JOURNAL OF NUMBER THEORY 4, 118–143 (1972)

An Elementary Proof of the Hasse–Weil Theorem for Hyperelliptic Curves

S. A. STEPANOV

Mendeleev Institute of Chemical Technology, Miusskaja pl., 9, Moscow, U.S.S.R.

Communicated by H. Zassenhaus

Received December 22, 1969

An elementary proof is given of the Hasse-Weil theorem about the number of solutions of the hyperelliptic congruence $y^2 \equiv f(x) \pmod p$, where the polynomial $f(x)$ has odd degree.

1. INTRODUCTION

Let $n \geqslant 3$ be an odd number, let r be any natural number and $p > 9n^2$ be a prime number. Let k_{p^r} be the Galois field consisting of $q = p^r$ elements. We shall consider in k_{p^r} the equation

$$y^2 = f(x), \tag{1}$$

where $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ is a polynomial with integral rational coefficients.

Let J_{p^r} be the number of solutions of the Eq. (1) in k_{p^r}. For the case $r = 1$, the estimate

$$| J_p - p | \leqslant \sqrt{3n}\, n \sqrt{p}$$

is proved in [1]. In the present article we prove the following

THEOREM. *Let* $r \geqslant 1$. *Then*

$$| J_{p^r} - p^r | \leqslant \sqrt{3n}\, n \sqrt{p^r}.$$

From this theorem a stronger result can be deduced. Namely, the following statement is true:

COROLLARY. *For* J_{p^r} *we have the estimate*

$$| J_{p^r} - p^r | \leqslant (n - 1)\, p^{r/2}.$$

2. Lemmas

We divide the elements of k_{p^r} into three classes:

(I) Elements $\alpha \in k_{p^r}$, for which $f(\alpha) \neq 0$ and the equation $y^2 = f(\alpha)$ is solvable in k_{p^r}. Let J_{+1} be the number of such elements. Note that we have for such an element α

$$1 - f(\alpha)^{\frac{p^r-1}{2}} = 0.$$

(II) Elements $\beta \in k_{p^r}$ for which the equation $y^2 = f(\beta)$ is insolvable in k_{p^r}. Let J_{-1} be the number of such elements. For such an element β we have

$$1 + f(\beta)^{\frac{p^r-1}{2}} = 0.$$

(III) Elements $\gamma \in k_{p^r}$ for which $f(\gamma) = 0$. Let J_0 be the number of such elements.

It is clear that

$$J_{+1} + J_0 + J_{-1} = p^r.$$

Further,

$$J_{p^r} = 2J_{+1} + J_0 .$$

Finally, for any element $x \in k_{p^r}$ we have

$$x^{p^r} - x = 0.$$

Let D be the differentiation operator

$$D = 2\frac{d}{dx}$$

and let $\mathbf{Z}$ be the ring of integral rational numbers. We shall apply the operator D to rational functions of x with coefficients from $\mathbf{Z}$ and also to rational functions from the field $k_p(x)$. Since differentiation in $k_p(x)$ and differentiation of the rational functions with coefficients from $\mathbf{Z}$ are the same, modulo p, we shall use the same notation for these differentiations.

Lemma 1. *Let rational functions* $r_j^{(i)}(x)$, $i = 1, 2, \ldots$; $j = 1, 2, \ldots$ *be defined over* $\mathbf{Z}$ *by the recurrent relations*

$$r_j^{(i)} = Dr_j^{(i-1)} - 2jr_{j+1}^{(i-1)} - \frac{df}{dx} f^{-1} r_j^{(i-1)} \tag{2}$$

in terms of initial functions $r_1^{(0)}(x), r_2^{(0)}(x), \ldots$ *. Then*

$$r_j^{(i)} = \sum_{s=0}^{i} \sum_{t=0}^{i-s} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_i{}^s C_{i-s}^t G_t D^{i-s-t} r_{j+s}^{(0)},$$

where the rational functions $G_t(x)$ *with coefficients from* $\mathbf{Z}$ *are determined by the following relations*

$$G_0 = 1, \qquad G_t = DG_{t-1} - \frac{df}{dx} f^{-1} G_{t-1}, \qquad t = 1, 2, \ldots . \tag{3}$$

Proof. We shall prove Lemma 1 by induction on i. For $i = 1$ the statement is obvious, since

$$r_j^{(1)} = Dr_j^{(0)} - 2jr_{j+1}^{(0)} - \frac{df}{dx} f^{-1} r_j^{(0)}, \qquad j = 1, 2, \ldots .$$

Under the inductive assumption

$$r_j^{(i-1)} = \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t-1} r_{j+s}^{(0)} .$$

Then in view of (2) we have

$$r_j^{(i)} = \sum_{s=0}^{i-s} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t \left(DG_t - \frac{df}{dx} f^{-1} G_t\right)$$
$$\times D^{i-s-t-1} r_{j+s}^{(0)}$$
$$+ \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$
$$+ \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^{s+1} 2^{s+1} \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t-1} r_{j+s+1}^{(0)}$$
$$= \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t G_{t+1} D^{i-s-t-1} r_{j+s}^{(0)}$$
$$+ \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$
$$+ \sum_{s=1}^{i} \sum_{t=0}^{i-s} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^{s-1} C_{i-s}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$

$$= \sum_{s=0}^{i-1} \sum_{t=1}^{i-s} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^{t-1} G_t D^{i-s-t} r_{j+s}^{(0)}$$

$$+ \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$

$$+ \sum_{s=1}^{i-1} \sum_{t=0}^{i-s} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_{i-1}^{s-1} C_{i-s}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$

$$+ (-1)^i 2^i \frac{(j+i-1)!}{(j-1)!} r_{j+i}^{(0)}$$

$$= D^i r_j^{(0)} + \sum_{t=1}^{i} (C_{i-1}^{t-1} + C_{i-1}^t) G_t D^{i-t} r_j^{(0)}$$

$$+ \sum_{s=1}^{i-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} (C_{i-1}^s + C_{i-1}^{s-1}) D^{i-s} r_{j+s}^{(0)}$$

$$+ \sum_{s=1}^{i-1} \sum_{t=1}^{i-s-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!}$$

$$\times \{C_{i-s}^s (C_{i-s-1}^{t-1} + C_{i-s-1}^t) + C_{i-1}^{s-1} C_{i-s}^t\} G_t D^{i-s-t} r_{j+s}^{(0)}$$

$$+ \sum_{s=1}^{i-1} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} (C_{i-1}^s + C_{i-1}^{s-1}) G_{i-s} r_{j+s}^{(0)}$$

$$+ (-1)^i 2^i \frac{(j+i-1)!}{(j-1)!} r_{j+i}^{(0)}$$

$$= \sum_{s=0}^{i} \sum_{t=0}^{i-s} (-1)^s 2^s \frac{(j+s-1)!}{(j-1)!} C_i{}^s C_{i-s}^t G_t D^{i-s-t} r_{j+s}^{(0)}$$

and Lemma 1 is proved.

LEMMA 2. *Let rational functions* $r_j^{(i)}(x)$, $i = 1, 2, \ldots$; $j = 1, 2, \ldots$, *be defined by* (2) *in terms of initial functions* $r_1^{(0)}(x), r_2^{(0)}(x), \ldots$. *Further let rational functions* $t_j^{(i)}(x)$, $i = 1, 2, \ldots; j = 1, 2, \ldots$ *over* $\mathbf{Z}$ *be defined by means of the recurrent relations*

$$t_j^{(i)} = Dt_j^{(i-1)} - 2(j+1)\, t_{j+1}^{(i-1)} + \frac{df}{dx} f^{-1} r_{j+1}^{(i-1)} \tag{4}$$

in terms of initial functions $t_1^{(0)}(x), t_2^{(0)}(x), \ldots$ *. Then*

$$t_j^{(i)} = \sum_{s=0}^{i} (-1)^s 2^s \frac{(j+s)!}{j!} C_i{}^s D^{i-s} t_{j+s}^{(0)} + \sum_{s=0}^{i-1} \sum_{t=1}^{i-s} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_i{}^s C_{i-s}^t G_t D^{i-s-t} r_{j+s+1}^{(0)},$$

where $G_t(x)$ *is defined by* (3).

