ACTA ARITHMETICA
XCV.4 (2000)

Purely cubic complex function fields with small units

by

R. Scheidler (Newark, DE)

1. Introduction. There is a considerable amount of literature on fundamental units in purely cubic number fields $\mathbb{Q}(\sqrt[3]{D})$ ($D \in \mathbb{Z}$ cubefree) and the solutions of certain Diophantine equations associated with these units. Oftentimes, the fundamental units of these fields are very large, but a number of families of fields with small units were analyzed in considerable detail. Stender [5] characterized families of fields where $D = m^3 + a$ or $D = m^3 + 3a$ with $a, m \in \mathbb{Z}$, a dividing m, and a is bounded above by some specified fraction of m. Rudman [2] improved on previous results and completely described the case $D = m^3 + a$ with a dividing $3m^2$. Finally, Williams [7] extended Rudman's work to values of D where $D = (m^3 - a)/e^3$, e divides $m^3 - a$, and a divides $3m^2$.

In this paper, we derive results analogous to those in [7] for purely cubic complex congruence function fields. That is, we compute the fundamental unit of a cubic extension of unit rank 1 of a rational function field in one variable with a generator ϱ such that $\varrho^3 = D = (M^3 - F)/E^3$ where D, E, F, M are polynomials over a finite field, D is cubefree, E^3 divides $M^3 - F$ and F divides M^2. While we make some use of the methods of Rudman [2] and Williams [7], our techniques are on the whole quite different and exploit properties of polynomials. We also give a complete analysis of the situation where the regulator of a purely cubic complex function field is 1.

For a general introduction to function fields, we refer the reader to [6]; the purely cubic case is discussed in considerable detail in [1] and [3, 4]. Let $k = \mathbb{F}_q$ be a finite field of order q whose characteristic p is not 3. For some element t that is transcendental over k, denote by $k[t]$ and $k(t)$ the ring of polynomials and the field of rational functions, respectively, over k in the

2000 *Mathematics Subject Classification*: Primary 11R16, 11R27; Secondary 11R58, 14H05.

Key words and phrases: purely cubic function field, fundamental unit, regulator.

Research supported by NSF grant DMS-9631647.

variable t. If $D \in k[t]$ is a nonconstant cubefree polynomial and ϱ is a fixed cube root of D in some algebraic closure of $k(t)$, then the cubic extension $K = k(t, \varrho)$ of $k(t)$ is a *purely cubic* (*congruence*) *function field* over the *field of constants* k. Note that the other cube roots of D are $\iota\varrho$ and $\iota^2\varrho$ where ι is a primitive cube root of unity (which may or may not lie in k). We denote by σ the automorphism on $K(\iota)$ that fixes elements in $k(\iota, t)$ and maps ϱ onto $\iota\varrho$, so $\varrho^\sigma = \iota\varrho$ and $\varrho^{\sigma^2} = \iota^2\varrho$.

The integral closure $\mathcal{O} = \overline{k[t]}$ of $k[t]$ in K is a ring and a $k[t]$-module of rank 3. If we write $D = GH^2$ with $G, H \in k[t]$ both squarefree and coprime, then a $k[t]$-basis of $\mathcal{O}$ (which is also a $k(t)$-basis of K) is $\{1, \varrho, \omega\}$ where ϱ is as before and $\omega = \varrho^2/H$. We note that in contrast to the number field case, it is easy to determine H from D; namely $H = \gcd(D, D')$ where D' is the formal derivative of D with respect to t. We also define $\overline{D} = G^2H$; then $\omega^3 = \overline{D}$, ω is also a generator of K over $k(t)$ and in the corresponding integral basis, one simply has to reverse the roles of ϱ and ω. The bases $\{1, \varrho, \varrho^2\}$ and $\{1, \omega, \omega^2\}$ generate submodules $\mathcal{O}_\varrho$ and $\mathcal{O}_\omega$, respectively, of $\mathcal{O}$; we observe that $\mathcal{O}_\varrho = \mathcal{O}$ if and only if D is squarefree and $\mathcal{O}_\omega = \mathcal{O}$ if and only if D is a square.

For an element $\alpha = A + B\varrho + C\omega \in K$ $(A, B, C \in k(t))$, the *conjugates* of α are $\alpha^\sigma = A + B\iota\varrho + C\iota^2\omega$ and $\alpha^{\sigma^2} = A + B\iota^2\varrho + C\iota\omega$. The *norm* and *trace* of α are the respective quantities

$$N(\alpha) = \alpha\alpha^\sigma\alpha^{\sigma^2} = A^3 + B^3GH^2 + C^3G^2H - 3ABCGH,$$
$$\mathrm{Tr}(\alpha) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} = 3A.$$

We have $N(\alpha), \mathrm{Tr}(\alpha) \in k(t)$, and if $\alpha \in \mathcal{O}$, then $N(\alpha), \mathrm{Tr}(\alpha) \in k[t]$. If $\alpha \in \mathcal{O}$, then $N(\alpha) \in k^* = k \setminus \{0\}$ if and only if α is a unit in $\mathcal{O}$.

The group $\mathcal{O}^*$ of units of $\mathcal{O}$ is an Abelian group whose torsion part is simply k^*. Its rank is the *unit rank* of K and a set of generators of the torsion-free part of $\mathcal{O}^*$ is a system of *fundamental units* of K. In contrast to purely cubic number fields (which are complex cubic fields and thus always have unit rank 1), the unit rank of a purely cubic function field can be 0, 1, or 2, depending on the form of q and D. The cases of different unit rank were completely characterized in [3]; in our context, we are only concerned with cubic function fields of unit rank 1 which we call *complex* in analogy to the terminology for cubic number fields. This case occurs if and only if $q \equiv 2 \pmod 3$, the degree $\deg(D)$ of D is divisible by 3, and the leading coefficient $\mathrm{sgn}(D)$ of D is a cube in k^*. Then k does not contain any primitive cube roots of unity, so if $\alpha \in K$, then $\alpha^\sigma, \alpha^{\sigma^2} \notin K$, but $\alpha^\sigma\alpha^{\sigma^2} = N(\alpha)\alpha^{-1} \in K$. Under these conditions, K can be embedded in the field $k((1/t))$ of *Puiseux series* over k. Nonzero elements in $k((1/t))$ are of the form $\alpha =$

$\sum_{i=m}^{\infty} a_i/t^i \in k((1/t))$ ($m \in \mathbb{Z}$, $a_i \in k$ for $i \geq m$, $a_m \neq 0$). Define

$$\begin{aligned} \deg(\alpha) &= -m && \text{the } \textit{degree} \text{ of } \alpha, \\ |\alpha| &= q^{\deg(\alpha)} = q^{-m} && \text{the } (\textit{absolute}) \textit{ value} \text{ of } \alpha, \\ \operatorname{sgn}(\alpha) &= a_m && \text{the } \textit{sign} \text{ of } \alpha, \\ \lfloor \alpha \rfloor &= \sum_{i=m}^{0} \frac{a_i}{t^i} && \text{the } \textit{principal part} \text{ of } \alpha. \end{aligned}$$

We also set $\deg(0) = -\infty$, $|0| = 0$, and $\lfloor 0 \rfloor = 0$. Note that $\lfloor \alpha \rfloor \in k[t]$ and $|\alpha - \lfloor \alpha \rfloor| < 1$. If $\alpha \in K$, then we let $\deg(\alpha^\sigma) = \deg(\alpha^{\sigma^2}) = \deg(\alpha^\sigma \alpha^{\sigma^2})/2$ and $|\alpha^\sigma| = |\alpha^{\sigma^2}| = \sqrt{|\alpha^\sigma \alpha^{\sigma^2}|} = q^{\deg(\alpha^\sigma)}$.

