ON THE DENSITY OF CONJUGATE FIXED POINTS OF A CORRESPONDENCE

BY

R. E. MacRae[1]

1. Introduction

In connection with another investigation the following question arose. Suppose that $P(x, z)$ is an irreducible polynomial in two variables over the finite field $k = GF(q)$. Let the pair (α, β) lie in the graph of P, that is let $P(\alpha, \beta) = 0$ where α and β are elements of the algebraic closure $\bar{k}$ of k. We now ask: how often does it occur that α and β are conjugate over k, that is, how often is $\beta = \alpha^{q^r}$ for some r? For example, how often does $\alpha + 1 = \alpha^{q^r}$? It is immediately clear that this situation will arise infinitely often for a given P so the question of "how often" must be answered in terms of a density. To attack this question we will find it useful to consider $P(x, z)$ as a correspondence from the projective line to itself. Then to say that $P(\alpha, \beta) = 0$ is to say (with finitely many exceptions) that there are points $\mathcal{P}_1$ and $\mathcal{P}_2$ on the projective line over k such that $x(\mathcal{P}_1) = \alpha$ and $z(\mathcal{P}_2) = \beta$. To say that α and β are conjugate is equivalent to saying that $\mathcal{P}_1 = \mathcal{P}_2$. More generally, let us replace the projective line by the Riemann surface $X^{K/k}$ for any function field K in one variable in which $k = GF(q)$ is the exact constant field. When P is any prime correspondence from K to K and $\mathcal{P}$ is in $X^{K/k}$ then we may let P act on $\mathcal{P}$ and produce an integral divisor $\mathcal{P}^P$ also on K. We are, therefore, interested in the set

$$A_p = \{\mathcal{P} \in X^{K/k} \mid \mathcal{P} \text{ divides } \mathcal{P}^P\}.$$

In order to measure the size of A_P in $X^{K/k}$ we use the ordinary Dirichlet density $\delta(A_p)$. It is the purpose of this paper to prove the following result.

Theorem. *If* (i) *both degrees of P are one and P is not the diagonal or* (ii) *the ratio of the degrees of P is not an integral power of q, then $\delta(A_p) = 0$.*

It seems quite likely that the above theorem is true more generally when P is assumed to be unequal to any power of the Frobenius correspondence or its Rosati adjoint. The methods available to us unfortunately break down when both degrees of P are equal but unequal unity.

The paper will consist of three more sections. The first of these deals with generalities concerned with correspondences and the Dirichlet density. Our treatment of the former is completely algebraic since the basic rationality questions involved make such a treatment more useful than the customary

Received March 7, 1972.

[1] This work was supported in part by a grant from the National Science Foundation.

geometric one Compare, for example, the algebraic treatment in [2]. Two somewhat non-standard applications of the Dirichlet density are given. The next section deals with an extended form of the theorem of Bézout in which improper intersections are considered. The final section gives a proof of the main theorem stated above.

2. Generalities

In this section we describe the necessary details concerning correspondences and density. The former will be done from an algebraic rather than a geometric point of view since this will suit our purposes better. The reader is assumed familiar with an algebraic treatment of functions fields in one variable including the Riemann-Roch Theorem. See, for example [2]. For the remainder of this section k except where indicated will denote an arbitrary field and K a function field in one variable over k such that k is algebraically closed in K and K is separably generated over k. K is in other words, a regular extension of k. Under these circumstances the ring $K \otimes_k k_1$ is an integral domain for every field extension, k_1, of k.

We begin with several technical propositions.

Proposition 2.1. *Let $\mathfrak{O}$ be an integrally closed k-algebra and k_1 a finitely and separably generated extension field of k such that $\mathfrak{O} \otimes_k k_1$ is an integral domain. Then $\mathfrak{O} \otimes_k k_1$ is integrally closed.*

Proof. The proof easily reduces to special cases. First, let $k_1 = k(x)$ be the rational function field in one variable. Then $\mathfrak{O} \otimes_k k_1$ is clearly a localization of the ring $\mathfrak{O} \otimes_k k[x] = \mathfrak{O}[x]$. The latter is, however, well known to be integrally closed when $\mathfrak{O}$ is. Second, let k_1 be a finite, separable extension of k. If $\omega_1, \cdots, \omega_n$ is a basis for k_1 over k then $1 \otimes \omega_1, \cdots, 1 \otimes \omega_n$ is clearly a basis for $\mathfrak{O} \otimes_k k_1$ over $\mathfrak{O}$ and for the quotient field, L, of $\mathfrak{O} \otimes_k k_1$ over the quotient field of $\mathfrak{O}$. It is easily seen that $\mathfrak{O} \otimes_k k_1$ is an integral extension of $\mathfrak{O}$. Now the discriminant of the basis $1 \otimes \omega_1, \cdots, 1 \otimes \omega_n$ is in k^* so it is a unit in $\mathfrak{O}$. Thus by well-known arguments the conductor of the integral closure of $\mathfrak{O} \otimes_k k_1$ is trivial. In otherwords, $\mathfrak{O} \otimes_k k_1$ is integrally closed.

Proposition 2.2. *Let $\mathfrak{O}_1$ and $\mathfrak{O}_2$ be integrally closed k-algebras whose quotient fields are finitely and separably generated extensions of k and such that $\mathfrak{O}_1 \otimes_k \mathfrak{O}_2$ is an integral domain. Then $\mathfrak{O}_1 \otimes_k \mathfrak{O}_2$ is integrally closed.*

Proof. Observe that $\mathfrak{O}_1 \otimes_k \mathfrak{O}_2 = K_1 \otimes_k \mathfrak{O}_2 \cap \mathfrak{O}_1 \otimes_k K_2$ where K_i is the quotient field of $\mathfrak{O}_i$, $i = 1, 2$. Then use Proposition 2.1.

