THE NONREGULAR ANALOGUE OF TCHEBOTAREV’S
THEOREM

MICHAEL FRIED
THE NONREGULAR ANALOGUE OF TCHEBOTAREV'S THEOREM

M. FRIED

Let \( L/K \) be a Galois extension of function fields in one variable where \( K \) has exact constants \( \mathcal{F}(q) \), the finite field with \( q \) elements. For \( l \) a fixed integer and \( \xi \) a conjugacy class of \( \mathfrak{G}(L/K) \), this paper counts the primes \( \wp \) of \( K \) of degree \( l \) for which the Artin symbol

\[
\left( \frac{L/K}{\wp} \right)
\]

equals \( \xi \) (Theorem 1.4). The answer depends on the restriction of elements of \( \xi \) to the algebraic closure of \( \mathcal{F}(q) \) in \( L \): a proper extension of \( \mathcal{F}(q) \) in general.

For \( l = 1 \) [Fr; Proposition 2] followed Dirichlet's celebrated argument using the rationality of \( L \)-series. Tchebotarev's original "field crossing argument" [T] is a part of the reduction to the cyclic case ([D] and [M]) that at once removes the restriction on \( l \) and the need for \( L \)-series (other than the Riemann hypothesis for curves over finite fields). This more elementary argument also improves the error estimates and therefore such practical applications as [FrS] and explicit forms of Hilbert's irreducibility theorem [Fr; §3]. We comment briefly on the latter (§2) to facilitate its use in [Fr, 2; §4] for the explicit production of rank 12 elliptic curves over \( \mathbb{Q} \).

Acknowledgement. This paper is a rewrite (with improvements) of Moshe Jarden's rewrite (with improvements) of our original notes. In particular, Lemma 1.2 improves one of the original arguments.

1. The nonregular analogue. Denote by \( \bar{K} \) the algebraic closure of a field \( K \). A field extension \( K/k \) of transcendence dimension 1 is a function field in one variable over \( k \) if \( k \) is algebraically closed in \( K \).

Denote by \( \mathcal{F}(q) = k \) the finite field of \( q \) elements. Let \( K \) be a function field of one variable over \( \mathcal{F}(q) \). Choose a separating transcendence base \( t \) for \( K/k \). Denote by \( \varnothing_k \) the integral closure of \( k[t] \) in \( K \). If \( K' = \mathcal{F}(q') \cdot K \), then \( \varnothing_{k'} = \mathcal{F}(q') \cdot \varnothing_k \). If \( \wp' \) is a prime ideal of \( \varnothing_{k'} \) lying over \( \wp \) of degree \( j \) and \( j \mid l \), then the relative residue class degree is \( [\varnothing_{k'}/\wp' : \varnothing_k/\wp] = l/j \). Hence, if \( g(\wp) \) denotes the number of prime ideals of \( \varnothing_{k'} \) lying over \( \wp \), then \( g(\wp) = j \).

Denote by \( F(q) \) the Frobenius element of \( \mathfrak{S}(\mathcal{F}(q)/\mathcal{F}(q)) \) (i.e., \( F(q)(x) = x^q \) for each \( x \in \mathcal{F}(q) \)). Consider a finite Galois extension \( L \) of \( K \) of
degree $n$ and a conjugacy class $\mathfrak{C}$ in $\mathfrak{G}(L/K)$ with, say, $c$ elements. Associate to $\mathfrak{C}$ the set

$$C = \left\{ \mathfrak{p} \in P'(K) \mid \left( \frac{L/K}{\mathfrak{p}} \right) = \mathfrak{C} \right\},$$

where $P'(K)$ is the set of all prime ideals of $\mathfrak{O}_K$ unramified in $\mathfrak{O}_L$, and

$$\left( \frac{L/K}{\mathfrak{p}} \right)$$

is the conjugacy class associated to a Frobenius element

$$\left[ \frac{L/K}{\mathfrak{p}} \right]$$

for $\mathfrak{p}$ a prime of $\mathfrak{O}_L$ lying over $\mathfrak{p}$.

