Ulam Quarterly — Volume 2, Number 1, 1993

Some Questions on Unique Factorization

Piotr Blass
Department of Mathematics
Palm Beach Atlantic College
West Palm Beach, FL 33402

Joseph Blass
Department of Mathematics
Bowling Green State University
Bowling Green, OH 43403

Jeffrey Lang
Department of Mathematics
University of Kansas
Lawrence, KS 66045

The simplest type of integral extension of a unique factorization domain B is obtained by adjoining to B an n-th root of one of its elements; that is, by forming the ring $B_n = B[z]/(z^n - g)$, where $n \in \mathbb{Z}^+$ and $g \in B$. When $n = 1$, $B_n = B$. When $n \geq 2$ it is natural to ask for what $g \in B$ will unique factorization be preserved? The case where B is a polynomial ring over an algebraically closed field k immediately comes to mind. In the one variable case we have a definitive answer: B_n is factorial if and only if $g \in B = k[x]$ is linear; for if $\deg(g) \geq 2$ then g factors completely in B as a product of linear factors and in B_n g will have two distinct factorizations.

With more variables the issue becomes more cloudy. This paper concentrates on the two variable case so that our principal question is

0.1. Question. *For what $g \in k[x,y]$, will $B_n = k[x,y,z]/(z^n - g)$ be a unique factorization domain?*

The one variable case suggests that the answer may be that if g is irreducible in $k[x,y]$ then B_n will be factorial, but the following example shows that this is not enough.

0.2. Example. Assume $\operatorname{char}(k) = p \neq 0$ and let $g = xy + x^{p+1} + y^{p+1}$. Then B_p is not factorial since $(z + xy)^p = (x + y^{p+1})(y + x^{p+1})$ is a non-unique factorization in B_p.

There are similar examples in characteristic 0.

Perhaps g in (0.2) is not irreducible enough; what if g is in some sense very irreducible? A generic g is about as irreducible as we can think of. We say that $g = \sum \alpha_{ij} x^i y^j \in k[x,y]$ of degree d is *generic* if the set of coefficients $\{\alpha_{ij} : 0 \leq i+j \leq d\}$ is algebraically independent over the prime subfield of k. Thus we obtain the following conjecture.

0.3. Conjecture. *If $g \in k[x,y]$ is generic and deg(g) ≥ 4, then for all $n \in \mathbb{Z}^+$, B_n is a unique factorization domain.*

This conjecture is partly motivated by the classical result of Max Noether [4], which was extended to all characteristics by Deligne [2]: a generic surface of degree ≥ 4 in projective 3-space has infinite cyclic divisor class group (see [5, pp. 130–131] for a definition of divisor class group). When R is a Krull domain, R is factorial if and only if the divisor class group of Spec R is 0.

For each $n \in \mathbb{Z}^+$ let $X_n = \operatorname{Spec} B_n \subseteq \mathbb{A}^3_k$ and denote the divisor class group of X_n by $\mathrm{Cl}(X_n)$. Then (0.3) becomes

0.4. Conjecture. *If g is generic and $\deg(g) \geq 4$, then $\mathrm{Cl}(X_n) = 0$ for all $n \in \mathbb{Z}^+$*

Note that $\mathrm{Cl}(X_n) = 0$ if and only if every curve on X_n is a complete intersection.

The following results summarize the progress we've made so far on (0.4) when $\mathrm{char}(k) = p > 2$. Here and throughout the rest of the paper $g \in k[x,y]$ is generic of degree ≥ 4.

