J. Korean Math. Soc. **54** (2017), No. 2, pp. 417–426
https://doi.org/10.4134/JKMS.j160002
pISSN: 0304-9914 / eISSN: 2234-3008

FUNDAMENTAL UNITS AND REGULATORS OF AN INFINITE FAMILY OF CYCLIC QUARTIC FUNCTION FIELDS

Jungyun Lee and Yoonjin Lee

Abstract. We explicitly determine fundamental units and regulators of an infinite family of cyclic quartic function fields L_h of unit rank 3 with a parameter h in a polynomial ring $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field of order q with characteristic not equal to 2. This result resolves the second part of Lehmer's project for the function field case.

1. Introduction

Lecacheux [9, 10] and Darmon [3] obtain a family of cyclic quintic fields over $\mathbb{Q}$, and Washington [22] obtains a family of cyclic quartic fields over $\mathbb{Q}$ by using coverings of modular curves. Lehmer's project [13, 14] consists of two parts; one is finding families of cyclic extension fields, and the other is computing a system of fundamental units of the families. Washington [17, 22] computes a system of fundamental units and the regulators of cyclic quartic fields and cyclic quintic fields, which is the second part of Lehmer's project.

We are interested in working on the second part of Lehmer's project for the families of function fields which are analogous to the type of the number field families produced by using modular curves given in [22]: that is, finding a system of fundamental units and regulators of families of cyclic extension fields over the rational function field $\mathbb{F}_q(t)$. In [11], we obtain the results for the quintic extension case. In this paper, we work on the quartic extension case; that is, we explicitly determine a system of fundamental units and regulators of the following infinite family of quartic function fields $\{L_h\}$ over $\mathbb{F}_q(t)$.

Received January 4, 2016.
2010 *Mathematics Subject Classification.* 11R29, 11R58.
Key words and phrases. regulator, function field, quintic extension.
The authors were supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2009-0093827), the first named author was also supported by the National Research Foundation of Korea(NRF) grant founded by the Korea government(2011-0023688), and the second named author by the National Research Foundation of Korea(NRF) grant founded by the Korea government(MEST)(2014-002731).

©2017 Korean Mathematical Society

Let $k = \mathbb{F}_q(t)$ be a rational function field and $L_h = k(\alpha_h)$ be a quartic extension over k generated by a root α_h of

$$F_h(x) = x^4 - h^2x^3 - (h^3 + 2h^2 + 4h + 2)x^2 - h^2x + 1,$$

where h is a monic polynomial in $\mathbb{F}_q[t]$ such that $h(h+2)(h^2+4)$ is square free in $\mathbb{F}_q[t]$. Then we show that $L_h = k(\alpha_h)$ is a real cyclic function field of unit rank three, and we explicitly determine a system of fundamental units and regulators of L_h as the following main theorem.

Theorem 1.1. *Let h be a monic polynomial in $\mathbb{F}_q[t]$ such that $h(h+2)(h^2+4)$ is square free in $\mathbb{F}_q[t]$. The regulator $R(L_h)$ of L_h is explicitly given by*

$$R(L_h) = 10(\deg h)^3.$$

Furthermore, a system of the fundamental units of L_h are $\{\alpha_h, \sigma(\alpha_h), \epsilon_h\}$ with the following unit group of L_h

$$U(L_h) = \mathbb{F}_q^* \times \langle \alpha_h, \sigma(\alpha_h), \epsilon_h \rangle,$$

where $\epsilon_h = h + \sqrt{h^2+4}$ and σ is a generator of the Galois group $Gal(L_h/k)$.