Proof. We shall prove Lemma 2 by induction on i. For $i = 1$ we have

$$t_j^{(1)} = Dt_j^{(0)} - 2(j+1)\, t_{j+1}^{(0)} + \frac{df}{dx} f^{-1} r_{j+1}^{(0)}$$

and therefore Lemma 2 is correct in this case. Under the inductive assumption

$$t_j^{(i-1)} = \sum_{s=0}^{i-1} (-1)^s 2^s \frac{(j+s)!}{j!} C_{i-1}^s D^{i-s-1} t_{j+s}^{(0)} + \sum_{s=0}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t-1} r_{j+s+1}^{(0)}.$$

Then by (2) and (4)

$$\begin{aligned} t_j^{(i)} = {} & \sum_{s=0}^{i-1} (-1)^s 2^s \frac{(j+s)!}{j!} C_{i-1}^s D^{i-s} t_{j+s}^{(0)} \\ & + \sum_{s=0}^{i-1} (-1)^{s+1} 2^{s+1} \frac{(j+s+1)!}{j!} C_{i-1}^s D^{i-s-1} t_{j+s+1}^{(0)} \\ & + \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t \left(DG_t - \frac{df}{dx} f^{-1} G_t\right) \\ & \times D^{i-s-t-1} r_{j+s+1}^{(0)} \\ & + \sum_{s=0}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t} r_{j+s+1}^{(0)} \\ & + \sum_{s=0}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+2} 2^{s+1} \frac{(j+s+1)!}{j!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t-1} r_{j+s+2}^{(0)} \end{aligned}$$

$$= \sum_{s=0}^{i-1} (-1)^s 2^s \frac{(j+s)!}{j!} C_{i-1}^s D^{i-s} t_{j+s}^{(0)}$$

$$+ \sum_{s=1}^{i} (-1)^s 2^s \frac{(j+s)!}{j!} C_{i-1}^{s-1} D^{i-s} t_{j+s}^{(0)}$$

$$+ \sum_{s=0}^{i-1} \sum_{t=0}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t G_{t+1} D^{i-s-t-1} r_{j+s+1}^{(0)}$$

$$+ \sum_{s=0}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^s C_{i-s-1}^t G_t D^{i-s-t} r_{j+s+1}^{(0)}$$

$$+ \sum_{s=1}^{i-1} \sum_{t=1}^{i-s} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_{i-1}^{s-1} C_{i-s}^t G_t D^{i-s-t} r_{j+s+1}^{(0)}$$

$$= \sum_{s=0}^{i} (-1)^s 2^s \frac{(j+s)!}{j!} C_i{}^s D^{i-s} t_{j+s}^{(0)} - \sum_{t=1}^{i} (C_{i-1}^{t-1} + C_{i-1}^t)\, G_t D^{i-t} r_{j+1}^{(0)}$$

$$+ (-1)^i 2^{i-1} \frac{(j+i-1)!}{j!} (C_{i-1}^{i-2} + C_{i-1}^{i-1})\, G_1 r_{j+i}^{(0)}$$

$$+ \sum_{s=1}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!}$$

$$\times \{C_{i-1}^s (C_{i-s-1}^{t-} + C_{i-s-1}^t) + C_{i-1}^{s-1} C_{i-s}^t\}\, G_t D^{i-s-t} r_{j+s+1}^{(0)}$$

$$+ \sum_{s=1}^{i-2} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} (C_{i-1}^s + C_{i-1}^{s-1})\, G_{i-s} r_{j+s+1}^{(0)}$$

$$= \sum_{s=0}^{i} (-1)^s 2^s \frac{(j+s)!}{j!} C_i{}^s D^{i-s} t_{j+s}^{(0)}$$

$$- \sum_{t=1}^{i} C_i{}^t G_t D^{i-t} r_{j+1}^{(0)} + (-1)^i 2^{i-1} \frac{(j+i-1)!}{j!} C_i^{i-1} G_1 r_{j+i}^{(0)}$$

$$+ \sum_{s=1}^{i-2} \sum_{t=1}^{i-s-1} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_i{}^s C_{i-s}^t G_t D^{i-s-t} r_{j+s+1}^{(0)}$$

$$+ \sum_{s=1}^{i-2} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_i{}^s G_{i-s} r_{j+s+1}^{(0)}$$

$$= \sum_{s=0}^{i} (-1)^s 2^s \frac{(j+s)!}{j!} C_i{}^s D^{i-s} t_{j+s}^{(0)}$$

$$+ \sum_{s=0}^{i-1} \sum_{t=1}^{i-s} (-1)^{s+1} 2^s \frac{(j+s)!}{j!} C_i{}^s C_{i-s}^t G_t D^{i-s-t} r_{j+s+1}^{(0)},$$

and Lemma 2 is proved.

LEMMA 3. *Let rational functions $G_t(x)$, $t = 1, 2, \ldots$ be defined by* (3) *and let $f(x) = \prod_{i=1}^{n} (x - x_i)$ be the decomposition of the polynomials $f(x)$ into linear factors in the algebraic closure of the field of rational numbers. Then*

$$G_t = \sum_{k=1}^{t} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=t}}^{t} \cdots \sum_{j_k=1}^{t} \sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \frac{a_{j_1,\ldots,j_k}^{(t)}}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_k})^{j_k}},$$

where the $a_{j_1,\ldots,j_k}^{(t)}$ are given by the recurrent relations

$$\begin{aligned} a_1^{(1)} &= -1 \\ a_{j_1,\ldots,j_k}^{(t)} &= -\sum_{r=1}^{k} (2(j_r - 1) + 1)\, a_{j_1,\ldots,j_r-1,\ldots,j_k}^{(t-1)}, \qquad t = 2, 3, \ldots \end{aligned} \tag{5}$$

Proof. We shall prove the lemma by induction on t. For $t = 1$ the statement is obvious. Under the inductive assumption

$$G_{t-1} = \sum_{k=1}^{t-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=t}}^{t-1} \cdots \sum_{j_k=1}^{t-1} \sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \sum_{r=1}^{k} \times \frac{a_{j_1,\ldots,j_r-1,\ldots,j_k}^{(t-1)}}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_r})^{j_r-1} \cdots (x - x_{i_k})^{j_k}}.$$

Then by (3)

$$\begin{aligned} G_t = {} & -2 \sum_{k=1}^{t-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=t}}^{t-1} \cdots \sum_{j_k=1}^{t-1} \sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \sum_{r=1}^{k} \sum_{s=1}^{k} \\ & \times \frac{(j_r - \delta_{rs})\, a_{j_1,\ldots,j_r-1,\ldots,j_k}^{(t-1)}}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_r})^{j_r-1} \cdots (x - x_{i_s})^{j_s+1} \cdots (x - x_{i_k})^{j_k}} \\ & - \sum_{k=1}^{t-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=t}}^{t-1} \cdots \sum_{j_k=1}^{t-1} \sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \sum_{i_{k+1}=1}^{n} \sum_{r=1}^{k} \\ & \times \frac{a_{j_1,\ldots,j_r-1,\ldots,j_k}^{(t-1)}}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_r})^{j_r-1} \cdots (x - x_{i_k})^{j_k} (x - x_{i_{k+1}})}, \end{aligned} \tag{6}$$

where δ_{rs} is Kronecker's symbol.

It is clear that G_t may be written in the form

$$G_t = \sum_{k=1}^{t} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=t}}^{t} \cdots \sum_{j_k=1}^{t} \sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \frac{a^{(t)}_{j_1,\ldots,j_k}}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_k})^{j_k}}. \tag{7}$$

If we now in (6) and (7) compare coefficients of the expression

$$\sum_{\substack{i_1=1 \\ i_1<i_2<\cdots<i_k}}^{n} \cdots \sum_{i_k=1}^{n} \frac{1}{(x - x_{i_1})^{j_1} \cdots (x - x_{i_k})^{j_k}},$$

we get

$$a^{(t)}_{j_1,\ldots,j_k} = -\sum_{r=1}^{k} (2(j_r - 1) + 1)\, a^{(t-1)}_{j_1,\ldots,j_r-1,\ldots,j_k}.$$

Thus Lemma 3 is proved.