Henceforth, we assume K to have unit rank 1. Then we have one fundamental unit ε of negative degree that is unique up to factors in k^*. $R = \deg(\varepsilon^\sigma)$ is the *regulator* of K; we have $R \in \mathbb{N}$ in contrast to the number field case where the regulator is an irrational number. In general, $|\varepsilon^\sigma|$ is very large—exponentially large in $|D|$, see [3]—but here, we will investigate fields with fundamental units whose absolute value is of order $|D|$. Specifically, we compute the fundamental units of the infinite family of fields $K = k(t, \sqrt[3]{D})$ where $D = (M^3 - F)/E^3$ with $E, F, M \in k[t]$, E^3 divides $M^3 - F$, and F divides M^2. As in the number field situation, the fundamental units of these fields lie almost always in the submodule $\mathcal{O}_\varrho$ of $\mathcal{O}$, and in one case, in $\mathcal{O}_\omega$. We also classify all purely cubic function fields of unit rank 1 whose regulator is 1. Our results are summarized in two tables at the end of Sections 4 and 5, respectively.

In the next section, we establish some general facts about units in purely cubic function fields. Section 3 deals with the case of constant F, and Section 4 discusses the more complicated setting where F is not constant. In the last section, we analyze the situation of minimal regulator.

2. General remarks on units in purely cubic function fields. Before we begin our investigation of fundamental units, we establish some notation. We use lower case letters to denote elements in the field of constants k. Polynomials in $k[t]$ (and occasionally rational functions in $k(t)$) are represented by upper case letters, and Greek letters will signify elements in $\mathcal{O}$ and K (with the exceptions of ι and σ defined in the previous section). For $Q \in k[t]$, Q' denotes the formal derivative of Q with respect to t. For $P, Q \in k[t]$, write $P \,|\, Q$ if P divides Q. Also, write $P^n \,\|\, Q$ ($n \in \mathbb{N}_0$) if P^n is an exact divisor of Q, i.e. $P^n \,|\, Q$ and $P^{n+1} \nmid Q$. For any field L, we denote by $L^* = L \setminus \{0\}$ the set of nonzero elements of L.

We begin with a few simple facts about finite fields and polynomials.

LEMMA 2.1. *Let L be a finite field of characteristic p and order q.*

1. *Every element in L is a pth power.*
2. *If $q \equiv 2 \pmod 3$, then every element in L is a cube.*
3. *If $Q \in L[t]$, then $Q' = 0$ if and only if Q is a pth power in $L[t]$.*

Proof. 1. $a = (a^{q/p})^p$ for all $a \in k$.

2. If $q = 2$, then this is certainly true. If $q > 2$, then for any $a \in k$, $(a^{(q+1)/2})^2 = a^2$, so $a^{(q+1)/2} = ua$ with $u = \pm 1$. Then $(ua^{(q+1)/6})^3 = a$.

3. If $Q' = 0$, then the only nonzero coefficients of Q are coefficients of terms that are pth powers of some power of t. Let $Q = \sum_{i=0}^{\deg(Q)} a_i t^{pi}$. Then by part 1, each a_i is a pth power, say $a_i = b_i^p$ for $i = 0, 1, \ldots, \deg(Q)$. Then $Q = (\sum_{i=0}^{\deg(Q)} b_i t^i)^p$. Conversely, if $Q = P^p$ for some $P \in k[t]$, then $Q' = pP^{p-1}P' = 0$. ∎

We continue with some observations about units in purely cubic function fields. For the remainder of this paper, we let k be a finite field of characteristic $p \neq 3$ and order $q \equiv 2 \pmod 3$. $K = k(t, \sqrt[3]{D})$ ($D = GH^2$ with $G, H \in k[t]$ squarefree and coprime) is a purely cubic function field of unit rank 1, so $\deg(D) \equiv 0 \pmod 3$ and $\operatorname{sgn}(D)$ is a cube in k^*.

LEMMA 2.2. *Let $\eta = a + V\varrho + W\omega \in \mathcal{O}$ be a unit in $\mathcal{O}$ ($a \in k^*$; $V, W \in k[t]$). Then $W \mid V^2H$, $V \mid W^2G$, and $V^2H/W + W^2G/V = 3a$.*

Proof. We have $N(\eta) = a^3 + V^3GH^2 + W^3G^2H - 3aVWGH \in k^*$, so $GH \mid N(\eta) - a^3$ and hence $N(\eta) = a^3$. Then

$$V^3H + W^3G - 3aVW = 0. \tag{2.1}$$

Write $V = V_0 \gcd(V, W)$ and $W = W_0 \gcd(V, W)$ with $V_0, W_0 \in k[t]$ and $\gcd(V_0, W_0) = 1$. Then from (2.1) $VV_0^2H + WW_0^2G - 3aV_0W_0 = 0$. Hence $W_0 \mid VV_0^2H$, so $W_0 \mid VH$ and $W \mid \gcd(V, W)VH \mid V^2H$. Similarly, $V \mid W^2G$. Finally from (2.1) $V^2H/W + W^2G/V = 3a$. ∎

THEOREM 2.3. *Let $\eta = 1 + V\varrho + W\omega \in \mathcal{O}$ be a unit in $\mathcal{O}$ with $VW \neq 0$. If η is a square in $\mathcal{O}$, say $\eta = (A + B\varrho + C\omega)^2$ with $A, B, C \in k[t]$, then $p = 2$, $G \mid V$, $H \mid W$, both V/G and W/H are squares in $k[t]$, and $A = 1$, $B^2 = W/H$, $C^2 = V/G$.*

Proof. We adapt the proof of Lemma 1 in [7] to serve our purpose. Suppose that $\eta = \beta^2$ with $\beta = A + B\varrho + C\omega$ and $A, B, C \in k[t]$. By part 2 of Lemma 2.1, $N(\beta)$ is a cube in k^*, say $N(\beta) = b^3$. As before, $1 = N(\eta) = N(\beta)^2 = b^6$, so $b^3 = \pm 1$, and since k does not contain any primitive cube roots of unity, $b = \pm 1$. If $b = -1$, replace β by $-\beta$, so we may assume that $N(\beta) = 1$. We have

$$\operatorname{Tr}(\beta^2) = \operatorname{Tr}(\eta) = 3, \quad \operatorname{Tr}((\beta\beta^\sigma)^2) = \operatorname{Tr}(\eta\eta^\sigma) = 3(1 - VWGH). \tag{2.2}$$

Set $Q = \mathrm{Tr}(\beta\beta^\sigma) = 3(A^2 - BCGH) \in k[t]$ and $R = \mathrm{Tr}(\beta) = 3A \in k[t]$. Using the fact that $N(\beta) = 1$, we compute $\mathrm{Tr}(\beta^2) = R^2 - 2Q$ and $\mathrm{Tr}((\beta\beta^\sigma)^2) = Q^2 - 2R$. Hence from (2.2),

$$R^2 - 2Q = 3, \quad Q^2 - 2R = 3(1 - VWGH). \tag{2.3}$$

Now set $P = V^2H/W$. Then $P \in k[t]$ and $3 - P = W^2H/V$ by Lemma 2.2. Furthermore, $P(3 - P) = VWGH$, so from (2.3) $((R^2 - 3)/2)^2 - 2R = 3(1 - 3P + P^2)$, or equivalently,

$$(R - 2)^2(R^2 + 4R + 6) = 3(3 - 2P)^2. \tag{2.4}$$

Thus, $(R^2+4R+6)/3$ is a square in $k[t]$, say $3U^2 = R^2+4R+6 = (R+2)^2+2$ with $U \in k[t]$. Setting $T = R + 2$, we obtain $3U^2 - T^2 = 2$.