2. Preliminary

Let L_h and $F_h(x)$ be the same as given in Section 1. Then all four roots $\alpha_{h,1}, \alpha_{h,2}, \alpha_{h,3}, \alpha_{h,4}$ of $F_h(x)$ are as follows:

$$\frac{h^2 + (h+2)\sqrt{h^2+4} \pm \sqrt{2h(h+2)(h^2+4) + 2h^2(h+2)\sqrt{h^2+4}}}{4},$$
$$\frac{h^2 - (h+2)\sqrt{h^2+4} \pm \sqrt{2h(h+2)(h^2+4) - 2h^2(h+2)\sqrt{h^2+4}}}{4}.$$

Let $K_h = k(\sqrt{h^2+4})$. Then K_h is a unique quadratic subfield of L_h and the fundamental unit ϵ_h of K_h is $h + \sqrt{h^2+4}$. It is known that L_h is a cyclic extension over k with

$$\mathrm{Gal}(L_h/k) = \langle \sigma \rangle, \text{ and } \mathrm{Gal}(L_h/K_h) = \langle \sigma^2 \rangle,$$

where σ is defined by

$$\begin{aligned}\sigma(\alpha_h) = {} & (h + \frac{1}{h+2}) - (h^3 + h^2 + 3h + \frac{3}{h+2})\alpha_h \\ & + (-h^2 + h - 2 + \frac{3}{h+2})\alpha_h^2 + (1 - \frac{1}{h+2})\alpha_h^3.\end{aligned}$$

We have Lagrange resolvent $r_1 = \alpha_{h,1} + \alpha_{h,2}i - \alpha_{h,3} - \alpha_{h,4}i$ for L_h, where $i^2 = -1$, and we find

$$\mathcal{R}_1 = r_1^4 = h^2(h+2)^2(h^2+4)(h-2i)^2 \in \mathbb{F}_q(i)(t).$$

We notice that the discriminant D_{K_h} of K_h is h^2+4 and primes in k dividing h and $h+2$ are ramified in L_h; hence, according to *conductor-discriminant* formula, it follows that the discriminant D_{L_h} of L_h over k is given by

$$D_{L_h} = h^2(h+2)^2(h^2+4)^3.$$

Proposition 2.1. *The infinite prime $\wp_\infty$ of k splits completely in L_h; so L_h has unit rank 3, and L_h is a real function field.*

Proof. Let $\mathfrak{P}_\infty$ be an infinite prime of $k(\sqrt[4]{\mathcal{R}_1})$ lying over $\wp_\infty \in k$ and $\tilde{\wp}_\infty$ (resp. $\tilde{\mathfrak{P}}_\infty$) be the infinite prime of $k(i)$ (resp. $k(i, \sqrt[4]{\mathcal{R}_1})$) lying over $\wp_\infty$ (resp. $\mathfrak{P}_\infty$). Then we have

$$k(i)_{\tilde{\wp}_\infty} = \mathbb{F}_q(i)((t^{-1})) \text{ and } k(i, \sqrt[4]{\mathcal{R}_1})_{\tilde{\mathfrak{P}}_\infty} = \mathbb{F}_q(i, \sqrt[4]{\mathcal{R}_1})((t^{-1})).$$

If we express $\mathcal{R}_1 = h^2(h+2)^2(h^2+4)(h-2i)^2$ in $\mathbb{F}_q(i)((t^{-1}))$, we have

$$\mathcal{R}_1 = a_d^8 t^{8d} + \text{ lower terms on } t,$$

where $h = \sum_{i=0}^{d} a_i t^i$ for $a_i \in \mathbb{F}_q$, $(i = 0, 1, \ldots, d-1)$ and $a_d \in \mathbb{F}_q^*$. Thus we have

$$\sqrt[4]{\mathcal{R}_1} \in \mathbb{F}_q(i)((t^{-1}))$$

and

$$k(i, \sqrt[4]{\mathcal{R}_1})_{\tilde{\mathfrak{P}}_\infty} = \mathbb{F}_q(i, \sqrt[4]{\mathcal{R}_1})((t^{-1})) = \mathbb{F}_q(i)((t^{-1})) = k(i)_{\tilde{\wp}_\infty};$$

