On the methods to construct UFD counterexamples to a cancellation problem

Stefan Maubach*

Radboud University Nijmegen
Toernooiveld 1, The Netherlands
s.maubach@math.ru.nl

April 24, 2007

Abstract

1 Introduction

This paper zooms in on what is essential in the example in the paper [3]. Let us repeat the example of this paper:

Define $R : \mathbb{C}[x,y,z] := \mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$, and let $A_{n,m} := R[u,v] = R[U,V]/(x^mU - y^nV - 1)$ where n,m are positive integers. Now it is shown in [3] that $A_{n,m}^{[1]} \cong A_{n',m'}^{[1]}$ for any positive integers n,m,n',m', while $A_{n,m} \cong A_{n',m'}$ implies that $\{n,m\} = \{n',m'\}$.

However, it seems like in this example, the ring R can be chosen much more freely. Let us, for now, write $A_{r,s} := R[U,V]/(rU - sV - 1)$ where $r,s \in R$. So we are looking for a ring R and elements r,s,r',s' in R such that (1) $A_{r,s} \not\cong A_{r',s'}$, while $A_{r,s}^{[1]} \cong A_{r's'}^{[1]}$, (2) $A_{r,s}$ and $A_{r's'}$ are $\mathbb{C}$-algebra UFDs of dimension 3.
It is not our goal to classify which rings R have elements r,s,r',s' having the above properties, but we want to discuss properties that enable us to give examples. These properties are mainly for the part of showing that $A_{r,s}$ is not isomorphic to $A_{r',s'}$, except 2.6.

*Funded by Veni-grant of council for the physical sciences, Netherlands Organisation for scientific research (NWO)

1.1 Notations

Notations: If R is a ring, then $R^{[n]}$ denotes the polynomial ring in n variables over R. We will use the letter k for a field of characteristic zero, and K for its algebraic closure. Denote by $\partial_X, \partial_Y, \ldots$ the derivative with respect to $X, Y, \ldots$. Very often, we will use small caps $x, y, z, \ldots$ for elements $X, Y, Z, \ldots$ modulo "something", where it is clear what "something" is.

2 Useful properties of the rings R and $A_{r,s}$

2.1 R must be a UFD, and $A_{r,s}$ must be a UFD.

It is perhaps not true that R *must* be a UFD to make $A_{r,s}$ into a UFD (which is what is needed), but it is very convenient. In order to prove that a ring is a UFD, it is sometimes necessary to compute the class field group (see [5]). The class field group tells one "how far" a ring is from being a UFD, as being a UFD is equivalent to the class group being trivial, for integrally closed noetherian rings. It is not always an easy task to do that, however. We will quote a few useful tools:

Theorem 2.1. *(Corollary 10.3 of [5]) Let $A = A_0 + A_1 + \ldots$ be a graded noetherian Krull domain such that A_0 is a field. Let $\mathfrak{m} = A_1 + A_2 + \ldots$. Then $Cl(A) \cong Cl(A_{\mathfrak{m}})$, where Cl is the class group.*

Theorem 2.2. *([6]) A local noetherian ring $(A, \mathfrak{m})$ with characteristic $A/\mathfrak{m} = 0$ and an isolated singularity is a UFD if its depth is ≥ 3 and the embedding codimension is $\leq dim(A) - 3$.*

The latter two theorems can be used to show that the hypersurface $X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n}$ is factorial if $n \geq 5$ and any $d_i \in \mathbb{N}^*$ (see for example [4] for a proof). However, theorem 2.2 is not that useful here, if one wants to have a 2-dimensional UFD.

One of the more straightforward tools is

Theorem 2.3. *(Nagata) Let A be a domain, and let $x \in A$ be a prime element. If $A[x^{-1}]$ is a UFD, then A is a UFD.*

This is especially useful in showing that $A_{r,s}$ is a UFD, depending on what r and s are.