Since $P(3-P) = VWGH$ and $VW \neq 0$, P is not constant, so by (2.4) R and hence both T and U are not constant. Then $3\,\mathrm{sgn}(U)^2 - \mathrm{sgn}(T)^2 = 0$, so 3 is a square in k^*; say $3 = a^2$ with $a \in k^*$. It follows that $(aU-T)(aU+T) = 2$. If $p \neq 2$, then both $aU - T$ and $aU + T$ are constant, contradicting the fact that T and U are not constant. So $p = 2$ and $\eta = A^2 + B^2\varrho^2 + C^2\omega^2 = A^2 + C^2G\varrho + B^2H\omega$. Comparing coefficients yields $A^2 = 1$, $C^2G = V$, $B^2H = W$. ∎

Lemma 2.4. *Let $\eta = \alpha^3/N$ where $\alpha \in \mathcal{O}$, $\alpha \neq 0$, and $N = N(\alpha) \in k[t]$ is cubefree. If η is a cube in K, then N is one of a, aD, $a\overline{D}$ with $a \in k^*$.*

Proof. Suppose $\eta = \beta^3$ for some $\beta \in \mathcal{O}$. Then $N = \gamma^3$ is a cube in K where $\gamma = \alpha/\beta \in K^*$. If $\gamma \in k$, then $N = a$ for some $a \in k^*$. If $\gamma \notin k$, then $\gamma \notin k(t)$ since N is cubefree. Therefore, γ is a generator of K over $k(t)$ with minimal polynomial $x^3 - N \in k[t][x]$. Let $\gamma = A + B\varrho + C\omega$ with $A, B, C \in k(t)$. Then $0 = \mathrm{Tr}(\gamma) = 3A$, so $A = 0$, and $0 = \mathrm{Tr}(\gamma\gamma^\sigma) = -3BCGH$, so $B = 0$ or $C = 0$. If $B = 0$, then $N = N(\gamma) = C^3\overline{D}$, so $C \in k^*$ since N is cubefree. Similarly, if $C = 0$, then $N = B^3D$ with $B \in k^*$. ∎

Lemma 2.5. *Let $\varepsilon = U + V\varrho + W\omega \in \mathcal{O}$ be a unit with $|\varepsilon| > 1$. Then $|\varepsilon| = |U|$.*

Proof. Since $|\varepsilon| > 1$ and $|N(\varepsilon)| = 1$, we have $|\varepsilon^\sigma| < 1$. Thus $|\varepsilon| = |\varepsilon + \varepsilon^\sigma + \varepsilon^{\sigma^2}| = |\mathrm{Tr}(\varepsilon)| = |U|$. ∎

We conclude this section with some equalities that will prove useful. If $\alpha = A + B\varrho + C\omega \in K$ $(A, B, C \in k(t))$, then

$$\begin{aligned} A &= \frac{1}{3}(\alpha + \alpha^\sigma + \alpha^{\sigma^2}), \\ B &= \frac{1}{3\varrho}(\alpha + \iota^2\alpha^\sigma + \iota\alpha^{\sigma^2}), \\ C &= \frac{1}{3\omega}(\alpha + \iota\alpha^\sigma + \iota^2\alpha^{\sigma^2}). \end{aligned} \tag{2.5}$$

3. The fundamental unit of $K = k(t, \sqrt[3]{D})$ with $D = (M^3 - a)/E^3$. We begin our investigation with the somewhat simpler case of constant F.

LEMMA 3.1. *Let $D = (M^3 - F)/E^3$ with $E, F, M \in k[t]$ and $E^3 \mid M^3 - F$. Then $\eta = M - E\varrho$ is a unit of $\mathcal{O}$ if and only if $F \in k^*$.*

Proof. Clearly, $\eta \in \mathcal{O}$, and $N(\eta) = M^3 - E^3 D = F$, so η is a unit if and only if F is constant. ∎

Henceforth, we let $K = k(t, \sqrt[3]{D})$ where

$$D = (M^3 - a)/E^3, \quad a \in k^*, \quad E, M \in k[t], \quad E^3 \mid M^3 - a. \tag{3.1}$$

We point out that there are infinitely many fields of the type described in (3.1). For example, let $b \in k^*$ and $E \in k[t]$ so that E' is squarefree. Set $a = b^3$ and $M = E^3 + b$. Then $(M^3 - a)/E^3 = E^6 + 3bE^3 + 3b^2$. To see that this is cubefree, suppose $P^3 \mid (M^3 - a)/E^3$ with $P \in k[t]$ irreducible, then $P \nmid E$ and $P^2 \mid 6E^5E' + 9bE^2E' = 3E^2E'(2E^3 + 3b)$, hence $P^2 \mid E'(2E^3 + 3b)$. Since E' is squarefree, $P \mid 2E^3 + 3b$. If $p = 2$, then this is impossible. Otherwise $P \mid (E^6 + 3bE^3 + 3b^2) - b(2E^3 + 3b) = E^3(E^3 + b)$, so $P \mid E^3 + b$ and $P \mid \gcd(2E^3 + 3b, E^3 + b) = 1$, which also yields a contradiction.

PROPOSITION 3.2. *For every polynomial D of the form* (3.1), *there exists a representation of D or $\overline{D}$ as given in* (3.1) *such that M is not a pth power.*

Proof. Let $D = (M^{3p^r} - b)/C^3$ with $b \in k^*$, $C, M \in k[t]$, $C^3 \mid M^{3p^r} - b$, and M is not a pth power. By part 1 of Lemma 2.1, b is a p^rth power in k^*; say $b = a^{p^r}$. Then $C^3 D = (M^3 - a)^{p^r}$.

Suppose first that r is even. Then $p^r \equiv 1 \pmod 3$. Since D is cubefree, $(M^3 - a)^{p^r - 1} \mid C^3$. Set $E = C/(M^3 - a)^{(p^r - 1)/3} \in k[t]$. Then we have $D = (M^3 - a)/E^3$ and a, E, M satisfy (3.1).

If r is odd, then $p^r \equiv 2 \pmod 3$. In this case, $(M^3 - a)^{p^r - 2} \mid C^3$. Set $E_0 = C/(M^3 - a)^{(p^r - 2)/3}$. Then $D = (M^3 - a)^2/E_0^3$ and $(M^3 - a)^2 = E_0^3 G H^2$. Since G is squarefree, it follows that $G \mid E_0$ and E_0/G is a square, say $E_0 = GE_1^2$. Then $M^3 - a = \pm E_1^3 G^2 H = \pm E_1^3 \overline{D}$ where we choose the sign so that the leading coefficients on both sides match in the case where $p \neq 2$. Set $E = E_1$ if the sign is positive and $E = -E_1$ if the sign is negative. Then $\overline{D} = (M^3 - a)/E^3$ with a, E, M as in (3.1). ∎

If $K = k(t, \sqrt[3]{D})$ where D is as in (3.1), then the previous proposition shows that there is no loss of generality in assuming that M is not a pth power in $k[t]$. It is a simple matter to find such a representation, since it is easy to compute p^rth roots in k^* (and hence in $k[t]$): if $q = p^l$, let $u = \lceil r/l \rceil \in \mathbb{N}$, i.e. u is the least integer not less than r/l, and $lu \geq r$. Then $a = a^{q^u} = a^{p^{lu}} = (a^{p^{lu-r}})^{p^r}$ for all $a \in k$. We observe that if we write $\overline{D}$ instead of D in the form (3.1), then the basis elements ϱ and ω need to be interchanged.

