ON THE RAMIFICATION OF ALGEBRAIC FUNCTIONS

PART II: UNAFFECTED EQUATIONS FOR CHARACTERISTIC TWO

BY

SHREERAM ABHYANKAR

1. Introduction. Let V be an r -dimensional normal irreducible algebraic variety, $r \geq 2$, with function field K/k where k is algebraically closed of characteristic p , and let P be a simple point of V . In a previous paper (see Theorem 2 of [A1]) we have proved that if Q is a point corresponding to P on the normalization of V in a finite algebraic extension L of K such that the branch locus D on V for the extension⁽¹⁾ L/K has a t -fold normal crossing ($t \leq r$) at P , then the local galois group $G(Q/P)$ of Q over P is a p_t -group, (definitions in [A1]). Now we may raise the converse question, i.e., the following *construction problem*: Given a pure $(r-1)$ -dimensional subvariety D of V having a t -fold normal crossing at P and given a p_t -group G , does there exist Q (in some extension L of K) such that $G(Q/P) = G$ and D is the branch locus⁽²⁾ at P (for the extension L/K)? Recall that G is said to be a p_t -group if G/π is the direct product of at most t cyclic subgroups where π is the (normal) subgroup of G generated by all the p -syllow subgroups of G ($\pi = 1$ if $p = 0$); we shall say that G is a *quasi p -group* if G is generated by its p -syllow subgroups, i.e., if $G = \pi$, i.e., if every element of G is a product of elements whose orders are powers of p (we are now assuming $p \neq 0$). The essential part of the above problem is then the case when $t = 1$ and G is a quasi p -group. Observe that since every permutation is a product of transpositions, the symmetric group S_n on n symbols is a quasi 2-group⁽³⁾. In this paper we solve the construction problem for $p = 2$ and $G = S_n$. Since we are taking $t = 1$, i.e., D has a simple point at P , it is obvious that without loss of generality we may take $r = 2$.

Let

$$F(Z) = Z^n + F_1 Z^{n-1} + F_2 Z^{n-2} + \cdots + F_n,$$

where $F_1, F_2, \dots, F_n$ are elements in $k[x, y]$ to be determined. Suppose we can choose $F_1, \dots, F_n$ such that the following three conditions hold:

Presented to the Society December 29, 1956 under the title *Unaffected equations*; received by the editors March 4, 1957.

⁽¹⁾ I.e., the branch locus on V for the transformation between V and its L -normalization.

⁽²⁾ I.e., the component of the branch locus passing through P coincides with the component of D passing through P .

⁽³⁾ Also observe that if G is a simple group and if the order of G is divisible by p , then G is a quasi p -group, hence in particular if $5 \leq p \leq n$ then the alternating group A_n on n symbols is a quasi p -group. Since every element of A_n is a product of 3-cycles, A_n is a quasi 3-group (for any n).

- (1) $F(Z)$ is irreducible in $k((x, y))[Z]$.
- (2) The galois group of $F(Z)$ over $k((x, y))$ is S_n , i.e., the equation $F(Z) = 0$ is *unaffected* over $k((x, y))$.
- (3) The Z -discriminant of $F(Z)$ is $v^h d$, where v is a polynomial in x, y of leading degree one, h is a positive integer and d is a polynomial in x, y with nonzero constant term.

Since v is of leading degree one, we may take (x, y) to be regular parameters at P and $v=0$ as the local equation of D at P . Let L be an extension of K gotten by adjoining a root of $F(Z)$ to K and let L^* be a root field of $F(Z)$ over K (i.e., L^* = a least normal extension of K containing L). Then from the results of [A1] and §2 of [A2] it follows that:

(I) There is only one point Q corresponding to P on the L -normalization of V , $D: v=0$ is the branch curve on V at P for the extension L/K , and $G(Q/P) = S_n$.

(II) There is only one point Q^* corresponding to P on the L^* -normalization of V , $D: v=0$ is the branch curve on V at P for the extension of L^*/K , and $G(Q^*/P) = G(L^*/K) = S_n$.

For $n=1$, $L=K$ and the problem makes no sense. For $n=2$, we may take $F_1 = xF_1^*$ and $F_2 = xF_2^*$ where F_1^* is an arbitrary nonzero polynomial in x and F_2^* is an arbitrary polynomial in x, y with a nonzero constant term; then conditions (1), (2), (3) are obviously satisfied. Having gotten rid of these trivialities, we may assume that $n > 2$.

