BEZOUT DOMAINS AND ELLIPTIC CURVES

ISAAC GOLDBRING AND MARC MASDEU

Abstract. Let k be a fixed algebraic closure of $\mathbb{Q}$ and $k(t)^{\mathrm{ac}}$ a fixed algebraic closure of $k(t)$. Let $S \subseteq k[t] \setminus \{0\}$ be a multiplicative set. Let $A = S^{-1}(k[t])$ and $\widetilde{A}$ be the the integral closure of A in $k(t)^{\mathrm{ac}}$. We use elliptic curves to develop a necessary condition on S for $\widetilde{A}$ to be a Bezout domain. We give some examples of S which fail to satisfy this condition. As a consequence, we eliminate some candidates for a good Rumely domain of characteristic 0 with algebraic subring k.

1. Introduction

A *Bezout domain* is an integral domain such that any finitely generated ideal is principal. Clearly a noetherian Bezout domain is a PID. Examples of non-noetherian Bezout domains are the ring of algebraic integers (see van den Dries and Macintyre (1990) 2.4) and the ring of holomorphic functions on a noncompact Riemann surface (see Forster (1981), 26.5).

In van den Dries and Macintyre (1990), a first-order axiomatization of the theory of the ring of algebraic integers is described. (See Marker (2002) for background material on model theoretic notions mentioned in this paper.) Included in these axioms are the axioms for *good Rumely domains*. A good Rumely domain is a Bezout domain which is not a field and which satisfies certain other algebraic properties, among them that its fraction field is algebraically closed; see van den Dries and Macintyre (1990) for the precise definition of a good Rumely domain. We should remark that the fundamental property in the definition of a good Rumely domain is the so-called "glueing condition", which was inspired by Rumely's remarkable local-global principle for points with algebraic integer coordinates on varieties defined over the field of algebraic numbers; see Rumely (1986). Van den Dries and Macintyre prove that any two good Rumely domains of characteristic $p > 0$ are elementarily equivalent. In characteristic 0, the situation is more complicated.

For any domain R, let

$$\mathrm{alg}(R) := \{x \in R \mid x \text{ is algebraic over the prime ring of } R\}$$

be the *algebraic subring* of R. Van den Dries and Macintyre prove that two good Rumely domains R_1 and R_2 of characteristic 0 are elementarily equivalent if and only if $\mathrm{alg}(R_1)$ and $\mathrm{alg}(R_2)$ are isomorphic. Note that for a good Rumely domain R, $\mathrm{alg}(R)$ is isomorphic to a ring lying between $\widetilde{\mathbb{Z}}$ and $\mathbb{Q}^{\mathrm{ac}}$, where $\widetilde{\mathbb{Z}}$ is the ring of all algebraic integers and $\mathbb{Q}^{ac}$ is the field of algebraic numbers. Remarkably, it is proven in their paper that any ring lying between $\widetilde{\mathbb{Z}}$ and $\mathbb{Q}^{\mathrm{ac}}$ is of the form $\mathrm{alg}(R)$ for some good Rumely domain R of characteristic 0. This good Rumely domain is constructed as a certain ultraproduct of localizations of $\widetilde{\mathbb{Z}}$. In van den Dries and Macintyre (1990), they ask "What is a *natural* example of a good Rumely domain of characteristic 0 whose algebraic subring is $\mathbb{Q}^{\mathrm{ac}}$?"

Since Bezout domains are integrally closed in their fraction field, the first natural candidate for a good Rumely domain containing $\mathbb{Q}^{\mathrm{ac}}$ that they considered was the integral closure of $\mathbb{Q}^{\mathrm{ac}}[t]$ in the algebraic closure of $\mathbb{Q}^{\mathrm{ac}}(t)$. Van den Dries and Macintyre eliminate this possibility in Example 5.3 of their paper, where they use an argument involving elliptic curves to show that this ring is not a Bezout domain. There appeared to be much flexibility in their argument and van den Dries suggested that their argument could be modified to eliminate other candidates of transcendence degree 1. The goal of this paper is to develop a necessary condition for the integral closure of $S^{-1}(\mathbb{Q}^{\mathrm{ac}}[t])$ in the algebraic closure of $\mathbb{Q}^{\mathrm{ac}}(t)$ to be a Bezout domain, where $S \subseteq \mathbb{Q}^{\mathrm{ac}}[t] \setminus \{0\}$ is a saturated multiplicatively closed set. As a result, we eliminate further natural candidates for a good Rumely domain of characteristic 0 containing $\mathbb{Q}^{\mathrm{ac}}$.

