
ideal I=x2^3*x1-x2,x2*x1^3-x1;
option(redSB);
ideal s=std(I);s;
```

since there is no default ordering.

Note especially that there is a global monomial ordering (7) in each case so that the CAS knows how to write output algorithmically, or interpret input algorithmically. The non-standard numbering here is to emphasize that $x_n \succ \cdots \succ x_1$.

Chapter 4

Monomial orderings and Gröbner bases

To learn how to write polynomials correctly, start with an example in one variable.

Is it a good idea to write $4x^2 + 7x^3 + 9x^5 + 5x^8$, $5x^8 + 9x^5 + 7x^3 + 4x^2$, or $9x^5 + 7x^3 + 5x^8 + 4x^2$? The first is suggestive of a local ordering in which $1 \succ x \succ x^2 \cdots$; the second, a global ordering in which $\cdots \succ x^2 \succ x \succ 1$; and the third probably of nothing in particular about writing polynomials in a particularly nice mathematical way, certainly not by ordering the coefficients. The first two suggest that there is a total ordering. They also might suggest that there is a well-ordering. Maybe the property that multiplication by x^k doesn't affect the ordering is not so clear; but once suggested is an obvious property to be expected.

Given that the third above should be discarded, is there any mathematical reason to prefer the first or the second? Perhaps the second reflects the way polynomials are generally written as polynomials, whereas the first reflects how they might be generally written as finite power series. So the choice here will be somewhat equivocal, siding for the second, while occassionally opting for the first, depending on the context.

Definition 7. *The binary operation $\succ$ on the monomials of $R := \mathbf{F}[x_n, \ldots, x_1]$ is a global monomial ordering iff*

1. *$\succ$ is a total ordering, (meaning any two monomials can be compared);*
2. *$\succ$ is a well-ordering, (meaning there is no infinite descending sequence of monomials);*
3. *$\underline{x^{\alpha}} \succ \underline{x^{\beta}}$ implies that $\underline{x^{\alpha+\gamma}} \succ \underline{x^{\beta+\gamma}}$ for any $\underline{\gamma} \in \mathbf{N}^n$. (In particular 1 is a minimum monomial.)*

Definition 8. *The binary operation$\prec$ on the monomials of $R := \mathbf{F}[x_n, \ldots, x_1]$ is a local monomial ordering iff*

1. *$\succ$is a total ordering;*
2. *$\succ$is a well-ordering, (meaning there is no infinite ascending sequence of monomials);*
3. *$\underline{x^{\alpha}} \succ \underline{x^{\beta}}$ implies that $\underline{x^{\alpha+\gamma}} \succ \underline{x^{\beta+\gamma}}$ for any $\underline{\gamma} \in \mathbf{N}^n$. (In particular 1 is a maximum monomial.)*

The most commonly used global monomial orderings are:

Definition 9.

$$\underline{x^{\alpha}} \succ_{lex} \underline{x^{\beta}}$$

iff $\alpha_i = \beta_i$ for all $i < j$ but $\alpha_j > \beta_j$.

Definition 10.

$$\underline{x}^{\underline{\alpha}} \succ_{grevlex} \underline{x}^{\underline{\beta}}$$

iff $(\sum_i \alpha_i > \sum_i \beta_i)$ *or* $(\sum_i \alpha_i = \sum_i \beta_i,\ \alpha_i = \beta_i$ *for all* $i > j$ *but* $\alpha_j < \beta_j)$.

Definition 11. *Let* M *be an* $n \times n$ *matrix with entries from* $\mathbf{N}$*, non-singular over* $\mathbf{Q}$*. Then*

$$\underline{x}^{\underline{\alpha}} \succ_{matrix} \underline{x}^{\underline{\beta}}$$

iff $M\underline{\alpha}^T \succ_{lex} = M\underline{\beta}^T$.

In computer algebra packages monomials are written left-most ring variable first; so writing $x^2 - y = 0$ has a completely different intent than writing $y - x^2 = 0$. And generalizing writing affine coordinates (x_1, x_2) to writing projective coordinates $(x_0 : x_1 : x_2)$ doesn't quite make x_0 seem to be the least important variable. The point of this is that it is more likely that the intent in general is to reduce x_ns rather than reduce x_1s, hence the choice of x_n as the left-most variable and x_1 the right-most.

Solving systems of polynomial equations is usually done by using a lex monomial ordering (9), elimination (32), and extension (33), discussed later on. Finding Gröbner bases (14), also discussed later, is usually easier with an ordering in which every decreasing sequence of monomials is finite; so by using a variant of a grevlex monomial ordering (10) instead of lex. Product orderings can come about when the polynomial ring is a universal object, meant to deal with several forms of the same problem at the same time. Computer algebra functions often use default monomial orderings for various reasons, some to make the function applicable to the widest range of input, some seemingly to make programming easier, without thinking about the theoretical consequences.

Note While there are global monomial orderings not given by non-singular $n \times n$ matrices with entries from $\mathbf{N}$, it seems to be standard practice to settle for these only. There is often theoretical interest in having different monomials have the same order after the first m tests of the monomial ordering, only being differentiated by the further tests that make up the total ordering.

Indeed it seems rare that something other than lex, grevlex or products thereof are used, though allowing the top row of M to be a set of weights is common in algebra packages. [Monomial orderings with m rows of weights should be used routinely when dealing with rings having m independent variables, though they seem only to be used by me.]

Not only do monomial orderings give a canonical way to write polynomials, they provide information for various algorithms that are based on the way polynomials are written. So define

Definition 12. *The leading monomial* $\underline{x}^{\underline{\alpha}}$*, leading coefficient* $c_{\underline{\alpha}}$*, and leading term* $c_{\underline{\alpha}}\underline{x}^{\underline{\alpha}}$ *of* $f := \sum_{\underline{\beta}} c_{\underline{\beta}}\underline{x}^{\underline{\beta}} \in \overline{\mathbf{F}}[\underline{x}]$ *are self-defining terms dependent on the global monomial ordering chosen.*

Use the notation $LM_{ord}(f)$, $LC_{ord}(f)$, $LT_{ord}(f)$ for these to emphasize the specific order, or just $LM(f)$, $LC(f)$, $LT(f)$ when it is safe to suppress the ordering in a given context. [The adjective trailing will replace leading when local monomial orderings are being used.]

Starting with polynomial rings in three variables, there is a difference in writing $x_1x_3 + x_2^2$ and $x_2^2 + x_1x_3$; the former possibly relative to lex $x_1 \succ x_2 \succ x_3$ and the latter possibly relative to grevlex $x_1 \succ x_2 \succ x_3$. One has leading term x_1x_3, the other x_2^2. Various algorithms rely on $LT(f)$ and/or its relation to the rest of f, namely $f - LT(f)$. Such algorithms are necessarily order-dependent.

4.1 Finitely-generated ideals and modules

Theorem 13 (Dickson's Lemma)**.** *Let $\emptyset \neq V \subset \mathbf{N}^n$. Then there is a finite subset $B \subset V$ such that for every $\underline{v} := (v_1, \ldots, v_n) \in V$ there is an element $\underline{b} := (b_1, \ldots, b_n) \in B$ that dominates it in the sense that $b_i \leq v_i$ for $1 \leq i \leq n$.*

Proof. (by induction on n) For $n = 1$, let $b := min\{v \ : \ v \in V\}$. Then $B := \{b\}$. For $n > 1$, define

$$V^* := \{(v_1, \ldots, v_{n-1}) \in \mathbf{N}^{n-1} \ : \ (v_1, \ldots, v_{n-1}, v_n) \in V\}.$$

By induction there is a finite $B^* \in V^*$ that dominates it. For each $(b_1, \ldots, b_{n-1}) \in B^*$ define $b_n := min\{b \ : (b_1, \ldots, b_{n-1}, b) \in V\}$; and $B^{**} := \{(b_1, \ldots, b_{n-1}, b_n) \ : \ (b_1, \ldots, b_{n-1}) \in B^*\}$. Then B^{**} dominates all those elements of V with $v_n \geq m := max\{b_n \ : \ (b_1, \ldots, b_n) \in B^{**}\}$. For each $0 \leq j < m$ define

$$V_j := \{(v_1, \ldots, v_{n-1}) \ : \ (v_1, \ldots, v_{n-1}, j) \in V\}.$$

Then again by induction there is a finite set B_j that dominates this. And $B_j^* := \{(b_1, \ldots, b_{n-1}, j) \ : (b_1, \ldots, b_{n-1}) \in B_j\}$ dominates V_j. So $B := B^{**} \cup_{j=0}^{m-1} B_j^*$ dominates all of V. ∎

4.2 Division, reduction, and Gröbner bases

Consider the ideal $I := \langle\, x_2^3 + x_2x_1 + x_1^5 \,\rangle$ of the ring $\overline{\mathbf{F}}[x_2, x_1]$ (related to the Klein quartic (13.1)), and the corresponding quotient ring $A := R/I$. Reduction modulo I is done by division by $x_2^3 + x_2x_1 + x_1^5$, either to determine whether elements of R are in I or to compute canonical forms of elements of A. So there is a reduction rule (6) corresponding to this division. This could be $x_2^3 \mapsto -x_2x_1 - x_1^5$ or $x_1^5 \mapsto -x_2^3 - x_2x_1$ or... depending on the monomial ordering chosen for R.

This should be very important theoretically. If lex $x_2 \succ x_1$ is chosen, then the reduction rule (6) is $x_2^3 \mapsto -x_2x_1 - x_1^5$. This highlights that A is an $\overline{\mathbf{F}}[x_1] - algebra$ with module basis $(1, x_2, x_2^2)$. If lex $x_1 \succ x_2$ is chosen, then the reduction rule is $x_1^5 \mapsto -x_1x_2 - x_2^3$, which highlights A being an $\overline{\mathbf{F}}[x_2] - algebra$ with module basis $(1, x_1, x_1^2, x_1^3, x_1^4)$.

The element $x_3 := x_2^2/x_1$ is integral over A since $x_3^2 + x_3 + x_2x_1^3 = 0$. In fact it is integral over $\overline{\mathbf{F}}[x_1]$ since $x_3^3 + x_3 + x_1^7 = 0$. The integral closure $\overline{A}$ of A in its field of fractions, $Q(A)$, can be written as $\overline{A} = \overline{\mathbf{F}}[x_3, x_2, x_1]/\overline{I}$, with at least the two choices

$$\overline{I} := \langle\, x_3^2 + x_3 + x_2x_1^3,\ x_3x_2 + x_2 + x_1^4,\ x_3x_1 - x_2^2,\ x_3^3 + x_3x_1 + x_1^5 \,\rangle$$

$$\overline{I} := \langle\, x_3^2 + x_3 + x_2x_1^3,\ x_3x_2 + x_2 + x_1^4,\ x_2^2 - x_3x_1 \,\rangle$$

The former has the reduction rule $x_3x_1 \mapsto x_2^2$, while the latter has reduction rule $x_2^2 \mapsto x_3x_1$. The latter has the advantage of highlighting that $\overline{A}$ is an $\overline{\mathbf{F}}[x_1] - algebra$ with module basis $(1, x_2, x_3)$. The advantage of the former is that it has an explicit copy of A as a subring, and that $\overline{A}$ is an $A - algebra$ with basis $(1, x_3)$.

The standard monomials in the former are x_1^k, $x_2x_1^k$, and $x_3x_1^k$, $k \geq 0$; in the latter, x_1^k, $x_2x_1^k$, $x_2^2x_1^k$, $k \geq 0$ and x_3.

Definition 14. *A generating set $B := \{b_1, \ldots, b_s\}$ for the ideal $I := \langle b_1, \ldots, b_s \rangle$ of $\mathbf{F}[x_n, \ldots, x_1]$ that it generates is called a Gröbner basis iff for every $f \in I$ there exists at least one $b_i \in B$ such that $LM(b_i) \mid LM(f)$. B is minimal iff $LM(b_i) \mid LM(b_j)$ iff $i = j$; and reduced iff $LM(b_i)$ doesn't divide any monomial of b_j for $i \neq j$.*

Theorem 15. *If $B := \{b_1, \ldots, b_s\}$ is a minimal Gröbner basis for I ordered so that $LM(b_1) \prec \cdots \prec LM(b_s)$ and $f \in I$ then f has a canonical form*

$$f = \sum_{i=0}^{N} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)}$$

with $LM(b_{j(k+1)})$ minimal such that $LM(b_{j(k+1)}) \mid LM(f - \sum_{i=0}^{k} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)})$.

Proof. This follows from the division algorithm, the fact that f is an R-linear combination of the basis elements and that there is a choice $LM(b_{j(k+1)}) \mid LM(f - \sum_{i=0}^{k} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)})$ because the latter term is an element of I and B is a Gröbner basis. □

Corollary 16. *If $B := \{b_1, \ldots, b_s\}$ is a Gröbner basis for $I \neq R$ and $f \in R$ then f has a canonical form*

$$f = \sum_{i=0}^{N} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)}$$

with $LM(b_{j(k+1)})$ minimal such that $LM(b_{j(k+1)}) \mid LM(f - \sum_{i=0}^{k} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)})$ (or $b_{j(k+1)} = 1$ if no such element of B exists).

Definition 17. *In the above,* $\underline{x}^{\underline{\alpha}(0)} b_{j(0)}$ *is called the signature of* f *(relative to* B*);*

$$\sum \{c_i \underline{x}^{\underline{\alpha}(i)} \ : \ b_{j(i)} = 1\}$$

is called the remainder of f *(after division by* I*).*

As an example, $B := \{x_2 - x_1^2,\ x_3 - x_1^3\}$ is a lex $x_3 \succ x_2 \succ x_1$ Gröbner basis. To find a grevlex $x_3 \succ x_2 \succ x_1$ one start with $g_1 := x_1^2 - x_2$ and $g_2 := x_1^3 - x_3$. Then $1g_2 - x_1 g_1 - g_3 = 0$ for $g_3 := x_2 x_1 - x_3$. $x_1 g_3 - x_2 g_1 - g_4 = 0$ for $g_4 := x_2^2 - x_3 x_1$; and $x_1 g_4 - x_2 g_3 + x_3 g_1 = 0$.

So $\{g_1, g_2, g_3, g_4\}$ is a Gröbner basis, but $\{g_1, g_3, g_4\}$ is a minimal, reduced Gröbner basis.

There is an alternative signature-based computation:

$$1 \cdot g_2 - x_1 g_1 = x_2 x_1 - x_3$$

$$(x_1 \cdot g_2 - x_1^2 g_1) - x_2 g_1 = x_2^2 - x_3 x_1$$

There is no need to reduce $x_1^2 \cdot g_2$.

Algorithms for both, called herein a Buchberger syzygy algorithm and a Faugère syzygy algorithm, are in the section on syzygies in R-modules (5.4).

Chapter 5

R-modules, syzygies, and Gröbner bases

5.1 Names versus variables

Start with a vector space example. Suppose $V_1 := (1,1,1,2,3)$, $V_2 := (2,0,1,-1,2)$, $V_3 := (-1,3,1,8,5)$, and $V_4 := (5,-3,1,-10,-1)$ are vectors in $\mathbf{Q}^5$, and that we want to describe all the $\mathbf{Q}$-linear dependencies among them. This could be done by using the notation $\mathbf{Q}\langle V_4, V_3, V_2, V_1\rangle$ to denote the $\mathbf{Q}$-module generated by V_4, V_3, V_2, V_1, and then the notation $\mathbf{Q}\langle V_3 + 2V_2 - 3V_1,\ V_4 - 4V_2 + 3V_1\rangle$ to describe the submodule of all such dependencies. But absent V_1 being an element of something, it is just a shorthand notation for input that gets replaced by its defined value $(1,1,1,2,3)$ when processed. In particular V_1 should not be expected to be seen as output in this latter case. In the former, wherein evaluation is not done, it is then necessary to use the definitions to describe a $\mathbf{Q}$-module map $ev : \mathbf{Q}\langle V_4, V_3, V_2, V_1\rangle \to \mathbf{Q}^5$ to do the evaluation. Of course a matrix such as $M := \begin{pmatrix} 0 & 1 & 2 & -3 \\ 1 & 0 & -4 & 3 \end{pmatrix}$ could be used to describe

$$M \begin{pmatrix} V_4 \\ V_3 \\ V_2 \\ V_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad M \begin{pmatrix} 5 & -3 & 1 & -10 & -1 \\ -1 & 3 & 1 & 8 & 5 \\ 2 & 0 & 1 & -1 & -2 \\ 1 & 1 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This could conceivably have been computed as a list of row-reductions:

$$\left(\begin{array}{rrrrr||rrrr} 1 & 1 & 1 & 2 & 3 & 0 & 0 & 0 & 1 \\ 2 & 0 & 1 & -1 & 2 & 0 & 0 & 1 & 0 \\ 0 & -2 & -1 & -5 & -4 & 0 & 0 & 1 & -2 \\ -1 & 3 & 1 & 8 & 5 & 0 & 1 & 0 & 0 \\ 0 & 4 & 2 & 10 & 8 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & -3 \\ 5 & -2 & 1 & -10 & -1 & 1 & 0 & 0 & 0 \\ 0 & -8 & -4 & -20 & -8 & 1 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -4 & 3 \end{array}\right)$$

5.2 Finite-dimensional R-modules

Let $M := R\langle G_s, \ldots, G_1\rangle$ be a finitely-generated R-module, for $R := \mathbf{F}[x_n, \ldots, x_1]$ with monomial ordering $\succ_R$. There are two standardly defined R-module orderings, designated TOP and POT for term-over-position and position-over-term respectively, suggestive of the definitions:

Definition 18. $\underline{x^\alpha} G_i \succ_{TOP} \underline{x^\beta} G_j$ *iff* $\underline{x^\alpha} \succ_R \underline{x^\beta}$ *or* $\underline{x^\alpha} = \underline{x^\beta}$ *and* $i < j$.

Definition 19. $\underline{x^\alpha} G_i \succ_{POT} \underline{x^\beta} G_j$ *iff* $i < j$ *or* $i = j$ *and* $\underline{x^\alpha} \succ_R \underline{x^\beta}$.

An element of M written as

$$h := \sum_{i=0}^{N} c_i \underline{x^{\alpha(i)}} G_{j(i)}$$

with $c_i \in \mathbf{F}$ and $\underline{x^{\alpha(i)}} G_{j(i)} \succ \underline{x^{\alpha(i+1)}} G_{j(i+1)}$ has signature $\underline{x^{\alpha(0)}} G_{j(0)}$. This is akin to a leading monomial of a polynomial in R. So it should be no surprise that submodules are finite-dimensional and have Gröbner bases with elements having signatures $\underline{x^\alpha} G_j$ dividing the signatures $\underline{x^{\alpha(0)}} G_{j(0)}$ of the elements of the submodule.

5.3 Ideals of R as R-modules

Let $I := \langle g_s, \ldots, g_1\rangle$ with $LM(g_s) \succ \cdots \succ LM(g_1)$ be an ideal of $R := \mathbf{F}[x_n, \ldots, x_1]$. Writing

$$f = \sum_{j=1}^{s} r_j g_j,\ r_j \in R$$

is meant to emphasize that any $f \in I$ is an R-linear combination of the given generators $g_s, \ldots, g_1$.

While a sum such as $\sum_{j=1}^{s} r_j g_j$ is evaluated in R as an element f, an element f is not evaluated in R as a sum $\sum_{j=1}^{s} r_j g_j$. So the question is whether there is a canonical sum corresponding to $f \in I$; and if so, how to compute it.

To get control over evaluation consider defining an R-module $M := R\langle G_s, \ldots, G_1\rangle$, with explicit R-linear evaluation map

$$ev\ :\ M \to R,\ ev(G_i) := g_i \text{ for } 1 \le i \le s.$$

The reason to have seemingly two different names, G_i and g_i, for the same object is that the latter, as above in the vector space example, is shorthand that gets evaluated as an element of R, whereas the former, an element of M, does not get evaluated (as an element of R) until the evaluation map is applied. That allows for the explicit writing of (unevaluated) R-linear combinations as elements of M as separate objects from (evaluated) R-linear combinations as elements of R.

[As a note, it may be easier to view the R-module $M := R\langle G_s, \ldots, G_1\rangle$ as a ring $S := R[G_s, \ldots, G_1]$ flattened to $\mathbf{F}[x_n, \ldots, x_1, G_s, \ldots, G_1]$ with an appropriate induced monomial ordering; then either avoid multiplication by any G_i or mod out by the ideal generated by the relations $G_i G_j - g_i G_j$.]

But for treating an ideal $I \in R$ as an R-module M, there is a natural (Schreyer) module ordering based on $ev(G_i) = g_i$ not available when the R-module generators don't correspond to ring elements.

Definition 20.

$$\underline{x^\alpha} G_i \succ_{Sch} \underline{x^\beta} G_j$$

iff

$$\underline{x^\alpha} LM(g_i) \succ_R \underline{x^\beta} LM(g_j)$$

or

$$\underline{x^\alpha} LM(g_i) = \underline{x^\beta} LM(g_j) \text{ and } LM(g_i) \succ_R LM(g_j).$$

This requires that the leading monomials $LM(g_i)$ be distinct so that it is a total ordering. It can be used on a fixed ordered set of generators.

Now instead of writing $f = \sum_{j=1}^{s} r_j g_j,\ r_i \in R$, the choice will be to write elements of M as

$$F := \sum_{i=0}^{N} c(i)\underline{x}^{\underline{\alpha}(i)} G_{j(i)},\ c(i) \in \mathbf{F}$$

with $\underline{x}^{\underline{\alpha}(i)} G_{j(i)} \succ_{Sch} \underline{x}^{\underline{\alpha}(i+1)} G_{j(i+1)}$, having values

$$ev(F) = \sum_{i=0}^{N} c(i)\underline{x}^{\underline{\alpha}(i)} g_{j(i)} \in R$$

Definition 21. *Given*

$$F := \sum_{i=0}^{n(F)} c(F,i)\underline{x}^{\underline{\alpha}(F,i)} G_{j(F,i)}$$

with $c(F,i) \in R$ *and* $\underline{x}^{\underline{\alpha}(F,i)} G_{j(F,i)} \succ_{Sch} \underline{x}^{\underline{\alpha}(F,i+1)} G_{j(F,i+1)}$, *define*

$$\underline{x}^{\underline{\alpha}(F,0)} G_{j(F,0)}$$

to be the signature $sig(F)$ *of* F *and*

$$ev(F) = \sum_{i=0}^{n} c(F,i)\underline{x}^{\underline{\alpha}(F,i)} g_{j(F,i)}$$

(*with* ev *the evaluation map*) *the value of* F.

5.4 Syzygies

Definition 22. *R-linear dependencies are called R-syzygies or just syzygies if the polynomial ring R is implicit.*

Definition 23. *For the ideal $I := \langle g_s, \ldots, g_1 \rangle \in R := \mathbf{F}[x_n, \ldots, x_1]$ with $LM(g_s) \succ_R \cdots \succ_R LM(g_1)$, the syzygy module $Syz(I)$ is the sub-module of the R-module $M := R\langle G_s, \ldots G_1 \rangle$ of all syzygies, that is elements with value 0.*

Consider the Gröbner basis algorithms of Faugère and Buchberger types as algorithms to compute $Syz(I)$ as a submodule of $M_s := R\langle G_s, \ldots G_1 \rangle$ or $M_N := R\langle G_N, \ldots G_1 \rangle$ respectively, by producing syzygies with minimal signatures. (This is not new in the sense that the syzygy module is mentioned often in the literature; but to commit to these algorithms being primarily syzygy algorithms rather than primarily Gröbner basis algorithms gives a different perspective on what is being computed and why.)

The Faugère strategy is to compute minimal R-linear combinations relative to the given $G_s, \ldots, G_1$ in increasing order of the signatures of those combinations, with those having value 0 corresponding to syzygies. These syzygies necessarily have minimal signatures.

The Buchberger strategy is to do the same to get a sygyzy among to current list of generators when the value is 0; or to append a new module variable with value equal to the value when that value is not 0 to get a syzygy among a larger set of module variables, at the expense of enlarging the R-module when this is necessary. The syzygies found have minimal signatures at the time they are found; but can be discarded later if their signatures are divisible by the signature of a subsequently found syzygy.

The Faugère approach probably starts with versions of Faugère, J.-C., "A new efficient algorithm for computing Gröbner bases without reduction to zero: F5", July 2002, (though I happen to have only the 2004 version.)

Buchberger's approach probably probably dates from his thesis in 1965, but Buchberger, B. "Groebner bases: an algorithmic method in polynomial ideal theory", Multidimensional Systems Theory, pp 184-232, 1985 might be more accessible as an early reference. However, this can be found in any basic text on commutative algebra.

The following syzygy versions of such algorithms as opposed to the more common view as Gröbner basis algorithms, is meant to explain what both algorithms actually produce, in particular to explain why there should be many so-called unnecessary computations.

5.5 A Faugère syzygy algorithm

Let $g_{\underline{\delta}}$ be notation meaning that $LM(g_{\underline{\delta}}) = \underline{x}^{\underline{\delta}}$. Given generators $g_{\underline{\delta}(j)}$ with $1 \leq j \leq s$ and $\underline{x}^{\underline{\delta}(j)} \prec \underline{x}^{\underline{\delta}(j+1)}$, for an ideal I of $R := \mathbf{F}[x_n, \ldots, x_1]$, define the R-module $M := R\langle G_{\underline{\delta}(s)}, \ldots, G_{\underline{\delta}(1)}\rangle$ and the evaluation map $ev : M \to R$ with $ev(G_{\underline{\delta}(j)}) := g_{\underline{\delta}(j)}$. Let $F_{\underline{\alpha},\underline{\beta}} \in M$ be notation meaning $sig(F_{\underline{\alpha},\underline{\beta}}) = \underline{x}^{\underline{\alpha}} G_{\underline{\beta}}$. and

$$F_{\underline{\alpha},\underline{\beta}} = \sum_{i=0}^{N} c_i \underline{x}^{\underline{\alpha}(i)} G_{\underline{\beta}(i)},\ c_i \in \mathbf{F},\ c_0 = 1,\ sig\left(\underline{x}^{\underline{\alpha}(i)} G_{\underline{\beta}(i)}\right) \succ sig\left(\underline{x}^{\underline{\alpha}(i+1)} G_{\underline{\beta}(i+1)}\right).$$

A Faugère canonical reduction is $\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}$ with $a_j \in \mathbf{F}$, $a_0 = 1$,

$$ev\left(\sum_{j=0}^{k-1} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) \succ ev\left(\sum_{j=0}^{k} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right),\ sig\left(\sum_{j=0}^{k-1} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) = sig\left(\sum_{j=0}^{k} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right),$$

and $sig(F_{\underline{\alpha}(k),\underline{\beta}(k)})$ minimum subject to these conditions.

Start with $F_{\underline{0},\underline{\delta}(i)} := G_{\underline{\delta}(i)}$ for $1 \leq i \leq s$. Then recursively compute canonical reductions for non-canonical elements with minimum signatures as long as there are such non-canonical elements to be reduced.

If $ev\left(\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) = 0$, then append $\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}$ to the list of (minimal) syzygies; otherwise append $ev\left(\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right)$ to the list of generators of I.

5.6 A Buchberger syzygy algorithm

Let $g_{\underline{\delta}}$ be notation meaning that $LM(g_{\underline{\delta}}) = \underline{x}^{\underline{\delta}}$. Given generators $g_{\underline{\delta}(j)}$ with $1 \leq j \leq s$ and $\underline{x}^{\underline{\delta}(j)} \prec \underline{x}^{\underline{\delta}(j+1)}$, for an ideal I of $R := \mathbf{F}[x_n, \ldots, x_1]$, define the R-module $M := R\langle G_{\underline{\delta}(s)}, \ldots, G_{\underline{\delta}(1)}\rangle$ and the evaluation map $ev : M \to R$ with $ev(G_{\underline{\delta}(j)}) := g_{\underline{\delta}(j)}$.

A Buchberger canonical reduction is $\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}$ with $a_j \in \mathbf{F}$, $a_0 = 1$,

$$ev\left(\sum_{j=0}^{k-1} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) \succ ev\left(\sum_{j=0}^{k} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right).$$

Start with $F_{\underline{0},\underline{\delta}(i)} := G_{\underline{\delta}(i)}$ for $1 \leq i \leq s$. Then recursively compute canonical reductions for non-canonical elements as long as there are non-canonical elements to be reduced.

If $ev\left(\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) = 0$, then append $\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}$ to the list of (minimal) syzygies; otherwise append a new module variable name $G_{\underline{\delta}}$ with $ev\left(G_{\underline{\delta}}\right) := ev\left(\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right)$ and append $\left(\sum_{j=0}^{N} a_j \underline{x}^{\underline{\gamma}(j)} F_{\underline{\alpha}(j),\underline{\beta}(j)}\right) - G_{\underline{\delta}}$ to the list of syzygies (among the whole list of generators).

[Note that this is harder to implement correctly in syzygy form in that the module must be augmented every time a new element is introduced. So it is easier to produce syzygies as input in the original ring; and if they need to be output, use the final module, with definitions of the Gröbner basis elements providing the evaluation map or write sums of products as sequences of ring element,generator pairs to avoid evaluation.]

5.7 Example 1

Consider the following example with $I := \langle g_{022},\ g_{112},\ g_{121}\rangle \subset R := \mathbf{F}[x,y,z]$ with the grevlex monomial ordering, $x \succ y \succ z$, for $g_{121} := xy^2z - 1$, $g_{112} := xyz^2 - yz^2$, and $g_{022} := y^2z^2 - z$.

In the Faugère approach, the computations could be written as follows.

$$F_{000,022} := 1 \cdot G_{022}$$

$$ev(F_{000,022}) = y^2z^2 - z$$

$$F_{000,112} := 1 \cdot G_{112}$$

$$ev(F_{000,112}) = xyz^2 - yz^2$$

$$F_{000,121} := 1 \cdot G_{121}$$

$$ev(F_{000,121}) = xy^2z - 1$$

$$F_{010,112} := y \cdot F_{000,112} - x \cdot F_{000,022} + 1 \cdot F_{000,002} = y \cdot G_{112} - x \cdot G_{022} + 1 \cdot G_{022}$$

$$ev(F_{010,112}) = xz - z$$

$$F_{001,121} := z \cdot F_{000,121} - y \cdot F_{000,112} - 1 \cdot F_{000,022} = z \cdot G_{121} - y \cdot G_{112} - 1 \cdot G_{022}$$

$$ev(F_{001,121}) = 0$$

$$F_{021,112} := yzF_{010,112} - F_{000,112} = y^2z \cdot G_{112} - xyz \cdot G_{022} + yz \cdot G_{022} - 1 \cdot G_{112}$$

$$ev(F_{021,112}) = 0$$

$$F_{030,112} := y^2F_{010,112} - 1 \cdot F_{000,121} = y^3 \cdot G_{112} - xy^2G_{022} + y^2 \cdot G_{022} + G_{022}$$

$$ev(F_{030,112}) = -y^2z + 1$$

$$F_{130,112} := x \cdot F_{030,112} + 1 \cdot F_{000,121} = xy^3 \cdot G_{112} - x^2y^2 \cdot G_{022} + xy^2 \cdot G_{022} + x \cdot G_{121} + 1 \cdot G_{121}$$

$$ev(F_{130,112}) = x - 1$$

This produces

$$syz(I) = \langle z \cdot G_{121} - y \cdot G_{112} - 1 \cdot G_{022},\ y^2z \cdot G_{112} - xyz \cdot G_{022} + yz \cdot G_{022} - 1 \cdot G_{112}\rangle$$

using only the original generators $G_{022}, G_{112}, G_{121}$, with a Gröbner basis

$$(y^2z^2 - z,\ xyz^2 - yz^2,\ xy^2z - 1,\ xz - z,\ -y^2z + 1,\ x - 1)$$

consisting of the non-zero values produced, as a byproduct of the syzygy computation.

The sub-module generators found are necessarily minimal, but possibly not reduced. They do provide for a way of computing a minimal R-linear combination of the original generators for any $f \in I$ by first dividing f by the Gröbner basis elements and replacing each divisor by the corresponding preimage, then reducing that relative to $syz(I)$ to make it canonical.

The Buchberger approach might be written as follows.

$$g_{022} := y^2z^2 - z$$

$$g_{112} := xyz^2 - yz^2$$

$$g_{121} := xy^2z - 1$$

$$y \cdot g_{112} - x \cdot g_{022} + 1 \cdot g_{022} - 1 \cdot g_{101} = 0,\ g_{101} := xz - z$$

$$1 \cdot g_{112} - yz \cdot g_{101} = 0$$

$$1 \cdot g_{121} - y^2 \cdot g_{101} - 1 \cdot g_{021} = 0,\ g_{021} := y^2z - 1$$

$$1 \cdot g_{022} - z \cdot g_{021} = 0$$

$$x \cdot g_{021} - y^2 \cdot g_{101} - 1 \cdot g_{021} - 1 \cdot g_{100} = 0,\ g_{100} := -x + 1$$

$$1 \cdot g_{101} + z \cdot g_{100} = 0$$

$$x \cdot g_{021} - y^2z \cdot g_{100} - 1 \cdot g_{021} + 1 \cdot g_{100} = 0$$

In $R\langle G_{121},\ G_{112},\ G_{022},\ G_{021},\ G_{101},\ G_{100}\rangle$, reducing the syzygies corresponding to the above gives a form of $syz(I)$ with

$$G_{121} + y^2z \cdot G_{100} - 1 \cdot G_{021},\ G_{112} + yz^2 \cdot G_{100},\ G_{022} - z \cdot G_{021},\ G_{101} + z \cdot G_{100}$$

describing $G_{121},\ G_{112},\ G_{022},\ G_{101}$ in terms of $G_{021},\ G_{100}$; and

$$x \cdot G_{021} + y^2z \cdot G_{100} - 1 \cdot G_{021} - 1 \cdot G_{100}$$

the only syzygy (and principal at that) relative to the minimal, reduced Gröbner basis $(-x + 1,\ y^2z - 1)$.

Again there is a canonical representation for any $f \in I$ gotten by division by the Gröbner basis elements, replacement of the basis elements by their preimages, and reduction modulo $syz(I)$ to get a canonical form.

5.8 Buchberger syzygy algorithm code

This is MAGMA code for a Buchberger syzygy algorithm, used to produce some of the output in the examples.