In Chapter I, for even n we shall construct an $\infty^{(n-2)/2}$ family of polynomials $F_1, \dots, F_n$ (in x, y) satisfying conditions (1), (2), (3) which would yield that many coverings of V of the required type. In §6 we give an $\infty^{(n-3)/2}$ family of coverings of the required type in case n is prime. For the general case of odd n , in §§7 and 8, we give two $\infty^{(n-3)/2}$ families of coverings of the required type.

2. Notations. We let $m = n - 2$ ($m > 0$). For a polynomial $h(Z)$ we shall denote by $Dh(Z)$ and Z -discriminant of $h(Z)$. For $t \in k[[x, y]]$ we shall let

$$d(t) = \text{leading degree of } t \text{ in } x \text{ and } y,$$

$$d_x(t) = \text{leading degree of } t \text{ in } x,$$

$$d_y(t) = \text{leading degree of } t \text{ in } y.$$

Observe that $d(0) = d_x(0) = d_y(0) = \infty$. Note that since we are in characteristic two, we shall not need to use the minus sign.

In the proofs we shall tacitly invoke the following fact: If H is a prime ideal in (the unique factorization domain) $k[[x, y]]$ such that $F(Z)$ has no multiple roots mod H , then the galois group of $F(Z)$ mod H (over the quotient field of $k[[x, y]]/H$) as a permutation group on the suitably arranged roots is a subgroup of the galois group of $F(Z)$ over $k((x, y))$, (see §61 of [V]). The prime ideals used will be the one generated by x and the one generated by y ; note that $k[[x, y]]/(x) = k[[y]]$ and $k[[x, y]]/(y) = k[[x]]$.

I. EVEN n

3. The galois group. Let

$$R(Z) = Z^m + R_1 Z^{m-1} + R_2 Z^{m-2} + \cdots + R_m = \prod_{i=1}^m (Z + u_i);$$

$$S(Z) = Z^m + xR_1 Z^{m-1} + x^2 R_2 Z^{m-2} + \cdots + x^m R_m = \prod_{i=1}^m (Z + xu_i);$$

$$\begin{aligned} f(Z) &= (Z^2 + x^{a+1}Z + x)S(Z) \\ &= Z^n + f_1 Z^{n-1} + f_2 Z^{n-2} + \cdots + f_n; \end{aligned}$$

where a is a nonnegative integer to be chosen and $u_1, u_2, \dots, u_m$ are distinct nonzero elements of $k[[x]]$ to be chosen. Let

$$g(Z) = (Z^{n-1} + y)Z = Z^n + yZ;$$

and let

$$F(Z) = f(Z) + g(Z) + Z^n \in k[[x, y]][Z].$$

Then

$$F(Z) = Z^n + f_1 Z^{n-1} + f_2 Z^{n-2} + \cdots + f_{n-2} Z^2 + (f_{n-1} + y)Z + f_n.$$

Since $f_i \equiv 0 \pmod{x}$ for $i=1, \dots, n$, we have

$$F(Z) = \begin{cases} g(Z) & [\text{mod } x], \\ f(Z) & [\text{mod } y]. \end{cases}$$

Now $Z^{n-1} + y$ is irreducible in $k[[y]][Z]$ and hence in $k((y))[Z]$. Since $n-1 \not\equiv 0(2)$, the galois group of $Z^{n-1} + y$, i.e., the galois group of $g(Z)$ over $k((y))$ is cyclic of order $n-1$ and if viewed as a permutation group on the roots of $g(Z)$ it is generated by an $(n-1)$ -cycle.

Since $g(Z)$ has no multiple roots and since $F(Z) \equiv g(Z) \pmod{x}$, $F(Z)$ has no multiple roots.

Again $Z^2 + x^{a+1}Z + x$ is irreducible in $k[[x]][Z]$ and hence in $k((x))[Z]$, also its roots are distinct. Therefore its galois group, i.e., the galois group of $f(Z)$ over $k((x))$ is cyclic of order 2 and if viewed as a permutation group on the roots of $f(Z)$ it is generated by a 2-cycle.

