COMPOSITIO MATHEMATICA

JEFFREY LANG

The factoriality of Zariski rings

Compositio Mathematica, tome 63, nº 3 (1987), p. 273-290

<http://www.numdam.org/item?id=CM_1987__63_3_273_0>

Compositio Mathematica 63: 273–290 (1987)

The factoriality of Zariski rings

JEFFREY LANG
Mathematics Department, University of San Francisco, San Francisco, CA 94117, USA
Present address: *Mathematics Dept., University of Kansas, Lawrence, KS 66044, USA*

Received 10 November 1986; accepted 19 February 1987

Introduction

Let k be an algebraically closed field of characteristic $p \neq 0$, $g \in k[x, y]$ be such that g_x and g_y have no common factors in $k[x, y]$, $E \subset A_k^3$ be the surface defined by the equation $z^p = g(x, y)$ and $A = k[x^p, y^p, g]$. In previous articles (see [1], [3] and [13]) E was called a Zariski surface and attempts were made to find generic conditions on g that would force the coordinate ring of E to be factorial. These papers used the fact that the coordinate ring of E is isomorphic to A and some partial results were obtained.

In this article the divisor class group of these surfaces is investigated from a slightly different angle. Let F be a non-algebraically closed field of characteristic $p \neq 0$. Let $\bar{F}$ be an algebraic closure of F. Given g in $\bar{F}[x, y]$ let F_g be the field extension of F obtained by adjoining the coefficients of g to F. This paper investigates the relationship between the singular points of the surface $z^p = g(x, y)$ in k^2 and the divisor class group of the ring $F_g[x^p, y^p, g]$.

After some preliminary results in Section 1, Zariski rings are discussed in Section 2. In this section singularity conditions affecting the order of the divisor class group of a Zariski ring are presented.

Some general facts about Zariski rings appear in Section 3.

In Section 4, the main section of the article, the fact that for $p > 3$, Zariski rings are factorial for a generic choice of g is proved by showing that for a generic g, the class group of the surface $z^p = g$ is trivial.

Section 5 closes this article with a theorem about logarithmic derivatives of the Jacobian derivation and some open problems.

0. Notation

(0.1) $GF(p^n)$ – the finite field with p^n elements.
(0.2) F – a field of characteristic $p \neq 0$.
(0.3) $\bar{F}$ – an algebraic closure of F.

(0.4) For $g \in \bar{F}[x, y]$ we denote by F_g the field extension of F obtained by adjoining to F the coefficients of g.
(0.5) For $g \in \bar{F}[x, y]$ we denote by A_g the ring $F_g[x^p, y^p, g]$. We call these rings **Zariski rings.**
(0.6) If A is a Krull ring we denote by $Cl(A)$ the divisor class group of A.
(0.7) Surface-irreducible, reduced, two dimensional quasiprojective variety over an algebraically closed field.
(0.8) If E is a surface we denote by $Cl(E)$ the divisor class group of the coordinate ring of E.
(0.9) k – an algebraically closed field of characteristic $p \neq 0$.
(0.10) A^n_k – affine n-space over k.
(0.11) k^n – the set of all n-tuples of elements of k.
(0.12) For $g \in k[x, y]$ we let $S_g = \{(\alpha, \beta) \in k^2 \colon g_x(\alpha, \beta) = g_y(\alpha, \beta) = 0\}$.

1. Preliminaries

The following results, (1.1) to (1.4), can be found in P. Samuel's 1964 Tata notes [17]. For the definition of a Krull ring the reader is referred to either Samuel's notes or R. Fossum's book, "The Divisor Class Group of a Krull Domain" [5]. All of the rings considered in this paper are noetherian integrally closed domains and are therefore Krull rings.

THEOREM 1.1. *Let $A \subset B$ be Krull rings. If each height one prime of B contracts to a prime of height less than or equal to one of A then there is a well defined group homomorphism $\phi \colon Cl(A) \to Cl(B)$. If B is integral over A or if B is A-flat then this condition is satisfied. (See [17] pp. 19–20 for details.)*

REMARK 1.2. Let B be a Krull ring of characteristic $p \neq 0$. Let Δ be a derivation of the quotient field of B such that $\Delta(B) \subset B$. Let $K = \ker\Delta$ and $A = B \cap K$. Then A is a Krull ring with B integral over A. Thus by (1.1) there is a well-defined map $\phi \colon Cl(A) \to Cl(B)$. Set $\mathscr{L} = \{t^{-1}\Delta t : t$ belongs to the quotient field of B and $t^{-1}\Delta t \in B\}$ and $\mathscr{L}' = \{u^{-1}\Delta u : u$ is a unit in $B\}$. Then $\mathscr{L}'$ is a subgroup of $\mathscr{L}$.

THEOREM 1.3.
(a) There exists a canonical homomorphism $\bar{\phi}$: $\ker \phi \to \mathscr{L}/\mathscr{L}'$.
(b) If L is the quotient field of B and $[L : K] = p$ and $\Delta(B)$ is not contained in any height one prime of B, then $\bar{\phi}$ is an isomorphism ([17] pp. 63–64).

THEOREM 1.4. *If* $[L:K] = p$, *then*
(a) there exists an $\alpha \in A$ *such that* $\Delta^p = \alpha\Delta$ *and*
(b) an element $t \in K$ *is equal to* Dv/v *for some* $v \in K$ *if and only if* $\Delta^{p-1}t - \alpha t = -t^p$ *([17] pp. 63–64.).*

REMARK 1.5. These results, (1.6) and (1.8) are to be found in [11] pages 394–395. These theorems assume that F is a field of characteristic $p \neq 0$, $g(x, y) \in F(x, y]$ is such that g_x and g_y have no common factors in $\bar{F}[x, y]$.

THEOREM 1.6. *(Ganong's Formula) Let* $D: F(x, y) \to F(x, y)$ *be the* F *derivation defined by* $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$. *Then for each* $\alpha \in F(x, y)$,

$$D^{p-1}\alpha - c\alpha = -\sum_{j=0}^{p-1} g^j \nabla(g^{p-j-1}\alpha)$$

where $D^p = cD$ *and* $\nabla = \partial^{2p-2}/\partial x^{p-1}\partial y^{p-1}$.

REMARK 1.7. In [11] the writer proved this result for the case $\deg(g_x) = \deg(g) - 1$. In [16] Stöhr and Voloch proved this formula in general.

THEOREM 1.8. *Let* $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$. *Let* $\mathscr{L}$ *be the additive group of logarithmic derivatives of* D *in* $F[x, y]$ *(See (1.2).) and* $A = F[x^p, y^p, g]$. *Then*

(i) $D^{-1}(0) \cap F[x, y] = A$,
(ii) $Cl(A) \cong \mathscr{L}$,
(iii) $t \in \mathscr{L}$ *implies that* $\deg t \leqslant \deg(g) - 2$,
(iv) *The coordinate ring of the surface defined by* $z^p = g(x, y)$ *is isomorphic to* $A \otimes \bar{F}$.

(See [11] pp. 393–394.)