Proposition 2.3. *Let K be a function field in one variable over k and assume it to be a regular extension of k. If $\mathfrak{O}$ is a k-algebra which is a noetherian, integrally closed, integral domain all of whose maximal ideals are of Krull dimension n and possess a residue class field that is not algebraic over $\bar{k}$, then $\mathfrak{O} \otimes_k K$*

inherits these properties except that the Krull dimension of the maximal ideals is $n + 1$.

Proof. Because of the assumed regularity, $\mathcal{O} \otimes_k K$ is an integral domain. By Proposition 2.1, $\mathcal{O} \otimes_k K$ is integrally closed. Let x be a transcendental element of K. Then $\mathcal{O} \otimes_k K$ is a finitely generated, integral extension of $\mathcal{O} \otimes_k k(x)$. Hence it suffices to prove that $\mathcal{O} \otimes_k k(x)$ is a noetherian ring all of whose maximal ideals are of Krull dimension $n + 1$ and possess a residue class field that is not algebraic over k. However, $\mathcal{O} \otimes_k k(x)$ is a localization of $\mathcal{O} \otimes_k k[x] = \mathcal{O}[x]$. Thus it is immediately clear that $\mathcal{O} \otimes_k k(x)$ is noetherian. Now in $\mathcal{O}[x]$ all of the maximal ideals are of Krull dimension $n + 1$ and are of the form $\mathcal{P} + (f(x))$ where $\mathcal{P}$ is a maximal ideal of $\mathcal{O}$ and $f(x)$ is irreducible modulo $\mathcal{P}$. Since $\mathcal{P}$ clearly has a void intersection with the non-zero elements of $k[x]$ we need only show that for every maximal ideal $\mathcal{P}$ of $\mathcal{O}$ there is a polynomial $f(x)$ that is irreducible modulo $\mathcal{P}$ and such that $\mathcal{P} + (f(x))$ has a void intersection with the non-zero elements of $k[x]$. Let z be an arbitrary preimage of an element that is transcendental over k modulo $\mathcal{P}$. Then $z - x$ will clearly serve our purposes.

Now let K_1 and K_2 be function fields in one variable over k and assume that both of them are regular extensions of k. It is an immediate consequence of Proposition 2.3 that $K_1 \otimes_k K_2$ is a Dedekind domain.

Definition 2.4. The (non-null) fractional ideals of the Dedekind domain $K_1 \otimes_k K_2$ are called the *correspondences from* K_1 *to* K_2. The prime (resp. integral) ideals of $K_1 \otimes_k K_2$ are called *prime* (resp. *integral*) *correspondences*. $\mathrm{Corr}_k(K_1, K_2)$ will denote the group (written additively) of all fractional ideals of $K_1 \otimes_k K_2$.

If we let L be the quotient field of $K_1 \otimes_k K_2$ it is clear that L may be regarded as a function field in one variable over both K_1 and K_2. The prime correspondences may then be regarded as the points in common to the Riemann surfaces of L over K_1 and L over K_2. In particular, each prime correspondence (and hence every correspondence) has two degrees;

$$g_1(P) = [K_1 \otimes_k K_2/P:K_1] \quad \text{and} \quad g_2(P) = [K_1 \otimes_k K_2/P:K_2].$$

Next we may regard P as a homomorphism from the divisor group $D^{K_1/k}$ of K_1 to the divisor group $D^{K_2/k}$ of K_2. Indeed let $\mathcal{P}$ be a prime divisor on K_1 and let $(\mathcal{P})$ be the extension of $\mathcal{P}$ to $K_1 \otimes_k K_2/P = L$ and then set

$$\mathcal{P}^P = N_{L/K_2}(\mathcal{P}).$$

Finally, extend this map to $D^{K_1/k}$ by linearity in the usual way.

In a similar fashion we may define a product of correspondences as follows. Let K_1, K_2 and K_3 be function fields in one variable over k and assume that all are regular extensions of k. Moreover let P be a prime correspondence from K_1 to K_2 and Q a prime correspondence from K_2 to K_3. Let

$$L = K_1 \otimes_k K_2/P$$

and denote by Q' the ideal in $L \otimes_k K_3$ generated by Q. We have

$$K_1 \otimes_k K_3 \leq L \otimes_k K_3 .$$

Define PQ to be the norm of Q' taken from the quotient field of $L \otimes_k K_3$ to the quotient field of $K_1 \otimes_k K_3$. We may obtain PQ in another way as the following theorem shows.

THEOREM 2.5. *Let $M = K_2 \otimes_k K_3/Q$ and let P' be the ideal of $K_1 \otimes_k M$ generated by P. Set R equal to the norm of P' taken from the quotient field of $K_1 \otimes_k M$ to the quotient field of $K_1 \otimes_k K_3$. Then $R = PQ$.*

Proof. By Proposition 2.3, $\mathfrak{D} = K_1 \otimes_k K_2 \otimes_k K_3$ is an integrally closed, noetherian domain all of whose maximal ideals have Krull dimension two. It is easy to see that the ideal S generated by P and Q in $\mathfrak{D}$ can have no prime divisors of Krull dimension one. Thus the primary decomposition $S = \bigcap Q_j$ has the property that each associated prime $\mathfrak{P}_j = \sqrt{Q_j}$ is maximal. Let

$$\mathcal{P}_j = \mathfrak{P}_j \cap K_1 \otimes_k K_3$$

and set $f_j = [\mathfrak{D}/\mathfrak{P}_j{:}K_1 \otimes_k K_3/\mathcal{P}_j]$. It is now easy to see that both R and PQ are equal to $\prod \mathcal{P}_j^{e_j f_j}$ where $e_j f_j$ equals the length of $\mathfrak{D}/Q_j$.