LEMMA 3.3. *Let D be as in* (3.1) *and assume that M is not a pth power in $k[t]$. Then $|E| < |\varrho|$.*

Proof. Taking the derivative of $DE^3 = M^3 - a$ shows that $E^2 \mid M^2M'$. Since $\gcd(E, M) = 1$, $E^2 \mid M'$, and since $M' \neq 0$ by part 3 of Lemma 2.1, we have $|E|^2 \leq |M'| < |M| = |E\varrho|$, so $|E| < |\varrho|$. ∎

THEOREM 3.4. *Let $K = k(t, \sqrt[3]{D})$ where D is as in* (3.1) *and M is not a pth power in $k[t]$. Then the fundamental unit of K is $\varepsilon = M - E\varrho$ and the regulator of K is $R = \deg(M)$.*

Proof. By Lemma 3.1, ε is a unit in $\mathcal{O}$. We note that $\varepsilon^{-1} = a^{-1}(M^2 + ME\varrho + E^2\varrho^2)$, so by Lemma 2.5 $|\varepsilon|^{-1} = |M|^2$. Suppose $\varepsilon = \eta^s$ where $\eta = A + B\varrho + C\omega \in \mathcal{O}$ with $A, B, C \in \mathcal{O}$ and $s \in \mathbb{N}$. Then $A \neq 0$ as otherwise $GH \mid N(\eta)$. Since $|\eta| < 1$, we have $|\eta^\sigma| > 1$, so from (2.5) and Lemma 3.3,

$$|\eta^\sigma| = |\varepsilon^\sigma|^{1/s} = |\varepsilon^\sigma \varepsilon^{\sigma^2}|^{1/(2s)} = |\varepsilon|^{-1/(2s)} = |M|^{1/s} = |E\varrho|^{1/s} < |\varrho|^{2/s}.$$

Using $|\varrho|^2 = |H\omega| \geq |\omega|$, from (2.5) we obtain

$$|B| \leq |\eta^\sigma|/|\varrho| < |\varrho|^{2/s-1}, \tag{3.2}$$

$$|C| \leq |\eta^\sigma|/|\omega| < |\varrho|^{2/s-1/2}. \tag{3.3}$$

If $B \neq 0$, then (3.2) implies $2/s - 1 > 0$, so $s = 1$, $\eta = \varepsilon$, and $R = \deg(M)$. Now suppose $B = 0$. Then $C \neq 0$ and from (3.3), $s \leq 3$. If $s = 2$, then comparing coefficients of the identity $(A + C\omega)^2 = M - E\varrho$ yields $2AC = 0$, so $p = 2$, and $A^2 = M$, contradicting our assumption that M is not a pth power in $k[t]$. If $s = 3$, then comparing coefficients of ω in $M - E\varrho = (A + C\omega)^3$ yields $3A^2C = 0$, contradicting $AC \neq 0$ and $p \neq 3$. ∎

4. The fundamental unit of $K = k(t, \sqrt[3]{D})$ with $D = (M^3 - F)/E^3$. We continue to investigate the more difficult case of nonconstant F.

LEMMA 4.1. *Let $D = (M^3 - F)/E^3$ with $E, F, M \in k[t]$, F cubefree, $E^3 \mid M^3 - F$, and $F \mid M^2$. Then $\gcd(M^3/F - 1, F) = \gcd(E, F) = 1$, so $E^3 \mid M^3/F - 1$.*

Proof. If $P \in k[t]$ is an irreducible divisor of F, then $P \mid M$, so $P \mid M^3/F$ and $P \nmid M^3/F - 1$. If $P \in k[t]$ is an irreducible common divisor of E and F, then $P \mid M$ and $P^3 \mid E^3$, so $P^3 \mid M^3 - E^3D = F$, contradicting the fact that F is cubefree. ∎

LEMMA 4.2. *Let $D = (M^3 - F)/E^3$ with $E, F, M \in k[t]$, F not constant and cubefree, and $E^3 \mid M^3 - F$. Then $F \mid M^2$ if and only if $F \mid HM$.*

Proof. Let $P \in k[t]$ be an irreducible divisor of F. Then $P \parallel F$ or $P^2 \parallel F$ since F is cubefree. Write $E^3GH^2 - F = M^3$.

Suppose first that $P \parallel F$. Then $P \mid M^2$ implies $P \mid M \mid HM$, and conversely, $P \mid HM$ implies $P \mid M \mid M^2$ or $P \mid H$. In the latter case, we have $P \mid M^3$, so $P \mid M^2$ as well.

Now suppose $P^2 \mid F$. Then $P^2 \mid M^2$ implies $P^2 \mid E^3GH^2$. Now $P \nwarrow E$ by Lemma 4.1, $P^2 \nwarrow G$ since G is squarefree, and $\gcd(G,H) = 1$, so $P \mid H$. Since $P \mid M$, it follows that $P^2 \mid HM$. Conversely, suppose $P^2 \mid HM$. Then $P \mid M$ since H is squarefree, so $P^2 \mid M^2$. ∎

LEMMA 4.3. *Let $D = (M^3 - F)/E^3$ with $E, F, M \in k[t]$, F not constant and cubefree, and $E^3 \mid M^3 - F$. Then*

$$\eta = \frac{(M - E\varrho)^3}{F} = 1 - \frac{3M^2}{F}E\varrho + \frac{3HM}{F}E^2\omega$$

is a unit of $\mathcal{O}$ if and only if F divides M^2.

Proof. We have $N(\eta) = (M^3 - E^3D)^3/F^3 = 1$. If η is a unit, then $\eta \in \mathcal{O}$, so from looking at the ϱ coefficient of η and using Lemma 4.1, $F \mid M^2$. If $F \mid M^2$, then by Lemma 4.2 $F \mid HM$, so $\eta \in \mathcal{O}$. ∎

We now proceed analogously to Section 3; however, since F is not constant here, the arguments from the previous section need to be somewhat refined. Henceforth, let $K = k(t, \sqrt[3]{D})$ where

$$\begin{aligned} &D = (M^3 - F)/E^3, \quad E, F, M \in k[t], \quad F \text{ nonconstant and cubefree,} \\ &E^3 \mid M^3 - F, \quad F \mid M^2. \end{aligned} \tag{4.1}$$

There are once again infinitely many fields of this type. For example, let $a \in k^*$ and $E \in k[t]$ a nonconstant polynomial so that $E^3 + a$ is squarefree. Set $M = E^3 + a$ and $F = aM^2$. Then M is squarefree, so F is cubefree, $F \mid M^2$, and $(M^3 - F)/E^3 = M^2$, so $G = 1$ and $H = M$.

We point out that the assumption of F in (4.1) being cubefree represents no loss of generality. For if $P \in k[t]$ is irreducible with $P^3 \mid F$, then $P^3 \mid M^3$ and hence $P^3 \mid E^3$ because D is cubefree. Then $D = (\widetilde{M}^3 - \widetilde{F})/\widetilde{E}^3$ where $\widetilde{M} = M/P$, $\widetilde{F} = F/P^3$, and $\widetilde{E} = E/P$. As shown below, we may also assume that M^3/F is not a pth power in $k[t]$.