Use the following notation:

$\hat{k} =$ the algebraic closure of $k$ in $L$;

$\hat{n} = \left[ \hat{k} : k \right], \quad n^0 = n/\hat{n} = \left[ L : \hat{k} \cdot K \right]$;

$P_l(K) = \{ \mathfrak{p} \in P(K) \mid \deg(\mathfrak{p}) = l \}$;

$P'_l(K) = \{ \mathfrak{p} \in P(K) \mid \mathfrak{p} \text{ is unramified in } L \text{ and } \deg(\mathfrak{p}) = l \}$;

$C_l(K) = \left\{ p \in P'_l(K) \mid \left( \frac{L/K}{p} \right) = \mathfrak{C} \right\}$;

$R(L/K) = \{ \mathfrak{p} \in P(K) \mid \mathfrak{p} \text{ is ramified in } L \}$;

$R_l(L/K) = \{ \mathfrak{p} \in R(L/K) \mid \deg(\mathfrak{p}) = l \}$;

$G = \mathfrak{G}(L/K)$.

Our first result counts the elements of $C_l(k)$, as did [Fr; Proposition 2]. But here a "field crossing argument" descendent from Tchebotarev's ideas ([T]—a similar argument appears in [FrHJ] applied to a different project) replaces the rationality of the Artin $L$-series. Thus the proof does not mimic Dirichlet's original argument. Indeed, in almost every way it is simpler than [Fr; Proposition 2] and it thereby simplifies the constant in the "$O$" notation.

**Theorem 1.1.** If an element $\tau$ (equivalently, every element) of $\mathfrak{C}$ satisfies

$$\text{res}_{\hat{k}}(\tau) = \text{res}_{\hat{k}}(F(q)),$$

(1)
\[
|C_1(K)| = (c/n^0) \cdot q + O(\sqrt{q}).
\]

The "\(O\)" notation indicates a function bounded by \(A \cdot \sqrt{q}\) with \(A\) a computable function of \(g(K)\) (the genus of \(K\)) and \(|R_1(L/K)|\). Otherwise, it does not depend on \(q\), on \(K\) or on \(L\).

**Proof.** Let \(\tau \in \mathbb{C}, f = \text{ord}(\tau)\) and \(k' = F(q')\). From (1) \(\hat{n} | f\). Thus \(K' = k' \cdot K\) is a finite Galois extension of \(K\) and for \(L' = k' \cdot L, [L' : K'] = [L : k \cdot K] = n^0\). Thus, we naturally identify \(\mathfrak{c}(K'/K)\) with \(\mathfrak{c}(k'/k)\) and thereby \(\mathfrak{c}(L'/K)\) with
\[
\{(\sigma_1, \sigma_2) \in \mathfrak{c}(L/K) \times \mathfrak{c}(k'/k) \mid \text{res}_k(\sigma_1) = \text{res}_k(\sigma_2)\}
\]

\([L; \text{p. } 198]\).

In particular, consider the extension of \(\tau\) to \(L'\) through the element \(\tilde{\tau} = (\tau, \text{res}_k(F(q)))\). Then \(\tilde{\tau}\) is also of order \(f\).

**Divide the rest of the proof into parts.**

**Part A. Field crossing argument.** If \(L(\tilde{\tau})\) is the fixed field of \(\tilde{\tau}\) in \(L'\) then \(L(\tau) = L(\tilde{\tau}) \cap L\) is of index \(f\) in \(L\). The restriction of the frobenius element to \(k' \cap L(\tilde{\tau})\) is the identity, so \(k' \cap L(\tilde{\tau}) = k\), \(k' \cdot L(\tilde{\tau}) = L'\) and \(L(\tilde{\tau})\) is a function field of one variable over \(k\). Let \(d = [k' : k] = [L' : L]\).