2. Singularity conditions on Zariski rings

REMARK 2.1. A surface in affine 3-space defined by an equation of the form $z^p = g(x, y)$ with only a finite number of isolated singularities is called a Zariski surface, where the ground field is algebraically closed of characteristic $p \neq 0$. The coordinate ring of such a surface is isomorphic to $k[x^p, y^p, g]$ where k is the ground field ([11] p. 393). Hereafter, in this paper all rings of the form $F[x^p, y^p, g]$ where F is a field, not necessarily algebraically closed, of characteristic $p \neq 0$ will be referred to as Zariski rings. This section studies Zariski rings defined over non-algebraically closed fields.

An important tool is the following lemma.

LEMMA 2.2. *Let $D: k(x, y) \to k(x, y)$ be the k-derivation defined by $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$ and c be such that $D^p = cD$. If $(a, b) \in k^2$ is such that $g_x(a, b) = g_y(a, b) = 0$, then $c(a, b) = (\sqrt{H(a, b)})^{p-1}$ where $H(x, y) = g_{xy}^2 - g_{xx}g_{yy}$.*

Proof. For each $\alpha \in k(x, y)$,

$$D^{p-1}\alpha - c\alpha = -\sum_{i=0}^{p-1} g^i \nabla(g^{p-i-1}\alpha) \tag{2.2.1}$$

by (1.6).

Set $\alpha = 1$, then $c = \Sigma_{i=0}^{p-1} g^i \nabla(g^{p-i-1})$.

Let $\bar{g} = g(x + a, y + b)$ and $\bar{c} = \Sigma_{i=0}^{p-1} \bar{g}^i \nabla(\bar{g}^{p-i-1})$. Then $\bar{c}(0, 0) = \Sigma_{i=0}^{p=1} g(a, b)^i \nabla(g^{p-i-1})\ (a, b) = c(a, b)$. By Taylor's formula,

$$g(x, y) = g(a, b) + g_{xx}(a, b)\frac{(x-a)^2}{2} + g_{xy}(a, b)\,(x-a)\,(y-b)$$
$$+ g_{yy}(a, b)\frac{(y-b)^2}{2} + \text{(higher degree terms)}.$$

Thus

$$\bar{g}(x, y) = g(a, b) + g_{xx}(a, b)\frac{x^2}{2} + g_{xy}(a, b)xy$$
$$+ g_{yy}(a, b)\frac{y^2}{2} + \text{(higher degree terms)}.$$

Let $\bar{\bar{g}} = \bar{g} - g(a, b)$ and $\bar{\bar{c}} = -\Sigma_{i=0}^{p-1} \bar{\bar{g}}\nabla(\bar{\bar{g}}^{p-i-1})$. Since $(\bar{\bar{g}})_x = (\bar{g})_x$ and $(\bar{\bar{g}})_y = (\bar{g})_y$ it follows that $\bar{\bar{c}}(x, y) = \bar{c}(x, y)$ and $\bar{\bar{c}}(0, 0) = c(a, b)$. Since $\bar{\bar{g}}(0, 0) = 0$ it follows that $\bar{\bar{c}}(0, 0) = \nabla(\bar{\bar{g}}^{p-1})(0, 0)$. A simple calculation yields that the lowest degree term in $\bar{\bar{g}}^{p-1}$ is

$$\left\{\sum_{i=0}^{(p-1)/2} \binom{p-1}{2i}\binom{2i}{i} g_{xy}^{p-2i-1}\left(\frac{g_{xx}}{2}\right)^i\left(\frac{g_{yy}}{2}\right)^i\right\}(a, b)\cdot x^{p-1}y^{p-1}.$$

Thus the lowest degree term of $\nabla(\bar{\bar{g}}^{p-1})$ is the constant term,

$$\sum_{i=0}^{(p-1)/2} (-1)^i \binom{(p-1)/2}{i} g_{xy}^{p-2i-1}(g_{xx}g_{yy})^i.$$

In the previous step a combinatorial identity was used (see [6] page 90, identity z.40). Thus the constant term in $\nabla(\bar{\bar{g}}^{p-1})$ is $(H(a,b))^{(p-1)/2}$. Therefore $\nabla(\bar{\bar{g}}^{p-1})(0,0) = (\sqrt{H(a,b)})^{p-1}$.

REMARK 2.3. Let F be a non-algebraically closed field of characteristic $p \neq 0$ and $\bar{F}$ an algebraic closure of F. For $g \in \bar{F}[x,y]$, let F_g be the field extension of F obtained by adjoining to F the coefficients of g. Throughout the remainder of this article g will always satisfy two conditions

(1) g_x and g_y have no common factors in $\bar{F}[x,y]$ and that g_x and g_y intersect in the maximum possible number of points in $\bar{F}^2((n-1)^2$ if $n \neq 0$ (mod p), $n^2 - 3n + 3$ otherwise, where $n = \deg(g)$.), and

(2) g_x, g_y and $H = g_{xy}^2 - g_{xx}g_{yy}$ are never simultaneously zero at any point in $\bar{F}^2$ (see [1] for the generic nature of these conditions). The effect of these conditions and others on the divisor class group of $A_g = F_g[x^p, y^p, g]$ will be explored in the rest of this paper. The assumption will always be made that g has no monomials of the form $x^{rp}y^{sp}$, since $F_g[x^p, y^p, g] = F_g[x^p, y^p, g + x^{rp}y^{sp}]$.

THEOREM 2.4. *If the ideal* $I = (g_x, g_y)F_g[x,y] \cap F_g[x]$ in $F_g[x]$ *is prime and if no two points of* $S_g = \{(\alpha,\beta) \in \bar{F}^2 : g_x(\alpha,\beta) = g_y(\alpha,\beta) = 0\}$ *have the same x-coordinate then for each* $(a,b) \in S_g$, *the field degree* $[F_g(a):F_g]$ *equals*

$$\begin{cases} (n-1)^2; & \textit{if} = \deg(g) \neq 0 \pmod p, \\ n^2 - 3n + 3; & \textit{if } n = 0 \pmod p. \end{cases}$$

Proof. Consider the case $n \neq 0$ (mod p). Let $f(x)$ be the resultant with respect to x of g_x and g_y. Then $f(x)$ is of degree $(n-1)^2$ and belongs to I([15] page 186). I is a principal ideal generated by a polynomial of degree at least $(n-1)^2$. Therefore $I = (f(x))$. If $(a,b) \in S_g$ then $f(a) = 0$ which implies that $[F_g(a):F_g] = (n-1)^2$. The $n \equiv 0$ (mod p) case is similar.

COROLLARY 2.5. *If* $m = (g_x, g_y)F_g[x,y]$ *is a prime ideal in* $F_g[x,y]$ *and if no two points of* S_g *have the same x-coordinate or the same y-coordinate, then* $F_g(a,b) = F_g(a) = F_g(b)$, *for all* $(a,b) \in S_g$.

Proof. By (2.4) both a and b are separable over F_g of degree equal to the number of elements in S_g. Then $F_g(a,b)$ is separable over F_g of degree equal to the number of F_g-injections of $F_g(a,b)$ into $\bar{F}$ ([15], p. 65). Since each such injection must take an element of S_g into another element of S_g it follows that $[F_g(a,b):F_g(a)] = [F_g(a,b):F_g(b)] = 1$.

Corollary 2.7. *If no two points of S_g have the same x or y coordinate and both of the ideals* $(g_x, g_y)F_g[x, y] \cap F_g[x]$ and $(g_x, g_y)F_g[x, y] \cap F_g[y]$ *are prime then* $F_g(a) = F_g(b) = F_g(a, b)$.