0.5. Theorem. *If $m \in \mathbb{Z}^+$ such that $\gcd(p,m) = 1$ and $\mathrm{Cl}(X_m) = 0$, then $\mathrm{Cl}(X_{p^r m}) = 0$ for all $r \in \mathbb{Z}^+$.*

0.6. Corollary. *If $n = p^s$ for some $s \in \mathbb{Z}^+$, then $\mathrm{Cl}(X_n) = 0$*

0.7. Corollary. *$\mathrm{Cl}(X_n) = 0$ for all n if and only if $\mathrm{Cl}(X_n) = 0$ for all n relatively prime to p.*

(0.7) is an obvious corollary of (0.5) and (0.6) is a consequence of (0.5) and the fact that $B_1 \cong k[x,y]$. In the next section we outline the proof of (0.5). We simply mention here that when $p = 2$, $\mathrm{Cl}(X_{2^s}) \cong \mathbb{Z}/2\mathbb{Z}$ for all $s \in \mathbb{Z}^+$ (see [7, pp. 359–360]). This leads us to reformulate (0.4).

0.8. Conjecture. *If g is generic of degree ≥ 4, then $\mathrm{Cl}(X_n) = 0$ for all n if $\mathrm{char}(k) \neq 2$.*

1. Radical Descent

If A is a Krull domain of characteristic $p \neq 0$ and $\Delta : A \to A$ is a derivation with kernel B, then B is a Krull domain and A is integral over

B. If the degree of the field of fractions of A over the field of fractions of B is $p \neq 0$ and $\Delta(A)$ is not contained in any height one prime of A then

(1.1) (a) there is a group homomorphism $\phi : \mathrm{Cl}(\mathrm{Spec}\, B) \to \mathrm{Cl}(\mathrm{Spec}\, A)$ such that $\ker \phi$ is isomorphic to the quotient $\mathcal{L}/\mathcal{L}'$ of the additive groups $\mathcal{L} = \{t^{-1}\Delta t \ : \ t \text{ and } t^{-1}\Delta t \in A\}$ and $\mathcal{L}' = \{u^{-1}\Delta u \ : \ u \in A^*\}$;

(b) there is a $b \in B$ such that $\Delta^p = b\Delta$;

(c) an element x of A belongs to $\mathcal{L}$ if and only if

$$\Delta^{p-1}x - bx + x^p = 0.$$

(See [8, pp. 62–64].)

1.2. Proposition. *Let D be the derivation on $k(x,y)$ defined by* $D = g_y \dfrac{\partial}{\partial x} - g_x \dfrac{\partial}{\partial y}$. *Then*

(a) $\ker D \cap k[x,y] = k[x^p, y^p, g] \cong B_p$;

(b) $\mathrm{Cl}(\mathrm{Spec}\, B_p)$ *is isomorphic to* $\mathcal{L}_0 = \{t^{-1}Dt \ : \ t \text{ and } t^{-1}Dt \in k[x,y]\}$;

(c) there exists $a_0 \in k[x^p, y^p, g]$ such that $D^p = a_0 D$ and $\deg(a_0) \leq (p-1)(\deg(g) - 2)$. ([6, pp. 616–622])

1.3. Discussion. Let $\mathcal{S} = \{Q \in k^2 \ : \ g_x(Q) = g_y(Q) = 0\}$. The cardinality of $\mathcal{S}$ is $(\deg(g)-1)^2$ when $\deg(g) \not\equiv 0 \pmod p$ and $(\deg(g))^2 - 3\deg(g) + 3$ otherwise ([6, pp. 287–288]). A simple application of Bezout's theorem yields that if $t \in k[x,y]$, then the number of $Q \in \mathcal{S}$ such that $t(Q) = 0$ can not exceed $\deg(t)(\deg(g)-1)$. In particular, if $t(Q) = 0$ for all $Q \in \mathcal{S}$ then $\deg(t) > \deg(g) - 2$ or $t = 0$.

1.4. Notation. The derivation D in (1.2) extends to a derivation on $k(x,y,z)$ with $D(z) = 0$. Since $D(z^n - g) = 0$, D induces a derivation on B_n which we denote by D_n. Let $\mathcal{L}_n = \{u^{-1}D_n u \ : \ u \text{ and } u^{-1}D_n u \in B_n\}$ and $\mathcal{L}'_n = \{u^{-1}D_n u \ : \ u \in B_n^*\}$. Then B_{np} is isomorphic to $\ker D_n \cap B_n$ and by (1.1) there is a group homomorphism $\phi_n : \mathrm{Cl}(X_{np}) \to \mathrm{Cl}(X_n)$ with $\ker(\phi_n) \cong \mathcal{L}_n/\mathcal{L}'_n$.