LEMMA 4. *Let*

$$a^{(t)}_{j_1,\ldots,j_k},\ j_1 + \cdots + j_k = t; \qquad t = 1, 2, \ldots$$

be given by relations (5). *Then*

$$a^{(t)}_{j_1,\ldots,j_k} = (-1)^t \frac{t!}{j_1! \cdots j_k!} \prod_{s=1}^{k} \prod_{\tau=1}^{j_s} (2(j_s - \tau) + 1).$$

Proof. We shall prove the lemma by induction on t. For $t = 1$ the statement is obvious. Under the inductive assumption

$$a^{(t-1)}_{j_1,\ldots,j_r-1,\ldots,j_k} = (-1)^{t-1} \frac{(t-1)!}{j_1! \cdots (j_r - 1)! \cdots j_k!} \times \prod_{\substack{s=1 \\ s\neq r}}^{k} \prod_{\tau=1}^{j_s} (2(j_s - \tau) + 1) \prod_{\tau=1}^{j_r-1} (2(j_r - \tau - 1) + 1).$$

Then by (5)

$$a^{(t)}_{j_1,\ldots,j_k} = (-1)^t \sum_{r=1}^{k} \frac{(t-1)!}{j_1! \cdots (j_r - 1)! \cdots j_k!} \prod_{s=1}^{k} \prod_{\tau=1}^{j_s} (2(j_s - 1) + 1)$$

$$= (-1)^t \frac{t!}{j_1! \cdots j_k!} \prod_{s=1}^{k} \prod_{\tau=1}^{j_s} (2(j_s - \tau) + 1).$$

and thus Lemma 4 is proved.

LEMMA 5. *Let rational functions* $F_k^{(i)}$ *be given over* $\mathbf{Z}$ *by means of the recurrent relations*

$$
\begin{aligned}
F_1^{(1)} &= \frac{df}{dx} f^{-1}, \\
F_k^{(i)} &= DF_k^{(i-1)} + 2(k-1)\, F_{k-1}^{(i-1)} + \frac{df}{dx} f^{-1} F_k^{(i-1)}, \quad k = 1, 2,..., i-1, \\
F_i^{(i)} &= 2(i-1)\, F_{i-1}^{(i-1)} + 2^{i-1}(i-1)!\, \frac{df}{dx} f^{-1}.
\end{aligned} \tag{8}
$$

Then the relations

$$F_k^{(i)} = 2iF_{k-1}^{(i-1)}$$

hold for $k = 2, 3,..., i$.

Proof. We prove Lemma 5 by induction on i. Iterating the last of the relations (8) we get

$$F_i^{(i)} = 2^{i-1} i!\, F_1^{(1)}$$

and therefore the statement holds for $k = i$. In particular, the statement of the lemma for $i = 2$ follows from the last equality. Under the inductive assumption,

$$F_k^{(i-1)} = 2(i-1)\, F_{k-1}^{(i-2)}, \qquad F_{k-1}^{(i-1)} = 2(i-1)\, F_{k-2}^{(i-2)}.$$

Further,

$$F_{k-1}^{(i-1)} = DF_{k-1}^{(i-2)} + 2(k-2)\, F_{k-2}^{(i-2)} + \frac{df}{dx} f^{-1} F_{k-1}^{(i-2)}$$

and by (8)

$$
\begin{aligned}
2(i-1)\, F_{k-1}^{(i-1)} &= D2(i-1)\, F_{k-1}^{(i-2)} + 4(i-1)(k-2)\, F_{k-2}^{(i-2)} \\
&\quad + \frac{df}{dx} f^{-1} 2(i-1)\, F_{k-1}^{(i-2)} \\
&= DF_k^{(i-1)} + 2(k-2)\, F_{k-1}^{(i-1)} + \frac{df}{dx} f^{-1} F_k^{(i-1)} \\
&= F_k^{(i)} - 2F_{k-1}^{(i-1)}.
\end{aligned}
$$

Hence

$$F_k^{(i)} = 2iF_{k-1}^{(i-1)}.$$

Thus the lemma is proved.

LEMMA 6. *Let rational functions* $F_k^{(i)}$, $k = 1, 2, \ldots, i$; $i = 1, 2, \ldots$ *be defined by the recurrent relations* (8) *and let* $f(x) = \prod_{s=1}^{n} (x - x_s)$ *be the decomposition of the polynomial* $f(x)$ *into linear factors in the algebraic closure of the field of rational numbers. Then*

$$F_1^{(i)} = \sum_{k=1}^{i} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=i}}^{i} \cdots \sum_{j_k=1}^{i} \sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \frac{b_{j_1,\ldots,j_k}^{(i)}}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_k})^{j_k}},$$

where $b_{j_1,\ldots,j_k}^{(i)}$ *are given by the relations*

$$b_1^{(1)} = 1, \qquad b_{j_1,\ldots,j_k}^{(i)} = \sum_{r=1}^{k} (1 - 2(j_r - 1))\, b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)}. \tag{9}$$

Proof. We shall prove the lemma by induction on i. For $i = 1$ the statement is obvious, since

$$F_1^{(1)} = \sum_{s_1=1}^{n} \frac{1}{(x - x_{s_1})}.$$

Under the inductive assumption,

$$F_1^{(i-1)} = \sum_{k=1}^{i-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=i}}^{i-1} \cdots \sum_{j_k=1}^{i-1} \sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \sum_{r=1}^{k} \times \frac{b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)}}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_r})^{j_r-1} \cdots (x - x_{s_k})^{j_k}}.$$

Then by (8) we have

$$\begin{aligned} F_1^{(i)} = {} & -2 \sum_{k=1}^{i-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=i}}^{i-1} \cdots \sum_{j_k=1}^{i-1} \sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \sum_{r=1}^{k} \sum_{t=1}^{k} \\ & \times \frac{(j_t - \delta_{rt})\, b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)}}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_r})^{j_r-1} \cdots (x - x_{s_t})^{j_t+1} \cdots (x - x_{s_k})^{j_k}} \\ & + \sum_{k=1}^{i-1} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=i}}^{i-1} \cdots \sum_{j_k=1}^{i-1} \sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \sum_{s_{k+1}=1}^{n} \sum_{r=1}^{k} \\ & \times \frac{b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)}}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_r})^{j_r-1} \cdots (x - x_{s_k})^{j_k} (x - x_{s_{k+1}})}, \end{aligned} \tag{10}$$

where δ_{rt} is Kronecker's symbol. It is clear that $F_1^{(i)}$ may be written in the form

$$F_1^{(i)} = \sum_{k=1}^{i} \sum_{\substack{j_1=1 \\ j_1+\cdots+j_k=i}}^{i} \cdots \sum_{j_k=1}^{i} \sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \frac{b_{j_1,\ldots,j_k}^{(i)}}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_k})^{j_k}}. \quad (11)$$

If we now in (10) and (11) compare coefficients of the expression

$$\sum_{\substack{s_1=1 \\ s_1<s_2<\cdots<s_k}}^{n} \cdots \sum_{s_k=1}^{n} \frac{1}{(x - x_{s_1})^{j_1} \cdots (x - x_{s_k})^{j_k}},$$

we get

$$b_{j_1,\ldots,j_k}^{(i)} = \sum_{r=1}^{k} (1 - 2(j_r - 1))\, b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)}.$$

Thus Lemma 6 is proved.