There is yet another way of looking at the product PQ. Indeed let K_{12} be the quotient field of $K_1 \otimes_k K_2$ and K_{13} equal to the quotient field of $K_1 \otimes_k K_3$. We regard K_{12} and K_{13} as function fields in one variable over K_1 and observe that both are regular extensions of K_1. Now P may be thought of as a point in the Riemann surface X^{K_{12}/K_1}. We then extend Q to

$$K_{12} \otimes_{K_1} K_{13}$$

by noting that $K_{12} \otimes_{K_1} K_{13}$ is a localization of

$$(K_1 \otimes_k K_2) \otimes_{K_1} (K_1 \otimes_k K_3) = K_1 \otimes_k K_2 \otimes_k K_3$$

which contains an ideal generated by Q. Call this extended ideal Q' and note that it need not be prime. However, we can still define P^Q in the usual way. The following theorem is clear from various definitions.

THEOREM 2.6. $PQ = P^Q$.

THEOREM 2.7. *Let K_1, K_2, K_2 be function fields in one variable over k and assume all are regular over k. If P and Q are prime correspondences from K_1 to K_2 and K_2 to K_3, respectively, then $\mathcal{P}^{PQ} = (\mathcal{P}^P)^Q$ for every $\mathcal{P}$ on the Riemann surface for K_1.*

Proof. Let $L = K_1 \otimes_k K_2/P$ and $M = K_2 \otimes_k K_3/Q$. Moreover let $\sum e_j R_j$ be factorization of the extension of Q to $L \otimes_k K_3$. If $\mathfrak{P}$ is a point on the Riemann surface for L we set $\mathcal{A}_j$ equal to the divisor on M obtained by extending $\mathfrak{P}$ to $L \otimes K_3/R_j$ and then taking the norm to M. Likewise let $\mathcal{A}$ be the divisor on M obtained by taking the norm of $\mathfrak{P}$ to K_2 and then extending to M. We claim $\mathcal{A} = \prod \mathcal{A}_j^{e_j}$. Indeed let $\mathcal{P}$ be the point of K_2

below $\mathfrak{P}$ and let $\mathcal{O}_{\mathcal{P}}$ be the associated valuation ring. Let $\mathfrak{D}_{\mathcal{P}}$ be the integral closure of $\mathcal{O}_{\mathcal{P}}$ in L. Then $\mathfrak{P} = \pi\mathfrak{D}_{\mathcal{P}}$ for suitable choice of π. We have

$$N_{L/K_2}\,\mathfrak{P} = N_{L/K_2}\,\pi\mathcal{O}_{\mathcal{P}}\,.$$

Let $\mathfrak{D}'_{\mathcal{P}j}$ be the integral closure of $\mathcal{O}_{\mathcal{P}}$ in $L \otimes_k K_3/R_j = T_j$ and let $\mathcal{O}'_{\mathcal{P}}$ be the integral closure of $\mathcal{O}_{\mathcal{P}}$ in M. Then $\mathcal{A} = N_{L/K_2}\,\pi\mathfrak{D}'_{\mathcal{P}}$ and $\mathcal{A}_j = N_{T_j/M}\,\pi\mathfrak{D}'_{\mathcal{P}}$. Hence it suffice to show that $N_{L/K_2}\,\pi$, considered as an element of M, equals $\prod\,(N_{T_j/M}\,\pi)^{e_j}$. This, however, follows by applying [6, II, §11, Chap. V, Lemma 1] to the pair of Dedekind domains $L \otimes_k K_3$ and $K_2 \otimes_k K_3$. Next let Q_j be the prime ideal of $K_1 \otimes_k K_3$ that lies below R_j and let f_j be the residue class degree. Then, by definition, $PQ = \sum e_j f_j Q_j$. If $\mathcal{P}$ is a point on the Riemann surface for K_1, then it is clear that $\mathcal{P}^{f_j Q_j}$ equals the divisor obtained by extending $\mathcal{P}$ to $T_j = L \otimes_k K_3/R_j$ and then taking the norm to K_3. By the remarks above $\prod\,(\mathcal{P}^{f_j Q_j})^{e_j}$ equals $(\mathcal{P}^P)^Q$ so the theorem is proved.

THEOREM 2.8. *Let K_1, K_2, K_3 and K_4 be function fields in one variable over k and assume all are regular extensions of k. If P, Q and R are correspondences from K_1 to K_2, K_2 to K_3 and K_3 to K_4, respectively, then $(PQ)R = P(QR)$.*

Proof. By Theorem 2.6, $(PQ)R = (P^Q)^R$ and $P(QR) = P^{QR}$. Hence $(PQ)R = (P^Q)^R = P^{QR} = P(QR)$ by Theorem 2.7.

THEOREM 2.9. *If K is a function field in one variable over k and a regular extension of k, then* $\mathrm{Corr}_k(K, K)$ *forms an associative ring with identity and there is a ring homomorphism of* $\mathrm{Corr}_k(K, K)$ *into the endomorphism ring of the divisor group $D^{K/k}$.*

Proof. All except the existence of an identity element is contained in preceding results. We consider the exact sequence $O \to D \to K \otimes_k K \to K \to 0$ given by sending $a \otimes b$ onto ab. The correspondence D is called the diagonal and it is clear that $DA = AD = A$ for every correspondence A in $\mathrm{Corr}_k\,(K, K)$.

Let us now regard P as a curve in its own right and determine the effect the singularities on the curve have. Let $\mathcal{O}_{\mathcal{P}_1}$ and $\mathcal{O}_{\mathcal{P}_2}$ be valuation rings of K_1 and K_2, respectively, and observe that $K_1 \otimes_k K_2$ is a localization of $\mathcal{O}_{\mathcal{P}_1} \otimes_k \mathcal{O}_{\mathcal{P}_2}$. Hence there is a unique prime ideal in $\mathcal{O}_{\mathcal{P}_1} \otimes_k \mathcal{O}_{\mathcal{P}_2}$ whose localization is P. We denote this ideal by P also. We have

$$\mathcal{O}_{\mathcal{P}_1} \otimes_k \mathcal{O}_{\mathcal{P}_2}/P = \mathcal{O}_{\mathcal{P}_1}\,\mathcal{O}_{\mathcal{P}_2} \quad \text{in} \quad L = K_1 \otimes_k K_2/P.$$