Lemma 2.4. *Let r or s be a prime element in R, assume R is a noetherian UFD, and assume r and s share no common factor. Then $A_{r,s}$ is a UFD.*

Proof. Write $r = r_1 r_2 \ldots r_k$ where the r_i are irreducible (which can be done since R is noetherian) and prime (which follows since R is a UFD). We will proceed by induction to k. If $k = 0$ then r is invertible and $A_{r,s} \cong R[V]$.

Now r_k is prime in $A_{r,s}$, since $A_{r,s}/(r_k) \cong R[U,V]/(r_k, -sV-1) = (R/r_k)[1/(s \mod r_k)]$ which is a domain. $A_{r,s}[r_k^{-1}] = R[r_k^{-1}][U,V]/(rU - sV - 1)$, which is a UFD by induction (as $r \in R[r_k^{-1}]$ has fewer irreducible factors) and Nagata's theorem. □

2.2 $R^* = A^*$

This also implies that r and s do not share a common factor other than a unit, as this common factor will become invertible in $A_{r,s}$.

2.3 R is rigid, $ML(A_{r,s}) = R$

R being rigid is defined as $\mathrm{LND}(R) = \{0\}$, i.e. there are no nontrivial G_a-actions on the variety associated to R. An equivalent definition is that the Makar-Limanov invariant is maximal, i.e.$ML(R) = R$. This is again not a required property, but it is very useful in making sure that $A_{r,s}$ has few automorphisms. The point being, that we will want to distinguish $A_{r,s}$ and $A_{r',s'}$ later on by computing their automorphism groups. Also, this will automatically take care of the next requirement.

In order to make a rigid ring, we bump into a strange phenomenon. It seems like "almost any" ring is rigid, but it is in general hard to prove that a ring is rigid. Note also that, through this difficulty, it is very dangerous to make statements as "almost any" ring is rigid, as it is hard to prove any such statement. On a side note, no examples are known of rigid rings R for which $ML(R^{[n]}) \neq ML(R)$, we refer to [1, 2] for comments on this difficult problem ("losing rigidity"). This is connected with the additional requirement that $ML(A_{r,s}) = R$: we have an extension A of the rigid ring R, and in general, $ML(A)$ can be anything: equal to R, strictly containing R (like being rigid itself), and we even cannot exclude $ML(A)$ being strictly contained in R. Note that, in this case, we do have $ML(A_{r,s}) \subseteq R$ as $s\partial_u + r\partial_v \in LND(A_{r,s})$, which has kernel R as can be easily checked.

There are a few ways of constructing and proving that a ring is rigid. A very useful lemma is the following (lemma 2.2 in [4]):

Lemma 2.5. *Let D be a nonzero locally nilpotent derivation on a domain A containing $\mathbb{Q}$. Then A embeds into $K[S]$ where K is some algebraically closed field of characteristic zero, in such a way that $D = \partial_S$ on $K[S]$.*

For example: one has a domain $R := \mathbb{C}^{[n]}/(F)$ where $F \in \mathbb{C}^{[n]}$. If there exists some nontrivial $D \in \mathrm{LND}(R)$, then we can see the elements and also variables of R as elements in $K[S]$. So, $F = 0$, but also $0 = \partial_S(F) = \sum(\partial_S X_i(S))\frac{\partial F}{\partial X_i}$. These two equations can yield that each $X_i(S)$ is constant in S. If that is the case, then D is the zero map, and one has a contradiction. This is exploited in both [3] and [4], using (an extension of) Mason's Theorem.

Incidentally, one can also use this method to restrict the amount of LNDs which exist on a ring. See [4] and [7].