Consider \(P_1^*(L(\tilde{\tau})) = \{q \in P(L(\tilde{\tau})) \mid \text{deg}(q) = 1 \text{ and } q \text{ is unramified over } K\}\). Define
\[
C_\tau = \left\{\mathfrak{p} \in P'(L) \mid \text{deg}(\mathfrak{p} \cap k) = 1 \text{ and } \left[\frac{L/K}{\mathfrak{p}}\right] = \tau\right\}.
\]

Then there is a map \(h: P_1^*(L(\tilde{\tau})) \to C_\tau\) as follows: For an element \(q \in P_1^*(L(\tilde{\tau}))\) there exists a unique \(q' \in P(L')\) lying over \(q\). Then \(\mathfrak{p} = h(q) = q' \cap \mathfrak{p}\). Since
\[
\left[\frac{L'/L(\tilde{\tau})}{q'}\right]
\]
is the frobenius acting on \(k'\), then it must be \(\tilde{\tau}\) and its restriction to \(L\) is therefore \(\tau\). From the formula
\[
\left[\frac{L'/K}{q'}\right] = \left(\left[\frac{L/K}{q' \cap \mathfrak{p}_L}\right], \left[\frac{K'/K}{q' \cap \mathfrak{p}_{K'}}\right]\right),
\]
\[
\left[\frac{L/K}{\mathfrak{p}}\right] = \tau.
\]

(3)
Also, if $p = \mathcal{P} \cap \mathcal{O}_K$, then $\mathcal{O}_K/p \subseteq \mathcal{O}_{L(\mathcal{P})}/q = k$. So $\mathcal{O}_K/p = k$ and $\mathcal{P} \in C_\tau$.

Finally, we conclude that for $\mathcal{P} \in C_\tau$, $h^{-1}(\mathcal{P})$ contains exactly $d$ elements. Since $\mathcal{O}_L/\mathcal{P} = k'$, for $q'$ a prime of $\mathcal{O}_L$ over $\mathcal{P}$, $\mathcal{O}_L/q' = k'$. So there are $[L' : L] = d$ primes $q'_1, \ldots, q'_d \in P(L')$ above $\mathcal{P}$ and

$$\left[ \frac{L'/K}{q'} \right] = \tilde{\tau}, \quad i = 1, \ldots, d.$$  

Thus, if $q'_i \cap \mathcal{O}_{L(\mathcal{P})} = q_i$, then $\mathcal{O}_{L(\mathcal{P})}/q_i = k$ and $q_i \in h^{-1}(\mathcal{P})$ with $q'_i$ the unique element of $P(L')$ that lies over $q_i$. Clearly, therefore, $q_1, \ldots, q_d$ are the distinct elements of $h^{-1}(\mathcal{P})$.

**Part B. Counting the cardinality of $C_\tau$.** From the Riemann hypothesis for curves

$$|P_1(L(\mathcal{P}))| = q + O\left(\sqrt{q}\right)$$

where $O(\sqrt{q})$ is bounded by $A \cdot \sqrt{q}$ with $A$ equal to twice the genus of $L(\mathcal{P})$. Thus $A$ is bounded by the maximum of 1 and $([L(\mathcal{P}) : k(t)] - 1) \cdot ([L(\mathcal{P}) : k(t)] - 2)$, for any nonconstant $t \in L$. In particular, $A$ is bounded by $[L : k(t)]^2$. From (4)

$$|P_1^*(L(\mathcal{P}))| = q + O\left(\sqrt{q}\right),$$

but here the $O$ notation must be adjusted to include a function of $|R_1(L/K)|$ as stipulated in the statement of the theorem. Since there are $d$ primes of $P_1^*(L(\mathcal{P}))$ for each one of $C_\tau$,

$$|C_\tau| = (1/d) \cdot q + O\left(\sqrt{q}\right).$$

**Part C. Conclusion of the proof.** From Part B

$$\left| \bigcup_{\tau \in \mathcal{C}} C_\tau \right| = \left( c/d \right) \cdot q + O\left(\sqrt{q}\right).$$

Over every element of $C_l(K)$ there lie exactly $g = [L(\mathcal{P}) : K]$ elements of $\bigcup C_\tau$. If we show that $g \cdot d = n^0$, then $|C_l(K)| = (c/n^0) \cdot q + O(\sqrt{q})$ and the theorem is done. But $g = n/f$ and $d = f/[k' : k]$ and the result follows immediately. \qed