```
//////////////////////////////////////////////////////
//aliases/////////////////////////////////////////////
//////////////////////////////////////////////////////
LM:=function(f) return LeadingMonomial(f); end function;
LT:=function(f) return LeadingTerm(f); end function;
REM:=function(f,g) return NormalForm(f,[g]); end function;
//////////////////////////////////////////////////////
///R-module ordering ////////////////////////////////
//////////////////////////////////////////////////////
C:=function(f,g)
   if (f[1]*LM(f[2]) gt g[1]*LM(g[2]))
   or (f[1]*LM(f[2]) eq g[1]*LM(g[2]) and LM(f[2]) gt LM(g[2]))
   then
      return +1;
   elif
      f[1]*LM(f[2]) lt g[1]*LM(g[2])
   then
      return -1;
   else
      return 0;
   end if;
end function;
//////////////////////////////////////////////////////
///Buchberger syzygy algorithm//////////////////////
//////////////////////////////////////////////////////
Buchberger:=function(R,G)
   GB:=Sort(G);
   SYZ:=[];
/////////Initialize NONCAN//////////////////////////
   NONCAN:=[];
   for i0 in [1..#GB-1] do
      for j0 in [i0+1..#GB] do
         lc:=LCM(LM(GB[i0]),LM(GB[j0]));
         Append(~NONCAN, [lc div LM(GB[j0]),GB[j0]]);
      end for;
   end for;
/////////Prune NONCAN///////////////////////////////
   Sort(~NONCAN,C);
   j1:=#NONCAN;
   while j1 gt 1 do
      i1:=j1-1;
      while i1 gt 0 do
         if NONCAN[j1][2] eq NONCAN[i1][2]
         and REM(NONCAN[j1][1],NONCAN[i1][1]) eq 0
         then
```

```
            Remove(~NONCAN,j1);
            j1-:=1;
            i1:=j1;
         end if;
         i1-:=1;
      end while;
      j1-:=1;
   end while;
////////////////////////////////////////////////////
///Put NONCAN[1] into canonical form////////////////
////////////////////////////////////////////////////
   while #NONCAN gt 0 do
      c:=NONCAN[1];
      d:=NONCAN[1][1]*NONCAN[1][2];
      i3:=1;
      while i3 le #GB and d ne 0 do
         if REM(LM(d), LM(GB[i3])) eq 0 then
            e:=LT(d) div LT(GB[i3]);
            c:=c cat [-e,GB[i3]];
            d:=d-e*GB[i3];
            i3:=1;
         else
            i3+:=1;
         end if;
      end while;
////////////////////////////////////////////////////
///If remanider is not 0, append it to GB to make a syzygy
////////////////////////////////////////////////////
      if d ne 0 then
         c:=c cat [-1,d];
         for j3 in [1..#GB] do
            lc:=LCM(LM(GB[j3]),LM(d));
            if LM(GB[j3]) gt LM(d) then
               Append(~NONCAN,[lc div LM(GB[j3]),GB[j3]]);
            elif LM(GB[j3]) lt LM(d) then
               Append(~NONCAN,[lc div LM(d),d]);
            end if;
         end for;
         Append(~GB,d);
         Sort(~GB);
      end if;
////////////////////////////////////////////////////
///update NONCAN////////////////////////////////////
////////////////////////////////////////////////////
      Remove(~NONCAN,1);
      Sort(~NONCAN,C);
      i4:=1;
      while i4 lt #NONCAN do
```

```
         j4:=#NONCAN;
         while j4 gt i4 do
            if (NONCAN[j4][2] eq NONCAN[i4][2]) then
               if REM(NONCAN[j4][1],NONCAN[i4][1]) eq 0 then
                  Remove(~NONCAN,j4);
               end if;
            end if;
            j4-:=1;
         end while;
         i4+:=1;
      end while;
      for i6 in [1..#SYZ] do
         j6:=#NONCAN;
         while j6 gt 0 do
            if (NONCAN[j6][2] eq SYZ[i6][2]) then
               if REM(NONCAN[j6][1],SYZ[i6][1]) eq 0 then
                  Remove(~NONCAN,j6);
               end if;
            end if;
            j6-:=1;
         end while;
      end for;
////////////////////////////////////////////////////////
///Append the syzygy found//////////////////////////////
////////////////////////////////////////////////////////
      Append(~SYZ,c);
   end while;
   return SYZ,GB;
end function;
////////////////////////////////////////////////////////
```

5.9 Faugère syzygy algorithm code

This is MAGMA code for a Faugère syzygy algorithm that produces output in some examples.

```
////aliases/////////////////////////////////////////////////
LM:=function(f) return LeadingMonomial(f); end function;
LT:=function(f) return LeadingTerm(f); end function;
REM:=function(f,g) return NormalForm(f,[g]); end function;
///Faug\‘ere syzygy algorithm//////////////////////////////
Faugere:=function(R,ev,G)
   S:=Sort(G);
   LMSYZ:=[];
   i:=1;
   while i le #S do
      ////only one S[i] per signature//////////////////////
      while i lt #S and LM(S[i+1]) eq LM(S[i]) do
         if LM(ev(S[i+1])) ge LM(ev(S[i])) then
            Remove(~S,i+1);
         else
            Remove(~S,i);
         end if;
      end while;
      ////reduce ev(S[i])///////////////////////////////////
      j:=1;
      while j lt i and ev(S[i]) ne 0 do
         if ev(S[j]) ne 0 then
            if REM(LM(ev(S[i])),LM(ev(S[j]))) eq 0
            and LM(ev(S[i]))*LM(S[j]) lt LM(ev(S[j]))*LM(S[i]) then
               S[i]-:=S[j]*LT(ev(S[i]))/LT(ev(S[j]));
               j:=0;
            end if;
         end if;
         j+:=1;
      end while;
      ////remove some pending elements//////////////////////
      j:=#S;
      while j gt i do
         if ev(S[i]) ne 0 and ev(S[j]) ne 0 then
            if REM(LM(S[j]),LM(S[i])) eq 0 then
               if LM(S[j])*LM(ev(S[i])) le LM(S[i])*LM(ev(S[j]))
               then
                  Remove(~S,j);
               end if;
            end if;
         end if;
         j-:=1;
      end while;
      ///add some pending elements////////////////////////////
      if ev(S[i]) ne 0 then
```

```
         for j in [1..i-1] do
            li:=LM(ev(S[i]));
            if ev(S[j]) ne 0 then
               lj:=LM(ev(S[j]));
               lc:=LCM(li,lj);
               if lj*LM(S[i]) gt li*LM(S[j]) then
                  Append(~S,(lc div li)*S[i]);
               end if;
               if lj*LM(S[i]) lt li*LM(S[j]) then
                  Append(~S,(lc div lj)*S[j]);
               end if;
            end if;
         end for;
         Sort(~S);
      else
         Append(~LMSYZ,LM(S[i]));
      end if;
      //// remove elements dominated by syzygies///////////////
      if LMSYZ ne [] then
         J:=ideal<R|Reduce(LMSYZ)>;
         MarkGroebner(J);
         j:=#S;
         while j gt i do
            if NormalForm(LM(S[j]),J) eq 0 then
               Remove(~S,j);
            end if;
            j-:=1;
         end while;
      end if;
      i+:=1;
   end while;
   evS:=[[S[i],ev(S[i])] : i in [1..#S]];
   return evS;
end function;
```

5.10 Faugère 2004 example

So the suggestion here is to use the Schreyer module ordering. Applied to the example in Faugère's F5 paper, this would give:

```
R<x,y,z,G013,G210,G102>:=PolynomialRing(Rationals(),6,"weight",[
1,1,1,4,3,3,
1,1,0,1,3,1,
1,0,0,0,2,1,
0,0,0,1,0,0,
0,0,0,0,1,0,
0,0,0,0,0,1]);
g013:=y*z^3-x^2;
g210:=x^2*y-z^2;
g102:=x*z^2-y^2;
ev:=hom<R->R|x,y,z,g013,g210,g102>;
G:=[G013,G210,G102];
F:=Faugere(R,ev,G);F;
//////////////////////////////////////////////////
 1: sig=000,102
1*G102,
x*z^2-y^2

 2: sig=000,210
1*G210,
x^2*y-z^2

 3: sig=000,013
1*G013,
y*z^3-x^2

 4: sig=100,013
x*G013-y*z*G102,
y^3*z-x^3

 5: sig=002,210
z^2*G210-x*y*G102,
x*y^3-z^4

 6: sig=200,013
x^2*G013-z^3*G210,
z^5-x^4

 7: sig=102,210 (principal)
x*z^2*G210-x^2*y*G102-y^2*G210+z^2*G102,
0

 8: sig=102,013 (principal)
x*z^2*G013-y*z^3*G102-y^2*G013+x^2*G102,
```

```
0

 9: sig=004,210
z^4*G210-x*y*z^2*G102-y^3*G102,
-z^6+y^5

10: sig=201,013
x^2*z*G013-x*y*z^2*G102-y^3*G102,
y^5-x^4*z

11: sig=210,013 (principal)
x^2*y*G013-y*z^3*G210-z^2*G013+x^2*G210,
0

12: sig=300,013
x^3*G013-x*z^3*G210-z^3*G102,
-x^5+y^2*z^3

13: sig=014,210
y*z^4*G210-x*y^2*z^2*G102-y^4*G102+z^3*G013,
y^6-x^2*z^3

14: sig=015,210 (non-principal)
y*z^5*G210-x*y^2*z^3*G102-x*y^3*G013+z^4*G013-x*y^2*G210+x*z^2*G102,
0
```

But to try to reconstruct the computations from the paper, a particular non-canonical? lex over grevlex monomial ordering on a ring with module variables and ring variables can be used:

```
R1<G013,G102,G210,x,y,z>:=PolynomialRing(Rationals(),6,"weight",[
1,0,0,0,0,0,
0,1,0,0,0,0,
0,0,1,0,0,0,
0,0,0,1,1,1,
0,0,0,1,1,0,
0,0,0,1,0,0]);
g013:=y*z^3-x^2;
g210:=x^2*y-z^2;
g102:=x*z^2-y^2;
ev1:=hom<R1->R1|g013,g102,g210,x,y,z>;
G1:=[G013,G210,G102];
F1:=Faugere(R1,ev1,G1);F1;
////////////////////////////////////////////
 1: sig=000,210
G210*1,
x^2*y-z^2
////////////////////////////////////////////
 2: sig=000,102
G102*1,
x*z^2-y^2

 3: sig=110,102
G102*x*y-G210*z^2
-x*y^3+z^4

 4: sig=210,102 (principal)
G102*x^2*y-G102*z^2-G210*x*z^2+G210*y^2
0

 5: sig=112,102
G102*x*y*z^2+G102*y^3-G210*z^4
z^6-y^5
////////////////////////////////////////////////
 6: sig=000,013
G013*1
y*z^3-x^2

 7: sig=100,013
G013*x-G102*y*z
y^3*z-x^3

 8: sig=200,013
G013*x^2-G210*z^3
z^5-x^4
```

```
 9: sig=003,013
G013*z^3-G102*x*y^2*z^2-G102*y^4+G210*y*z^4
y^6-x^2*z^3

10: sig=102,013 (principal)
G013*x*z^2-G013*y^2-G102*y*z^3+G102*x^2
0

11: sig=201,013
G013*x^2*z-G102*x*y*z^2-G102*y^3
y^5-x^4*z

12: sig=210,013 (principal)
G013*x^2*y-G013*z^2-G210*y*z^3+G210*x^2
0

13: sig=300,013
G013*x^3-G102*z^3-G210*x*z^3
-x^5+y^2*z^3

14: sig=130,013 (secondary)
G013*x*y^3-G013*z^4+G102*x*y^2*z^3-G102*x*z^2-G210*y*z^5+ G210*x*y^2
0

15: sig=006,013 (secondary)
G013*z^6-G013*y^5-G102*x*y^2*z^5-G102*y^4*z^3+G102*x*z^4
      +G102*y^2*z^2+G210*y*z^7-G210*y^4
0
```

The canonical lex over grevlex monomial ordering on a ring with module variables and ring variables can be used:

```
R1<G013,G210,G102,x,y,z>:=PolynomialRing(Rationals(),6,"weight",[
1,0,0,0,0,0,
0,1,0,0,0,0,
0,0,1,0,0,0,
0,0,0,1,1,1,
0,0,0,1,1,0,
0,0,0,1,0,0]);
g013:=y*z^3-x^2;
g210:=x^2*y-z^2;
g102:=x*z^2-y^2;
ev1:=hom<R1->R1|g013,g210,g102,x,y,z>;
G1:=[G013,G210,G102];
//////////////////////////////////////////////////////////
 1: sig=000,102
G102,
x*z^2-y^2
////////////////////////////////
 2: sig=000,210
G210,
x^2*y-z^2

 3: sig=002,210
G210*z^2-G102*x*y,
x*y^3-z^4

 4: sig=102,210 (principal)
G210*x*z^2-G210*y^2-G102*x^2*y+G102*z^2,
0

 5: sig=004,210
G210*z^4-G102*x*y*z^2-G102*y^3,
-z^6+y^5
////////////////////////////////////
 6: sig 000,013
G013,
y*z^3-x^2

 7: sig =100,013
G013*x-G102*y*z,
y^3*z-x^3

 8: sig=200,013
G013*x^2-G210*z^3,
z^5-x^4

 9: sig=003,013
```

```
G013*z^3+G210*y*z^4-G102*x*y^2*z^2-G102*y^4,
y^6-x^2*z^3

10: sig=102,013 (principal)
G013*x*z^2-G013*y^2-G102*y*z^3+G102*x^2,
0

11: sig=201,013
G013*x^2*z-G102*x*y*z^2-G102*y^3,
y^5-x^4*z

12: sig=210,013 (principal)
G013*x^2*y-G013*z^2-G210*y*z^3+G210*x^2,
0

13: sig=300,013
G013*x^3-G210*x*z^3-G102*z^3,
-x^5+y^2*z^3

14: sig=130,013 (secondary)
G013*x*y^3-G013*z^4-G210*y*z^5+G210*x*y^2+G102*x*y^2*z^3-
G102*x*z^2,
0

15: sig=006,013
G013*z^6-G013*y^5+G210*y*z^7-G210*y^4-G102*x*y^2*z^5-G102*y^4*z^3
+G102*x*z^4+G102*y^2*z^2,
0
```

The latter is done with essentially a position over term ordering so that the non-principal syzygies (at least in this example) involving a higher-ranked module variable (called secondary above) are principal syzygies relative to the Gröbner basis found using only lower-ranked module variables, as can be seen from the coefficients $x * y^3 - z^4$ and $z^6 - y^5$ of $G013$ in the last two computations, which were Gröbner basis elements found using only $G210$ and $G102$.

Compare this to only one non-principal (but not predictable) syzygy in the former. Which approach is better is probably not at all clear from just one such example.

The strong argument in favor of the Faugère approach is that all syzygies found are minimal syzygies relative to the given generators, whereas many of the minimal syzygies among the Gröbner basis elements found from even a best Buchberger approach implementation are superfluous when reduced to syzygies among the original generators. The fact that the Faugère approach produces some seemingly extraneous Gröbner basis elements should not be viewed as a drawback, but merely as a postponement of certain reductions that are not allowed when first encountered, many of which may never be necessary.

Again the theoretical measure should be in terms of producing a Gröbner basis for a syzygy module (not in terms of producing a Gröbner basis for the ideal); whereas the computational measure should be in terms of the number of individual divisions needed (not the number of signatures reduced).

5.11 Example 2

Consider an example with $R := \mathbf{Q}[f_1, f_3, f_5, f_7]$ having weighted grevlex monomial ordering defined by the matrix $M := \begin{pmatrix} 1 & 3 & 5 & 7 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Let $g_{3,0,0,0} := f_1^3 - f_3$, $g_{2,1,0,0} := f_1^2 f_3 - f_5$, $g_{2,0,1,0} := f_1^2 f_5 - f_7$, and $I := \langle g_{3,0,0,0},\ g_{2,1,0,0},\ g_{2,0,1,0} \rangle$. To compute all the syzygies among these three generators, it is possible to process signatures in increasing order, with or without starting with the principal syzygies

$$F_{3000,2100} := f_1^3 \cdot G_{2,1,0,0} - f_1^2 f_3 \cdot G_{3,0,0,0} - f_3 \cdot G_{2,1,0,0} + f_5 \cdot G_{3,0,0,0},$$

$$F_{3000,2010} := f_1^3 \cdot G_{2,0,1,0} - f_1^2 f_5 \cdot G_{3,0,0,0} - f_3 \cdot G_{2,0,1,0} + f_7 \cdot G_{3,0,0,0},$$

$$F_{2100,2010} := f_1^2 f_3 \cdot G_{2,0,1,0} - f_1^2 f_5 \cdot G_{2,1,0,0} - f_5 \cdot G_{2,0,1,0} + f_7 \cdot G_{2,1,0,0}.$$

Input to the Faugère syzygy algorithm

```
R=QQ[f1,f3,f5,f7,G2010,G2100,G3000,MonomialOrder=>{
                                    Weights=>{1,3,5,7,7,5,3},
                                    Weights=>{1,1,1,0,3,3,3},
                                    Weights=>{1,1,0,0,2,3,3},
                                    Weights=>{1,0,0,0,2,2,3},
                                    Weights=>{0,0,0,0,1,0,0},
                                    Weights=>{0,0,0,0,0,1,0},
                                    Weights=>{0,0,0,0,0,0,1}}];
g3000:=f1^3-f3;
g2100:=f1^2*f3-f5;
g2010:=f1^2*f5-f7;
ev:=map(R,R,matrix{{f1,f3,f5,f7,g2010,g2100,g3000}});
G:={G2010,G2100,G3000};
F=Faugere(R,ev,G); toString(F)
```

produces the output (only slightly edited)

```
{G3000, f1^3-f3},
{G2100, f1^2*f3-f5},
{f1*G2100-f3*G3000, f3^2-f1*f5},
{G2010, f1^2*f5-f7},
{f1*G2010-f5*G3000, f3*f5-f1*f7},
{f1^3*G2100-f1^2*f3*G3000-f3*G2100+f5*G3000, 0},
{f3*G2010-f5*G2100, f5^2-f3*f7},
{f1^3*G2010-f1^2*f5*G3000-f3*G2010+f7*G3000, 0},
{f1^2*f3*G2010-f1^2*f5*G2100-f5*G2010+f7*G2100, 0},
{f3^2*G2010-f3*f5*G2100-f1*f5*G2010+f5^2*G3000+f1*f7*G2100-f3*f7*G3000, 0}
```

This shows there is only one minimal syzygy with signature $f_3^2 G_{2,0,1,0}$ not divisible by the signature of any principal syzygy. The remainders in this syzygy computation

$$f_1^3 - f_3,\ f_1^2 f_3 - f_5,\ f_3^2 - f_1 f_5,\ f_1^2 f_5 - f_7,\ f_3 f_5 - f_1 f_7,\ f_5^2 - f_3 f_7$$

form a Gröbner basis for I.

Buchberger's algorithm can be viewed as a syzygy algorithm as well, though one producing syzygies among the GB elements produced rather than those among the generators only.

The input

```
R<f1,f3,f5,f7>:=PolynomialRing(Rationals(),4,"weight",
                  [1,3,5,7,
                   1,1,1,0,
                   1,1,0,0,
                   1,0,0,0]);
G:=[f1^3-f3,f1^2*f3-f5,f1^2*f5-f7];
syz,gb:=Buchberger(R,G);
syz;
gb;
```

produces the output syzygies (again only slightly edited)

```
 f1(f1^2*f3-f5)-f3(f1^3-f3)-1(f3^2-f1*f5),
 f1(f1^2*f5-f7)-f5(f1^3-f3)-1(f3*f5-f1*f7),
 f1^2(f3^2-f1*f5)-f3(f1^2*f3-f5)+f5(f1^3-f3),
 f3(f1^2*f5-f7)-f5(f1^2*f3-f5)-1(f5^2-f3*f7),
 f1^2(f3*f5-f1*f7)-f5(f1^2*f3-f5)+f7(f1^3-f3)-1(f5^2-f3*f7),
 f3(f3*f5-f1*f7)-f5(f3^2-f1*f5)-f1(f5^2-f3*f7),
 f1^2(f5^2-f3*f7)-f5(f1^2*f5-f7)+f7(f1^2*f3-f5),
 f3(f5^2-f3*f7)-f5(f3*f5-f1*f7)+f7(f3^2-f1*f5).
```

and Gröbner basis elements

```
////////////////////
    f1^3-f3,
    f1^2*f3-f5,
    f3^2-f1*f5,
    f1^2*f5-f7,
    f3*f5-f1*f7,
    f5^2-f3*f7
```

5.12 Example 3

Let $g_{8,0,0,0} := f_1^8 - f_8$, $g_{2,0,0,1} := f_1^2 f_8 - f_{10}$, and $g_{3,0,1,0} := f_1^3 f_{10} - f_{13}$.

$$I := \langle g_{8,0,0,0},\ g_{2,0,0,1},\ g_{3,0,1,0} \rangle \subset R := \mathbf{F}[f_1, f_{13}, f_{10}, f_8]$$

with weighted grevlex monomial ordering induced by the subscript weights has a Faugère syzygy computation:

```
G8000
        f1^8-f8
G2001
        f1^2*f8-f10,
G3010
        f1^3*f10-f13,
f1^6*G2001-f8*G8000+f1^3*G3010
        -f1^3*f13+f8^2
f1^5*G3010-f10*G8000
        -f1^5*f13+f10*f8
f1^8*G2001-f1^2*f8*G8000+f10*G8000-f8*G2001
        0
f8*G3010-f1*f10*G2001
        f1*f10^2-f13*f8
f1^8*G3010-f1^3*f10*G8000+f13*G8000-f8*G3010
        0
f1^2*f8*G3010-f1^3*f10*G2001-f10*G3010+f13*G2001
        0
f1^6*f8*G2001-f8^2*G8000+f1^3*f8*G3010+f1*f13*G2001
        -f1*f13*f10+f8^3
f1^6*f10*G2001-f10*f8*G8000+f1^3*f10*G3010+f13*G3010
        -f13^2+f10*f8^2
f1^5*f10*G3010-f10^2*G8000+f1^2*f13*G3010
        -f1^2*f13^2+f10^2*f8
f1^6*f10*G3010-f1*f10^2*G8000-f1^6*f13*G2001+f13*f8*G8000
   -f8^2*G3010+f1*f10*f8*G2001
        0
f1*f8^2*G3010-f1^2*f10*f8*G2001-f10^2*G2001
        f10^3-f1*f13*f8^2
f1^7*f8^2*G2001-f1*f8^3*G8000+f1^4*f8^2*G3010+f1^2*f13*f8*G2001
   +f13*f10*G2001
        -f13*f10^2+f1*f8^4
f1^7*f10^2*G2001-f1*f10^2*f8*G8000+f1^4*f10^2*G3010
   -f1^6*f13*f8*G2001+f13*f8^2*G8000-f1^3*f13*f8*G3010
   +f1*f13*f10*G3010-f1*f13^2*G2001-f8^3*G3010+f1*f10*f8^2*G2001
         0
f1^5*f10^2*G3010-f10^3*G8000-f1^7*f13*f8*G2001+f1*f13*f8^2*G8000
   -f1^4*f13*f8*G3010+f1^2*f13*f10*G3010-f1^2*f13^2*G2001
   -f1*f8^3*G3010+f1^2*f10*f8^2*G2001+f10^2*f8*G2001
         0
f1^7*f10*f8^2*G2001-f1*f10*f8^3*G8000+f1^4*f10*f8^2*G3010
```

```
   +f1*f13*f8^2*G3010
         -f1*f13^2*f8^2+f1*f10*f8^4
f1^6*f10^2*f8*G2001-f10^2*f8^2*G8000+f1^3*f10^2*f8*G3010
   +f13*f10*f8*G3010
         -f13^2*f10*f8+f10^2*f8^3
f1^6*f10^3*G2001-f10^3*f8*G8000-f1^7*f13*f8^2*G2001
   +f1*f13*f8^3*G8000+f1^3*f10^3*G3010-f1^4*f13*f8^2*G3010
   +f13*f10^2*G3010-f1^2*f13^2*f8*G2001-f1*f8^4*G3010
   +f1^2*f10*f8^3*G2001-f13^2*f10*G2001+f10^2*f8^2*G2001
         0
```

that produces only the principal syzygies among the generators and a Gröbner basis consisting of $f_1^8 - f_8$, $f_1^2 f_8 - f_{10}$, $f_1^3 f_{10} - f_{13}$, $-f_1^3 f_{13} + f_8^2$, $-f_1^5 f_{13} + f_{10} f_8$, $f_1 f_{10}^2 - f_{13} f_8$, $-f_1 f_{13} f_{10} + f_8^3$, $-f_{13}^2 + f_{10} f_8^2$, and $-f_{13} f_{10}^2 + f_1 f_8^4$.

5.13 Example 4

Find a minimal, reduced Gröbner basis for the ideal generated by $f_{1,0,2} := x_3x_1^2 + x_2^2$, $f_{2,1,0} := x_3^2x_2 + x_1^2$, and $f_{3,0,0} := x_3^3 + x_2^2x_1$ using the canonical version of the Buchberger algorithm.

	102	210	300	031	130	005	023	050
102	1							
210	212	2						
300	302	310	3					
031	132	231	$*$	4				
130	$--$	230	$--$	131	5			
005	105	$*$	$*$	035	$*$	7		
023	123	$--$	$*$	033	$--$	025	6	
050	$*$	250	$*$	051	150	$*$	$--$	12

$$3,1,0 \ : \ ev(x_2 \cdot G_{3,0,0} - x_1 \cdot G_{2,1,0} + 1 \cdot G_{1,0,2}) = x_2^3x_1 + x_2^2 =: ev(G_{0,3,1})$$
$$2,1,2 \ : \ ev(x_1^2 \cdot G_{2,1,0} - x_3x_2 \cdot G_{1,0,2}) = -x_3x_2^3 + x_1^4 =: ev(G_{1,3,0})$$
$$3,0,2 \ : \ ev(x_1^2 \cdot G_{3,0,0} - x_3^2 \cdot G_{1,0,2} + x_2 \cdot G_{2,1,0}) = x_2^2x_1^3 + x_2x_1^2 =: ev(G_{0,2,3})$$
$$1,3,1 \ : \ ev(x_1 \cdot G_{1,3,0} + x_3 \cdot G_{0,3,1}) = x_1^5 + x_3x_2^2 =: ev(G_{0,0,5})$$
$$2,3,0 \ : \ ev(x_3 \cdot G_{1,3,0} + x_2^2 \cdot G_{2,1,0} - x_1^2 \cdot G_{1,0,2}) = 0$$
$$1,0,5 \ : \ ev(x_3 \cdot G_{0,0,5} - x_1^3 \cdot G_{1,0,2} + 1 \cdot G_{0,2,3} - x_2 \cdot G_{2,1,0}) = 0$$
$$0,3,3 \ : \ ev(x_2 \cdot G_{0,2,3} - x_1^2 \cdot G_{0,3,1}) = 0$$
$$1,2,3 \ : \ ev(x_3 \cdot G_{0,2,3} - x_2^2x_1 \cdot G_{1,0,2} + x_2 \cdot G_{0,3,1} - x_2 \cdot G_{1,0,2}) = 0$$
$$1,3,2 \ : \ ev(x_3x_1 \cdot G_{0,3,1} - x_2^3 \cdot G_{1,0,2}) = -x_2^5 + x_3x_2^2x_1 =: ev(G_{0,5,0})$$
$$0,5,1 \ : \ ev(x_1 \cdot G_{0,5,0} + x_2^2 \cdot G_{0,3,1} - x_2^2 \cdot G_{1,0,2}) = 0$$
$$2,3,1 \ : \ ev(x_3^2 \cdot G_{0,3,1} - x_2^2x_1 \cdot G_{2,1,0} + 1 \cdot G_{0,2,3} - x_2 \cdot G_{2,1,0}) = 0$$
$$1,5,0 \ : \ ev(x_3 \cdot G_{0,5,0} - x_2^2 \cdot G_{1,3,0} + x_1 \cdot G_{0,2,3} - x_2x_1 \cdot G_{2,1,0}) = 0$$
$$0,2,5 \ : \ ev(x_1^2 \cdot G_{0,2,3} - x_2^2 \cdot G_{0,0,5} - x_2 \cdot G_{1,3,0}) = 0$$
$$0,3,5 \ : \ ev(x_2^3 \cdot G_{0,0,5} - x_1^4 \cdot G_{0,3,1} + x_2^2 \cdot G_{1,3,0}) = 0$$

Now use the Faugère syzygy algoritm.

$$F_{000,102} := G_{102}, \ ev(F_{000,102}) = x_3x_1^2 + x_2^2$$
$$F_{000,210} := G_{210}, \ ev(F_{000,210}) = x_3^2x_2 + x_1^2$$
$$F_{000,300} := G_{300}, \ ev(F_{000,300}) = x_3^3 + x_2^2x_1$$
$$F_{010,300} := x_2 \cdot G_{300} - x_3 \cdot G_{210} + 1 \cdot G_{102}, \ ev(F_{010,300}) = x_2^3x_1 + x_2^2$$
$$F_{002,210} := x_1^2 \cdot G_{210} - x_3x_2 \cdot G_{102}, \ ev(F_{002,210}) = -x_3x_2^3 + x_1^4$$
$$F_{002,300} := x_1^2 \cdot G_{300} - x_3^2 \cdot G_{102} + x_2 \cdot G_{210}, \ ev(F_{002,300}) = x_2^2x_1^3 + x_2x_1^2$$
$$F_{003,201} := x_1(x_1^2 \cdot G_{210} - x_3x_2 \cdot G_{102}) + x_3(x_2 \cdot G_{300} - x_3 \cdot G_{2,1,0} + 1 \cdot G_{1,0,2}), \ ev(F_{003,201}) = x_1^5 + x_3x_2^2$$
$$F_{111,300} := x_3x_1(x_2 \cdot G_{300} - x_3 \cdot G_{210} + 1 \cdot G_{102}) - x_2^3 \cdot G_{102}, \ ev(F_{111,300}) = -x_2^5 + x_3x_2^2x_1$$
$$F_{023,210} := x_2^2(x_1(x_1^2 \cdot G_{210} - x_3x_2 \cdot G_{102}) + x_3(x_2 \cdot G_{300} - x_3 \cdot G_{210} + 1 \cdot G_{102}), \ ev(F_{023,210}) = 0$$
$$F_{004,300} := -x_1^2(x_1^2 \cdot G_{300} - x_3^2 \cdot G_{102} + x_2 \cdot G_{210}) + x_2(x_1^2 \cdot G_{210} - x_3x_2 \cdot G_{102}), \ ev(F_{004,300}) = 0$$

```
R8<x3,x2,x1,G300,G210,G102>:=PolynomialRing(Rationals(),6,"weight",[
1,1,1,3,3,3,
1,1,0,3,3,1,
1,0,0,3,2,1,
0,0,0,1,0,0,
0,0,0,0,1,0,
0,0,0,0,0,1]);
g102:=x3*x1^2+x2^2;
g210:=x3^2*x2+x1^2;
g300:=x3^3+x2^2*x1;
ev8:=hom<R8->R8|x3,x2,x1,g300,g210,g102>;
G8:=[G300,G210,G102];
F8:=Faugere(R8,ev8,G8);
F8;