THEOREM 2.10. *Except for a finite set of point pairs $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{O}_{\mathcal{P}_1}\,\mathcal{O}_{\mathcal{P}_2}$ is the integral closure of $\mathcal{O}_{\mathcal{P}_1}$ and $\mathcal{O}_{\mathcal{P}_2}$ in L. (We assume here that $K_1 = K = K_2$.)*

Proof. Let x be a separating element of K over k and let $\mathfrak{D}$ be the integral closure of $k[x]$ in K. First note that $\mathfrak{D} \otimes_k k[x] = \mathfrak{D}[x]$ is an integrally closed noetherian domain of Krull dimension two and that $\mathfrak{D} \otimes_k \mathfrak{D}$ is a finitely generated (as a module) integral extension of $\mathfrak{D}[x]$. Hence $\mathfrak{D} \otimes_k \mathfrak{D}$ is a noetherian domain of Krull dimension two. By Proposition 2.2, $\mathfrak{D} \otimes_k \mathfrak{D}$ is integrally closed as well. Now since $K \otimes_k K$ is a localization of $\mathfrak{D} \otimes_k \mathfrak{D}$ there is a unique prime ideal of $\mathfrak{D}_k \otimes \mathfrak{D}$ whose localization is P. Call this prime P as well. Now $\mathfrak{D} \otimes_k \mathfrak{D}/P$ is a noetherian domain of Krull dimension one but not necessarily integrally closed. By localizing away a finite set of non-zero prime ideals of $\mathfrak{D} \otimes_k \mathfrak{D}/P$ we get a Dedekind domain. We can, therefore, find a finite set of maximal ideals of $\mathfrak{D}$ such that by localizing them away using a multiplicative set M we have $\mathfrak{D}_M \otimes_k \mathfrak{D}_M/P_M$ as a Dedekind domain. The result now follows immediately.

We turn now to the notion of the Rosati adjoint. When P is a prime correspondence from K_1 to K_2 we may reverse the roles of K_1 and K_2 and get a prime correspondence P^* from K_2 to K_1 which is called the Rosati adjoint of P. It is clear that $P = P^{**}$. One extends the adjoint operation to any correspondence from K_1 to K_2 by linearity in the customary way.

THEOREM 2.11. *Let P be a correspondence from K_1 to K_2 and Q a correspondence from K_2 to K_3. Then $(PQ)^* = Q^*P^*$.*

Proof. This is an immediate consequence of Theorem 2.5.

When $k = GF(q)$ there is a special correspondence that we need to consider. We will assume that K is a function field in one variable over k and that k is exact in K and thus K is a regular extension of k since k is perfect.

DEFINITION 2.12. Let the exact sequence $0 \rightarrow F_{q^r} \rightarrow K \otimes_k K \rightarrow K \rightarrow 0$ be defined by sending $a \otimes b$ onto ab^{q^r}. One calls F_{q^r} a *Frobenius correspondence.*

It is clear that $F_q^r = F_{q^r}$ and the degrees of F_{q^r} are 1 and q^r. When $k_n = GF(q^n)$ and $K_n = K \otimes_k k_n$ we may extend F_{q^r} to K_n by considering the ideal of $K_n \otimes_{k_n} K_n$ generated by F_{q^r}.

LEMMA 2.13. *F_{q^r} remains prime in $K_n \otimes_{k_n} K_n$.*

Proof. $0 \rightarrow F_{q^r} \rightarrow K \otimes_k K \rightarrow K \rightarrow 0$ implies

$$0 \rightarrow (F_{q^r}) \rightarrow K \otimes_k K \otimes_k k_n \rightarrow K_n \rightarrow 0$$

exact. However, $K \otimes_k K \otimes_k k_n = K_n \otimes_{k_n} K_n$.

We will denote the extension of F_{q^r} to K_n by F_{q^r} as well.

THEOREM 2.14. *If P is a prime correspondence from K_n to K_n, then PF_{q^r}, $F_{q^r}P$, $PF_{q^r}^*$ and $F_{q^r}^*P$ are all of the form p^eQ where Q is a prime and p is the characteristic of k.*

Proof. By use of the Rosati adjoint we need only consider PF_{q^r} and $PF_{q^r}^*$. In order to compute $PF_{q^r}^*$ we consider P as a prime ideal in $K_n \otimes_{k_n} k_n K_n^{q^r}$. Since $K_n \otimes_{k_n} K_n$ is a purely inseparable extension of $K_n \otimes_{k_n} k_n K_n^{q^r}$ there is but one prime that lies above P. Call it Q. Thus $PF_{q^r}^* = p^eQ$. The computation of PF_{q^r} is entirely similar.

We turn, finally, to the Dirichlet density. Here k will be the finite field $GF(q)$ and K a function field in one variable over k in which k is exact.

DEFINITION 2.15. The infinite series $Z_{K/k}(u) = \sum u^{g(\mathfrak{a})}$, where the sum is taken over all integral divisors $\mathfrak{a}$ on K, will be called the *Zeta Function of K over k.*

By a simple application of the Riemann-Roch Theorem one obtains the following pair of standard results.

THEOREM 2.16. *$Z_{K/k}(u)$ converges absolutely and uniformly inside the complex disc $|u| < 1/q$. Moreover, inside this disc $Z_{K/k}(u) = \prod (1 - u^{g(\mathfrak{P})})^{-1}$ where the product is taken over all points $\mathfrak{P}$ on the Riemann surface for K.*

THEOREM 2.17. *There is a polynomial $P_{K/k}(u)$ of degree $2g$ (g equals the genus of K) with integral coefficients, constant term 1 and leading coefficient q^g such that $Z_{K/k}(u) = P_{K/k}(u)/((1 - u)(1 - qu))$ inside the disc of radius $1/q$. Moreover, $P_{K/k}(1) = h$ and $P_{K/k}(1/q) = h/q^g$ where h is the projective class number of K.*

We can now define several Dirichlet densities of a subset of the Riemann surface of K.

