PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 1, January 2009, Pages 73–83
S 0002-9939(08)09474-4
Article electronically published on August 13, 2008

DIRICHLET'S THEOREM FOR POLYNOMIAL RINGS

LIOR BARY-SOROKER

(Communicated by Ted Chinburg)

Abstract. We prove the following form of Dirichlet's theorem for polynomial rings in one indeterminate over a pseudo algebraically closed field F. For all relatively prime polynomials $a(X), b(X) \in F[X]$ and for every sufficiently large integer n there exist infinitely many polynomials $c(X) \in F[X]$ such that $a(X) + b(X)c(X)$ is irreducible of degree n, provided that F has a separable extension of degree n.

Introduction

Dirichlet's classical theorem on primes in arithmetic progressions states that if a, b are relatively prime positive integers, then there are infinitely many $c \in \mathbb{N}$ such that $a + bc$ is a prime number. Following a suggestion of Landau, Kornblum proved an analog of Dirichlet's theorem for the ring of polynomials $F[X]$ over a finite field F [Kor19]. Later, Artin refined Kornblum's result and proved that if $a(X), b(X) \in F[X]$ are relatively prime, then for every sufficiently large integer n there exists $c(X) \in F[X]$ such that $a(X) + b(X)c(X)$ is irreducible of degree n [Ros02, Theorem 4.8].

To avoid repetition, we shall say that Dirichlet's theorem holds for a polynomial ring $F[X]$ and a set of positive integers $\mathcal{N}$, if for any relatively prime polynomials $a, b \in F[X]$ there exist $n_0 > 0$ and infinitely many $c \in F[X]$ such that $a + bc$ is irreducible of degree n, for any $n \geq n_0$ in $\mathcal{N}$.

Jarden raised the question of whether the Artin-Kornblum result can be generalized to other fields. Of course, if F is algebraically closed, then the polynomial $a(X) + b(X)c(X)$ is reducible unless it is of degree 1. On the other hand, if F is Hilbertian, then there are infinitely many $\alpha \in F$ such that $a(X) + b(X)\alpha$ is irreducible in $F[X]$. To get irreducible polynomials of higher degree in this case, one may first choose $c(X) \in F[X]$ relatively prime to $a(X)$ and of high degree, and then find $\alpha \in F$ for which $a(X) + b(X)c(X)\alpha$ is irreducible over F.

Artin's proof of the result quoted in the first paragraph is based on a weak form of Weil's theorem on the Riemann hypothesis for absolutely irreducible curves over finite fields. The theorem roughly states that if a finite field F is large compared to the coefficients of the equations defining the curve, then the curve has F-rational points. This makes it plausible that for infinite fields F with the latter property the

Received by the editors January 29, 2007, and, in revised form, July 23, 2007, September 11, 2007, and January 2, 2008.

2000 *Mathematics Subject Classification.* Primary 12E30, 12E25.

Key words and phrases. Dirichlet's theorem, arithmetic progression, field arithmetics, Hilbert's irreducibility theorem, PAC field.

ring $F[X]$ should satisfy Dirichlet's theorem. Such fields are called PAC (Pseudo Algebraically Closed). Explicitly, a field F is **PAC** if every nonempty absolutely irreducible variety defined over F has an F-rational point. (See [FJ05, Chapter 11] for a comprehensive discussion of PAC fields and [FJ05, Theorem 18.6.1] for an abundance of algebraic extensions of countable Hilbertian fields which are PAC).

Of course, if F is algebraically closed, then it is PAC, but, as pointed out above, Dirichlet's theorem does not hold for $F[X]$ (for any infinite $\mathcal{N}$). Let $\mathcal{N}(F)$ be the set of all positive integers n such that F has a separable extension of degree n. Our main result asserts that Dirichlet's theorem holds for $\mathcal{N}(F)$.

Theorem A. *Let F be a PAC field. Then Dirichlet's theorem holds for $F[X]$ and $\mathcal{N}(F)$.*

The proof of Theorem A uses a weak form of Hilbert's Irreducibility Theorem that PAC fields satisfy and then argues as in the third paragraph. Roquette was the first to observe that a PAC field which has a rich Galois structure (namely, is ω-free) is Hilbertian [FJ05, Corollary 27.3.3].

We elaborate Roquette's approach and show in Corollary 1.4 that if F is PAC, $f \in F[X,Y]$ is irreducible, and the splitting field of $f(X,Y)$ over $F(Y)$ is regular over F, then, under some necessary assumptions, there are infinitely many specializations $Y \mapsto \alpha \in F$ for which $f(X,\alpha)$ remains irreducible over F.