The next two lemmas consider the cardinality of $C_l(K)$ for $l$ general, but $L/K$ is cyclic. Again, let $K$ be a function field in one variable over $F(q) = k$. 
Lemma 1.2. Let $K'$ be a finite extension of $K$ and let $F(q^u)$ be the algebraic closure of $k$ in $K'$. For a multiple $v$ of $u$ let

$$P_{v/u}(K'/K) = \{v' \in P_{v/u}(K') \mid \deg(v' \cap \mathfrak{O}_K) \neq v\}.$$  

Then, for any $\varepsilon > \frac{1}{2}$, $|P_{v/u}(K'/K)| = O(q^{v\cdot \varepsilon})$. The constant in the $O$ notation may be chosen independent of $v$.  

Proof. If $v' \in P_{v/u}(K'/K)$, then $\mathfrak{O}_{K'}/v' = F(q^v)$. Therefore, the residue field of $v = \mathfrak{O}_K \cap v'$ is $F(q^j)$, with $j$ a proper divisor of $v$. So $j \leq v/2$. Over every such $v$ there lie at most $[K' : K]$ elements of $P(K')$. Thus, from the simple estimate $|P_j(K)| = O(q^j)$, conclude that

$$|P_{v/u}(K'/K)| \leq [K' : K] \sum_{j \leq v/2} |P_j(K)| = O\left((v/2) \cdot q^{v/2}\right) = O(q^{v \cdot \varepsilon}).$$

Return to the notation of the proof of Theorem 1.1 where $\hat{k}$ is the algebraic closure of $k$ in $L$.

Lemma 1.3. Assume that $L/K$ is a cyclic extension and that the unique element $\tau$ of $G$ generates $\mathfrak{G}(L/K)$. Let $\nu$ be a positive integer for which

$$\text{Res}_K(\tau) = \text{Res}_K(F(q^\nu)).$$

For any $\varepsilon > \frac{1}{2}$, $|C_\nu(K)| = (1/v \cdot n^0) \cdot q^{\nu} + O(q^{\nu \cdot \varepsilon})$ where the constant in the $O$ notation may be chosen to be independent of $v$.

Proof. Let $k' = F(q^\nu)$, $\hat{k}' = k' \cdot \hat{k}$ and $L' = k' \cdot L$. Then $L'$ is a cyclic extension of $K'$ and $\hat{k}'$ is the algebraic closure of $k'$ in $L'$. Also, (7) implies that $\hat{k} \cap k' = k$. As in the proof of Theorem 1.1, identify $\mathfrak{G}(L'/K)$ with $\{(\sigma_1, \sigma_2) \in \mathfrak{G}(L/K) \times G(k'/k) \mid \text{Res}_K(\sigma_1) = \text{Res}_K(\sigma_2)\}$. Consider $\tau' = (\tau, \text{Res}_K(F(q^\nu)))$. Since $\tau'$ fixes $k'$, $\tau' \in \mathfrak{G}(L'/K')$. Define

$$C_{\tau'} = \left\{v' \in P(K') \text{ of degree 1 (over } k') \mid \left(\frac{L'/K'}{v'}\right) = \tau'\right\}.$$

As $R_\nu(L'/K')$ consists of extensions of elements of $\bigcup_{j \neq v} R_j(L/K)$,

$$|R_\nu(L'/K')| \leq |R(L/K)| \cdot \max\{\deg(v) \mid v \in R(L/K)\}.$$  

From Theorem 1.1 conclude

$$|C_{\tau'}| = (1/n^0) \cdot q^{\nu} + O(q^{\nu/2}).$$

Define $C_{\tau'}' = \{v' \in C_{\tau'} \mid \deg(\mathfrak{O}_K \cap v') = v\}.$
From (8) and Lemma 1.2, \(|C'\) = \((1/n_0) \cdot q^v + O(q^{v+\varepsilon})\).