In this paper, we make the following conventions. We let $k := \mathbb{Q}^{\mathrm{ac}}$ and $A := S^{-1}(k[t])$. We also let $\widetilde{A}$ denote the integral closure of A in the algebraic closure of $k(t)$. Since the case $S = \{1\}$ was eliminated in van den Dries and Macintyre (1990), we may assume $\{1\} \subsetneq S$. Since k is algebraically closed, S is generated by linear polynomials of the form $t - a$ for $a \in k$. We let $X := \{a \in k \mid t - a \in S\} \subseteq k$.

Throughout, n and m, sometimes with subscripts, range over $\mathbb{N}$ and l, sometimes with subscripts, ranges over $\mathbb{Z}$.

We would like to thank Lou van den Dries for many helpful discussions concerning this paper.

2. A Necessary Condition for $\widetilde{A}$ to be Bezout

In this section, we prove a theorem giving a necessary condition for $\widetilde{A}$ to be Bezout and give a few elementary examples for which this condition is not met. Our theorem rests on the following result.

Lemma 2.1. *Let B be an integrally closed domain with fraction field K. Let $\widetilde{B}$ be the integral closure of B in K^{ac}. Suppose $\widetilde{B}$ is a Bezout domain.*

Then for every finitely generated ideal I of B, there is an $n \geq 1$ such that I^n is prinicipal.

Proof. See van den Dries and Macintyre (1990), Proposition 5.2. □

Let $E \subseteq \mathbb{P}^2(k)$ be an elliptic curve defined over k by the affine equation $w^2 = t^3 + bt + c$, where $b, c \in k$. As usual, we have the point at infinity $O \in \mathbb{P}^2(k) \setminus \mathbb{A}^2(k)$, which serves as the identity element for the group law on E. Let $E' := E \setminus \{O\}$. For $P \in E'$, we let $t(P)$ denote its t-coordinate. We set

$$E_{\text{bad}} := \{P \in E' \mid t(P) \in X\}.$$

By $\langle E_{\text{bad}} \rangle$ we mean the subgroup of E generated by E_{bad}.

Theorem 2.2. *Suppose $\widetilde{A}$ is Bezout. Then for every $P \in E'$, there is an $n \geq 1$ such that $nP \in \langle E_{\text{bad}} \rangle$.*

Proof. The theorem is trivial if $P \in E_{\text{bad}}$, so we assume that $P \notin E_{\text{bad}}$. Let $C := k[t, w]/I(E')$ be the affine coordinate ring of E'. Identify $k[t]$ with a subring of C by viewing t as the function $P \mapsto t(P)$. For any $Q \in E' \setminus E_{\text{bad}}$, let

$$\mathfrak{m}_Q := \{\frac{g}{h} \in S^{-1}C \mid g(Q) = 0\}.$$

Note that $\mathfrak{m}_Q$ is a maximal ideal of $S^{-1}C$ for every $Q \in E' \setminus E_{\text{bad}}$.