DEFINITION 2.18. Let A be a subset of the Riemann surface of K and let A_n equal the number of points in A of degree n. Set

$$A(u) = \left(\sum A_n u^n/(-\log(1 - qu))\right).$$

Let $\bar{\delta}(A) = \limsup A(u)$, $\underline{\delta}(A) = \liminf A(u)$ and $\delta(A) = \lim A(u)$ where the limits are taken as u approaches $1/q$ along the real axis from the left. We call $\bar{\delta}(A)$, $\underline{\delta}(A)$ and $\delta(A)$ the *upper*, *lower* and *ordinary Dirichlet densities of A*, respectively.

By virtue of the preceding two theorems and the Riemann-Roch Theorem we have the following result whose proof is easy and is left to the reader.

THEOREM 2.19. *For every subset A of the Riemann surface for K, $\bar{\delta}(A)$ and $\underline{\delta}(A)$ exist and $0 \leq \underline{\delta}(A) \leq \bar{\delta}(A) \leq 1$. Moreover $\sigma(A)$ exists if and only if $\bar{\delta}(A) = \underline{\delta}(A)$ in which case $\delta(A) = \bar{\delta}(A) = \underline{\delta}(A)$.*

The following two variants of the Dirichlet density theorem will be used later.

THEOREM 2.20. *Let $k = GF(q)$ and K a function field in one variable which contains k as exact constant field. Let $n = p_1 \cdots p_r$ be a product of distinct primes. Set $k_n = GF(q^n)$ and $K_n = K \otimes_k k_n$. If A consists of the set of points on the Riemann surface for K that remain totally inert in K_n then*

$$\delta(A) = \prod_{j=1}^{r} (1 - p_j^{-1}) = \varphi(n)/n.$$

Proof. K_n is an unramified cyclic extension of K. Denote the Artin reciprocity map as usual by $(K_n/K/\mathcal{P})$ where $\mathcal{P}$ is a point on the Riemann surface for K. Now $\mathcal{P}$ is totally inert if and only if $(K_n/K/\mathcal{P})$ generates the Galois group. Hence $(K_n/K/\mathcal{P})$ can take on any of $\varphi(n)$ values. Thus by the usual density theorem $\delta(A) = \varphi(n)/n$. See [1].

THEOREM 2.21. *Let $k = GF(q)$ and K a function field in one variable which contains k as exact constant field. Let L be a finite extension field of K in which k remains exact. If A is the set of all points on the Riemann surface for L that have residue class degree exceeding one over K, then $\delta(A) = 0$.*

Proof. We have the equality $\sum u^{g(\mathfrak{P})} = \sum_{j=2}^{n} (\sum t_{j,\mathfrak{P}}\, u^{jg(\mathcal{P})})$ where $n = [L:K]$, $\mathfrak{P}$ ranges over the non-ramified pointts in A and the points $\mathcal{P}$ are those in the Riemann surface for K that lie below these points. Since $0 \leq t_{j,\mathcal{P}} \leq n$ for each j and $\mathcal{P}$, it is clear that $\sum t_{j,\mathfrak{P}}\, u^{jg(\mathcal{P})}$, $j = 2, \cdots, n$ converges at $u = 1/q$. Hence

$$\lim_{u\to 1/q} (\textstyle\sum u^{g(\mathfrak{P})}/(-\log\ (1 - qu)))$$
$$= \textstyle\sum_{j=2}^{n} \lim_{u\to 1/q} (\sum t_{j,\mathcal{P}}\, u^{jg(\mathcal{P})}/(-\log\ (1 - qu))) = 0.$$

That is to say, $\delta(A) = 0$.

3. An extension of Bézout's Theorem

The customary form of Bézout's Theorem gives very exact information on the number of points in what one might call a proper intersection. We will need less exact information on the number of points in an improper intersection. I am indebted to I. Fischer for suggesting the key step in the following theorem.

THEOREM 3.1. *Let k be an algebraically closed field and let $f_1, \cdots, f_m$ be homogeneous polynomials in $k[x_0, \cdots, x_r]$. If $f_1, \cdots, f_m$ have only finitely many common zeros, the number of distinct such zeros is at most the product of the degrees of $f_1, \cdots, f_m$.*

In order to prove this result we begin with some preliminaries. Let k be an arbitrary field.

DEFINITION 3.2. If $\mathfrak{a}$ is a homogeneous ideal in $k[x_0, \cdots, x_r]$ then

$$\chi(\mathfrak{a}, n) = \dim_k (k[x_0, \cdots, x_r]_n\, \mathfrak{a}_n)$$

is the *characteristic function of $\mathfrak{a}$*.

By the well-known theory [3, §3.24] $\chi(\mathfrak{a}, n) = \sum_{j=0}^{d} e_j \binom{n}{j}$ for all sufficiently large n where $e_0, \cdots, e_d$ are rational integers and e_d is positive. Moreover d is the projective dimension of $\mathfrak{a}$ and e_d is called the degree of $\mathfrak{a}$ and when $\mathfrak{a} = (f)$ the degree of $\mathfrak{a}$ is the ordinary degree of f. The main technical result is the following [3, §3.24].

PROPOSITION 3.3. *Let $\mathfrak{a}$ be a homogeneous ideal of $k[x_0, \cdots, x_r]$ and let f*

be a homogeneous polynomial that is not a zero divisor modulo $\mathfrak{A}$. Then

$$\deg(\mathfrak{A} + (f)) = \deg(f)\deg(\mathfrak{A}).$$

We now make a non-standard definition which marks the first departure from the usual theory.

Definition 3.4. Let $\mathfrak{A}$ be a homogeneous ideal in $k[x_0, \cdots, x_r]$. We set $\operatorname{Deg}(\mathfrak{A}) = \deg(\sqrt{\mathfrak{A}})$.

By virtue of [3, §3.24] we have the following.

