

MA4L7 Algebraic curves

Miles Reid

Part 4. Graded rings and proof of (I–III)

9 Introduction

9.1 Definitions of graded rings and graded modules

A graded ring (over k) is a commutative ring R with a 1, having a direct sum decomposition $R = \bigoplus_{n \geq 0} R_n$ with the assumptions

1. $R_0 = k$;
2. The ring multiplication takes $R_{n_1} \times R_{n_2} \rightarrow R_{n_1+n_2}$;
3. R is generated over k by finitely many elements $x_i \in R_{n_i}$, that are homogeneous of degree n_i .

The first cases you meet have all the generators in degree 1: the homogeneous coordinate ring $k[x_{0\dots n}]$ of \mathbb{P}^n or $k[X]_{\text{homog}} = k[x_{0\dots n}]/I_X$ of a projective subvariety $X \subset \mathbb{P}^n$. Since our current treatment works with irreducible varieties, we almost always assume that R is an integral domain.

Another common case that we have already seen many times is the sections ring $R(C, D)$ associated to a hyperelliptic curve C and its hyperelliptic divisor D that is a linear system g_2^1 . In this case the graded ring is

$$k[x_1, x_2, z]/(z^2 - f_{2g+2}(x_1, x_2))$$

where $\deg z = g+1$. This means that for $a = 0, \dots, g$, the $a+1$ homogeneous monomials $S^a(x_1, x_2)$ base $\mathcal{L}(C, aD)$; we need one further generator z in degree $g+1$ that satisfies a relation in degree $2g+2$ that (in characteristic $\neq 2$) we take to be $z^2 - f_{2g+2}(x_1, x_2)$. Then for every $a \geq g+1$, the RR space $\mathcal{L}(C, aD)$ is based by $S^a(x_1, x_2)$ and $S^{a-g-1}(x_1, x_2)z$. (Check that this gives $a+1 + a - g = 1 - g + 2a$, in accordance with RR for a regular divisor.)

A *graded module* M over a graded ring R , is an R -module with a direct sum decomposition $M = \bigoplus_{n \in \mathbb{Z}} M_n$ satisfying the assumptions

1. $R_n \neq 0$ only for $n \geq -c$ (for some c);
2. The ring action takes $R_{n_1} \times M_{n_2} \rightarrow M_{n_1+n_2}$;
3. M is generated over k by finitely many elements $m_i \in M_{n_i}$ that are homogeneous of degree n_i .

9.2 Sections ring $R(C, D)$

The general case that I use most commonly is the *sections ring*

$$R(C, D) = \bigoplus_{n \geq 0} \mathcal{L}(C, nD)$$

corresponding to a free linear system $|D|$ on a curve C . The *free* assumption is that $\mathcal{L}(C, D)$ (in degree 1) has two sections s_1, s_2 defining effective divisors $D_1 = \text{div } s_1 + D$ and $D_2 = \text{div } s_2 + D$ with disjoint support (as in the Castelnuovo free pencil trick).

Remark 9.1 Since we are mostly only interested in the ratio $s_1 : s_2$, I sometimes have in mind that $s_2 = 1 \in k(C)$, so that $D = D_2 > 0$ and s_2 corresponds to $1 \in \mathcal{L}(C, D)$ or to the natural inclusion $s_2 : \mathcal{O}_C \hookrightarrow \mathcal{O}_C(D)$; however, even if I do this, I still insist that $s_2 \in R_1$ is an element of degree 1 (as opposed to the unit element $1 \in R_0$).

A free linear system comes about automatically from any nonconstant rational function $f \in k(C)$ or its morphism $\varphi : C \rightarrow \mathbb{P}^1$, with $D_1 = \varphi^{-1}(0)$ the divisor of zeros and $D_2 = \varphi^{-1}(\infty)$ the poles of $x = s_1/s_2$.

My main trick is to set $S = k[s_1, s_2]$ for the homogeneous coordinate ring of \mathbb{P}^1 , and view $R(C, D)$ as a module over S .