1*G102,
        x3*x1^2+x2^2

1*G210,
        x3^2*x2+x1^2
1*G300,
        x3^3+x2^2*x1
x2*G300-x3*G210,
        x2^3*x1-x3*x1^2
x1^2*G210-x3*x2*G102,
        -x3*x2^3+x1^4
x1^2*G300-x3^2*G102,
        x2^2*x1^3-x3^2*x2^2
x1^3*G210-x3*x2*x1*G102+x3*x2*G300-x3^2*G210,
        x1^5-x3^2*x1^2
x3*x1^2*G210-x3^2*x2*G102+x2^2*G210-x1^2*G102,
        0
x3*x1^2*G300-x3^3*G102-x2^2*x1*G102+x2^2*G300,
        0
x3*x2*x1*G300-x3^2*x1*G210-x2^3*G102,
        -x2^5-x3^2*x1^3
x3^2*x2*G300-x3^3*G210-x2^2*x1*G210+x1^2*G300,
        0
x2^2*x1^3*G210-x3*x2^3*x1*G102+x3*x2^3*G300
   -x3^2*x2^2*G210-x1^4*G300+x3^2*x1^2*G102,
        0
```

5.14 Buchberger

The Buchberger algorithm is usually described in terms of computing Spolynomials and reducing them. See for instance http://en.wikipedia.org/wiki/Buchberger's_algorithm or most any textbook on commutative algebra. Obviously from the above examples, it is possible to rephrase it in terms of canonical reduction relative to the current list of generators, focusing on producing syzygies, with a Gröbner basis as a byproduct.

The Buchberger criterion, that any set closed under the combined operations of computing Spolynomials and reducing them, is a Gröbner basis, can be viewed as suggesting a canonical set of syzygies that can be used to define a canonical division with remainder relative to a fixed ordered Gröbner basis for the ideal it generates. In turn that suggests that one should not only try to compute a Gröbner basis for an ideal, but also a canonical set of syzygies describing that canonical division with remainder. And theoretically this gives an immediate transparent proof why the Buchberger criterion gives a Gröbner basis. [Note that division was defined using individual term quotients rather than more general polynomial quotients.]

Let $R := \mathbf{F}[x_n, \ldots, x_1]$ be a polynomial ring with a given global monomial ordering. The definition of *Spolynomials* used here will be:

$$Spolynomial(f,g) = \frac{LCM(LM(f), LM(g))}{LT(f)} f - \frac{LCM(LM(f), LM(g))}{LT(g)} g$$

with $f \succ g$.

A set $b_0, \ldots, b_{N-1}$ (ordered so that $b_0 \prec \cdots \prec b_{N-1}$) is closed under the combined operation of Spolynomials and reduction iff

$$Spolynomial(b_i, b_j) = \sum_{k=0}^{K} c_k \underline{x}^{\underline{\alpha}(k)} b_{l(k)}$$

with $LM(SPolynomial(b_i, b_j)) = LM(c_0 \underline{x}^{\underline{\alpha}(0)} b_{l(0)}) \succ \cdots \succ LM(c_K \underline{x}^{\underline{\alpha}(K)} b_{l(K)})$. Assume as well that the set is minimal and reduced, so that $LM(b_i)$ doesn't divide any term of any b_j (other than $LT(b_i)$). Then there is a minimal set of syzygies among the b_i gotten from interreducing all the syzygies

$$Spolynomial(b_i, b_j) - \sum_{k=0}^{K} c_k \underline{x}^{\underline{\alpha}(k)} b_{l(k)}$$

above.

Theorem 24. *Given an ordered set $b_0 \prec \cdots \prec b_{N-1}$ of elements of a polynomial ring $R := \mathbf{F}[\underline{x}]$, there exists a minimal, reduced set of syzygies of the form*

$$syz(\underline{\gamma}, k) := \underline{x}^{\underline{\alpha}(0)} b_{j(0)} + \sum_{i=1}^{K} c_i \underline{x}^{\underline{\alpha}(i)} b_{j(i)} = 0$$

with $c_i \in \mathbf{F}$ and

$$LM(\underline{x}^{\underline{\alpha}(0)} b_k) = LM(c_1 \underline{x}^{\underline{\alpha}(1)} b_{l(1)}) \succ \cdots \succ LM(c_K \underline{x}^{\underline{\alpha}(K)} b_{j(K)})$$

Corollary 25. *The division algorithm with respect to the ordered set $b_0 \prec \cdots \prec b_{N-1}$ (and the default $b_N := 1$ if no other divisor works) gives both a canonical set of quotients and a canonical remainder:*

$$f = \sum_{k=0}^{K} c_k \underline{x}^{\underline{\alpha}(k)} b_{l(k)}$$

with

$$LM(f) = LM(\underline{x}^{\underline{\alpha}(0)} b_{l(0)}) \succ \cdots \succ LM(c_K \underline{x}^{\underline{\alpha}(K)} b_{j(K)}).$$

Corollary 26. *For $f \in I := \langle b_0, \ldots, b_{N-1} \rangle$, $LM(b_{j(0)}) | LM(f)$ with $j(0) \neq N$; so $b_0, \ldots, b_{N-1}$ is a Gröbner basis for I.*

Corollary 27. *For $f \in R$, those terms with $b_{j(k)} = b_N = 1$ form the canonical remainder $NF(f, I)$.*

5.15 Faugère

Theorem 28. *The Faugère syzygy algorithm herein produces reductions that include minimum signature reductions with values $LM(b)$ for all $b \in B$ with B a minimal Gröbner basis for I.*

Proof. First note that the Faugère syzygy algorithm doesn't process every signature. To reduce a signature $\underline{x}^{\underline{\gamma}} G_{\underline{\beta}}$, it is necessary to find a signature $\underline{x}^{\underline{\alpha}} G_{\underline{\beta}}$ that is, with $\underline{x}^{\underline{\alpha}} | \underline{x}^{\underline{\gamma}}$ and $\underline{x}^{\underline{\alpha}}$ maximum. Then multiply the reduction of $\underline{x}^{\underline{\alpha}} G_{\underline{\beta}}$ by $\underline{x}^{\underline{\gamma}-\underline{\alpha}}$.

Let B be a minimal Gröbner basis for I. For each $LM(b)$ with $b \in B$, let $R_{\underline{\gamma},\underline{\beta}}$ be a representation with $LM(ev(R_{\underline{\gamma},\underline{\beta}})) = LM(b)$ and signature $\underline{x}^{\underline{\gamma}} G_{\underline{\beta}}$ minimum.

- Suppose that $LM(ev(F_{\underline{\gamma},\underline{\beta}})) \succ LM(b)$. Then for some $c \in \mathbf{F}$, $LM(F_{\underline{\gamma},\underline{\beta}} - cR_{\underline{\gamma},\underline{\beta}}) \prec \underline{x}^{\underline{\gamma}} G_{\underline{\beta}}$. But then $F_{\underline{\gamma},\underline{\beta}} - (F_{\underline{\gamma},\underline{\beta}} - cR_{\underline{\gamma},\underline{\beta}}) = cR_{\underline{\gamma},\underline{\beta}}$, so $F_{\underline{\gamma},\underline{\beta}}$ is not completely reduced.
- Suppose that $LM(ev(F_{\underline{\gamma},\underline{\beta}})) \prec LM(b)$. Then for some $c \in \mathbf{F}$, $LM(R_{\underline{\gamma},\underline{\beta}} - cF_{\underline{\gamma},\underline{\beta}}) \prec \underline{x}^{\underline{\gamma}} G_{\underline{\beta}}$. But then $LM(ev(R_{\underline{\gamma},\underline{\beta}} - cF_{\underline{\gamma},\underline{\beta}})) = LM(b)$, contradicting the minimality of the signature $\underline{x}^{\underline{\gamma}} G_{\underline{\beta}}$.
- Suppose that $LM(ev(F_{\underline{\gamma},\underline{\beta}})) = LM(b)$. Then $LM(ev(F_{\underline{\gamma},\underline{\beta}})) = \underline{x}^{\underline{\gamma}-\underline{\alpha}} LM(ev(F_{\underline{\alpha},\underline{\beta}}))$. That, in turn means that $LM(ev(F_{\underline{\alpha},\underline{\beta}})) | LM(b)$ implies $\underline{\alpha} = \underline{\gamma}$.

□

Corollary 29. *Given an ordered set of generators $g_{\underline{\beta}(0)} \prec \cdots \prec g_{\underline{\beta}(N-1)}$ for an ideal $I \in R$, and the R-module $R\langle G_{\underline{\beta}(N-1)}, \ldots, G_{\underline{\beta}(0)} \rangle$ with R-linear map defined by $ev(G_{\underline{\beta}(i)}) := g_{\underline{\beta}(i)}$ for $0 \leq i \leq N-1$, there exists a minimal set of minimal, reduced relations of the form*

$$F_{\underline{\gamma},\underline{\delta}} - \sum_{i=0} c_i \underline{x}^{\underline{\varepsilon}(i)} F_{\underline{\alpha}(i),\underline{\beta}(i)} = \sum_{i=0} a_i \underline{x}^{\underline{\lambda}(i)} G_{\underline{\mu}(i)}$$

that correspond to minimal expressions for the values

$$\sum_{k=0} a_k \underline{x}^{\underline{\lambda}(k)} g_{\underline{\mu}(k)}$$

or to minimal syzygies if the value is 0.

Proof. Every minimal syzygy is computed when its signature is reduced. Every element of a minimal, reduced Gröbner basis has presentations as R-linear combinations of the original generators. That element (or at least one with the same leading monomial) is produced as a value when the signature of the R-linear combination with smallest signature for it is reduced. □

5.16 Example 5

As a test example try $R := \mathbf{Q}[x_4, x_3, x_2, x_1]$ with a (default) grevlex monomial ordering. And let

$$I := \langle x_4^{13} - x_3, x_4^{10} - x_2, x_4^8 - x_1 \rangle.$$

Start by interreducing the generators to get

$$g_{2,0,0,1} := x_4^2 x_1 - x_2, \; g_{3,0,1,0} := x_4^3 x_2 - x_3, \; g_{8,0,0,0} := x_4^8 - x_1.$$

A list of of the reductions actually done in this Buchberger syzygy algorithm, and in what order can be put in a table:

0012	16												
2001	2012 20	1											
1020	1022 18	2021 5	4										
1110	1112 19	2111 14	1120 12	11									
0013	0013 17	2013 –	1023 –	1113 –	12								
1102	1112 20	2102 6	1122 8	1112 13	1113 –	5							
3010	3012 –	3011 4	3020 7	3110 16	3013 –	3112 –	2						
1300	1312 –	2301 32	1320 –	1310 22	1313 –	1302 31	3310 –	19					
2200	2212 –	2201 21	2220 –	2210 23	2213 –	2202 –	2210 –	2300 24	20				
3100	3112 –	3101 11	3120 –	3110 15	3113 –	3102 –	3110 –	3300 –	3200 25	10			
0005	0015 26	2005 34	1025 –	1115 –	0015 –	1105 33	3015 –	1305 –	2205 –	3105	13		
1004	1014 28	2004 30	1024 –	1114 –	1014 –	1104 29	3014 –	1304 –	2204 –	3104 –	1005 27	14	
0050	0052 35	2051 –	1050 9	1150 –	0053 –	1152 –	3050 –	1350 –	2250 –	3150 –	0055 –	1054 –	8
8000	8012 –	8001 10	8020 –	8110 –	8013 –	8102 –	8010 36	8300 –	8200 –	8100 37	8005 –	8004 –	8050 –	3

So of the $\binom{13}{2} = 78$ possible reductions, only $37 - 3 = 34$ are done, and only $13 - 3$ new Gröbner basis elements are found, 1 of which is unnecessary. The Gröbner basis elements found are:

```
g0012:=f10*f8^2-f13^2,
g2001:=f1^2*f8-f10,
g1020:=f1*f10^2-f13*f8,
g1110:=f1*f13*f10-f8^3,
(g0013:=-f10*f8^3+f13^2*f8),
g1102:=-f1*f13*f8^2+f10^3,
g3010:=f1^3*f10-f13,
g1300:=f1*f13^3-f10^4,
g2200:=f1^2*f13^2-f10^2*f8,
g3100:=f1^3*f13-f8^2,
g0005:=-f8^5+f10^4,
g1004:=-f1*f8^4+f13*f10^2,
g0050:=f10^5-f13^2*f8^3,
g8000:=f1^8-f8
```

and the syzygies in order are:

```
 4:f8(f1^3*f10-f13)-f1*f10(f1^2*f8-f10)-1(f1*f10^2-f13*f8)
 5:f1*f8(f1*f10^2-f13*f8)-f10^2(f1^2*f8-f10)-1(-f1*f13*f8^2+f10^3)
 6:f1(-f1*f13*f8^2+f10^3)+f13*f8(f1^2*f8-f10)-f10(f1*f10^2-f13*f8)
 7:f10(f1^3*f10-f13)-f1^2(f1*f10^2-f13*f8)-f13(f1^2*f8-f10)
 8:f10^2(-f1*f13*f8^2+f10^3)+f13*f8^2(f1*f10^2-f13*f8)-1(f10^5-f13^2*f8^3)
 9:f1(f10^5-f13^2*f8^3)-f10^3(1*f10^2-f13*f8)f13*f8(f1*f13*f8^2+f10^3)
10:f8(1^8-f8)f1^6(1^2*f8-f10)-f1^3(f1^3*f10-f13)-1(f1^3*f13-f8^2)
11:f8(f1^3*f13-f8^2)-f1*f13(f1^2*f8-f10)-1(f1*f13*f10-f8^3)
12:f10(f1*f13*f10-f8^3)-f13(f1*f10^2-f13*f8)-1(-f10*f8^3+f13^2*f8)
13:f10(-f1*f13*f8^2+f10^3)+f8^2(f1*f13*f10-f8^3)-1(-f8^5+f10^4)
14:f1*f8(f1*f13*f10-f8^3)-f13*f10(f1^2*f8-f10)-1(-f1*f8^4+f13*f10^2)
15:f10(f1^3*f13-f8^2)-f1^2(f1*f13*f10-f8^3)-f8^2(f1^2*f8-f10)
16:f13(f1^3*f10-f13)-f1^2(f1*f13*f10-f8^3)-f8^2(f1^2*f8-f10)-1(f10*f8^2-f13^2)
17:1(-f10*f8^3+f13^2*f8)+f8(f10*f8^2-f13^2)
18:f8^2(f1*f10^2-f13*f8)-f1*f10(f10*f8^2-f13^2)-f13(f1*f13*f10-f8^3)
19:f8^2(f1*f13*f10-f8^3)-f1*f13(f10*f8^2-f13^2)-1(-f8^5+f10^4)-1(f1*f13^3-f10^4)
20:f10*f8(f1^2*f8-f10)-f1^2(f10*f8^2-f13^2)-1(f1^2*f13^2-f10^2*f8)
21:f8(f1^2*f13^2-f10^2*f8)-f13^2(f1^2*f8-f10)+f10(f10*f8^2-f13^2)
22:f10(f1*f13^3-f10^4)-f13^2(f1*f13*f10-f8^3)+1(f10^5-f13^2*f8^3)
23:f10(f1^2*f13^2-f10^2*f8)-f1*f13(f1*f13*f10-f8^3)+f8(-f1*f13*f8^2+f10^3)
24:f13(f1^2*f13^2-f10^2*f8)-f1(f1*f13^3-f10^4)-f10^2(f1*f10^2-f13*f8)
25:f13(f1^3*f13-f8^2)-f1(f1^2*f13^2-f10^2*f8)-f8(f1*f10^2-f13*f8)
26:f10(-f8^5+f10^4)+f8^3(f10*f8^2-f13^2)-1(f10^5-f13^2*f8^3)
27:f8(-f1*f8^4+f13*f10^2)-f1(-f8^5+f10^4)+f10^2(f1*f10^2-f13*f8)
28:f10(-f1*f8^4+f13*f10^2)+f1*f8^2(f10*f8^2-f13^2)-f13(-f1*f13*f8^2+f10^3)
29:f13(-f1*f8^4+f13*f10^2)-f8^2(-f1*f13*f8^2+f10^3)+f10^2(f10*f8^2-f13^2)
30:f1(-f1*f8^4+f13*f10^2)+f8^3(f1^2*f8-f10)-f13(f1*f10^2-f13*f8)
     +f8(f10*f8^2-f13^2)
31:f8^2(f1*f13^3-f10^4)+f13^2(-f1*f13*f8^2+f10^3)+f10^3(f10*f8^2-f13^2)
32:f1*f8(f1*f13^3-f10^4)-f13^3(f1^2*f8-f10)+f10^2*f8(f1*f10^2-f13*f8)
     +f13*f10(f10*f8^2-f13^2)
33:f1*f13(-f8^5+f10^4)-f8^3(-f1*f13*f8^2+f10^3)-f13*f10^2(f1*f10^2-f13*f8)
     +f10^2*f8(f10*f8^2-f13^2)
34:f1^2(-f8^5+f10^4)+f8^4(f1^2*f8-f10)-f1*f10^2(f1*f10^2-f13*f8)
     -f13*f8(f1*f10^2-f13*f8)+f8^2(f10*f8^2-f13^2)
35:f8^2(f10^5-f13^2*f8^3)-f10^4(f10*f8^2-f13^2)-f13^2(-f8^5+f10^4)
36:f10(f1^8-f8)-f1^5(f1^3*f10-f13)-f1^2(f1^3*f13-f8^2)-f8(f1^2*f8-f10)
37:f13(f1^8-f8)-f1^5(f1^3*f13-f8^2)-f1^3*f8(f1^2*f8-f10)
     -f1*f10(f1^2*f8-f10)-1(f1*f10^2-f13*f8)
```

In the Faugère approach, the input:

```
R=QQ[x4,x3,x2,x1,G8000,G3010,G2001,MonomialOrder=>{
        Weights=>{1,1,1,1,8,4,3},
        Weights=>{1,1,1,0,8,4,2},
        Weights=>{1,1,0,0,8,3,2},
        Weights=>{1,0,0,0,8,3,2},
        Weights=>{0,0,0,0,1,0,0},
        Weights=>{0,0,0,0,0,1,0},
        Weights=>{0,0,0,0,0,0,1}}];
g8000=x4^8-x1;
g3010=x4^3*x2-x3;
g2001=x4^2*x1-x2;
ev=map(R,R,matrix{{x4,x3,x2,x1,g8000,g3010,g2001}});
G={G8000,G3010,G2001};
F=Faugere(R,ev,G);toString F
```

produces output (slightly modified for space and form)

```
 1:G2001,
      x4^2*x1-x2
 2:G3010,
      x4^3*x2-x3
 3:x1*G3010-x4*x2*G2001,
      x4*x2^2-x3*x1
 4:x4*x1^2*G3010-x4^2*x2*x1*G2001-x2^2*G2001,
      -x4*x3*x1^2+x2^3
 5:x4^2*x1*G3010-x4^3*x2*G2001-x2*G3010+x3*G2001,
      0
 6:G8000,
      x4^8-x1
 7:x4*x2^2*x1^2*G3010-x4^2*x2^3*x1*G2001+x3*x1^3*G3010
    -x4*x3*x2*x1^2*G2001-x2^4*G2001,
      x2^5-x3^2*x1^3
 8:x1*G8000-x4^6*G2001-x4^3*G3010,
      x4^3*x3-x1^2
 9:x2*G8000-x4^5*G3010,
      x4^5*x3-x2*x1
10:x1^2*G8000-x4^6*x1*G2001-x4^3*x1*G3010-x4*x3*G2001,
      x4*x3*x2-x1^3
11:x2*x1*G8000-x4^5*x1*G3010-x4^3*x3*G2001-x3*G3010,
      -x2*x1^2+x3^2
12:x2^2*G8000-x4^5*x2*G3010-x4^2*x3*G3010,
      x4^2*x3^2-x2^2*x1
13:x2^2*x1*G8000-x4^5*x2*x1*G3010-x4^2*x3*x1*G3010-x3^2*G2001,
      -x2^2*x1^2+x3^2*x2
14:x4^2*x1*G8000-x4^8*G2001-x2*G8000+x1*G2001,
      0
15:x4*x2^2*G8000-x4^6*x2*G3010-x3*x1*G8000+x4^6*x3*G2001
```