2.4 R must be a characteristic subring of $A_{r,s}$

A characteristic subring is a subring which stays invariant under all automorphisms. If $ML(A_{r,s}) = R$, then $A_{r,s}$ will automatically have this property:

Lemma 2.6. *The Makar-Limanov invariant of a ring B is a characteristic subring of B.*

For a proof, see for example [3] lemma 4. This does imply that

Corollary 2.7. *Any $\varphi \in Aut_{\mathbb{C}}(A_{r,s})$ satisfies $\varphi(R) = R$.*

Lemma 2.8. $\mathrm{LND}(A_{r,s}) = RE$ *where* $E = s\partial_u + r\partial_v$.

Proof. Since $ML(A_{r,s}) = R$, any $D \in \mathrm{LND}(A_{r,s})$ will satisfy $D(r) = D(s) = 0$. Therefore, $0 = D(ru - sv - 1)$ implies $rD(u) = sD(v)$. Now here it is handy if one knows $A_{r,s}$ to be a UFD (otherwise the following may still be true, but much more complicated) as we can conclude that $D(u) = st, D(v) = rt$ for some $t \in A_{r,s}$ (since r, s share no common factor). So $D = tE$, and now we can use the well-known result that if $fD \in LND(B)$ for some ring B, then $D \in LND(B)$ and $D(f) = 0$. This implies $D \in RE$. □

2.5 The restriction $\mathcal{F} : Aut_{\mathbb{C}}(A_{r,s}) \longrightarrow Aut_{\mathbb{C}}(R)$ must be surjective

Note that this restriction $\mathcal{F}$ exists because of corollary 2.7. What we require here is surjectivity. This property moves the problem to determining $Aut_R(A_{r,s})$.

2.6 (r, s) is a height 2 ideal of R

We will need in lemma 3.2 that $(r, s) \neq R$, which is implied by this requirement, but we mainly need this requirement for the following:

Lemma 2.9. *If $rad(r, s) = rad(r', s')$ then $A_{r,s}^{[1]} \cong A_{r',s'}^{[1]}$.*

Proof. Let us write $X_{r,s}$ for the variety associated to $A_{r,s}$. We have a G_a-action on $A_{r,s}$ (associated to $s\partial_u + r\partial_v$).

Since the Ga action is locally trivial (in fact the basic open subsets $\mathcal{D}_X(r)$ and $\mathcal{D}_X(s)$ cover $X_{r,s}$ and satisfy $\mathcal{D}_X(s) = \mathcal{D}_{\operatorname{spec} R}(s) \times \mathbb{C}$, $\mathcal{D}_X(r) = \mathcal{D}_{\operatorname{spec} R}(r) \times \mathbb{C}$). Therefore $X_{r,s}$ is the total space of an algebraic principal Ga bundle over $\operatorname{spec}(R)\backslash\mathcal{V}$ where $\mathcal{V}$ is the set of all prime ideals containing (r, s). The same for $X_{r',s'}$. Now we can take their fiber product over the base: $X_{r,s} \times_{R\backslash\mathcal{V}} X_{r',s'}$. By standard arguments, this is isomorphic to $X_{r,s} \times \mathbb{C}$ as well as $X_{r',s'} \times \mathbb{C}$. So $A_{r,s}^{[1]} = \mathcal{O}(X_{r,s} \times \mathbb{C}) = \mathcal{O}(X_{r',s'} \times \mathbb{C}) = A_{r',s'}^{[1]}$. □

3 The R- automorphism group of $A_{s,t}$

If one has $R, A_{r,s}$ satisfying everything in the previous section, then there are some things which come for free. To be more precise, $Aut_R(A_{r,s})$ can be described, and we can give a simple requirement such that $A_{r,s} \ncong A_{r',s'}$.