9.3 Simplest application

Let $C_a \subset \mathbb{P}^2$ be a nonsingular curve of degree a . Assume that the coordinate points $(0, 0, 1) \notin C_a$, and choose coordinates (x_1, x_2, z) on \mathbb{P}^2 . Then the equation of C_a is monic in z , of the form

$$F_a = z^a + \sum_{i=1}^a c_{a-i}(x_1, x_2)z^i,$$

with $c_{a-i} \in S_{a-i}$. The homogeneous coordinate ring of C_a is of course simply $k[C_a]_{\text{homog}} = k[x_1, x_2, z]/(F_a)$.

Now as a module over $S = k[x_1, x_2]$, it is the free graded module based by $1, z, z^2, \dots, z^{a-1}$. I write

$$\begin{aligned} k[C_a]_{\text{homog}} &= S \oplus S(-1) \oplus \cdots \oplus S(-(a-1)) \\ &= \bigoplus_{i=1}^a S(-a_i). \end{aligned} \tag{9.1}$$

Here $a_i = i - 1$, and $S(-i) = S \cdot z^i$ is a copy of S as a module over itself, but with basis z^i in degree i . The homogeneous part of $S(-i)$ in degree d is thus the vector space $k[x_1, x_2]_{d-i}$ (based by the monomials $S^{d-i}(x_1, x_2)$).

I make the convention that $S^{d-i}(x_1, x_2) = \emptyset$ if $d < i$, and count them as $\#S^{d-i}(x_1, x_2) = [d - i + 1]_+$, where $[n]_+ = n$ or 0 if $n < 0$.

The degree d part of $k[C_a]_{\text{homog}}$ is thus

$$\sum_{i=0}^{a-1} S^{d-i}(x_1, x_2) \quad \text{of dimension} \quad \sum_{i=0}^{a-1} [d - i + 1]_+,$$

This gives the precise result for $\mathcal{L}(C_a, dH)$ (where H is the hyperplane section, say $x_2 = 0$).

$$l(C, dH) = \begin{cases} \binom{d+2}{2} & \text{if } d < a \\ 1 - g + da & \text{if } d \geq a - 2 \end{cases}$$

Here $g = \binom{a-1}{2} = l((a-3)H)$. In the cases $d = a-2, a-1$ both formulas are valid, and coincide.

9.4 Proof of (I)

(I) is the statement that $\deg \text{div } x = 0$ for every $x \in k(C)$. The proof uses easy material on modules over a DVR.

Recall that $C = C_x \cup C_y$, where for any $x \in k(C)$, the affine curve C_x has affine coordinate ring $A_x = k[C_x]$ the integral closure of $k[x] \subset k(x)$ in the field extension $k(C)$, and C_y the analogous construction for $y = x^{-1}$. Each of C_x and C_y is normal, so nonsingular. The two constructions coincide on the overlap, over $k[x, x^{-1}]$.

Now A_x is a finite module over $k[x]$ by the main proposition on integral closure. Any point $P \in \mathbb{A}_x^1$ has the local ring $\mathcal{O}_{\mathbb{A}_x^1, P}$ which is a DVR, and I can localise A_x near P to give the module $A_{x,P} = A_x \otimes_{k[x]} \mathcal{O}_{\mathbb{A}^1, P}$.

Lemma 9.2 *Let A be a PID and M a finite A -module.*

Then M is isomorphic to a direct sum of torsion modules $A/(a_i)$ with $a_i \in A$ plus a free A -module A^r .

In particular, a torsion-free finite module over a DVR is free.

Proof Start from $M = A^n/N$, with A^n a free module corresponding to a set of generators $e_i \in M$, and N the submodule of relations. Then N is generated by a set of relations

$$\sum_{j=1}^n a_{ij} e_j = 0.$$

Now, since the coefficients belong to a PID, the matrix (a_{ij}) can be reduced by row and column operations to the form

$$\begin{pmatrix} \text{diag } a_i & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $M \cong \bigoplus A/(a_i) \oplus A^r$. Q.E.D.