```
    +x1^2*G3010-x4*x2*x1*G2001,
      0
16:x1^4*G8000-x4^6*x1^3*G2001-x4^3*x1^3*G3010+x4*x2*x1^2*G3010
    -x4^2*x2^2*x1*G2001-x4*x3*x1^2*G2001-x2^3*G2001,
      -x1^5+x2^4
17:x4*x1^3*G8000-x4^7*x1^2*G2001-x4^4*x1^2*G3010-x4^2*x3*x1*G2001
    -x3*x2*G2001,
      -x4*x1^4+x3*x2^2
18:x4*x3*x1^2*G8000-x4^7*x3*x1*G2001-x2^3*G8000+x4^5*x2^2*G3010
    -x4^4*x3*x1*G3010+x4^2*x3*x2*G3010-x4*x1^3*G3010
    +x4^2*x2*x1^2*G2001-x4^2*x3^2*G2001+x2^2*x1*G2001,
      0
19:x4*x3*x2*x1*G8000-x4^6*x3*x1*G3010-x4^4*x3^2*G2001-x4*x2*x1^2*G3010
    +x4^2*x2^2*x1*G2001-x4*x3^2*G3010+x2^3*G2001,
      x4*x3^3-x2^4
20:x2^4*G8000-x4^5*x2^3*G3010-x4^2*x3*x2^2*G3010-x4*x3^2*x1*G3010
    +x4^2*x3^2*x2*G2001,
      x4*x3^3*x1-x2^4*x1},
21:x4^3*x2*G8000-x4^8*G3010-x3*G8000+x1*G3010,
       0
22:x2^4*x1*G8000-x4^5*x2^3*x1*G3010-x4^2*x3*x2^2*x1*G3010-x3^2*x2^2*G2001,
      -x2^4*x1^2+x3^2*x2^3
23:x2^5*G8000-x4^5*x2^4*G3010-x3^2*x1^3*G8000+x4^6*x3^2*x1^2*G2001
    +x4^3*x3^2*x1^2*G3010-x4^2*x3*x2^3*G3010+x4*x2^2*x1^3*G3010
    -x4^2*x2^3*x1^2*G2001-x4*x3^2*x2*x1*G3010+x4^2*x3^2*x2^2*G2001
    +x3*x1^4*G3010-x4*x3*x2*x1^3*G2001+x4*x3^3*x1*G2001-x2^4*x1*G2001,
       0
24:x4*x3^3*x2*x1*G8000-x4^6*x3^3*x1*G3010-x4^4*x3^4*G2001
    -x4*x3^2*x2*x1^2*G3010+x4^2*x3^2*x2^2*x1*G2001-x4*x3^4*G3010
    +x3^2*x2^3*G2001,
      x4*x3^5-x3^2*x2^4
```

Chapter 6

Isomorphism

6.1 Finite fields

Finite fields of characteristic p are either $F_p := \mathbf{Z}_p$ or an extension of it gotten by using an irreducible polynomial $\pi(x) \in \mathbf{Z}_p[x]$ of degree m to produce $\mathbf{F}_{p^m} := \mathbf{F}_p[a]/\langle \pi(a) \rangle$. Up to isomorphism there is only one such for each prime power order p^m.

It is worthwhile to try to prove that the non-zero elements form a cyclic group under multiplication. It is also worthwhile to use the Euclidean algorithm to prove which finite fields are subfields of which others. And it is worthwhile to figure out how to use the extended Euclidean algorithm to produce multiplicative inverses, hence to prove that these are really fields and not just quotient rings.

6.2 Isomorphism versus equality

There is a general problem in deciding whether some object should be viewed as a sub-object of some other object or can be mapped isomorphically to a sub-object of some other object.

Start with a simple example of such.

$$A := \mathbf{F}_2[a]/\langle a^4 + a + 1 \rangle$$

$$B := \mathbf{F}_2[b]/\langle b^4 + b^3 + 1 \rangle$$

are both finite fields. Are they equal or isomorphic?

One way to view this is that there is a field isomorphism $\phi : B \to A$, possibly defined by $\phi(b) := a^7$ (with inverse $\psi(a) := b^{13}$). Another is that $b = a^7$ and $B = A$ are the same object $\mathbf{F}_{16}$ viewed two different ways.

Is this any different from, say, a change of basis in vector spaces? There, there is no thought that change of basis is an isomorphism between two distinct vector spaces, just an admission that there are various ways to view the same vector space. Isomorphism of vector spaces comes from mapping one vector space to another, most likely of different dimension; and identifying the image with the domain modulo the kernel.

The same is true here for function fields. Suppose $\mathbf{K} := \mathbf{F}(x_2/h_2, x_1/h_1)/I$ is a function field of dimension 1 with $I := \langle f(x_2/h_2, x_1/h_1) \rangle$. If $x_3/h_3 \in \mathbf{K} \backslash \mathbf{F}$ and $x_4/h_4 \in \mathbf{K} \backslash \mathbf{F}(x_3/h_3)$, then there is an irreducible relation $\overline{f}(x_4/h_4, x_3/h_3)$ induced by $f(x_2/h_2, x_1/h_1)$, defining a sub-function field of $\mathbf{K}$, $B := \mathbf{F}(x_4/h_4, x_3/h_3)/J$, $J := \langle \overline{f}(x_4/h_4, x_3/h_3) \rangle$. But for most choices of x_3/h_3 and x_4/h_4, $B = \mathbf{K}$.

So why worry here about a subtle difference between equality and isomorphism? Consider the affine quotient rings involved:

$$A_1 := \mathbf{F}[x_2, x_1]/I,\ I := \langle f(x_2, x_1)\rangle,$$
$$A_2 := \mathbf{F}[x_4, x_3]/J,\ J := \langle \overline{f}(x_4, x_3)\rangle.$$

We have already made the case above that these can be very different. Standard methods are to describe what are called birational maps, which have problems being maps unless they are restricted appropriately. These maps are at the level of $\phi : A_1 \to A_2$; when, in fact, they should all be the *identity map* on $\mathbf{K}$ the function field these have in common.

The problem with birational maps is then that the affine points of A_i miss some set of points V_i, so the birational map between A_1 and A_2 only makes sense when one avoids $V_1 \cup V_2$.

There are no such problems with the identity map. Blowups are of the form of taking different affine views of the function field. These have exceptional divisors, describing V_i, which should be irrelevant once these are treated as change of basis of the function field. [Desingularization is probably about coordinatizing the points of the function field, and possibly finding explicit local parameter, local unit pairs at each point, not about finding weak desingularizations or strong desingularizations with normal crossings of exceptional divisors (http://en.wikipedia.org/wiki/Resolution_of_singularities), all of which should be irrelevant.]

A related question is, as mentioned earlier, why one produces new names for functions? Clearly(?) it is to use those names in place of writing out explicitly what the functions are in terms of the variables currently in use. That means that if s is a name for a/b, then the reduction rule should be $a/b \mapsto s$ rather than $s \mapsto a/b$. [As a warning, if one uses only polynomial reduction rules then $a \mapsto sb$ rather than $sb \mapsto a$; but either of these has to be used in conjunction with factoring out b in all computations.]

6.3 Example

Here is another interesting example.

$$\mathbf{K} := \overline{\mathbf{F}}(x_2, x_1)/\langle x_2^{12} + x_2^4 x_1^{10} + x_2^2 x_1^{11} + x_2 x_1^{10} + x_1^7 \rangle.$$

The divisors are:

$$((x_2)) = -5A_j \cdot Q_j - 1 \cdot P_0 + 1 \cdot P_1 + 3 \cdot P_2 + 7 \cdot P_3;$$
$$((x_1)) = -4A_j \cdot Q_j - 2 \cdot P_0 - 1 \cdot P_1 - 1 \cdot P_2 + 12 \cdot P_3.$$

with either $A_1 = 2$ or $A_1 = A_2 = 1$.

It is possible to resolve this using what is referred to here as multi-blowups. Start with $(-5)(-1) - (-4)(-1) = 1$ to motivate a change of variables $x_2 = x_4^{-5} x_3^{-1}$, $x_1 = x_4^{-4} x_3^{-1}$, with $x_4 := x_1/x_2$ and $x_3 := x_2^4/x_1^5$. This produces

$$\mathbf{K} := \overline{\mathbf{F}}(x_4, x_3)/\langle 1 + x_3^2 + x_4^6 x_3 + x_4^{15} x_3^3 + x_4^{32} x_3^7 \rangle.$$

If $char \neq 2$, then there are two points Q_1 and Q_2 with x_4 as local parameter, with slightly different local units x_3 satisfying the above relation with x_4, but starting with constant term either i or $-i$.

In $char = 2$, $i = 1 = -i$, so continue with $x_5 := x_3 + 1$ to move the singularity to $x_5 = 0 = x_4$. Then $x_5 = x_4^3 x_6$ for $x_6 := x_5/x_4^3$ gives

$$\mathbf{K} = \overline{\mathbf{F}}_2(x_6, x_4)/\langle x_6^2 + (1 + x_4^3 x_6) + x_4^9 (1 + x_4^3 x_6)^3 + x_4^{26} (1 + x_4^3 x_6)^7 \rangle.$$

Use $x_7 := x_6 + 1$ to move the singularity to $x_7 = 0 = x_4$. Then use $(3)(1) - (2)(1) = 1$ to motivate $x_7 = x_9^3 x_8$, $x_4 = x_9^2 x_8$, with $x_9 := x_7/x_4$ and $x_8 := x_4^3/x_7^2$ to get

$$\mathbf{K} = \overline{\mathbf{F}}_2(x_9, x_8)/\langle x_8 + (1 + x_9^3 x_8) + x_9^{12} x_8^6 (1 + x_9^6 x_8^3 (1 + x_9^3 x_8))^3 + x_9^{46} x_8^{23} (1 + x_9^8 x_8^3 (1 + x_9^2 x_8))^7 \rangle.$$

Then there is only one point Q_1. [Note that by adding the extra term $x_2^6 x_1^5$ to the initial relation, $char = 3$ would have been the exception instead of $char = 2$. Or by adding the extra term $-2x_2^6 x_1^5$, even $char = 0$ could have been an exception to the first blowup being a resolution of the singularity at the origin.]

Chapter 7

Varieties

Definition 30. *The variety of an ideal I is*

$$V(I) := \{\underline{a} \ : \ f(\underline{a}) = 0 \text{ for all } f \in I\}.$$

For now it will remain ambiguous where $\underline{a}$ lives. In linear algebra, it is common to solve for such common zeros by row-reducing an augmented matrix to triangular form and then back-substituting. The generalization here is called elimination (32) and extension (33) That is, it is possible to eliminate one variable at a time, using a lex monomial ordering (9), then solve for the common zeros of the elements of the ideal in only the lowest variable, and extend those zeros recursively, one variable at a time.

7.1 Finite variety examples

Start with a very simple example:

$$I_2 := \langle x_2^2 - x_1, \ x_1^2 - x_1 \rangle \subset \mathbf{F}[x_2, x_1].$$

$I_1 := I_2 \cap \mathbf{F}[x_1] = \langle x_1^2 - x_1 \rangle$ eliminates x_2. The zeros of $x_1^2 - x_1$ are $x_1 = 0$ and $x_1 = 1$. These can be extended to $(x_2, x_1) = (0, 0)$, $(x_2, x_1) = (1, 1)$, and $(x_2, x_1) = (-1, 1)$. [There is reason to count $(0, 0)$ with multplicity 2, in that the number of zeros (when finite) should match the number of standard monomials; those being $\{1, \ x_1, \ x_2, \ x_2 x_1\}$ here.]

Try

$$(x_3^2 - 2x_3 - 3x_2, \ x_3 x_2 - 3x_2, \ x_3 x_1^2 - x_3 x_1, \ x_2^2 - x_2, \ x_2 x_1 - x_2, \ x_1^3 - x_1^2)$$

a lex Gröbner basis for the ideal I of $\mathbf{Q}[x_3, x_2, x_1]$ that it generates, has elimination ideals

$$I_2 := \langle \ x_2^2 - x_2, \ x_2 x_1 - x_2, \ x_1^3 - x_1^2 \ \rangle;$$

$$I_1 := \langle \ x_1^3 - x_1^2 \ \rangle.$$

The roots $x_1 = 0, 1$ of $x_1^3 - x_1^2 = 0$ can be extended.

$$\langle \ x_2^2 - x_2, \ x_2 x_1 - x_2, \ x_1^3 - x_1^2, \ x_1 - 0 \ \rangle;$$

$$\langle \ x_2^2 - x_2, \ x_2 x_1 - x_1, \ x_1^3 - x_1^2, \ x_1 - 1 \ \rangle;$$

have bases:

$$B_{2,0} := (x_2, \ x_1);$$

$$B_{2,1} := (x_2^2 - x_2,\ x_1 - 1)$$

respectively.

Then

$$\langle x_3^2 - 2x_3 - 3x_2,\ x_3x_2 - 3x_2,\ x_3x_1^2 - x_3x_1,\ x_2 - 0,\ x_1 - 0\rangle;$$

$$\langle x_3^2 - 2x_3 - 3x_2,\ x_3x_2 - 3x_2,\ x_3x_1^2 - x_3x_1,\ x_2 - 0,\ x_1 - 1\rangle;$$

$$\langle x_3^2 - 2x_3 - 3x_2,\ x_3x_2 - 3x_2,\ x_3x_1^2 - x_3x_1,\ x_2 - 1,\ x_1 - 1\rangle;$$

reduce respectively to

$$\langle x_3^2 - 2x_3,\ x_2,\ x_1\rangle;$$

$$\langle x_3^2 - 2x_3,\ x_2,\ x_1 - 1\rangle;$$

$$\langle x_3 - 3,\ x_2 - 1,\ x_1 - 1\rangle.$$

The variety $V(I)$ is $\{(0,0,0),\ (2,0,0),\ (0,0,1),\ (2,0,1),\ (3,1,1)\}$, as a set, though there is again algebraic reason to count $(0,0,0)$ twice.

7.2 Examples of dimension 1

Now try simple examples that are not finite, such as

$$I_2 := \langle x_2 - x_1^2\rangle.$$

Elimination gives $I_1 := \emptyset$, so $x_1 = (a_1)$ for any $a_1 \in \mathbf{F}$. Extension gives $(x_2, x_1) = (a_1^2, a_1)$ for any $a_1 \in \mathbf{F}$.

Try a slightly harder example,

$$I_2 := \langle x_2x_1 - 1\rangle.$$

Elimination gives $I_1 := \emptyset$; so $x_1 = a_1$ is a zero for any $a_1 \in \mathbf{F}$. Extension gives $(x_2, x_1) = (1/a_1, a_1)$ for $a_1 \neq 0$.

There are two ways to deal with this possible lack of extension when $a_1 = 0$. The first is to think in affine terms; and produce a theorem that explains when extension might fail, namely when the leading coefficient (here the leading coefficient of $x_2x_1 - 1$ being x_1) vanishes. The second is to think in other terms. The projective version with $x_2x_1 - x_0^2 = 0$ would be to extend $(x_1 : x_0) = (a_1 : 1)$ to $(x_2 : x_1 : x_0) := (1/a_1 : a_1 : 1)$ for $a_1 \neq 0$, $(x_1 : x_0) := (0 : 1)$ to $(x_2 : x_1 : x_0) := (1 : 0 : 0)$, and even $(x_1 : x_0) := (1 : 0)$ to $(x_2 : x_1 : x_0) := (0 : 1 : 0)$.

This may explain extension without failures; but the correspondence in the example between $(0 : 1)$ and its extension to $(1 : 0 : 0)$ is not straightforward. So maybe a better solution would be to look at zeros in $(\mathcal{P}^1(\mathbf{F}))^2$ instead of $\mathbf{F}^2$ or $\mathcal{P}^2(\mathbf{F})$. Then $x_1 = (a_1 : 1)$ extends to $(x_2, x_1) = ((1/a_1 : 1), (a_1 : 1))$ for $a_1 \neq 0$, $x_1 = (0 : 1)$ to $(x_2, x_1) = ((1 : 0), (0 : 1))$, and $x_1 = (1 : 0)$ to $(x_2, x_1) = ((0 : 1), (1 : 0))$.

CLO example 1, section 5, chapter 8, with ideal

$$I_2 := \langle\ x_2x_1^2 - x_2 + 1\ \rangle$$

has affine variety

$$V(I) := \{(-1/(a_1^2 - 1), a_1)\ :\ a_1 \in \mathbf{F}\backslash\{\pm 1\}\}$$

computable by elimination and extension using a lex monomial ordering, as above.

The projective version

$$I^{(h)} := \langle\ x_2x_1^2 - x_2x_0^2 + x_0^3\ \rangle,$$

would extend $(x_1 : x_0) = (a_1 : 1)$ to $(-1/(a_1^2 - 1) : a_1 : 1)$ for $a_1 \neq \pm 1$, would extend $(x_1 : x_0) = (\pm 1 : 1)$ to $(1 : 0 : 0)$, and would extend $(x_1 : x_0) = (1 : 0)$ to $(x_2 : x_1 : x_0) = (0 : 1 : 0)$ when viewed in $\mathcal{P}^2(\overline{\mathbf{F}})$.

The solution there is to use zeros in $\mathcal{P}^1(\mathbf{F}) \times \mathbf{F}$ to get $(x_1) = (\pm 1)$ extending to $((x_2 : x_0), x_1) = ((1 : 0), \pm 1)$. The suggestion here is to use zeros in $(\mathcal{P}^1(\mathbf{F}))^2$.

$$I^{(H)} := \langle\ x_2 x_1^2 - x_2 h_1^2 - h_2 x_1^2\ \rangle$$

would then extend $(x_1 : h_1) = (a_1 : 1)$ to $((-1/(a_1^2 - 1) : 1),), (a_1 : 1))$ for $a_1 \neq \pm 1$, extend $(x_1 : h_1) = (\pm 1 : 1)$ to $((1 : 0), (\pm 1 : 1))$, and extend $(x_1 : h_1) = (1 : 0)$ to $((x_2 : h_2), (x_1 : h_1)) = ((0 : 1), (1 : 0))$.

Make this slightly harder and symmetric as (14.2) with ideal

$$I_2 := \langle\ x_2^2 x_1^2 - x_2^2 - x_1^2\ \rangle$$

with affine variety

$$V(I) := \{(\pm a_1/\sqrt{a_1^2 - 1}, a_1)\ :\ a_1 \in \mathbf{F} \backslash \{\pm 1\}\}.$$

The projective version

$$I^{(h)} := \langle\ x_2^2 x_1^2 - x_2^2 x_0^2 - x_1^2 x_0^2\ \rangle,$$

would extend $(x_1 : x_0) = (a_1 : 1)$ to $(\pm a_1/\sqrt{a_1^2 - 1} : a : 1)$ for $a_1 \neq \pm 1$, would extend $(x_1 : x_0) = (\pm 1 : 1)$ to $(1 : 0 : 0)$, and would extend $(x_1 : x_0) = (1 : 0)$ to $(x_2 : x_1 : x_0) = (0 : 1 : 0)$ when viewed in $\mathcal{P}^2(\mathbf{F})$.

The suggested solution there is to use zeros in $\mathcal{P}^1(\mathbf{F}) \times \mathbf{F}$. to get $(x_1) = (\pm 1)$ extending to $((x_2 : x_0), x_1) = ((1 : 0), \pm 1)$. The suggestion here is to use zeros in $(\mathcal{P}^1(\mathbf{F}))^2$.

$$I^{(H)} := \langle\ x_2^2 x_1^2 - x_2^2 h_1^2 - h_2^2 x_1^2\ \rangle$$

would then extend $(x_1 : h_1) = (a_1 : 1)$ to $((\pm a/\sqrt{a_1^2 - 1} : 1),), (a_1 : 1))$ for $a_1 \neq \pm 1$, extend $(x_1 : h_1) = (\pm 1 : 1)$ to $((1 : 0), (\pm 1 : 1))$, and extend $(x_1 : h_1) = (1 : 0)$ to $((x_2 : h_2), (x_1 : h_1)) = ((0 : 1), (1 : 0))$.

$$V(I^{(H)}) = \{((1 : 0), (\pm 1 : 1)), ((\pm 1 : 1), (1 : 0))\}$$
$$\cup \{((\pm a/\sqrt{a^2 - 1} : 1), (a : 1)) : a \in \overline{\mathbf{F}} \backslash \{\pm 1\}\}.$$

This could be computed as an affine variety by appending the relations

$$(x_2 - 1)(h_2 - 1),\ h_2(h_2 - 1),\ (x_1 - 1)(h_1 - 1),\ h_1(h_1 - 1).$$

And this makes more sense in that there are clearly two values $x_1 = \pm 1$ at which affine extension fails, and projective extension doesn't help. At least the suggested variety and extension produces different extensions at these two points.

Try an example from the Klein quartic 13.1,

$$I_3 := \langle x_3 x_1 - x_2^2,\ x_3^2 + x_3 + x_2 x_1^3,\ x_3 x_2 + x_2 + x_1^4,\ x_2^3 + x_2 x_1 + x_1^5 \rangle.$$

The affine zeros $(x_3, x_2, x_1) = (a_2^2/a_1, a_2, a_1)$, with $a_2^3 + a_2 a_1 + a_1^5 = 0$ are not a problem for $a_1 \neq 0$. $a_1 = 0$ should extend to $(a_2, a_1) = (0, 0)$ and then to $(a_3, a_2, a_1) = (0, 0, 0)$ or $(a_3, a_2, a_1) = (1, 0, 0)$. Projectively, the homogenized version would have $(a_1 : a_0) = (1 : 0)$ extending to $(a_2 : a_1 : a_0) = (1 : 0 : 0)$, then to $(a_3 : a_2 : a_1 : a_0) = (1 : 0 : 0 : 0)$.

The suggestion here is that $(x_1 : h_1) = (1 : 0)$ extend to $((x_2 : h_2), (x_1 : h_1)) = ((1 : 0), (1 : 0))$ and then to $((x_3 : h_3), (x_2 : h_2), (x_1 : h_1)) = ((1 : 0), (1 : 0), (1 : 0))$. The suggestion from CLO would not seem to generalize. Maybe I'm missing something, but the examples of succesive blowups (**??**) worked out in the

literature are eluding me, as is the reason to settle for some mixed projective and affine set rather than what is proposed here.

So why is there even a suggestion of using zeros in $\mathcal{P}^m(\mathbf{F}) \times \mathbf{F}^n$? Maybe the answer comes from the idea of blowups (??), wherein projective coordinates are appended to affine ones to deal with the values of x_i/x_j at points at which both x_i and x_j vanish but the quotient could take on any projective value. The problem with this, again is that it doesn't generalize recursively, absent reducing mixed coordinate answers from one recursion to several affine answers before proceeding.

7.3 Elimination and extension

Definition 31. *Let $(R_j := \overline{\mathbf{F}}[x_j, \ldots, x_1] \ : \ 1 \le j \le n)$ be a nested sequence of multivariate polynomial rings with lex monomial ordering with $x_n \succ \cdots \succ x_1$. If I is an ideal of $R := R_n$, then the elimination ideals are*

$$I_j := I \cap \mathbf{F}[x_j, \ldots, x_1], \ 1 \le j \le n.$$

Theorem 32. *If B is a Gröbner basis for I then*

$$B_j := B \cap R_j, \ 1 \le j \le n$$

is a Gröbner basis for I_j.

Proof Clearly $\langle B_j \rangle \subseteq I_j$. If there were $f \in I_j$ but $f \notin \langle B_j \rangle$, then $LM(f)$ could not be divisible by $LM(b)$ for any $b \in B$.

Theorem 33. *If $(a_n, \ldots, a_1) \in V(I)$, then $(a_j, \ldots, a_1) \in V(I_j)$ extends to $(a_{j+1}, a_j, \ldots, a_1) \in V(I_{j+1})$.*

Computationally it is relatively easy to change either projective or rational problems into affine ones. The ideal

$$I^{(h)} := \langle x_n(x_{n-1} - 1) \cdots (x_1 - 1), x_{n-1}(x_{n-1} - 1) \cdots (x_0 - 1), \ \ldots, \ x_0(x_0 - 1) \rangle$$

can be appended to restrict F^{n+1} to $\mathcal{P}^n(\mathbf{F})$; while

$$I^{(H)} := \langle (x_n - 1)(h_n - 1), h_n(h_n - 1) \cdots (x_1 - 1)(h_1 - 1), h_1(h_1 - 1) \rangle$$

can be appended to restrict F^{2n} to $(\mathcal{P}^1(\mathbf{F}))^n$.

Consider the extension theorem from CLO 3.1. Written in our notation this is

Theorem 34 (CLO: The Extension Theorem)**.** *Write the elements of a Gröbner basis for $I := I_n \in R := R_n := \overline{\mathbf{F}}[x_n, \ldots, x_1]$ as $f_{j,k} \in R_j \backslash R_{j-1}$ for $1 \le k \le k(j)$, each viewed as an element of $R_{j-1}[x_j]$ with leading coefficient $g_{j,k} \in R_{j-1}$. If $(a_{j-1}, \ldots, a_1) \in V(I_{j-1})$ and $g_{j,k}(a_{j-1}, \ldots, a_1) \neq 0$ for some k, then there is at least one $a_j \in \overline{\mathbf{F}}$ such that $(a_j, \ldots, a_1) \in V(I_j)$.*

What is wrong with this? First, it is not constructive, and it doesn't really say that $V(I_n)$ is gotten by extension as our theorem does. The example considered there has $f_{2,1} := x_2 - x_1$, $f_{3,1} := x_3x_1 - 1$ and $f_{3,2} := x_3x_2 - 1$. While any $a_1 \in \overline{\mathbf{F}}$ extends to $a_2 = a_1$, this only extends to $a_3 = 1/a_1$ when $a_1 \neq 0$.

Were this done in rational terms, $f_{2,1} := x_2h_1 - x_1h_2$, $f_{3,1} := x_3x_1 - h_3h_1$ and $f_{3,2} := x_3x_2 - h_3h_2$. Any $(a_1 : b_1) \in \mathcal{P}(\overline{\mathbf{F}})$ extends to $(a_2 : b_2) = (a_1 : b_1)$, then to $(a_3 : b_3) = (b_1 : a_1)$.

But consider another example, with $f_{2,1} := x_2^3 + x_2x_1 + x_1^5$, $f_{3,1} := x_3x_1 - x_2^2$, and $f_{3,2} := x_3x_2 + x_2 + x_1^4$. Then any $a_1 \in \overline{\mathbf{F}}$ extends to a_2 such that $a_2^3 + a_2a_1 + a_1^5 = 0$, and there are between 1 and 3 such values. But the CLO extension theorem would say that this extends to $a_3 := a_2^2/a_1$ for $a_1 \neq 0$ (and $a_2 \neq 0$). It says nothing whatsoever about what happens when $a_1 = 0 = a_2$, yet this should extend to

any $a_3 \in \overline{\mathbf{F}}$. Our theorem says that constructively $f_{2,1}(x_2) = x_2^3 + x_2 a_1 + a_1^5 = 0$ produces the values a_2 extending a_1. Then for $a_1 = 0 = a_2$, $f_{3,1}(x_3, 0, 0) = 0 = f_{3,2}(x_3, 0, 0)$ means any $a_3 \in \overline{\mathbf{F}}$ extends; while for $a_1 \neq 0 \neq a_2$, $f_{3,1}(x_3, a_2, a_1) = x_3 a_1 - a_2^2 = 0$ and $f_{3,2}(x_3, a_2, a_1) = x_3 a_2 + a_2 + a_1^4 = 0$ have common solution $a_3 = a_2^2/a_1 = -(a_2 + a_1^4)/a_2$ as extension.

So were one to write a theorem of this flavor but constructively, do it in rational terms (with statement essentially the proof).

Theorem 35 (Constructive rational extension)**.** *Let*

$$d_j(x_j, h_j) := gcd\{f_{j,k}(x_j, h_j, a_{j-1}, b_{j-1}, \ldots, a_1, b_1) \ : \ 1 \leq k \leq k(j)\}.$$

- *If $d_j(x_j, h_j)$ depends on x_j, then there is extension to $(a_j : 1)$ for a_j any root of $d_j(x_j, 1)$.*
- *If it doesn't depend on x_j but does depend on h_j, then there is extension to $(a_j : b_j) = (1 : 0)$ and there is extension to $(a_j : b_j)$ when $d_j(x_j, 1) = 0$.*
- *If it is independent of both, then there is extension to any $(a_j : b_j) \in \mathcal{P}^1(\overline{\mathbf{F}})$.*

Chapter 8

Formal series

Definition 36.

$$f(t) := \sum_{j=0}^{\infty} f_j t^j$$

is called a formal power series. If the elements of the corresponding sequence $(f_j : j \in \mathbf{N})$ *of coefficients are implicitly assumed to come from the ring* R*, then* $f(t) \in R[[t]]$ *(with a local monomial ordering (8)). It is common in other areas of mathematics to call* $f(t)$ *a generating function for the sequence of coefficients.*

Formal power series can be added and multiplied just as with power series in general; the difference being that there is no evaluation map with which to be concerned, hence no analytical baggage involving convergence and related subjects.

It is probably a worthwhile exercise to write down addition and multiplication rules for formal power series. But more importantly computationally it is probably more important to think about how to represent them finitely. That is, unless there is a nice closed form, as, say a rational function, then probably the best that can be done is to store the first m terms. [This is not unlike defining Taylor polynomials as initial parts of Taylor series, though polynomials should really be written in global form with the largest power of t leftmost, and Taylor polynomials in local form, with the smallest power of t leftmost. That is, the ordering is implicitly a local monomial ordering (8), in that $1 \succ t$ (as opposed to a global assumption that $t \succ 1$). Local reduction rules are tricky in that a rule such as $t \mapsto t^2$, if allowed, could be applied countably many times to keep reducing t forever.

Definition 37.

$$f(t) := \sum_{j=s}^{\infty} f_j t^j$$

with $s \in \mathbf{Z}$ *is called a formal Laurent series.*

Addition and multiplication are a bit harder to define for Laurent series than for power series, if proper attention is given to the least subscript. [Again, it is probably a worthwhile exercise to try to define these before searching for a definition.]

Both of these ideas can be generalized as well to more than one formal variable, with more than one choice of local monomial ordering, subject of course to the local assumption $1 \succ t_j$ for each j.

What are the examples of series in this context? The first is in expanding functions at points on a curve. So, for instance, the curve defined by the relation $xy - 1 = 0$ has points P_a with local paramaters t_a and

series expansions that can be written as

$$x = a + t_a,\ y = \frac{1}{a + t_a}.$$

Of course

$$\frac{1}{a+t_a} = \frac{1}{a}\left(\frac{1}{1+t_a/a}\right) = \frac{1}{a}\sum_{j=0}^{\infty}\left(\frac{-t}{a}\right)^j = \sum_{j=0}^{\infty}\left(\frac{(-1)^j}{a^{j+1}}\right)t^j.$$

When $a = 0$ this reduces to just $x = t_0,\ y = 1/t_0$; whereas for $a = \infty$ (if considered), then (by symmetry) it should be that $x = 1/t_\infty,\ y = t_\infty$.

A second example comes from Rees algebras. These are generating functions for powers of an ideal.

Definition 38. *Let $I := \langle g_1, \ldots, g_s\rangle$ be an ideal of the multivariate polynomial ring R. Let $R[It] := \sum_{j=0}^{\infty} I^j t^j$ with $I^0 := R$. Since it is an element of the polynomial ring $R[t]$, consider the ring map*

$$\phi[G_1, \ldots, G_s] \ : \ R \to R[t]$$

defined by extending $\phi(G_i) := g_i t$. Then $R[G_1, \ldots, G_s]/ker(\phi)$ is a presentation of the Rees algebra of $I \in R$, the Rees algebra itself being the image, a subset of $R[t]$.

Usually in this context, the local monomial ordering is called a grading and the image of the map ϕ is not referred to as either a formal power series or a generating function.

This presentation allows for the computation of integral closures of ideals by reducing that problem to one of integral closures of rings (47). See below for this, and for an alternative to Rees algebras, and an alternative method for computing integral closures of ideals.

8.1 Points using coordinates or Laurent series

The example ideal above

$$I := \langle\, x_2^2 x_1^2 - x_2^2 - x_1^2 \,\rangle$$

has divisors

$$((x_2)) = (-1)\cdot P_1 + (-1)\cdot P_2 + 0\cdot P_3 + 0\cdot P_4 + 1\cdot P_5 + 1\cdot P_6;$$
$$((x_1)) = 0\cdot P_1 + 0\cdot P_2 + (-1)\cdot P_3 + (-1)\cdot P_4 + 1\cdot P_5 + 1\cdot P_6.$$

as bookkeeping devices for the number of poles or zeros of the variables viewed as rational functions relative to different points, whatever points are.

The Laurent series (37) in the local parameters t_i at point P_i for these could be

$$\begin{array}{rclrcl}
x_1 &=& 1 + u_1 t_1 & x_2 &=& 1/t_1 \\
x_1 &=& -1 + u_2 t_2 & x_2 &=& 1/t_2 \\
x_1 &=& 1/t_3 & x_2 &=& 1 + u_3 t_3 \\
x_1 &=& 1/t_4 & x_2 &=& -1 + u_4 t_4 \\
x_1 &=& t_5 & x_2 &=& i t_5 + u_5 t_5^2 \\
x_1 &=& t_6 & x_2 &=& -i t_6 + u_6 t_6^2
\end{array}$$

for u_i some series expansion for $1 \le i \le 6$.

For other points P_j,

$$x_1 = x_1(P) + t_j,\ x_2 = x_2(P) + t_j u_j$$

with $x_2(P) = \pm x_1(P)/\sqrt{x_1^2(P) - 1}$ for $x_1(P) \neq \pm 1$.

Clearly this is more descriptive information than just having affine coordinates: $(x_2(P_j), x_1(P_j))$ in that there are some points with Laurent series that are not power series which shouldn't have affine coordinates; and an affine set of coordinates relative to a particular set of rational functions may not be sufficient to distinguish points.

It should also be pointed out again that power series and Laurent series implicitly use a local monomial ordering in that the assumption is that $t^i \succ t^j$ for $i < j$. So polynomials in t written as series will be in the reverse order to that used when they are written as polynomials.

Chapter 9

Elimination and Extension

From Cox, Little, and O'Shea, chapter 3, section 1

Theorem 39. *The Extension Theorem* *Let* $I := \langle f_1, \ldots, f_s \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ *and let* I_1 *be the first elimination ideal for* I. *For each* $1 \leq i \leq s$, *write* f_i *in the form*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms in which } x_i \text{ has degree } < N_i,$$

Suppose that we have a partial solution $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. *If* $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, *then there exists* $a_1 \in \mathbf{C}$ *such that* $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

This is proven in chapter 3, section 6, with exercises to make it constructive and generalize it to any algebraically closed field, not just $\mathbf{C}$.

There is even an example suggested, using the equations $xy = 1$ and $xz = 1$, given to show that the only partial solution that doesn't extend is $(y, z) = (0, 0)$.

Consider this theorem very carefully.

From the theorem itself it is not clear whether the intent was to start with a Gröbner basis for I. And indeed the example is not in terms of a Gröbner basis, as that would have been $\{xz - 1, y - z\}$.

Yet it is follwed by examples with more than one step in which a Gröbner basis is computed as a first step.

But then there is

Theorem 40. *The Closure Theorem* *Let* $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{C}^n$ *and let* I_l *be the* l*th elimination ideal of* $(f_1, \ldots, f_s)$. *Then:*

- $\mathbf{V}(I_l)$ *is the smallest affine variety containing* $\pi_l(V) \subset \mathbf{C}^{n-l}$.
- *When* $V \neq \emptyset$ *there is an affine variety* $W \subset\neq V(I_l)$ *such that* $V(I_l) - W \subset \pi_l(V)$.

This puts the emphasis on how $V(I_l)$ and $\pi_l(V)$ are related; whereas the emphasis should be on recursively constructing $V(I)$ one elimination ideal at a time. That is, given a partition of $V(I_{j-1})$, it should be possible to constructively produce a partition of $V(I_j)$.

One can argue that going back and computing varieties of the missing W will fill in the missing part of $V(I)$; but this should have been part of the original extension theorem, or at least be mentioned as a corollary of the closure theorem, if indeed it follows from that.

For $1 \leq j \leq n$, let $R_j := \overline{\mathbf{F}}[x_j, \ldots, x_1]$, with lex monomial ordering $x_j \succ \cdots \succ x_1$ be a nested set of multivariate polynomial rings over the algebraically closed field $\overline{\mathbf{F}}$ (here with $\mathbf{F}$ the rationals or a finite field).

Theorem 41 (Affine Elimination Theorem). *If B is a Gröbner basis for the ideal I of $R := R_n$, then $B_j := B \cap R_j$ is a Gröbner basis for $I_j := I \cap R_j$, for $1 \leq j \leq n$.*

Proof : If $f \in I_j$ then there is some $b \in B$ with $LM(b)|LM(f)$. But then $LM(f) \in R_j$ implies that $LM(b) \in R_j$; and the lex monomial ordering gives that $b \in R_j$. So $b \in B_j$.

The reason to define these elimination ideals I_j relative to the lex monomial ordering on R would seem to be to be able to recursively construct the varieties $V(I_j)$ for $1 \leq j \leq n$ to get $V(I) = V(I_n)$.

Algorithm 42 (Affine Extension Algorithm). *The following algorithm computes a partition $\dot{\cup} V_{\underline{m}}(I_j)$ of $V(I_j)$ for $1 \leq j \leq n$ recursively, using input $B = B_n$ a Gröbner basis for $I = I_n$.*

$$V_{\underline{m}}(I_j) := \{(a_j, \ldots, a_1) \in \overline{\mathbf{F}}^j \ : \ P_{\underline{m}}(I_j)\}$$

for some set of conditions $P_{\underline{m}}(I_j)$ consisting of equalities and inequalities. [*It does not use any factorization subroutine, but one could be used in conjunction with it.*]

Suppose that the partition $\dot{\cup} V_{\underline{m}}(I_{j-1})$ of $V(I_{j-1})$ is given. To extend the part $V_{\underline{m}}(I_{j-1})$:

1. *Initialize $Q := P_{\underline{m}}(I_{j-1})$ and $l := 0$.*
2. $$A := interreduce\{b_i^*(x_j) := b_i(x_j, a_{j-1}, \ldots, a_1) \ : \ (a_j, \ldots, a_1) \text{ satisfies } Q \text{ and } b_i(x_j, \ldots, x_1) \in B_j \backslash B_{j-1}\},$$
   viewed as a set of elements of $\overline{\mathbf{F}}[a_{j-1}, \ldots, a_1][x_j]$.
3. *If A has no non-zero elements, then any $a_j \in \overline{\mathbf{F}}$ can be used for extension. So set $P_{\underline{m},l}(I_j) := Q$, and stop.*
4. *Otherwise let $f(x_j)$ be the smallest non-zero element of A.*
5. *If $f \in \overline{\mathbf{F}}$, then setting $f(a_j) = 0$ is a contradiction, so stop.*
6. *Otherwise let $c := radical(LC(f))$. If the conditions $Q \cup \{c \neq 0\}$ are non-contradictory, set*
   $$P_{\underline{m},l}(I_j) := Q \cup \{c \neq 0\} \cup \{f(a_j) = 0\}$$
   and increment l.
7. *If the conditions $Q \cup \{c = 0\}$ are non-contradictory, replace Q by them and return to step 2.*

Proof : The algorithm just breaks the problem into cases. The main thing to prove is that roots of the smallest non-zero polynomial in A are roots of all the polynomials in A, so that these produce the only extensions in each case.

Suppose that the non-zero elements of A are ordered so that $f_0(x_j) \prec \cdots \prec f_s(x_j)$. Then because of the lex monomial ordering

$$LM(f_{r-1}(x_j)) f_r(x_j) = \sum_{k=0}^{r-1} c_k(x_j, a_{j-1}, \ldots, a_1) f_k(x_j)$$

for each $1 \leq r \leq s$, with $LM(f_{r-1}(x_j))$ independent of x_j. So if $f_k(a_j) = 0$ for all $k < r$ then $f_r(a_j) = 0$ as well. In particular any root of $f_0(x_j)$ must be a root of $f_r(x_j)$ for all $0 \leq r \leq s$. And, of course, any extension value a_j must be a root of all of these as well.

Consider the following test examples:

1. $$I := \langle x_2 x_1 \rangle$$
2. $$I := \langle x_3 x_1,\ x_3 x_2 \rangle$$
3. $$I := \langle (x_2^2+1)(x_1^2-1),\ x_3(x_2^2+1),\ x_3^2 x_1 + x_3 x_2 + x_1^2 - 1 \rangle$$
4. $$I := \langle x_3^2 x_1^2 + x_3 x_2 + x_1^3,\ x_3^2(x_2+x_1) + x_3 x_1^2 + x_2^2 \rangle$$
5. $$I := \langle x_3 x_1 - 1,\ x_3 x_2 - 1 \rangle = \langle x_2 - x_1,\ x_3 x_1 - 1 \rangle$$
6. The Lagrange multiplier problem from CLO.
7. The robotics problem from CLO.

The first shows that while

$$V(I_2) = \{(a_2, a_1) \in \overline{\mathbf{F}} \ :\ a_1 \neq 0,\ a_2 = 0\} \cup \{(a_2, a_1) \in \overline{\mathbf{F}} \ :\ a_1 = 0\},$$

the extension theorem in CLO would say nothing about the case $a_1 = 0$. And the closure theorem would just say that the case $a_1 = 0$ was missed. So instead of producing the union of two lines, the two theorems produce one line, pointing out that one point of it is missing.

The third is a little more intricate in that extension from $V(I_1)$ to $V(I_2)$ would be silent on the case $x_1^2 - 1 = 0$. Then having already dismissed that case, the theorem would have been silent on the case $x_2^2 + 1 = 0$ in extending $V(I_2)$ to $V(I_3)$.

That is, even with both theorems, there is no real attempt at producing the variety $V(I)$, just in deciding to leave out certain parts of it so that the supposedly largest part can be constructed.

Note also that in the algorithm above, resultants were not mentioned. They were replaced by interreduction and a syzygy. But had they not, the resultants are sloppy substitutes for computations of gcd's relative to a given variable in a multivariate polynomial ring setting.

As a non-trivial example, consider:

```
P=QQ[a3,a2,a1,MonomialOrder=>Lex];
R=P[x3,x2,x1,MonomialOrder=>Lex];
I=ideal(x3^2*(x2+x1)+x3*x1^2+x2^2,x3^2*x1^2+x3*x2+x1^3);
toString(gens gb I)
------------------------
x2^5+x2^4*x1^4+x2^4*x1-2*x2^3*x1^5-x2^3*x1^4
   -x2^2*x1^6-x2^2*x1^5+2*x2*x1^7-x2*x1^6+x1^9+x1^8,
------------------------
x3*x1^9-4*x3*x1^7-x3*x1^5+2*x2^4+2*x2^3*x1^4+x2^3*x1^3+x2^3*x1
   +x2^2*x1^7-5*x2^2*x1^5-x2*x1^8+x2*x1^6-2*x2*x1^5-x1^9-x1^8+3*x1^7-x1^6,
2*x3*x2*x1^3-x3*x1^6+x3*x1^4-x2^3-x2^2*x1^4+x2*x1^5+x1^6+x1^5,
x3*x2^2+x3*x2*x1-x3*x1^4-x2^2*x1^2+x2*x1^3+x1^4, x3^2*x1^2+x3*x2+x1^3,
x3^2*x2+x3^2*x1+x3*x1^2+x2^2

I1=I+ideal(x1-a1);
toString gens gb I1

x2^5+(a1^4+a1)*x2^4+(-2*a1^5-a1^4)*x2^3+(-a1^6-a1^5)*x2^2
   +(2*a1^7-a1^6)*x2+a1^9+a1^8,

(a1^9-4*a1^7-a1^5)*x3+2*x2^4+(2*a1^4+a1^3+a1)*x2^3+(a1^7-5*a1^5)*x2^2
   +(-a1^8+a1^6-2*a1^5)*x2-a1^9-a1^8+3*a1^7-a1^6,
2*a1^3*x3*x2+(-a1^6+a1^4)*x3-x2^3-a1^4*x2^2+a1^5*x2+a1^6+a1^5,
x3*x2^2+a1*x3*x2-a1^4*x3-a1^2*x2^2+a1^3*x2+a1^4, a1^2*x3^2+x3*x2+a1^3,
x3^2*x2+a1*x3^2+a1^2*x3+x2^2}}
-------
I2=I1+ideal(x2-a2);
toString gens gb I2

a2^5+a2^4*a1^4+a2^4*a1-2*a2^3*a1^5-a2^3*a1^4-a2^2*a1^6
   -a2^2*a1^5+2*a2*a1^7-a2*a1^6+a1^9+a1^8,

(a1^9-4*a1^7-a1^5)*x3
   +2*a2^4+2*a2^3*a1^4+a2^3*a1^3+a2^3*a1+a2^2*a1^7-5*a2^2*a1^5
   -a2*a1^8+a2*a1^6-2*a2*a1^5-a1^9-a1^8+3*a1^7-a1^6,
(2*a2*a1^3-a1^6+a1^4)*x3
   -a2^3-a2^2*a1^4+a2*a1^5+a1^6+a1^5,
(a2^2+a2*a1-a1^4)*x3
   -a2^2*a1^2+a2*a1^3+a1^4, a1^2*x3^2+a2*x3+a1^3,
(a2+a1)*x3^2+a1^2*x3+a2^2

radical ideal (a1^9-4*a1^7-a1^5)
--P_{0,0,0}=\{ a_1^5-4a_1^3-a_1\neq 0,\
--(a1^9-4*a1^7-a1^5)*a3
--   +2*a2^4+2*a2^3*a1^4+a2^3*a1^3+a2^3*a1+a2^2*a1^7-5*a2^2*a1^5
--   -a2*a1^8+a2*a1^6-2*a2*a1^5-a1^9-a1^8+3*a1^7-a1^6=0\}
```

```
I001=I2+ideal(a1^5-4*a1^3-a1);
toString gens gb I001
a1^5-4*a1^3-a1,
a2^2*a1^4-4*a2^2*a1^2-a2^2,
2*a2^4+a2^3*a1^3+8*a2^3*a1^2+a2^3*a1+2*a2^3
   -3*a2^2*a1^3-a2^2*a1-13*a2*a1^4-8*a2*a1^3-3*a2*a1^2
   -2*a2*a1-21*a1^4-21*a1^3-5*a1^2-5*a1,

(2*a2-a1^3+a1)*x3+4*a2^3*a1^3-17*a2^3*a1-a2^2*a1+a2*a1^2+a1^3+a1^2,
2*a1*x3^2+(-a1^4+5*a1^2)*x3-4*a2^3*a1^2+17*a2^3+a2^2-a2*a1+a1^2-a1