Note that in order to get an irreducible specialization for a polynomial $f(X,Y)$, Roquette finds a specialization that preserves the Galois group $\mathrm{Gal}(f(X,Y),F(Y))$. Therefore it is somewhat unexpected that we can find an irreducible specialization even if $\mathrm{Gal}(f(X,Y),F(Y))$ does not occur as a Galois group over F.

As a preparation to the use of Corollary 1.4, we prove a result over an arbitrary infinite field which is interesting for its own sake.

Proposition B. *Let F be an infinite field with an algebraic closure $\tilde{F}$ and let $a(X),b(X) \in F[X]$ be relatively prime polynomials. Then for every sufficiently large positive integer n there exists $c(X) \in F[X]$ for which $f(X,Y) = a(X)+b(X)c(X)Y$ is irreducible over $F(Y)$ of degree n in X and $\mathrm{Gal}(f(X,Y),\tilde{F}(Y)) \cong S_n$.*

Finally, note that each infinite algebraic extension F of a finite field K is PAC [FJ05, Corollary 11.2.4]. By Theorem A, Dirichlet's theorem holds for $F[X]$ and $\mathcal{N}(F)$. This result already follows from a quantitative form of the result of Artin-Kornblum. Nevertheless, our proof has the advantage that the constructions are essentially explicit: The polynomial $c(X)$ in Theorem A equals the polynomial $c(X)$ appearing in Proposition B times some factor, say α, coming from the PACness property. The construction in Proposition B is explicit, as it uses nothing but the Euclidean algorithm.

Notation. Throughout this paper we denote by F an infinite field, by $F[X]$ and $F[X,Y]$ the polynomial rings over F in one and two variables, respectively, and by $\tilde{F}$ a fixed algebraic closure of F. As mentioned earlier $\mathcal{N}(F)$ denotes the set of all positive integers such that F has a separable extension of degree n. If we have a Galois extension, say K/F, then $\mathrm{Gal}(K/F)$ denotes its Galois group. The absolute Galois group of F is denoted by $\mathrm{Gal}(F)$, i.e., $\mathrm{Gal}(F) = \mathrm{Aut}(\tilde{F}/F)$. For a polynomial $a \in F[X]$ we write a' for its derivative. Finally, we abbreviate and say "for large n" instead of "$(\exists n_0 \in \mathbb{N})(\forall n > n_0)$".

1. Field crossing argument

Let K be a finitely generated regular extension of a field M. Suppose we have finite Galois extensions E/K and N/M, E regular over K, together with an embedding $\gamma\colon A \to G$, where $A = \mathrm{Gal}(N/M)$ and $G = \mathrm{Gal}(E/K)$. Identify $\mathrm{Gal}(EN/K)$ with $G \times A$ and let $\Delta = \{(\gamma(\sigma), \sigma) \in \mathrm{Gal}(EN/K) \mid \sigma \in A\}$.

The famous field crossing argument uses γ to "twist" E/K to D/K, where D is the fixed field of Δ in EN. Let ψ be an unramified M-place of D of degree 1 over K. Extend it to an N-place of $DN = NE$. Its restriction to E is an unramified M-place φ of E over K, with decomposition group $\gamma(A)$ and residue field N [FJ05, proof of Lemma 24.1.1]. Moreover, the canonical homomorphism $\varphi^*\colon A \to G$ defined by φ is exactly γ [FHJ84, Remark on page 9].

Next assume that N and E are the Galois closures of some separable extensions N'/M and E'/K, respectively, of degree n. Let $A' = \mathrm{Gal}(N/N')$ and $G' = \mathrm{Gal}(E/E')$ be their respective Galois groups and let $\Sigma = A/A'$ and $\Theta = G/G'$ be the corresponding sets of left cosets. Then $|\Sigma| = |\Theta| = n$, and A and G act naturally (by left multiplication) on Σ and Θ, respectively. A key observation is that if the above embedding γ respects this extra structure (i.e., there exists an injection, and hence a bijection, $\gamma^*\colon \Sigma \to \Theta$ such that $\gamma(a)\gamma^*(\sigma) = \gamma^*(a\sigma)$, for all $a \in A$, $\sigma \in \Sigma$, or, in other words, $\gamma\colon (A, \Sigma) \to (G, \Theta)$ is an embedding of permutation groups), then a stronger conclusion holds:

Lemma 1.1. *In the notation and under the assumptions above, any M-place φ of E for which $\varphi^* = \gamma$ restricts to an M-place φ' of degree n of E', unramified over K with residue field N'.*

Proof. Viewing A' as an element in Σ we have $\gamma^*(A') = gG'$ for some $g \in G$. Without loss of generality we may assume that $g = 1$, that is, $\gamma^*(A') = G'$. (Otherwise, we replace (γ, γ^*) with (γ', γ'^*), where $\gamma'(a) = g^{-1}\gamma(a)g$ and $\gamma'^*(\sigma) = g^{-1}\gamma^*(\sigma)$, $a \in A$ and $\sigma \in A/A'$.) As A' is the stabilizer of itself (in A) and G' is the stabilizer of G' (in G), we have $\gamma(A') = G' \cap \gamma(A)$. Let E'' be the decomposition field of ψ, i.e., the fixed field of $\gamma(A)$. Then $\mathrm{Gal}(E/E'E'') = G' \cap \gamma(A) = \gamma(A')$. Therefore the residue field of $E'E''$ under φ is N', and hence, so is the residue field of E'. In particular, the degree of $\varphi' = \varphi|_{E'}$ is $[N' : M] = n$. □

In what follows we shall apply the previous lemma to get a weak form of Hilbert's Irreducibility Theorem for PAC fields and, more generally, for fields which have a PAC extension.

A polynomial $f(X, Y) \in F[X, Y]$ is called **absolutely irreducible** if $f(X, Y)$ is irreducible over $\tilde{F}$. If in addition the Galois groups of $f(X, Y)$ over $F(Y)$ and over $\tilde{F}(Y)$ are equal, then $f(X, Y)$ is said to be **X-stable** over F. Thus, a polynomial $f(X, Y)$ is X-stable if and only if it is irreducible and its splitting field over $F(Y)$ is regular over F [FJ05, Remark 16.2.2].

Examples.
i.) Every absolutely irreducible polynomial $f(X, Y)$ which is Galois over $F(Y)$ is X-stable over F.
ii.) Every polynomial $f(X, Y)$ of degree n in X with symmetric Galois group S_n over $\tilde{F}(Y)$ is X-stable.
iii.) (Jarden) If an absolutely irreducible polynomial $f(X, Y)$ has a simple Galois group G over $F(Y)$, then f is X-stable over F (since the Galois group of $f(X, Y)$ over $\tilde{F}(Y)$ is a nontrivial normal subgroup of G).

iv.) [MM99] contains many explicit stable polynomials over $\mathbb{Q}$ (and hence over any field of characteristic zero); e.g., $f(X,Y) = X^n - Y(nX - n + 1)$ is X-stable with symmetric Galois group over $\mathbb{Q}(Y)$ [MM99, Theorem 9.4].

A field extension M/F is said to be a **PAC extension** if for every nonempty variety V of dimension r defined over M and for every dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over M there exists an M-point $a \in V(M)$ such that $\varphi(a) \in F^r$ [JR94]. PAC extensions generalize PAC fields since F is a PAC field if and only if F/F is a PAC extension. (Note that an extension M/F such that M is a PAC field, need not be a PAC extension; see Section 3.2 for details.) The property of a PAC extension can be reformulated in terms of places: M/F is a PAC extension if and only if for every separable finite extension $D/M(Y_1,\dots,Y_r)$ with D regular over M, there exist infinitely many M-places φ of D/M of degree 1 such that $\varphi(Y_i) \in F$, $i = 1,\dots,r$.

The following proposition establishes a weak form of Hilbert's Irreducibility Theorem for stable polynomials over a field which has a PAC extension.

Proposition 1.2. *Let M/F be a PAC extension, let $f(X,Y) \in M[X,Y]$ be an X-stable polynomial over M of degree n in X, and let N'/M be a separable extension of degree n with Galois closure N. Consider* $\mathrm{Gal}(N/M)$ *and* $\mathrm{Gal}(f(X,Y),M(Y))$ *as permutation groups of degree n via the action on the cosets of* $\mathrm{Gal}(N/N')$ *in* $\mathrm{Gal}(N/M)$ *and the action on the roots of $f(X,Y)$ over $M(Y)$, respectively. If there exists an embedding of permutation groups $\gamma\colon \mathrm{Gal}(N/M) \to \mathrm{Gal}(f(X,Y),M(Y))$, then there exist infinitely many $\alpha \in F$ for which $f(X,\alpha)$ is irreducible over M. Moreover, N' is generated by a root of $f(X,\alpha)$ over M.*

Remark 1.3. The assumption on γ is necessary. Indeed, $\mathrm{Gal}(N/M)$ is isomorphic as a permutation group to $\mathrm{Gal}(f(X,\alpha),M)$ which is a subgroup of $\mathrm{Gal}(f(X,Y),M(Y))$ (for all but a finite number of α's).