Since the integral closure of $S^{-1}C$ in the algebraic closure of its fraction field is equal to $\widetilde{A}$, Lemma 2.1 implies that there is $n \geq 1$ such that $\mathfrak{m}_P^n$ is principal. Suppose $\mathfrak{m}_P^n = (S^{-1}C)u$. If $Q \in E' \setminus E_{\text{bad}}$ is such that $u \in \mathfrak{m}_Q$, then $\mathfrak{m}_P^n \subseteq \mathfrak{m}_Q$, implying that $\mathfrak{m}_P = \mathfrak{m}_Q$, whence $P = Q$. So the only zero of u on $E' \setminus E_{\text{bad}}$ is at P. Hence, there are $P_1, \ldots, P_m \in E_{\text{bad}}$ and $l_1, \ldots, l_m, l$ such that

$$\operatorname{div}(u) = n(P) + \sum_{i=1}^{m} l_i(P_i) + l(O).$$

Specializing, one gets that $nP \in \langle E_{\text{bad}} \rangle$. □

Since the contrapositive of the previous theorem is how we will find non-Bezout domains, we state it as a corollary.

Corollary 2.3. *Suppose there is an elliptic curve E and a point $P \in E'$ such that $nP \notin \langle E_{\text{bad}} \rangle$ for all $n \geq 1$. Then $\widetilde{A}$ is not Bezout.*

We finish this section with two simple examples illustrating our use of the preceding corollary. In both of our examples, we will need the fact that any elliptic curve E as above has infinite torsion-free rank; see van den Dries and Macintyre (1990), 5.5 for a proof of this fact.

Example 2.4. Let E be any elliptic curve as above and let E_{tor} be the torsion subgroup of E. If S is such that $X \subseteq \{t(P) : P \in E_{\text{tor}}\}$, then $\widetilde{A}$ is not Bezout. To see this, note that $\langle E_{\text{bad}} \rangle \leq E_{\text{tor}}$, and since E has infinite (in particular, positive) rank, there is $P \in E' \setminus E_{\text{tor}}$. Such a P satisfies the hypotheses of Corollary 2.3.

Example 2.5. Suppose S is finitely generated. Then $\widetilde{A}$ is not Bezout. To see this, take any elliptic curve E as above and let $P_1, \ldots, P_m \in E'$ be the distinct zeros of the generators of S on E'. Then $E_{\text{bad}} = \{P_1, \ldots, P_m\}$, and since E has infinite rank, there is a P as in Corollary 2.3.

3. The Number Field Example

The goal of this section if to prove the following result.

Theorem 3.1. *Let K be a number field. If $X \subseteq K$, then $\tilde{A}$ is not Bezout.*

Throughout this section, we fix a number field K. Define the field $\sqrt{K}$ to be the compositum of all the quadratic extensions of K. It is clear that for any elliptic curve E defined over k, $E_{\text{bad}} \subseteq E(\sqrt{K})$. In order to prove Theorem 3.1, it is enough, by Corollary 2.3, to find an elliptic curve E, defined over k, and a point $P \in E'$ such that, for all $n \geq 1$, $nP \notin E(\sqrt{K})$.

We will need the following very particular version of Hilbert's Irreducibility Theorem; see Serre (1992). Of course, we could omit the following lemma and just rely upon the aforementioned result, but in this way we keep things more elementary.

Lemma 3.2. *Let $F(t, w) = t^3 - w^2 + 1$ and let L be a number field containing K. Then there exists $w_0 \in K$ such that $F(t, w_0)$ is irreducible in $L[t]$.*

Proof. Let $\mathfrak{p}$ be a prime of K, unramified in L and not containing the rational prime 2. Choose any $z \in \mathfrak{p} \setminus \mathfrak{p}^2$ and set $w_0 := z - 1$. Then $w_0 + 1 \in \mathfrak{p}$ and $w_0 - 1 \notin \mathfrak{p}$ (for otherwise $\mathfrak{p}$ would divide 2). If the polynomial $t^3 - w_0^2 + 1$ were to have a root $t_0 \in L$, then taking $\mathfrak{P}$ any prime of L over $\mathfrak{p}$, we would have that $t_0^3 \in \mathfrak{P} \setminus \mathfrak{P}^2$, which is not possible because any prime dividing t_0^3 divides it at least to the third power. □

