Bull. Math. Soc. Sci. Math. Roumanie
Tome 57(105) No. 3, 2014, 271–277

Some examples of two-dimensional regular rings

by
[1]Tiberiu Dumitrescu and [2]Cristodor Ionescu

Abstract

Let B be a ring and $A = B[X,Y]/(aX^2 + bXY + cY^2 - 1)$ where $a, b, c \in B$. We study the smoothness of A over B and the regularity of A, when B is a ring of algebraic integers.

Key Words: Smooth algebra, regular ring, ring of algebraic integers.
2010 Mathematics Subject Classification: Primary 13H05, Secondary 13F05, 11R04.

1 Introduction

In [5], Roberts investigated the $\mathbb{Z}$-smoothness and the regularity of the ring $\mathbb{Z}[X,Y]/(aX^2 + bXY + cY^2 - 1)$, $a, b, c \in \mathbb{Z}$. He showed that smoothness depends on a, b, c mod 2 (cf. [5, Theorem 1]), while regularity depends on a, b, c mod 4 (cf. [5, Theorem 2]).

In this note, we use ideas from [5] to study the regularity of the ring $A := B[X,Y]/(aX^2 + bXY + cY^2 - 1)$, $a, b, c \in B$, where B is a ring of algebraic integers. As expected this regularity depends on a, b, c mod $(\sqrt{2B})^2$ (see Corollary 4). Our main result (Theorem 2) gives a description of the singular locus of B. On the way, we show that the smoothness of A over B can be easily described: if B is an arbitrary ring, then A is smooth over B iff $a, c \in \sqrt{(2,b)B}$ (Theorem 1). Finally, Example 2 suggests that our arguments can be also used in certain higher degree cases. Throughout this paper all rings are commutative and unitary. For any undefined terminology our standard reference is [4].

2 Smoothness

Let B be an arbitrary ring. The smoothness of $B[X,Y]/(aX^2 + bXY + cY^2 - 1)$ over B can be described easily.

Theorem 1. *Let B be a ring and $a, b, c \in B$. Then $A = B[X,Y]/(aX^2 + bXY + cY^2 - 1)$ is smooth over B iff $a, c \in \sqrt{(2,b)B}$.*

Proof: Let J' be the jacobian ideal of A and set $f = aX^2 + bXY + cY^2$. By Euler's formula for homogeneous functions, we have $2f = X(\partial f/\partial X) + Y(\partial f/\partial Y)$, hence $2 \in J'$, because the image of f in A is 1. Moding out by $2B$, we may assume that B has characteristic 2. We have to show that A is smooth over B iff a, c are nilpotent modulo b. Set $C = B[X, Y]$. Note that $J' = JA$ where

$$J = (bX, bY, f-1)C = (bX, bY, aX^2 + cY^2 - 1)C = (b, aX^2 + cY^2 - 1)C$$

because $b = aX(bX) + cY(bY) - b(aX^2 + cY^2 - 1)$. So A is smooth over B iff $J = C$, cf. [3, Proposition 5.1.9]. Now $J = C$ iff $aX^2 + cY^2 - 1$ is invertible modulo b iff a, c are nilpotent modulo b. □

Corollary 1. ([5, Theorem 1].) *Let $A = \mathbb{Z}[X,Y]/(aX^2 + bXY + cY^2 - 1)$. Then A is smooth over $\mathbb{Z}$ iff b is odd or a, b, c are all even.*

Proof: By Theorem 1, A is smooth over $\mathbb{Z}$ iff $a, c \in \sqrt{(2,b)\mathbb{Z}}$ iff b is odd or a, b, c are all even. □

Similar results can be stated for any ring of algebraic integers. Here are two examples.

Corollary 2. *Let $A = \mathbb{Z}[(1+\sqrt{-7})/2][X,Y]/(aX^2+bXY+cY^2-1)$ and set $\theta = (1+\sqrt{-7})/2$. Then A is smooth over $\mathbb{Z}[\theta]$ iff one of the following cases occurs:*
(i) b is not divisible by θ or $\bar{\theta}$,
(ii) b is not divisible by θ and a, b, c are all divisible by $\bar{\theta}$,
(iii) b is not divisible by $\bar{\theta}$ and a, b, c are all divisible by θ,
(iv) a, b, c are all divisible by 2.