Remark 2.8. Let k be an algebraically closed field of characteristic $p \neq 0$ and $D: k[x, y] \to k[x, y]$ be defined by $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$. Let $\mathscr{L}$ be the group of logarithmic derivatives of D in $k[x, y]$. By (1.4) an element $t \in k[x, y]$ is in $\mathscr{L}$ if and only if $D^{p-1}t - ct = -t^p$ where $D^p = cD$. It follows that if $(a, b) \in S_g$, then $c(a, b)t(a, b) = t(a, b)^p$, which by (2.2) implies that $(t(a, b))^p = (\sqrt{H(a, b)})^{p-1}(t(a, b))$. Since $H(a, b) \neq 0$ by condition (2), the set of solutions in k to the polynomial equation $z^p - (\sqrt{H(a, b)})^{p-1}z = 0$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Thus $\theta: \mathscr{L} \to \mathbb{Z}/p\mathbb{Z}$ defined by $\theta(t) = t(a, b)/\sqrt{H(a, b)}$ is a homomorphism of additive groups.

Theorem 2.9. *Let g satisfy conditions (1) and (2). If* $0 \neq t \in \mathscr{L}$ *then* $t(Q) \neq 0$ *for at least*

$$\begin{cases} (n-1)(n-1-\deg(t)), & \text{if } n \not\equiv 0 \pmod p \\ (n-1)(n-2-\deg(t))+1, & \text{if } n = 0 \pmod p \end{cases}$$

points $Q \in S_g$, *where* $n = \deg(g)$.

Proof. Let $0 \neq t \in \mathscr{L}$. By condition (1), each irreducible factor of t in $k[x, y]$ is relatively prime to either g_x or g_y. Therefore t can be factored in $k[x, y]$ as $t = uv$ where u is relatively prime to g_x and v is relatively prime to g_y (If t is already prime to g_x then let $u = t$ and $v = 1$.). Then u meets g_x in at most $(n - 1)\deg(u)$ points and v meets g_y in at most $(n - 1)\deg(v)$ points. Thus u (resp. v) is 0 at most $(n - 1)\deg(u)$ (resp. $(n - 1)\deg(v)$) points of S_g. This implies that t is not 0 for at least

$$\begin{cases} (n-1)^2 - ((n-1)\deg(u) + (n-1)\deg(v)), & \text{if } n \not\equiv 0 \pmod p \\ n^2 - n + 3 - ((n-1)\deg(u) + (n-1)\deg(v)), & \text{if } n = 0 \pmod p \end{cases}$$

points of S. Since $\deg(u) + \deg(v) = \deg(t)$ the desired result is obtained.

Corollary 2.10 *Let g satisfy (1) and (2). If* $0 \neq t \in \mathscr{L}$ *then* $t(Q) \neq 0$ *for at least* $(n - 1)$ *points of* S_g *if* $n \neq 0$ ((mod p)) *and for at least one point of* S_g *otherwise.*

Proof. By (1.8) deg $t \leqslant n - 2$. The result is now an immediate consequence of (2.9).

COROLLARY 2.11. *Let g satisfy (1) and (2). Then the homomorphism $\Phi: \mathscr{L} \to \oplus_{Q \in S_g} \mathbb{Z}/p\mathbb{Z} \cdot \sqrt{H(Q)}$ defined by $\Phi(t) = (t(Q))_{Q \in S_g}$ is an injection.*

COROLLARY 2.12. *If $(g_x, g_y)F_g[x, y] \cap F_g[x]$ is prime in $F_g[x]$ and if no two points of S_g have the same x-coordinate then the restriction of $\theta: \mathscr{L} \to \mathbb{Z}/p\mathbb{Z}$ to $\mathscr{L}_g = \mathscr{L} \cap F_g[x, y]$ is an injection.*

Proof. For $t \in \mathscr{L}_g$, $\theta(t) = t(a, b)$ where $(a, b) \in S_g$. Suppose that $\theta(t) = 0$. Let $(a', b') \in S_g$. As in the proof of (2.5) there exists an F_g-isomorphism from $F_g(a, b)$ onto $F_g(a', b')$ such that $\sigma(a) = a'$ and $\sigma(b) = b'$. Since $t(a, b) = 0$, then $\sigma(t(a, b)) = t(a', b') = 0$. Therefore Φ as defined in (2.11) maps t to 0 in $\oplus_{Q \in S_s} \mathbb{Z}/p\mathbb{Z} \cdot \sqrt{H(q)}$. By (2.11), $t = 0$.

DEFINITION 2.13. The conditions on g that no two points of S_g have the same x-coordinate and that $(g_x, g_y)F_g[x, y] \cap F_g[x]$ is a prime ideal in $F_g[x]$ will hereafter be referred to as conditions (3) and (4) respectively.

THEOREM 2.14. *Let g satisfy conditions (1)–(4). Let $A_g = F_g[x^p, y^p, g]$. If $p = 2$, then $Cl(A_g) \cong \mathbb{Z}/2\mathbb{Z}$. If $p > 2$, then $Cl(A_g)$ is trivial or is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

PROOF The $p > 2$ case is an immediate consequence of (2.12). Assume then that $p = 2$. Then $D(g_x)/g_x = (g_{xx}g_y - g_{xy}g_x)/g_x = g_{xy}$ is a nonzero element of $\mathscr{L}_g$ by condition (2). By (2.12), $Cl(A_g) \cong \mathbb{Z}/2\mathbb{Z}$.

EXAMPLE 2.15. If $p > 2$, $g = x^2 - y^2$ and $F = GF(p)$, then g satisfies conditions (1)–(4). Since $z^p = x^2 - y^2$ is clearly not factorial, $Cl(A_g) \cong \mathbb{Z}/p\mathbb{Z}$.

EXAMPLE 2.16 Let k be an algebraically closed field of characteristic $p \neq 0$. Let $n \geqslant 4$ be a positive integer. Let $\{T_{ij}: 0 \leqslant i + j \leqslant n\}$ be a set of indeterminates over k. Let $F = k(T_{ij})$ and $g = \Sigma_{0 \leqslant i+j \leqslant n} T_{ij}x^i y^j$.

Then g satisfies conditions (1)–(3). To see this let $R(x)$ be the resultant with respect to x of g_x and g_y. Then $R(x) \not\equiv 0$. This can be demonstrated by showing that for some specialization of the T_{ij}, $R(x) \neq 0$. If n is not divisible by p, then $g = xy + (1/n)(x^n - y^n)$ gives $R(x) = x^{(n-1)^2} + x$.

Furthermore, if D is the discriminant of $R(x)$, then D is a nonzero polynomial expression in the T_{ij}. Again this can be shown by demonstrating that $D \neq 0$ for some specialization of the T_{ij}. For example, if $n \neq 0, 2 \pmod p$, and $g = xy + (1/n)(x^n - y^n)$, then $D = n(n-2)$. Similarly, it is easy to show that if $\bar{R}(x)$ is the resultant of g_x and H and if $\bar{D}$ is the resultant of $R(x)$ and $\bar{R}(x)$, then $\bar{D}$ is a nonzero polynomial in the T_{ij}. Again if we specialize and let $g = xy + (1/n)(x^n - y^n)$ then $\bar{D}$ becomes $n^2 - 2n + 2$. One concludes that

(a) $R(x)$ is a nonzero polynomial in the T_{ij} and x of degree in x equal to $(n-1)^2$ if $n \neq 0 \pmod p$, of degree $n^2 - 3n + 3$ otherwise. Therefore g_x and g_y are relatively prime,
(b) D is a non-zero polynomial in the T_{ij} which implies that g_x and g_y intersect in the maximum possible number of points in $\bar{F}^2$.
(c) $\bar{D}$ is also a nonzero polynomial in the T_{ij} which implies condition (2).