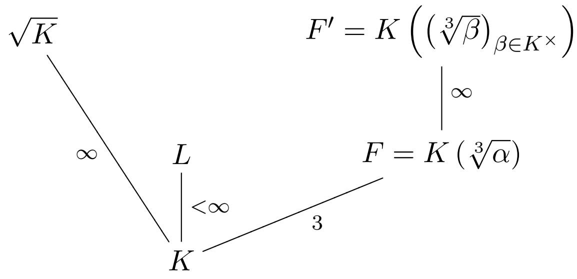
$\sqrt{K}$
$F' = K\left(\left(\sqrt[3]{\beta}\right)_{\beta\in K^\times}\right)$
∞
∞
L
$F = K\left(\sqrt[3]{\alpha}\right)$
$<\infty$
3
K

Figure 1. Fields appearing in the proof of Theorem 3.1

The following proposition is the key ingredient in the proof of Theorem 3.1.

Proposition 3.3. *There exists an elliptic curve E, defined over $\mathbb{Q}$, and a cubic extension F of K such that* $\operatorname{rk}(E(F)) > \operatorname{rk}(E(K))$.

Proof. Note first that, without loss of generality, we can assume that K contains the cube roots of unity. Let $F' = K\left(\{\sqrt[3]{\beta}\}_{\beta\in K^\times}\right)$ be the algebraic extension of K obtained by adjoining all the cube roots of elements in K.

Claim. *Let $\mathfrak{p}$ be any (finite) prime of K. Then there is some prime $\mathfrak{P}$ of F' dividing $\mathfrak{p}$ such that the residue field $\kappa(\mathfrak{P})$ corresponding to $\mathfrak{P}$ is finite.*

In order to prove the claim, consider the extension of completed fields $F'_{\mathfrak{P}}/K_{\mathfrak{p}}$ and the corresponding extension of residue fields $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. Let

$$K_1 := K_{\mathfrak{p}}(\{\sqrt[3]{\beta}\}_{\beta\in K_{\mathfrak{p}}^\times})$$

be the algebraic extension of $K_{\mathfrak{p}}$ obtained by adjoining all the cube roots of elements in $K_{\mathfrak{p}}$. There is a unique extension of the valuation given by $\mathfrak{p}$ to K_1. Also, as K_1 is a finite extension of $K_{\mathfrak{p}}$ (see Lang (1994), II Prop 3.6), it is complete with respect to this valuation. Clearly the field F' is contained in K_1 and the valuation induced by $\mathfrak{p}$ in K_1 restricts to a valuation $\mathfrak{P}$ of F'. The embedding $F'_{\mathfrak{P}} \hookrightarrow K_1$ induces an embedding of the corresponding residue fields. Since the residue field of $K_{\mathfrak{p}}$ is finite and K_1 is a finite extension of $K_{\mathfrak{p}}$, we know that the residue field of K_1 is finite, whence it follows that $\kappa(\mathfrak{P})$ is finite. This proves the claim.

Note that the residue field $\kappa(\mathfrak{P})$ is then finite for *any* prime $\mathfrak{P}$ of F' dividing $\mathfrak{p}$ as the extension F'/K is Galois, implying all primes above $\mathfrak{p}$ are conjugate.

Let $E \subseteq \mathbb{P}^2(k)$ be the elliptic curve defined by the affine equation $w^2 = t^3 + 1$. The claim readily implies that $E(F')$ has finite torsion. In fact, as proven in Silverman (1986) VII Prop 3.1, for any prime $\mathfrak{P}$ of F', prime-to-$\mathfrak{P}$ torsion injects in $E(\kappa(\mathfrak{P}))$, which is finite by the claim. Let r_0 be the exponent of $E(F')_{\mathrm{tor}}$ (i.e. if $P \in E(F')$ is torsion, then $r_0 P = O$) and let $r := \mathrm{lcm}(r_0, 3)$. Consider the extension $L := K([r]^{-1}E(K))$, that is L is the extension obtained by adjoining to K the coordinates of all the points $Q \in E$ such that $rQ \in E(K)$. By Silverman (1986) VIII Prop 1.5, $[L : K] < \infty$.