Proof. Let $K = M(Y)$, let E be the splitting field of $f(X,Y)$ over $M(Y)$, and let $E' = K(x)$, where $x \in E$ is a root of $f(X,Y)$. Then E is the Galois closure of E'/K and $n = [E' : K]$. The field crossing argument gives a field extension D/K, regular over M, with the property that any M-place ψ of degree 1 of D, unramified over K, yields an M-place φ of E for which $\varphi^* = \gamma$. Now by Lemma 1.1 such φ restricts to an M-place φ' of degree n of E', unramified over K over the same place of K with residue field N'. As M/F is PAC, there exist infinitely many M-places φ of D of degree 1 unramified over K such that $\alpha = \varphi(Y) \in F$. Then the corresponding place φ' of E' has residue field N'. But the residue field of E' is generated by a root of $f(X,\alpha)$, so $f(X,\alpha)$ is irreducible. □

The last result of this section deals with the special case where the Galois group of the stable polynomial is the symmetric group. In this case the condition on γ is redundant.

Corollary 1.4. *Let M/F be a PAC extension, let $f(X,Y) \in M[X,Y]$ be a polynomial of degree n in X, and let N/M be a separable extension of degree n. Assume that the Galois group of $f(X,Y)$ over $\tilde{M}(Y)$ is S_n. Then there exist infinitely many $\alpha \in F$ for which $f(X,\alpha)$ is irreducible over M and N is generated by a root of $f(X,\alpha)$ over M.*

2. Polynomials over infinite fields

2.1. **Technical background and basic tools.** The following result is a special case of Gauss' Lemma.

Lemma 2.1. *A polynomial $f(X,Y) = a(X) + b(X)Y \in F[X,Y]$ is irreducible if and only if $a(X)$ and $b(X)$ are relatively prime.*

Lemma 2.2. *Let $a, b, c \in F[X]$ such that $\gcd(a,b) = 1$ and $c \neq 0$. Then there exists a finite subset $S \subseteq F$ such that for each $\alpha \in F \smallsetminus S$ the polynomials $a + \alpha b$ and c are relatively prime. Moreover, if $b' \neq 0$, we may choose S such that $a + \alpha b$ is also separable.*

Proof. Let $S = \{-\frac{a(\gamma)}{b(\gamma)} \mid \gamma \in \tilde{F}, b(\gamma) \neq 0 \text{ and } c(\gamma) = 0\} \cap F$. Then $a + \alpha b$ and c have no common zero in $\tilde{F}$, for any $\alpha \notin S$. Hence these polynomials are relatively prime. Next let $d(Y) \in F[Y]$ be the discriminant of $a(X) + Yb(X)$ over $F(Y)$; then $b'(X) \neq 0$ implies that $d(Y) \neq 0$. In this case add all the roots of $d(Y)$ to S. □

Lemma 2.3. *Let $a, b, p_1, p_2 \in F[X]$ be pairwise relatively prime polynomials and let $\alpha_1, \alpha_2 \in F$ be distinct nonzero elements. Then for any $n > \deg p_1 + \deg p_2$ there exists $c \in F[X]$ of degree n and separable $h_1, h_2 \in F[X]$ such that $a = p_i h_i + bc\alpha_i$ and $\gcd(h_i, ap_i) = 1$ for $i = 1, 2$.*

Proof. Write $b_i = b\alpha_i$. Since $\gcd(p_i, b_i p_{3-i}) = 1$ for $i = 1, 2$, we have

$$a = p_i h_{i,0} + b_i p_{3-i} c_i \qquad i = 1, 2, \tag{1}$$

with $\deg c_i < \deg p_i$. For $\bar{c} = p_1 c_2 + p_2 c_1$ and $h_{i,1} = h_{i,0} - b_i c_{3-i}$, we have

$$a = p_i h_{i,1} + b_i \bar{c} \qquad i = 1, 2. \tag{2}$$

Here $h_{i,1}$ is relatively prime to b_i, since a and p_i are relatively prime. Taking (1) with $i = 2$ and (2) with $i = 1$ modulo p_2, we get

$$p_1 h_{1,1} \equiv a - b_1 \bar{c} \equiv a - b_1 p_1 c_2 \equiv b_2 p_1 c_2 - b_1 c_2 p_1 \equiv b p_1 c_2 (\alpha_2 - \alpha_1) \pmod{p_2}.$$

Therefore $h_{1,1}$ is relatively prime to p_2, since bp_1c_2 is relatively prime (by (1) with $i = 2$). Similarly, $h_{2,1}$ is relatively prime to p_1.