1.5. Proposition. *Let* $t = \sum_{i=0}^{n-1} t_i z^i \in B_n$, *where* $t_i \in k[x,y]$, $0 \leq i \leq n-1$. *For each i let* $J(i) = \{j \ : \ 0 \leq j < n \text{ and } pj \equiv i \pmod n\}$. *Then $t \in \mathcal{L}_n$ if and only if for each i,* $0 \leq i < n$,

$$D^{p-1}t_i - a_0 t_i = - \sum_{j \in J(i)} t_j^p g^{(pj-i)/n},$$

where a_0 is as in (1.2(c)).

Proof. By (1.1), $t \in \mathcal{L}_n$ if and only if $D_n^{p-1}t - a_0 t = -t^p$, which holds if and only if $\sum_i \left(D^{p-1}t_i - a_0 t_i\right) z^i = -\sum_i t_i^p z^{ip}$. Since $1, z, \ldots, z^{n-1}$, is a basis for the field of fractions of B_n over $k(x,y)$ and since $z^n = g$ in B_n, we obtain the conclusion by comparing powers of z on both sides of the above equation. □

1.6. Lemma. *Let* $t = \sum_{i=0}^{n-1} t_i z^i \in B_n$, *where* $t_i \in k[x,y]$, $0 \le i < n$. *If* $t \in \mathcal{L}_n$, *then* $\deg(t_i) \le \deg(g) - 2$ *for each* i.

Proof. We consider the case $\deg(g) \ne 0 \pmod p$; the other case is similar. Let r be such that $\deg(t_r) \ge \deg(t_i)$ for each i. We have $pr = nq + s$ for $q, s \in \mathbb{Z}$ with $q \ge 0$, $0 \le s < n$. By (1.5), $D^{p-1}t_s - a_0 t_s = -t_r^p g^q$. By (1.2), $\deg(a_0) \le (p-1)(\deg(g) - 2)$. A simple induction shows that

$$\deg\left(D^{p-1}t_s\right) \le \deg(t_s) + (p-1)(\deg(g) - 2).$$

Thus

$$p\deg(t_r) \le \deg\left(D^{p-1}t_s - a_0 t_s\right) \le \deg(t_s) + (p-1)(\deg(g) - 2) \le$$

$$\le \deg(t_r) + (p-1)(\deg(g) - 2).$$

Hence $\deg(t_r) \le \deg(g) - 2$. □

1.7. Theorem. *Let* $H = g_{xx}g_{yy} - g_{xy}^2$, *the hessian of* g. *For each* $Q \in \mathcal{S}$ *let* $\sqrt{H(Q)}$ *denote a fixed root of the equation* $T^2 = H(Q)$. *Then* $a_0(Q) = \left(\sqrt{H(Q)}\right)^{p-1}$ *for each* $Q \in \mathcal{S}$. ([3, Theorem 1.5])

1.8. Lemma. *Suppose* $n = pm$, *where* $m, n, p \in \mathbb{Z}^+$. *Then the composition* $B_m \xrightarrow{\cong} k[x,y,z^p]/(z^n - g) \hookrightarrow B_n$ *maps* $\mathcal{L}_m$ *isomorphically onto* $\mathcal{L}_n$.

Proof. Let $t = \sum_{i=0}^{n-1} t_i z^i \in \mathcal{L}_n$ where $t_i \in k[x,y]$. By (1.5), $\gcd(i,p) = 1$ implies $D^{p-1}t_i = a_0 t_i$. Then for each $Q \in \mathcal{S}$, $0 = \left(D^{p-1}t_i\right)(Q) = a_0(Q)t_i(Q)$. For a generic g, $H(Q) \ne 0$ for all $Q \in \mathcal{S}$. By (1.3), (1.6) and (1.7), $t_i = 0$ whenever $\gcd(i,p) = 1$. Thus $t \in k[x,y,z^p]/(z^n - g) \cong B_m$. Therefore the isomorphism $B_m \to k[x,y,z^p]/(z^n - g)$ maps $\mathcal{L}_m$ onto $\mathcal{L}_n$.□