LEMMA 7. *Let* $b_{j_1,\ldots,j_k}^{(i)}$, $j_1 + \cdots + j_k = i$; $i = 1, 2,\ldots$ *be defined by the recurrent relations* (9). *Then*

$$b_{j_1,\ldots,j_k}^{(i)} = \frac{i!}{j_1! \cdots j_k!} \prod_{t=1}^{k} \prod_{\tau=1}^{j_t} (1 - 2(j_t - \tau)).$$

Proof. We shall prove the lemma by induction on i. The statement of the lemma is obvious for $i = 1$. Under the inductive assumption,

$$b_{j_1,\ldots,j_r-1,\ldots,j_k}^{(i-1)} = \frac{(i-1)!}{j_1! \cdots (j_r - 1)! \cdots j_k!} \times \prod_{\substack{t=1 \\ t\neq r}}^{k} \prod_{\tau=1}^{j_t} (1 - 2(j_t - \tau)) \prod_{\tau=1}^{j_r-1} (1 - 2(j_r - \tau - 1)).$$

Further by (9) we have

$$b_{j_1,\ldots,j_k}^{(i)} = \sum_{r=1}^{k} \frac{(i-1)!}{j_1! \cdots (j_r - 1)! \cdots j_k!} \prod_{t=1}^{k} \prod_{\tau=1}^{j_t} (1 - 2(j_t - \tau))$$

$$= \frac{i!}{j_1! \cdots j_k!} \prod_{t=1}^{k} \prod_{\tau=1}^{j_t} (1 - 2(j_t - \tau))$$

and thus Lemma 7 is proved.

LEMMA 8. *The expressions $F_k^{(i)}$, $k = 1, 2,\dots, i$; $i = 1, 2,\dots$ defined by the recurrent relations* (8) *are rational functions with coefficients from* $\mathbf{Z}$ *of the form*

$$F_k^{(i)} = \frac{P_k^{(i)}}{f^{i-k+1}}$$

where the degree of the polynomial $P_k^{(i)}$ does not exceed

$$\nu_k^{(i)} = (i - k + 1)(n - 1).$$

Further, if $r_j^{(0)}(x)$, $t_j^{(0)}(x)$, $j = 1, 2,\dots$ are polynomials with coefficients from $\mathbf{Z}$, *then the expressions $r_j^{(i)}(x)$ and $t_j^{(i)}(x)$, $i = 1, 2,\dots$; $j = 1, 2,\dots$ defined by* (2) *and* (4) *are rational functions of the form*

$$r_j^{(i)} = \frac{R_j^{(i)}}{f^i}, \qquad t_j^{(i)} = \frac{T_j^{(i)}}{f^i}$$

with coefficients from $\mathbf{Z}$.

Proof. The second part of the statement follows easily from (2) and (4). The proof of the first part will be made by induction on i. For $i = 1$ the statement is obvious, since $F_1^{(1)} = df/dx\, f^{-1}$. In view of (8) the statement is also obvious for $k = i$, $i = 1, 2,\dots$. Under the inductive assumption,

$$F_k^{(i-1)} = \frac{P_k^{(i-1)}}{f^{i-k}}, \qquad F_{k-1}^{(i-1)} = \frac{P_{k-1}^{(i-1)}}{f^{i-k+1}},$$

where the degrees of the polynomials $P_k^{(i-1)}$ and $P_{k-1}^{(i-1)}$ do not exceed $(i - k)(n - 1)$ and $(i - k + 1)(n - 1)$ respectively. But for $i \neq k$

$$F_k^{(i)} = DF_k^{(i-1)} + 2(k - 1)\, F_{k-1}^{(i-1)} + \frac{df}{dx} f^{-1} F_k^{(i-1)}.$$

Further, it is clear that

$$DF_k^{(i-1)} = \frac{Q_k^{(i-1)}}{f^{i-k+1}}$$

and that the degree of the polynomial $Q_k^{(i-1)}$ does not exceed

$$(i - k + 1)(n - 1).$$

Hence

$$F_k^{(i)} = \frac{P_k^{(i)}}{f^{i-k+1}}$$

and the degree of polynomial $P_k^{(i)}$ does not exceed $(i - k + 1)(n - 1)$. Lemma 8 is proved.

LEMMA 9. *Let the rational functions* $F_k^{(i)}(x), r_j^{(i)}(x), t_j^{(i)}(x), k = 1, 2,..., i$; $i = 1, 2,...; j = 1, 2,...$ *be defined by the recurrent relations* (2), (4) *and* (8). *Let* $r_j^{(0)}(x)$ *and* $t_j^{(0)}(x), j = 1, 2,...,$ *be polynomials with coefficients from* $\mathbf{Z}$. *Then the polynomials* $P_k^{(i)}(x)$, $R_j^{(i)}(x)$ *and* $T_j^{(i)}(x)$, *which are the numerators of* $F_k^{(i)}(x)$, $r_j^{(i)}(x)$, *and* $t_j^{(i)}(x)$ *respectively, can be written in the form*

$$P_k^{(i)} = 2^{-i} i!\, \tilde{P}_k^{(i)}, \qquad R_j^{(i)} = 2^{-i} i!\, \tilde{R}_j^{(i)}, \qquad T_j^{(i)} = 2^{-i} i!\, \tilde{T}_j^{(i)},$$

where $\tilde{P}_k^{(i)}$, $\tilde{R}_j^{(i)}$, *and* $\tilde{T}_j^{(i)}$ *are polynomials with coefficients from* $\mathbf{Z}$.

Proof. First we prove that $(2j - 3)!!\, 2^j/j!$ is an integer for all $j = 2, 3,...$. We have

$$\frac{(2j-3)!!\, 2^j}{j!} = \frac{2(2j-2)!}{j!\,(j-1)!}.$$

On the other side,

$$\frac{(2j-3)!!\, 2^j}{j!} = \frac{4(2j-3)!}{j!\,(j-2)!}.$$

Define

$$A = \frac{(2j-2)!}{j!\,(j-2)!}, \qquad B = \frac{(2j-3)!}{j!\,(j-3)!}.$$

It is clear that A and B are integers. Further, we have

$$\frac{2A}{j-1} = \frac{4B}{j-2} \quad \text{or} \quad \frac{A}{j-1} = \frac{2B}{j-2}.$$

Hence $A(j - 2) = 2B(j - 1)$ or $A = (A - 2B)(j - 1)$ and therefore $A/j - 1 = A - 2B$ is an integer, so $(2j - 3)!!2^j/j!$ is also an integer.

We prove that $R_j^{(i)}$ and $T_j^{(i)}$ can be represented in the form

$$R_j^{(i)} = 2^{-i} i!\, \tilde{R}_j^{(i)}, \qquad T_j^{(i)} = 2^{-i} i!\, \tilde{T}_j^{(i)}.$$

In view of Lemmas 1 and 2, it is enough to prove that G_t, $t = 1, 2,...,$ can be written in the form $G_t = Q_t/f_t$ and that $Q_t = 2^{-t} t!\, \tilde{Q}_t$, where $\tilde{Q}_t$ is a polynomial with coefficients from $\mathbf{Z}$.

The first statement follows easily from (3). Further, in view of Lemma 3, to prove the second statement it is enough to show that

$$a^{(t)}_{j_1,\dots,j_k}, \; j_1 + \cdots + j_k = t; \qquad k = 1, 2,\dots, t; \quad t = 1, 2,\dots$$

can be represented in the form

$$a^{(t)}_{j_1,\dots,j_k} = 2^{-t} t! \, \tilde{a}^{(t)}_{j_1,\dots,j_k},$$

where

$$\tilde{a}^{(t)}_{j_1,\dots,j_k} \in \mathbf{Z}.$$

By Lemma 4,

$$\begin{aligned} a^{(t)}_{j_1,\dots,j_k} &= (-1)^t \frac{t!}{j_1! \cdots j_k!} \prod_{s=1}^{k} \prod_{\tau=1}^{j_s} (2(j_s - \tau) + 1) \\ &= (-1)^t \frac{t!}{j_1! \cdots j_k!} (2j_1 - 1)!! \cdots (2j_k - 1)!! . \end{aligned}$$

Hence

$$a^{(t)}_{j_1,\dots,j_k} = \frac{t!}{2^t} (-1)^t \frac{2^{j_1}(2j_1 - 1)!!}{j_1!} \cdots \frac{2^{j_k}(2j_k - 1)!!}{j_k!},$$

and so

$$\tilde{a}^{(t)}_{j_1,\dots,j_k} = (-1)^t \frac{2^{j_1}(2j_1 - 1)!!}{j_1!} \cdots \frac{2^{j_k}(2j_k - 1)!!}{j_k!}$$

is an integer.