this implies that

$$k(\sqrt[4]{\mathcal{R}_1})_{\mathfrak{P}_\infty} = k_{\wp_\infty},$$

which completes the proof. □

The *infinite prime* $\wp_\infty$ of k splits completely in L_h; so we have $k \subseteq L_h \subseteq k_\infty = \mathbb{F}_q((t^{-1}))$, where k_∞ is the completion of k at $\wp_\infty$. For a nonzero element $a = \sum_{i=-m}^{\infty} c_i t^{-i} \in k_\infty$ with $m \in \mathbb{Z}$, $c_i \in \mathbb{F}_q (i \geq -m)$ and $c_{-m} \neq 0$, we define

$$\deg a = m.$$

Let $U(L_h)$ (resp. $U(K_h)$) be the unit group of the maximal order of L_h (resp. K_h). Let

$$U(L_h/K_h) := \{\, \epsilon \in U(L_h) \mid N_{L_h/K_h}(\epsilon) = \epsilon \cdot \sigma^2(\epsilon) \in \mathbb{F}_q^* \}.$$

It is known [4] that there is $\eta_h \in L_h$ with

$$U(L_h/K_h) = \mathbb{F}_q^* \times \langle \eta_h, \sigma(\eta_h) \rangle,$$

and we call η_h *a relative fundamental unit* of L_h over K_h.

Let $R(L_h)$ (resp. $R(K_h)$) be the regulator of L_h (resp. the regulator of K_h) and for ϵ_i $(i = 1, 2, 3) \in U(L_h)$,

$$\mathcal{R}(\epsilon_1, \epsilon_2, \epsilon_3) := \det \begin{pmatrix} \deg \epsilon_1 & \deg \epsilon_2 & \deg \sigma(\epsilon_3) \\ \deg \sigma(\epsilon_1) & \deg \sigma(\epsilon_2) & \deg \sigma^2(\epsilon_3) \\ \deg \sigma^2(\epsilon_1) & \deg \sigma^2(\epsilon_2) & \deg \sigma^3(\epsilon_3) \end{pmatrix}.$$

Let D_{L_h/K_h} (resp. $D_{L_h/k}$) denote the discriminant of L_h over K_h (resp. L_h over k).

3. Determination of relative fundamental units

In this section, we show that the relative fundamental unit η_h of L_h over K_h is equal to a root α_h of

$$F_h(x) = x^4 - h^2x^3 - (h^3 + 2h^2 + 4h + 2)x^2 - h^2x + 1$$

up to constant in $\mathbb{F}_q^*$. It is known [4] that

$$Q_{L_h} := [U(L_h) : U(K_h)U(L_h/K_h)] \in \{1, 2\}$$

and

$$\mathcal{R}(\epsilon_{K_h}, \eta_h, \sigma(\eta_h)) = Q_{L_h}R(L_h).$$

We note that for $\alpha \in U(L_h/K_h)$ and $\beta \in U(K_h)$, we have

$$\mathcal{R}(\beta, \alpha, \sigma(\alpha)) = 2\deg(\beta)\Big((\deg\alpha)^2 + (\deg\sigma(\alpha))^2\Big).$$

Thus, for determination of $R(L_h)$ and a relative unit η_h, we need a lower bound and an upper bound of $(\deg\eta_h)^2 + \deg(\sigma(\eta_h))^2$.

Proposition 3.1. *Let $\eta_h \in L_h$ be such that*

$$U(L_h/K_h) = \mathbb{F}_q^* \times \langle\eta_h, \sigma(\eta_h)\rangle.$$

Then we have

$$4.5(\deg h)^2 \le (\deg\eta_h)^2 + \deg(\sigma(\eta_h))^2 \le 5(\deg h)^2.$$

Proof. Since $\alpha_h \in U(L_h/K_h)$, we have for integers a, b

$$\alpha_h = \eta_h^a\sigma(\eta_h)^b$$

and

$$(\deg\alpha_h)^2 + (\deg\sigma(\alpha_h))^2 = (a^2 + b^2)\Big((\deg\eta_h)^2 + \deg(\sigma(\eta_h))^2\Big).$$