Proposition 3.5. (i) $\operatorname{Deg}(\mathfrak{A}) \leq \deg(\mathfrak{A})$ *and* (ii) $\operatorname{Deg}(\mathfrak{A}) = \sum \deg(\mathfrak{P}_i)$ *where $\mathfrak{P}_i$ ranges over the isolated prime divisors of $\mathfrak{A}$.*

Theorem 3.6. *Let $\mathfrak{A}$ be a homogeneous ideal of $k[x_0, \cdots, x_r]$ generated by the homogeneous polynomials $f_1, \cdots, f_m$. Then*

$$\operatorname{Deg}(\mathfrak{A}) \leq \deg(f_1) \cdots \deg(f_m).$$

Proof. The proof is clear when $m = 1$. Let $\mathfrak{B}$ be the ideal generated by $f_1, \cdots, f_{m-1}$. We assume by induction that

$$\operatorname{Deg}(\mathfrak{B}) \leq \deg(f_1) \cdots \deg(f_{m-1}).$$

Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_s$ be the isolated prime divisors of $\mathfrak{B}$ and let $\mathfrak{P}_1, \cdots, \mathfrak{P}_t$ be the isolated prime divisors of $\mathfrak{A} = \mathfrak{B} + (f_m)$. Clearly each $\mathfrak{P}_i$ is an isolated prime divisor of some $\mathfrak{P}_j + (f_m)$. Hence

$$\operatorname{Deg}(\mathfrak{A}) = \sum \deg(\mathfrak{P}_i) \leq \sum \operatorname{Deg}(\mathfrak{P}_j + (f_m)).$$

Now if f_m is in $\mathfrak{P}_j$ we see that

$$\operatorname{Deg}(\mathfrak{P}_j + (f_m)) = \deg(\mathfrak{P}_j) \leq \deg(f_m)\deg(\mathfrak{P}_j).$$

On the other hand, when f_m is not in $\mathfrak{P}_j$, it is not a zero divisor modulo $\mathfrak{P}_j$, so

$$\operatorname{Deg}(\mathfrak{P}_j + (f_m)) \leq \deg(\mathfrak{P}_j + (f_m)) = \deg(f_m)\deg(\mathfrak{P}_j).$$

Putting all of this together yields

$$\operatorname{Deg}(\mathfrak{A}) \leq \deg(f_m) \sum \deg(\mathfrak{P}_j) = \deg(f_m)\operatorname{Deg}(\mathfrak{B}) \\ \leq \deg(f_m)\deg(f_{m-1}) \cdots \deg(f_1).$$

It is obvious that Theorem 3.1 is a special case of Theorem 3.6.

4. Main results

In this section k will denote the finite field $GF(q)$ and K will be a function field in one variable in which k is the exact constant field. Since k is perfect, K is, of course, a regular extension of k. By P we will mean a prime correspondence from K to itself. That is to say, P is a non-zero prime ideal of the Dedekind ring $K \otimes_k K$. When $L = K \otimes_k K/P$, we denote by K_1

and K_2 the two copies of K contained in L and set $m = [L:K_1]$ and $n = [L:K_2]$. Let $X^{K/k}$ be the Riemann surface for K over k. Finally let

$$A_P = \{\mathcal{P} \in X^{K/k} \mid \mathcal{P} \text{ divides } \mathcal{P}^P\}.$$

THEOREM 4.1. *If* (i) $m = n = 1$ *and P is not the diagonal or* (ii) m/n *is not an integral power of q, then* $\delta(A_P) = 0$.

The proof will be broken into a number of component propositions. Let us first dispose of case (i) of the theorem.

THEOREM 4.1.1. *If $m = n = 1$ and P is not the diagonal, then* $\delta(A_P) = 0$.

Proof. In this case P may be regarded as an automorphism of K over k. Moreover $A_P = \{\mathcal{P} \in X^{K/k} \mid \mathcal{P} = \mathcal{P}^P\}$. Let L be the fixed field of P. We claim that $[K:L]$ is finite. It suffices to show that the automorphism group of K over k is finite. When .the genus of K is greater than or equal to two, the group is finite by the Schwartz-Klein Theorem [5, theorem on p. 66]. Suppose the genus of K is zero or one. We know there is a divisor $\mathcal{A}$ on K of degree one [1, Chap. 5, Theorem 5]. By the Riemann-Roch Theorem and the assumption on the genus, one has dim $(\mathcal{A}) \geq 1$. Hence there is a k-rational point in $X^{K/k}$. When the genus of K is zero, $K = k(x)$ and the automorphism group is $PGL_2(k)$ which is, of course, finite when k is. When the genus of K is one, the automorphism group is, except for a possible exceptional finite part, isomorphic to the group of k-rational points in $X^{K/k}$ and this is finite when k is. See [2, Chap. IV, §2.2]. Putting this all together we see that A_P is precisely the set of points in the Riemann surface for K that are totally inert over L. By Theorem 2.21, $\delta(A_P) = 0$.

We next prove case (ii) with certain additional assumptions which will be removed later.

THEOREM 4.1.2. *Let m/n be unequal to any integral power of q. If P is absolutely irreducible* (*that is, k is exact in* $L = K \otimes_k K/P$) *and* $q > \max\{m, n\}$, *then* $\delta(A_P) = 0$.