--P_{0,0,1}=\{ a1^5-4*a1^3-a1=0,
               a2^2*a1^4-4*a2^2*a1^2-a2^2=0,
               2*a2^4+a2^3*a1^3+8*a2^3*a1^2+a2^3*a1+2*a2^3
                  -3*a2^2*a1^3-a2^2*a1-13*a2*a1^4-8*a2*a1^3-3*a2*a1^2
                  -2*a2*a1-21*a1^4-21*a1^3-5*a1^2-5*a1=0,\
                2*a2-a1^3+a1\neq 0,\
       (2*a2-a1^3+a1)*a3+4*a2^3*a1^3-17*a2^3*a1-a2^2*a1+a2*a1^2+a1^3+a1^2=0\}
I002=I001+ideal(1*a2-a1^3+a1);
toString gens gb I002

a1,
a2
--P_{0,0,2}=\{ a1=0,\ a2=0\}
```

```
P=QQ[a4,a3,a2,a1,MonomialOrder=>Lex];
R=P[x6,x5,x4,x3,x2,x1,MonomialOrder=>Lex];
I=ideal(x6^2+x5^2-1,x4^2+x3^2-1,x6*x4-x5*x3+x4-x2,x6*x3+x5*x4+x3-x1);
toString(gens gb I)
----------------
---------------
4*x3^2*x2^2+4*x3^2*x1^2-4*x3*x2^2*x1-4*x3*x1^3+x2^4+2*x2^2*x1^2-4*x2^2+x1^4,
2*x4*x2+2*x3*x1-x2^2-x1^2,
4*x4*x3*x1-2*x4*x1^2-4*x3^2*x2+2*x3*x2*x1-x2^3-x2*x1^2+4*x2,
x4^2+x3^2-1,
x5-x4*x1+x3*x2,
2*x6-x2^2-x1^2+2
----------------------------
I2=I+ideal(x1-a1,x2-a2);
toString gens gb I2

(4*a2^2+4*a1^2)*x3^2+(-4*a2^2*a1-4*a1^3)*x3+a2^4+2*a2^2*a1^2-4*a2^2+a1^4,

2*a2*x4+2*a1*x3-a2^2-a1^2,
4*a1*x4*x3-2*a1^2*x4-4*a2*x3^2+2*a2*a1*x3-a2^3-a2*a1^2+4*a2,
x4^2+x3^2-1,
x5-a1*x4+a2*x3,
2*x6-a2^2-a1^2+2

--P_{0,0,0}=\{ a2^2+a1^2\neq 0,\
--(4*a2^2+4*a1^2)*a3^2+(-4*a2^2*a1-4*a1^3)*a3+a2^4+2*a2^2*a1^2-4*a2^2+a1^4=0\}

I001=I2+ideal(a2^2+a1^2);
toString gens gb I001

a1^2,
a2*a1,
a2^2,

a2*x4+a1*x3,
a1*x4*x3-a2*x3^2+a2,
x4^2+x3^2-1,
x5-a1*x4+a2*x3,
x6+1

I002=I001+ideal(a2,a1,x3-a3);
toString gens gb I002

a1,
a2,
x4^2+a3^2-1,
x5,
x6+1
```

```
--P_{0,0,1}=\{ a1=0,\ a2=0\}

I0000=I2+ideal(x3-a3);
toString gens gb I0000

4*a3^2*a2^2+4*a3^2*a1^2-4*a3*a2^2*a1-4*a3*a1^3+a2^4+2*a2^2*a1^2-4*a2^2+a1^4

2*a2*x4+2*a3*a1-a2^2-a1^2,
(4*a3*a1-2*a1^2)*x4-4*a3^2*a2+2*a3*a2*a1-a2^3-a2*a1^2+4*a2,
x4^2+a3^2-1,

x5-a1*x4+a3*a2,
2*x6-a2^2-a1^2+2

--P_{0,0,0,0}=\{ a2^2+a1^2\neq 0,\
--4*a3^2*a2^2+4*a3^2*a1^2-4*a3*a2^2*a1-4*a3*a1^3+a2^4+2*a2^2*a1^2-4*a2^2+a1^4=0,\
-- a2\neq 0,\ 2*a2*a4+2*a3*a1-a2^2-a1^2=0\}

I0001=I0000+ideal(a2);
toString gens gb I0001

a2,
2*a3*a1-a1^2

x4^2+a3^2-1,

x5-a1*x4,
2*x6-a1^2+2

--P_{0,0,0,1}=\{ a2=0, a1\neq 0,\ 2*a3-a1=0,\ a4^2+a3^2-1=0\}
```

Consider the example from the middle of page 119 in CLO, rewritten in this notation:

$$I := \langle x_3x_2 - 1,\ x_3x_1 - 1\rangle.$$

Using the algorithm above, a Gröbner basis $B := \{x_2 - x_1,\ x_3x_1 - 1\}$ is computed. Then $P_0 = \emptyset$ and $P_{0,0} = \{a_2 - a_1 = 0\}$ are straightforward. But then there are two cases, $P_{0,0,0} = \{a_2 - a_1,\ a_1 \neq 0,\ a_3a_1 - 1 = 0\}$ and $P_{0,0,1} = \{a_2 - a_1 = 0, a_1 = 0, -1 = 0\}$. There is no extension in the latter case.

The analysis in the book is that extension might fail to happen when the coefficients a_2, a_1 in $x_3a_2 - 1$ and $x_3a_1 - 1$ are both 0.

So let's change this slightly.

$$I := \langle x_3x_2,\ x_3x_1\rangle.$$

Using the algorithm above, a Gröbner basis $B := \{x_3x_2,\ x_3x_1\}$ is computed. Then $P_0 = \emptyset$ and $P_{0,0} = \emptyset$ are straightforward. But then there are several cases,

$$P_{0,0,0} = \{a_1 \neq 0,\ a_3 = 0\},\ P_{0,0,1} = \{a_1 = 0,\ a_2 \neq 0,\ a_3 = 0\},\ P_{0,0,2} = \{a_1 = 0,\ a_2 = 0\}.$$

Following the analysis in the book, extension might fail to happen when the coefficients a_2, a_1 in x_3a_2 and x_3a_1 are both 0, which is case $(0, 0, 2)$ above, where extension should happen, but is not explained by their extension theorem.

Now let's consider their closure theorem applied to these examples.

$$\pi_2(V(I_3)) = \{(a_2, a_1) \in \overline{\mathbf{F}}^2 \ : \ a_2 - a_1, \ a_1 \neq 0\}.$$

$$V(I_2) = \{(a_2, a_1) \in \overline{\mathbf{F}} \ a_2 - a_1 = 0\}$$

So $W_2 = \{(0,0)\}$ is the difference.

$$\pi_1(V(I_3)) = \{(a_1) \in \overline{\mathbf{F}} \ : \ a_1 \neq 0\}.$$

$$V(I_1) = \{(a_1) \in \overline{\mathbf{F}}\}$$

So $W_1 = \{(0)\}$ is the difference.

In the altered example, we have to deal with the problem of their extension theorem not giving all of $V(I_3)$. So are we meant to apply closure to what comes out of their extension theorem, or are we meant to know what $V(I_3)$ actually is?

If we know

$$V_{0,0,0}(I_3) = \{(a_3, a_2, a_1 \in \overline{\mathbf{F}}^3 \ : \ a_1 \neq 0, \ a_3 = 0\},$$

$$V_{0,0,1}(I_3) = \{(a_3, a_2, a_1) \in \overline{\mathbf{F}}^3 \ : \ a_1 = 0, \ a_2 \neq 0, \ a_3 = 0\},$$

and

$$V_{0,0,2}(I_3) = \{(a_3, a_2, a_1 \in \overline{\mathbf{F}}^3 \ : \ a_1 = 0, \ a_2 = 0\};$$

then

$$\pi_2(V_{0,0,0}(I_3)) = \{(a_2, a_1 \in \overline{\mathbf{F}}^2 \ : \ a_1 \neq 0\},$$

$$\pi_2(V_{0,0,1}(I_3)) = \{(a_2, a_1) \in \overline{\mathbf{F}}^2 \ : \ a_1 = 0, \ a_2 \neq 0\},$$

and

$$\pi_2(V_{0,0,2}(I_3)) = \{(a_2, a_1 \in \overline{\mathbf{F}}^2 \ : \ a_1 = 0, \ a_2 = 0\};$$

which is all of $\overline{\mathbf{F}}^2$. But if we couldn't figure out $V_{0,0,2}(I_3)$, then we would be missing $W = \{(0,0)\}$. Does this give us any further insight into extension? No. So what does it do?

I claim that their extension only guarantees there is at least one extension under certain conditions, and doesn't really produce all extensions. Similarly, the closure theorem only suggests that sometimes there are clearly sets that don't extend, with some nebulous claim that what is missed is smaller than what is not.

But try the really simple-minded example of the union of two lines:

$$I := \langle x_2 x_1 \rangle.$$

$P_0 = \emptyset$, $P_{0,0} = \{a_1 \neq 0, a_2 = 0\}$, $P_{0,1} = \{a_1 = 0\}$.

Their extension theorem would only apply to give $V_{0,0}(I_2)$, with no claim when $a_1 = 0$. Their closure theorem applied to only $V_{0,0}(I_2)$ would give $W = \{0\}$ missing, whereas applied to $V(I_2)$ would give $V(I_1)$. But there isn't even a suggestion that one should go back and examine the case in which $a_1 = 0$ to see if there is indeed any extension there. So maybe they miss one of the two lines altogether.

$$I := \langle (x_2^2+1)(x-1^2-1),\ x_3(x_2^2+1),\ x_3^2x_1+x_3x_2+x_1^2-1\rangle.$$

$$P_0 = \emptyset.$$

$$B(0,0) = (x_2^2+1)(a_1^2-1)$$

$$P_{0,0} = \{a_1^2-1\neq 0,\ a_2^2+1=0\}$$

$$B(0,1) = \emptyset$$

$$P_{0,1} = \{a_1^2-1=0\}$$

$$B(0,0,0) = \{x_3^2a_1+x_3a_2+a_1^2-1\}$$

$$P_{0,0,0} = \{a_1^2-1\neq 0,\ a_2^2+1=0,\ a_1\neq 0,\ a_3^2a_1+a_3a_2+a_1^2-1=0\}$$

$$B(0,0,1) = \{x_3a_2-1\}$$

$$P_{0,0,1} = \{a_1=0,\ a_2^2+1=0,\ a_3a_2-1=0\}$$

$$B(0,1,0) = \{x_3(a_2^2+1),\ x_3^2a_1+x_3a_2\}$$

$$P_{0,1,0} = \{a_1^2-1=0,\ a_2^2+1\neq 0,\ a_3^2a_1+a_3a_2=0\}$$

$$B(0,1,1) = \{x_3^2a_1+x_3a_2\}$$

$$P_{0,1,1} = \{a_1^2-1=0,\ a_2^2+1=0,\ a_3^2a_1+a_3a_2=0\}$$

Using CLO extension only $V_{0,0}(I_2)$ would have been found. Then $V_{0,0,0}(I_3)$ would have been found.

So we'll try for elimination and extension to look like

$$((a_n : b_n), \ldots, (a_1 : b_1)) \in V(I_n) \subseteq (\mathbf{P}^1(\overline{\mathbf{F}}))^n \equiv ((a_j : b_j), \ldots, (a_1 : b_1)) \in V(I_j) \subseteq (\mathbf{P}^1(\overline{\mathbf{F}}))^j.$$

Let $R_j := \overline{\mathbf{F}}[x_j, \ldots, x_1]$ for $1 \leq j \leq n$ be a nested sequence of multivariate polynomial rings, each with the lex monomial ordering. Let I be an ideal of $R := R_n$, with Gröbner basis B.

Proposition 43. *$I_j := I \cap R_j$ is an ideal of R_j with Gröbner basis $B_j := B \cap R_j$ for each $1 \leq j \leq n$.*

Proof It is straightforward to see that I_j is an ideal of R_j, regardless of the monomial ordering. If $f \in I_j$, then $f \in I$. So there is some $b \in B$ with $LM(b)|LM(f)$. But $LM(f) \in R_j$, so $LM(b) \in R_j$. In the lex monomial ordering, this implies that $b \in R_j$.

Proposition 44. *If $((a_n : b_n), \ldots, (a_1 : b_1)) \in V(I)$, then $((a_j : b_j), \ldots, (a_1 : b_1)) \in V(I_j)$ for all $1 \leq j \leq n$.*

Proof Straightforward.

Proposition 45. *If $((a_{j-1} : b_{j-1}), \ldots, (a_1 : b_1)) \in V(I_{j-1})$ for some $1 \leq j \leq n$, then there is at least one extension $((a_j : b_j), \ldots, (a_1 : b_1)) \in V(I_j)$.*

Proof Suppose that $B_j \backslash B_{j-1}$ is non-empty. For each $b \in B_j \backslash B_{j-1}$, consider $b((x_j : h_j), (a_{j-1} : b_{j-1}), \ldots, (a_1 : b_1)$ as an element of $S_j := \overline{\mathbf{F}}[x_j : h_j]$ of some degree d. That is,

$$b(x_j : h_j) = \sum_{k=0}^{d} x_j^{d-k} h_j^k \phi_k((a_{j-1} : b_{j-1}), \ldots, (a_1 : b_1)).$$

If $\phi_0((a_{j-1} : b_{j-1}), \ldots, (a_1 : b_1)) = 0$ but $b(x_j : h_j) \not\equiv 0$, then either $(x_j : h_j) = (1 : 0)$ is the only extension, or there is a smaller polynomial satisfied by ????

Corollary 46. *$V(I_j)$ is the set of all such extensions of $V(I_{j-1})$.*

Proof Straightforward????

Chapter 10

Evaluation

Let $R := \overline{\mathbf{F}}[x_n, \ldots, x_1]$ be a multivariate polynomial ring. Let $I := \langle g_1, \ldots, g_s \rangle$ be an ideal of R. Let $A := R/I$ be the corresponding quotient ring. Its field of fractions $Q(A) := \overline{\mathbf{F}}(x_n, \ldots, x_1)/I$ is a function field, $\mathbf{K}$. By definition then each $f(x_n, \ldots, x_1) \in \mathbf{K}$ can be written at least one way as a quotient of polynomials, say,

$$f(x_n, \ldots, x_1) = \frac{num(f)(x_n, \ldots, x_1)}{den(f)(x_n, \ldots, x_1)},$$

with $den(f)(x_n, \ldots, x_1)$ not the zero function and $gcd(num(f), den(f)) = 1$.

So it would seem natural to try to evaluate $f(x_n, \ldots, x_1)$ by choosing $(a_m, \ldots, a_1) \in \overline{\mathbf{F}}^n$ and defining

$$f(a_n, \ldots, a_1) = \frac{num(f)(a_n, \ldots, a_1)}{den(f)(a_n, \ldots, a_1)}.$$

For this to be well-defined it must be that $g_i(a_n, \ldots, a_1) = 0$ for $1 \leq i \leq s$ and that $den(f)(a_n, \ldots, a_1) \ncong 0$.

This leads to considering the affine variety

$$V := \{(a_n, \ldots, a_1) \in \overline{\mathbf{F}}^n \ : \ g_i(a_n, \ldots, a_1) = 0, \ 1 \leq i \leq s\}.$$

We talk about points $P := (a_n, \ldots, a_1) \in \overline{\mathbf{F}}^n$, with coordinates a_j in that there are obvious coordinate functions $x_j/1$ with $(x_j/1)(a_n, \ldots, a_1) = a_j/1 = a_j \in \overline{\mathbf{F}}$.

Suppose we try to write this projectively. If $D_1 := deg(num(f))$, $D_2 := deg(den(f))$, and $D := max\{D_1, D_2\}$, then $\overline{num}(f)(x_n, \ldots, x_0) := x_0^{D-D_1} num(f)(x_n/x_0, \ldots, x_1/x_0)$ and $\overline{den}(f)(x_n, \ldots, x_0) := x_0^{D-D_1} den(f)(x_n/x_0, \ldots, x_1/x_0)$ are both homogeneous polynomials of degree D, so

$$\overline{f}(x_n, \ldots, x_0) = \frac{\overline{num}(f)(x_n, \ldots, x_0)}{\overline{den}(f)(x_n, \ldots, x_0)}$$

is a homogeneous, rational function of degree D.

For $(a_n : \cdots : a_0) \in \mathbf{P}^n(\overline{\mathbf{F}})$

$$\overline{f}(a_n, \ldots, a_0) = \frac{\overline{num}(f)(a_n, \ldots, a_0)}{\overline{den}(f)(a_n, \ldots, a_0)}$$

is well-defined if $\overline{g}_i(a_n, \ldots, a_0) = 0$ for $1 \leq i \leq s$ and that $\overline{den}(f)(a_n, \ldots, a_0) \neq 0$.

This leads to considering the projective variety

$$\overline{V} := \{(a_n : \ldots : a_0) \in \mathbf{P}^m(\overline{\mathbf{F}}) \ : \ \overline{g}_i(a_n, \ldots, a_0) = 0, \ 1 \leq i \leq s\}.$$

We talk about points $P := (a_n : \ldots : a_0) \in \mathbf{P}^n(\overline{\mathbf{F}})$, but not quite with coordinates a_j/a_i in that x_j/x_i has $(x_j/x_i)(a_n : \ldots : a_0) = a_j/a_i \in \overline{\mathbf{F}}$ only if $a_i \neq 0$.

Suppose we try to homogenize each variable individually. If $D_{1,i} := deg(num(f), x_i)$, $D_{2,i} := deg(den(f), x_i)$, and $D_i := max\{D_{1,i}, D_{2,i}\}$, then $num^*(f)(x_n, h_n, \ldots, x_1, h_1) := \prod_{i=1}^n h_i^{D_i - D_{1,i}} num(f)(x_n/h_n, \ldots, x_1/h_1)$ and $den^*(f)(x_n, h_n, \ldots, x_1, h_1) := \prod_{i=1}^n h_i^{D_i - D_{2,i}} den(f)(x_n/h_n, \ldots, x_1/h_1)$ are both multi-homogeneous polynomials of multi-degree $(D_n, \ldots, D_1)$, so

$$f^*(x_n, h_n, \ldots, x_1, h_1) = num^*(f)(x_n, h_n \ldots, x_1, h_1)/den^*(f)(x_n, h_n \ldots, x_1, h_1)$$

is a multi-homogeneous rational function of multi-degree $(D_n, \ldots, D_1)$.

For $((a_n : b_n), \ldots, (a_1 : b_1)) \in (\mathbf{P}^1(\overline{\mathbf{F}}))^n$

$$f^*(a_n, b_n, \ldots, a_1, b_1) = num^*(f)(a_n, b_n, \ldots, a_1, b_1)/den^*(f)(a_n, b_n, \ldots, a_1, b_1)$$

is well-defined if $g_i^*(a_n, b_n \ldots, a_1, b_1) = 0$ for $1 \leq i \leq s$ and that $den^*(f)(a_n, b_n \ldots, a_1, b_1) \neq 0$.

This leads to considering the rational variety

$$V^* := \{(a_n, b_n \ldots, a_1, b_1) \in (\mathbf{P}^1(\overline{\mathbf{F}}))^n \ : \ g_i^*(a_n, b_n \ldots, a_1.b_1) = 0\}.$$

We talk about points $P := ((a_n : b_n), \ldots, (a_1 : b_1)) \in (\mathbf{P}^1(\overline{\mathbf{F}}))^n$, with coordinate functions x_j/h_h having $(x_j/h_j)((a_n : b_n) \ldots, (a_1 : b_1)) = a_j/b_j \in \overline{\mathbf{F}} \cup \{\infty\} = \mathbf{P}^1(\overline{\mathbf{F}})$.

10.1 Exceptions

The real problem is not one of affine versus projective versus rational; it is one of making sense of $a/0$. We can certainly decide that $a/0 = \infty$ when $a \neq 0$, but that still leaves the case $0/0$.

In calculus, we resort to the use of L'Hopital's rule to deal with this, whereas we should probably try to write series expansions for numerator, denominator, and or quotient. If we then think in terms of a (formal) Laurent series for $f \in \mathbf{K}$ we could decide on its having value ∞ when there are negative terms and value equal to the constant term otherwise. This gives values in $\mathbf{P}^1(\overline{\mathbf{F}})$ always.

So, instead of viewing points P already in terms of coordinates, let's view an assignment of Laurent series as a field isomorphism P from the function field $\mathbf{K}$ into the Laurent series ring $\overline{\mathbf{F}}((t))$, meaning that $P(f) = 0$ iff $f \in I$. (And let's ask that $tu_P(t) \in P(\mathbf{K})$ for some unit $u_P(t)$.)

Some of these isomorphisms should be considered equivalent. So $P_1 \equiv P_2$ iff $P_2 P_1^{-1} \ : \ P_1(\mathbf{K}) \to P_2(\mathbf{K})$ is defined by multiplication by the unit $u_{P_2}(t) u_{P_1}^{-1}(t)$.

Then points of a function field are equivalence classes of such field isomorphisms, $[P]$. Since the Laurent series $[P](f)$ depends on the representative chosen for $[P]$, it is important to decide what quantities are independent of the choice of representative. The trailing exponent is one such. This is referred to as the valuation $\nu_P(f)$ in the context of discrete valuation rings. The other quantity independent of the choice of representative is

$$f(P) := \begin{cases} P(f)(0) & \nu_P(f) \geq 0 \\ \infty & \nu_P(f) < 0 \end{cases}.$$

This can be reinterpreted as

$$f(P) := \begin{cases} (P(f)(0) : 1) \in \mathbf{P}^1(\overline{\mathbf{F}}) & \nu_P(f) \geq 0 \\ (1 : 0) \in \mathbf{P}^1(\overline{\mathbf{F}}) & \nu_P(f) < 0 \end{cases}.$$

10.2 Homogeneous polynomials

What is the real reason to consider homogeneous polynomials of degree D? It certainly can't be that $f(ax_n, \ldots, ax_0) = a^D f(x_n, \ldots, x_0)$. It isn't even possible to add such polynomials of different degrees. Rather it is to have

$$\frac{f(ax_n, \ldots, ax_0)}{g(ax_n, \ldots, ax_0)} = \frac{f(x_n, \ldots, x_0)}{g(x_n, \ldots, x_0)}$$

for f, g of the same degree and $a \neq 0$; so that the rational, homogeneous function f/g has well-defined values at projective points $(c_n : \cdots : c_0)$.

Think about this in terms of Laurent series. Every multi-homogeneous rational function f takes on some value $f(P)$ in $\mathbf{P}^1(\overline{\mathbf{F}})$ at a given point $[P]$. And this is independent of any topological or geometric considerations; it is dependent only on the formal Laurent series expansions of f.

10.3 Homgenization

Do we always get projective varieties by starting with affine varieties and homogenizing the defining polynomials?

As an example start with $x_2^2 + x_1^2 + 1$ defining the affine variety

$$V := \{(a_2, a_1) \in \overline{\mathbf{F}}^2 \ : \ a_2^2 + a_1^2 + 1 = 0\}.$$

Homogenization is usually done formally, here as

$$x_0^2 \left(\left(\frac{x_2}{x_0} \right)^2 + \left(\frac{x_1}{x_0} \right)^2 + 1 \right) = x_2^2 + x_1^2 + x_0^2.$$

Let this define a projective variety

$$\overline{V} := \{(a_2 : a_1 : a_0) \in \mathbf{P}^2(\overline{\mathbf{F}}) \ : \ a_2^2 + a_1^2 + a_0^2 = 0\}.$$

This already involves some slight cheating in that whle it is possible to evaluate homogeneous rational functions such as $\left(\frac{x_2}{x_0} \right)^2 + \left(\frac{x_1}{x_0} \right)^2 + 1$ at a projective point $(a_2 : a_1 : a_0)$ when $a_0 \neq 0$, it is not possible to evaluate the homogeneous polynomial $x_2^2 + x_1^2 + x_0^2$ at any projective point. It is possible to think of it as the numerator of some homogeneous rational function; in which case, it is possible to decide that the value of the said homogeneous rational function should be zero, when this numerator is zero but the denominator is not. So asking for $a_2^2 + a_1^2 + a_0^2 = 0$ plays triple duty, in that the denominator could be chosen not only as above x_0^2, but also as x_1^2 or x_2^2.

The Jacobian criterion in the affine case is that $2x_2 = 2x_1 = 0$. But the affine point $(0, 0)$ is not a point of the variety; so the affine variety is non-singular.

The Jacobian criterion in the projective case is that $2x_2 = 2x_1 = 2x_0 = 0$. But $(0 : 0 : 0)$ is not a projective point; so the projective variety is non-singular? Well almost. For the Jacobian criterion to apply, the formal partial derivatives need to be defined. If we cheat and use homogeneous polynomials, they are; but if we use homogeneous rational functions, they are not when the denominator vanishes. So there could conceivably be singularities here when $a_0 = 0$; and there are two such projective points $(\pm i : 1 : 0)$ with $a_0 = 0$.

Now try a slightly harder problem, starting with the polynomial $x_3^2 + x_2^2 + x_1^2$, again irreducible for characteristic not 2. This defines an affine variety

$$V := \{(a_3, a_2, a_1) \in \overline{\mathbf{F}}^3 \ : \ a_3^2 + a_2^2 + a_1^2 = 0\}.$$

Homogenization gives

$$x_0^2 \left(\left(\frac{x_3}{x_0} \right)^2 + \left(\frac{x_2}{x_0} \right)^2 + \left(\frac{x_1}{x_0} \right)^2 \right) = x_3^2 + x_2^2 + x_1^2,$$

independent of x_0 Let this define a projective variety

$$\overline{V} := \{(a_3 : a_2 : a_1 : a_0) \in \mathbf{P}^3(\overline{\mathbf{F}}) \ : \ a_3^2 + a_2^2 + a_1^2 = 0\}.$$

This has a singularity at $(0 : 0 : 0 : 1)$, but probably has singularities at lots of points $(a_3 : a_2 : a_1 : 0)$ as well.

A fix for this is to homogenize variables individually rather than to homogenize polynomials and/or rational functions. This fix clears up lots of other similar problems as well, as documented in previous chapters, by letting homogeneous rational functions take on values in $\mathbf{P}^1(\overline{\mathbf{F}})$ insted of just $\overline{\mathbf{F}}$.

Clearing denominators gives

$$h_1^2h_2^2h_3^2\left(\left(\frac{x_3}{h_3}\right)^2+\left(\frac{x_2}{h_2}\right)^2+\left(\frac{x_1}{h_1}\right)^2\right)=x_3^2h_2^2h_1^2+h_3^2x_2^2h_1^2+h_3^2h_2^2x_1^2,$$

not independent of h_3, h_2, h_1 Let this define a variety

$$\overline{V}:=\{((a_3:b_3),(a_2:b_2),(a_1:b_1))\in(\mathbf{P}^1(\overline{\mathbf{F}}))^3\ :\ a_3^2b_2^2b_1^2+b_3^2a_2^2b_1^2+b_3^2b_2^2a_1^2=0\}.$$

This has a singularity at $((0:1),(0:1),(0:1))$, but also at $((1:0),(1:0),(a_1:b_1))$, $((1:0),(a_2:b_2),(1:0))$, as well as at $((a_3:b_3),(1:0),(1:0))$.

Chapter 11

Integrality

11.1 Meta-definition

An element y is said to be integral if it is the root of a monic polynomial

$$f(T) := 1T^d + a_1T^{d-1} + \cdots + a_{d-1}T^1 + a_dT^0,$$

for some positive integer d. But there are various possibilities for where the coefficients a_j could live and even where y should live that give decidedly different flavors to the theory involved. And certainly asking for conditions on $f(T)$ such as irreducibility could make a difference as well. Indeed, there is a difference in using the same polynomial $f(T) := T^2 + 1$ to define an integral extension

$$A := \mathbf{F}[y]/\langle f(y)\rangle$$

over a field $\mathbf{F}$ over which $f(T)$ is irreducible as opposed to a field where it is not, in that the latter will have zero divisors while the former will be a field extension.

$A \supset B$ is said to be integrally closed over B iff every $y \in A$ is integral over B. There is always low-hanging fruit to define and/or prove, such as transitivity of integral closure, and structure induced on A by B; all important as groundwork before the actual investigation of the subject can get started.

11.2 Integral closures of rings

Definition 47. *Let B be a quotient ring. An element y is integral over B iff if it is the root of a monic polynomial*

$$f(T) := 1T^d + a_1T^{d-1} + \cdots + a_{d-1}T^1 + a_dT^0,$$

for some positive integer d, with $a_j \in B$ for $1 \leq j \leq d$. The quotient ring $A := B[y]/\langle f(y)\rangle$ is called an integral extension of B.

$$Q(A) := \{g/h \ : \ g, h \in A\}$$

is called the field of fractions of A. The integral closure (of B in $Q(A)$) is the set of all elements of $Q(A)$ integral over B.

The Klein example (13.1) had several related extensions. For $B := \mathbf{F}[x]$, the integral extension $A := B[y]/\langle y^3 + x^3y + x\rangle$ is supposedly integrally closed in $Q(A)$; whereas for $B := \mathbf{F}[y]$, the extension $A := B[x]/\langle yx^3 + y + x^3\rangle$ is not even integral, yet there are elements such as $z := yx$ in A integral over B. Indeed, the integral closure of B is $C := B[w, z]/\langle w^2 + w + zy^3, wz + z + y^4, z^2 - wy\rangle$ with $w := yx^2$, This second A could have been written as an integral extension $A := B[z]/\langle z^3+zy+y^5\rangle$, in which case $w := z^2/y \in Q(A)\backslash A$; but the integral closure would have been the same.

What structure should be expected of an integral extension and/or its integral closure? The advantage of an integral extension over a non-integral extension is that there is an implicit B-module basis for a B-algebra, namely the d independent powers of the integral element. The monic polynomial induces the multiplication rules. It is not a strict B-algebra as written when $d > 2$, but can be made so by using all the module basis elements and all the induced multiplication rules. That is,

$$\mathbf{F}[z_2, z_1; y]/\langle z_2^2 + z_2y + z_1y^5,\ z_2z_1 + z_1y + y^5,\ z_1^2 - z_2\rangle$$

is a strict B-algebra. The point of this type of presentation is clearly to highlight the (non-trivial) reduction rules corresponding to multiplication:

$$z_2 \cdot z_2 \mapsto -1z_2 - y^3z_1,\ z_2 \cdot z_1 \mapsto -z_1 - y^4z_0,\ z_1 \cdot z_1 \mapsto z_2,$$

with standard monomials z_iy^j for $0 \leq i \leq 2$ and $0 \leq j$. And the integral closure has a similar structure.