We note that

$$\alpha_h = h^2 + h + 1 + \frac{2}{h} + \cdots$$

and

$$\sigma(\alpha_h) = -h - 1 - \frac{1}{h} + \frac{2}{h^3} + \cdots.$$

Thus, we have

$$\deg\alpha_h = 2\deg h \text{ and } \deg\sigma(\alpha_h) = \deg h.$$

Finally, we obtain that

$$(\deg\eta_h)^2 + \deg(\sigma(\eta_h))^2 \le (\deg\alpha_h)^2 + (\deg\sigma(\alpha_h))^2 = 5(\deg h)^2.$$

Now, we note that

$$D_{L_h} = N_{K_h/k}(D_{L_h/K_h})D_{K_h}^2 = h^2(h+2)^2(h^2+4)^3.$$

Since $D_{K_h} = h^2 + 4$, we have that

$$N_{K_h/k}(D_{L_h/K_h}) = h^2(h+2)^2(h^2+4).$$

Moreover, we have

$$D_{L_h/K_h} \mid (\eta_h - \sigma^2(\eta_h))^2$$

and

$$N_{K_h/k}(D_{L_h/K_h}) \mid N_{K_h/k}(\eta_h - \sigma^2(\eta_h))^2.$$

Thus we have

$$h^2(h+2)^2(h^2+4) \mid (\eta_h - \sigma^2(\eta_h))^2(\sigma(\eta_h) - \sigma^3(\eta_h))^2.$$

We observe that for $c_1, c_2 \in \mathbb{F}_q^*$, $\sigma^2(\eta_h) = c_1/\eta_h,\ \sigma^3(\eta_h) = c_2/\sigma(\eta_h)$

$$\deg(\eta_h - c_1/\eta_h) = |\deg \eta_h|, \text{ and } \deg(\sigma(\eta_h) - c_2/\sigma(\eta_h)) = |\deg \sigma(\eta_h)|;$$

thus, we have

$$\begin{aligned}\deg h^2(h+2)^2(h^2+4) &\le 2|\deg \eta_h| + 2|\deg \sigma(\eta_h)|\\ &\le 2\sqrt{2}\Big((\deg \eta_h)^2 + (\deg \sigma(\eta_h))^2\Big)^{\frac{1}{2}},\end{aligned}$$

so that we get

$$\Big(\deg h^2(h+2)^2(h^2+4)\Big)^2 \le 8 \cdot \Big((\deg \eta_h)^2 + (\deg \sigma(\eta_h))^2\Big).$$

Consequently, we obtain that

$$4.5(\deg h)^2 \le (\deg \eta_h)^2 + (\deg \sigma(\eta_h))^2.$$

□

Theorem 3.2. *A root α_h of $F_h(x)$ is a relative fundamental unit of L_h over K_h up to constant in $\mathbb{F}_q^*$.*

Proof. Since $\alpha_h \in U(L_h/K_h)$, we have for integers a, b

$$\alpha_h = \eta_h^a \sigma(\eta_h)^b$$

and

$$(\deg \alpha_h)^2 + (\deg \sigma(\alpha_h))^2 = (a^2+b^2)\Big((\deg \eta_h)^2 + \deg(\sigma(\eta_h))^2\Big). \qquad (1)$$

From (1) and Proposition 3.1, it follows that

$$5(\deg h)^2 \ge 4.5(a^2+b^2)(\deg h)^2.$$

Thus, we have

$$a^2 + b^2 = 1;$$

this implies that α_h is $\eta_h^{\pm 1}$ or $\sigma(\eta_h)^{\pm 1}$, which completes the proof. □

4. Proof of the main result

In this section, we first compute Q_{L_h}, and we then complete the proof of Theorem 1.1. We need the following two lemmas. Lemma 4.1 is a criterion for determining whether Q_{L_h} is 1 or not. A similar criterion in the number field case is given in [4].