Corollary 9.3 *The following numbers coincide:*

1. *The degree $d = [k(C) : k(x)]$ of the field extension $k(x) \subset k(C)$.*
2. *The rank of the free module $A_{x,P} = A_x \otimes_{k[x]} \mathcal{O}_{\mathbb{A}^1, P}$ over the DVR $\mathcal{O}_{\mathbb{A}^1_x, P}$ for any $P \in \mathbb{A}^1_x$.*
3. *The dimension over k of the quotient vector space $A_{x,P}/m_P A_{x,P}$ for any $P \in \mathbb{A}^1_x$.*
4. *The degree $\deg \text{div}(x - a_P)$ of the divisor of zeros of $x - a_P$ on C_x .*
5. *The same as (2-4) with x replaced by y .*

In particular, this proves that $\deg \text{div } x$ on C_x equals $\deg \text{div } y$ on C_y , which gives (I).

9.5 Proof of (II), coarse form

(II) is the statement that there exists a family $\{D_n\}$ of divisors on C with $\deg D_n \rightarrow \infty$ but $1 + \deg D_n - l(C, D_n)$ bounded. This section gives a coarse proof, with no attempt to give a sharp bound, that is, to say anything precise about the genus of C . A more precise version is given below, with equalities and a formula for $g(C)$.

Recall that I set A_x for the integral closure of $k[x]$ in $k(C)$. It is finite over $k[x]$ and, as a subring of $k(C)$, it contains a basis v_1, \dots, v_d of $k(C)$ over $k(x)$ (which is d -dimensional, as we just saw).

Where $x = \infty$ I made the same construction for $y = x^{-1}$ to get the remaining points of $C = C_x \cup C_y$. Each v_i is regular on C_x , so that its

divisor of poles lies over $y = 0$. It follows that there is some n_0 so that $y^{n_0}v_i \in A_y$ for $i = 1, \dots, d$.

Then $v_i \in \mathcal{L}(C, n_0D)$, where D is the divisor of zeros of y . Therefore for $n \geq n_0$, the vector space $\mathcal{L}(C, nD)$ contains the subspace $\bigoplus_{i=1}^d k[x]_{\leq n-n_0} \cdot v_i$, of dimension $d(n - n_0 + 1)$, whereas $\deg nD = nd$.

Now $1 + nd - d(n - n_0 + 1)$ is independent of n , which proves (II).

9.6 The sections ring $R(C, D)$ is a free S -module

Let S be a ring and M an S -module. A sequence s_1, s_2, \dots in S is a *regular sequence* for M if s_1 is a nonzerodivisor of M , then s_2 is a nonzerodivisor of M/s_1M and so on. In general, one requires each s_{i+1} a nonzero divisor of $M/(s_1, \dots, s_i)M$ for each i , but here I only need regular sequences of length 2. The rings and modules here are all graded, with s_1, s_2 of degree 1.

Let $R(C, D)$ and $s_1, s_2 \in \mathcal{L}(C, D)$ be as in 9.2, and set $S = k[s_1, s_2]$.

Proposition 9.4 (A) s_1, s_2 is a regular sequence for $R(C, D)$.

(B) The sections ring $R(C, D)$ is a free graded module over S , of the form

$$R(C, D) = \bigoplus S(-a_i) = S \oplus S(-a_2) \oplus \dots \oplus S(-a_d) \quad (9.2)$$

with $a_1 = 0 < a_2 \leq \dots \leq a_d$.

(C) For every $n \in \mathbb{Z}$, we have $l(C, nD) = \sum_{i=1}^d [n - a_i + 1]_+$. In particular, for every $n \geq a_d - 1$, this gives equality

$$l(nD) = \sum_{i=1}^d (n - a_i + 1) = 1 - g + \deg nD, \quad (9.3)$$

where

$$g = \sum_{i=1}^d [a_i - 1]_+ = \sum_{i=2}^d (a_i - 1). \quad (9.4)$$

(Including the -1 in the first summand would give $\sum_{i=1}^d (a_i - 1) = g - 1$.)

Proof of (A) The only multiplication involved in $S \times R(C, D) \rightarrow R(C, D)$ is multiplication in the function field $k(C)$, so it is clear that s_1 is a nonzerodivisor.