(b) above also implies condition (3). (See [18] pages 23 to 31 for further discussion on the resultant.)

Remark 2.17. Note that for any specialization of the T_{ij} for which $R(x)$, D, and $\bar{D}$ become nonzero, then for that choice of g conditions (1), (2) and (3) will be met. Thus conditions (1), (2) and (3) are generic conditions on g.

(2.16 continued . . .) Condition (4) is also met. First of all, $g_x = t_{10} + 2t_{20}x + t_{11}y + \ldots$ and $g_y = t_{01} + 2t_{02}y + t_{11}x + \ldots$. Then $k[T_{ij}][x, y]/(g_x, g_y) = k[t_{00}, t_{20}, t_{11}, t_{02}, \ldots][x, y]$. Therefore g_x and g_y generate a prime ideal in $k[t_{ij}][x, y]$. By condition (1), the ideal generated by g_x and g_y in $k[t_{ij}][x, y]$ does not meet the multiplicatively closed set generated by the nonzero elements of $k[T_{ij}]$. Thus g_x and g_y generate a maximal ideal in $k(T_{ij})[x, y]$, implying condition (4). Therefore $Cl(A_g) \cong \mathbb{Z}/2\mathbb{Z}$ if $p = 2$ and $Cl(A_g) \cong 0$ or $\mathbb{Z}/p\mathbb{Z}$ if $p > 2$. (For $p \geqslant 5$ see (2.34)).

Question 2.18. Is condition (4) a generic condition on g?

Theorem 2.19. *Let g satisfy conditions (1)–(3). Let $(f(x)) = (g_x, g_y)F_g[x, y] \cap F_g[x]$. Suppose that $f(x)$ factors into a product of r-irreducible factors in $F_g[x]$. Then the order of $CL(A_g) \leqslant p^r$.*

Proof. Let $f(x) = f_1(x) \ldots f_r(x)$ be a factorization of $f(x)$ in $F_g[x]$ into prime factors. For each $i = 1, \ldots, r$, let α_i be a root of $f_i(x)$ in $\bar{F}$. For each i, there is a $\beta_i \in \bar{F}$ such that $(\alpha_i, \beta_i) \in S_g$. Let $\bar{\theta} : \mathscr{L}_g \to \oplus_{i=0}^r \mathbb{Z}/p\mathbb{Z}$ be defined by $\bar{\theta}(t) = (t(\alpha_i, \beta_i)/\sqrt{H(\alpha_i, \beta_i)})_{i=1}^r$. Let $t \in \ker \bar{\theta}$ and let $(\alpha, \beta) \in S_g$. Then $f_i(\alpha) = 0$ for some $i = 1, \ldots, r$. Therefore α is conjugate to α_i so that there exists an F_g-automorphism $\sigma : \bar{F} \to \bar{F}$ such that $\sigma(\alpha_i) = \alpha$. Then $\sigma(\alpha_i, \beta_i) = (\alpha, \beta)$. Since $t(\alpha_i, \beta_i) = 0$ this implies that $t(\alpha, \beta) = \sigma t(\alpha_i, \beta_i) = 0$. By (2.11) t is identically 0. Thus $\bar{\theta}$ is an injection. By (1.8), the order of $Cl(A_g) \leqslant p^r$.

REMARK 2.20. The ideal generated by $f(x)$ in (2.19) is identical to the ideal generated by the resultant, $R(x)$, of g_x and g_y with respect to x. This is because in this case, $R(x)$ is of degree equal to the number of elements in S_g. Since $R(x) \in (f(x))$ and $f(\alpha) = 0$ for each $(\alpha, \beta) \in S_g$, then $(R(x)) = (f(x))$. (See [15] p. 185.).

EXAMPLE 2.21. Let $F = GF(3)$ and $g = -y + xy + x^4 + y^4$. Then g satisfies conditions (1)–(3). Note that $(g_x, g_y)F_g[x, y] \cap F_g[x] = (x^9 - x + 1)F_g[x]$. It can be shown that the prime factorization of $x^9 - x + 1$ over $F_g = GF(3)$ is $x^9 - x + 1 = (x^3 - x + 1)(x^6 + x^4 + x^3 + x^2 - x - 1)$. Thus by (2.1) the class group of $F_g[x^3, y^3, g]$ is 0, $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Since $D(g_x)/g_x = 1$ is in $\mathscr{L}_g$, $Cl(A_g)$ is either $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

This calculation can be verified as follows. (1.3)–(1.6) are used to calculate $\mathscr{L}$, the logarithmic derivatives of D in $\bar{F}[x, y]$. Then $\mathscr{L}_g = \mathscr{L} \cap F_g[x, y]$. Thus $t \in \mathscr{L}$ if and only if $t = \alpha_{00} + \alpha_{10}x + \alpha_{01}y + \alpha_{20}x^2 + \alpha_{02}y^2$ where

$$\begin{aligned} \alpha_{00} + \alpha_{10} + \alpha_{20} &= \alpha_{00}^3, \\ -\alpha_{10} + \alpha_{20} &= \alpha_{10}^3, \\ -\alpha_{01} &= \alpha_{01}^3, \\ \alpha_{02} &= \alpha_{20}^3, \\ \alpha_{20} &= \alpha_{02}^3. \end{aligned} \tag{2.22}$$

By eliminating variables we find that $\alpha_{00}^{3^5} - \alpha_{00}^{3^4} + \alpha_{00}^{3^2} + \alpha_{00}^3 - \alpha_{00} = 0$ and that the rest of the α_{ij} depend on α_{00}. Therefore the order of $\mathscr{L}$ is 3^5. Also if $\alpha_{00}^3 = \alpha_{00}$ then all other $\alpha_{ij} = 0$. Thus $\mathscr{L}_g$ is of order 3 generated by $t = 1$.

2.23. For more details on how to explicitly calculate $\mathscr{L}$ the reader is referred to [9], [10], [11] and [12].

This next result refines the upper bound in (2.19) slightly.

COROLLARY 2.24. *Let g satisfy conditions (1)–(3). Let $(f(x)) = (g_x, g_y)F_g[x, y] \cap F_g[x]$. Let $f(x) = f_1(x)f_2(x) \ldots f_r(x)$ be a prime factorization of $f(x)$ in $F_g[x]$ such that for some $s = 1, \ldots, r$, $\deg f_1 + \deg f_2 + \ldots + \deg f_s > (n-1)(n-2)$ where $n = \deg(g)$. Then the order of $Cl(Ag) \leqslant p^s$.*

Proof. Uses the same type of argument used in (2.19) and the result of (2.9).