By Lemma 3.2, there exists some $w_0 \in K$ such that $\sqrt[3]{w_0^2 - 1} \notin L$. Let $\alpha := w_0^2 - 1$ and define $F := K(\sqrt[3]{\alpha})$. Note that F/K is a Galois extension and $F \cap L = K$ since $[F : K] = 3$ is prime and $\sqrt[3]{\alpha} \notin L$. Note also that $P := (\sqrt[3]{\alpha}, w_0) \in E(F) \setminus E(K)$.

There is a natural map induced by the embedding of K in F:

$$e : E(K)/pE(K) \longrightarrow E(F)/pE(F) \tag{1}$$

It is injective for any prime p different from 3. In fact, from the kernel-cokernel exact sequence associated to the Kummer maps for $E(K)$ and $E(F)$ (see Silverman (1986) VIII.2), $\ker(e)$ is a subgroup of $H^1(\mathrm{Gal}(F/K), E[p])$, which is trivial because $\#E[p] = p^2$ while $\#\,\mathrm{Gal}(F/K) = 3$.

Suppose, towards a contradiction, that $nP \in E(K)$ for some $n \geq 1$. After replacing P by a suitable multiple, we may assume that $n = p$ is prime. By how L has been constructed, we know that $p \neq 3$ and P is not torsion. Moreover, by the embedding in (1), since pP becomes divisible by p in F, it becomes divisible by p in K. Choose $Q \in E(K)$ such that $pP = pQ$. Then $P - Q \in E_{\mathrm{tor}} \cap E(F) \subseteq E_{\mathrm{tor}} \cap E(F') \subseteq E(L)$. Since $Q \in E(K) \subseteq E(L)$, we conclude that $P \in E(F) \cap E(L) = E(K)$, a contradiction.

We have thus proven that for all $n \geq 1$, $nP \notin E(K)$. This implies that $\mathrm{rk}\,(E(F)) > \mathrm{rk}\,(E(K))$, as desired. □

Corollary 3.4. *There exists a number field F, an elliptic curve E, defined over $\mathbb{Q}$, and $P \in E(F)$ such that $nP \notin E(\sqrt{K})$ for all $n \geq 1$.*

Proof. Choose E and F as in the previous proposition and choose $P \in E(F)$ independent of $E(K)$. If $nP \in E(\sqrt{K})$, then $nP \in E(\sqrt{K}) \cap E(F) = E(K)$, contradicting the choice of P. □

Note that the preceding corollary immediately proves Theorem 3.1.

4. Questions

We conclude this paper with several questions that we were unable to answer concerning further examples of our method as well as refinements of the method.

Question 1. *If $X \subseteq \mathbb{R}^{\mathrm{alg}} := k \cap \mathbb{R}$, is $\widetilde{A}$ Bezout?* We were able to prove the following partial result.

Proposition 4.1. *There is an elliptic curve E, defined over $\mathbb{Q}$, and a point $P \in E'$ such that $nP \notin E_{\mathrm{bad}}$ for all $n \geq 1$.*

Proof. (Sketch) Let Γ be the lattice $\mathbb{Z} + \mathbb{Z}i$. Let $g_2(\Gamma)$ and $g_3(\Gamma)$ be the invariants of Γ. Note that $g_3(\Gamma) = 0$ and $g_2(\Gamma) \in \mathbb{R}^{>0}$; see Debarre (2005), pg. 15. Let $\omega := g_2(\Gamma)^{\frac{1}{4}} \in \mathbb{R}$ and let $\Lambda := \omega\Gamma$. Note that $g_2(\Lambda) = 1$ and $g_3(\Lambda) = 0$. Hence, if $E \subseteq \mathbb{P}^2(\mathbb{C})$ is the elliptic curve defined by the affine equation $w^2 = 4t^3 - t$ and $\wp$ is the Weierstrauss $\wp$-function associated to the lattice Λ, then the map

$$\phi : \mathbb{C}/\Lambda \to E, \qquad z + \Lambda \mapsto [\wp(z) : \wp'(z) : 1]$$

is an isomorphism of complex Lie groups.