To finish the proof of the lemma it remains to prove that $P^{(i)}_k$, $k = 1, 2,\dots, i$; $i = 1, 2,\dots$ can be represented in the form $P^{(i)}_k = 2^{-i} i! \, \tilde{P}^{(i)}_k$. We consider separately the cases $k > 1$ and $k = 1$. Let $k = 1$. In view of Lemma 6, it is enough to show that $b^{(i)}_{j_1,\dots,j_k}$, $j_1 + \cdots + j_k = i$; $k = 1, 2,\dots, i$; $i = 1, 2,\dots$ can be represented in the form

$$b^{(i)}_{j_1,\dots,j_k} = 2^{-i} i! \, \tilde{b}^{(i)}_{j_1,\dots,j_k},$$

where $\tilde{b}^{(i)}_{j_1,\dots,j_k} \in \mathbf{Z}$. By Lemma 7 we have

$$\begin{aligned} b^{(i)}_{j_1,\dots,j_k} &= \frac{i!}{j_1! \cdots j_k!} \prod_{t=1}^{k} \prod_{\tau=1}^{j_t} (1 - 2(j_t - \tau)) \\ &= (-1)^i \frac{i!}{j_1! \cdots j_k!} (2j_1 - 3)!! \cdots (2j_k - 3)!! \end{aligned}$$

and the last statement follows from the fact that

$$(-1)^i \frac{2^{j_1}(2j_1-3)!!}{j_1!} \cdots \frac{2^{j_k}(2j_k-3)!!}{j_k!}$$

is an integer.

Let now $k \geqslant 2$. In this case we shall prove the statement of the lemma by induction on i. For $i = 1$ the statement is obvious. Under the inductive assumption for $k \geqslant 2$

$$P_k^{(i-1)} = 2^{-i+1}(i-1)!\, \tilde{P}_k^{(i-1)}.$$

Moreover,

$$P_1^{(i-1)} = 2^{-i+1}(i-1)!\, \tilde{P}_1^{(i-1)}$$

and all $\tilde{P}_k^{(i-1)}$, $k = 1, 2,..., i-1$, have integer rational coefficients. By Lemma 5 we have $F_k^{(i)} = 2iF_{k-1}^{(i-1)}$ for $k = 2, 3,..., i$. Hence in view of Lemma 8 $P_k^{(i)} = 2iP_{k-1}^{(i-1)}$, and so $P_k^{(i)} = 2^{-i}i!\, \tilde{P}_k^{(i)}$. The lemma is proved.

3. Basic Construction

Let $m < p^r/2$ be a natural number. We consider the polynomial

$$S_0(x) = \left(1 + f^{\frac{p^r-1}{2}}\right) \sum_{j=1}^{2m} r_j^{(0)}(x)(x^{p^r} - x)^{j-1} + \sum_{j=1}^{2m} t_j^{(0)}(x)(x^{p^r} - x)^j,$$

where $r_j^{(0)}(x)$, $t_j^{(0)}(x)$ are polynomials with coefficients from $\mathbf{Z}$.

Define $S_i(x)$, $i = 1, 2,...$, in the following way:

$$S_i(x) = D^i S_0(x).$$

We shall say that the expression $S_i(x)$ has "necessary form" if it can be written as

$$S_i(x) = \left(1 + f^{\frac{p^r-1}{2}}\right) \sum_{j=1}^{2m} r_j^{(i)}(x)(x^{p^r} - x)^{j-1}$$
$$+ \sum_{j=1}^{2m} t_j^{(i)}(x)(x^{p^r} - x)^j + p^r U_i(x),$$

where $r_j^{(i)}(x)$, $t_j^{(i)}(x)$, $U_i(x)$ are rational functions with coefficients from the ring $\mathbf{Z}$.

LEMMA 10. *Let $S_{i-1}(x)$ have "necessary form". Then for the expression $S_i(x)$ to have "necessary form" it is sufficient that the relation*

$$2t_1^{(i-1)}(x) = \frac{df}{dx} f^{-1} r_1^{(i-1)}(x)$$

holds.

In that case, the rational functions $r_j^{(i)}(x)$, $t_j^{(i)}(x)$ are defined by relations (2) *and* (4) *respectively, and moreover,*

$$U_i(x) = \sum_{k=0}^{i-1} D^{i-k-1} H_k(x), \tag{12}$$

where

$$H_k(x) = \sum_{j=1}^{2m-1} \left(2j\left(1 + f^{\frac{p^r-1}{2}}\right) x^{p^r-1} r_{j+1}^{(k)} + f^{\frac{p^r-3}{2}} \frac{df}{dx} r_j^{(k)}\right) (x^{p^r} - x)^{j-1}$$
$$+ f^{\frac{p^r-3}{2}} \frac{df}{dx} r_{2m}^{(k)} (x^{p^r} - x)^{2m-1} + 2x^{p^r-1} \sum_{j=1}^{2m} jt_j^{(k)} (x^{p^r} - x)^{j-1}$$

Proof. We have

$$S_i(x) = (1 + f^{\frac{p^r-1}{2}})$$
$$\times \left(\sum_{j=1}^{2m} (Dr_j^{(i-1)})(x^{p^r} - x)^{j-1} - 2 \sum_{j=1}^{2m} (j-1)\, r_j^{(i-1)} (x^{p^r} - x)^{j-2}\right)$$
$$- f^{\frac{p^r-1}{2}} \frac{df}{dx} f^{-1} \sum_{j=1}^{2m} r_j^{(i-1)} (x^{p^r} - x)^{j-1} + \sum_{j=1}^{2m} (Dt_j^{(i-1)})(x^{p^r} - x)^j$$
$$- 2 \sum_{j=1}^{2m} jt_j^{(i-1)} (x^{p^r} - x)^{j-1} + 2p^r\left(1 + f^{\frac{p^r-1}{2}}\right) x^{p^r-1} \sum_{j=1}^{2m} (j-1)$$
$$\times r_j^{(i-1)} (x^{p^r} - x)^{j-2} + p^r f^{\frac{p^r-3}{2}} \frac{df}{dx} \sum_{j=1}^{2m} r_j^{(i-1)} (x^{p^r} - x)^{j-1}$$
$$+ 2p^r x^{p^r-1} \sum_{j=1}^{2m} jt_j^{(i-1)} (x^{p^r} - x)^{j-1} + p^r DU_{i-1}(x).$$

We add and subtract the expression

$$\frac{df}{dx} f^{-1} \sum_{j=1}^{2m} r_j^{(i-1)} (x^{p^r} - x)^{j-1}$$

in the right-hand side of the last equality. Then $S_i(x)$ can be written in the form

$$S_i(x) = (1 + f^{\frac{p^r-1}{2}}) \Bigg(\sum_{j=1}^{2m} (Dr_j^{(i-1)})(x^{p^r} - x)^{j-1}$$

$$- 2 \sum_{j=1}^{2m} (j-1)\, r_j^{(i-1)}(x^{p^r} - x)^{j-2} - \frac{df}{dx} f^{-1} \sum_{j=1}^{2m} r_j^{(i-1)}(x^{p^r} - x)^{j-1} \Bigg)$$

$$+ \frac{df}{dx} f^{-1} \sum_{j=1}^{2m} r_j^{(i-1)}(x^{p^r} - x)^{j-1} + \sum_{j=1}^{2m} (Dt_j^{(i-1)})(x^{p^r} - x)^j$$

$$- 2 \sum_{j=1}^{2m} jt_j^{(i-1)}(x^{p^r} - x)^{j-1} + p^r H_{i-1}(x) + p^r\, DU_{i-1}(x)$$

$$= (1 + f^{\frac{p^r-1}{2}}) \Bigg(\sum_{j=1}^{2m-1} \left(Dr_j^{(i-1)} - 2jr_{j+1}^{(i-1)} - \frac{df}{dx} f^{-1} r_j^{(i-1)} \right) (x^{p^r} - x)^{j-1}$$

$$+ \left(Dr_{2m}^{(i-1)} - \frac{df}{dx} f^{-1} r_{2m}^{(i-1)} \right) (x^{p^r} - x)^{2m-1} \Bigg)$$

$$+ \sum_{j=1}^{2m-1} \left(Dt_j^{(i-1)} - 2(j+1)\, t_{j+1}^{(i-1)} + \frac{df}{dx} f^{-1} r_{j+1}^{(i-1)} \right) (x^{p^r} - x)^j$$

$$+ (Dt_{2m}^{(i-1)})(x^{p^r} - x)^{2m} + \frac{df}{dx} f^{-1} r_1^{(i-1)} - 2t_1^{(i-1)} + p^r U_i(x).$$

The statement of the lemma follows from this in an obvious way.