Lemma 4.1. *Let $U(K_h) = \mathbb{F}_q^* \times \langle \epsilon_h \rangle$ and $U(L_h/K_h) = \mathbb{F}_q^* \times \langle \eta_h, \sigma(\eta_h) \rangle$. If $c\epsilon_h \eta_h^{1-\sigma}$ is not a square in $U(L_h)$ for any $c \in \mathbb{F}_q^*$, then*

$$Q_{L_h} = 1.$$

Proof. Suppose that $Q_{L_h} \neq 1$. Then we can take $u \in U(L_h) - U(K_h)U(L_h/K_h)$. As $u^{1+\sigma^2} \in U(K_h)$, we have

$$u^{1+\sigma^2} = c_1 \epsilon_h^{2\lambda+1} \text{ or } u^{1+\sigma^2} = c_2 \epsilon_h^{2\lambda} \quad (c_1, c_2 \in \mathbb{F}_q^*).$$

If $u^{1+\sigma^2} = c_2 \epsilon_h^{2\lambda} \, (c_2 \in \mathbb{F}_q^*)$, then $\frac{u}{\epsilon_h^\lambda} \Big(\frac{u}{\epsilon_h^\lambda}\Big)^{\sigma^2} \in \mathbb{F}_q^*$ which implies that $u \in U(L_h/K_h)U(L_h/K_h)$. Thus we have $u^{1+\sigma^2} = c_1 \epsilon_h^{2\lambda+1} \quad (c_1 \in \mathbb{F}_q^*)$; so we get

$$c_1 \epsilon_h = \frac{u}{\epsilon_h^\lambda} \Big(\frac{u}{\epsilon_h^\lambda}\Big)^{\sigma^2}.$$

If we let $u_1 = \frac{u}{\epsilon_h^\lambda} \in U(L)$, then we have

$$c_1 \epsilon_h = u_1^{1+\sigma^2} \quad (c_1 \in \mathbb{F}_q^*).$$

Since $u_1^{1+\sigma} \in U(L_h/K_h)$, we have

$$u_1^{1+\sigma} = c_3 \eta_h^A \sigma(\eta_h)^B \quad (c_3 \in \mathbb{F}_q^* \text{ and } A, B \in \mathbb{Z}). \tag{2}$$

We note that if A and B have the same parity (that is, both are even or odd), then

$$\eta_h^A \sigma(\eta_h)^B = c_4 \Big(\eta_h^{\frac{A+B}{2}} \sigma(\eta_h)^{\frac{-A+B}{2}}\Big)^{1+\sigma} \quad (c_4 \in \mathbb{F}_q^*);$$

therefore, we get

$$\Big(u_1/(\eta_h^{\frac{A+B}{2}} \sigma(\eta_h)^{\frac{-A+B}{2}})\Big)^{1+\sigma} \in \mathbb{F}_q^*;$$

so we have $u_1 \in U(L_h/K_h)U(L_h/K_h)$, which is a contradiction. This shows that A and B have not the same parity. In other words, $A-1$ and B have same parity. Thus (2) implies that

$$\Big(u_1/(\eta_h^{\frac{A+B-1}{2}} \sigma(\eta_h)^{\frac{-A+B+1}{2}})\Big)^{1+\sigma} = c_3 \eta_h \quad (c_3 \in \mathbb{F}_q^*).$$

Since $(\eta_h^{\frac{A+B-1}{2}} \sigma(\eta_h)^{\frac{-A+B+1}{2}})^{1+\sigma^2} \in \mathbb{F}_q^*$, by letting

$$u_2 := \frac{u_1}{\eta_h^{\frac{A+B-1}{2}} \sigma(\eta_h)^{\frac{-A+B+1}{2}}},$$

we have

$$u_2^{1+\sigma} = c_3\eta_h \text{ and } u_2^{1+\sigma^2} = c_4\epsilon_h \quad (c_3, c_4 \in \mathbb{F}_q^*); \tag{3}$$

therefore,

$$c_5\epsilon_h\eta_h^{1-\sigma} = u_2^2 \text{ for } u_2 \in U(L_h) \text{ and } c_5 \in \mathbb{F}_q^*,$$

which completes the proof. □

We first show that $c\epsilon_h\eta_h^{1-\sigma}$ is not square in $U(L_m)$ for any $c \in \mathbb{F}_q^*$. Then by Lemma 4.1 we get

$$Q_{L_h} = 1.$$

It then follows that $R(L_h) = 10(\deg h)^3$ and

$$U(L_h) = \mathbb{F}_q^* \times \langle \alpha_h, \sigma(\alpha_h), \epsilon_h \rangle,$$

where $\epsilon_h = h + \sqrt{h^2+4}$.

