<table>
<thead>
<tr>
<th>項目</th>
<th>結果</th>
</tr>
</thead>
<tbody>
<tr>
<td>タイトル</td>
<td>A Note on a Supersingular Function Field</td>
</tr>
<tr>
<td>契約</td>
<td>Washio, Tadashi; Kodama, Tetsuo</td>
</tr>
<tr>
<td>引用</td>
<td>長崎大学教育学部自然科学研究報告, vol.37, p.17-21; 1986</td>
</tr>
<tr>
<td>発行日</td>
<td>1986-02-28</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/32497">http://hdl.handle.net/10069/32497</a></td>
</tr>
</tbody>
</table>

NAOSITE: Nagasaki University’s Academic Output SITE

http://naosite.lb.nagasaki-u.ac.jp
1. Preliminary. The purpose of this note is to study the supersingularity of a certain hyperelliptic function field by using information about the Hasse-Witt matrix.

Let $K = \text{GF}(q)$ be a finite field of characteristic $p \neq 2$ and let $A = K(x, y)$ be an algebraic function field over $K$ defined by $y^2 = x^{2g+1} + a (a \neq 0, a \in K)$, where $g$ denotes a positive integer satisfying $(p, 2g + 1) = 1$. Using information about the Hasse-Witt matrix of $A$, the supersingularity of $A$ is studied only in the case that $2g + 1$ is a power of a prime number.

Then it is clear that the genus of $A$ is equal to $g$. Moreover, let us denote by $A_n$ the constant field extension of $A$ of degree $n$ ($n = 1, 2, \ldots$). It is clear that $A_n$ is the algebraic function field having $K_n = \text{GF}(q^n)$ as its exact field of constants.

Moreover, let us denote by $h_n$ the class number of $A_n$, i.e., the order of the finite group of divisor classes of degree zero in $A_n$.

Then, $A$ is said to be supersingular if $(p, h_n) = 1$ for all $n$. As is well known, the supersingularity is also stated as follows. The $L$-function of $A$ is put in the form

$$L(u) = 1 + a_1 u + a_2 u^2 + \ldots + a_g u^g + \ldots + q^{g-1} + a_{g+1} u^{g+1} + q^g u^{2g}.$$ 

Then $A$ is supersingular if and only if $a_1 = a_2 = \ldots = a_g = 0$ (mod. $p$) (Rosen[3], Stichtenoth[4]). Moreover, if we denote the $L$-function of $A_n$ by

$$L_n(u) = 1 + a_1^{(n)} u + \ldots + a_g^{(n)} u^g + \ldots + q^{ng} u^{2g},$$

then, using the Newton’s formulas, we have
\[ n a_n = a_1^{(1)} a_{n-1} + a_1^{(2)} a_{n-2} + \ldots + a_1^{(n-1)} a_1 + a_1^{(n)} \quad (n = 1, \ldots, g). \]

It is then well-known that
\[ a_1^{(n)} = N^{(n)} - q^n - 1. \]

So, if \( g < p \) and \( N^{(n)} \equiv 1 \pmod{p} \) \((n=1,\ldots,g)\), then \( a_1^{(n)} \equiv 0 \pmod{p} \) and hence \( a_n \equiv 0 \pmod{p} \) \((n=1,\ldots,g)\), i.e., \( A \) is supersingular.

On the other hand, let \( M = (a_{ij}) \) be the Hasse-Witt matrix of \( A \). Put
\[ M^{(p^n)} = (a_{ij}^{p^n}) \quad \text{and} \quad L^n = M^{(p^n)} M^{(p)} \ldots M^{(p^{r-1})} \quad (n = 1, \ldots, g), \]

where \( r \) means the integer such that \( K_n = GF(q^n) = GF(p^r) \).

Then, it is well-known that the relation between \( A \) and \( N^{(n)} \) is given by
\[ \text{Trace}(L^n) = 1 - N^{(n)} \]

where \( \overline{s} \) denotes the residue class of an integer \( s \) modulo \( p \) and it is identified with the element of \( K \) (Manin\[2\], Washio\[5\]).

Therefore, summing up, we get the following lemma.