Compare \(C_v(K)\) and \(C'\), by the argument of Part A of the proof of Theorem 1.1, especially expression (3): for every element \(p \in C_v(K)\) there are exactly \(v\) primes \(p_1', \ldots, p_v'\), of \(\Theta_{K'}\) over \(p\) with

\[
\left( \frac{L'/K'}{p_i'} \right) = \tau'.
\]

Thus \(p_i' \in C'\). Conversely, if \(p' \in C'\) then (3) shows \(\Theta_K \cap p' \subseteq C_v(K)\). The lemma follows easily. \(\square\)

The proof of our main theorem reduces the computation of \(|C_t(K)|\) in the general case to the case where \(L/K\) is cyclic. Among other places, [D] and [M] contain the idea for this.

**Theorem 1.4.** Let \(\mathcal{C}\) be a conjugacy class of cardinality \(c\) of \(\Theta(L/K)\) represented by an element \(\tau\). Let \(v\) be a positive integer for which

\[
(9) \quad \text{res}_K(\tau) = \text{res}_K(F(q^v)).
\]

For any integer \(l > 0\), \(C_t(K)\) is empty if \(l \equiv v \mod \hat{n}\). Otherwise, if \(e > \frac{1}{2}\), then

\[
(10) \quad |C_t(K)| = \left( \frac{c}{l \cdot n_0} \right) \cdot q^l + O(q^{e-1})
\]

where the constant in the \(O\) notation may be chosen independent of \(v\).

**Proof.** If \(C_t(K)\) contains a prime \(p\) and if \(\mathfrak{P} \in P(L)\) lies over \(p\), then

\[
\text{res}_K\left( \left[ \frac{L/K}{\mathfrak{P}} \right] \right) = \text{res}_K(F(q^v)).
\]

But (9) implies

\[
\text{res}_K\left( \left[ \frac{L/K}{\mathfrak{P}} \right] \right) = \text{res}_K(F(q^v)).
\]

Clearly, \(l \equiv v \mod \hat{n}\). Now assume that \(\hat{n} \mid l - v\).

Let \(d = (v, \hat{n}) = (l, \hat{n})\). Then the algebraic closure of \(k\) in the fixed field \(K' = L^{(\tau)}\) of \(\tau\) is \(F(q^d)\). Define:

\[
C_{l/d}(K') = \left\{ p' \in P(K') \mid \left( \frac{L/K'}{p'} \right) = \tau, \deg(p') = l/d, \right. \left. p' \text{ is unramified over } K \text{ and } \deg(\Theta_K \cap p') = l \right\}.
\]
From Lemmas 1.2 and 1.3, with \( n' = [L: \hat{k} \cdot K'] \),

\[
|C'_{l/d}(K')| = \left( \frac{d}{l} \cdot n' \right) \cdot (q^d)^{1/d} + O(q^{d \cdot \varepsilon \cdot (l/d)})
\]

\[
= \left( \frac{d}{l} \cdot n' \right) \cdot q^l + O(q^{\varepsilon \cdot l}).
\]

Consider the map \( h: C'_{l/d}(K') \to C_l(K) \) by \( h(p') = \mathfrak{G}_K \cap p' \). Since

\[
\left( \frac{L/K'}{p'} \right) = \tau
\]

there exists a unique element \( \mathfrak{P} \in P(L) \) over \( p' \) and it satisfies

\[
\left[ \frac{L/K'}{\mathfrak{P}} \right] = \tau.
\]

By the definition of \( K' \),

\[
\tau = \left[ \frac{L/K}{\mathfrak{P}} \right].
\]

Thus \( p \in C_l(K) \).

Conversely, suppose \( p \in C_l(K) \) and \( \mathfrak{P} \in P(L) \) lies over \( p \) with

\[
\left[ \frac{L/K}{\mathfrak{P}} \right] = \tau.
\]

Then for \( p' = K' \cap \mathfrak{P} \),

\[
\left[ \frac{L/K'}{p'} \right] = \tau.
\]

So \( p' \in C'_{l/d}(K') \) and \( h(p') = p \).