It is thus enough to show that $c\epsilon_h\eta_h^{1-\sigma}$ is not square in $U(L_h)$ for any $c \in \mathbb{F}_q^*$. To determine whether $c\epsilon_h\eta_h^{1-\sigma}$ is a square in $U(L_h)$ or not, we need the following lemma.

Lemma 4.2. *Let E be a quadratic extension of F. If $\tau \in E$ is square in E, then $N_{E/F}(\tau)$, $Tr_{E/F}(\tau) + 2\sqrt{N_{E/F}(\tau)}$ and $Tr_{E/F}(\tau) - 2\sqrt{N_{E/F}(\tau)}$ are square in F.*

Proof. Using the following formulas in Proposition 3.1 in [15],

$$\sqrt{\tau} = \frac{\tau + \sqrt{N_{E/F}(\tau)}}{\sqrt{Tr_{E/F}(\tau) + 2\sqrt{N_{E/F}(\tau)}}} \quad \text{and}$$

$$\sqrt{\tau} = \frac{\tau - \sqrt{N_{E/F}(\tau)}}{\sqrt{Tr_{E/F}(\tau) - 2\sqrt{N_{E/F}(\tau)}}},$$

the result follows immediately. □

Proof of Theorem 1.1. In Theorem 3.2, we find that

$$\eta_h = c\alpha_h \ (c \in \mathbb{F}_q^*).$$

Let $\tau_h = c\epsilon_h\alpha_h/\sigma(\alpha_h)$ $(c \in \mathbb{F}_q^*)$. We note that

$$N_{L_h/K_h}(c\tau_h) = c^2\epsilon_h^2,$$

$$Tr_{L_h/K_h}(\tau_h) + 2\sqrt{N_{L_h/K_h}(\tau_h)} = c\epsilon_h\Big(-2h - h^2 - \frac{h^3}{2} - \frac{1}{2}h(h+2)\sqrt{h^2+4}\Big),$$

and

$$Tr_{L_h/K_h}(\tau_h) - 2\sqrt{N_{L_h/K_h}(\tau_h)} = c\epsilon_h\Big(-4 - 2h - h^2 - \frac{h^3}{2} - \frac{1}{2}h(h+2)\sqrt{h^2+4}\Big).$$

Let

$$\delta_{h,1} := c\epsilon_h\Big(-2h - h^2 - \frac{h^3}{2} - \frac{1}{2}h(h+2)\sqrt{h^2+4}\Big),$$

and

$$\delta_{h,2} := c\epsilon_h\Big(-4 - 2h - h^2 - \frac{h^3}{2} - \frac{1}{2}h(h+2)\sqrt{h^2+4}\Big).$$

Moreover, if $\delta_{h,1} \in K_h$ is square in K_h, then $N_{K_h/k}(\delta_{h,2})$ and $Tr_{K_h/k}(\delta_{h,1}) + 2\sqrt{N_{K_h/k}(\delta_{h,1})}$ and $Tr_{K_h/k}(\delta_{h,1}) - 2\sqrt{N_{K_h/k}(\delta_{h,1})}$ are square in k. We note that

$$N_{K_h/k}(\delta_{h,1}) = -c^2(4h^4 + 16h^3 + 32h^2 + 64h + 64),$$

which is not square in k for any $c \in \mathbb{F}_q^*$.