EXAMPLE 2.25. Let $F = GF(3)$, $g = xy + x^4 + y^4$. Then $g_x = y + x^3$, $g_y = x + y^3$ and $H = 1$. Then g satisfies (1)–(3). $f(x) = x^9 - x = (x^2 - x - 1)(x^2 + x - 1)(x^2 + 1)(x + 1)(x - 1)x$. By (2.24) the order of $Cl(A_g) \leqslant 3^4$.

This can be verified by direct computation of $\mathscr{L}_g$. One finds that $\mathscr{L}$ is of order 3^5 generated by 1, $x - y$, $ax - a^3y$, $x^2 + y^2$, $ax^2 + a^3y^2$ where $a \in GF(9) - GF(3)$. Thus, in fact, $\mathscr{L}_g$ and therefore $Cl(A_g)$ is of order 3^3.

REMARK 2.26. If g satisfies conditions (1)–(4), then $Cl(A_g) \cong \mathbb{Z}/2\mathbb{Z}$ if $p = 2$ and $Cl(A_g) = 0$ or $\mathbb{Z}/p\mathbb{Z}$ if $p > 2$. Example (2.15) shows that these conditions are not enough to insure that $Cl(A_g) = 0$ if $p > 2$. The next theorem adds one more condition, that appears to be not a generic one, that guarantees that $Cl(A_g) = 0$.

THEOREM 2.27. *Let g satisfy conditions (1) and (2). If for each* $(\alpha, \beta) \in S_g$, $\sqrt{H(\alpha, \beta)} \notin F_g(\alpha, \beta)$. *Then* $Cl(A_g) = 0$.

Proof. If $Cl(A_g) \neq 0$ then by (2.11) there exists $(\alpha, \beta) \in S_g$, $t \in \mathscr{L}_g$ such that $t(\alpha, b) = n\sqrt{H(\alpha, \beta)}$ for some $n \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Since $t \in F_g[x, y]$, this is a contradiction.

COROLLARY 2.28. *Let g satisfy conditions (1)–(4). Suppose also that no two elements of S_g have the same y-coordinate. If for some* $(\alpha, \beta) \in S_g$, $\sqrt{H(\alpha, \beta)} \notin F_g(\alpha)$ *then* $Cl(A_g) = 0$.

Proof. Let $(a, b) \in S_g$. Then there is an F_g-automorphism of $\bar{F}$ that maps (α, b) to (α, β). If $\sqrt{H(a, b)} \in F_g(a) = F_g(a, b)$ by (2.5), then $\sigma\sqrt{H(a, b)} \in F_g(\alpha)$. But $(\sigma\sqrt{H(a, b)})^2 = \sigma H(a, b) = H(\alpha, \beta)$. This implies that $\sigma\sqrt{H(a, b)} = \pm\sqrt{H(\alpha, \beta)} \in F_g(\alpha)$. A contradiction.

REMARK 2.29. There are two reasons why the hypothesis of (2.27) appears to be not a generic one. The first is that in calculations I found that this condition appears to hold about half the time. The second, and this might explain the first, is that for any finite field, $GF(p^m)$, $(p^m + 1)/2$ elements of it have a square root in $GF(p^m)$.

EXAMPLE 2.30. Let $p = 3$ and $g = x^2 + y^2$. Then $g_x = 2x$, $g_y = 2y$ and $H = 2$. The conditions of (2.27) are easily seen to hold. Therefore $Cl(A_g) = 0$. This is verified by the fact that $\mathscr{L}$ is of order three generated by $\sqrt{2} \notin F_g = GF(3)$.

REMARK 2.31. The next two results were proved by Blass [3]. Although in the introduction to his article Blass assumes that the degree of g is divisible by p, the proofs of these results are independent of this assumption.

LEMMA 2.32. *Let g be as in (2.16) and $p \geqslant 5$. Then the Galois group of $\overline{k(T_{ij})}/k(T_{ij})$ acts as the full symmetric group on S_g (see [3] page 10).*

LEMMA 2.33. *Let g be as in* (2.16) *and $p \leqslant 5$. Let $Q_1 \neq Q_2 \in S_g$. Then there exists an automorphism $\sigma \in Gal((\overline{k(T_{ij})}/k(T_{ij}))$ such that $\sigma(\sqrt{H(Q_1)}) = -\sqrt{H(Q_1)}$, $\sigma(\sqrt{H(Q_2)}) = -\sqrt{H(Q_2)}$, $\sigma\sqrt{H(Q)} = \sqrt{H(Q)}$ for all $Q \in S_g$ with $Q \neq Q_1, Q_2$ and such that σ act as the identity of S_g (see [3] page 10).*

EXAMPLE 2.34. Let $g = \Sigma T_{ij}x^iy^j$ be as in (2.16). Then the ring $A_g = k(T_{ij})[x^p, y^p, g]$ is factorial where $p \geqslant 5$. This result follows immediately from (2.27) and (2.33).

3. Properties of $Cl(A_g)$

REMARK 3.1. Before moving on to the main section of this article, some general facts about $Cl(A_g)$ should be mentioned. First of all, we have that if $A = \bar{F}[x^p, y^p, g]$, then $Cl(A_g)$ injects into $Cl(A)$. The simplest way to see this, is to observe that $Cl(A) \cong \mathscr{L}$, $Cl(A_g) \cong \mathscr{L}_g$ and that $\mathscr{L}_g \hookrightarrow \mathscr{L}$. Then any general statements that can be made about $Cl(A)$ concerning order, type, etc., can also be made about $Cl(A_g)$. In [11] the following results were proved for $Cl(A)$ which therefore also apply for $Cl(A_g)$.

THEOREM 3.2. *Let g satisfy conditions (1) and (2). Then $Cl(F_g)$ is a p-group of type $(p, \ldots, p)$ of order p^m, where $m \leqslant$ $\deg(g)(\deg(g) - 1)/2$ (see [11] page 397).*

THEOREM 3.3. *Let g satisfy conditions (1) and (2). For each positive integer n, let $A_g^{(n)} = F_g[x^{p^n}, y^{p^n}, g]$. Then,*
(a) *for each n, $Cl(A_g^{(n)})$ injects into $Cl(A_g^{(n+1)})$,*
(b) *for each n, $Cl(A_g^{(n)})$ is a p-group of type $(p^{i_1}, \ldots, p^{i_r})$* where each $i_j \leqslant n$,
(c) *the order of $Cl(A_g^{(n)}) = p^f$, where $f \leqslant$ $n(\deg(g))(\deg(g - 1)/2$ ([11] page 406).*

4. The main theorem

This section begins by presenting a new algorithm (see [12] page 247) for computing the divisor class group of a Zariski ring $A = k[x^p, y^p, g]$ defined over an algebraically closed field k of characteristic $p \neq 0$.

Then Theorem (4.14) proves that the ring $\overline{k(T_{ij})}[x^p, y^p, g]$, where $g = \Sigma T_{ij}x^iy^i$ is as in example (2.16), is factorial. P. Blass proved this result for the case $\deg(g) = 0 \pmod p$ in [3].

The algorithm and Theorem (4.14) are then combined to prove that for a generic g, the ring A is factorial.