LEMMA 11. *Let* $F_k^{(i)}$, $k = 1, 2, \ldots, i$; $i = 1, 2, \ldots$ *be defined by recurrent relations* (8). *In order that the expression* $S_i(x)$, $i = 1, 2, \ldots, 2m - 1$ *have "necessary form," it is sufficient that the relations*

$$2^{2i} t_i^{(0)} = \sum_{k=1}^{i} \tilde{F}_k^{(i)} r_k^{(0)}, \qquad i = 1, 2, \ldots, 2m - 1, \tag{14}$$

hold, where $\tilde{F}_k^{(i)}$ *are defined by the equalities*

$$F_k^{(i)} = 2^{-i} i!\, \tilde{F}_k^{(i)}. \tag{15}$$

Proof. We shall prove Lemma 11 by induction on i. For $i = 1$ the statement follows from Lemma 10. Let the statement hold for $i = j - 1$. We prove it for $i = j$. Consider the j relations

$$2^{2i} t_i^{(0)} = \sum_{k=1}^{i} \tilde{F}_k^{(i)} r_k^{(0)}, \qquad i = 1, 2, \ldots, j. \tag{16}$$

From these relations it follows for $j = 1$ that

$$2t_1^{(0)} = \frac{df}{dx} f^{-1} r_1^{(0)}$$

and hence the expression $S_1(x)$ has "necessary form." Moreover, for $i = 1$, the relations (2) hold. By (8) and (15),

$$iF_k^{(i)} = 2\left(D\tilde{F}_k^{(i-1)} + 2(k-1)\tilde{F}_{k-1}^{(i-1)} + \frac{df}{dx} f^{-1}\tilde{F}_k^{(i-1)}\right),$$
$$k = 1, 2, \ldots, i-1,$$
$$i\tilde{F}_i^{(i)} = 2\left(2(i-1)\tilde{F}_{i-1}^{(i-1)} + 2^{2(i-1)}\frac{df}{dx} f^{-1}\right).$$

Hence for $i = 2, 3, \ldots, j$, we have

$$\begin{aligned} 2^{2i} i t_i^{(0)} &= 2\sum_{k=1}^{i-1}\left(D\tilde{F}_k^{(i-1)} + 2(k-1)\tilde{F}_{k-1}^{(i-1)} + \frac{df}{dx} f^{-1}\tilde{F}_k^{(i-1)}\right) r_k^{(0)} \\ &\quad + 2\left(2(i-1)\tilde{F}_{i-1}^{(i-1)} + 2^{2(i-1)}\frac{df}{dx} f^{-1}\right) r_i^{(0)} \\ &= 2\sum_{k=1}^{i-1}(D\tilde{F}_k^{(i-1)})\, r_k^{(0)} + 2\sum_{k=1}^{i-1} 2k\tilde{F}_k^{(i-1)} r_{k+1}^{(0)} \\ &\quad + 2\frac{df}{dx} f^{-1}\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)} r_k^{(0)} + 2^{2i-1}\frac{df}{dx} f^{-1} r_i^{(0)}. \end{aligned}$$

We add and subtract the sum

$$2\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)}\, Dr_k^{(0)}$$

in the right-hand side of the last equality. Then we have

$$\begin{aligned} 2^{2i} i t_i^{(0)} &= 2\sum_{k=1}^{i-1}(D\tilde{F}_k^{(i-1)})\, r_k^{(0)} + 2\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)}\, Dr_k^{(0)} \\ &\quad - 2\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)}\, Dr_k^{(0)} + 2\sum_{k=1}^{i-1} 2k\tilde{F}_k^{(i-1)} r_{k+1}^{(0)} \\ &\quad + 2\frac{df}{dx} f^{-1}\sum_{k=1}^{i-1} F_k^{(i-1)} r_k^{(0)} + 2^{2i-1}\frac{df}{dx} f^{-1} r_i^{(0)} \\ &= 2D\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)} r_k^{(0)} - 2\sum_{k=1}^{i-1}\tilde{F}_k^{(i-1)}\left(Dr_k^{(0)} - 2kr_{k+1}^{(0)} - \frac{df}{dx} f^{-1} r_k^{(0)}\right) \\ &\quad + 2^{2i-1}\frac{df}{dx} f^{-1} r_i^{(0)}. \end{aligned}$$

Whence by (2)

$$2^{2i} i t_i^{(0)} = 2D \sum_{k=1}^{i-1} \tilde{F}_k^{(i-1)} r_k^{(0)} - 2 \sum_{k=1}^{i-1} \tilde{F}_k^{(i-1)} r_k^{(1)} + 2^{2i-1} \frac{df}{dx} f^{-1} r_i^{(0)}.$$

Apply the condition

$$2^{2(i-1)} t_{i-1}^{(0)} = \sum_{k=1}^{i-1} \tilde{F}_k^{(i-1)} r_k^{(0)}$$

and obtain

$$2^{2i} i t_i^{(0)} = 2^{2i-1} D t_{i-1}^{(0)} - 2 \sum_{k=1}^{i-1} \tilde{F}_k^{(i-1)} r_k^{(1)} + 2^{2i-1} \frac{df}{dx} f^{-1} r_i^{(0)}.$$

Hence in view of (2) we have

$$2^{2(i-1)} t_{i-1}^{(1)} = \sum_{k=1}^{i-1} \tilde{F}_k^{(i-1)} r_k^{(1)}, \qquad i = 2, 3,..., j.$$

By the hypothesis of induction, the validity of the last relations is sufficient to insure that the expressions $S_2(x),..., S_j(x)$ have "necessary form," hence the validity of the relations (16) is sufficient to insure that $S_1(x), S_2(x),..., S_j(x)$ have "necessary form." The lemma is proved.

LEMMA 12. *Let $g(x)$ be a polynomial, not identically zero, from the ring $K_p[x]$. Further let*

$$g(\alpha) = \frac{g'(\alpha)}{1!} = \frac{g''(\alpha)}{2!} = \cdots = \frac{g^{(i)}(\alpha)}{i!} = 0.$$

Then α is a root of the polynomial $g(x)$ of order at least $i + 1$.

Proof. We suppose that α is a root of $g(x)$ of order j and that $j < i + 1$. Then

$$g(x) = (x - \alpha)^j h(x), \qquad h(\alpha) \neq 0,$$

and we have

$$\frac{g^{(j)}(x)}{j!} = h(x) + \frac{r(x)(x - \alpha)}{j!}.$$

Under condition $g^{(j)}(\alpha)/j! = 0$ and hence $h(\alpha) = 0$. But, by assumption, $h(\alpha) \neq 0$, and this contradiction proves the lemma.

LEMMA 13. *For any natural number $m \leqslant \sqrt{p^r/3n}$ there exists a polynomial $S_0(x)$, not identically zero, in the ring $k_p[x]$, of degree at most*

$$\frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n$$

such that all elements of the second class are roots of $S_0(x)$ of order at least $2m$.