Proof: We have $2 = \theta\bar{\theta}$. By Theorem 1, A is smooth over $B = \mathbb{Z}[\theta]$ iff $a, c \in \sqrt{(2,b)B} = (\theta, b)B \cap (\bar{\theta}, b)B$. As θB and $\bar{\theta}B$ are maximal ideals, the assertion is clear. □

Corollary 3. *Let $A = \mathbb{Z}[\theta][X,Y]/(aX^2+bXY+cY^2-1)$, $\theta = (\sqrt{2}+\sqrt{6})/2$. Then A is smooth over $\mathbb{Z}[\theta]$ iff b is not divisible by $1+\theta$ or a, b, c are all divisible by $1+\theta$.*

Proof: It can be checked by PARI-GP (see [2]) that $B = \mathbb{Z}[\theta]$ is a PID and $2B = (1+\theta)^4 B$. So $\sqrt{(2,b)B} = (1+\theta, b)B$. Apply Theorem 1. □

3 Regularity

Throughout this section we fix the following notations. Let B be a ring of algebraic integers, that is, the integral closure of $\mathbb{Z}$ in a finite field extension of $\mathbb{Q}$. It is well-known (e.g. [1, Chapter 6]) that B is a Dedekind domain, hence $II^{-1} = B$ for every nonzero ideal I of B. Fix $a, b, c \in B$. We study the regularity of the ring

$$A = B[X,Y]/(aX^2 + bXY + cY^2 - 1).$$

Set $g = aX^2 + bXY + cY^2 - 1$ and $C = B[X, Y]$.

Lemma 1. *If $Q \in Spec(A)$ and $Q \cap B \not\supseteq (2,b)B$, then A_Q is a regular ring.*

Proof: Since $P := Q \cap B \not\supseteq (2,b)B$, Theorem 1 shows that the composed morphism

$$B_P \to B_P \otimes_B A = B_P[X,Y]/(g) \to A_Q$$

is smooth. Hence A_Q is regular, because B is regular. □

Let Γ be the (finite) set of prime ideals P of B such that $P \supseteq (2,b)B$ and $P \not\supseteq (a,c)B$. By Theorem 1, A is smooth over B iff $\Gamma = \emptyset$.

Lemma 2. *If $Q \in Spec(A)$, then $Q \cap B \in \Gamma$ iff $Q \cap B \supseteq (2,b)B$.*

Proof: Assume that $P := Q \cap B \supseteq (2,b)B$. As $(a,b,c)A = A$, it follows that $Q \not\supseteq (a,c)B$, so $P \not\supseteq (a,c)B$, that is, $P \in \Gamma$. The converse is obvious. □

Let $P \in \Gamma$. Since B is a ring of algebraic integers and $2 \in P$, it follows that B/P is a finite (thus perfect) field of characteristic 2. If $z \in B$, let $\bar{z}$ denote its image in B/P. Let $d, e \in B$ be such that

$$\bar{d}^2 = \bar{a} \text{ and } \bar{e}^2 = \bar{c}. \tag{3.1}$$

Note that $d, e \in B$ are uniquely determined modulo P. If $a \notin P$ (hence $d \notin P$), consider the polynomial $F_P \in C$ given by

$$F_P := d^2 g(\frac{-eY-1}{d}, Y) = a(eY+1)^2 + bd(-eY-1)Y + d^2cY^2 - d^2 = \tag{3.2}$$

$$= (ae^2 - bde + cd^2)Y^2 + (2ae - bd)Y + (a - d^2).$$

If $a \in P$ (hence $c, e \notin P$, because $P \in \Gamma$), define $F_P \in C$ by

$$F_P := e^2 g(X, \frac{-1}{e}) = ae^2X^2 - beX + (c - e^2). \tag{3.3}$$

Lemma 3. *Let $M \in Spec(A)$ and $P = M \cap B$. Then the ring A_M is not regular iff $P \supseteq (2,b)B$ and $F_P P^{-1} A \subseteq M$.*