LEMMA 4.4. *Let D be as in* (4.1) *and suppose M^3/F is a p^rth power in $k[t]$ where $r \in \mathbb{N}$. Let $F = XY^2$ with $X, Y \in k[t]$ squarefree and coprime, and set $\overline{F} = X^2Y$. Then there exists $Q \in k[t]$ such that*

$$\frac{M^3}{F} = \begin{cases} (\overline{F}Q^3)^{p^r} & \text{if } r \text{ is even,} \\ (FQ^3)^{p^r} & \text{if } r \text{ is odd.} \end{cases}$$

Proof. Clearly $XY \mid M$. Write $M^3/F = R^{p^r}$, so $M^3 = XY^2R^{p^r}$. It follows that $X^2Y \mid R^{p^r}$, hence $XY \mid R$ and $X^{p^r+1}Y^{p^r+2} \mid M^3$.

Suppose first that r is even, so $p^r \equiv 1 \pmod 3$. Since X is squarefree, we have $X^{p^r+2} \mid M^3$, hence $X^{p^r+1} \mid R^{p^r}$, implying $X^{2p^r} \mid R^{p^r}$. Write

$R^{p^r} = X^{2p^r}Y^{p^r}S$ with $S \in k[t]$. Then S is a p^rth power, and since $M^3 = X^{2p^r+1}Y^{p^r+2}S$, S is also a cube in $k[t]$. Let $S = Q^{3p^r}$ with $Q \in k[t]$. Then $R = X^2YQ^3 = \overline{F}Q^3$.

Now assume that r is odd, so $p^r \equiv 2 \pmod 3$. Since Y is squarefree and $Y^{p^r+2} \mid M^3$, we see that $Y^{p^r+4} \mid M^3$, hence $Y^{p^r+2} \mid R^{p^r}$, implying $Y^{2p^r} \mid R^{p^r}$. Write $R^{p^r} = X^{p^r}Y^{2p^r}S$. Then we see as before that S is both a p^rth power and a cube in $k[t]$, so $S = Q^{3p^r}$ for some $Q \in k[t]$. In this case, $R = XY^2Q^3 = FQ^3$. ∎

PROPOSITION 4.5. *For every polynomial D of the form* (4.1)*, there exists a representation of D or $\overline{D}$ as given in* (4.1) *such that M^3/F is not a pth power.*

Proof. Let $D = (N^3 - B)/C^3$ with $B, C, N \in k[t]$, $C^3 \mid N^3 - B$, $B \mid N^2$, B nonconstant and cubefree, say $B = XY^2$ with X, Y squarefree and coprime. Suppose $N^3/B = R^{p^r}$ with $R \in k[t]$ not a pth power. Then

$$D = \frac{B(R^{p^r} - 1)}{C^3} = \frac{B(R-1)^{p^r}}{C^3}.$$

Suppose first that r is even, so $p^r \equiv 1 \pmod 3$. Since D is cubefree and $\gcd(B, C) = 1$ by Lemma 4.1, $(R-1)^{p^r-1} \mid C^3$. Set $E = C/(R-1)^{(p^r-1)/3}$. Then $D = B(R-1)/E^3$. From the previous lemma, $BR = (XYQ)^3$ with $Q \in k[t]$. Setting $M = XYQ$ and $F = B$, we obtain $D = (M^3 - F)/E^3$ with $F \mid M^2$, $E^3 \mid M^3 - F$, and $M^3/F = X^2YQ^3 = R$, again by Lemma 4.4.

If r is odd, then $p^r \equiv 2 \pmod 3$. In this case, $(R-1)^{p^r-2} \mid C^3$. Set $E_0 = C/(R-1)^{(p^r-2)/3}$. Then $D = B(R-1)^2/E_0^3$ and $XY^2(R-1)^2 = E_0^3GH^2$. Since B is coprime to both C and $N^3/B - 1$ by Lemma 4.1, it is also coprime to E_0 and $R-1$, so $X \mid G$. Thus, E_0G/X is a square, hence $(G/X) \mid E_0$ and the quotient of E_0 and G/X must be a square. Write $E_0 = E_1^2G/X$. Then $X^2Y(R-1) = \pm E_1^3G^2H = \pm E_1^3\overline{D}$, where we again choose the sign so that the leading coefficients on both sides match if $p \neq 2$. Set $E = E_1$ if the sign is positive and $E = -E_1$ if the sign is negative. If $\overline{B} = X^2Y$, then $\overline{D} = \overline{B}(R-1)/E^3$. From Lemma 4.4, $\overline{B}R = (XYQ)^3$ for some $Q \in k[t]$. Setting $F = \overline{B}$ and $M = XYQ$, we obtain $\overline{D} = (M^3 - F)/E^3$ with $F \mid M^2$, $E^3 \mid M^3 - F$, and $M^3/F = XY^2Q^3 = BQ^3 = R$ by the previous lemma. ∎

LEMMA 4.6. *Let D be as in* (4.1) *and assume that M^3/F is not a pth power in $k[t]$. Then $|E| < |\varrho|$.*

Proof. By Lemma 4.1 $E^3 \mid M^3/F - 1$. Taking derivatives shows that E^2 divides

$$\left(\frac{M^3}{F} - 1\right)' = \frac{M^2}{F}\left(3M' - \frac{MF'}{F}\right),$$

where we note that $F \mid MF'$. Since E and M^2/F are coprime by Lemma 4.1, $E^2 \mid 3M' - MF'/F$. Since M^3/F is not a pth power in $k[t]$, we have $(M^3/F)'$

$\neq 0$ by part 3 of Lemma 2.1, so $3M' - MF'/F \neq 0$ and $|E|^2 \leq |M'| < |M| = |E\varrho|$, implying $|E| < |\varrho|$. ∎

THEOREM 4.7. *Let $K = k(t, \sqrt[3]{D})$ where D is as in* (4.1), *and M^3/F is not a pth power. Set*

$$\eta = \frac{(M - E\varrho)^3}{F} = 1 - \frac{3M^2}{F}E\varrho + \frac{3HM}{F}E^2\omega.$$

Then the fundamental unit of K is

1. *$\varepsilon = E - (M/GH)\omega$ if and only if $F = aD$ for some $a \in k^*$, in which case $\eta = -a^{-1}\varepsilon^3$;*
2. *η otherwise.*

The regulator of K is $R = \deg(E) = \deg(M^3/F)/3$ in case 1 *and $R = \deg(M^3/F) = 3\deg(E) - \deg(D) - \deg(F)$ in case* 2.

Proof. By Lemma 4.3, η is a unit in $\mathcal{O}$. We note that

$$\eta^{-1} = (M^2 + ME\varrho + E^2\varrho^2)^3/F^2,$$

so by Lemma 2.5, $|\eta|^{-1} = |M|^6/|F|^2$.

Suppose first that η is a cube. Since F is not constant, by Lemma 2.4, $F \in \{aD, a\overline{D}\}$ for some $a \in k^*$. Since G and H are both squarefree, $GH \mid M$. Suppose $F = a\overline{D}$. Then $H^2 \mid M^3 - E^3D = a\overline{D}$, a contradiction. Thus $F = aD$ and a simple calculation shows that $\eta = -a^{-1}\varepsilon^3$ where $\varepsilon = E - (M/GH)\omega$. So it suffices to show that ε is not a power of an element $\gamma \in \mathcal{O}$.