Let G be the galois group of $F(Z)$ over $k((x, y))$ viewed as a permutation group on the roots of $F(Z)$, i.e., as a subgroup of the symmetric group S_n on n -symbols. Since $F(Z) \equiv f(Z) \pmod{y}$, G contains an $(n-1)$ -cycle and since $F(Z) \equiv g(Z) \pmod{x}$, G contains a 2-cycle. Suppose if possible that $F(Z)$ is reducible in $k((x, y))[Z]$ and hence in $k[[x, y]][Z]$. Since $F(Z) \equiv g(Z) \pmod{x}$, $F(Z)$ must have a linear factor $Z + t$ with $t = t(x, y) \in k[[x, y]]$. Let $d_x(t) = b$. Since $F(Z) \equiv g(Z) \pmod{x}$, $t(0, y) = 0$, i.e., $b > 0$. Since $F(Z) \equiv f(Z) \pmod{y}$, $t(x, 0) = xu_i$ for some i , say $t(x, 0) = xu_1$; then

$$\infty > d_x(xu_1) \geq d_x(t) = b.$$

Now

$$f_n = (xu_1xu_2 \cdots xu_m)x, \quad \text{and} \quad f_{n-1} \in k[[x]].$$

Hence

$$d_x(f_n) \geq d_x(x^m x u_1) \geq m + b > b \quad \text{and} \quad d_x(f_{n-1} + y) = 0.$$

Now $F(t) = 0$ implies

$$(f_{n-1} + y)t = t^n + f_1 t^{n-1} + f_2 t^{n-2} + \dots + f_{n-2} t^2 + f_n.$$

Therefore

$$\begin{aligned} b &= d_x[(f_{n-1} + y)t] = d_x(t^n + f_1 t^{n-1} + \dots + f_{n-2} t^2 + f_n) \\ &\geq \min [d_x(t^n), d_x(f_1 t^{n-1}), \dots, d_x(f_{n-2} t^2), d_x(f_n)] \\ &\geq \min [d_x(t^2), d_x(f_n)] \\ &> b. \end{aligned}$$

This being a contradiction, we conclude that $F(Z)$ is irreducible in $k((x, y))[Z]$ and hence G is transitive. Thus G is a transitive subgroup of S_n containing a 2-cycle and an $(n-1)$ -cycle. Hence by Lemma 1, §10, $G = P_n$.

4. The discriminant. Now

[illegible]

We want to arrange matters so that the coefficients of the odd powers in $f(Z)$ other than Z are all zero, i.e.,

$$\begin{aligned} x^{a+1} + xR_1 &= 0, \\ x^2R_1 + x^{a+3}R_2 + x^3R_3 &= 0, \\ x^4R_3 + x^{a+5}R_4 + x^5R_5 &= 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot &, \\ x^{m-2}R_{m-3} + x^{a+m-1}R_{m-2} + x^{m-1}R_{m-1} &= 0; \end{aligned}$$

i.e.,

$$F'(Z) = x^m d + y.$$

Therefore

$$DF(Z) = (x^m d + y)^n.$$

Since the $m/2$ parameters $R_2, R_4, \dots, R_m$ are arbitrary we get an $\infty^{m/2}$ family of coverings of the required type.

II. ODD n

Let

$$\begin{aligned} S(Z) &= Z^m + S_1 Z^{m-1} + S_2 Z^{m-2} + \cdots + S_m, \\ f(Z) &= Z^n + f_1 Z^{n-1} + f_2 Z^{n-2} + \cdots + f_m \\ &= (Z^2 + x^a Z + x)S(Z) \\ &= Z^{m+2} + (x^a + S_1)Z^{m+1} + (x + x^a S_1 + S_2)Z^m \\ &\quad + (xS_1 + x^a S_2 + S_3)Z^{m-1} \\ &\quad + (xS_2 + x^a S_3 + S_4)Z^{m-2} \\ &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &\quad + (xS_{m-2} + x^a S_{m-1} + S_m)Z^2 \\ &\quad + (xS_{m-1} + x^a S_m)Z + xS_m, \end{aligned}$$

where a (an integer) ≥ 1 and $S_1, S_2, \dots, S_m$ are elements to be determined in $k[x]$ of positive leading degrees: Let

$$g(Z) = Z^n + y.$$

Since $g(Z)$ is irreducible in $k((y))[Z]$ and since $n \equiv 0(2)$, the galois group of $g(Z)$ over $k((y))$ as a permutation group on the roots of $g(Z)$ is generated by an n -cycle. Let

$$F(Z) = f(Z) + g(Z) + Z^n.$$

Then

$$F(Z) = Z^n + f_1 Z^{n-1} + \cdots + f_{n-1} Z + f_n + y,$$

so that

$$F(Z) \equiv \begin{cases} g(Z) & [\text{mod } x], \\ f(Z) & [\text{mod } y]. \end{cases}$$