```
LIB "normal.lib";
ring r=2,(z,y),lp;
ideal i=z3+zy+y5;
list nor=normal(i);nor;
def R=nor[1][1];
setring R;
option(redSB);
ideal s=std(norid);s;

//s[1]=z^3+z*y+y^5
//s[2]=T(1)*y+z^2
//s[3]=T(1)*z+z+y^4
//s[4]=T(1)^2+T(1)+z*y^3
```

This is a strict affine r/i-algebra presentation. The problem with this is that $T(1)$ is a name for the fraction z^2/y. Should there then be a reduction rule $z^2/y \mapsto T(1)$ or a reduction rule $T(1) \mapsto z^2/y$? Since neither of these are polynomial, change these to polynomial reduction rules $z^2 \mapsto T(1)y$ and $T(1)y \mapsto z^2$.

Try the slightly harder example:

```
 LIB ‘‘normal.lib’’;
 ring r=2,(y,x),dp;
 ideal i=y7+y3x+x11;
 list nor=normal(i);nor;
//   characteristic : 2
//   number of vars : 6
//        block   1 : ordering dp
//                  : names    T(1) T(2) T(3) T(4)
//        block   2 : ordering dp
//                  : names    y x
//        block   3 : ordering C
//      _[1]=yx5
//      _[2]=y6
//      _[3]=x10
//      _[4]=x8
//      _[5]=y2x
 def R=nor[1][1];
 setring R;
 option(redSB);
 ideal s=std(norid);s;
//s[1]=x^11+y^7+y^3*x
//s[2]=T(4)*y^2+x^7
//s[3]=T(4)*x^4+y^5+y*x
//s[4]=T(3)+T(4)*x^2
//s[5]=T(2)*x+y^4
//s[6]=T(2)*y+T(4)*x^3+y
//s[7]=T(1)*y+x^4
//s[8]=T(1)*x^3+T(4)*y
//s[9]=T(4)^2+T(1)+y^3*x^3
//s[10]=T(2)*T(4)+y^2*x^6
//s[11]=T(1)*T(4)+y^4+x
//s[12]=T(2)^2+T(2)+y*x^9
//s[13]=T(1)*T(2)+y^3*x^3
//s[14]=T(1)^2+T(4)*x


 R=ZZ/2[y,x];
 I=ideal(y^7+y^3*x+x^11);
 A=R/I;
 icf=icFractions A;
 toString icf

 {(y^5+y*x)/(x^4), (y^4)/(x), y, x}

 g=gens gb ideal integralClosure A;
 toString g

     matrix {{x^11+y^7+y^3*x,
              w_(2,0)*x+y^4,
```

```
  w_(2,0)*y^3+x^10+y^3,
  w_(2,0)^2+w_(2,0)+y*x^9,
  w_(6,0)*y^2+x^7,
  w_(6,0)*x^3+w_(2,0)*y+y,
  w_(6,0)*w_(2,0)+y^2*x^6,
  w_(6,0)^2*y+y^4*x^3+x^4,
  w_(6,0)^3+y*x^10+y^4+x
}}
```

Maybe it is clear that the elements $T(4) = w_{6,0}$ and that $T(2) = w_{2,0}$. An $\mathbf{F}[x]$-module basis should be $(1, y, y^2, y^3, T(1), T(2), T(4))$, whereas $\mathbf{F}[y, x]/\langle y^7 + y^3x + x^{11}\rangle$-module basis should be $(1, T(1), T(2), T(4))$.

Clearly the `normal` function has a bug that allows extra generators (and hence extra relations) to creep into the strict affine algebra presentation desired. But the `integralClosure` function doesn't even try for any type of algebra presentation, settling for any quotient ring presentation.

Regardless, the choice of prepending the new elements to the old ring means that the reduction rules are invariably backwards in that multiples of new elements are reduced to old elements, rather than the other way around.

This is an example in one-point form, so there should be weights (pole orders) for each basis element, and a weighted presentation:

```
loadPackage "QthPower";
wtr=matrix{{11,7}};
R=ZZ/2[y,x,Weights=>entries weightGrevlex(wtr)];
GB={y^7+y^3*x+x^11};
ic=qthIntegralClosure(wtr,R,GB);
toString ic

    ({x^7,
      y*x^7,
      y^6+y^2*x,
      y^2*x^7,
      y^5*x^3+y*x^4,
      y^3*x^7,
      y^4*x^6
    },{
      p_0^2+p_0+p_5*p_6^9,
      p_0*p_1+p_1+p_6^10,
      p_0*p_2+p_3*p_6^6,
      p_0*p_3+p_3+p_4*p_6^6,
      p_0*p_4+p_1*p_6^3,
      p_0*p_5+p_2*p_6^3+p_5,
      p_1^2+p_3*p_6+p_4*p_6^7,
      p_1*p_2+p_5*p_6^7,
      p_1*p_3+p_2*p_6^4+p_5*p_6,
      p_1*p_4+p_3*p_6^4,
      p_1*p_5+p_0*p_6,
      p_2^2+p_1*p_6^3+p_4,
      p_2*p_3+p_6^7,
      p_2*p_4+p_0*p_6+p_6,
```

```
       p_2*p_5+p_4*p_6^3,
       p_3^2+p_0*p_6,
       p_3*p_4+p_5*p_6^4,
       p_3*p_5+p_1,
       p_4^2+p_2*p_6,
       p_4*p_5+p_6^4,
       p_5^2+p_3
      },
 (ZZ/2)[p_0, p_1, p_2, p_3, p_4, p_5, p_6],
matrix {{37,  33,  27,  22,  17,  11,   7}}
      )
```

This is then a strict $\mathbf{F}_2[f_7]$-algebra with module basis $(f_0 := 1, f_{11}, f_{17}, f_{22}, f_{27}, f_{33}, f_{37})$, and multiplication rules corresponding to the ideal generators above.

11.3 Non-integral extensions

What happens with non-integral extensions? It is possible to ask for elements integral over

$$\overline{\mathbf{F}}[x_2, x_1]/\langle x_2^3 + x_2x_1 + x_1^5 + x_2x_1\pi(x_2, x_1)\rangle$$

for any polynomial $\pi(x_2, x_1)$ with constant term 0. Both x_2^2/x_1 and x_1^4/x_2 should be in the intergal closure; but this is independent of the choice of the polynomial $\pi(x_2, x_1)$.

Try the example

$$A := \overline{\mathbf{F}}_2[x_2, x_1]/\langle x_2^3x_1^9 + x_2^2 + x_2x_1 + x_1^3\rangle,$$

as opposed to

$$A := \overline{\mathbf{F}}_2[x_2, x_1]/\langle x_2^2 + x_2x_1 + x_1^3\rangle.$$

Both have $x_3 := x_2/x_1$ in their integral closure, but in the latter it is possible to get away without x_2, just having

$$\overline{A} := \overline{\mathbf{F}}_2[x_3, x_1]/\langle x_3^2 + x_3 + x_1\rangle.$$

In the former,

$$\overline{A} := \overline{\mathbf{F}}_2[x_3, x_2, x_1]/\langle x_2 - x_3x_1, x_3^3x_1^{10} + x_3^2 + x_3 + x_1\rangle,$$

is probably what should be written, but

$$\overline{A} := \overline{\mathbf{F}}_2[x_3, x_2, x_1]/\langle x_2^3x_1^9 + x_2^2 + x_2x_1 + x_1^3,\ x_3x_1 - x_2,\ x_3^2 + x_3 + (x_2^3x_1^7 + x_1)\rangle,$$

is what shows that x_3 is integral over A.

What is really true in terms of integral extensions is gotten from using $x_4 := x_2x_1^9$ to get the integral extension

$$\overline{\mathbf{F}}_2[x_4, x_1]/\langle x_4^3 + x_4^2 + x_4x_1^{10} + x_1^{21}\rangle$$

with $x_5 := (x_4^2 + x_4)/x_1^{10} = x_2^2x_1^8 + (x_2/x_1)$ integral in that $x_5^2 + x_5 + (x_4 + 1)x_1 = 0$.

Maybe what we should really consider is $C(P, Q(A))$ for various choices of P. Let

$$A := \overline{\mathbf{F}}[x_2, x_1]/\langle x_2^3x_1^4 + x_2^2 + x_2x_1 + x_1^3\rangle.$$

Then consider $P_1 := \overline{\mathbf{F}}[x_1]$, $P_2 := \overline{\mathbf{F}}[x_2]$, and $P_3 := A$.

$C(P_1, Q(A))$ has basis $(1, r_1 := x_2x_1^4, r_2 := x_2^2x_1^3 + x_2/x_1)$ and induced relations

$$r_1^2 + r_1 - r_2x_1^5,\ r_2r_1 + r_1 + x_1^4,\ r_2^2 + r_2 + (r_1 + 1)x_1;$$

$C(P_2, Q(A))$ has basis $(1, s_1 := x_2^3x_1, r_2 := x_2^3x_1^2 + x_1, x_2^2x_1^3 + x_1^2/x_2)$ and induced relations

$$s_1^2 - s_2x_2^3 + s_1,\ s_2s_1 - s_3x_2^4,\ s_2^2 + s_1x_2 + x_2^5,\ s_3s_1 + s_1 + x_2^4,\ s_3s_2 + s_2 + s_1x_2,\ s_3^2 + s_3 + s_2;$$

$C(A, Q(A))$ has basis $(1, t_1 := x_2/x_1)$ and induced relations

$$t_1^3x_1^5 + t_1^2 + t_1 + x,$$

not

$$x_2^3x_1^4 + x_2^2 + x_2x_1 + x_1^3, t_1x_1 - x_2,\ t_1x_2 + x_2^3x_1^3 + x_2 + x_1^2,\ t_1^2 + t_1 + x_2^3x_1^2 + x_1.$$

Chapter 12

Algebraic curves

12.1 Computation-driven theory

I spend my time doing computations using various Computer Algebra Systems, namely MAGMA, MACAULAY2 and SINGULAR in order to try to understand algebraic curves (and some algebraic surfaces of higher dimension as well). These computations are carried out relative to an appropriate algebraic extension of $\mathbf{F}_p$ in positive characteristic p or an appropriate algebraic extension of $\mathbf{Q}$ in characteristic 0, while the theory may apply to more general algebraically closed fields.

There are three basic flavors of computation that I do.

- There are Gröbner basis (14) computations (done relative to whatever monomial ordering (4) emphasizes the appropriate ideas, not a default lex (9) or grevlex (10) ordering).
- There are formal Laurent series expansions (37) $\sum_{j=\nu(g)}^{\infty} g_{j,P} t^j$ of rational functions $g \in \mathbf{K}$ (48), for some function field $\mathbf{K}$ (48) and some point P (49).
- There are integral closures (47) of integral domains in one-point form (??), wherein all $g \in \mathbf{K}$ have values $g(P) \in \overline{\mathbf{F}}$ at all points P except at a special point P_∞ at which those functions have all of their poles.

From this viewpoint (arrived at after working countless examples over a sufficiently long period of time) I have chosen a non-standard view of algebraic curves. In particular consider the following.

- Nothing I do requires any Geometry, Topology, or Analysis; it is all algebra (as should have been implicit in the acronym CAS as opposed to, say, CAGTAS).
- The main object being studied is a function field $\mathbf{K}$.
- The secondary objects studied are formal Laurent series expansions, (akin to using Taylor series to understand the behavior of some function at some point).
- The algebraic curve $\mathbf{X} = \mathbf{X}(\mathbf{K})$ is defined from the function field $\mathbf{K}$, not the other way around.
- Rational functions (elements of the function field $\mathbf{K}$) naturally take on values in $\overline{\mathbf{F}} \cup \{\infty\}$; so using them to coordinatize an algebraic curve should mean that points can be described by elements of $(\overline{\mathbf{F}} \cup \{\infty\})^m$, rather than as elements of affine m-space $\overline{\mathbf{F}}^m$, and definitely not as elements of projective m-space $\mathcal{P}^m(\overline{\mathbf{F}})$. The fact that $(\mathcal{P}^1(\overline{\mathbf{F}}))^m$ doesn't have a name, while these other two do should be a clue that this is not the standard way to view things.
- Affine algebraic curves are restrictions of algebraic curves to certain rational functions and the points at which those rational functions take on affine values.
- Projective algebraic curves (or any curves with hybrid projective and affine coordinates as might be produced by blowups) should be irrelevant.
- An affine curve that is non-singular (??) and in one-point position (??) should provide more information than a traditional non-singular model or any covering of the curve by affine patches. In particular, I use the former to produce a nice basis for the ring $\mathbf{L}(\infty P_\infty)$ of all rational functions with no poles except possibly at P_∞ to get bases for any Riemann-Roch space (??) $\mathbf{L}(mP_\infty)$. In addition, the algebraic genus (??) of the algebraic curve is a nice byproduct of this.

12.2 Theory

Consider the following function field approach to a purely algebraic view of algebraic curves. [There are notes after the definitions, since there are some subtle differences (and some not so subtle differences) between the usage here versus elsewhere.]

Definition 48. *Start with an algebraically closed field* $\overline{\mathbf{F}}$ *(here restricted to* $\overline{\mathbf{Q}}$ *or* $\overline{\mathbf{F}}_p$ *for computational purposes). Let* $R := \overline{\mathbf{F}}[x_2/h_2, x_1/h_1]$ *be a multivariate polynomial ring in two free (rational) variables. Let* $f(x_2/h_2, x_1/h_1) \in R$ *be an irreducible polynomial.* $I := \langle f(x_2/h_2, x_1/h_1) \rangle$ *a principal ideal of* R*, and* $A := R/I$ *the corresponding quotient ring of dimension* 1*, an integral domain since* f *is irreducible. Then let* $Q(A) = \overline{\mathbf{F}}(x_2/h_2, x_1/h_1)/I$ *be the field of fractions of* A*. That field* $\mathbf{K} := Q(A)$ *is a function field of dimension* 1*, (the fundamental object used here to define an algebraic curve, not the other way around). Elements of* $\mathbf{K}$ *will be called rational functions (or just functions), which are already necessarily homogenized relative to every variable.*

Note on function fields and rational functions Most of what I know about function fields is probably a result of having read Stichtenoth's book a few decades ago. There, function fields of this type are viewed as integral extensions of $\overline{\mathbf{F}}(x_1)$, which suggests that x_1 is an independent variable and others such as x_2 are dependent on it. We may not care ultimately about either x_1 or x_2, so will reserve judgment as to what should or shouldn't be viewed as the independent variable.

Rational functions as described here are variants of regular functions, absent the topological baggage, and with individual homogenization rather than overall homogenization. [They are already homogeneous in every variable (explicitly or implicitly), so there is no sense in saying the total degree of the numerator and denominator must be the same.]

Definition 49. *Let* $\overline{\mathbf{F}}((t))$ *be the formal Laurent series ring (37) over* $\overline{\mathbf{F}}$ *in the variable* t*. Consider ring homomorphisms* $\pi_i : \overline{\mathbf{F}}(x_2/h_2, x_1/h_1) \to \mathbf{F}((t))$ *with* $kernel(\pi_i) = I$ *and* $tu_i(t) \in image(\pi_i)$ *for some unit* $u_i(t)$*, lifted to field isomorphisms* $P_i : K \to P_i(\mathbf{K}) \subset \overline{\mathbf{F}}((t))$*. Define* $P_i \sim P_j$ *iff* $\nu_{P_i}(f) = \nu_{P_j}(f)$ *for all* $f \in \mathbf{K}$ *(with* ν_P *the valuation defined immediately below as the trailing exponent of the Laurent series at* P *). This defines an equivalence relation. Then the equivalence class of isomorphisms* $[P_i]$ *is a point of* $\mathbf{K}$*, with the algebraic curve* $\mathbf{X} = \mathbf{X}(\mathbf{K})$*, being the set of all such points.*

Note on points and curves

This is not the standard way to view points of an algebraic curve; as it is standard to define an algebraic variety first, then talk about such things as the function field. The standard way presupposes that the algebraic curve should be either projective or affine, without considering what is natural relative to the function field. Here there is no such bias, which leads to a completely different choice of what points really are. Elsewhere it is barely admitted that $t^{\nu_P} u(t)$ is a Laurent series, formal or otherwise; and definitely not that it is related to a value of a function at a point, with that value allowed to be ∞.

Definition 50. *Any $t_P \in \mathbf{K}$ with $P(t_P) := tu_P(t)$, (that is, with valuation 1), which depends on the particular representative of $[P]$, is called a local parameter. Every element $g \in \mathbf{K}$ then has image $\sum_{j=\nu_P(g)}^{\infty} g_{j,P} t^j$, with the trailing exponent $\nu_P(g)$, the valuation of g at $[P]$, being independent of the particular choice of local parameter t_P or even representative $P \in [P]$. While the particular expansion of g may depend on the choice of local parameter, what is also independent of it is the coordinate*

$$g(P) := \begin{cases} 0, & \nu_P(g) > 0 \\ g_0 := g_{0,P}, & \nu_P(g) = 0 \\ \infty, & \nu_P(g) < 0 \end{cases}.$$

Rewrite this as

$$g(P) := \begin{cases} (g_0 : 1), & \nu_P(g) \geq 0 \\ (1 : 0), & \nu_P(g) < 0 \end{cases} \in \mathcal{P}^1(\mathbf{F}).$$

Note on discrete valuation rings and coordinates

The standard approach is instead to consider discrete valuation rings. The relation to these is in terms of the trailing exponent corresponding to the valuation; so we shall use the notation $\nu_P(g)$ for this trailing exponent to emphasize this correspondence. The difference is that valuations are used to highlight maximal orders $\{g \ : \ \nu_P(g) \geq 0\}$, maximal ideals $\{g \ : \ \nu_P(g) > 0\}$, and units $\{g \ : \ \nu_P(g) = 0\}$. This would seem to highlight the affine viewpoint rather than what we wish to highlight. That is, it tends to focus on the quotient ring $A := \overline{\mathbf{F}}[x_2, x_1]/I$ (the maximal order) rather than its field of fractions $Q(A)$ viewed as the function field $\mathbf{K} = \overline{\mathbf{F}}(x_2, x_1)/I$.

It is probably worthwhile as an exercise to try to write a definition for a discrete valuation ring by figuring out how trailing exponents of formal Laurent series work, before resorting to looking up a standard definition.

Coordinates are usually either affine, gotten from finding the common zeros of the functions defining the affine curve; or they are projective, gotten by finding common zeros of homogenized functions defining the projective curve. They can even be a mixture of affine and projective, gotten from blowing up affine points in the standard way (assuming this is really a well-defined recursive method).

We shall make the case that focusing on an affine part of a curve can, for better or worse, hide various things about the curve at the non-affine points, (13.1) that there are problems coordinatizing curves there, and that desingularization of an affine curve may be a misleading concept, in that it ignores singularities that are not at affine points.

Chapter 13

Examples

13.1 Klein quartic example

Before we get too far theoretically, let's consider an example. The Klein quartic, defined by the symmetrically pleasing homogeneous equation

$$X^3Y + Y^3Z + Z^3X = 0,$$

as it can be found in (http://en.wikipedia.org/wiki/Klein_quartic) is meant to be a projective curve rather than an affine 2-dimensional surface. So maybe it is supposed to be the projective variety (30)

$$V := \{(X : Y : Z) \in \mathcal{P}^2(\mathbf{C}) \ : \ X^3Y + Y^3Z + Z^3X = 0\}.$$

But as soon as we start talking about regular functions as quotients of homogeneous polynomials (of the same degree) in $\mathbf{C}[X, Y, Z]$, we are probably admitting to viewing the defining equation above as a polynomial version of

$$\left(\frac{X}{Z}\right)^3 \left(\frac{Y}{Z}\right) + \left(\frac{Y}{Z}\right)^3 + \left(\frac{X}{Z}\right) = 0.$$

If we further try to write down divisors (bookkeeping devices for poles and zeros at different points or relative to different discrete valuation rings)

$$((X/Z)) = (-2) \cdot P_1 + (-1) \cdot P_2 + (3) \cdot P_3;$$

$$((Y/Z)) = (-3) \cdot P_1 + (2) \cdot P_2 + (1) \cdot P_3;$$

then maybe we are suggesting that at P_1, $(X : Z) = (1 : 0)$, $(Y : Z) = (1 : 0)$, and even $(X : Y) = (0 : 1)$. Projectively this is written as $(X : Y : Z) = (0 : 1 : 0)$, which really only describes two out of three of these ratios. Similarly at P_2, $(X : Z) = (1 : 0)$, $(Y : Z) = (0 : 1)$, and $(X : Y) = (1 : 0)$, with $(X : Y : Z) = (1 : 0 : 0)$ again only describing two of these. And at P_3, $(X : Z) = (0 : 1)$, $(Y : Z) = (0 : 1)$, and $(X : Y) = (1 : 0)$, with $(X : Y : Z) = (0 : 0 : 1)$ again only describing two of these.

These three points are at least coordinatized by their $(X : Y : Z)$ coordinates. Does this make sense in general? Consider an affine version such as

$$X^3Y + Y^3 + X = 0,$$

gotten by setting $Z = 1$. The affine algebraic curve

$$V := \{(X, Y) \in \mathbf{C}^2 \ : \ X^3Y + Y^3 + X = 0\}$$

misses the points at which $Z = 0$, but at least the values (X, Y) can be viewed as pairs of individual values X and Y that happen to satisfy the defining equation. If the projective algebraic curve were treated this same way, namely as giving values to separate functions X, Y, and Z; then it would really be treated more like an affine algebraic surface of dimension 2 with affine points other than the origin grouped together projectively rather than as a way of evaluating individual homogeneous rational functions such as X/Z and Y/Z.

(An alternative might be to consider the projective curve as shorthand for a colllection of affine curves each gotten by setting one projective coordinate equal to 1.)

This already might suggest (though it took me a long time to see it) that a more appropriate generalization of an affine algebraic curve is gotten by homogenizing each of its variables (implicitly or explicitly) so that each can individually be viewed as a rational function with its own separate value.

So

$$\left(\frac{X_1}{H_1}\right)^3 \left(\frac{X_2}{H_2}\right) + \left(\frac{X_2}{H_2}\right)^3 + \left(\frac{X_1}{H_1}\right) = 0.$$

has algebraic variety

$$V := \{((X_1 : H_1), (X_2 : H_2)) \in (\mathcal{P}^1(\mathbf{C}))^2 \ : \ X_1^3 X_2 H_2^2 + H_1^3 X_2^3 + X_1 H_1^2 H_2^3 = 0\}$$

with its elements at least giving separate information about the rational functions X_1/H_1 and X_2/H_2.

The quotient ring

$$A := \mathbf{C}\left[\frac{X_1}{H_1}, \frac{X_2}{H_2}\right] / \left\langle \left(\frac{X_1}{H_1}\right)^3 \left(\frac{X_2}{H_2}\right) + \left(\frac{X_2}{H_2}\right)^3 + \left(\frac{X_1}{H_1}\right) \right\rangle$$

has a field of fractions $Q(A)$, a function field. There is reason to believe that this function field $\mathbf{K} := Q(A)$ is the primary object to be studied, not the algebraic curve.

Let's consider first that K can be defined by just about any two of its elements together with the induced irreducible polynomial relation they satisfy (in the same sense that a finite field can be defined by almost any one of its elements and the induced irreducible relation it satisfies (6.1)).

So take

$$\frac{X_3}{H_3} := \left(\frac{X_1}{H_1}\right)\left(\frac{X_2}{H_2}\right).$$

Then

$$\mathbf{K} = \mathbf{C}\left(\frac{X_3}{H_3}, \frac{X_2}{H_2}\right) / \left\langle \left(\frac{X_3}{H_3}\right)^3 + \left(\frac{X_3}{H_3}\right)\left(\frac{X_2}{H_2}\right) + \left(\frac{X_2}{H_2}\right)^5 \right\rangle,$$

even though the quotient ring

$$B := \mathbf{C}\left[\frac{X_3}{H_3}, \frac{X_2}{H_2}\right] / \left\langle \left(\frac{X_3}{H_3}\right)^3 + \left(\frac{X_3}{H_3}\right)\left(\frac{X_2}{H_2}\right) + \left(\frac{X_2}{H_2}\right)^5 \right\rangle$$

is not the same as the original quotient ring A.

There is also a problem with birational maps, in the sense that they are attempts to map between quotient rings such as A and B above. Since the affine variety associated with A misses both P_1 and P_2, whereas the affine variety associated with B misses only P_1, but give the same coordinates to both P_2 and P_3, there might be problems identifying these two quotient rings unless at least P_1 and P_2 are avoided. Yet there is a clear identification (the identity map!) at the level of the function field $\mathbf{K}$ that can be used as an alternative.

Note that A is considered as normal (meaning affine non-singular) because any singularity is not at an affine point, whereas B happens to have a double point because P_2 and P_3 both have the same coordinates.

Even the term double point should send up a red flag in the sense that this suggests that points are different objects from elements of the variety, or that points are not uniquely determined by the coordinate system being used. There is actually another function $X_4/H_4 := (X_3/H_3)(X_1/H_1)$ with

$$((X_2/H_2)) = (-3) \cdot P_1 + (2) \cdot P_2 + (1) \cdot P_3;$$

$$((X_3/H_3)) = (-5) \cdot P_1 + (1) \cdot P_2 + (4) \cdot P_3.$$

$$((X_4/H_4)) = (-7) \cdot P_1 + (7) \cdot P_3.$$

that desingularizes the algebraic curve at the double point. That is, X_4/H_4 takes on different values $(1:1)$ at P_2 and $(0:1)$ at P_3. So a description using all three rational functions as coordinate functions would get us back to an affine non-singular model (with a singularity, a cusp, hidden at the non-affine point P_1).

Consider a bunch of versions of this particular function field $\mathbf{K}$, some affine, some projective, some rational, grouped in threes, one each.

$$f_1(x_2,x_1) := x_2^3 + x_2x_1^3 + x_1 \in R_1 := \overline{\mathbf{F}}[x_2,x_1],$$
$$I_1 := \langle f_1\rangle \subset R_1,\ A_1 := R_1/I_1,\ Q(A_1) := \overline{\mathbf{F}}(x_2,x_1)/I_1$$
$$V(I_1) := \{(a_2,a_1) \in \overline{\mathbf{F}}^2\ :\ f_1(a_2,a_1) = 0\}$$

$$f_2(x_2,x_1,x_0) := x_2x_1^3 + x_2^3x_0 + x_1x_0^3 \in R_2 := \overline{\mathbf{F}}[x_2,x_1,x_0],$$
$$I_2 := \langle f_2\rangle \subset R_2,\ A_2 := R_2/I_2,\ Q(A_2) := \overline{\mathbf{F}}(x_2,x_1,x_0)/I_2$$
$$V(I_2) := \{(a_2 : a_1 : a_0) \in \mathcal{P}^2(\overline{\mathbf{F}})\ :\ f_2(a_2,a_1,a_0) = 0\}$$

$$f_3(x_2/h_2,x_1/h_1) := (x_2/h_2)^3 + (x_2/h_2)(x_1/h_1)^3 + (x_1/h_1) \in R_3 := \overline{\mathbf{F}}[x_2/h_2,x_1/h_1],$$
$$I_3 := \langle f_3\rangle \subset R_3,\ A_3 := R_3/I_3,\ Q(A_3) := \overline{\mathbf{F}}(x_2/h_2,x_1/h_1)/I_3$$
$$V(I_3) := \{((a_2 : b_2),(a_1 : b_1)) \in \mathcal{P}^1(\overline{\mathbf{F}})\ :\ f_3(a_2/b_2,a_1/b_1) = 0\}$$

$$f_4(y_2,y_1) := y_1^5 + y_2^3 + y_2y_1 \in R_4 := \overline{\mathbf{F}}[y_2,y_1],$$
$$I_4 := \langle f_4\rangle \subset R_4,\ A_4 := R_4/I_4,\ Q(A_4) := \overline{\mathbf{F}}(y_2,y_1)/I_4$$
$$V(I_4) := \{(a_2,a_1) \in \overline{\mathbf{F}}^2\ :\ f_4(a_2,a_1) = 0\}$$

$$f_5(y_2,y_1,y_0) := y_1^5 + y_2^3y_0^2 + y_2y_1y_0^3 \in R_5 := \overline{\mathbf{F}}[y_2,y_1,y_0],$$
$$I_5 := \langle f_5\rangle \subset R_5,\ A_5 := R_5/I_5,\ Q(A_5) := \overline{\mathbf{F}}(y_2,y_1,y_0)/I_5$$
$$V(I_5) := \{(a_2 : a_1 : a_0) \in \mathcal{P}^2(\overline{\mathbf{F}})\ :\ f_5(a_2,a_1,a_0) = 0\}$$

$$f_6(y_2/h_2,y_1/h_1) := (y_1/h_1)^5 + (y_2/h_2)^3 + (y_2/h_2)(y_1/h_1) \in R_6 := \overline{\mathbf{F}}[y_2/h_2,y_1/h_1],$$
$$I_6 := \langle f_6\rangle \subset R_6,\ A_6 := R_6/I_6,\ Q(A_6) := \overline{\mathbf{F}}(y_2/h_2,y_1/h_1)/I_6$$
$$V(I_6) := \{((a_2 : b_2),(a_1 : b_1)) \in \mathcal{P}^1(\overline{\mathbf{F}})\ :\ f_6(a_2/b_2,a_1/b_1) = 0\}$$

$$f_7(z_2,z_1) := z_1^7 + z_2^5 + z_2^4 \in R_7 := \overline{\mathbf{F}}[z_2,z_1],$$
$$I_7 := \langle f_7 \rangle \subset R_7,\ A_7 := R_7/I_7,\ Q(A_7) := \overline{\mathbf{F}}(z_2,z_1)/I_7$$
$$V(I_7) := \{(a_2,a_1) \in \overline{\mathbf{F}}^2 \ :\ f_7(a_2,a_1) = 0\}$$

$$f_8(z_2,z_1,z_0) := z_1^7 + z_2^5 z_0^2 + z_2^4 z_0^3 \in R_8 := \overline{\mathbf{F}}[z_2,z_1,z_0],$$
$$I_8 := \langle f_8 \rangle \subset R_8,\ A_8 := R_8/I_8,\ Q(A_8) := \overline{\mathbf{F}}(z_2,z_1,z_0)/I_8$$
$$V(I_8) := \{(a_2 : a_1 : a_0) \in \mathcal{P}^2(\overline{\mathbf{F}}) \ :\ f_8(a_2,a_1,a_0) = 0\}$$

$$f_9(z_2/h_2,z_1/h_1) := (z_1/h_1)^7 + (z_2/h_2)^5 + (z_1/h_1)^4 \in R_9 := \overline{\mathbf{F}}[z_2/h_2,z_1/h_1],$$
$$I_9 := \langle f_9 \rangle \subset R_9,\ A_9 := R_9/I_9,\ Q(A_9) := \overline{\mathbf{F}}(z_2/h_2,z_1/h_1)/I_9$$
$$V(I_9) := \{((a_2 : b_2),(a_1 : b_1)) \in \mathcal{P}^1(\overline{\mathbf{F}}) \ :\ f_9(a_2/b_2,a_1/b_1) = 0\}$$

$$f_{10}(w_2,w_1) := w_2^2 w_1^4 + w_1^5 + w_2^3 \in R_{10} := \overline{\mathbf{F}}[w_2,w_1],$$
$$I_{10} := \langle f_{10} \rangle \subset R_{10},\ A_{10} := R_{10}/I_{10},\ Q(A_{10}) := \overline{\mathbf{F}}(w_2,w_1)/I_{10}$$
$$V(I_{10}) := \{(a_2,a_1) \in \overline{\mathbf{F}}^2 \ :\ f_{10}(a_2,a_1) = 0\}$$

$$f_{11}(w_2,w_1,w_0) := w_2^2 w_1^4 + w_1^5 w_0 + w_2^3 w_0^3 \in R_{11} := \overline{\mathbf{F}}[w_2,w_1,w_0],$$
$$I_{11} := \langle f_{11} \rangle \subset R_{11},\ A_{11} := R_{11}/I_{11},\ Q(A_{11}) := \overline{\mathbf{F}}(w_2,w_1,w_0)/I_{11}$$
$$V(I_{11}) := \{(a_2 : a_1 : a_0) \in \mathcal{P}^2(\overline{\mathbf{F}}) \ :\ f_{11}(a_2,a_1,a_0) = 0\}$$

$$f_{12}(w_2/h_2,w_1/h_1) := (w_2/h_2)^2 (w_1/h_1)^4 + (w_1/h_1)^5 + (w_2/h_2)^3 \in R_{12} := \overline{\mathbf{F}}[w_2/h_2,w_1/h_1],$$
$$I_{12} := \langle f_{12} \rangle \subset R_{12},\ A_{12} := R_{12}/I_{12},\ Q(A_{12}) := \overline{\mathbf{F}}(w_2/h_2,w_1/h_1)/I_{12}$$
$$V(I_{12}) := \{((a_2 : b_2),(a_1 : b_1)) \in \mathcal{P}^1(\overline{\mathbf{F}}) \ :\ f_{12}(a_2/b_2,a_1/b_1) = 0\}$$

Regardless of the form, there are rational functions with divisors

$$((x_1 = x_1/x_0 = x_1/h_1)) = (-2) \cdot P_1 + (-1) \cdot P_2 + 3 \cdot P_3$$

$$((x_2 = x_2/x_0 = x_2/h_2)) = (-3) \cdot P_1 + 2 \cdot P_2 + 1 \cdot P_3$$

$$((y_1 = y_1/y_0 = y_1/h_1)) = (-3) \cdot P_1 + 2 \cdot P_2 + 1 \cdot P_3$$

$$((y_2 = y_2/y_0 = y_2/h_2)) = (-5) \cdot P_1 + 1 \cdot P_2 + 4 \cdot P_3$$

$$((z_1 = z_1/z_0 = z_1/h_1)) = (-5) \cdot P_1 + 1 \cdot P_2 + 4 \cdot P_3$$

$$((z_2 = z_2/z_0 = z_2/h_2)) = (-7) \cdot P_1 + 0 \cdot P_2 + 7 \cdot P_3$$

$$((w_1 = w_1/w_0 = w_1/h_1)) = 3 \cdot P_1 + (-2) \cdot P_2 + (-1) \cdot P_3$$

$$((w_2 = w_2/w_0 = w_2/h_2)) = 5 \cdot P_1 + (-1) \cdot P_2 + (-4) \cdot P_3$$

There is the common object to all of this, namely the function field $\mathbf{K} := Q(A_i)$. All of the variables used above, whether written explicitly rationally or not, can be viewed as elements of this function field. As such they naturally take on values from $\overline{\mathbf{F}} \cup \{\infty\}$, an invariant of the Laurent series expansions at a given point. At P_1, $x_1, x_2, y_2, z_2, w_1, w_2$ have respective coordinate values $\infty, \infty, \infty, \infty, 0, 0$; at P_2, $\infty, 0, 0, 1, \infty, \infty$; and at P_3, $0, 0, 0, 0, \infty, \infty$.

The limitation of affine coordinates should be obvious, in that there are different functions that have no affine coordinates at different points. Is this a problem? Well restriction to A_i gives a different perspective depending on i, since behavior at non-affine points is ignored. So, for instance A_1 is non-singular in some affine sense, as is A_4. More importantly, as mentioned above, birational maps are attemps at mapping at the level of the quotient ring A_i instead of at the level of the function field $Q(A_i)$. Since all the $Q(A_i)$ are the same function field $\mathbf{K}$, these birational maps are really the identity map on $\mathbf{K}$ (unless you are of the school that thinks that giving new names to existing objects constitutes an isomorphism rather than an identification), whereas there are obvious domain and range problems with trying to restrict to maps between the A_i. This leads to all sorts of red herrings, such as exceptional divisors in blowups.

The limitation to projective coordinates is that they are not really individual coordinates of individual functions (unless you view them in $\overline{\mathbf{F}}^{m+1}$, but rather a bunch of ratios of same, some of which end up being $0/0$). Yet this is the standard generalization chosen of affine coordinates instead of the rational coordinates suggested here as a much better alternative.

It should bother anyone, as it does me now, to talk about multiple points, absent the realization that what is happening is that algebraic curves viewed relative to a given ordered list of rational functions are really projections of the actual algebraic curve, with the possibility that some points may look the same if only described by those particular coordinates and some other points may be hidden.

It would seem that a minimum requirement for understanding an algebraic curve would be a choice of coordinate functions that would at least distinguish points of the curve from each other. Only then are we ready to talk about properties at a given point on the algebraic curve.

So a strongly desingularized model for the Klein curve may be in terms of several rational functions, not just two. For instance, start from the defining equation $x^3y + y^3z + z^3x = 0$, and use $x_1 := x/y$, $x_2 := z/x$, $x_3 := y/z$ to get a Gröbner basis for the ideal of induced relations:

$$x_3^2x_2^2 + x_2^2x_1 + x_3x_1,\ x_2^2x_1^2 + x_3^2x_2 + x_2x_1,\ x_3^2x_1^2 + x_3x_1^2 + x_3x_2,\ x_3x_2x_1 - 1.$$

This has local parameters $t_i := x_i$ and local units $u_i := x_{i+1}/x_i^2$ at P_i, $1 \leq i \leq 3$.

A different presentation, in special position, is non-singular everywhere except at P_1 where all the coordinate functions have their poles. This has rational functions $f_3 := y/z$, $f_5 := xy/z^2$, and $f_7 := x^2y/z^3$, with ideal of induced relations having Gröbner basis

$$f_7^2 + f_5f_3^2 + f_7,\ f_7f_5 + f_3^4 + f_5,\ f_5^2 - f_7f_3$$

describing a strict $\overline{\mathbf{F}}[f_3]$-algebra with module basis $(1, f_5, f_7)$. The relations are those needed to describe the algebra multiplication, the subscripts reflect the pole orders at the special point at infinity. The monomial ordering used is a weight-over-grevlex (though grevlex-over-weight is useful as well), not a default monomial ordering, in order that the reduction rules (6) at least reduce products of basis elements to module form.

Given that there is a recognition that there are rational functions of some sort related to projective curves, and even discrete valuation rings to explain the size of zeros or poles, it is surprising (at least to me) that there is no mention of explicit Laurent series expansions or any serious use of coordinates in $\overline{\mathbf{F}} \cup \{\infty\}$.

These formal Laurent series are in terms of a local parameter,t, and a local unit, $u = u(t)$, meaning a power series in t with non-zero constant term. Here these could be chosen as

$$x_1 = t_1^{-2}u_1^{-1},\ x_2 = t_1^{-3}u_1^{-1},\ t_1 := x_1/x_2,\ u_1 := x_2^2/x_1^3,$$

$$x_1 = t_2^{-1},\ x_2 = t_2^2u_2,\ t_2 := 1/x_1,\ u_2 := x_2x_1^2,$$

$$x_1 = t_3^3u_3^2,\ x_2 = t_3u_3,\ t_3 := x_1/x_2^2,\ u_3 := x_2^3/x_1,$$

gotten from multi-blowups (??) at P_1, P_2, and P_3.

So we could settle for either

$$x_1(P_1) = \infty,\ x_2(P_2) = \infty,$$
$$x_1(P_2) = \infty,\ x_2(P_2) = 0,$$
$$x_1(P_3) = 0,\ x_2(P_3) = 0;$$

or

$$f_3(P_1) = f_5(P_1) = f_7(P_1) = \infty,$$
$$f_3(P_2) = f_5(P_2) = 0,\ f_7(P_2) = 1,$$
$$f_3(P_3) = f_5(P_3) = f_7(P_3) = 0.$$

Then P_1, P_2, P_3 are at least distinguished from each other. If we looked only at affine varieties, then we would have to ignore either P_1 and P_2 in the first case or just P_1 in the second. If we tried projective coordinates, then

$$(x_0(P_1) : x_1(P_1) : x_2(P_1)) = (0 : 0 : 1),$$
$$(x_0(P_2) : x_1(P_2) : x_2(P_3)) = (0 : 1 : 0),$$
$$(x_0(P_1) : x_1(P_2) : x_2(P_3)) = (1 : 0 : 0)$$

might make sense in the first case; whereas

$$(x_0(P_1) : f_3(P_1) : f_5(P_1) : f_7(P_1)) = (0 : 0 : 0 : 1),$$
$$(x_0(P_2) : f_3(P_2) : f_5(P_2) : f_7(P_2)) = (1 : 0 : 0 : 1),$$
$$(x_0(P_3) : f_3(P_3) : f_5(P_3) : f_7(P_3)) = (1 : 0 : 0 : 0)$$

might make sense in the second case.

An alternative is

$$x_1(P_1) = (1 : 0),\ x_2(P_1) = (1 : 0),$$
$$x_1(P_2) = (1 : 0),\ x_2(P_2) = (0 : 1),$$
$$x_1(P_3) = (0 : 1),\ x_2(P_3) = (0 : 1);$$

or

$$f_3(P_1) = f_5(P_1) = f_7(P_1) = (1 : 0),$$
$$f_3(P_2) = f_5(P_2) = (0 : 1),\ f_7(P_2) = (1 : 1),$$
$$f_3(P_3) = f_5(P_3) = f_7(P_3) = (0 : 1).$$

These are both gotten by considering variables (at least implicitly) as rational functions with individual coordinates from the projective line gotten by homogenizing each variable separately rather than homogenizing equations with only one extra homogenizing variable overall.

Chapter 14

Genus 0

14.1 Paramterization

It is important to notice that genus 0 curves are special in that the function field is isomorphic to $\mathbf{F}(x_0/h_0)$. That means that all rational functions are parameterized by x_0/h_0. To understand how a given pair of functions are related, it is sufficient to compare their pararmeterizations instead of looking at the parameterless equations they satisfy. [The local parameter is $t_P := x_0/h_0 - (x_0/h_0)(P)$ and the local unit is $u_P := 1$, with relation $\overline{f}(t_p, u_P) = 0$.]

A common example is given by

$$y^2 - x^3 - x^2 = 0,$$

meaning

$$(x_2/h_2)^2 - (x_1/h_1)^3 - (x_1/h_1)^2 = 0$$

This has

$$x_2/h_2 = (x_0/h_0)^3 - (x_0/h_0),\ x_1/h_1 = (x_0/h_0)^2 - 1.$$

So there is a double point at $x_2/h_2 = (0:1) = x_1/h_1$ corresponding to $x_0/h_0 = (\pm 1 : 1)$. And there is a cusp at $x_2/h_2 = (1:0) = x_1/h_1$ corresponding to $x_0/h_0 = (1:0)$. Another common example is given by

$$x^2 - y^3 = 0,$$

meaning

$$(x_2/h_2)^2 - (x_1/h_1)^3 = 0.$$

This has

$$x_2/h_2 = (x_0/h_0)^3,\ x_1/h_1 = (x_0/h_0)^2;$$

so there are cusps at both $x_2/h_2 = x_1/h_1 = x_0/h_0 = (0:1)$ and $x_2/h_2 = x_1/h_1 = x_0/h_0 = (1:0)$.

The circle $x_2^2 + x_1^2 - 1 = 0$ does not have the origin $x_2 = 0 = x_1$ as a solution; so use $x_3 := x_2 - 1$ to change it to $x_3(x_3 + 2) + x_1^2 = 0$ that has $x_3 = 0 = x_1$ as a solution. Then try the rational map $x_3 = t^2 u$ and $x_1 = tu$ for $t := x_3/x_1$ and $u := x_1^2/x_3$ to get $t^2u(t^2u + 2) + t^2u^2 = 0$. Cancel the common factor t^2u (as exceptional divisors are meaningless in the function field approach) to get the irreducible relation $2 + u + t^2u = 0$ between t and u. This happens to be easy to solve to get $u = -2/(1 + t^2)$, which gives the standard rational parameterization of the circle as $x_2 = (1 - t^2)/(1 + t^2)$ and $x_1 = -2t/(1 + t^2)$. If t is restricted to $\mathcal{P}^1(\mathbf{R})$, this gives the traditional circle, whereas if t comes from $\mathcal{P}^1(\mathbf{C})$, ...

14.2 Circle example

Let's see what we can learn from a circle, with defining equation

$$x_2^2 + x_1^2 - 1 = 0.$$

This has solutions $x_1 = a$, $x_2 = \pm\sqrt{1-a^2}$, but we usually think that $a \in \mathbf{R}$ with $|a| \leq 1$, whereas the theory of algebraic curves usually calls for an algebraically closed field such as $\mathbf{C} = \overline{\mathbf{R}}$. There this circle is just the restriction of the curve to points with both coordinates in $\mathbf{R}$. (For $a \in \mathbf{R}$ with $|a| \geq 1$ the restriction looks like an hyperbola instead.) Over finite fields our geometric intuition is of even less use; and in characteristic 2 the defining polynomial $(x_2^2 + x_1^2 - 1) = (x_2 + x_1 + 1)^2$ is not even irreducible.

So let's avoid characteristic 2 in this example, and extend $x_1 = a \in \overline{\mathbf{F}}$ to $(x_2, x_1) = (\pm\sqrt{1-a^2}, a) \in \overline{\mathbf{F}}^2$. Should there be any other points on the curve? If we homogenize the equation to get

$$x_2^2 + x_1^2 - x_0^2 = 0,$$

then the affine points above are $(x_2 : x_1 : x_0) = (\pm\sqrt{1-a^2} : a : 1) \in \mathcal{P}^2(\overline{\mathbf{F}})$, but $(x_1 : x_0) = (1 : 0) \in \mathcal{P}^1(\overline{\mathbf{F}})$ extends to $(x_2 : x_1 : x_0) = (\pm i : 1 : 0) \in \mathcal{P}^2(\overline{\mathbf{F}})$.

Now consider what happens when we use $h_1 := x_1^{-1}$ and $h_2 := x_2^{-1}$ as our variables to get

$$h_2^2 h_1^2 - h_2^2 - h_1^2 = 0.$$

This has affine solutions $h_1 := b \in \overline{\mathbf{F}}$, extending to $(h_2, h_1) = (\pm b/\sqrt{b^2-1}, b)$ unless $b = \pm 1$. If we homogenize the equation, then

$$h_2^2 h_1^2 - h_2^2 h_0^2 - h_1^2 h_0^2 = 0$$

has affine solutions $h_1 := (b : 1) \in \mathcal{P}^1(\overline{\mathbf{F}})$, extending to $(h_2 : h_1 : h_0)) = (\pm b/\sqrt{b^2-1} : b : 1)$ unless $b = \pm 1$. But $(h_1 : h_0) = (1 : 0)$ extends to $(h_2 : h_1 : h_0) = (0 : 1 : 0)$, whereas $(h_2 : h_1 : h_0) = (1 : 0 : 0)$ is not an extension of $(h_1 : h_0) = (0 : 0)$. [This can be avoided by making this into an affine problem, then reading off the results projectively, but maybe it is really $(\infty : \pm 1 : 1)$ in disguise.]

Now see what happens when each variable is homogenized separately to get

$$x_2^2 h_1^2 + h_2^2 x_1^2 - h_2^2 h_1^2 = 0.$$

This would seem to get us the original affine solutions now written as $((x_2 : h_2), (x_1 : h_1)) = ((\pm\sqrt{1-a^2} : 1), (a : 1)) \in (\mathcal{P}^1(\overline{\mathbf{F}}))^2$ and only one non-affine solution $((x_2 : h_2), (x_1 : h_1)) = ((1 : 0), (1 : 0)) \in (\mathcal{P}^1(\overline{\mathbf{F}}))^2$.

The reason there were not two solutions is that this is now a singular equation. Define $x_3/h_3 := (x_2/h_2)/(x_1/h_1)$. The ideal of relations is then

$$\langle x_2^2 h_1^2 + h_2^2 x_1^2 - h_2^2 h_1^2,\ x_3 h_2 x_1 - h_3 x_2 h_1,\ x_3^2 x_1^2 + h_3^2 x_1^2 - h_3^2 h_1^2 \rangle.$$

So $((x_2 : h_2), (x_1 : h_1)) = ((1 : 0), (1 : 0)) \in (\mathcal{P}^1(\overline{\mathbf{F}}))^2$. extends to

$$((x_3 : h_3), (x_2 : h_2), (x_1 : h_1)) = ((\pm 1 : 1), (1 : 0), (1 : 0)) \in (\mathcal{P}^1(\overline{\mathbf{F}}))^3.$$

[This can be reduced to affine terms by adding the relations $h_i(h_i - 1) = 0 = (x_i - 1)(h_i - 1)$ for all i, similar to appending the relations $h_0(h_0 - 1) = h_1(h_1 - 1)(h_0 - 1) = (h_2 - 1)(h_1 - 1)(h_0 - 1) = 0$ to reduce a projective curve to affine terms.]

The takeaway from this is that:

- Any affine part of an algebraic curve misses some points, and those may be important points.

- Projective coordinates give only partial information about how the underlying variables are related when more than one coordinate is 0.
- The proposed rational coordinates are not so restricted, though they are only shorthand for the underlying Laurent series expansions of each rational function used to coordinatize the curve.
- In any case, it is probably necessary to make a problem affine by adding non-homogeneous relations to the homogeneous ones, in order to use elimination and extension to solve for coordinates of points recursively.
- Extension has exceptions in the affine case, is not really extension in the projective case, and seems to work just fine relative to these new rational coordinates. That is, the previous affine exceptions are asymptotes, expressible by appending a value ∞; and the new rational coordinates extend naturally from m-tuples to $(m+1)$-tuples as the affine coordinates do but the projective coordinates don't.

ity

Chapter 15

Presentations

Algebras were initially defined over a field $\mathbf{F}$ as finite-dimensional vector spaces with a multiplication $y_i y_j = \sum_k r_{i,j,k} y_k$ for $r_{i,j,k} \in \mathbf{F}$. This was later generalized to finite-dimensional modules over a ring. For us the ring is $R := \overline{\mathbf{F}}[\underline{x}]$, and the following are my more restrictive definitions.

15.1 Strict affine algebras

Consider the quotient ring

$$A := \mathbf{F}[x_2, x_1]/\langle x_2^3 + x_2 x_1 + x_1^5 \rangle,$$

which has $x_3 := x_2^2/x_1$ integral over it. It is possible to present the integral closure as

$$\overline{A} := \mathbf{F}[x_3; x_2, x_1]/\langle x_3^2 + x_3 + x_2 x_1^3,\ x_3 x_2 + x_2 + x_1^4,\ x_3 x_1 - x_2^2,\ x_2^3 + x_2 x_1 + x_1^5 \rangle.$$

This presentation is as a strict affine A-algebra (52) in that there is an A-module generating set $(1, x_3)$ with quadratic relation $x_3^2 + x_3 + x_2 x_1^3$ defining the only non-trivial multiplication rule $x_3 \cdot x_3 = -1 \cdot x_3 - x_2 x_1^3 \cdot 1$. The linear relations $x_3 x_2 + x_2 + x_1^4$ and $x_3 x_1 - x_2^2$ define syzygies $x_2 \cdot x_3 + (x_2 + x_1^4) \cdot 1 = 0$ and $x_1 \cdot x_3 + (-x_2^2) \cdot 1 = 0$ (if one thinks of this over A and writes coefficients on the left).

This is supposed to be the theory from the SINGULAR book, so let's see how close we get in the three CAS's we're using.