Proof: By Lemma 1, A_M is regular if $P \not\supseteq (2,b)B$. Assume that $P \supseteq (2,b)B$. By Lemma 2, $P \in \Gamma$, so F_P is defined as in (3.2) or (3.3). Set $K = B/P$. We use the notations after Lemma 2. The image of g in $K[X,Y]$ is

$$\bar{a}X^2 + \bar{c}Y^2 + \bar{1} = (\bar{d}X + \bar{e}Y + \bar{1})^2 \tag{3.4}$$

because $\bar{b} = 0$, $\bar{d}^2 = \bar{a}$ and $\bar{e}^2 = \bar{c}$. Let Q be the inverse image of M in $C = B[X,Y]$ and set

$$Z_P := dX + eY + 1. \tag{3.5}$$

As $P \subseteq Q$ and $g \in Q$, we get $g - Z_P^2 \in Q$, so $Z_P \in Q$. Assume that $a \notin P$ (the case $a \in P$, $c \notin P$ is similar: we use (3.3) instead of (3.2)). Then $d \notin P$. We have $dX = Z_P - eY - 1$, so

$$d^2 g = a(dX)^2 + bd(dX)Y + d^2(cY^2 - 1) =$$

$$= a(Z_P - eY - 1)^2 + bd(Z_P - eY - 1)Y + d^2(cY^2 - 1) =$$

$$= aZ_P^2 - 2aZ_P(eY + 1) + bdZ_P + d^2 g(\frac{-eY - 1}{d}, Y) =$$

$$= aZ_P^2 - 2aZ_P(eY + 1) + bdZ_P + F_P \tag{3.6}$$

cf. (3.2). By [6, Theorem 26, page 303], A_M is not regular iff $g \in Q^2 C_Q$ iff $d^2 g \in Q^2 C_Q$, because $d \notin Q$. Since aZ_P^2, $2aZ_P(eY+1)$ and bdZ_P belong to Q^2, (3.6) shows that $d^2 g \in Q^2 C_Q$ iff $F_P \in Q^2 C_Q$. Thus

$$A_M \text{ is not regular iff } F_P \in Q^2 C_Q. \tag{3.7}$$

By (3.6), $F_P = (d^2 g - aZ_P^2) + 2aZ_P(eY + 1) - bdZ_P$ where $d^2 g - aZ_P^2 \in PC$ (cf. 3.4 and 3.5) and $2, b \in P$; so the coefficients of F_P are in P. Also, $P \not\subseteq Q^2 C_Q$ because $C/PC = K[X,Y]$ is a regular ring. So, by (3.7), A_M is not regular iff $F_P C = P(F_P P^{-1})C \subseteq Q^2 C_Q$ iff $F_P P^{-1} C \subseteq QC_Q$ iff $F_P P^{-1} C \subseteq Q$ iff $F_P P^{-1} A \subseteq M$. □

Theorem 2. *The singular locus of A is $V(H)$ where*

$$H = \prod_{P \in \Gamma} (P, F_P P^{-1})A$$

and $\Gamma = \{P \in Spec(B) \mid P \supseteq (2,b)B \text{ and } P \not\supseteq (a,c)B\}$.

Proof: Apply Lemmas 2 and 3. □

Let $P \in \Gamma$. According to (3.1), d, e are elements of B (uniquely determined modulo P) such $d^2 \equiv a$, $e^2 \equiv c$ modulo P. Note that since $2 \in P$, the elements $2de$, d^2, e^2 are uniquely determined modulo P^2.

Corollary 4. *The ring A is regular iff for every $P \in \Gamma$ we have:*
(i) if $a \notin P$, then $b \equiv 2de$, $cd^2 \equiv ae^2$, $a \not\equiv d^2$ modulo P^2,
(ii) if $a \in P$, then $a \equiv b \equiv 0$, $c \not\equiv e^2$ modulo P^2.