Since $F(Z) \equiv g(Z) \pmod{x}$, $F(Z)$ is free from multiple roots and irreducible in $k((x, y))[Z]$ and the galois group G of $F(Z)$ over $k((x, y))$ considered as a permutation group on the roots of $F(Z)$, i.e., as a subgroup of S_n , is transitive and contains an n -cycle.

5. **A special case, n prime.** Suppose we try to arrange matters so that

where $u_1, \dots, u_m$ are distinct elements in $k[[x]]$; $f_2, f_4, \dots, f_{n-1}$ are polynomials in x without constant terms (and they depend on the $(m-1)/2$ free parameters $R_2, R_4, \dots, R_{m-1}$) and d is a polynomial in x with a nonzero constant term. Hence the galois group of $f(Z)$ over $k((x))$ is generated by a 2-cycle. Now

$$\begin{aligned} F(Z) &= Z^n + f_2 Z^{n-2} + f_4 Z^{n-4} + \dots + f_{n-1} Z + (x^{n-1}d + y), \\ F'(Z) &= Z^{n-1} + f_2 Z^{n-3} + f_4 Z^{n-5} + \dots + f_{n-1}. \end{aligned}$$

Hence $F(Z) = ZF'(Z) + (x^{n-1}d + y)$ and therefore

$$DF(Z) = (x^{n-1}d + y)^{n-1}.$$

Also the galois group G of $F(Z)$ over $k((x, y))$ is a transitive subgroup of S_n containing an n -cycle and a 2-cycle. If n is prime, then by Lemma 2 of §10 (also see footnote 4 there) $G = S_n$ and we have an $\infty^{(m-1)/2}$ family of unaffected coverings of the required type. However this argument (i.e., Lemma 2) does not apply if n is not prime.

6. The general case (n odd). In the general case, suppose we could arrange matters so that $S(Z)$ instead of being factorizable (into distinct linear factors) is irreducible over $k((x))$ and has for its galois group a cyclic group of order m . Now the galois group of $Z^2 + x^a Z + x$ over $k((x))$ is still cyclic of order 2. Since m is odd, by Lemma 4, §10, we could then conclude that the galois group of $f(Z)$ over $k((x))$ is cyclic of order $2m$ and hence if considered as a subgroup of $G \subset S_n$ it would be generated (as in paragraph two on page 191 of [V]) by a permutation of type $(h_1, h_2)(h_3, h_4, \dots, h_n)$ where the symbols $h_1, h_2, \dots, h_n$ are all distinct. Since G contains an n -cycle, Lemma 3, §10, would tell us that $G = S_n$. The galois group of $S(Z)$ over $k((x))$ will be made cyclic of order m by finding $S_1, S_2, \dots, S_m$ in $k[x]$, (of positive leading degrees), such that

- (1) $S(Z)$ is irreducible in $k[[x]][Z]$, and
- (2) $S(Z)$ is completely reducible (into linear factors) in $k[[u]][Z]$ where $u = x^{1/m}$.

To arrange that $DF(Z) = v^h d$ with $d(v) = 1$ and $d(d) = 0$, we may adapt the method of §4 or the method of §5, i.e., either (A) we kill the coefficients of all the odd powers in $f(Z)$ other than Z^n or (B) we kill the coefficients of all the even powers in $f(Z)$ other than the constant term. In case (A) we have

$$\begin{aligned} F(Z) &= Z^n + f_1 Z^{n-1} + f_3 Z^{n-3} + \dots + f_{n-2} Z^2 + (f_n + y), \\ F'(Z) &= Z^{n-1} \end{aligned}$$

and hence

$$DF(Z) = (f_n + y)^{n-1} [\text{with } d((f_n + y)) = 1].$$

In case (B) we have

$$F(Z) = Z^n + f_2 Z^{n-2} + f_4 Z^{n-4} + \cdots + f_{n-1} Z + (f_n + y),$$

$$F'(Z) = Z^{n-1} + f_2 Z^{n-3} + f_4 Z^{n-5} + \cdots + f_{n-1},$$

so that $F(Z) = ZF'(Z) + (f_n + y)$ and hence

$$DF(Z) = (f_n + y)^{n-1} \text{ [with } d((f_n + y)) = 1].$$

We expound these two methods in the next two sections respectively.