```
                     SINGULAR                                /
 A Computer Algebra System for Polynomial Computations       /   version 4.0.1
                                                           0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann     \   Sep 2014
FB Mathematik der Universitaet, D-67653 Kaiserslautern        \

LIB "normal.lib";
ring R=0,(x2,x1),lp;
ideal I=x2^3+x2*x1+x1^5;I;
//       I[1]=x2^3+x2*x1+x1^5
list nor=normal(I);nor;
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering dp
```

```
//                  : names    T(1)
//        block   2 : ordering lp
//                  : names    x2 x1
//        block   3 : ordering C
//      _[1]=x2^2
//      _[2]=x1
def Rbar=nor[1][1];
setring Rbar;
option(redSB);
ideal Ibar=std(norid);Ibar;
//    Ibar[1]=x2^3+x2*x1+x1^5
//    Ibar[2]=T(1)*x1-x2^2
//    Ibar[3]=T(1)*x2+x2+x1^4
//    Ibar[4]=T(1)^2+T(1)+x2*x1^3
```

This can be viewed as the desired $A = R/I$-algebra.

```
Macaulay2, version 1.7

R=QQ[x2,x1,MonomialOrder=>{Lex}];
I=ideal(x2^3+x2*x1+x1^5);
A=R/I;
ic=integralClosure(A);
G=gens gb ideal ic;
    x1^5+x2^3+x2*x1,
    w_(0,0)*x1-x2^2,
    w_(0,0)*x2+x1^4+x2,
    w_(0,0)^2+w_(0,0)+x2*x1^3
```

But Macaulay2's code is written so that the input monomial ordering is ignored in favor of a default grevlex monomial ordering.

```
R<x2,x1>:=PolynomialRing(Rationals(),2);
I:=ideal<R|x2^3+x2*x1+x1^5>;
N:=Normalisation(I);
x2@N[1][2];
--   $.2
x1@N[1][2];
--   $.1
G:=GroebnerBasis(N[1][1]);G;
--    $.1^4 + $.2*$.3 + $.2,
--    $.1^3*$.2 + $.3^2 + $.3,
--    $.1^2*$.2^3 + $.3^3 + $.3^2,
--    $.1*$.2^5 + $.3^4 + $.3^3,
--    $.1*$.3 - $.2^2,
--    $.2^7 + $.3^5 + $.3^4
```

And Magma, for better or worse is under no constraint to even have A explicitly as a subring. It chooses a lex monomial ordering overall, and moreover one that is probably the reverse of the best lex monomial ordering in general.

But all three of these ignore the fact that A itself is a P-algebra for the Noether normalization $P := \overline{\mathbf{F}}[x_1]$. A has P-module basis $(1, x_2, x_3 := x_2^2)$ The one relation $x_2^3 + x_2x_1 + x_1^5$ induces the multiplication rules $x_2 \cdot x_2 = x_3$, $x_3 \cdot x_2 = -x_1 \cdot x_2 + (-x_1^5) \cdot 1$, and $x_3 \cdot x_3 = -x_1 \cdot x_3 + (-x_1^5) \cdot x_2$. But then $\overline{A}$ can also be viewed as a P-algebra with P-module basis $(1, x_2, x_4 := x_3/x_1)$ and multiplication rules $x_2 \cdot x_2 = x_1 \cdot x_4$, $x_4 \cdot x_2 = -x_1 \cdot x_2 + (-x_1^5) \cdot 1$, and $x_4 \cdot x_4 = -1 \cdot x_4 + (-x_1^3) \cdot x_2$.

Definition 51. *Let $P := \mathbf{F}[\underline{x}]$ be a multivariate polynomial ring, $A := P[\underline{y}]/I$ an integral domain with no y_i independent of P. Then P is called a Noether normalization of A. And $\overline{A}$ is called a strict affine P-algebra iff I has a minimal, reduced Gröbner basis B having quadratic elements of the form*

$$y_i \cdot y_j - \sum_k p_{i,j,k} y_k$$

necessary to define the P-algebra multiplication, linear elements

$$\sum_k p_k y_k$$

defining any syzygies (P-linear relations) among the P-generators, and no other relations. If there are no P-linear relations then this is a strict P-algebra and if there are P-relations of larger degree than 2, then this is not strict.

Definition 52. *If P is replaced by the quotient ring A above, then $\overline{A}$ can be called a strict affine A-algebra, again with or without the adjectives affine and/or strict.*

So why choose either an affine P-algebra or an affine A-algebra presentation? The MAGMA output above should suggest that having no structure and a default monomial ordering is not the best way to get get output that contains readable information, whether it is mathematically correct or not.

Choosing to present over a Noether normalization rather than the input ring at least recognizes that there is a minimal subring P over which this can be done (though there are numerous choices for P). This does sacrifice having the input ring A as an explicit subring of $\overline{A}$. If one thinks that A is important then this is not desired, but if one views things from the perspective of the output, there are numerous choices of both A and P that would produce the same $\overline{A}$, with some giving nicer presentations than others.

In this particular example there is further structure that can be used. From the divisors

$$((x_1)) = (-3) \cdot P_1 + (2) \cdot P_2 + (1) \cdot P_3$$
$$((x_2)) = (-5) \cdot P_1 + (1) \cdot P_2 + (4) \cdot P_3$$
$$((x_4)) = (-7) \cdot P_1 + (0) \cdot P_2 + (7) \cdot P_3$$

it makes sense to use the names $f_3 := x_1$, $f_5 := x_2$, and $f_7 := x_4$ to reflect the pole orders at P_1. Then using $P := \overline{\mathbf{F}}[f_3]$, there is a nice P-algebra presentation with ideal of induced relations

$$I := \langle f_7^2 + f_5 f_3^3 + f_7,\ f_7 f_5 + f_3^4 + f_5,\ f_5^2 - f_7 f_3 \rangle.$$

This corresponds to the P-multiplication (reduction rules)

$$f_7^2 = -f_5 f_3^3 - f_7,\ f_7 f_5 = -f_3^4 - f_5,\ f_5^2 = f_7 f_3,$$

which have the nice property that the reduction of any element is to a standard polynomial with the same pole order at P_1. The useful byproducts of this are at there is a nice basis for the Riemann-Roch spaces

of (equivalence classes of) functions (modulo the curve) of the form $\{f_i f_3^j \ : \ i \in \{0,5,7\},\ j \geq 0\}$, and the genus of the curve is 3, the number of missing pole orders (since $1,2,4$ are said orders.

Note that to get this presentation some care must be given to the choice of monomial ordering. There is an induced ordering based on the pole orders, so one cannot just settle for some default/ input ordering. Here one can either extend a matrix $\begin{pmatrix} 5 & 3 \\ 1 & 0 \end{pmatrix}$ to $\begin{pmatrix} 7 & 5 & 3 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ or a matrix $\begin{pmatrix} 1 & 0 \\ 5 & 3 \end{pmatrix}$ to $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 7 & 5 & 3 \end{pmatrix}$, called weight-over-grevlex and grevlex-over-weight for obvious reasons.

15.2 Special position

The affine form of the Klein quartic:

$$A := \mathbf{F}[y,x]/\langle y^3 + yx^3 + x\rangle$$

is an integral extension of a polynomial ring $P := \mathbf{F}[x]$ (so having P as a given Noether normalization), non-singular and integrally closed. [It is considered flattened when written this way instead of $A := P[y]/\langle y^3 + yx^3 + x\rangle$.]

The other affine form

$$A := \mathbf{F}[x,y]/\langle x^3y + x + y^3\rangle$$

is a non-integral extension of a polynomial ring $P := \mathbf{F}[y]$; again with given Noether normalization P, but not *integral*, though it is still non-singular, integrally closed, and flattened (as opposed to $A := P[x]/\langle yx^3+x+y^3\rangle$. It is possible to change variables, using $\overline{x} := xy$ in place of x to get

$$B := (\mathbf{F}[y])[\overline{x}]/\langle \overline{x}^3 + y\overline{x} + y^5\rangle,$$

which is integral, but not non-singular or integrally closed, since

$$\left(\frac{\overline{x}^2}{y}\right)^3 - 2\left(\frac{\overline{x}^2}{y}\right)^2 + \left(\frac{\overline{x}^2}{y}\right) - y^7 = 0.$$

Why would one give up nice properties such as being non-singular and integrally closed for being integral? The equivalence classes modulo the ideal of relations in the first correspond to classes of rational functions that have may have poles (Laurent series that may not be power series when x and/or y have such series). The equivalence classes modulo the ideal of relations in the second correspond to classes of rational functions that have may have poles (Laurent series that may not be power series when only y may have such a series, since this forces $\overline{x}$ to have such as well).

And there is really no tradeoff, in the sense that it is possible to compute the integral closure of the second as

$$C := (\mathbf{F}[z,\overline{x};y])/\langle z^2 + z + \overline{x}y^3,\ z\overline{x} + \overline{x} + y^4,\ \overline{x}^2 - zy\rangle$$

or

$$D := (\mathbf{F}[z;\overline{x},y])/\langle z^2 + z + \overline{x}y^3,\ z\overline{x} + \overline{x} + y^4,\ zy - \overline{x}^2,\ \overline{x}^3 + \overline{x}y + y^5\rangle.$$

C is written as an $\mathbf{F}[y]$-algebra with basis $(1,\overline{x},z)$, whereas D is written as an $\mathbf{F}[\overline{x},y]$-algebra with basis $(1,z)$. Which is better? While that is subjective; however, if somehow the integral closure were given first in some objective way that didn't suggest one over the other, it would seem that the choice would be to write it as an algebra over the smallest subring over which it is a finite integral extension, namely a Noether normalization such as $P := \mathbf{F}[y]$ here.

To provide perspective on this crucial point, consider the implementations of de Jong's algorithm for integral closures. SINGULAR's original `normal` function produced only a quotient ring, which didn't really match the theory in their SINGULAR text, which is that it be an affine algebra over the input ring. This was subsequently changed for the better, so that at least the output matched the theory, with necessarily a default product ordering to preserve the input. MACAULAY2's `integralClosure` output is merely a quotient ring containing an explicit copy of the input, again necessarily with a default product ordering. MAGMA's `Normalisation` function returns not only a quotient ring generally not containing an explicit copy of the input (though it does provide a map from the input), but it chooses a very bad default monomial ordering.

Also there are divisors, bookkeeping devises to keep track of zeros and poles of rational, homogeneous functions:

$$((x)) = (-2)\cdot Q_1 + (-1)\cdot Q_2 + 3\cdot Q_3;$$
$$((y)) = (-3)\cdot Q_1 + 2\cdot Q_2 + 1\cdot Q_3;$$
$$((\overline{x})) = (-5)\cdot Q_1 + 1\cdot Q_2 + 4\cdot Q_3;$$
$$((z)) = (-7)\cdot Q_1 + 7\cdot Q_3.$$

So C has a natural weight function corresponding to the pole order at the point Q_1, hence the one-point presentation given in the introduction:

$$\mathbf{F}[f_7, f_5; f_3]/\langle f_7^2 + f_5 f_3^3 + f_7,\ f_7 f_5 + f_3^4 + f_5,\ f_5^2 - f_7 f_3\rangle.$$

Again, this has, as a by-product, that the genus of the curve is $g = 3$, the number of non-negative integers with no corresponding function of that weight, as the *standard* monomials, f_3^j, $f_5 f_3^j$, and $f_7 f_3^j$, $j \geq 0$ cover all weights other than 1, 2, and 4. These standard monomials can be used to generate the Riemann-Roch spaces of (classes of rational, homogeneous) functions (modulo the curve) with poles of orders between 0 and some fixed positive integer m inclusive, for any m. Not only that, but these functions can be evaluated affinely at any point other than the special point at infinity where they all have poles.

Compare all this to what can be read off the non-singular model presentation. That presentation is meant to be able to do two things. One is to separate points, the other is to produce explicit local parameters for all points. If there is a singularity (affine or not), it is relatively simple theoretically to place that singularity at the origin. If there is more than one point (that is, set of Laurent series) there, then often the orders of the zeros of the variables are different, and a simple blow-up will separate the points there. But several blow-ups may have to be used to separate those points when the Laurent series agree for several smallest terms. And even when there is only one point projected onto the origin, not having a local parameter will register as a having a singularity.

To see this behavior, consider the following two examples. The divisors are:

$$\mathbf{F}_2[y, x]/\langle y^5 + y^3 x^5 + x^7\rangle.$$

$$((x)) = (-2)\cdot Q_1 + (-3)\cdot Q_2 + 5\cdot Q_3;$$
$$((y)) = (-5)\cdot Q_1 + (-2)\cdot Q_2 + 7\cdot Q_3.$$

So the origin, Q_3, has a singularity not because there are several underlying points, but rather because there is no explicit local parameter there. The Jacobian ideal would be $\langle y^4 + y^2 x^5,\ y^3 x^4 + x^6\rangle$, showing that the curve and its partial derivatives are all zero in the affine sense only at the origin. A simple blow-up there would introduce additional projective coordinates $(z : h)$ with $zx - yh = 0$ inducing the relation $z^5 + z^3 x^3 + x^2 = 0$. From

$$((z/h)) = ((y/x)) = (-3)\cdot Q_1 + 1\cdot Q_2 + 2\cdot Q_3$$

it is clear that there is still a singularity at the origin. A second blow-up probably introduces new projective coordinates, but of what flavor? For now let's pretend to ignore h and y; and just start with $z^5 + z^3 x^3 + x^2 = 0$. Then introducing $(u : v)$ with $zv - xu = 0$ induces $z^3 + z^4 v^3 + v^2 = 0$.

$$((v/u)) = ((x/z)) = 1\cdot Q_1 + (-4)\cdot Q_2 + 3\cdot Q_3$$

Then introducing $(r : s)$ with $rz - sv = 0$ induces $z + z^5 r^3 + r^2 = 0$.

$$((r/s)) = ((v/z)) = 4\cdot Q_1 + (-5)\cdot Q_2 + 1\cdot Q_3.$$

Loosely, it would require keeping local parameters v, z, and r, at Q_1, Q_2, and Q_3 respectively, maybe with the relations $z^3 + z^4v^3 + v^2 = 0$ and $z + z^5r^3 + r^2 = 0$ from above, possibly with the additional induced relation

$$v^{15}r^8 + v^{14} + v^{12}r^6 + v^{11}r^9 + v^{10}r^{12} + v^8r^7 + v^7r^{10} + v^5r^5 + v^4r^8 + v^2r^3 + r^9 = 0$$

explicitly relating r and v, or the whole ideal of induced relations among the three variables.

Also would it have been possible to jump directly to the output of the last blow-up from the first by looking at the divisors and computing a local parameter at the origin as x^3/y^2? Well, maybe; but that probably would not have resolved singularities at the other two points.

Chapter 16

Interpreting CAS output for normalisation

The equation

$$x^3y + y^3z + z^3x = 0$$

is somehow supposed to define the Klein quartic, which is supposed to be a non-singular, projective curve. How does a CAS know this? It probably doesn't.

In MAGMA,

```
R<x,y,z>:=PolynomialRing(Rationals(),3);
I:=ideal<R|x^3*y+y^3*z+z^3*x>;
N:=Normalisation(I);
G:=GroebnerBasis(N[1][1]);G;
x@N[1][2];
y@N[1][2];
z@N[1][2];
```

produces output

```
[    x^3*y + x*z^3 + y^3*z ]


x,y,z
```

In SINGULAR,

```
 LIB "normal.lib";
 ring r=0,(x,y,z),dp;
 ideal i=x3y+y3z+z3x;
 list nor=normal(i);nor;
```

produces

```
[1]:[1]:
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering dp
```

```
//                   : names    x y z
//         block   2 : ordering C
[2]:[1]:      _[1]=1
> def Rbar=nor[1][1];
> setring Rbar;
> ideal s=std(norid);s;
s[1]=x3y+y3z+xz3
> normap;
normap[1]=x
normap[2]=y
normap[3]=z
```

And in Macaulay2,

```
R=QQ[x,y,z];
I=ideal(x^3*y+x*z^3+y^3*z);
A=R/I;
time icf=icFractions(A)
ic=gens gb ideal integralClosure A
```

produces