Moreover, if $\delta_{h,2} \in K_h$ is square in K_h, then $N_{K_h/k}(\delta_{h,2})$ and $Tr_{K_h/k}(\delta_{h,2}) + 2\sqrt{N_{K_h/k}(\delta_{h,2})}$ and $Tr_{K_h/k}(\delta_{h,2}) - 2\sqrt{N_{K_h/k}(\delta_{h,2})}$ are square in k. We note that

$$N_{K_h/k}(\delta_{h,2}) = -4c^2h^4. \tag{4}$$

If -1 is not square in O_k/q, then (4) is not square in k for any $c \in \mathbb{F}_q^*$. On the other hand, if -1 is square in O_k/q with$a^2 = -1$ in O_k/q, then we have

$$Tr_{K_h/k}(\delta_{h,2}) + 2\sqrt{N_{K_h/k}(\delta_{h,2})} = c(2a^2h^4 + 4a^2h^3 + (8a^2 + 4a)h^2 + 8a^2h)$$

and

$$Tr_{K_h/k}(\delta_{h,2}) - 2\sqrt{N_{K_m/k}(\delta_{h,2})} = c(2a^2h^4 + 4a^2h^3 + (8a^2 - 4a)h^2 + 8a^2h);$$

both are not square in k for any $c \in \mathbb{F}_q^*$.

Hence, from Lemma 4.2, it follows that $\delta_{h,1}$ and $\delta_{h,2}$ are not square in K_h and τ_h is not square in L_h. This completes the proof. □

5. Infinitely many family of quartic function fields

In this section, we show that there are infinitely many primes q such that $(h(t)^2 + 4)(h(t) + 2)h(t)$ is square free in $\mathbb{F}_q[t]$, where $h(t)$ is a given monic polynomial in $\mathbb{Z}[t]$. Consequently, Theorem 1.1 holds for infinitely many family of quartic function fields.

Lemma 5.1. *For a field K, a nonzero polynomial $f(x) \in K[x]$ is square free if and only if $f(x)$ is relatively prime to $f'(x)$ in $K[x]$.*

Proof. Let $f(x)$ be a nonzero polynomial in $K[x]$. If $f(x)$ is square free, then $f(x)$ and $f'(x)$ have no common factors in $K[x]$; thus they are relatively prime. For the converse, if we assume that $f(x)$ is not square free, then $f(x)$ and $f'(x)$ have some common factor in $K[x]$; so $f(x)$ and $f'(x)$ are not relatively prime in $K[x]$. □

Lemma 5.2. (1) *Let K be a field and $f(x) \in K[x]$ be a square free polynomial. Then for $g(x) \in K[x]$, if $f(g(x))$ is relatively prime to $g'(x)$, then $f(g(x))$ is square free in $K[x]$.*

(2) *For $f(x),\ g(x) \in \mathbb{Z}[x]$, if $f(g(x))$ is square free in $\mathbb{Q}[x]$, then $\overline{f}(\overline{g}(x)) \in \mathbb{F}_q[x]$ is square free for every prime q, where $\bar{f}$ (resp. $\bar{g}$) denotes the reduction of coefficients of f (resp. g) modulo q.*

Proof. (1) It is sufficient to show that $f(g(x))$ and $f'(g(x))g'(x)$ are relatively prime by Lemma 5.1. Since $f(x)$ is square free in $K[x]$, $f(x)$ and $f'(x)$ are relatively prime in $K[x]$; so $f(g(x))$ and $f'(g(x))$ are also relatively prime in $K[x]$. Thus, if $f(g(x))$ and $g'(x)$ are relatively prime by our assumption, then $f(g(x))$ is square free in $K[x]$.