1.9. Discussion. Assume $m \in \mathbb{Z}^+$ and $\gcd(p,m) = 1$. We need to study the action of $\mathcal{G} = \mathrm{Gal}(k, \mathbb{F}_p(\alpha_{ij}))$ on $\mathcal{S}$ (recall $g = \sum \alpha_{ij}x^iy^j$). Let N denote the cardinality of $\mathcal{S}$. Let $\mathcal{S}_m = \{(\alpha,\beta,\gamma) \in k^3 \ : \ (\alpha,\beta) \in \mathcal{S} \text{ and } \gamma^m = g(\alpha,\beta)\}$. Since g is generic $g(Q) \ne 0$ for all $Q \in \mathcal{S}$. Then $\mathcal{S}_m$ consists of mN points which we can list as Q_{ij}, $1 \le i \le N$, $1 \le j \le m$, in such a way that if $Q_{ij} = (\alpha,\beta,\gamma)$, then $(\alpha,\beta) = Q_i$.

Let ω be a primitive m-th root of unity in k and π the $k(x,y)$-automorphism on $k(x,y,z)$ defined by $\pi(z) = \omega z$. Then π induces an automorphism on B_m and let $T : B_m \to k[x,y]$ denote the trace map. Since each

$Q_{ij} \in X_m$ we may define $t(Q_{ij})$ for $t \in B_m$ by evaluating any preimage of t in $k[x, y, z]$ at Q_{ij}. Observe that if i is fixed and $t(Q_{ij}) = 0$ for each j, then $[T(t)](Q_{ij}) = 0$ for each j, which yields $[T(t)](Q_i) = 0$.

Now $t = \sum_r t_r z^r$ for unique $t_r \in k[x, y]$, $0 \leq r < m$. If s is a non negative integer less than m, then $t(Q_{ij}) = 0$ for each j implies $(z^{m-s}t)(Q_{ij}) = 0$ for each j, which we just saw implies

$$0 = [T(z^{m-s}t)](Q_i) = (mz^m t_s)(Q_i) = mg(Q_i)t_s(Q_i),$$

and hence $t_s(Q_i) = 0$ for each s. We summarize this in a lemma.

1.10. Lemma. *Assume* $\gcd(p, m) = 1$ *and* $t = \sum_{r=0}^{m-1} t_r z^r \in B_m$. *If for a fixed* i, $t(Q_{ij}) = 0$ *for each* j, *then* $t_r(Q_i) = 0$ *for each* r.

1.11. Lemma. *Assume* $\gcd(p, m) = 1$. *For each* $t \in \mathcal{L}_m$ *and* $Q_{ij} \in \mathcal{S}_m$ *there exists* $r_{ij} \in \mathbb{F}_p$ *such that* $t(Q_{ij}) = r_{ij}\sqrt{H(Q_i)}$. *Furthermore, the map* $\theta : \mathcal{L}_m \to \bigoplus_{i,j} \mathbb{F}_p \cdot \sqrt{H(Q_{ij})}$ *defined by* $\theta(t) = (t(Q_{ij}))$ *is an injection of additive groups.*

Proof. Given $t \in \mathcal{L}_m$, $D_m^{p-1}t - a_0 t = -t^p$ by (1.1). Evaluate both sides of this equality at Q_{ij} we obtain $a_0(Q_i)t(Q_{ij}) = t^p(Q_{ij})$. By (1.7) we obtain the first assertion. The second one follows by (1.3), (1.6) and (1.10). □

1.12. Theorem. *Let* $\mathcal{G} = \mathrm{Gal}(k, \mathbb{F}_p(\alpha_{ij}))$. *Then* $\mathcal{G}$ *acts on* $\mathcal{S}$ *as the full symmetric group. Furthermore, for each pair* $Q', Q'' \in \mathcal{S}$, *there exists a* $\sigma \in \mathcal{G}$ *such that* σ *acts as the identity on* $\mathcal{S}$ *and*

$$\sigma(\sqrt{H(Q)}) = \begin{cases} -\sqrt{H(Q)}, & Q = Q', Q'' \\ \sqrt{H(Q)}, & \textit{otherwise}. \end{cases}$$