4.1. Let k be an algebraically closed field of characteristic $p \neq 0$. Let $g \in k[x, y]$ satisfy condition (1). Then by (1.8), $Cl(k[x^p, y^p, g])$ is isomorphic to $\mathscr{L}$, the additive group of logarithmic derivatives of $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$ in $k[x, y]$. If $t \in k[x, y]$ is in $\mathscr{L}$ then by (1.8), $\deg(t) \leqslant n - 2$ where $n = \deg(g)$. Furthermore, t is in $\mathscr{L}$ if and only if $D^{p-1}t - ct = -t^p$ where $D^p = cD$. By (1.6) it follows that t is in $\mathscr{L}$ if and only if

(4.2) (a) $\nabla(G^r t) = 0$ for $r = 0, 1, \ldots, p - 2$, and

(b) $\nabla(G^{p-1}t) = t^p$, where $\nabla = \partial^{2p-2}/\partial x^{p-1}\partial y^{p-1}$.

Thus the elements of $\mathscr{L}$ can be determined in the following way.

Let $t = \Sigma_{0 \leqslant i+j \leqslant n-2}\alpha_{ij}x^iy^j$ be a polynomial in x and y with undetermined coefficients. Substitute t into (4.2a) and (4.2b) and compare coefficients.

When t is substituted into (4.2a) one obtains linear expressions in the α_{ij} with coefficients in k, say $l_s = 0$, $0 \leqslant s \leqslant m$ with m a nonnegative integer. When t is substituted into (4.2b) one obtains p-linear equations of the form $l_{ij}(\alpha) = \alpha_{ij}^p$, $0 \leqslant i + j \leqslant n - 2$, where $l_{ij}(\alpha)$ is a linear expression in the α_{ij} with coefficients in k.

Thus it is readily seen that $\mathscr{L}$ is isomorphic to the additive group of solutions to the p-linear system of equations

$$l_s = 0, 0 \leqslant s \leqslant n \quad \text{and} \quad l_{ij}(\alpha) = \alpha_{ij}^p, 0 \leqslant i + j \leqslant n - 2. \tag{4.3}$$

In [12] an algorithm for computing the number of solutions to a system such as (4.3) was described.

What follows is a description of another algorithm which better suits the purposes of this article.

Let $N = n(n - 1)/2$. let C be the coefficient matrix of the linear expressions l_{ij}, $0 \leqslant i + j \leqslant n - 2$. Then C is an N by N square matrix.

Assume first of all that $\det C \neq 0$. Then each linear expression l_s with $0 \leqslant s \leqslant m$ can be expressed as a linear combination of the l_{ij} with coefficients in k. Thus beginning with l_1 there exists a_{ij}, $0 \leqslant i + j \leqslant N$ such that $\Sigma a_{ij}l_{ij} = l_1$. Since $l_1(\alpha) = 0$, this leads to $\Sigma a_{ij}\alpha_{ij}^p = 0$, which results in the linear equation $l_1' : \Sigma a_{ij}^{(1/p)}\alpha_{ij} = 0$. Thus for each s, $0 \leqslant s \leqslant m$, another linear equation l_s', $0 \leqslant s \leqslant m$, is produced. From these $2m$ linear equations, choose a basis l_1'', l_2'', $\ldots$, l_u'' where $0 \leqslant u \leqslant 2m$. Now repeat the first step of generating linear equations by writing each l_s'', $0 \leqslant s \leqslant u$, as a linear combination of the l_{ij}. From these $2u$ linear equations, choose a basis and continue this process. One of two possibilities will take place. One, is that at some point N independent linear equations will be produced in N unknowns. If this is the case then each $\alpha_{ij} = 0$ which implies that $\mathscr{L} = 0$.

The alternative to this situation is that at some point R linearly independent equations will be produced and no more than that, with $R < N$. Any new equations produced will be a linear combination of these R independent equations. If this is the case then the number of solutions to the system (4.3) is p^{N-R}. To see this, choose $N - R$ p-linear expressions from the equations $l_{ij} = \alpha_{ij}^p$ so that the linear part of these equations together with the R linear equations form a k-basis for the space of all linear expressions in the α_{ij} with coefficients in k. This can be done since the l_{ij} are a basis for this space. It then follows that the system of equations consisting of these R linear and $N - R$ p-linear equations is equivalent to the original system (4.3). For if $l_{cd} = \alpha_{cd}^p$ is one of the p-linear equations in (4.3) then l_{cd} is a linear combination of the linear expressions in the $N - R$ p-linear equations and the R constructed linear equations. It then follows that α_{cd}^p is a linear combination of the α_{ij}^p that appear in the $N - R$ p-linear equations. This of course leads to another linear equation after taking p-th roots which must by assumption be dependent on the P linear expressions. It then follows from Bezout's theorem that there are p^{N-R} solutions (see 4.4) below).

If it turns out that det $C = 0$, where C is the coefficient matrix of the linear expressions l_{ij} in (4.3), than the rank of $C = N - M$ for some $M > 0$. Therefore from the equations $l_{ij} = \alpha_{ij}^p$, $0 \leqslant i + j \leqslant n - 2$, one can immediately generate M linear equations. These M linear equations are then combined with the m linear equations $l_s = 0$, $0 \leqslant s \leqslant m$, and a basis for the linear equations is chosen. At this point there are $N - M$ p-linear equations whose linear parts are linearly independent and some linearly independent linear equations. If these linear expressions (from the $N - M$ p-linear equations and the linear equations) are dependent then some nontrivial linear combinations of these expressions are 0. As above, these combinations will produce nontrivial homogeneous linear equations. A basis for the linear equations is then chosen and combined with the p-linear equations to form a system that is equivalent to the original system (4.3). This process is repeated until one of two possibilities occurs. Either N independent linear equations will be produced in which case $\mathscr{L} = 0$ or R linearly independent linear equations will be produced where $R < N$ and where the linear expressions from the p-linear equations and the R linear equations cannot be used to produce any new linear equations that are independent from the existing linear homogeneous equations. If this is the case then $\mathscr{L}$ is of order p^{N-R}. To see this consider the k-vector space spanned by the linear expressions in these p-linear equations and in the R linearly independent homogeneous linear equations. Then a basis for this space can be constructed that includes the R linearly independent linear equations. Then arguing as above one sees that the system of equations consisting of the R linear equations and those p-linear equations used to construct the basis is equivalent to the system (4.3). This equivalent system must consist of a total of N equations otherwise there would be more unknowns than equations and hence an infinite number of solutions, which would imply that $\mathscr{L}$ is infinite. This contradicts (3.1). Therefore an equivalent system of $N - R$ p-linear and R linear equations in N unknowns has been constructed with these properties that are easy to verify:

(4.4) (a) There are no intersections at infinity, and

(b) The multiplicity of each point of intersection is one.

Then by Bezout's theorem the total number of intersection points is p^{N-R}.

This then is the algorithm for determining the order of $\mathscr{L}$.

REMARK 4.5. Although this algorithm is much more clumsy than the algorithm in [12] for computing the divisor class group of $A = k[x^p, y^p, g]$, it proves very useful in determining $Cl(A)$ for a generic g.