7. **Method A (killing odd powers).** To kill the odd powers in $f(Z)$ other than Z^n we have to satisfy the following equations:

$$x + x^a S_1 + S_2 = 0,$$

$$xS_2 + x^a S_3 + S_4 = 0,$$

$$xS_4 + x^a S_5 + S_6 = 0,$$

• • • • •

$$xS_{m-3} + x^a S_{m-2} + S_{m-1} = 0,$$

$$xS_{m-1} + x^a S_m = 0,$$

i.e., (by successive substitutions):

$$S_2 = x + x^a S_1,$$

$$S_4 = x^2 + x^{a+1}S_1 + x^aS_3,$$

$$S_6 = x^3 + x^{a+2}S_1 + x^{a+1}S_3 + x^aS_5,$$

• • • • •

$$S_{2i} = x^i + x^{a+i-1}S_1 + x^{a+i-2}S_3 + \cdots + x^a S_{2i-1},$$

.....

$$S_{m-1} = S_{2(m-1)/2}$$

$$= x^{(m-1)/2} + x^{a+(m-3)/2}S_1 + x^{a+(m-5)/2}S_3 + \cdots + x^aS_{m-2},$$

$$x^{a-1}S_m = S_{m-1}.$$

Let

$$a = \frac{m-1}{2}.$$

Let $S_1, S_3, \dots, S_{m-2}$ be arbitrary elements in $k[x]$ of positive leading degrees and let $S_2, S_4, \dots, S_{m-1}, S_m$ be determined by the above equations. Then

$S_{2i} = x^i d_{2i}$ (for $i = 1, 2, \dots, (m-1)/2$) and $S_m = x d_m$.

where $d_2, d_4, \dots, d_{m-1}, d_m$ are polynomials in x with nonzero constant terms. Now

$$S(Z) = Z^m + xT_1Z^{m-1} + xT_2Z^{m-2} + \cdots + xT_{m-1}Z + xd_m,$$

with $T_i \in k[x]$. Since $d_m(0) = 1 \neq 0$, $S(Z)$ is irreducible over $k((x))$. Let $u^m = x$ and $Z = uZ^*$. Let

$$S(Z) = u^m S^*(Z^*).$$

Then

$$\begin{aligned} S^*(Z) &= Z^m + u^{m-1}T_1Z^{m-1} + u^{m-2}T_2Z^{m-2} + \cdots + uT_{m-1}Z + d_m \\ &\equiv Z^m + 1 \pmod{u}. \end{aligned}$$

Since $m \neq 0(2)$, $S^*(Z)$ and hence $S(Z)$ is completely reducible in $k[[u]][Z]$ (into distinct linear factors). Thus we have obtained an $\infty^{(m-1)/2}$ family of polynomials $F(Z)$ of the required type.

[We could even kill all the coefficients of $f(Z)$ except f_m and f_n , thus: We want

$$\begin{aligned} x^a + S_1 &= 0, \\ x + x^a S_1 + S_2 &= 0, \\ xS_1 + x^a S_2 + S_3 &= 0, \\ xS_2 + x^a S_3 + S_4 &= 0, \\ &\vdots \\ xS_{m-3} + x^a S_{m-2} + S_{m-1} &= 0, \\ xS_{m-1} + x^a S_m &= 0. \end{aligned}$$

Solving successively:

$$\begin{aligned} S_1 &= x^a \equiv 0 \pmod{x}, \\ S_2 &= x + x^{2a} \equiv 0 \pmod{x}, \\ S_3 &= x^{a+1} + x^{a+1} + x^{3a} \equiv 0 \pmod{x}, \\ &\vdots \\ S_i &= xS_{i-2} + x^a S_{i-1} \equiv 0 \pmod{x}, \\ &\vdots \\ S_{m-1} &= xS_{m-3} + x^a S_{m-2} \equiv 0 \pmod{x}. \end{aligned}$$