Suppose $\varepsilon = \gamma^s$ where $\gamma = A + B\varrho + C\omega \in \mathcal{O}$ with $A, B, C \in k[t]$ and $s \in \mathbb{N}$. We have $\varepsilon^{-1} = \varepsilon^\sigma\varepsilon^{\sigma^2} = E^2 + (M^2/D)\varrho + (M/GH)E\omega$, so $|\varepsilon|^{-1} = |E|^2$ by Lemma 2.5. Then as in the proof of Theorem 3.4, $|\gamma^\sigma| = |\varepsilon^\sigma|^{1/s} = |\varepsilon|^{1/(2s)} = |E|^{1/s} < |\varrho|^{1/s}$ by Lemma 4.6. As before, we obtain

$$|B| \leq |\varepsilon^\sigma|/|\varrho| < |\varrho|^{1/s-1}, \quad |C| \leq |\varepsilon^\sigma|/|\omega| < |\varrho|^{1/s-1/2}. \tag{4.2}$$

Since $s > 0$, (4.2) implies $B = 0$. If $C \neq 0$, then (4.2) shows that $s < 2$, so $s = 1$. If $C = 0$, then $-E + (M/GH)\omega = A^s$ which yields a contradiction. This proves case 1 of the theorem.

Suppose now that η is not a cube and assume that $\eta = \varepsilon^s$ where $\varepsilon = A + B\varrho + C\omega \in \mathcal{O}$ with $A, B, C \in k[t]$ and $s \in \mathbb{N}$, $s \not\equiv 0 \pmod 3$. If $A = 0$, then $GH \mid N(\varepsilon)$ which is impossible. Suppose $B = 0$. Since s is not divisible by 3, the constant coefficient of ε^s is a multiple of A, so comparing constant coefficients in the equality $\eta = \varepsilon^s$ shows that $A \in k^*$. But then $C^3G^2H = N(\varepsilon) - A^3 \in k$, which is a contradiction. The assumption $C = 0$ yields a similar contradiction. So $ABC \neq 0$. By Lemma 4.6, $|M| = |E\varrho| < |\varrho|^2$, so

$$|\varepsilon^\sigma| = |\eta^\sigma|^{1/s} = |\eta|^{-1/(2s)} = \left(\frac{|M^3|}{|F|}\right)^{1/s} < \left(\frac{|\varrho|^6}{|F|}\right)^{1/s}. \tag{4.3}$$

Thus, $|B| \leq |\varepsilon^\sigma|/|\varrho| < |\varrho|^{6/s-1}$, hence $s \leq 5$, i.e. $s \in \{1, 2, 4, 5\}$.

Suppose first that s is even. Then η is a square, so by Theorem 2.3, $p = 2$ and $H \,|\, (HM/F)E^2$. If $s = 2$, then comparing coefficients of ω implies $B^2H = HME^2/F$, in which case $M^3/F = (BM/E)^2$. If $s = 4$, then again comparing coefficients of ω shows that $C^4\overline{D} = HME^2/F$, implying $M^3/F = (C^2GM/E)^2$. In either case, M^3/F is a square, contrary to our assumption that M^3/F is not a pth power in $k[t]$. So we only need to rule out the case $s = 5$.

Assume $\eta = (A + B\varrho + C\omega)^5$. Then

$$1 = A^5 + 10A^2B^3GH^2 + 20A^3BCGH + 5B^4CG^2H^3 + 30AB^2C^2G^2H^2 + 10A^2C^3G^2H + 5BC^4G^3H^2, \tag{4.4}$$

$$-3\frac{M^2}{F}E = 5A^4B + 5AB^4GH^2 + 30A^2B^2CGH + 10A^3C^2G + 10B^3C^2G^2H^2 + 20ABC^3G^2H + C^5G^3H, \tag{4.5}$$

$$3\frac{MH}{F}E^2 = 10A^3B^2H + B^5GH^3 + 5A^4C + 20AB^3CGH^2 + 30A^2BC^2GH + 10B^2C^3G^2H^2 + 5AC^4G^2H. \tag{4.6}$$

Assume first that $p \neq 5$. Then from (4.6), $H \,|\, FA^4C$. Since $GH \,|\, A^3 - N(\varepsilon)$, H and A are coprime, so $H \,|\, FC$. Then $GH^2 \,|\, FB^3GH^2 + FC^3G^2H - 3FABCGH = F(A^3 - N(\varepsilon))$, and from (4.4), $D \,|\, F(A^5 - 1)$. Hence $D/F \,|\, (A^5 - 1) - A^2(A^3 - N(\varepsilon)) = N(\varepsilon)A^2 - 1$.

Suppose that A is not constant. Then by (2.5) and (4.3), $|D/F| \leq |A|^2 \leq |\varepsilon^\sigma|^2 < |D^2/F|^{2/5}$, implying $|F|^{3/5} > |D|^{1/5}$ or $|F| > |D|^{1/3}$. Then

$$|\varepsilon^\sigma| < \left(\frac{|D|^2}{|F|}\right)^{1/5} < |D|^{(2-\frac{1}{3})\frac{1}{5}} = |D|^{1/3},$$

so from (2.5), $|B| \leq |\varepsilon^\sigma|/|\varrho| < 1$, implying the contradiction $B = 0$. So A must be constant. Then $N(\varepsilon) = A^3$ and from (4.4), $A^5 = 1$. Dividing (4.4) by $5BCGH$ gives

$$0 = 2A^2\frac{B^2H}{C} + 4A^3 + B^3GH^2 + 6ABCGH + 2A^2\frac{C^2G}{B} + C^3G^2H.$$

Applying Lemma 2.2 to ε yields $B^2H/C + C^2G/B = 3A$, so

$$0 = 10A^3 + GH(B^3H + 6ABC + C^3G). \tag{4.7}$$

If $p = 2$, then (4.7) is equivalent to $0 = BCGH(B^2H/C + C^2G/B) = ABCGH$, contradicting $ABC \neq 0$. If $p \neq 2$, then (4.7) implies $GH \,|\, A^3$, contradicting the fact that A is constant. So the case where $p \neq 5$ leads to a contradiction and hence $p = 5$. Multiplying (4.5) by (4.6) and by GH yields $M^3E^3D/F^2 = (BCGH)^5$, or equivalently, $(M^3/F)(M^3/F - 1) = (BCGH)^5$. Thus, M^3/F must be a fifth power in $k[t]$, contradicting our

assumption that M^3/F is not a pth power. So η is not a fifth power in $\mathcal{O}$, and $\varepsilon = \eta$. ∎

We point out that in the case where $F = aD$ with $a \in k^*$, we have $\overline{D} = (E^3 + a)/\widetilde{M}^3$ with $\widetilde{M} = M/GH \in k[t]$, so $\overline{D}$ is of the form (3.1).

We summarize our results from the previous two sections in Table 1 below. Here, $D = (M^3 - F)/E^3$ where $E, F, M \in k[t]$, $E^3 \mid M^3 - F$, $F \mid M^2$, and M^3/F is not a pth power in $k[t]$.

Table 1. Fundamental units of $K = k(t, \sqrt[3]{(M^3 - F)/E^3})$

F	Fundamental unit
Nonzero constant	$M - E\varrho$
Constant multiple of D	$E - \dfrac{M}{GH}\omega$
All other cases	$1 - 3\dfrac{M^2}{F}\varrho + 3\dfrac{HM}{F}\omega$

5. Characterization of minimal regulator. In this section, we determine when exactly the regulator of a purely cubic complex function field is 1.

LEMMA 5.1. *Let* $\alpha = A + B\varrho + C\omega \in \mathcal{O}$ $(A, B, C \in k[t])$ *with* $A \neq 0$. *If* $|\alpha^\sigma| < 1$, *then* $BC \neq 0$, $|A| = |B\varrho| = |C\omega|$, *and* $\lfloor B\varrho \rfloor = \lfloor C\omega \rfloor$.