EXAMPLE 4.6. Let k be an algebraically closed field of characteristic 3 and $g = x + y + x^5 + y^5$. Applying this algorithm one finds that $Cl(A)$ is isomorphic to the additive group of solutions to the system

$$\begin{aligned} -\alpha_{20} + \alpha_{11} - \alpha_{02} &= -\alpha_{00}^3, \\ \alpha_{01} &= -\alpha_{10}^3 \\ \alpha_{10} &= -\alpha_{01}^3 \\ \alpha_{00} &= -\alpha_{11}^3 \\ -\alpha_{12} &= -\alpha_{30}^3 \\ \alpha_{30} &= -\alpha_{21}^3 \\ \alpha_{03} &= -\alpha_{12}^3 \\ -\alpha_{21} &= -\alpha_{03}^3 \end{aligned} \tag{4.7}$$

$$l_1 : \alpha_{12} + \alpha_{21} = 0$$
$$l_2 : \alpha_{02} = 0$$
$$l_3 : \alpha_{20} = 0.$$

This system is easily seen to be equivalent to the system

$$\begin{aligned}
\alpha_{11} &= \alpha_{00}^3, \quad \alpha_{12} = \alpha_{30}^3 \\
\alpha_{01} &= -\alpha_{10}^3, \quad \alpha_{30} = -\alpha_{21}^3 \\
\alpha_{10} &= -\alpha_{01}^3, \quad \alpha_{21} = -\alpha_{03}^3 \qquad (4.8) \\
l_1 : \alpha_{12} + \alpha_{21} &= 0
\end{aligned}$$

In the first step of the algorithm (with det $C \neq 0$) one obtains the linear equations

$$l_1 : \alpha_{12} + \alpha_{21} = 0 \quad \text{and} \quad l_2 : \alpha_{30} + \alpha_{03} = 0 \qquad (4.9)$$

In the next step no new independent equations are produced. Thus the order of $Cl(A)$ is $p^{8-2} = 3^6$.

The most important application of this algorithm is the next result.

THEOREM 4.10. *Let k be an algebraically closed field of characteristic $p \neq 0$, $n \geqslant 4$ be a positive integer, $\{T_{ij} : 0 \leqslant i + j \leqslant n\}$ be a set of indeterminates over k, $F = k(T_{ij})$ and $g = \Sigma_{0 \leqslant i+j \leqslant n} T_{ij} x^i y^j$. If $Cl(\overline{k(T_{ij})}[x^p, y^p, h]) \cong 0$ then $Cl(k[x^p, y^p, \tilde{g}]) \cong 0$ for a generic choice of coefficients $a_{ij} \in k$ of $\tilde{g} = \Sigma_{0 \leqslant i+j \leqslant n} a_{ij} x^i y^j$.*

Proof. Assume that $Cl(\overline{k(T_{ij})}[x^p, y^p, g])$ is 0. When the algorithm in (4.1) is applied to g, we arrive at the system of equations (4.3) consisting of p-linear and linear equations with coefficients in the polynomial ring $GF(p)[T_{ij}]$. In the next step of the algorithm additional linear equations are generated, this time with coefficients in $[GF(p)(T_{ij})]^{(1/p)}$ where for a field L of characteristic $p \neq 0$, $L^{(1/p^n)}$ is the field of all elements $\alpha \in I$ such that $a^{p^n} \in L$. In the m-th step, more linear homogeneous equations are generated with coefficients in the field $[GF(p)(T_{ij})]^{(1/p^m)}$. The class group of $\overline{k(T_{ij})}\ [x^p, y^p, g]$ is trivial if and only if eventually N linearly independent homogeneous linear equations in N unknowns are generated by this algorithm, $N = (n - 1)n/2$. That is, if and only if N homogeneous linear equations in N unknowns are generated with coefficient matrix B such that $\det(B) \neq 0$. Note that $\det(B) \in [GF(p)$

$(T_{ij})]^{(1/p^s)}$ for some positive integer s. Therefore $(\det(B))^{p^s} \in GF(p)(T_{ij})$ and $\det B \neq 0$ if and only if $(\det(B))^{p^s} \neq 0$.

Thus if the class group of $\overline{k(T_{ij})}[x^p, y^p, g]$ is 0 and $a_{ij} \in k$ is any specialization of g such that $(\det(B))^{p^s}$ is defined and nonzero then the same sequence of steps that led to the construction of N linearly independent homogeneous linear equations in N unknowns will also do the same for $\tilde{g} = \Sigma a_{ij} x^i y^j$, which proves the theorem.

REMARK 4.11. Another proof of (4.10) was given by Blass and Lang in [4], but an error was discovered by the authors in that proof (see [4], pages 36–39).

REMARK 4.12. Although the next result may have application only to the $p = 2$ or 3 case by virtue of (4.14), the proof of it easily follows the same line of argument used in (4.10).

THEOREM 4.13. *Let k, g and $\tilde{g}$ be as in (4.10). If the order of $Cl(k(T_{ij})[x^p, y^p, g])$ is p^r for some r, then the order of $Cl(k[x^p, y^p, \tilde{g}])$ is p^r for a generic $\tilde{g} \in k[x, y]$.*

THE MAIN THEOREM 4.14. *Let k be an algebraically closed field of characteristic $p \geqq 5$, $n \geqslant 4$ a positive integer, $\{T_{ij} : 0 \leqq i + j \leqq n\}$ be a set of indeterminates over k, $F = k(T_{ij})$, $g = \Sigma T_{ij} x^i y^j$ and $A = \bar{F}[x^p, y^p, g]$. Then $Cl(A) = 0$.*

Proof. By (2.11) and (2.16) the map $\Phi : \mathscr{L} \to \oplus_{Q \in S_g} \mathbb{Z}/p\mathbb{Z} \cdot \sqrt{H(Q)}$ defined by $\Phi(t) = (t(Q))_{Q \in S_g}$ is an injection. From (2.33) it follows that the elements $\sqrt{H(Q)}$, $Q \in S_g$, are independent over the prime subfield of k. Therefore each element of t can be uniquely identified with a sum $\Sigma_{Q \in S_g} n_Q \sqrt{H(Q)}$ where $0 \leqslant n_Q < p$ for each Q.

Suppose that $t \in \mathscr{L}$ and let $t = \Sigma n_Q \sqrt{H(Q)}$. Consider two cases.

Case 1. $n = \deg(g) \neq 0((\mathrm{mod}\ p))$.

Let $Q', Q'' \in S_g$. By (2.3) there exists $\sigma \in \mathrm{Gal}\,(\bar{F}/F)$ such that $\sigma\sqrt{H(Q')} = -\sqrt{H(Q')}$, $\sigma\sqrt{H(Q'')} = -\sqrt{H(Q'')}$, $\sigma\sqrt{H(Q)} = \sqrt{H(Q)}$ if $Q \neq Q', Q''$ and σ acts as the identity on the elements of S_g.

Since $t \in \mathscr{L}$ it follows that $\sigma(t) \in \mathscr{L}$, which implies that $t - \sigma(t) = 2(n_{Q'}\sqrt{H(Q')} + n_{Q''}\sqrt{H(Q'')}) \in \mathscr{L}$. Thus $(t + \sigma(t))(Q) = 0$ for al $Q \neq Q'$, Q''. By (2.10) this implies that $t - \sigma(t) \equiv 0$. Thus $n_{Q'} = n_{Q''} = 0$. Since Q' and Q'' are arbitrary it follows that $t \equiv 0$.

Case 2. $n = \deg(g) = 0 \pmod p$.