**Lemma 1.** If \( g < p \) and \( \text{Trace}(L^n) = 0 \) for \( 1 \leq n \leq g \), then \( A \) is supersingular.

Moreover, we have known the following result about the Hasse-Witt matrix ([6]).

**Lemma 2.** Let \( M \) be the Hasse-Witt matrix with respect to the basis \( dx/y, xdx/y, \ldots, x^{2g+1}dx/y \) of the \( K \)-module of holomorphic differentials. Then, \( M = (a_{ij}) \) has at most one non-zero element in each row and in each column. Especially, for \( 1 \leq i, j \leq g \), \( a_{ij} \neq 0 \) if and only if \( i \equiv pj \pmod{2g+1} \).

2. Results. We will state the main results which will be proven in 3. Let
\[ K = GF(q) = GF(p^n) \]
be a finite field of characteristic \( p \neq 2 \) and let
\[ A = K(x, y) \]
be an algebraic function field over \( K \) defined by
\[ y^2 = x^{2g+1} + a \quad (a \neq 0, \ a \in K), \]

where \( g \) means a positive integer such that \( (p, 2g+1) = 1 \). Put
\[ f = 2g + 1 \]
and assume that \( f \) is a power of a prime number.

**Theorem 1.** Let \( t \) be the order of \( p \) in the finite cyclic group \( (\mathbb{Z}/f\mathbb{Z})^* = \mathbb{Z}/f\mathbb{Z} - \{0\} \). If \( g < p \) and \( t \) is even, then \( A \) is supersingular.

In the case of \( p \equiv -1 \pmod{f} \), it is evident that \( g < p \) and \( p^2 \equiv 1 \pmod{f} \) and so Theorem 1 leads to the following result.
COROLLARY 1. If \( p \equiv -1 \pmod{f} \), then \( A \) is supersingular.

In the case that \( p \) is a primitive root modulo \( f \), the order of \( p \) in \((\mathbb{Z}/f\mathbb{Z})^*\) is equal to \( \varphi(f) \). Since \( f \) is a power of an odd prime, \( \varphi(f) \) is even. Therefore, applying Theorem 1, we have the following result.

COROLLARY 2. If \( g < p \) and \( p \) is a primitive root modulo \( f \), then \( A \) is supersingular.

Clearly, if \( f \) is a prime number and \( q \) is a primitive root modulo \( f \), then \( A \) is supersingular and \( N^{(n)} \) is explicitly determined as follows.

THEOREM 2. \( f \) is a prime number and \( q \) is a primitive root modulo \( f \) if and only if \( N^{(n)} = q^n + 1 \) for \( n = 1, ..., g \). In this case,
\[
L(u) = 1 + q^u u^2 \eta \quad \text{and} \quad h = 1 + q^e,
\]
where \( h \) means the class number of \( A \).

3. Proofs. Let us now study the Hasse-Witt matrix \( M \) in the case that \( f = 2g + 1 \) is a power of an odd prime number.

LEMMA 3. Let \( t \) be the order of \( p \) in \((\mathbb{Z}/f\mathbb{Z})^*\). Assume that \( t \) is even and put \( t = 2d \). If \( rn \geq d \), then \( L^n = 0 \).

PROOF. We assume that \( L^n \neq 0 \). Then, because of
\[
L^n = MM^{(u)}...M^{(p^{rn-1})} = (a_{ij}^{(u)})(a_{ij}^{p^{rn-1}}),
\]
there exist some \( i_0, i_1, ..., i_n \) \((\leq i_0, i_1, ..., i_n \leq g)\) satisfying
\[
a_{i_0 i_1} a_{i_1 i_2} ... a_{i_{rn-1} i_{rn}} p^{rn-1} \neq 0.
\]
So, by making use of Lemma 2, we get the congruences
\[
i_0 \equiv p i_1 \pmod{f}, \quad i_1 \equiv p i_2 \pmod{f}, \quad ..., \quad i_{rn-1} \equiv p i_n \pmod{f}.
\]
From \( rn \geq d \), we see \( i_0 \equiv p^{e} i_d \equiv i_d \pmod{f} \) and so \( i_0 + i_d \equiv 0 \pmod{2g + 1} \). This is a contradiction to \( 1 \leq i_0, i_d \leq g \). Therefore we have \( L^n = 0 \).