Let $a = (m-1)/2$. Then by what we have shown above, it follows that: $S_{m-1} = x^{(m-1)/2} d_{m-1} = x^a d_{m-1}$ where d_{m-1} is a polynomial in x with $d_{m-1}(0) \neq 0$. Choose S_m so that $x^a S_m + xS_{m-1} = 0$, i.e., $S_m = x d_{m-1}$. Then $f_m = xS_{m-2} + x^a S_{m-1} + S_m = xe$ with $e(0) \neq 0$. If we replace x by xe we obtain $F(Z) = Z^n + xZ^2 + x^2d + y$, where $d \in k[x]$ with $d(0) \neq 0$.]

8. Method B (killing even powers). To kill the even powers in $f(Z)$ other than the constant term, we have to satisfy the following equations:

$$\begin{aligned} R_{2i+1} &= u^{(m(m+1)/2)-mi+m-2i-1-m} d_{2i+1} \\ &= u^{(m^2+m-(2m+4)i-2)/2} d_{2i+1} \end{aligned}$$

for $i=0, 1, \dots, (m-1)/2$; now $i < (m-1)/2$ implies $2i < m-1$ which implies $2(m+2)i < (m+2)(m-1) = m^2 + m - 2$, and hence $(2m+4)i < m^2 + m - 2$ so that $m^2 + m - (2m+4)i - 2 > 0$; also for $i = (m-1)/2$ we have $m^2 + m - (2m+4)i - 2 = m^2 + m - ((2m+4)(m-1)/2) - 2 = 0$. Thus $R_j \equiv 0 \pmod{u}$ for $j=1, 2, \dots, m-1$ and $R_m \not\equiv 0 \pmod{u}$. Since $m \not\equiv 0(2)$, $Z^m + R_m(0)$ factors into distinct linear factors in $k[Z]$ and hence $R(Z)$ and hence $S(Z)$ factors into distinct linear factors in $k[[u]][Z]$. Thus there results an $\infty^{(m-1)/2}$ family of polynomials $F(Z)$ of the required type.

[For instance, we could take $S_2 = S_4 = \dots = S_{m-1} = 0$. Then $S_1 = x^a$, $S_3 = x^{a+1}$, $\dots$, $S_m = x^{a+(m-1)/2} = x^{m+1}$. So that $f_2 = x + x^a S_1 + S_2 = x + x^{a+1}$, and for $i=2, 3, \dots, m/2$: $f_{2i} = S_{2i} + x^a S_{2i-1} + S_{2i-2} = x^{2a+i-1}$. Then

$$\begin{aligned} F(Z) &= Z^n + (x + x^{(n+3)/2})Z^{n-2} + x^{n+2}Z^{n-4} + x^{n+3}Z^{n-6} + \dots \\ &\quad + x^{n+(n-1)/2}Z + (x^n + y).] \end{aligned}$$

III. APPENDIX

9. A remark. If, in Chapters I and II, we replace any reference to "a polynomial in x (respectively in y or in x and y)" by "a power series in x (respectively in y or in x and y)," then we get much larger families of polynomials

$$F(Z) = Z^n + F_1 Z^{n-1} + \dots + F_n \in k[[x, y]][Z];$$

where the parameters (for instance in §4: $R_2, R_4, \dots, R_m$) are allowed to take values in $k[[x, y]]$. Let $y^* = x^m d + y$ in case of §4; $y^* = x^{n-1} d + y$ in case of §5 and $y^* = f_n + y$ in case of §§7 and 8. Then (x, y^*) are regular parameters in $k[[x, y]]$ and hence we may replace y by y^* . Let $A = k[[x, y]]$, $E = k((x, y))$, E' = an extension of E gotten by adjoining a root of $F(Z)$ to E , E^* = a root field of $F(Z)$ over E containing E' , A' = the integral closure of A in E' . Then it follows from the considerations of Chapters I and II that: (1) $F(Z)$ is irreducible in $E[Z]$, (2) E^* is a least galois extension of E containing E' , (3) $G(E^*/E) = S_n$, and (4) $DF(Z) = y^{n-1}$ or y^n . It is obvious that the maximal ideal in A is ramified in the extension A'/A . From (4) it follows that if H is any other prime ideal in A which is ramified in the extension A'/A then $H = yA$. In the algebro-geometric case it followed from the "purity of the branch locus (Theorem 1 of [A1])" that yA is indeed ramified.^(3a) In the present algebroid case, we must directly prove that yA is ramified. In the case of Chapter I, $F_{n-1} = y$ and $F_1, F_2, \dots, F_{n-2}, F_n \in k[[x]]$ and in case of