The order of \( h^{-1}(p) \) is therefore the number of \( \mathfrak{P} \in P(L) \) that lie over \( p \) and satisfy

\[
\left[ \frac{L/K}{\mathfrak{P}} \right] = \tau.
\]

They are conjugate among each other by the centralizer, \( C_G(\tau) \), of \( \tau \). Thus,

\[
|h^{-1}(p)| = |C_G(\tau)|/|D(\mathfrak{P})| = |G|/|D(\mathfrak{P})| \cdot |\mathfrak{C}| = [K' : K]/c
\]

where \( D(\mathfrak{P}) = \mathfrak{G}(L/K') \) is the decomposition group of \( \mathfrak{P} \) in \( G \). From (11),

\[
|C_l(K)| = (d \cdot c/l \cdot n' \cdot [K' : K]) \cdot q^l + O(q^{\varepsilon \cdot l})
\]

\[
= (c/l \cdot n^0) \cdot q^l + O(q^{\varepsilon \cdot l}).
\]
2. Application to Hilbert's irreducibility theorem. We review quickly (so as to display the improvements) the heart of the application of Theorem 1.1. to the explicit form of Hilbert's Irreducibility Theorem of [Fr; §3]. For simplicity start over \( \mathbb{Q} \), but the idea works as well over any number field.

Consider \( f(x, y) \in \mathbb{Z}[x, y] \), an irreducible polynomial that is monic in \( y \).

**Goal:** Find an explicit arithmetic progression \( P \) in \( \mathbb{Z} \) for which \( f(x_0, y) \) is irreducible over \( \mathbb{Q} \) for \( x_0 \in P \). Here is how to find \( P \).

Let \( \Omega_f \) be the splitting field of \( f \) over \( \mathbb{Q}(x) \). Identify \( \Omega_f/\mathbb{Q}(x) \) with a (transitive) subgroup \( G \) of \( S_n \), \( n = \deg_y(f) \). Let \( I \) be any proper subset of \( \{1, 2, \ldots, n\} \) and let \( S_{n,I} \) be the subgroup of \( S_n \) consisting of elements that map \( I \) into itself. Let \( G_I = G \cap S_{n,I} \) and let \( T_I \) be the transitive representation of \( G \) arising from the action of \( G \) on the right cosets of \( G_I \). Choose \( \tau_I \in G \) such that \( T_I(\tau_I) \) fixes no integer. Finally, choose \( \mathcal{C} = \{\tau(1), \ldots, \tau(r)\} \subseteq G \) such that \( \tau_I \in \mathcal{C} \) for each \( I \).

Let \( p(i) \) be a prime of \( \mathbb{Z} \) and \( a(i) \in \mathbb{Z} \), \( i = 1, \ldots, r \), with the following properties. Let \( L_i \) be the reduction modulo \( p(i) \) of \( \Omega_f \) and use the notation of §1 to define \( \mathbb{F}(p(i)) \) as the algebraic closure of \( \mathbb{F}(p(i)) \) in \( L_i \). Then the decomposition group of some prime lying over \( x - a(i) \mod(p(i)) \) in \( L_i \) contains \( \tau(i) \) whose restriction to \( \mathbb{F}(p(i)) \) is \( \mathbb{F}(p(i)) \), and \( L_i^{(\tau(i))} \) (as in Part A of the proof of Theorem 1.1) has an \( \mathbb{F}(p(i)) \)-rational point lying over \( x - a(i) \mod(p(i)) \). Let \( g(L) \) be the genus of \( L \).

**Theorem 2.1.** Let \( P = \{a, a + \prod_{i=1}^r p(i), a + 2 \cdot \prod_{i=1}^r p(i), \ldots\} \) with \( a \equiv a(i)(p(i)) \), \( i = 1, \ldots, r \). Then \( f(x_0, y) \) is irreducible for \( x_0 \in P \). The distinct primes \( p(i) \), \( i = 1, \ldots, r \) may be chosen subject only to the conditions

1. restriction of \( \tau(i) \) to \( \mathbb{F}(p(i)) \) generates \( \mathfrak{S}(\mathbb{F}(p(i))/\mathbb{F}(p(i))) \); and
2. \( p(i) > 2 \cdot g(L_i^{(\tau(i))}) \).