To say that s_2 is a nonzerodivisor modulo s_1 means any $f_2 \in R(C, D)_{n-1}$ that becomes a multiple of s_1 after multiplying by s_2 , was already a multiple of s_1 . That is, for $f_1, f_2 \in R(C, D)_{n-1}$,

$$s_2 f_2 = s_1 f_1 \implies f_2 = s_1 c \text{ for some } c \in R(C, D)_{n-2}.$$

We have already seen this argument in Part 3 in the form of the Castelnuovo free pencil trick.

Bearing in mind that we are dealing with elements of the field $k(C)$, I can simply define c by $c = f_1/s_2 = f_2/s_1 \in k(C)^\times$. I claim that c satisfies $\text{div } c + (n-2)D \geq 0$.

In fact, $cs_1 = f_2 \in \mathcal{L}((n-1)D)$ and $cs_2 = f_1 \in \mathcal{L}((n-1)D)$ are given. As usual, since s_1, s_2 define a free pencil in $|D|$, write $\text{div } s_1 + D = D_1$ and $\text{div } s_2 + D = D_2$, where D_1 and D_2 are effective divisors with disjoint support.

Then

$$\begin{aligned} \text{div}(cs_1) + (n-1)D &= \text{div } c + (n-2)D + D_1 \geq 0 \quad \text{and} \\ \text{div}(cs_2) + (n-1)D &= \text{div } c + (n-2)D + D_2 \geq 0. \end{aligned}$$

Now D_1 and D_2 have disjoint support, so it follows that $\text{div } c + (n-2)D \geq 0$ and $c \in \mathcal{L}(C, (n-2)D) = R(C, D)_{n-2}$. This proves (A).

The argument boils down to saying that the sequence

$$0 \rightarrow R(C, D)_{n-2} \rightarrow R(C, D)_{n-1} \oplus R(C, D)_{n-1} \rightarrow R(C, D)_n$$

is exact, where the first arrow is $c \mapsto s_2 c, s_1 c$ and the second is $f_1, f_2 \mapsto s_1 f_1 - s_2 f_2$. (This is *Koszul complex* of s_1, s_2 ; the sequence s_1, s_2 is regular if and only if its Koszul complex is exact.)

Proof of (B)

Lemma 9.5 *Set $S = k[s_1, s_2]$, and let M be a finite graded S -module for which s_1, s_2 is a regular sequence. Then M is a free graded S -module, that is, $M = \bigoplus S(-b_i)$ for some $b_i \in \mathbb{Z}$.*

Proof Write $\overline{M} = M/(s_1 M + s_2 M)$. Then \overline{M} is a graded vector space over k , say $\overline{M} = \bigoplus k \cdot \bar{e}_i$ with \bar{e}_i of degree b_i . Each basis element can be lifted to $e_i \in M$ of the same degree, and $M = \bigoplus e_i$.

Proof of (C) By (B), $R(C, D) = \bigoplus S(-a_i)$ for some a_i , that I write in increasing order. Now since $\mathcal{L}(C, 0D) = R_0 = k$, it follows that $a_1 = 0$ and $a_i \geq 1$. The formula for $l(nD)$ is a straightforward calculation.

9.7 A counterexample: Macaulay’s quartic curve $\Gamma_4 \subset \mathbb{P}^3$

The proof that s_1, s_2 is a regular sequence for the sections ring $R(C, D)$ uses the assumption that the homogeneous component R_n in each degree is the whole vector space $\mathcal{L}(C, nD)$.

The classic counterexample is Macaulay’s quartic curve Γ_4 , the image of the embedding $\mathbb{P}^1 \hookrightarrow \mathbb{P}_{\langle x, y, z, t \rangle}^3$ given by (u^4, u^3v, uv^3, v^4) . At each point of the image either $x \neq 0$ or $t \neq 0$, and on those affine opens y/x (respectively z/t) is a local parameter. The homogeneous coordinate ring $k[\Gamma_4]_{\text{homog}}$ is the complete linear system in every degree except 1: for example, you can see that the quadratic monomials in (u^4, u^3v, uv^3, v^4) include every monomial of degree 8.