(2) If $f(g(x))$ is square free in $\mathbb{Q}[x]$, $f(g(x))$ and $g'(x)$ are relatively prime in $\mathbb{Q}[x]$ by Lemma 5.1; hence, there exist $h_1(x)$ and $h_2(x)$ in $\mathbb{Q}[x]$ such that

$$f(g(x))h_1(x) + g'(x)h_2(x) = 1.$$

Thus we have

$$\bar{f}(\bar{g}(x))\bar{h}_1(x) + \bar{g}'(x)\bar{h}_2(x) = 1;$$

equivalently, $\bar{f}(\bar{g}(x))$ and $\bar{g}'(x)$ are relatively prime. It thus follows that $\overline{f}(\overline{g}(x))$ is square free in $\mathbb{F}_q[x]$ for every prime q from the part (1). □

Theorem 5.3. *Let $h(t)$ be of the type $t^k + c \in \mathbb{F}_q[t]$ with $(c^2+4)(c+2)c \in \mathbb{F}_q^*$. Then $(h(t)^2+4)(h(t)+2)h(t)$ is square free in $\mathbb{F}_q[t]$ for any power q of a prime except $q = 2$ or q dividing k.*

Proof. From Lemma 5.2(1), we obtain the result. □

References

[1] W. E. H. Berwick, *Algebraic number-fields with two independent units*, Proc. London Math. Soc. **34** (1932), 360–378.

[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1971.

[3] H. Darmon, *Note on a polynomial of Emma Lehmer*, Math. Comp. **56** (1991), no. 194, 795–800.

[4] M.-N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de* $\mathbb{Q}$, Publ. Math. Besançon, 1977/1978, fasc. **2**, pp. 1–26 & 1–53.

[5] ———, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1987), no. 177, 179–182.

[6] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkorpern*, Mathematische Abhandlungen, Band 3, Walter de Gruyter, Berlin (1975), 285–379, Originally published, 1950.

[7] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*, J. Number Theory **102** (2003), no. 1, 90–106.

[8] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J. **121** (1991), 1–13.

[9] O. Lecacheux, *Unités d'une famille de corps cycliques réeles de degré 6 liés* à *la courbe modulaire* $X_1(13)$, J. Number Theory **31** (1989), no. 1, 54–63.

[10] ———, *Unités d'une famille de corps liés* à *la courbe* $X_1(25)$, Ann. Inst. Fourier (Grenoble) **40** (1990), no. 2, 237–253.

[11] J. Lee and Y. Lee, *Fundamental units and regulators of quintic function fields*, preprint.

[12] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*, Experiment. Math. **12** (2003), no. 2, 211–225.

[13] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), no. 182, 535–541.

[14] D. H. Lehmer and E. Lehmer, *The Lehmer project*, Math. Comp. **61** (1993), no. 203, 313–317.

[15] S. R. Louboutin, *Hasse unit indices of dihedral octic CM-fields*, Math. Nachr. **215** (2000), 107–113.

[16] ______, *The simplest quartic fields with ideal class groups of exponents less than or equal to 2*, J. Math. Soc. Japan **56** (2004), no. 3, 717–727.

[17] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), no. 182, 543–556.

[18] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[19] Y. Y. Shen, *Unit groups and class numbers of real cyclic octic fields*, Trans. Amer. Math. Soc. **326** (1991), no. 1, 179–209.

[20] A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Experiment. Math. **8** (1999), no. 2, 119–133.

[21] F. Thaine, *Jacobi sums and new families of irreducible polynomials of Gaussian periods*, Math. Comp. **70** (2001), no. 236, 1617–1640.

[22] L. C. Washington, *A family of cyclic quartic fields arising from modular curve*, Math. Comp. **57** (1991), no. 196, 763–775.

[23] H. C. Williams and C. R. Zarnke, *Computer calculation of units in cubic fields*, Proceedings of the Second Manitoba Confference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972), pp. 433–468. Congressus Numerantium, No. VII, Utilitas Math., Winnipeg, Man., 1973.

[24] Z. Zhang and Q. Yue, *Fundamental units of real quadratic fields of odd class number*, J. Number Theory **137** (2014), 122–129.

Jungyun Lee
Institute of Mathematical Sciences
Ewha Womans University
Seoul 120-750, Korea
E-mail address: `lee9311@ewha.ac.kr`

Yoonjin Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: `yoonjinl@ewha.ac.kr`