Proof. We shall try to find the polynomial $S_0(x)$ in the form

$$S_0(x) = (1 + f^{\frac{p^r-1}{2}}) \sum_{j=1}^{m} r_j^{(0)}(x)(x^{p^r} - x)^{j-1} + \sum_{j=1}^{m} t_j^{(0)}(x)(x^{p^r} - x)^j$$

with indeterminate polynomial-valued coefficients $r_j^{(0)}(x)$ and $t_j^{(0)}(x)$. We shall consider $S_0(x)$ as a polynomial over the ring $\mathbf{Z}$. However, we must avoid having all of the polynomials $r_j^{(0)}(x)$, $j = 1, 2,..., m$, identically zero modulo p.

Let $\tilde{F}_k^{(i)}$ be defined by equalities $\dot{F}_k^{(i)} = 2^{-i} i! \, \tilde{F}_k^{(i)}$ where the $F_k^{(i)}$ are given by (8). If we choose $r_j^{(0)}$ and $t_j^{(0)}$ so that the following relations over $\mathbf{Z}$ hold:

$$2^{2i} t_i^{(0)} = \sum_{k=1}^{i} \tilde{F}_k^{(i)} r_k^{(0)}, \qquad i = 1, 2,..., m, \tag{17}$$

$$0 = \sum_{k=1}^{m} \tilde{F}_k^{(i)} r_k^{(0)}, \qquad i = m + 1,..., 2m - 1, \tag{18}$$

then by Lemma 11 all the expressions $S_i(x)$, $i = 0, 1,..., 2m - 1$, have "necessary form".

Find a nontrivial solution over k_p of the system (18) in polynomials $r_k^{(0)}$. It follows from Lemmas 8 and 9 that the rational functions $\tilde{F}_k^{(i)}$ can be written in the form

$$\tilde{F}_k^{(i)} = \frac{\tilde{P}_k^{(i)}}{f^{i-k+1}}, \tag{19}$$

where $\tilde{P}_k^{(i)}$ are polynomials with integral rational coefficients, and the degree of $\tilde{P}_k^{(i)}$ does not exceed $\nu_k^{(i)} = (i - k + 1)(n - 1)$. Write

$$r_k^{(0)} = f^{m-k+1} r_k \,. \tag{20}$$

It is clear from (19) that in this case the system (18) is equivalent to the system

$$\sum_{k=1}^{m} \tilde{P}_k^{(i)} r_k = 0, \qquad i = m + 1,..., 2m - 1, \tag{21}$$

with polynomial coefficients $\tilde{P}_k^{(i)}$. Let

$$\tilde{P}_k^{(i)} = \sum_{j=0}^{\nu_k^{(i)}} a_{j,k}^{(i)} x^j, \qquad i = m+1,..., 2m-1; \quad k = 1, 2,..., m.$$

We write $\mu_k = (m^2 - m + k)(n-1)$ and look for r_k in the form

$$r_k = \sum_{l=0}^{\mu_k} b_{l,k} x^l.$$

Then system (21) can be written in the form

$$\sum_{q=0}^{\mu_k+\nu_k^{(i)}} \left(\sum_{k=1}^{m} \sum_{j+l=q} a_{j,k}^{(i)} b_{l,k} \right) x^q = 0, \qquad i = m+1,..., 2m-1.$$

In this case the following equalities

$$\sum_{k=1}^{m} \sum_{l=0}^{\mu_k} a_{q-l,k}^{(i)} b_{l,k} = 0,$$
$$q = 0, 1,..., \mu_k + \nu_k^{(i)}; \qquad i = m+1,..., 2m-1, \tag{22}$$

must hold. In the last system there are $M = \sum_{k=1}^{m} (\mu_k + 1)$ variables $b_{l,k}$ and $N \leqslant \sum_{i=m+1}^{2m-1} (\mu_k + \nu_k^{(i)} + 1)$ equations. We have

$$M = (n-1) \sum_{k=1}^{m} (k + m^2 - m) + m$$
$$= (n-1)\, m^3 - \frac{n-1}{2} m^2 + \frac{n+1}{2} m,$$

$$N \leqslant (n-1) \sum_{j=1}^{m-1} (j + m^2 + 1n) + m - 1$$
$$= (n-1)\, m^3 - \frac{n-1}{2} m^2 + \frac{n+1}{2} m - n.$$

Thus $M - N \geqslant 1n$ and system (22) has a nontrivial solution in elements $b_{l,k}$ of the ring $\mathbf{Z}$, where $b_{l,k}$ can be chosen so that not all of them are zero in k_p.

Further, let $t_j^{(0)}(x)$, $j = 1, 2,..., m$ be defined by (17). From (19) and (20) it is clear that all the $t_j^{(0)}$ are polynomials.

Let rational function $\tilde{r}_j^{(i)}$ and $\tilde{t}_j^{(i)}$ be defined by the equalities

$$r_j^{(i)} = 2^{-i} i!\, \tilde{r}_j^{(i)} \qquad t_j^{(i)} = 2^{-i} i!\, \tilde{t}_j^{(i)}.$$

Then by Lemmas 8 and 9, $\tilde{r}_j^{(i)}$ and $\tilde{t}_j^{(i)}$ can be written in the form

$$\tilde{r}_j^{(i)} = \frac{\tilde{R}_j^{(i)}}{f^i}, \qquad \tilde{t}_j^{(i)} = \frac{\tilde{T}_j^{(i)}}{f^i}, \tag{23}$$

where $\tilde{R}_j^{(i)}$, $\tilde{T}_j^{(i)}$ are polynomials with coefficients from **Z**.

In this case all the expressions $2^i[S_i(x)/i!]$, $i = 0, 1,..., 2m - 1$, can be written in the form

$$2^i \frac{S_i(x)}{i!} = (1 + f^{\frac{p^r-1}{2}}) \sum_{j=1}^{m} \tilde{r}_j^{(i)}(x)(x^{p^r} - x)^{j-1}$$
$$+ \sum_{j=1}^{m} \tilde{t}_j^{(i)}(x)(x^{p^r} - x)^j + \frac{2^i p^r}{i!} U_i(x),$$

where $U_i(x)$ are defined by (12) and (13). In view of Lemmas 8 and 9 and relation (13) it is clear that $H_k(x)$ are rational functions of the form

$$H_k = 2^{-k} k! \frac{\tilde{Q}_k}{f^k} , \tag{24}$$

where $\tilde{Q}_k(x)$ are polynomials with coefficients from **Z** .

We shall find an upper bound for the exponent of the highest power of the prime number p that divides $i!/k!(i - k - 1)!$, $i = 1, 2,..., 2m - 1$; $k = 1, 2,..., i - 1$. Let $\nu(i)$ be the exponent of p in $i!$. It is obvious that

$$\nu(i) = \left[\frac{i}{p}\right] + \left[\frac{i}{p^2}\right] + \cdots + \left[\frac{i}{p^s}\right].$$

But $m \leqslant \sqrt{p^r/3n}$ and so $i < p^{r/2}$. Hence we may write

$$\nu(i) = \frac{i}{p} + \frac{i}{p^2} + \cdots + \frac{i}{p^s} - \theta_s^{(i)},$$
$$\nu(k) = \frac{k}{p} + \frac{k}{p^2} + \cdots + \frac{k}{p^s} - \theta_s^{(k)},$$
$$\nu(i - k - 1) = \frac{i - k - 1}{p} + \frac{i - k - 1}{p^2} + \cdots + \frac{i - k - 1}{p^s} - \theta_s^{(i-k-1)},$$

where $0 \leqslant \theta_s^{(i)} < s$, $0 \leqslant \theta_s^{(k)} < s$, $0 \leqslant \theta_s^{(i-k-1)} < s$ and $s < r/2$. It follows that

$$\nu(i) - \nu(k) - \nu(i - k - 1)$$
$$= \theta_s^{(k)} + \theta_s^{(i-k-1)} - \theta_s^{(i)} + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^s}$$

from which

$$\nu(i) - \nu(k) - \nu(i-k-1) < 2s + \frac{(1-p^{-s})}{p-1}.$$

Since $2s < r$, for integers r and s we have $2s \leqslant r - 1$ and

$$\nu(i) - \nu(k) - \nu(i-k-1) < r.$$

In this case it follows from (12) and (14) that $(2^i p^r/i!)U_i(x)$ are rational functions of the form

$$\frac{2^i p^r}{i!} U_i = p \frac{V_i}{f^{i-1}}, \tag{25}$$

where $V_i(x)$ are polynomials with coefficients from $\mathbf{Z}$.