However, the absent $w = u^2v^2$ means that $xw = y^2$ is an element of $k[\Gamma_4]_{\text{homog}}$, but not a multiple of x in it (that is, not an element of the ideal $(x) \subset k[\Gamma_4]_{\text{homog}}$). Hence the ideal of Γ_4 contains $x(tw) - t(xw)$ where $xw \notin (x)$. It follows that x is a zerodivisor modulo t , which contradicts regular sequence.

The defining equations of Γ_4 are

$$\begin{aligned} x^2z &= y^3, \\ xt = yz \quad \text{and} \quad xz^2 &= y^2t, \\ z^3 &= yt^2. \end{aligned} \tag{9.5}$$

Notice the “rolling factors” $x \mapsto z$ and $y \mapsto t$ in the three cubic equations. Rather than independent relations, they can be viewed as a single bihomogeneous equation of bidegree 3, 1 in the quadric surface $xt = yz$ (isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$), whereas the three equations on the right are cubics in \mathbb{P}^3 that contain Γ_4 plus copies of the lines $x = y = 0$ or $z = t = 0$ added to make a curve of bidegree 3, 3.

The fault is not with the embedded curve, but with its affine cone $k[\Gamma_4]_{\text{homog}}$, and specifically with its maximal ideal (x, y, z, t) . Write $\mathcal{C}\Gamma_4$ for the affine variety $\text{Spec}(k[\Gamma_4]_{\text{homog}})$, which is the affine cone in \mathbb{A}^4 over Γ_4 , defined by (9.5).

This cone is nonsingular outside the origin. Its bad property is that if we take the intersection of $\mathcal{C}\Gamma_4$ with any hyperplane through the origin, it automatically has an “extra nilpotent sticking out at zero” (or embedded prime in the sense of primary decomposition). The point is the missing ring element $w = u^2v^2$. Whereas w is not in the ring, each of its multiples $(x, y, z, t) \cdot w$ is: $xw = y^2$, $yw = xz$, etc. These elements are then torsion modulo any of x, y, z, t .

It is striking that one can calculate the dimension of $k[\Gamma_4]_{\text{homog}}/(x, t)$ (or $k[\Gamma_4]_{\text{homog}}/(l_1, l_2)$ for any general linear forms l_1, l_2 in x, y, z, t), and get the answer 5 (rather than the expected value $4 = \deg \Gamma_4$). See Ex. ?? for more on this.

9.8 The dual (or canonical) module \mathcal{K}

I use the above definitions and notation. The key construction that provides the canonical divisor K_C starts from the graded S -module

$$\begin{aligned}\mathcal{K} &= \text{Hom}_S(R(C, D), S(-2)) \\ &= S(-2) \oplus S(a_2 - 2) \oplus \cdots \oplus S(a_d - 2).\end{aligned}\tag{9.6}$$

The easy thing this does is provide nice numerical properties, relating exactly to what I want for K_C and the Riemann–Roch spaces $\mathcal{L}(K_C + nD)$ for $n \in \mathbb{Z}$. The specific result is as follows (compare with Proposition 9.4, (C)):

Proposition 9.6 *1. For every $n \in \mathbb{Z}$, the dimension of the degree n piece of \mathcal{K} is given by*

$$\dim \mathcal{K}_n = \sum_{i=1}^d [a_i + n - 1]_+.\tag{9.7}$$

2. In particular, for $n \geq 1$ every term is ≥ 0 , so this gives

$$\begin{aligned}\dim \mathcal{K}_n &= \sum_{i=1}^d (a_i + n - 1) = \sum_{i=1}^d (a_i - 1) + nd \\ &= g - 1 + \deg nD.\end{aligned}\tag{9.8}$$

(This agrees with $1 - g + \deg(K_C + nD)$ once I establish K_C .)