^(3a) Added in proof. Proof of Theorem 1 of [A1] is incorrect. A correct proof is being published by Zariski. However in the present situation the algebro-geometric case follows from the algebroid case by passing to completions.

Chapter II, $F_n = y$ and $F_1, F_2, \dots, F_{n-1} \in k[[x]]$. Hence it is enough to prove the following:

LEMMA. *Let k be an algebraically closed field, $E = k((x, y))$, $F(Z) = Z^n + F_1 Z^{n-1} + \dots + F_n$, ($n > 1$), $F_1, F_2, \dots, F_{t-1}, F_{t+1}, \dots, F_n \in k[[x]]$; $F_t = y$; E' = an extension of E gotten by adjoining a root of $F(Z)$; v = the valuation of E given by the irreducible nonunit y of $k[[x, y]]$. Then v is ramified in E' .*

Proof. Let k_1 be an algebraic closure of $k((x))$ and let $E'_1 = k_1((y))$; we may canonically assume that $E \subset E_1$. Let E_1 be a root field of $F(Z)$ over E_1 ; we may assume that $E' \subset E'_1$. It is clear that the valuation of E_1 with valuation ring $k_1[[y]]$ is the unique extension of v to E_1 ; we will call it again v . Let w be an extension of v to E'_1 . Let $z_1, \dots, z_n$ be the roots of $F(Z)$, $E^* = E(z_1, z_2, \dots, z_n)$, and let w^* be the E^* -restriction of w . $0 < vD(F(Z)) = w(\prod_{i \neq j} (z_i - z_j))$. Hence $w(z_i - z_j) > 0$ for some $i \neq j$, say $w(z_1 - z_2) > 0$. Let $c \in k_1$ such that $v(z_1 - c) > 0$. Let $z'_1 = z_1 - c$. Then $w(z'_1) > 0$ and $w(z'_2) > 0$. Let $G(Z) = F(Z + c) = Z^n + G_1 Z^{n-1} + \dots + G_n$. Let $q = c^n + F_1 c^{n-1} + \dots + F_{t-1} c^{n-t+1} + F_{t+1} c^{n-t+1} + \dots + F_n$. Then $q \in k_1$ and $G_n = G(0) = F(c) = q + c^{n-t}y$. Hence either $v(G_n) = 0$ or $v(G_n) = v(y)$. Since $G_n = z'_1, z'_2, \dots, z'_n$, $w(z'_1) > 0$, $w(z'_2) > 0$, $w(z'_i) \geq 0$ for $i = 3, 4, \dots, n$, we conclude that $v(G_n) = v(y)$ and $0 < w^*(z'_1) < w^*(y)$. Therefore w^* is ramified over v . Hence v is ramified in E' .

10. **Lemmas on groups.** In Lemmas 1, 2 and 3, G is a transitive subgroup of the permutation group S_n on n symbols $1, 2, \dots, n$.

LEMMA 1. *If G contains a 2-cycle and an $(n-1)$ -cycle, then $G = S_n$.*

Proof. See last paragraph on page 191 of [V].

LEMMA 2. *If n is an odd prime number and G contains a 2-cycle and an n -cycle, then $G = S_n^{(4)}$.*

First proof. Say $t = (1, 2, \dots, n)$ is the n -cycle in G and let s be the 2-cycle in G . Since G is transitive, we may assume that $s = (1, N)$. Now t^{N-1} is again an n -cycle: $t^{N-1} = (1, N, \dots)$ and hence we may assume that $N = 2$. Then $st = (1, 2)(1, 2, \dots, n) = (1, 3, 4, \dots, n)$, i.e., G contains a 2-cycle and an $(n-1)$ -cycle. Now invoke Lemma 1.