```
| x3y+y3z+xz3 |
```

Each of these suggests somehow that the quotient ring $A = R/I$ is integrally closed/normal. But none of these actually addresses what type of curve or surface with which we should be dealing.

That is, there is nothing algebraically to differentiate between this describing a two-dimensional affine surface or a one-dimensional projective surface, given in terms of homogeneous polynomials. (The equation itself could even be used to define a two-dimensional projective surface, were there a fourth (homogenizing) variable in the ring.) And my choice is to use a completely different type of curve, which is neither affine nor projective.

Let's investigate this a bit. Suppose we start from the viewpoint of rational functions (elements of the function field) as objects capable of having zeros and poles at various points, whatever any of that means.

Then there are divisors, bookkeeping devises, for said zeros and poles:

$$\left(\left(\frac{x}{z}\right)\right) = (-2)P_1 + (-1)P_2 + 3P_3,$$

$$\left(\left(\frac{y}{z}\right)\right) = (-3)P_1 + 2P_2 + 1P_3,$$

suggesting that there should be a point at which both functions have poles, one at which only x/z has poles, and a third at which both have zeros.

The projective or affine viewpoint (as opposed to the function field one) is that rational functions are not really defined at points at which they have poles. This leads to defining a topology, regular functions, and all sorts of things that are irrelevant or even counterproductive, algebraically. The alternative is to let rational functions have the value ∞ at points where they have poles.

Maybe a minimum requirement for a good description of a curve, whatever a curve is, is one that has, at each point, an explicit local parameter, an element that has a simple zero at that point.

So maybe for the Klein curve, that should be in terms of $t_1 := x/y$, $t_2 := z/x$, and $t_3 := y/z$, with induced relations

$$t_1^3 t_3^3 + t_3^2 + t_1,\ t_2^3 t_1^3 + t_1^2 + t_2,\ t_3^3 t_2^3 + t_2^2 + t_3,\ t_1 t_2 t_3 - 1.$$

But absent allowing the value ∞, all three points above will have to be avoided, making the choice of variables as local parameters at those three points irrelevant.

Algebraically it makes perfectly good sense to talk about the function field, whether in terms of x/z and y/z or in terms of t_1, t_2, and t_3. But one has to make a decision about how to evaluate rational functions, especially if they are given explicitly as quotients of polynomials and the denominator evaluates to 0.

Does it make sense to define away such points at any cost? The answer here is absolutely not, given that there is a simple algebraic way to deal with them.

Chapter 17

Testing mathematical theory using CASs

It is possible to write definitions, theorems, and proofs, absent any examples, and produce a mathematically correct theory. Moreover theorems need not produce any useful information. Even if the theory is motivated by certain examples, those examples are often jettisoned before writing up the theory that was motivated by those examples.

The exact opposite should be true. It should be that examples are there to test whatever changes are made to the theory. Or if someone else has a similar theory examples can be used to compare or contrast those theories.

It is especially important to have test examples for code written to implement theory. The more well-thought-out examples, the better. And it is important to have both input and output in test examples, to let users know what was actually expected theoretically and why.

So a computer algebra system is not merely a scratch pad for doing various calculations not amenable to hand computation. It should be a tool for testing and improving (algebraic) theory. It is especially interesting when there are several implementations of the same or different algorithms that give seemingly different answers, that there be common examples relative to which they can be analyzed. This can lead to an understanding of what the underlying theory should be and what should be expected when it is applied to actual examples.

When I started along this path, I had in hand what I believed was a new algorithm for computing integral closures of rings in positive characteristic that were in special position, meaning that the variables represented rational functions that had no poles except possibly at a special point P_∞, this being useful in dealing with linear codes derived from algebraic curves.

The object I wanted to produce was the ring of all rational functions that had no poles except possibly at P_∞, so typically the integral closure of a quotient ring in special position. I was not at all interested in the quotient ring I started with, other than that it could be used to produce the ring $\mathbf{L}(\infty\mathbf{P}_\infty)$ that I desired.

And the curious thing was that while the algebraic geometry underlying all this was mired in geometry, topology, and/or analysis, this was seemingly a completely algebraic problem. That is, I could be blissfully ignorant of everything save the algebra, and still produce what I wanted to. (That still seems to be the case.)

I was able to

1. start with a polynomial ring such as $P := \mathbf{F_q}[x]$;
2. adjoin some element y satisfying an integral equation over P, say $y^5 + y^4 + x^7 = 0$;
3. use it to define an integral extension
$$A := \mathbf{F_q}[y, x]/\langle y^5 + y^4 + x^7 \rangle;$$
4. use the Frobenius map in characteristic $p > 0$ to do essentially linear algebra on a P-module $A/\Delta(x)$;
5. and produce the ring $C(A, Q(A))$, the integral closure of the ring A in its field of fractions $Q(A)$.

Since this was a departure from the ways this was usually done, I expected to use various coded algorithms in various CASs to compare my results with those already being produced by others based on a different approach to the subject. What I found surprised me, namely that there seemed to be no commonly accepted form for this integral closure.

17.1 IntegralClosure

When I started, MAGMA only had `IntegralClosure` available. The code

```
Q:=Rationals();
FF<x>:=FunctionField(Q);
PR<y>:=PolynomialRing(FF);
f:=y^5+y^4+x^7;
A<Y>:=RationalExtensionRepresentation(FunctionField(f));
C<X>:=CoefficientRing(A);
INT:=Integers(C);
ICA:=IntegralClosure(INT,A);
B:=Basis(ICA);
for i in [1..#B] do i-1,B[i]; end for;
```

produced output

```
0 1
1 Y
2 1/X*Y^2 + 1/X*Y
3 1/X^3*Y^3 + 1/X^3*Y^2
4 1/X^5*Y^4 + 1/X^5*Y^3
```

This is necessarily a basis for the integral closure of A viewed as a $\mathbf{Q}[x]$-algebra.

There is no attempt to produce a presentation of any sort, though it suffices to try to reduce $B[i] * B[j]$ manually to get a set of relations defining the algebra multiplications. [Note that it should be possible to use only $X, Y, (Y^4 + Y^3)/X^5$ to get the presentation I expected.]

17.2 Normalisation

At some later time MAGMA introduced `Normalisation`, which allows for more than just one independent variable, and gives a presentation as well.

The code

```
R<y,x>:=PolynomialRing(Rationals(),2);
I:=ideal<R|y^5+y^4+x^7>;
N:=Normalisation(I);
G:=GroebnerBasis(N[1][1]);G;
y@N[1][2];
x@N[1][2];
```

produces the output

```
    $.1^4 + $.2*$.3 + $.2,
    $.1^3*$.2 - $.3^2 - $.3,
    $.1^2*$.2^3 + $.3^3 + $.3^2,
    $.1*$.2^5 - $.3^4 - $.3^3,
    $.1*$.3 + $.2^2,
    $.2^7 + $.3^5 + $.3^4

$.3
$.2
```

This clearly produced a larger quotient ring with variables corresponding to $-x^2/y, x, y$ and a default lex monomial ordering on them. But this would seem to have a different number of elements than what `IntegralClosure` produced.

Note that even a lex monomial ordering in the reverse order here would have produced a better presentation. That is, the further code

```
P<g7,g5,g3>:=PolynomialRing(Q,3,"weight",[7,5,3,1,1,0,1,0,0]);
phi:=hom<Parent(G[1])->P|g3,g5,g7>;
J:=ideal<P|[phi(G[i]) : i in [1..#G]]>;
B:=GroebnerBasis(J);B;
```

produces the relations

```
g7^2 - g5*g3^3 + g7,
g7*g5 + g3^4 + g5,
g5^2 + g7*g3
```

17.3 integralClosure

Macaulay2 has `icFractions` to produce a set of fractions defining the integral closure as a quotient ring explicitly containing the input quotient ring A; and `integralClosure` which can be used with `gens gb ideal` to produce a presentation based on them.

```
R=QQ[y,x];
I=ideal(y^5+y^4+x^7);
A=R/I;
time icf=icFractions(A);
toString icf
g=gens gb ideal integralClosure A;
toString g
```

produces output

```
{(-x^4)/y^2, (-y*x^2-x^2)/y, y, x}

         x^7+y^5+y^4,
         w_(4,1)*y+y*x^2+x^2,
         w_(4,1)*x^5-y^5-2*y^4-y^3,
         w_(4,0)*y-w_(4,1)*x^2-x^4,
         w_(4,0)*x^3-y^3-y^2,
         w_(4,1)^2+w_(4,0)+2*w_(4,1)*x^2+x^4,
         w_(4,0)*w_(4,1)*x+y^3+2*y^2+y,
         w_(4,0)^2+y*x+x
```

This produces two new variables, and uses a default product monomial ordering, differentiating between new and old variables.

17.4 normalC

Now consider SINGULAR. When I started with SINGULAR what was used is what is now called `normalC` and not the current `normal`.

```
LIB "normal.lib";
ring r=0,(y,x),dp;
ideal i=y5+y4+x7;
list nor=normalC(i);nor;
normap;
def R=nor[1][1];
setring R;
option(redSB);
ideal s=std(norid);s;
```

produces output

```
normap[1]=T(1)
normap[2]=T(2)

s[1]=T(1)*T(2)+T(4)^2+T(2)
s[2]=T(1)^2+T(2)*T(3)+T(1)
s[3]=T(4)^3-T(3)^2
s[4]=T(3)^2*T(4)-T(1)*T(5)
s[5]=T(1)*T(3)*T(4)+T(3)*T(4)+T(2)*T(5)
s[6]=T(2)^2*T(4)-T(1)*T(3)
s[7]=T(3)^3-T(2)^2*T(5)
s[8]=T(2)*T(3)^2-T(1)*T(3)+T(4)*T(5)-T(3)
s[9]=T(2)^2*T(3)-T(1)*T(4)^2
s[10]=T(2)*T(4)^2*T(5)+T(2)*T(3)*T(4)-T(2)^2*T(5)-T(1)*T(4)+T(5)^2-T(4)
s[11]=T(2)^3*T(5)-T(1)*T(3)^2+T(3)*T(4)*T(5)-T(3)^2
s[12]=T(2)*T(3)*T(4)^2-T(1)*T(4)^2-T(4)^2+T(3)*T(5)
s[13]=T(2)^4+T(2)*T(3)*T(4)+T(1)*T(4)
```

This produces three new variables, and a default grevlex monomial ordering on the presentation with the old variables first.

17.5 normal

That was redone as the current `normal`, so that the results would match the theory in the SINGULAR text. So

```
list nor=normal(i);nor;
```

produces output

```
_[1]=y2x2
_[2]=-x6
_[3]=yx4
_[4]=y3
```

with

```
def R=nor[1][1];
setring R;
option(redSB);
ideal s=std(norid);s;
```

producing

```
s[1]=x^7+y^5+y^4
s[2]=T(3)*y^2-x^4
s[3]=T(3)*x^3+y^3+y^2
s[4]=T(2)*x-y^2-y
s[5]=T(2)*y+T(3)*x^2
s[6]=T(1)*y-x^2
s[7]=T(1)*x^2-T(3)*y
s[8]=T(3)^2+y*x+x
s[9]=T(2)*T(3)-T(1)*x-x^3
s[10]=T(1)*T(3)+T(2)
s[11]=T(2)^2+T(3)*y*x+T(3)*x
s[12]=T(1)*T(2)-y*x-x
s[13]=T(1)^2-T(3)
```

Here again there are three new variables, but the presentation is that of an affine algebra over the input, with a default product monomial ordering highlighting that the relations are of degrees at most 2 in the new variables.

This matches the theory in the SINGULAR book, namely that the result should be a strict affine algebra over the input, with the input relations explicit, linear relations among the new variables reflecting their definitions, and quadratic relations corresponding to the multiplication defining an algebra over the input.

17.6 Initial summary

So here are several seemingly different answers as to what the integral closure of a common input might be. Are they the same in some sense? And, if so, can that be shown? Which, if any of these is best, or at least useful, in any sense?

Absent knowing that this problem and ones like it had structure that could be used to understand these answers, I'm not sure I could have figured out how to show these were all isomorphic. [Indeed the existence of said structure was what led me to discovering errors in the original coding that caused premature termination.] That is, I should be able to write code that takes one of these as input and produces another. [That is slightly different than checking whether one CAS thinks the answer from another is correct by rewriting the output from one as input for another.]

17.7 Structure

This particular problem is one with some structure to the input, and expected induced structure to the output. That is, it was based on two rational functions y, x with poles only at one special point P_∞, of orders $7, 5$ respectively. Theoretically, the output should describe the quotient ring consisting of all rational functions with no poles except at P_∞.

So the input quotient ring has the form of a $\mathbf{Q}[f_5]$-algebra with module basis $(1, f_7, f_7^2, f_7^3, f_7^4)$. It is not unreasonable to expect a similar form of the output quotient ring.

Let's see if we can come close to doing this.

17.8 normal, weighted

`normal` now has an option of computing a denominator in the second variable; so using that and a weighted monomial ordering:

```
ring r=0,(f7,f5),wp(7,5);
ideal i=f7^5+f7^4+f5^7;
list nor=normal(i,"var2"); nor;
```

produces rational functions described by

```
      _[1]=f7^4+f7^3
      _[2]=f7^3*f5^2+f7^2*f5^2
      _[3]=f7^2*f5^4+f7*f5^4
      _[4]=f5^5
```

with

```
def R=nor[1][1];
setring R;
option(redSB);
ideal s=std(norid);s;
```

producing the presentation with ideal of relations

```
s[1]=f7^5+f5^7+f7^4
s[2]=T(3)*f5-f7^2-f7
s[3]=T(3)*f7^3+f5^6
s[4]=T(2)*f5^2-T(3)*f7
s[5]=T(2)*f7^2+f5^4
s[6]=T(1)*f7+f5^2
s[7]=T(1)*f5^2-T(2)*f7
s[8]=T(3)^2-T(2)*f7*f5-T(2)*f5
s[9]=T(2)*T(3)-T(1)*f5+f5^3
s[10]=T(1)*T(3)+f7*f5+f5
s[11]=T(2)^2+f7*f5+f5
s[12]=T(1)*T(2)+T(3)
s[13]=T(1)^2+T(2)
```

There are still three new variables and a presentation as an algebra over the input as before, with no suggestion of any induced structure. But it is possible to figure out that the pole orders of $T(1), T(2), T(3)$ are respectively $3, 6, 9$. So maybe it makes sense to have produced a module basis $(1, f_3, f_6, f_7, f_9)$ over $\mathbf{Q}[f_5]$, though that is not exactly what is highlighted in the above presentation. But, based on the pole orders, what should be sought, is a module basis $(1, f_5, f_7)$ over $\mathbf{Q}[f_3]$ instead.

So the further input

```
ring R1=0,(f9,f7,f6,f5,f3),wp(9,7,6,5,3);
map phi=R,f3,f6,f9,f7,f5;
option(redSB);
ideal s1=std(phi(s));s1;
```

produces the output

```
s1[1]=f6+f3^2
s1[2]=f9-f3^3
s1[3]=f5^2+f7*f3
s1[4]=f7*f5+f3^4+f5
s1[5]=f7^2-f5*f3^3+f7
```

which shows that from this perspective that $f6$, $f9$ are unnecessary, leaving only the 3 relations defining the multiplication in the $\mathbf{Q}[f_3]$-algebra presentation of the integral closure.

17.9 integralClosure, weighted

In Macaulay2

```
R=QQ[f7,f5,MonomialOrder=>{Weights=>{7,5},Weights=>{1,0}}];
I=ideal(f7^5+f7^4+f5^7);
A=R/I;
time icf=icFractions(A);
toString icf
g=gens gb ideal integralClosure A;
toString g
```

produces rational functions

```
 {(-f5^4)/f7^2, (-f7*f5^2-f5^2)/f7, f7, f5}
```

with presentation

```
f7^5+f5^7+f7^4,
w_(4,1)*f7+f7*f5^2+f5^2,
w_(4,1)*f5^5+f5^7-f7^4-f7^3,
w_(4,0)*f7-w_(4,1)*f5^2-f5^4,
w_(4,0)*f5^3-f7^3-f7^2,
w_(4,1)^2+w_(4,0)+2*w_(4,1)*f5^2+f5^4,
w_(4,0)*w_(4,1)*f5+f7^3+2*f7^2+f7,
w_(4,0)^2+f7*f5+f5
```

The induced pole orders of $w_{4,1}, w_{4,0}$ should be $10, 6$ respectively. The input

```
B=QQ[f10,f7,f6,f5,MonomialOrder=>{Weights=>{10,7,6,5},
                                  Weights=>{1,1,1,0},
                                  Weights=>{1,1,0,0},
                                  Weights=>{1,0,0,0}}];
phi=map(B,ring(g_(0,0)),matrix{{f6,f10,f7,f5}});
J=phi(g);J
```

produces

```
f7^5+f5^7+f7^4
f10f7+f7f5^2+f5^2
f10f5^5+f5^7-f7^4-f7^3-f10f5^2-f5^4+f7f6
-f7^3+f6f5^3-f7^2
f10^2+2f10f5^2+f5^4+f6
f7^3+f10f6f5+2f7^2+f7 f6^2+f7f5+f5
```

Is it clear from this that $f10 + f5^2$ is a rational function with pole order 3? Maybe if one knows there should be only one standard function for each pole order, that would lead to trying to find some way of reducing $f10$ mod $f5^2$ to some rational function of lower pole order. And isn't it important that the rational function of pole order 3 be explicit in the presentation? Maybe

```
B=QQ[f10,f7,f6,f5,f3,MonomialOrder=>{Weights=>{10,7,6,5,3},
                     Weights=>{1,1,1,1,0},
                     Weights=>{1,1,1,0,0},
                     Weights=>{1,1,0,0,0},
                     Weights=>{1,0,0,0,0}}];
phi=map(B,ring(g_(0,0)),matrix{{f6,f10,f7,f5}});
J=ideal(flatten entries(phi(g)));J;
K=J+ideal(f10+f5^2+f3);
G=gens gb K;
toString G
```

producing

```
f6+f3^2,
f10+f7*f3+f3,
f5^2-f7*f3,
f7*f5+f3^4+f5,
f7^2+f5*f3^3+f7
```

shows that $f6, f10$ can be replaced by $f3$.

17.10 Normalisation, weighted

In MAGMA the input

```
R<f7,f5x>:=PolynomialRing(Rationals(),2,"weight",[7,5,1,0]);
I:=ideal<R|f7^5+f7^4+f5^7>;
N:=Normalisation(I);N;
G:=GroebnerBasis(N[1][1]);G;
f7@N[1][2];
f5@N[1][2];
P<f7,f5,f3>:=PolynomialRing(Rationals(),3,"weight",[7,5,3,1,1,0,1,0,0]);
phi:=hom<Parent(G[1])->P|f3,f5,f7>;
J:=ideal<P|[phi(G[i]) : i in [1..#G]]>;
B:=GroebnerBasis(J);B;
```

produces

```
 f7^2 - f5*f3^3 + f7,
 f7*f5 + f3^4 + f5,
 f5^2 + f7*f3
```

17.11 The qth-power algorithm

My qth-power algorithm in Macaulay2 (or the earlier version in Magma) is supposed to deal with specifically these particular problems, with weights applied to the input inducing similar weights on the output.

```
loadPackage "QthPower";
wtr=matrix{{7,5}};
R=QQ[f7,f5,Weights=>entries weightGrevlex(wtr)];
GB={f7^5+f7^4+f5^7};
time ic0=rationalIntegralClosure(wtr,R,GB);
toString ic0
```

produces first

```
f5^5,
f7^4+f7^3,
f7^3*f5^2+f7^2*f5^2,
f7*f5^5,
f7^2*f5^4+f7*f5^4

p_0^2-p_2*p_4-p_3*p_4^3,
p_0*p_1-p_2*p_4^2,
p_0*p_2-p_3*p_4+p_4^3,
p_0*p_3+p_1*p_4+p_4,
p_1^2-p_0*p_4+p_1,
p_1*p_2-p_3*p_4^2,
p_1*p_3+p_4^2,
p_2^2+p_1*p_4+p_4,
p_2*p_3+p_0,
p_3^2+p_2

      QQ[p_0, p_1, p_2, p_3, p_4],
matrix {{  9,   7,   6,   3,   5}})
```

then

```
 ic=minimization(ic0);
 toString ic
```

produces

```
matrix {{  9,   7,   6,   5,   3}},
      QQ[p_0, p_1, p_2, p_3, p_4],

 p_3^2+p_1*p_4,
 p_1*p_3+p_4^4+p_3,
 p_1^2-p_3*p_4^3+p_1
```

This corresponds to first producing a $\mathbf{Q}[f_5]$-module basis $(f_0 := 1, f_3, f_6, f_7, f_9)$, and then minimizing it to extract a $\mathbf{Q}[f_3]$-module basis (f_0, f_5, f_7).

Since all of these answers are *mathematically correct*, what is the takeaway from all of this?

1. Should presentations be as affine algebras over the input A as the theory in the SINGULAR book suggests, affine algebras over a Noether normalization P as I expected, or just some quotient ring that describes it technically correctly, with no particular form?
2. What structure, if any, is induced on the new variables by the old variables?
3. Should the new variables be treated differently from the old variables?
4. What information should be explicit in the presentation?
5. Is it even necessary to have a presentation, or do the fractions suffice?

Maybe examples such as the one above are too special to be used to answer such questions? Or maybe trying to generalize beyond such examples forces a tradeoff between generalizing and losing useful information. But tradeoffs that lose information do not lead to real generalizations, in that it should not be necessary to lose information in special cases when generalizations are made.

`normal.lib` in SINGULAR is too inclusive in what it tries to tackle. It deals with splitting compound input into separate problems, which should be done before and independent of the actual integral closurecomputation, so that each integral closure input can be rethought in terms of its structure. If a minimal ideal generator factors in any way, then it doesn't really conform to being a minimal relation among the variables. And any structure to be had, will come from minimal relations among the generators, applicable to a specific part of a compound problem.

`integralClosure` in MACAULAY2's `IntegralClosure` package and `Normalisation` in MAGMA both suffer from having no theory to suggest what presentation is being given. That leaves the interpretation open to the user; unlike SINGULAR, which spells out the intended result, and what it is supposed to look like theoretically.

But the test examples in both `IntegralClosure.m2` and `normal.lib` suffer from only having input, with no intended output relative to which to compare the output produced. If the code is not changed one can infer that the output is what is intended, but with no reason why that should be the case.

In the `normal` case the output produced is meant to mirror the theory in the book, but using any of the available reduction options destroys that theory, with no explanation of why the reduction is being done. At least with my `minimization`, it should be clear that a better choice of Noether normalization leads to a smaller, better presentation relative to that Noether normalization.

Since none of the theory/code save mine has to do with viewing the integral closure of A relative to a Noether normalization P of A, and there is no acknowledgment that there is structure induced on the integral closure by that on the quotient ring from which it is produced, should there be a reworking of the theory relative to this viewpoint, or is the existing theory adequate?

17.12 non-integral extensions

There are certainly examples that are easy to produce that would seem to suggest that integral closure over the input ring A might be different from integral closure over some Noether normalization P. Consider $y^3x^4 + y^2 + x^3 = 0$ as defining a non-integral extension

$$A := \mathbf{F}[y, x]/\langle y^3x^4 + y^2 + x^3\rangle$$

of either $P := \mathbf{F}[x]$ or $P := \mathbf{F}[y]$. Clearly $(y/x)^2+y^3x^2+x = 0$ is an integral equation over A. But y isn't even integral over $\mathbf{F}[x]$, let alone y/x. But if $z := yx^4$, then the defining equation corresponds to $z^3+z^2+x^{11} = 0$,

integral over $\mathbf{F}[x]$. And $w := (z^2 + z)/x^5$ is integral over $\mathbf{F}[x]$, since it satisfies $w^2 + (z + 1)x = 0$ with z already integral over $\mathbf{F}[x]$.

But $w = y^2x^3 + y/x$ suggests that this should probably be considered as the element generating the integral closure of A over A, rather than just using y/x. So maybe it is possible to at least make non-integral extensions into integral extensions before computing integral closures of them.

17.13 Other nagging questions

What is the import of giving a new variable name to a particular rational function? That is, in the example above why use $f_3 := f_5^2/f_7 = -(f_7^4 + f_7^3)/f_5^5$? My answer would have been to be able to replace $(f_7^4 + f_7^3)/f_5^5$ by $-f_3$. If one considers generators of the ideal of relations in the quotient ring of a presentation in terms of reduction rules $LT(b) \mapsto LT(B) - b$, then various monomial orderings given rise to different reduction rules. While we may have to put up with a polynomial form $f_7^4 \mapsto -f_5^5 f_3 - f_7^3$, it would seem to make no sense to settle for $f_3 f_5^5 \mapsto -f_7^4 - f_7^3$. Yet a default product monomial ordering seems to result in the latter. Of course so does any monomial ordering that leaves the relations in (a Gröbner basis for) the input unchanged (when the input is not already integrally closed).

Also why homogenize or homogenize with weights ever? The answer must be in terms of a projective mindset. But this is almost always antithetical to a true weighted ordering of the variables; Or it completely destroys the intended algebraic form of the integral closure, to produce some projective form of a curve or surface, which I clearly think is misguided, from a purely algebraic viewpoint. Perhaps it is a good geometric viewpoint, but that is usually accepted rather than motivated in books on algebraic geometry.

Chapter 18

Integral closure of ideals

Definition 53. *Let I be an ideal of an integrally closed (quotient) ring $A := R/J$. An element $y \in A$ is integral over I iff if it is the root of a monic polynomial*

$$f(T) := 1T^d + a_1T^{d-1} + \cdots + a_{d-1}T^1 + a_dT^0,$$

for some positive integer d, with $a_j \in I^j$ for $1 \leq j \leq d$. The integral closure (of I in A) is the set of all elements of $Q(A)$ integral over I.

The theory to get this idea started should first be that this closure $C(I, A)$ is again an ideal. If it is clear that $C(I, A)C(I^j, A) \subseteq C(I^{j+1}, A)$ for all j, then is there a (smallest) j for which equality holds. That could lead to algorithms for computing $C(I^j, A)$ for all j.

18.1 Rees algebras

Definition 54. *Let $I := \langle g_1, \ldots, g_s \rangle$ be an ideal in an integrally closed (quotient) ring $A := R/J$. Let $A[It] := \sum_j I^j t^j$ be the formal generating function for the powers of I^j (with $I^0 := A$). Let $\phi : A[G_1, \ldots, G_s] \to A[t]$ be defined by extending $\phi(G_i) := g_i t$ for $1 \leq i \leq s$. Then (a presentation for) the Rees algebra of I is $A[G_1, \ldots, G_s]/kernel(\phi)$.*

It would be nice if the integral closure of the Rees algebra as a ring were related to the integral closures of the powers of I. Indeed,

Theorem 55. *The integral closure of $A[It]$ is $\sum_j C(I^j, A)t^j$.*

Consider a simple example such as $I := \langle x_2^2, x_2x_1, x_1^3 \rangle \in A := R := P := \mathbf{Q}[x_2, x_1]$. Consider the presentation of the Rees algebra

$$Rees(I) = A[G_3, G_2, G_1]/\langle G_2x_1^2 - G_1x_2, G_3x_1 - G_2x_2, G_2^2x_1 - G_3G_1, G_2^3x_2 - G_3^2G_1 \rangle.$$

With the map ϕ external to the presentation, an element of I^j corresponds to several elements of $Rees(I)$. For instance the element $x_2^3x_1^3$ corresponds to $\phi(x_2^3x_1^3) = x_2^3x_1^3t^0 \in I^0t^0$, $\phi(G_3x_2x_1^3) = \phi(G_2x_2^2x_1^2) = \phi(G_1x_2^3) = x_2^3x_1^3t^1 \in I^1t^1$, $\phi(G_3G_2x_1^2) = \phi(G_2^2x_2x_1) = \phi(G_3G_1x_2) = x_2^3x_1^3t^2 \in I^2t^2$, and $\phi(G_2^3) = x_2^3x_1^3t^3 \in I^3t^3$, since $x_2^3x_1^3$ is in I^j for all $j \leq 3$. While the elements of $ker(\phi)$, homogeneous in the G_i, can be used to reduce the above to a canonical copy for each j, the copies with different j are necessarily not identified, in order

that the j-th level of $Rees(I)$ be $I^j t^j$, making this algebra a formal generating function for the sequence $(I^j \ : \ 0 \leq j)$.

Instead consider an ideal

$$rees_0(I) := \langle g_i - G_i t^{-1} \ : \ 1 \leq i \leq s \rangle \in A[G_s, \ldots, G_1][t^{-1}]$$

in which the map ϕ is internal, since it is defined by the generators. [The use of t^{-1} instead of t is supposed to suggest a local monomial ordering (8) in which $1 \succ t^{-1} \succ \cdots$, as opposed to a grading; but in either case t or t^{-1} could be supressed if elements are implicitly ordered or graded appropriately.] Then the element $x_2^3 x_1^3$ above doesn't need to correspond to one element for each j for which $x_2^3 x_1^3 \in I^j$; it suffices to have only one, here $NormalForm(x_2^3 x_1^3, rees_0(I)) = G_2^3 t^{-3}$.

Definition 56. *Given an ideal $I := \langle g_i \ : \ 1 \leq i \leq s \rangle \in A$, recursively define $rees_j(I)$, starting with $rees_0(I) := \langle g_i - G_i t^{-1}, \ : \ 1 \leq i \leq s \rangle$ as follows. If $\{g_l \in C(I^{j-1}) \ : \ l \in L(j)\}$ is a generating set for those elements of $C(I^j)$ not already in the product $C(I^{j-1})C(I)$, then*

$$rees_j(I) := rees_{j-1}(I) + \langle g_l t^{1-j} - G_l t^{-j} \ : \ l \in L(j) \rangle.$$

Then $rees(I)$ is the (finite) union of the $rees_j(I)$, $j \geq 0$.

Then each element of the ring $z \in A$ will have $NormalForm(z, rees(I))$ of the form rt^{-m}, meaning that $z \in C(I^j)$ for all $j \leq m$, rather than having one image $r_j t^{-j}$ for each such $j \leq m$.

That means in particular that if $C(I^l)$ for all $l \leq j$ are desired, it is possible to compute $rees_j(I)$ instead of all of $rees(I)$, unlike the standard method which requires all of the integral closure $C(Rees(I), Q(Rees(I))$ of the ring $Rees(I)$ be computed. And if only $C(I^j)$ is required for a single j, then it is possible to compute $rees_1(I^j)$ directly. [Note also that while Rees algebras have the appealing theoretical property that $C(Rees(I)) = \sum_j C(I^j) t^{-j}$ (a generating function for the sequence $C(I^j)$), $rees(I)$ has the following advantage, as noted in the examples above and reiterated in the final example below.]

Theorem 57. *For $f \in A$, $f \in C(I^j)$ iff t^{-j} divides $NormalForm(f, rees_j(I))$.*

Proof : If $f \in A$ can be reduced to $NormalForm(f, rees_j(I)) = rt^{-j}$ for some $r \in A[G_1, \ldots, G_s]$. Then $f \in C(I^l)$ for any $l \leq j$.

A simple example shows how much more complicated the presentation of the integral closure of the Rees algebra $C(Rees(I), Q(Rees(I))$ is than the proposed $rees(I)$. Try $I := \langle x_4, x_3, x_2, x_1 \rangle$ as an ideal of the quotient ring $A := \mathbf{F}[y_1; x_4, x_3, x_2, x_1]/\langle y_1^4 - x_4 x_3 x_2 x_1 \rangle$.

Even $Rees(I)$ has a presentation as $A[G_4, G_3, G_2, G_1]/\langle G_i x_j - G_j x_i \ : \ i < j \rangle$ while its integral closure is

$$A[G_5, G_4, G_3, G_2, G_1]/\langle G_i x_j - G_j x_i \ : \ 1 \leq i < j \leq 4, G_5 x_j - G_j y_1 \ : \ 1 \leq j \leq 4,$$

$$G_5 y_1^3 - G_4 x_3 x_2 x_1, \ G_5^2 y_1^2 - G_4 G_3 x_2 x_1, \ G_5^3 y_1 - G_4 G_3 G_2 x_1, \ G_5^4 - G_4 G_3 G_2 G_1 \rangle.$$

Compare this to

$$rees(I) = rees_1(I) = \langle y_1 - G_5 t^{-1}, \ x_j - G_j t^{-1}, \ 1 \leq j \leq 4, (G_5^4 - G_4 G_3 G_2 G_1) t^{-4} \rangle.$$

[Note that A, as an affine P-algebra, should really be written as $\mathbf{F}[y_3, y_2, y_1; x_4, x_3, x_2, x_1]/J$ with J having minimal, reduced Gröbner basis consisiting of $y_1^2 - y_2$, $y_2 y_1 - y_3$, $y_2^2 - x_4 x_3 x_2 x_1$, $y_3 y_1 - x_4 x_3 x_2 x_1$, $y_3 y_2 - y_1 x_4 x_3 x_2 x_1$, $y_3^2 - y_2 x_4 x_3 x_2 x_1$, assuming an appropriate monomial ordering.]

18.2 Local versus global example

Consider the simple example

$$I := \langle x_2^5 + x_2^2, x_1^5 + x_1^2 \rangle \in A = R = P := \mathbf{F}[x_2, x_1].$$

Is $C(I) = \langle x_2^5 + x_2^2,\ x_2^4x_1^4 + x_2^4x_1 + x_2x_1^4 + x_2x_1,\ x_1^5 + x_1^2 \rangle$ more closely related to the integral closure $C(\langle x_2^2, x_1^2 \rangle) = \langle x_2^2, x_2x_1, x_1^2 \rangle$, or the integral closure $C(\langle x_2^5, x_1^5 \rangle) = \langle x_2^5, x_2^4x_1, x_2^3x_1^2, x_2^2x_1^3, x_2x_1^4, x_1^5 \rangle$? Assuming the former is the obvious choice, then using a local monomial ordering gives $C(I) = \langle x_2^2(1 + x_2^3), x_2x_1(1 + x_2^3)(1 + x_1^3), x_1^2(1 + x_1^3) \rangle$. So it is better to write $I = \langle x^2u,\ y^2v \rangle$ and $C(I) = \langle x_2^2u,\ x_2x_1uv,\ x_1^2v \rangle$ with $u := 1 + x^3$ and $v := 1 + y^3$ being units. In this simple example, $rees(I)$ is generated by $x_2^2u - G_2t^{-1}$ and $x_1^2v - G_1t^{-1}$, with $(x_2x_1uv)^2 \mapsto G_2G_1uvt^{-2}$ showing that $x_2x_1uv \in C(I)$. So $rees(C(I))$ has additional relations $x_2x_1uv - G_3t^{-1}$, and $(G_3^2 - G_2G_1uv)t^{-2}$.