Proof: (*i*). By Theorem 2 (or Lemma 3), A is regular iff $(P, F_P P^{-1})A = A$ for every $P \in \Gamma$. Fix $P \in \Gamma$, set $K = B/P$ and assume that $a \notin P$. Note that F_P is defined in (3.2); denote F_P briefly by $\alpha Y^2 + \beta Y + \gamma$. We have the following chain of equivalences:

$$(P, F_P P^{-1})A = A \Leftrightarrow C = (P, g, F_P P^{-1})C = (P, Z_P^2, F_P P^{-1})C \text{ (cf. 3.5)} \Leftrightarrow$$

$$\Leftrightarrow C = (P, Z_P, F_P P^{-1})C.$$

Hence $(P, F_P P^{-1})A = A$ iff the following ring is the zero ring

$$C/(P, Z_P, F_P P^{-1})C \simeq B_P[X,Y]/(P, Z_P, \frac{F_P}{p})B_P[X,Y] \simeq$$

$$\simeq K[X,Y]/(Z_P, \frac{F_P}{p})K[X,Y] \simeq K[Y]/(\frac{F_P}{p})K[Y]$$

where $p \in P$ is such that $pB_P = PB_P$; for the last isomorphism we used the fact that $d \notin P$. Thus $(P, F_P P^{-1})A = A$ iff $\alpha/p \in pB_P$, $\beta/p \in pB_P$ and $\gamma/p \notin pB_P$ iff $\alpha \in P^2$, $\beta \in P^2$ and $\gamma \notin P^2$ iff $ae^2 + cd^2 \equiv bde$, $bd \equiv 2ae$ and $a \not\equiv d^2$ where the congruences are modulo P^2. From $ae^2 + cd^2 \equiv (bd)e$ and $bd \equiv 2ae$, we get $ae^2 + cd^2 \equiv bde \equiv (2ae)e$ and $bd \equiv 2d^2e$ (because $2a \equiv 2d^2$), so $cd^2 \equiv ae^2$ and $b \equiv 2de$ because $d \notin P$. The argument is reversible. Case (ii) can be done similarly. □

Remark 1. *Note that condition $a - d^2 \notin P^2$ in Corollary 4 means that a is not a quadratic residue modulo P^2.*

Corollary 5. ([5, Theorem 2].) *Let $A = \mathbb{Z}[X,Y]/(aX^2 + bXY + cY^2 - 1)$. Then A is regular but not smooth over $\mathbb{Z}$ iff one of the following cases occurs (all congruences below are modulo 4):*

(1) $a \equiv 3$, $b \equiv 2$, $c \equiv 3$,
(2) $a \equiv 0$, $b \equiv 0$, $c \equiv 3$,
(3) $a \equiv 3$, $b \equiv 0$, $c \equiv 0$.

Proof: Assume that A is not smooth over $\mathbb{Z}$. With the notations of Corollary 4, we have $\Gamma = \{2\mathbb{Z}\}$. We can take $d = a$ and $e = c$. By Corollary 4, A is regular iff

(i) if a is odd, then $b - 2ac \in 4\mathbb{Z}$, $ac(a - c) \in 4\mathbb{Z}$, $a - a^2 \notin 4\mathbb{Z}$,
(ii) if a is even, then $a \in 4\mathbb{Z}$, $b \in 4\mathbb{Z}$, $c - c^2 \notin 4\mathbb{Z}$.

The conclusion follows. □

Example 1. *Consider the ring*

$$D = \mathbb{Z}[\theta][X,Y]/((1-\theta)X^2 + \theta XY + (1-\theta)Y^2 - 1)$$

where $\theta = (1 + \sqrt{-7})/2$. Using the notations above, we have: $\Gamma = \{P\}$, where $P = \theta\mathbb{Z}[\theta]$, $a = c = 1 - \theta$, $b = \theta$, $d = e = 1$. We check the conditions in part (i) of Corollary 4: $b - 2de = \theta - 2 = \theta^2 \in P^2$, $cd^2 - ae^2 = 0 \in P^2$, $a - d^2 = -\theta \notin P^2$. So D is a regular ring. By Corollary 2, D is not smooth over $\mathbb{Z}[\theta]$.