Lemma 3.1. *Let $\varphi \in Aut_{\mathbb{C}}(A_{r,s})$. Then $\varphi^{-1}E\varphi = \lambda E$ where $\lambda \in R^*$.*

Proof. $\varphi^{-1}(LND(A_{r,s}))\varphi = \text{LND}(A_{r,s})$, as can be easily proved since conjugating an LND yields another LND (showing $\subseteq$), and conjugating with φ^{-1} gives $\supseteq$. Therefore, $RE = R(\varphi^{-1}E\varphi)$ and the result follows. □

Lemma 3.2. *$\varphi \in Aut_R A_{n,m}$ if and only if φ is an R-homomorphism satisfying $\varphi(u, v) = (ts + u, tr + v) = exp(tE)$ for some $t \in R$. Consequently, $Aut_R A_{n,m} \cong < R, + >$ as groups.*

Proof. We know by corollary 3.1 that $\varphi^{-1}(E)\varphi = \lambda E$ for some $\lambda \in R^*$. Define $(F, G) := \varphi(u, v)$. Also, $\varphi|_R = Id.$. So now

$$\begin{aligned}
(\lambda s, \lambda r) &= \varphi(\lambda s, \lambda r) \\
&= \varphi\lambda E(u, v) \\
&= \varphi(\varphi^{-1}E\varphi)(u, v) \\
&= E(F, G) \\
&= (sF_u + rF_v, sG_u + rG_v)
\end{aligned}$$

where the subscript denotes partial derivative.

Let us consider the first equation,

$$\lambda s = sF_u + rF_v.$$

Defining $H := F - \lambda u$, we see that $-sH_u = rH_v$. By the following lemma 3.3 we see that $H = p \in R$, so

$$F = p + \lambda u.$$

The second equation yields $\lambda r = sG_u + rG_v$. Defining $H := G - \lambda v$, yields $-rH_v = sH_u$, which by the following lemma 3.3 yields $H = q \in R$ and thus $G = q + \lambda v$. Now

$$\begin{aligned}
0 &= \varphi(ru - sv - 1) \\
&= r\varphi(u) - s\varphi(v) - 1 \\
&= rF - sG - 1 \\
&= r(p + \lambda u) - s(q + \lambda v) - 1 \\
&= rp - sq + \lambda(ru - sv) - 1 \\
&= rp - sq + \lambda - 1.
\end{aligned}$$

Now due to 2.6, $1 - \lambda = rp - sq$ are in a maximal ideal, hence $\lambda = 1$. Therefore, $rp = sq$, and since r and s share no common factor, and R is a UFD, we get that $p = st$ and $q = rt$ for some $t \in R$. Thus any automorphism must have the given form. It is not difficult to check that maps of this form are well-defined homomorphisms which are automorphisms. □

Lemma 3.3. *If $H \in A_{r,s}$ such that $-sH_u = rH_v$, then $H \in R$.*

Proof. We can find polynomials $p_i(v) \in R[v]$ such that $H = \sum_{i=0}^{d} p_i u^i$ for some $d \in \mathbb{N}$. Requiring that r does not divide coefficients of $p_i(v)$ if $i \geq 1$ (which we can do as $ru = sv + 1$) we force the p_i to be unique. The equation $-y^n H_u = x^m H_v$ yields

$$\sum_{i=0}^{d-1} -(i+1)sp_{i+1}u^i = \sum_{i=0}^{d} rp_{i,v}u^i$$

where $p_{i,v} \equiv \frac{\partial p_i}{\partial v}$. Substitute $sv + 1$ for ru to obtain a unique representation:

$$\textstyle\sum_{i=0}^{d-1} -(i+1)sp_{i+1}u^i = \quad rp_{0,v} + \sum_{i=0}^{d-1}(sv+1)p_{i+1,v}u^i,$$

so

$$-sp_1 = \quad rp_{0,v} + (sv+1)p_{1,v}$$

and

$$-(i+1)sp_{i+1} = \quad (sv+1)p_{i+1,v}$$

for each $i \geq 1$.