Proof. $|B\varrho - C\omega| = |\alpha^\sigma - \alpha^{\sigma^2}| < 1$, so $BC \neq 0$, $\lfloor B\varrho \rfloor = \lfloor C\omega \rfloor$ and $|B\varrho| = |C\omega|$. Let $B\varrho + C\omega = 2\lfloor B\varrho \rfloor + \delta$ with $\delta \in \mathcal{O}$ and $|\delta| < 1$. If $p \neq 2$, then $2(A - \lfloor B\varrho \rfloor) = |\alpha^\sigma + \alpha^{\sigma^2} + \delta| < 1$, so $A = \lfloor B\varrho \rfloor$ and $|A| = |B\varrho|$. Suppose now that $p = 2$. Then $\alpha = A + \delta$ and $\alpha^\sigma \alpha^{\sigma^2} = A\alpha + BCGH + \delta^2$, so $|A\alpha| = |BCGH|$. Since $|\alpha| = |A|$ and $|B\varrho| = |C\omega|$, we have $|A| = |B\varrho|$. ∎

LEMMA 5.2. *If* $R = 1$, *then* $\deg(D) = 3$ *or* $\deg(\overline{D}) = 3$.

Proof. Let $\varepsilon^{-1} = A + B\varrho + C\omega$ with $A, B, C \in k[t]$. Then $A \neq 0$. Since $R = 1$, by Lemmas 2.5 and 5.1, $\lfloor B\varrho \rfloor = \lfloor C\omega \rfloor = U$ for some $U \in k[t]$, and $\deg(U) = \deg(A) = \deg(\varepsilon^{-1}) = 2R = 2$. Write $B\varrho = U + \gamma$, $C\omega = U + \delta$ with $\gamma, \delta \in \mathcal{O}$ and $|\gamma|, |\delta| < 1$. Then

$$\begin{aligned}(B^3H - C^3G)GH = B^3\varrho^3 - C^3\omega^3 &= (U + \gamma)^3 - (U + \delta)^3 \\ &= (\gamma - \delta)(3U^2 + 3U(\gamma + \delta) + \gamma^2 + \gamma\delta + \delta^2),\end{aligned}$$

so $\deg(B^3H - C^3G) < 2\deg(U) - \deg(GH) = 4 - \deg(GH)$. Thus, $\deg(GH) \leq 3$ as otherwise $B^3H = C^3G$ and $D = (BC^{-1}H)^3$ would be a cube in $k[t]$. So we must have $\deg(\varrho) + \deg(\omega) \leq 3$ and hence $\deg(\varrho) = 1$, in which case $\deg(D) = 3$, or $\deg(\omega) = 1$, in which case $\deg(\overline{D}) = 3$. ∎

LEMMA 5.3. *Let $D = t^3 + rt + s$ be squarefree where $r, s \in k$ and $r \neq 0$. Then $R > 1$.*

Proof. Since D is squarefree, $\omega = \varrho^2$, so $\deg(\omega) = 2\deg(\varrho) = 2$. Suppose $R = 1$. Then $\deg(\varepsilon^{-1}) = 2$. Let $\varepsilon^{-1} = A + B\varrho + C\omega$. By Lemmas 2.5 and 5.1, $\deg(A) = \deg(B\varrho) = \deg(C\omega) = 2$, so A is quadratic, B is linear, and C is constant. Without loss of generality, assume that $C = 1$ and let $A = at^2 + bt + c$ and $B = dt + e$ with $a, b, c, d, e \in k$, $ad \neq 0$. Then

$$N(\varepsilon^{-1}) = (at^2 + bt + c)^3 + (dt + e)^3(t^3 + rt + s) + (t^3 + rt + s)^2 - 3(at^2 + bt + c)(dt + e)(t^3 + rt + s).$$

Comparing coefficients of t^i for $1 \leq i \leq 6$ yields

$$0 = a^3 + d^3 + 1 - 3ad, \tag{5.1}$$

$$0 = a^2b + d^2e - ae - bd, \tag{5.2}$$

$$0 = 3a^2c + 3ab^2 + 3de^2 + d^3r + 2r - 3be - 3cd - 3adr, \tag{5.3}$$

$$0 = 6abc + b^3 + e^3 + 3d^2er + d^3s + 2s - 3ce - 3aer - 3bdr - 3ads, \tag{5.4}$$

$$0 = 3ac^2 + 3b^2c + 3de^2r + 3d^2es + r^2 - 3ber - 3cdr - 3aes - 3bds, \tag{5.5}$$

$$0 = 3bc^2 + e^3r + 3de^2s + 2rs - 3cer - 3bes - 3cds. \tag{5.6}$$

Now the factorization of (5.1) is $(a+d+1)(a+\iota(\iota d+1))(a+\iota^2(\iota^2 d+1)) = 0$ where we recall that ι is a primitive cube root of unity, so either $a = d = 1$ or $a = -(d + 1)$.

Suppose first that $a = d = 1$. Then (5.3) implies $b^2 - be + e^2 = 0$, so $b = e = 0$ as otherwise be^{-1} would be a primitive cube root of unity in k. Then from (5.5), $0 = 3c^2 + r^2 - 3cr$. If $p = 2$, then this would once again imply that cr^{-1} is a primitive cube root of unity. If $p \neq 2$, then we have $(2c/r - 1)^{-2} = -3$, so -3 is a square in k, say $-3 = m^2$ with $m \in k^*$. But then $(m - 1)/2$ is a primitive cube root of unity, so $m = 1$ and $-3 = 1$, contradicting $p \neq 2$.

Now suppose that $a = -(d + 1)$. Then $d \neq -1$ as $a \neq 0$. Substituting this into (5.2) yields $(d^2 + d + 1)(b + e) = 0$, so $b = -e$. Continuing the substitution with (5.3) results in the equality

$$3(d^2 + d + 1)c + (d^3 + 3d^2 + 3d + 2)r = 0,$$

so after dividing by $d^2 + d + 1$, we obtain $3c = -(d+2)r$. Substituting these expressions for a, b, and c into (5.4) and (5.5) and dividing by $d^2 + d + 1$, we obtain

$$er + (d + 2)s = 0 \tag{5.7}$$

and

$$3es - (d + 1)r^2 = 0. \tag{5.8}$$

Since $d \neq -1$ and $r \neq 0$, $es \neq 0$. Combining (5.7) and (5.8) and dividing by r yields

$$3e^2 + (d+1)(d+2)r = 0. \tag{5.9}$$

Performing the substitutions for a, b, and c on (5.6) and dividing by er yields

$$r(d^3 + 6d^2 + 6d + 2) + 3e^2(2d+1) = 0. \tag{5.10}$$

We now substitute (5.9) into (5.10) and obtain $-dr(d^2+d+1) = 0$, contradicting $dr \neq 0$. ∎

We note that $D(t) = t^3 + rt + s$ is squarefree if and only if $4r^3 + 27s^2 \neq 0$. If $p = 2$, then D is squarefree if and only if $s = 0$. If $p \neq 2$, then by part 2 of Lemma 2.1, it is always possible to write $s = -2a^3$ for some $a \in k$ (assuming $q \equiv 2 \pmod 3$). Then D is squarefree if and only if $r \neq -3a^2$.

Lemma 5.3 shows that not all polynomials $D(t)$ of degree 3 give rise to a function field with regulator 1. This is in contrast to real quadratic function fields, where every quadratic polynomial generates a field with regulator 1; this field is in fact itself a field of rational functions.