Now we consider the expressions $2^i(S_i(x)/i!)$, $i = 0, 1,..., 2m-1$, in the field $k_p(x)$. It follows from (25) that in this case

$$2^i \frac{S_i(x)}{i!} = (1 + f^{\frac{p^r-1}{2}}) \sum_{j=1}^{m} \tilde{r}_j^{(i)}(x)(x^{p^r} - x)^{j-1} + \sum_{j=1}^{m} \tilde{t}_j^{(i)}(x)(x^{p^r} - x)^j. \tag{26}$$

Note that $2^i(S_i(x)/i!)$ differs from $S_0^{(i)}(x)/i!$ only by a nonzero constant factor in k_p. Further, in view of (23) and (26) it is clear that all elements of the second class are zeros of the expressions $2^i(S_i(x)/i!)$, $i = 0, 1,...,$ $2m-1$, and hence also zeros of $S_0^{(i)}(x)/i!$.

We show that the polynomial $S_0(x)$ is not identically zero. Note that not all polynomials $r_j^{(0)}(x)$ are zero in $K_p[x]$. Denote the degree of the polynomial $r_k^{(0)}(x)$ by δ_k and the degree of the polynomial $t_i^{(0)}(x)$ by γ_i. Since the degree of the polynomial r_k does not exceed $(m^2 - m + k)(n-1)$ we get from (20) that $\delta_k \leqslant m^2(n-1) + m + n - k$. Further, by Lemma 8 and by (17) we have $\gamma_i \leqslant m^2(n-1) + m + n - i - 1$. But $p^r > 9n^2$ and $m \leqslant \sqrt{p^r/3n}$, so that

$$\begin{aligned} \delta_k + \frac{n}{2} &\leqslant m^2(n-1) + m + \frac{3n}{2} - k < \frac{p^r}{2}, \qquad k = 1, 2,..., m, \\ \gamma_i + \frac{n}{2} &\leqslant m^2(n-1) + m + \frac{3n}{2} - i - 1 < \frac{p^r}{2}, \quad i = 1, 2,..., m. \end{aligned} \tag{27}$$

The degree of the polynomial $(1 + f^{(p^r-1)/2})\, r_k^{(0)}(x^{p^r} - x)^{k-1}$ is equal to $\rho_k = (n/2)p^r - (n/2) + \delta_k + p^r(k-1)$ and the degree of the polynomial $t_i^{(0)}(x^{p^r} - x)^i$ is equal to $\omega_i = \gamma_i + p^r i$. Since n is odd, it follows from (27) that $\rho_k \neq \omega_i$ for any $i, k = 1, 2, \ldots, m$. Moreover, $\rho_j > \rho_k$, $\omega_j > \omega_k$ for $j > k$. Hence the terms

$$(1 + f^{\frac{p^r-1}{2}})\, r_1^{(0)},\ (1 + f^{\frac{p^r-1}{2}})\, r_2^{(0)}(x^{p^r} - x), \ldots, (1 + f^{\frac{p^r-1}{2}})\, r_m^{(0)}(x^{p^r} - x)^{m-1},$$
$$t_1^{(0)}(x^{p^r} - x),\ t_2^{(0)}(x^{p^r} - x)^2, \ldots, t_m^{(0)}(x^{p^r} - x)^m$$

in the polynomial $S_0(x)$ cannot cancel out. Then by Lemma 12 all elements of the second class are roots of the polynomial $S_0(x)$ of order at least $2m$.

Finally, we estimate the degree of $S_0(x)$. The degrees of the polynomials

$$(1 + f^{\frac{p^r-1}{2}})\, r_j^{(0)}(x^{p^r} - x)^{j-1}, \qquad j = 1, 2, \ldots, m,$$

do not exceed

$$\frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n.$$

The degrees of the polynomials $t_j^{(0)}(x^{p^r} - x)^j, j = 1, 2, \ldots, m$, do not exceed

$$mp^r + (n - 1) m^2 + n - 1.$$

Hence the degree of the polynomial $S_0(x)$ is at most

$$\frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n.$$

Lemma 13 is proved.

LEMMA 14. *For any natural number $m \leqslant \sqrt{p^r/3n}$ there exists a polynomial $T_0(x)$, not identically zero in the ring $k_p[x]$, of degree at most*

$$\frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n$$

such that all elements of the first class are roots of $T_0(x)$ of order at least $2m$.

Proof. The proof of this lemma is analogous to the proof of Lemma 13, with the difference that we now try to find the polynomial $T_0(x)$ in the form

$$T_0(x) = (1 - f^{\frac{p^r-1}{2}}) \sum_{j=1}^{m} S_j^{(0)}(x)(x^{p^r} - x)^{j-1} + \sum_{j=1}^{m} u_j^{(0)}(x)(x^{p^r} - x)^j.$$

4. Proof of the Theorem

The number of roots of a polynomial does not exceed its degree. So by Lemma 13,

$$2mJ_{-1} \leqslant \frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n,$$

or

$$2m(p^r - J_{+1} - J_0) \leqslant \frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n.$$

Therefore,

$$2m \left(p^r - \frac{J_{p^r}}{2} - \frac{J_0}{2}\right) \leqslant \frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n.$$

But $J_0 \leqslant n$. Hence,

$$2m \left(p^r - \frac{J_{p^r}}{2} - \frac{n}{2}\right) \leqslant \frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n.$$

Thus we get

$$J_{p^r} \geqslant p^r + \frac{p^r}{m} - (n - 1) m - \frac{n}{2} - \frac{p^r + 1}{2m} n. \tag{28}$$

By Lemma 14,

$$2m \frac{J_{p^r} - J_0}{2} \leqslant \frac{p^r - 1}{2} n + (m - 1) p^r + (n - 1) m^2 + n,$$

or

$$J_{p^r} \leqslant p^r - \frac{p^r}{m} + (n - 1) m + n + \frac{p^r + 1}{2m} n. \tag{29}$$

Take

$$m = \left[\sqrt{\frac{p^r}{3n}}\right].$$

Then by (28) and (29),

$$J_{p^r} \geqslant p^r - \sqrt{3n}\, n \sqrt{p^r}; \qquad J_{p^r} \leqslant p^r + \sqrt{3n}\, n \sqrt{p^r}.$$

Hence

$$| J_{p^r} - p^r | \leqslant \sqrt{3n}\, n \sqrt{p^r}.$$

The theorem is proved.

Finally let us show how the corollary follows from the theorem. By the theory of zeta-functions of fields of algebraic functions [2, p. 321],

$$J_{p^r} - p^r = \omega_1{}^r + \cdots + \omega_{2g}^r, \tag{30}$$

where $\omega_1, \ldots, \omega_{2g}$ are roots of the zeta-functions of the field $k_p(x, \sqrt{f(x)})$; in this case, $2g = n - 1$. Hence for any natural r

$$| \omega_1{}^r + \cdots + \omega_{n-1}^r | \leqslant \sqrt{3n}\, n \sqrt{p^r}.$$

From here it follows by elementary arguments [3, p. 138] that $| \omega_j | \leqslant \sqrt{p}$ so that from (30) we obtain

$$| J_{p^r} - p^r | \leqslant (n - 1)\, p^{r/2}.$$

References

1. С. А. Степанов, О числе точек гиперэллиптической кривой над простым конечным полем, *Izv. Akad. Nauk Series Math.* **33** (1969), 1171–1181.
2. M. Eichler, "Einführung in die Theorie der Algebraischen Zahlen and Funktionen" Birkhäuser Verlag Basel, Stuttgart, 1963.
3. S. Lang, "Abelian Varieties," Tracts in Pure and Applied Mathematics, No. 7., Intersciences, New York, 1959.