([1, p. 297] *and* [3, p. 354])

1.13. Lemma. *Assume* $\gcd(p, m) = 1$. *Then* $\mathcal{L}_m = 0$.

Proof. Let $t \in \mathcal{L}_m$ and suppose $t \neq 0$. Assume $\theta(t) = \left(r_{ij}\sqrt{H(Q_i)}\right)$. Given $\sigma \in \mathcal{G}$, $\sigma(t) \in \mathcal{L}_m$ and the action of σ on t is compatible with the action of σ on $\theta(t)$. By (1.12), there are $\sigma', \sigma'' \in \mathcal{G}$ such that

$$\sigma'(\sqrt{H(Q)}) = \begin{cases} -\sqrt{H(Q_i)}), & i = 1, 2 \\ \sqrt{H(Q_i)}, & \text{otherwise}, \end{cases}$$

$$\sigma''(\sqrt{H(Q)}) = \begin{cases} -\sqrt{H(Q_i)}), & i = 1, 3 \\ \sqrt{H(Q_i)}, & \text{otherwise}. \end{cases}$$

Then $\hat{t} = t - \sigma'(t) - \sigma''(t) + \sigma''\sigma'(t) \in \mathcal{L}_m$ and has the property that $\hat{t}(Q_{ij}) = 0$ for all $i \geq 2$ and $1 \leq j \leq m$. Note also that $\hat{t} \neq 0$ since the first coordinate of $\theta(\hat{t}) = 4r_{11}\sqrt{H(Q_1)}$. $\hat{t} = \sum_{s=0}^{m-1} t_s z^s$, where $t_s \in k[x,y]$, $0 \leq s < m$. By (1.10) $t_s(Q_i) = 0$ for each s and $i \geq 2$. If $\deg(g) \neq 0 \pmod p$, $\mathcal{S}$ has $(\deg(g) - 1)^2$ points. By (1.3) and (1.6) we get each $t_s = 0$, a contradiction. The case where p divides $\deg(g)$ is slightly more complicated but very similar and we omit the details. □

1.14. Theorem. *If* $\gcd(p,m) = 1$, *then* $\mathrm{Cl}(X_{p^r m})$ *injects into* $\mathrm{Cl}(X_{p^{r-1}m})$ *for all* $r \in \mathbb{Z}^+$. *In particular,* $\mathrm{Cl}(X_m) = 0$ *implies* $\mathrm{Cl}(X_{p^r m}) = 0$ *for all* $r \in \mathbb{Z}^+$.

Proof. Use (1.4), (1.8) and (1.13).

References

1. Blass, P. and Lang, J., *Zariski Surfaces and Differential Equations in Characteristic $p > 0$,* Marcel Decker, Monographs in Pure and Applied Math., 106, 1987.
2. Deligne, P. and Katz, N., *Groupes de Monodromie en Geometrie Algébrique,* Lecture Notes in Mathematics, 340, Springer-Verlag, 1973.
3. Grant, A. and Lang, J., *Applications of the fundamental group and purely inseparable descent to the study of curves on Zariski surfaces,* J. Alg., 132:2 (1990).
4. Grothendieck, A., *SGAI,* Lecture Notes in Mathematics, 224, Springer-Verlag, New York, 1971.
5. Hartshorne, R., *Algebraic Geometry,* Springer-Verlag, New York, 1977.
6. Lang, J., *The divisor class group of the surface $z^{p^m} = G(x,y)$ over fields of characteristic $p > 0$,* J. Alg., 84 (1983).
7. Lang, J., *Generic Zariski surfaces,* Compositio Mathematica, 73 (1990).
8. Samuel, P., *Lectures on unique factorization domains,* Tata Lectures Notes, 1964.