COROLLARY. Assume that \( p \) is a primitive root modulo \( f \). If \( rn \geq g \), then \( L^n = 0 \). Especially, \( L^g = 0 \).

PROOF. The order of \( p \) in \((\mathbb{Z}/f\mathbb{Z})^*\) is equal to \( \varphi(f) \) and \( \varphi(f) \) is even. So, because of \( rn \geq g \geq \varphi(f)/2 \), Lemma 3 leads to \( L^n = 0 \).

LEMMA 4. Assume that the order of \( p \) in \((\mathbb{Z}/f\mathbb{Z})^*\) is even. Then all the diagonal elements of \( L^n \) are zero for \( n = 1, 2, ... \).
PROOF. We assume that some diagonal element is not zero. Then, there exist some $i_0, i_1, ..., i_{m-1}$ ($1 \leq i_0, i_1, ..., i_{m-1} \leq g$) satisfying

$$a_{i_0i_1}a_{i_1i_2}a_{i_2i_{m-1}}p^{m-1} \neq 0,$$

and so

$$i_0 \equiv p i_1 \pmod{f}, i_1 \equiv p i_2 \pmod{f}, ..., i_{m-1} \equiv p i_0 \pmod{f}.$$

Then, by renumbering, we have infinitely many congruences $i_k \equiv p i_{k+1} \pmod{f}$ ($k = 0, 1, 2, ...$) with $1 \leq i_0, i_1, ..., i_n \leq g$.

Thus, denoting by $2d$, the order of $p$ in $(\mathbb{Z}/f \mathbb{Z})^*$ we get $i_k \equiv p^d i_{k+1} \equiv -i_d \pmod{f}$ and hence $i_0 + i_d \equiv 0 \pmod{f}$. This contradicts with $1 \leq i_0, i_d \leq g$. So, all the diagonal elements of $L_n$ are zero for all $n$.

PROOF of Theorem 1. It is clear that the desired assertion follows at once from Lemmas 1 and 4.

PROOF of Theorem 2. The proof is done without using information about the Hasse-Witt matrix but with using quadratic characters. For $n=1, 2, ..., \text{let } \chi_n$ be the quadratic character of $K_n = GF(q)$ and let $d_n = (f, q^{n-1})$.

It is then well-known that

$$N^{(n)} = q^n + 1 + c_n,$$

where $c_n = \sum_{b \in K_n} \chi_n(b^f a) \quad \text{(Hasse[1])}.$

We assume that $f$ is a prime number and $q$ is a primitive root modulo $f$. Then, for $n=1, ..., g$, we get $q^n \equiv 1 \pmod{f}$ and so $d_n = 1$.

Therefore, because of $K_n = K_n^*$, we have

$$c_n = \sum_{b \in K_n} \chi_n(b+a) = \sum_{b \in K_n} \chi_n(b) = 0$$

and hence $N^{(n)} = q^n + 1$ which is the required result.

Conversely, let us assume that $N^{(n)} = q^n + 1$, i.e., $c_n = 0$ for $n=1, ..., g$. Then $c_n$ can be expressed in the form

$$c_n = d_n u_n + \chi_n(a) \quad (u_n \in \mathbb{Z}).$$

This implies that

$$d_n u_n = -\chi_n(a) = \pm 1.$$

Therefore we obtain $d_n = 1$ for $n=1, ..., g$.

Moreover, let $k$ be a prime divisor of $f = 2g + 1$. Then, according to $(k, p) = 1$, we see $(k, q^{k-1} - 1) = k$ and so $k \mid d_{k-1}$. This means that $k > g + 1$. Hence $k$ coincides with $f$, i.e., $f$ is a prime number.

Therefore, in view of $q^n \equiv 1 \pmod{f}$ for $n=1, ..., g$, it is clear that $q$ is a primitive root modulo $f$. In this case, we have $a_1^{(n)} = c_n = 0$ for $n=1, ..., g$.

So, because of $g < p$, the Newton's formulas lead to $a_n = 0$ for $n=1, ..., g$. 
Thus we get $L(u) = 1 + q^g u^{2g}$ and so $h = L(1) = 1 + q^g$. Hence Theorem 2 is completely proved.

References