Suppose $P \in E(k)$ is such that $nP \in E_{\mathrm{bad}}$. Choose $a \in \mathbb{C}$ such that $\phi(a) = P$. Then $\wp(na) \in \mathbb{R}^{\mathrm{alg}}$, whence $\wp(\overline{na}) = \wp(na)$ since Λ is closed under conjugation. This implies that $na \equiv \pm n\overline{a} \mod \Lambda$. From this it follows that $\mathrm{Re}(a) \in \mathbb{Q} \cdot \omega$ or $\mathrm{Im}(a) \in \mathbb{Q} \cdot \omega$. It thus suffices to find an $a \in \mathbb{C}$ such that $\mathrm{Re}(a), \mathrm{Im}(a) \notin \mathbb{Q} \cdot \omega$ and such that $\phi(a) \in E(k)$. We now indicate how to find such a point.

Let $P \in E(k) \setminus E_{\mathrm{tor}}$ and write $P = \phi(\alpha + \beta i)$, $\alpha, \beta \in \mathbb{R}$. If $\alpha, \beta \notin \mathbb{Q} \cdot \omega$, we are done. Assume that $\alpha \in \mathbb{Q} \cdot \omega$. (The case that $\beta \in \mathbb{Q} \cdot \omega$ is treated similarly.) Choose $m > 0$ such that $m\alpha \in \mathbb{Z} \cdot \omega$. Then $mP = \phi(m\beta i) \in E(k)$. One can then show that $\phi(m\beta + m\beta i) \in E(k)$ and it suffices to show that $m\beta \notin \mathbb{Q} \cdot \omega$. Towards a contradiction, suppose that there is m' such that $mm' \in \mathbb{Z} \cdot \omega$. Then $m'mP = \phi(m'm\beta + m'm\beta i) = O$, contradicting that P is not torsion. □

Since we needed to find $P \in E(k)$ such that $nP \notin \langle E_{\mathrm{bad}} \rangle$ for all $n \geq 1$, the preceding result is not enough to allow us to conclude that $\widetilde{A}$ is not Bezout. In fact, $E_{\mathrm{bad}} \subseteq E(Y)$, where $Y := \mathbb{R}^{\mathrm{alg}} \cup \mathbb{R}^{\mathrm{alg}}i$, and it seems that $\langle E(Y) \rangle = E$. It may be that a refinement of Corollary 2.3 might be needed to settle this case; see Question 3 below.

Question 2. *If $X \subseteq \widetilde{\mathbb{Z}}$, is $\widetilde{A}$ Bezout? More generally, if $X \subseteq \mathcal{O}$ for $\mathcal{O}$ a proper valuation ring of $\mathbb{Q}^{\mathrm{ac}}$, is $\widetilde{A}$ Bezout?* We were unable to find any useful literature on points on elliptic curves defined over the rationals with algebraic integer coordinates. When $X \subseteq \mathcal{O}$ (as when $X \subseteq \mathbb{R}^{\mathrm{alg}}$), we were able to use elementary properties of the division polynomials associated to any elliptic curve E defined over $\mathbb{Q}$ to find $P \in E'$ such that $nP \notin E_{\text{bad}}$ for all $n \geq 1$. However, as one takes combinations of points, the valuations of t-coordinates drop and it once again appears that $\langle E_{\text{bad}} \rangle = E$.

Question 3. *Can Corollary 2.3 be refined so as to weaken the conditions the point P needs to satisfy?* We have two such refinements in mind. One refinement would be to only require the existence of a point P such that $nP \notin \langle E_{\text{bad}} \rangle$ for all $n \in \{1, \ldots, N\}$, where N is some fixed positive integer. Such a bound would follow from a bound on n in Theorem 2.2. A case that this would settle would be when $X \subseteq (\mathbb{Q}^{\text{ac}} \setminus \mathcal{O})$, where $\mathcal{O}$ is a proper valuation ring of $\mathbb{Q}^{\text{ac}}$. To see this, one can choose any elliptic curve defined over $\mathbb{Q}$ and find a point whose t-coordinate has sufficiently large valuation.