**Proof.** The proof of [Fr; Theorem 3] shows that it is sufficient to choose the \( p \)'s and \( a \)'s so that the decomposition group of a prime of \( L_i \) over \( x - a(i) \mod(p(i)) \) contains \( \tau(i) \). Note that this is so according to the proof of Theorem 1.1 if \( L_i^{(\tau(i))} \) has an \( \mathbb{F}(p(i)) \)-rational point lying over \( x - a(i) \mod(p(i)) \); it is irrelevant whether \( L_i/\mathbb{F}(p(i))(x) \) is ramified over \( x - a(i) \mod(p(i)) \). Condition (2), according to the Riemann hypothesis for curves, guarantees the existence of an \( a(i) \) corresponding to an allowable \( p(i) \).
REFERENCES


Received May 20, 1982. Supported by NSF Grant MCS 80-03253.

UNIVERSITY OF CALIFORNIA
IRVINE, CA 92717
PACIFIC JOURNAL OF MATHEMATICS
EDITORS

DONALD BABBITT (Managing Editor)
University of California
Los Angeles, CA 90024

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113

HUGO ROSSI
University of Utah
Salt Lake City, UT 84112

R. FINN and H. SAMELSON
Stanford University
Stanford, CA 94305

C. C. MOORE and ARTHUR OGUS
University of California
Berkeley, CA 94720

ASSOCIATE EDITORS

R. ARENS
E. F. BECKENBACH
B. H. NEUMANN
F. WOLF
K. YOSHIDA

(1906–1982)

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF OREGON
UNIVERSITY OF BRITISH COLUMBIA
UNIVERSITY OF SOUTHERN CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
STANFORD UNIVERSITY
UNIVERSITY OF COLORADO
UNIVERSITY OF HAWAII
MONTANA STATE UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF NEVADA, RENO
UNIVERSITY OF UTAH
NEW MEXICO STATE UNIVERSITY
WASHINGTON STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the Pacific Journal of Mathematics should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. 39. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California 90024.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 50 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is issued monthly as of January 1966. Regular subscription rate: $132.00 a year (6 Vol., 12 issues). Special rate: $66.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics ISSN 0030-8730 is published monthly by the Pacific Journal of Mathematics at P.O. Box 969, Carmel Valley, CA 93924. Application to mail at Second-class postage rates is pending at Carmel Valley, California, and additional mailing offices. Postmaster: Send address changes to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS. A NON-PROFIT CORPORATION
Copyright © 1984 by Pacific Journal of Mathematics
Kenneth F. Andersen and Wo-Sang Young, On the reverse weak type inequality for the Hardy maximal function and the weighted classes $L(\log L)^k$ ................................................................. 257
Richard Eugene Bedient, Double branched covers and pretzel knots ........ 265
Harold Philip Boas, Holomorphic reproducing kernels in Reinhardt domains ................................................................. 273
Janey Antonio Daccach and Arthur Gabriel Wasserman, Stiefel’s theorem and toral actions ................................................................. 293
Michael Fried, The nonregular analogue of Tchebotarev’s theorem ........ 303
Stanley Joseph Gurak, Minimal polynomials for circular numbers .......... 313
Norimichi Hirano and Wataru Takahashi, Nonlinear ergodic theorems for an amenable semigroup of nonexpansive mappings in a Banach space .......... 333
Jim Hoste, Sewn-up $r$-link exteriors ................................................................. 347
Mohammad Ahmad Khan, The existence of totally dense subgroups in LCA groups ................................................................. 383
Mieczysław Kula, Murray Angus Marshall and Andrzej Sładek, Direct limits of finite spaces of orderings ................................................................. 391
Luis Montejano Peimbert, Flat Hilbert cube manifold pairs .................. 407
Steven C. Pinault, An a priori estimate in the calculus of variations ........ 427
McKenzie Y. K. Wang, Some remarks on the calculation of Stiefel-Whitney classes and a paper of Wu-Yi Hsiang’s ................................................................. 431
Brian Donald Wick, The calculation of an invariant for Tor ................. 445
Wolfgang Wollny, Contributions to Hilbert’s eighteenth problem .......... 451