Proof. It is easily seen that $\mathcal{P}$ is in A_P if and only if there is a point $\mathfrak{P}$ in $X^{L/k}$ that lies over $\mathcal{P}$ in both K_1 and K_2. By Theorem 2.10, $g(\mathfrak{P}) = g(\mathcal{P})$ for almost all such $\mathcal{P}$. We let

$$B_P = \{\mathfrak{P} \in X^{L/k} \mid N_{L/K_1}\mathfrak{P} = N_{L/K_2}\mathfrak{P} \text{ and } \mathfrak{P} \text{ is of relative degree one over } K\}.$$

It clearly suffices to show $\delta(B_P) = 0$. Let $B_r = \{\text{all } \mathfrak{P} \in B_P \mid g(\mathfrak{P}) = r\}$ and set $|B_r|$ equal to the number of elements of B_r. We next let

$$C_P = \{\text{all integral divisors } \mathcal{A} \text{ on } L \mid N_{L/K_1}\mathcal{A} = N_{L/K_2}\mathcal{A}\},$$

$$C_r = \{\text{all } \mathcal{A} \in C_P \mid g(\mathcal{A}) = r\}$$

and $| C_r |$ equal the number of elements of C_r. Clearly $| B_r | \leq | C_r |$. Hence it suffices to show $\lim_{u \to 1/q} (\sum | C_r | u^r/(-\log (1 - qu))) = 0$. For this limit to vanish it in turn suffices to show that $\lim_{u \to 1/q} \sum | C_r | u^r$ exists and is finite. Thus if we can show that there is a positive constant c such that $| C_r | \leq cn^r$ for all r we are done since $n < q$ by hypothesis (we are here assuming without loss that $m \leq n$). In order to show the above inequality, let $\mathcal{A}$ be in C_r and let $\omega_1, \cdots, \omega_s$ be a k-basis for $L(\mathcal{A})$. Next let $\mathcal{B} = N_{L/K1} \mathcal{A} = N_{L/K_1} \mathcal{A}$ and let $\eta_1, \cdots, \eta_t$ be a k-basis for $L(\mathcal{B})$. It is easily seen that $N_{L/K_1} (L(\mathcal{A})) \leq L(\mathcal{B})$ for $i = 1, 2$. Now if $\sum a_j \omega_j \mathcal{A}$ is in $L(\mathcal{A})$, then one has

$$N_{L/K_1} (\sum a_j \omega_j \mathcal{A}) = \sum F_j(a_1, \cdots, a_s)\eta_j$$

and

$$N_{L/K_2}(\sum a_j \omega_j \mathcal{A}) = \sum G_j(a_1, \cdots, a_s)\eta_j$$

where the F_j and G_j are homogeneous polynomials of degrees m and n, respectively. It is clear that $\sum a_j\omega_j \mathcal{A}$ is in C_P if and only if there is an element a in k^* such that

$$aF_j(a_1, \cdots, a_s) = G_j(a_1, \cdots, a_s) \quad \text{for} \quad j = 1, \cdots, t.$$

We wish to count the number of solutions for this system in k. Since we will need only an upper estimate it suffices to estimate the number of solutions in $\bar{k}$ (the algebraic closure of k) of the system

$$a_0^{n-m}F_j(a_1, \cdots, a_s) - G_j(a_1, \cdots, a_s) = 0, \quad j = 1, \cdots, t.$$

Let us explicitly note at this point that $n - m \neq 0$ since m/n is not a power of q and, in fact, $n - m > 0$ by assumption. We first claim that the above system of equations has only a finite number of solutions. Indeed if it did not then there would be a solution on the hyperplane $a_0 = 0$. But this means that the system

$$G_j(a_1, \cdots, a_s) = 0, \quad j = 1, \cdots, t$$

possesses a non-trivial solution. But this says that $N_{L/K_2}(\sum a_j \omega_j) = 0$ (we have passed here to $\bar{L} = L \otimes_k \bar{k}$ and $\bar{K} = K \otimes_k \bar{k}$.) But then $\sum a_j \omega_j = 0$ and each $a_j = 0$. Finally by the Extended Bézout Theorem 3.1, the number of solutions of the system is at most n^t. Now $t = \dim (\mathcal{B}) = r + 1 - g_k$ for all r sufficiently large (g_k is the genus of K). Next note that there are at most h linearly inequivalent elements of C_r where h is the projective class number of L. Thus for all sufficiently large r, $| C_r | \leq hn^{r+1-g_k}$ and there then clearly exists a positive constant c such that $| C_r | \leq cn^r$ for all r.

It is now necessary to remove the special hypotheses that were used in Theorem 4.1.2.

PROPOSITION 4.2. *Let m/n be unequal to any integral power of q. If P is not absolutely irreducible and $\delta(A_P) \neq 0$ then there is a finite extension*

$k_r = GF(q^r)$ of k and a prime correspondence Q on $K_r = K \otimes_k k_r$ such that $\delta(A_Q) \neq 0$, Q is absolutely irreducible and the ratio of the degrees of Q is unequal to any integral power of q^r.

Proof. Let k_r be the algebraic closure of k in $L = K \otimes_k K/P$. Then two copies of K_r are contained in L in an obvious way. Call them K_{1r} and K_{2r}. We have the exact sequence $0 \to P_r \to K_r \otimes_{k_r} K_r \to L \to 0$. Now for almost all $\mathcal{P}$ in A_P there is a point $\mathfrak{P}$ on the Riemann surface for L that lies over $\mathcal{P}$ in both K_1 and K_2 and such that $g(\mathfrak{P}) = g(\mathcal{P})$. Hence $\mathcal{P}$ must decompose completely in K_r since the latter is an unramified abelian extension of K. Say $\mathcal{P}$ splits into $\mathcal{P}_1, \cdots, \mathcal{P}_r$ in K_r. Then $\mathcal{P}_1^{P_r}$ is divisible by some $\mathcal{P}_i$. Let F_q be the Frobenius correspondence in K and denote by F_q as well the extension of F_q to K_r. Then $\mathcal{P}_j$ divide $\mathcal{P}_j^{P_r F} q^a$, $j = 1, \cdots, r$ for a suitable $a < r$. Thus $\delta(P_r F_q a) \neq 0$ for some $a < r$. Now $P_r F_q a$ need not be prime but it is at worst of the form $P_r F_q a = p^b Q$ where Q is prime and p is the characteristic of k. Note that the degrees of Q are K/rp^b and nq^a/rp^b and their ratio is certainly not a power of q^r. Moreover, $\delta(A_Q)$ is not zero since $\delta(P_r F_q a) \neq 0$. In order to see that Q is absolutely irreducible we note that Q is obtained by considering P_r in $K_r \otimes_{k_r} K_r$ and observing that Q lies beneath P_r in $K_r \otimes_{k_r} k_r K_r^{q^a}$. Now k_r is exact in $K_r \otimes_{k_r} k_r K_r^{q^a}/Q$ since it is exact in the larger field $K_r \otimes_{k_n} K_r/P_r = L$ by hypothesis.