THEOREM 5.4. *$R = 1$ if and only if one of the following holds*:

1. *$D = GH^2$ where G and H are linear*,
2. *$D = M^3 - a$ where $a \in k^*$ and $M \in k[t]$ is linear*,
3. *$D = (M^3 - a)^2$ where $a \in k^*$ and $M \in k[t]$ is linear.*

If $D = GH^2$ with $G = at + b$ and $H = at + c$ where $a, b, c \in k$, $a \neq 0$, and not both b and c are 0, then

$$\begin{aligned}
\varrho &= a\left(t + \frac{b+2c}{3} - \left(\frac{b-c}{3}\right)^2 t^{-1} + \dots\right),\\
\omega &= a\left(t + \frac{2b+c}{3} - \left(\frac{b-c}{3}\right)^2 t^{-1} + \dots\right),\\
\varepsilon &= \frac{b-c}{3} + \varrho - \omega.
\end{aligned}$$

If $D = M^3 - a$ with $M = bt + c$ where $a, b, c \in k$ and $ab \neq 0$, then

$$\begin{aligned}
\varrho &= bt + c - \frac{a}{3b^2} t^{-2} + \dots,\\
\omega &= b^2t^2 + 2bct + c^2 - \frac{2a}{3b} t^{-1} + \dots = \varrho^2,\\
\varepsilon &= bt + c - \varrho.
\end{aligned}$$

If $D = (M^3 - a)^2$ *with* $M = bt + c$ *where* $a, b, c \in k$ *and* $ab \neq 0$, *then*

$$\begin{aligned}\varrho &= b^2t^2 + 2bct + c^2 - \frac{2a}{3b}t^{-1} + \ldots = \omega^2,\\ \omega &= bt + c - \frac{a}{3b^2}t^{-2} + \ldots,\\ \varepsilon &= bt + c - \omega.\end{aligned}$$

P r o o f. Assume first that one of the three conditions on D above are satisfied.

If $\deg(G) = \deg(H) = 1$, then let $G = at + b$ and $H = at + c$ where $a, b, c \in k$, $a \neq 0$ and not both b and c are 0. Then $D = M^3 - F$ with $F \mid M^2$ where $M = at+c = H$ and $F = (c-b)(at+c)^2$. From Theorem 4.7, we obtain (after multiplying by $(b-c)/3$) $\varepsilon = (b-c)/3+\varrho-\omega$ and $R = \deg(M^3/F) = 1$. It is a simple matter to verify the expressions for ϱ and ω.

If $D = M^3 - a$ with $a \in k^*$ and $M \in k[t]$ linear, then it is easy to see that D is squarefree, so $\omega = \varrho^2$. Once again, the expressions for ϱ and ω are easily checked. By Theorem 3.4, $R = \deg(M) = 1$ and $\varepsilon = M - \varrho$.

If $D = (M^3 - a)^2$ with $a \in k^*$ and $M \in k[t]$ linear, then $\overline{D} = M^3 - a$, so we only need to reverse the roles of ϱ and ω in the previous setting to obtain the correct expressions for ε, ϱ, and ω in this case. Once again, $R = \deg(M) = 1$.

Now assume $R = 1$ and suppose that D is of neither of the forms described above. By Lemma 5.2, $\deg(D) = 3$ or $\deg(\overline{D}) = 3$. If $\deg(D) = 3$, then D is squarefree, as otherwise D would satisfy case 1. Hence $D = G$ and $\overline{D} = G^2$ with $\deg(G) = 1$. Similarly, if $\deg(\overline{D}) = 3$, then $\overline{D}$ is squarefree, so $D = H^2$ and $\overline{D} = H$ with $\deg(H) = 3$. Either way, one of D, $\overline{D}$ is squarefree of degree 3 and the other is the square of the first. Let $U \in \{D, \overline{D}\}$ have degree 3, say $U = a^3t^3 + bt^2 + ct + d$ with $a, b, c, d \in k$ and $a \neq 0$. Set $x = a^{-1}t - a^{-3}b/3$. Then $U = x^3 + rx + s$ for some $r, s \in k$. If $r = 0$, then $U = x^3 + s$, so D would satisfy case 2 or 3. Hence $r \neq 0$. Let $\widetilde{K} = k(x, \widetilde{\varrho})$ where $\widetilde{\varrho} \in k((1/x))$ with $\widetilde{\varrho}(x) = \varrho(t) = \varrho(ax + a^{-2}b/3)$. By Lemma 5.3, $\widetilde{R} > 1$ where $\widetilde{R}$ is the regulator of $\widetilde{K}$.

The map $\psi : k[t] \to k[t]$ that maps t onto x is a k-automorphism of the polynomial ring $k[t]$ which has natural extensions to k-automorphisms of $k(t)$, $\mathcal{O}$, K, and $k((1/t))$, respectively; in particular, $\widetilde{K} = \psi(K) = K$; however, elements in K are represented with respect to the variable t, whereas elements in $\widetilde{K}$ are expressed in terms of the variable x. ψ preserves degrees; that is, if $\alpha \in k((1/t))$, then $\deg_t(\alpha) = \deg_x(\psi(\alpha))$; here the subscript on the degree refers to the variable with respect to which the degree is taken. Since $0 = \deg_t(N(\varepsilon)) = \deg_x(\psi(N(\varepsilon)) = \deg_x(N(\psi(\varepsilon))$ and $2R = \deg_t(\varepsilon^{-1}) = \deg_x(\psi(\varepsilon^{-1})) = \deg_x(\psi(\varepsilon)^{-1})$, $\psi(\varepsilon)^{-1}$ is a unit in $\widetilde{K}$ of

degree $2R > 0$. Thus $\widetilde{R} \mid R$ (it is in fact easy to see that the two regulators are equal), contradicting $R = 1$ and $\widetilde{R} > 1$. ∎

We point out that by [3, 4], K has genus $\deg(GH) - 2$. Hence the fields identified in part 1 of Theorem 5.4 are rational (i.e. genus 0) function fields, whereas the fields described in parts 2 and 3 of the theorem and in Lemma 5.3 are elliptic (i.e. genus 1) function fields. Once again, we summarize our results in a table:

Table 2. Fields $K = k(t, \sqrt[3]{D})$ with regulator $R = 1$

D	Fundamental unit	Field type
GH^2 with $G, H \in k[t]$ linear and $\operatorname{sgn}(G) = \operatorname{sgn}(H)$	$\dfrac{G-H}{3} + \varrho - \omega$	Rational
$M^3 - a$ with $a \in k^*$ and $M \in k[t]$ linear	$M - \varrho$	Elliptic
$(M^3 - a)^2$ with $a \in k^*$ and $M \in k[t]$ linear	$M - \omega$	Elliptic

References

[1] M. Mang, *Berechnung von Fundamentaleinheiten in algebraischen, insbesondere rein-kubischen Kongruenzfunktionenkörpern*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1987.

[2] R. J. Rudman, *On the fundamental unit of a purely cubic field*, Pacific J. Math. 46 (1973), 253–256.

[3] R. Scheidler and A. Stein, *Voronoi's algorithm in purely cubic congruence function fields of unit rank* 1, Math. Comput. 69 (2000), 1245–1266.

[4] —, —, *Unit computation in purely cubic function fields of unit rank* 1, in: Proceedings of the Third Algorithmic Number Theory Symposium ANTS-III, Lecture Notes in Comput. Sci. 1423, Springer, Berlin, 1998, 592–606.

[5] H.-J. Stender, *Über die Grundeinheit für spezielle unendliche Klassen reiner kubischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 33 (1969), 203–215.

[6] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[7] H. C. Williams, *Some results on fundamental units in cubic fields*, J. Reine Angew. Math. 286/287 (1976), 75–85.

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, U.S.A.
E-mail: scheidle@math.udel.edu

Received on 23.3.1998
and in revised form 17.3.2000 (3354)