Let t, Q', Q'', be as in case 1. Then $t' = n_{Q'}\sqrt{H(Q')} + n_{Q''}\sqrt{H(Q'')} \in \mathscr{L}$. Let $Q \neq Q', Q''$ belong to S_g. By (2.33) there exists $\bar\sigma \in \mathrm{Gal}\,(\bar F/F)$ such that $\bar\sigma\sqrt{H(Q')} = -\sqrt{H(Q')}$, $\bar\sigma\sqrt{H(Q)} = -\sqrt{H(Q)}$, $\bar\sigma\sqrt{H(Q'')} = \sqrt{H(Q'')}$ and $\bar\sigma$ is the identity on S_g. Then $t' - \bar\sigma t' = 2n_{Q'}\sqrt{H(Q')} \in \mathscr{L}$. If $n_{Q'} \neq 0$, then by (2.32) there exists for each $Q \in S_g$ a $t_Q \in \mathscr{L}$ such that $t_Q(Q) \neq 0$ and t_Q is 0 at every other element of S_g. The t_Q's would necessarily be independent over $\mathbb{Z}/p\mathbb{Z}$, contradicting (3.2). Therefore $n_{Q'} = 0$. Since Q' is arbitrary, $t \equiv 0$.

Thus $\mathscr{L} = 0$.

The main result of this article now follows as a corollary to (4.10) and (4.14).

THE MAIN RESULT (4.15). *Let k be a field of characteristic $p \geqslant 5$, $g \in k[x, y]$ be of degree at least* 4 *and $A = k[x^p, y^p, g]$. Then for a generic g the ring A is factorial.*

REMARK 4.16. For an alternate proof of case 2 of Theorem (4.14) see [3].

5. On finding $\mathscr{L}$

5.1. In [1] an algorithm and computer program was given for calculating the order and type of $\mathscr{L}$, the group of logarithmic derivatives of $D = g_y(\partial/\partial x) - g_x(\partial/\partial y)$ in $k[x, y]$, where the coefficients of g are in $GF(p^m)$ for some m. An algorithm for calculating the actual elements of $\mathscr{L}$ was not given, partly because it could not be found in what finite field are the coefficients of the elements of $\mathscr{L}$. The next result answers this question.

THEOREM 5.2. *Let $g \in GF(p^m)$ for some m and k be an algebraic closure of $GF(p^m)$. If $t \in \mathscr{L}$, then $t \in F_g(\{\alpha, \beta, \sqrt{H(\alpha, \beta)} : (\alpha, \beta) \in S_g\})$, the field extension of F_g obtained by adjoining all α, β, $\sqrt{H(\alpha, \beta)}$ for $(\alpha, \beta) \in S_g$ to F_g.*

Proof. Let $K = F_g(\{\alpha, \beta, \sqrt{H(\alpha, \beta)} : (\alpha, \beta) \in S_g\})$. Let E be the field extension of K obtained by adjoining the coefficients of the elements of $\mathscr{L}$ to K. Then K and E are finite fields with E algebraic over K, hence separable over K (see [14] pages 63 and 64). Let σ be a K-injection of E into k. Then σ can be extended to form a $K[x, y]$-injection of $E[x, y]$ into $k[x, y]$ by letting $\sigma(\Sigma a_{ij}x^iy^j) = \Sigma\sigma(a_{ij})x^iy^j$.

If $t \in \mathscr{L}$ then by (1.4), $D^{p-1}t - ct = -t^p$. It follows that $D^{p-1}(\sigma t) - c\sigma(t) = -(\sigma(t))^p$. Thus $\sigma(t) \in \mathscr{L}$. By (2.8), for all $(\alpha, \beta) \in S_g$ and $t \in \mathscr{L}$, there exists $r \in \mathbb{Z}/p\mathbb{Z}$ such that $t(\alpha, \beta) = r\sqrt{H(\alpha, \beta)}$. Therefore for all such $(\alpha, \beta) \in S_g$, $\sigma(t)(\alpha, \beta) = \sigma(t(\alpha, \beta)) = \sigma(r\sqrt{H(\alpha, \beta)}) = r\sqrt{H(\alpha, \beta)} = t(\alpha, \beta)$.

Then $\sigma(t) - t \in \mathscr{L}$ and $(\sigma(t) - t)(\alpha, \beta) = 0$ for all $(\alpha, \beta) \in S_g$. By (2.10) $\sigma(t) - t \equiv 0$. Hence there is but one K-injection of E into k which implies that $[E:K] = 1$ ([14] page 65).

The reader is left with some open problems. Among them are:

(5.3) What is $Cl(k[x^p, y^p, g])$ for a generic choice of g if $p = 2$ or 3?

(5.4) Is condition (4) of (2.13) a generic condition?

(5.5) How does the order of $Cl(k[x^p, y^p, g])$ stratify the coefficient space of g? For example, for $p > 3$, we saw that on a subset of the coefficient space of g of codimension 0 this order is p^0. What then is the relationship between p^s for $s = 0, 1, 2, \ldots$ and the codimension of the subset of the coefficient space of g consisting of those $g \in k[x, y]$ such that the order of $Cl(k[x^p, y^p, g])$ is p^s?

(5.6) Is $k[x^{p^n}, y^{p^n}, g]$ factorial for a generic g?

(5.7) The author gratefully acknowledges the many insightful conversations with Professors Piotr Blass, Michael Fried and William Heinzer.

References

1. P. Blass: Zariski Surfaces. *Dissertations Mathematicae* 200 (1980).
2. P. Blass: Some geometric applications of a differential equation in characteristic $p > 0$ to the theory of algebraic surfaces. *Contemp. Math.* A.M.S. 13 (1982).
3. P. Blass: Picard groups of Zariski Surfaces I. *Comp. Math.* 54 (1985) 3–86.
4. P. Blass and J. Lang: Picard groups of Zariski Surfaces II. *Comp. Math.* 54 (1985) 36–39.
5. R. Fossum: *The Divisor Class Group of a Krull Domain.* Springer-Verlag, New York (1973).
6. H.W. Gould: *Combinatorial Identities.* Morgantown, W. Va (1972).
7. R. Hartshorne: *Algebraic Geometry.* Springer-Verlag, New York (1977).
8. I. Kaplansky: *Commutative Rings.* Allyn and Bacon, Boston (1970).
9. J. Lang: An example related to the affine theorem of Castelnuovo. *Michigan Math. J.* 28 (1981).
10. J. Lang: The divisor classes of the hypersurfaces $z^{p^n} = G(x_1, \ldots, x_m)$ in characteristic $p > 0$. *Trans A.M.S.* 278 2 (1983).
11. J. Lang: The divisor class group of the surface $z^{p^n} = G(x, y)$ over fields of characteristic $p > 0$. *J. Alg.* 84, 2 (1983).
12. J. Lang: The divisor classes of the surface $z^p = G(x, y)$, a programmable problem. *J. Alg.* 100, (1986).
13. J. Lang: Locally factorial generic Zariski surfaces are factorial. *J. Alg.*, to appear.
14. M. Nagata: *Local Rings.* John Wiley & Sons, Inc. (1962).
15. M. Nagata: *Field Theory.* Marcel Dekker, Inc. (1977).
16. Stohr and Voloch: *A formula for the Cartier operator on plane algebraic curves.* Submitted for publication.
17. P. Samuel: *Lectures on Unique Factorization Domains. Tata Lecture Notes* (1964).
18. R. Walker: *Algebraic Curves.* Princeton University Press, Princeton, (1950).