Let $i \geq 1$ and assume that p_{i+1} has degree k with respect to v. Let $\alpha \in R$ be the top coefficient of p_{i+1}, seen as a polynomial in v. Then $-(i+1)s\alpha = sk\alpha$, but that gives a contradiction. So for each $i \geq 1 : p_{i+1} = 0$. This leaves the equation $0 = rp_{0,v}$ which means that $p_0 \in R$. Thus $H = p_0 u^0 \in R$. □

Theorem 3.4. *Let R, $A_{r,s}$, $A_{r',s'}$ satisfy the requirements of the previous section. Suppose that $r's \neq rs'$. Then $A_{r,s} \not\cong A_{r',s'}$.*

Proof. Let $\Phi : A_{r,s} \longrightarrow A_{r',s'}$ be an automorphism. Since $\Phi(ML(A_{r,s}) = ML(A_{r',s'})$ we know that $\Phi(R) = R$. Since any automorphism of R is the restriction of an automorphism of $A_{r',s'}$ by 2.5 (this is exactly the spot where we use this requirement), we can compose Φ by an appropriate automorphism of $A_{r',s'}$, and can assume that Φ is the identity on R.

Now set $K := Q(R)$, the quotient field of R. Identify $K \otimes_R A_{r,s}$ with $K[v]$, $K \otimes_R A_{r',s'}$ with $K[v']$, and note that Φ can be extended to a K-isomorphism $K[v] \longrightarrow K[v']$. So we can assume that $\Phi(v) = \alpha v' + \beta$ where $\alpha \in K^*, \beta \in K$.

Of each ring $A_{r,s}$ and $A_{r',s'}$ we know the set of locally nilpotent derivations. Let $\mathrm{LND}(A_{r,s}) = RE$ and $\mathrm{LND}(A_{r',s'}) = RE'$, where $E(u) = s, E(v) = r, E'(u') = s', E'(v') = r'$. Since $\Phi^{-1}\,\mathrm{LND}(A_{r',s'})\Phi = \mathrm{LND}(A_{r,s})$, we must have $\Phi^{-1}E'\Phi = \lambda E$ where $\lambda \in A_{r,s}^* = R^*$.

A computation shows that

$$\lambda r = \lambda E(v) = \Phi^{-1}E'\Phi(v) = \alpha r'$$

and similarly $\lambda s = \alpha s'$. From this we deduce that there exist $t_1, t_2 \in R$ such that $t_1(r, s) = t_2(r', s')$. Since R is a UFD this implies that $(rs' = r's)$. □

4 Conclusions

Combining 2.9 and 3.4 it is possible to construct more examples which are UFD cancellation counterexamples. Of course, "the" cancellation problem, is still open:

Cancellation problem: If $A^{[1]} = \mathbb{C}^{[n]}$, then $A \cong \mathbb{C}^{[n-1]}$.

Now it would be very interesting if one can find a ring R and r, s such that $A_{r,s} \cong \mathbb{C}^{[n]}$. Then it may be possible to find $r', s' \in R$ such that $A_{r',s'} \ncong A_{r,s}$.

However, the author does not expect that such R, r, s exists.

References

[1] A. Crachiola, *On the AK-invariant of certain domains*, Ph-D. thesis, Wayne State University, may 2004.

[2] A. Crachiola and L. Makar-Limanov, *On the rigidity of small domains*, J. Algebra 284 (2005), no. 1, 1-12.

[3] D.Finston, S.Maubach, *The Automorphism Group of Certain Factorial Threefolds and a Cancellation Problem*, to appear in Isr.J.of Math.

[4] D.Finston, S.Maubach, *Constructing (almost) rigid rings and a UFD having infinitely generated Derksen and Makar-Limanov invariant*, preprint 2007.

[5] R. Fossum, *The Divisor Class Group of a Krull Domain*, Springer-Verlag 1973.

[6] R. Hartshorne and A. Ogus, *On the factoriality of local rings of small embedding codimension*, Comm. Algebra 1 (1974), 415–437.

[7] S. Maubach, *Infinitely generated Derksen and Makar-Limanov invariant*, preprint (2006).