Second proof. Since n is prime, G is primitive. Now invoke Example 14 on page 163 of [C] or Satz 4 of [F].

LEMMA 3. *If n is odd and G contains an n -cycle t and a permutation s of type: $s = (1, 2)(h_1, h_2, \dots, h_m)$ where $m = n-2$ and the letters $1, 2, h_1, h_2, \dots, h_m$ are all distinct. Then $G = S_n$.*

(4) It is not necessary to assume the existence of an n -cycle (in the second proof this is not used any way), for G is transitive implies that the order of G is divisible by n (see Cor. I on p. 142 of [C], this corresponds to the fact that the polynomial $F(Z)$ is irreducible) so that G contains a permutation g of order n and since n is prime g must be an n -cycle.

Proof. Since G is transitive, we may assume that $t = (1, p_1, p_2, \dots, p_{n-1})$. Let j be such that $p_j = 2$. Let

$$t^j = (1, 2, q_3, \dots, q_u)(\dots) \dots (\dots)$$

be an expression of t^j in terms of disjoint cycles. Then (order of t^j) = l.c.m. of the lengths of these cycles. Therefore u divides n . Since n is odd, we have $u > 2$. We may relabel the letters so that $q_3 = 3$. Let $a = s^m$ and $b = s^2$. Since m is odd, we have

$$a = (1, 2), \text{ and } b = (r_1, r_2, \dots, r_m),$$

where $r_1, r_2, \dots, r_m$ is a rearrangement of $3, 4, \dots, n$. Conjugating a by t^j we have: $a^* = (2, 3) \in G$. We may write b so that $r_1 = 3$ and then relabel the letters so as to have: $b = (3, 4, \dots, n)$. Then

$$a^*b = (2, 4, 5, \dots, n, 3) = an(n-1)\text{-cycle}.$$

Now invoke Lemma 1.

LEMMA 4. Let K be a field and $\bar{K}$ an overfield of K , let $K_1, \dots, K_s$ be subfields of $\bar{K}$ which are galois extensions of K with $[K_i:K] = m_i$. Assume that $m_1, \dots, m_s$ are pairwise coprime and let K^* be the compositum of $K_1, \dots, K_s$. Then K^*/K is galois and $G(K^*/K)$ is the direct product of $G(K_1/K), \dots, G(K_s/K)$.

Proof. It is clear that the general case follows from the case $s=2$, so let us assume that $s=2$. Let L be a galois extension of K containing K^* . Then K_1/K and K_2/K are galois implies that $G(L/K_1)$ and $G(L/K_2)$ are normal subgroups of $G(L/K)$; hence $G(L/K^*) = G(L/K_1) \cap G(L/K_2)$ is a normal subgroup of $G(L/K)$, i.e., K^*/K is galois.

Let $G_1 = G(K^*/K_1)$, $G_2 = G(K^*/K_2)$, $G = G(K^*/K)$, $H_1 = G/G_1 = G(K_1/K)$, $H_2 = G/G_2 = G(K_2/K)$. Then G_1 and G_2 are normal subgroups of G and $G_1 \cap G_2 = G(K^*/K^*) = 1$, hence G_1G_2 is the direct product of G_1 and G_2 . Let g, g_1, g_2, h_1, h_2 , be the orders of G, G_1, G_2, H_1, H_2 , respectively. Then $g_1h_1 = g = g_2h_2$. Since $(h_1, h_2) = 1$, h_1 must divide g_2 . Since $G_2 = G_2/G_1 \cap G_2$ which is isomorphic to a subgroup of $G/G_1 = H_1$, we have that g_2 divides h_1 . Therefore $g_2 = h_1$ so that $g = g_1h_1 = g_1g_2$. Therefore $G = G_1G_2$.

BIBLIOGRAPHY

- A1. S. Abhyankar, *On the ramification of algebraic functions*, Amer. J. Math. vol. 77 (1955) pp. 575-592.
- A2. ———, *Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$* , Ann. of Math. vol. 63 (1956) pp. 491-526.
- C. R. D. Carmichael, *Groups of finite order*, Dover, 1956.
- F. Ph. Furtwängler, *Über Kriterium . . .*, Math. Ann. vol. 85 (1922) pp. 34-40.
- V. B. L. Van der Waerden, *Modern algebra*, vol. I, New York, 1949.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.