Finally we eliminate the remaining extraneous hypothesis.

PROPOSITION 4.3. *Let m/n be unequal to any integral power of q and assume that P is absolutely irreducible. If $\delta(A_P) \neq 0$, then there is a finite extension $k_r = GF(q^r)$ of k such that the extension P_r of P to $K_r = K \otimes_k k_r$ is absolutely irreducible, $\delta(A_{P_r}) \neq 0$, q^r is greater than both degrees of P_r and the ratio of those degrees is unequal to any integral power of q^r.*

Proof. For the sake of argument assume $m < n$. If $n < q$ we are clearly done. Suppose that $m < q \leq n$. Let p_1 be the smallest rational prime such that $n < q^{p_1}$. Moreover let $p_1 < p_2 < \cdots$ be the rational primes bigger than p_1 written in order. Let $A_P = B_s \cup C_s$ where C_s consists of all $\mathcal{P}$ in A_P that are totally inert in $k_r \otimes_k K$ where $r = p_1 \cdots p_s$ and let B_s be the complement of C_s in A_P. By Theorem 2.20,

$$\bar{\delta}(C_s) \leq \textstyle\prod_{j=1}^{s} (1 - p_j^{-1}).$$

We claim $\delta(B_s) \neq 0$ for some s. If this were not the case we would have $\bar{\delta}(A_P) = \bar{\delta}(C_s)$ for all s. However, $\bar{\delta}(C_s)$ can be made arbitrarily small when s is sufficiently large since the dominating product $\prod_{j=1}^{s} (1 - p_j^{-1})$ is a partial product of the reciprocal of the Riemann Zeta function evaluated at one. Let us assume, therefore, that s has been selected so that $\delta(B_s) \neq 0$. Now $B_s = \bigcup_{j=1}^{s} D_j$ where D_j consists of all $\mathcal{P}$ in B_s such that $\mathcal{P}$ is totally decomposed in $k_{p_j} \otimes_k K$. Hence $\delta(D_j) \neq 0$ for some j. We call p_j simply p. Let $K_p = K \otimes_k k_p$ and $L_p = L \otimes_k k_p$ and recall that L_p is a field since P

is absolutely irreducible ($L = K \otimes_k K/P$.) Let $\mathcal{P}$ be an element of $D = D_j$ and let $\mathcal{P}_1, \cdots, \mathcal{P}_p$ be the primes of K_p that lie above it. Moreover, denote by P_p the extension of P to K_p. Now $\mathcal{P}_1$ divides $\mathcal{P}_i^{P_p}$ for some i. Thus for some $a < p$, $\mathcal{P}_j$ divides

$$\mathcal{P}_j^{P_p F^*_{q^a}}, \quad j = 1, \cdots, p$$

where F_q^* is the Rosati adjoint of the Frobenius correspondence (extended to K_p.) One sees that $\delta(A_p F^*_{q^a}) \neq 0$ for some $a < p$. Now $P_p F^*_{q^a}$ may not be prime but because of pure inseparability $P_p F^*_{q^a} = p_0^e Q$ where Q is prime and p_0 is the characteristic of k. Clearly $\delta(A_Q) \neq 0$. The degrees of Q are $m_0 = mq^a/p_0^e$ and $n_0 = n/p_0^e$. Hence m_0/n_0 is not an integral power of q^p. Moreover, $m_0 \leq mq^a < q^p$ and $n_0 \leq n < q^p$. Finally we must show that Q is absolutely irreducible. To this end we consider P_p as a prime ideal of $K_p \otimes_{k_p} k_p K_p^{q^a}$ and observe that Q is the prime of $K_p \otimes_{k_p} K_p$ that lies above it. Since k_p is exact in $K_p \otimes_{k_p} k_p K_p^{q^a}/P_p = L_p$ and $K_p \otimes_{k_p} K_p^{q^a}/Q$ is a purely inseparable extension of L_p, k_p must remain exact since it is a perfect field. Returning now to the hypothesis made at the beginning of the proof we see that we are reduced to the case that $q \leq m < n$. In order to handle this case repeat the argument above using F_q instead of F_q^*. As above we obtain $m_0 \leq m < q^p$ and $n_0 \leq nq^a$. If $n_0 < q^p$ we are done and if $q^p \leq n_0$ we are back in the first case. The only substantial difference in the argument occurs when we seek to prove Q absolutely irreducible. Here P_p is a prime in $K_p \otimes_{k_p} K_p$ and Q is the prime that lies below it in $K_p \otimes_{k_p} k_p K_p^{q^a}$. Thus

$$k_p = K_p \otimes_{k_p} k_p K_p^{q^a}/Q \leq K_p \otimes_{k_p} K_p/P_p = L_p$$

and since k_p is exact in L_p it remains exact in the smaller field.

The proof of Theorem 4.1 is now complete. It is, of course, natural to conjecture that the hypotheses (i) and (ii) in P are excessive. We should have simply that $\delta(A_p) = 0$ when P is not a power of either F_q or F_q^*. The reader may easily verify that the case $m = n$ is the only substantial impediment to a proof for this conjecture. Since the case $m = n = 1$ has been taken care of some sort of inductive argument would seem indicated but none has yet appeared.

References

1. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1967.
2. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York, 1966.
3. W. Krull, *Idealtheorie*, Chelsea, New York, 1948.
4. R. E. MacRae, *On unique factorization in certain rings of algebraic functions*, J. Algebra, vol. 17 (1971), pp. 243-261.
5. P. Samuel, *Lectures on old and new results on algebraic curves*, Tata Institute, Bombay, 1966.
6. O. Zariski and P. Samuel, *Commutative algebra, vols. I and II*, Van Nostrand, New York, 1958 and 1960.

The University of Colorado
Boulder, Colorado