Corollary 6. *Let $A = \mathbb{Z}[\sqrt{-5}][X,Y]/(aX^2 + bXY + cY^2 - 1)$ and $P = (2, 1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$.*

(i) *A is smooth over $\mathbb{Z}[\sqrt{-5}]$ iff $b \notin P$ or $a, b, c \in P$.*
(ii) *A is regular but not smooth over $\mathbb{Z}[\sqrt{-5}]$ iff one of the following cases occurs:*
(1) *$a - \sqrt{-5}$, b, $c - \sqrt{-5}$ are divisible by 2,*
(2) *a, b, $c - \sqrt{-5}$ are divisible by 2,*
(3) *$a - \sqrt{-5}$, b, c are divisible by 2.*

Proof: By Theorem 1, A is smooth over $B = \mathbb{Z}[\sqrt{-5}]$ iff $a, c \in \sqrt{(2,b)B} = P + bB$. Hence (i) follows. Assume that A is not smooth over B; hence $b \in P$ and $(a, c) \nsubseteq P$. We have $\Gamma = \{P\}$ (see the notations above) and $P^2 = 2B$. We translate the regularity conditions in Corollary 4; note that we can take $d = a$ and $e = c$. Part (i) of Corollary 4 says that if $a \notin P$, we must have the congruences modulo (2): $b \equiv 0$, $ca^2 \equiv ac^2$, $a \not\equiv a^2$; we get $a \equiv \sqrt{-5}$, $b \equiv c \equiv 0$ or $a \equiv c \equiv \sqrt{-5}$, $b \equiv 0$. Part (ii) of Corollary 4 says that if $a \in P$ (hence $c \notin P$), we must have the congruences modulo $a \equiv b \equiv 0$, $c \not\equiv c^2$; we get $a \equiv b \equiv 0$, $c \equiv \sqrt{-5}$. ∎

The arguments in the proof of Theorem 2 can be also used in certain higher degree cases. We close our note with an example in this direction.

Example 2. *We show that for every prime p, the following ring is regular but not smooth over* $\mathbb{Z}$

$$D = \mathbb{Z}[X, Y]/((p + 1)X^p + p^2Y^p - 1).$$

Using Euler's formula as in the proof of Theorem 1, we can prove easily that the jacobian ideal of D *is* $J = pD \neq D$*, so* D *is not smooth over* $\mathbb{Z}$*. Set* $g = (p + 1)X^p + p^2Y^p - 1$*. Assume there exists a maximal ideal* Q *of* $E := \mathbb{Z}[X, Y]$ *containing* g *such that* D_{QD} *is not regular; then* $g \in Q^2D_{QD}$*, so* $g \in Q^2$*. As* $J = pD$*,* $p \in Q$*. Set* $Z := X - 1$*. Since* g *and* Z^p *are congruent modulo* pE*, we get* $Z^p \in (g, pE) \subseteq Q$*, hence* $Z \in Q$*. As* $X = Z + 1$*, we get*

$$g = (p + 1)(Z + 1)^p + p^2Y^p - 1 = (p + 1)[Z^p + \sum_{k=1}^{p-1} \binom{p}{k} Z^{p-k}] + p^2Y^p + p.$$

Note that the bracket above belongs to Q^2 *because* $p, Z \in Q$*. So* $g \in Q^2$ *implies* $p(pY^p + 1) = p^2Y^p + p \in Q^2$*, hence* $p \in Q^2$ *because* $pY^p + 1 \notin Q$ *(as* $p \in Q$*). We reached a contradiction, because* $E/pE = \mathbb{Z}_p[X, Y]$ *is a regular ring, so* $p \notin Q^2$*.*

References

[1] S. Alaca, K. Williams, *Algebraic Number Theory*, Cambridge University Press, 2004.

[2] H. Cohen, *Pari-GP*, now maintained by K. Belabas, http://www.parigp-home.de.

[3] J. Majadas, A. Rodicio, *Smoothness, Regularity and Complete intersection,* Cambridge University Press, 2010.

[4] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.

[5] L. Roberts, Some examples of smooth and regular rings. Canad. Math. Bull. **23**(1980), pp. 255–259.

[6] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Van Nostrand, Princeton 1960.

Received: 24.06.2013

Revised: 17.12.2013

Accepted: 28.01.2014

[1]Department of Mathematics,
University of Bucharest
E-mail: tiberiu@fmi.unibuc.ro,
tiberiu_dumitrescu2003@yahoo.com

[2]Simion Stoilow Institute of Mathematics,
Romanian Academy
E-mail: cristodor.ionescu@imar.ro