3. For $n \geq 0$ the first term in the sum is $[-2+1]_+ = 0$, and the remaining terms are all ≥ 0 , so

$$\dim \mathcal{K}_0 = \sum_{i=2}^d (a_i - 1) = g.\tag{9.9}$$

4. For every $n \in \mathbb{Z}$,

$$\begin{aligned}l(nD) - \dim \mathcal{K}_{-n} &= \sum_{i=1}^d [n - a_i + 1]_+ - \sum_{i=1}^d [a_i - n - 1]_+ \\ &= 1 - g + n \deg D.\end{aligned}\tag{9.10}$$

5. The difference of degrees between the free S -module \mathcal{K} of (9.6) and the free S -module $R(C, D)$ of (9.2) gives

$$\begin{aligned}\deg \mathcal{K} - \deg R(C, D) &= \sum (a_i - 2) - \sum (-a_i) \\ &= 2 \sum_{i=1}^d (a_i - 1) = 2g - 2.\end{aligned}\tag{9.11}$$

The proof is straightforward. For (4), note that in each term, either $n \geq a_i - 1$, in which case the first term is $n - a_i + 1$ and the second term is zero, or $n \leq a_i - 1$, in which case the first term is zero and the second term is again $n - a_i + 1$ (two minus signs cancel), so that in any case, the expression gives $\sum(n - a_i + 1)$.

9.9 The canonical module \mathcal{K} as an $R(C, D)$ -module

As defined in the preceding section, $\mathcal{K} = \text{Hom}_S(R(C, D), S(-2))$ is only a module over $S = k[s_1, s_2]$. This relates to \mathbb{P}^1 rather than to C . It can be turned into a module over the sections ring $R(C, D)$ by *premultiplication*.

In more detail, $f \in R(C, D)$ acts on $\text{Hom}_S(R(C, D), S(-2))$ taking the homomorphism φ to the new homomorphism $f \cdot \varphi$ given by

$$(f \cdot \varphi)(r) = \varphi(fr) \quad \text{for } r \in R(C, D).$$

Premultiplication is an important issue, that applies in any discussion of duality. It means first multiply by f , then apply the homomorphism φ .

Perhaps a more natural way to describe this action is to think of \mathcal{K} as the dual of the free S -module $R(C, D)$ (the little twist (-2) only modifies its graded structure). Namely, multiplication by f defines a homomorphism $\mu_f: R(C, D) \rightarrow R(C, D)$ of free S -modules. With the given basis $\{z_i\}$, this map is given as usual by a matrix $F = (m_{ij})$, with $fz_i = \sum m_{ij}z_j$.

The dual (or “adjoint”) map on the dual module $f^\vee: \mathcal{K} \rightarrow \mathcal{K}$ is then given simply by the transpose matrix. To spell it out, fix a basis element $t \in S(-2)$, and write $\{z_k^\vee\}$ for the basis of \mathcal{K} dual to $\{z_i\}$, so that the dual element is

$$z_k^\vee: z_j \mapsto \begin{cases} t & \text{if } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

The action of f on an element φ of the dual module \mathcal{K} is the composite of multiplication by f on $R(C, D)$ followed by applying φ to the product. Referring specifically to the dual basis element z_k^\vee , compose the multiplication given by $fz_i = \sum m_{ij}z_j$ with z_k^\vee , to get

$$(f \cdot z_k^\vee)(z_i) = z_k^\vee(fz_i) = z_k^\vee\left(\sum m_{ij}z_j\right) = m_{ik}t.$$

In other words, $f \cdot z_k^\vee$ takes $z_i \mapsto m_{ik}t$, and this is the element $\sum m_{ik}z_i^\vee$ of \mathcal{K} . Thus in the dual basis, f acts on \mathcal{K} by the transpose matrix tF .

9.10 The canonical divisor K_C and the canonical line bundle $\mathcal{O}_C(K_C)$

It follows from the above discussion that \mathcal{K} with its given structure of $R(C, D)$ module is torsion free: a matrix and its transpose have the same rank. Thus its localisation at any point of C is a locally free module of rank 1.

This defines the canonical line bundle $\mathcal{O}_C(K_C)$ over C and the canonical divisor class K_C .

Several issues around this still needs clarifying, but no time.