Another valuable improvement in the method would be to be more specific about how nP is generated by elements of E_{bad} in Theorem 2.2. For example, this would be useful in analyzing the case $X \subseteq \mathbb{R}^{\text{alg}}$. With the notations of Question 1, call a point $P \in E(Y)$ of type I if $P \in E(\mathbb{R}^{alg})$ and of type II if $w(P) \in \mathbb{R}^{\text{alg}}i$. It is easy to verify that the sum of two points of $E(Y)$ of the same type is still in $E(Y)$, whereas the sum of two points of $E(Y)$ of different types no longer remains in $E(Y)$. If one could refine the method to disallow such combinations, then one could settle the case $X \subseteq \mathbb{R}^{\text{alg}}$.

Question 4. One should note that the only special role that elliptic curves played is that there is a group law on $\text{Pic}^0(E)$ such that the specialization map is a homomorphism. This begs the question: *Is there any advantage in working with Jac(C) for an arbitrary smooth projective curve C?*

Question 5. *Can one give a necessary and sufficient condition on X for when $\widetilde{A}$ is Bezout?* From the case that X is contained in a number field, we have seen that inverting a "small" collection of elements leads to $\widetilde{A}$ being non-Bezout. The following lemma, which is a modification of van den Dries and Macintyre (1990), 5.5, shows that inverting a "large" collection of elements leads to $\widetilde{A}$ being Bezout.

Lemma 4.2. *Suppose A has only finitely many maximal ideals. Then $\widetilde{A}$ is Bezout.*

Proof. We may assume that A is not a field. Let L be a finite extension of $k(t)$. Then since A is a Dedekind domain with only finitely many maximal ideals, so is its integral closure in L. By standard facts in commutative algebra (see Bourbaki (1972), pg. 495), this integral closure must necessarily be a PID. Thus $\widetilde{A}$ is a directed union of principal ideal domains, and hence is a Bezout domain. □

It is shown in Moret-Bailly (1987) that when $A = k[t]_{(t)}$, $\widetilde{A}$ is not a Rumely domain (even though it is Bezout) for it fails to satisfy the "glueing condition." It is unclear whether the same arguments show that $\widetilde{A}$ does not have the glueing condition for any S such that A has only finitely many maximal ideals.

The preceding lemma led us to the naïve conjecture that $\widetilde{A}$ is Bezout if and only if A has finitely many maximal ideals. Thus far, Corollary 2.3 has not led to any progress on this conjecture.

References

[1] N. Bourbaki, *Commutative algebra (English translation)*, Reading 1972.

[2] O. Debarre, *Complex tori and abelian varieties*, SMF/AMS texts and monographs, v. 11, Providence, RI: American Mathematical Society, c2005.

[3] L. van den Dries and A. Macintyre, *The logic of Rumely's local-global principle*, J. reine angew. Math. **407** (1990), 33-56.

[4] O. Forster, *Lectures on Riemann surfaces*, New York-Berlin-Heidelberg 1981.

[5] S. Lang, *Algebraic Number Theory, 2nd ed.*, Springer-Verlag, 1994.

[6] D. Marker, *Model Theory: An Introduction*, Springer-Verlag New York, 2002.

[7] L. Moret-Bailly, *Points entiers des variétés arithmétiques*, in: Séminaire de théorie des nombres, Paris '85-'86, 147-154, Basel-Stuttgart-Boston 1987.

[8] R. Rumely, *Arithmetic over the ring of all algebraic integers*, J. reine angew. Math. **368** (1986), 127-133.

[9] J. P. Serre, *Topics in Galois Theory*, Jones and Barlett Publishers, 1992.

[10] J. Silverman, *The arithmetic of elliptic curves*, New York-Berlin-Heidelberg 1986.

University of Illinois, Department of Mathematics, 1409 W. Green street, Urbana, IL 61801

E-mail address: igoldbr2@math.uiuc.edu

URL: www.math.uiuc.edu/~igoldbr2

University of Illinois, Department of Mathematics, 1409 W. Green street, Urbana, IL 61801

E-mail address: marc.masdeu@gmail.com