Take $c = \bar{c} + p_1 p_2 s$ for some $s \in F[X]$. Then, for $h_i = h_{i,1} - b_i p_{3-i} s$, we have

$$a = p_i h_i + b_i c \qquad i = 1, 2.$$

To conclude the proof it suffices to find $s \in F[X]$ such that h_1 and h_2 are separable, $\gcd(h_i, ap_i) = 1$, and $\deg c = n$. Choose $s \in F[X]$ for which $\deg s = n - (\deg p_1 + \deg p_2) \geq 1$, $(bp_i s)' \neq 0$, and $\gcd(s, h_{i,1}) = 1$ for $i = 1, 2$ (e.g., $s(X) = (X - \beta)^{n-1}(X - \gamma)$, where $\beta, \gamma \in F$ are not roots of $h_{1,1} h_{2,1} b p_1 p_2$).

By Lemma 2.2 with $h_{i,1}$, $bp_{3-i}s$, ap_i (for $i = 1, 2$) we get a finite set $S \subseteq F$ such that for each $\alpha \in F \smallsetminus S$ the polynomial $h_{i,1} - \alpha b p_{3-i} s$ is separable and relatively prime to ap_i. Replace s with αs, for some $\alpha \neq 0$ for which $\alpha_i \alpha \in F \smallsetminus S$, if necessary, to assume that $\alpha_1, \alpha_2 \in F \smallsetminus S$. This s has all the required properties. □

The next lemma gives a criterion, which we shall use to prove Proposition B, for a transitive group to be primitive and, further, to be the symmetric group (cf. [Ser92, Lemma 4.4.3]).

Lemma 2.4. *Let $A \leq S_n$ be a transitive group and let e be a positive integer in the segment $\frac{n}{2} < e < n$ such that $\gcd(e, n) = 1$. Then, if A contains an e-cycle, it is primitive. Moreover, if A also contains a transposition, then $A = S_n$.*

Proof. Let $\Delta \neq \{1,\dots,n\}$ be a block of A. We have $|\Delta| \leq \frac{n}{2}$, since $|\Delta| \mid n$. For the first assertion, it suffices to show that $|\Delta| = 1$, and since $\gcd(e,n) = 1$, it even suffices to prove that $|\Delta| \mid e$. Without loss of generality assume that $\sigma = (1\ 2\ \cdots\ e) \in A$ and $1 \in \Delta$. Then $\{1,\dots,e\} \not\subseteq \Delta$, since $e > \frac{n}{2} \geq |\Delta|$. Hence $\Delta \neq \sigma\Delta$, which implies that $\Delta \cap \sigma\Delta = \emptyset$. As $\sigma(x) = x$ for any $n \geq x > e$, we have $\Delta \subseteq \{1,\dots,e\}$. Consequently, Δ is a block of $\langle\sigma\rangle$, so $|\Delta| \mid e$.

The second assertion follows since a primitive group containing a transposition is the symmetric group [DM96, Theorem 3.3A]. □

The following number-theoretic lemma will be needed later.

Lemma 2.5. *For any prime p and positive integers n, m satisfying $n \geq 2m + \log n(1 + o(1))$, there exists an integer e in the segment $\frac{n}{2} < e < n - m$ such that $\gcd(e, np) = 1$.*

Proof. Let e be

$$\begin{array}{ll} \frac{n}{2} + 2, & \text{if } n \text{ is even but not divisible by 4,} \\ \frac{n}{2} + 1, & \text{if } n \text{ is divisible by 4, or} \\ \frac{n+1}{2}, & \text{if } n \text{ is odd.} \end{array}$$

Then e is the first integer greater than $\frac{n}{2}$ for which $\gcd(e,n) = 1$. If $p \nmid e$, we are done (and we only need $n > 2m + 4$). Next assume that $p \mid e$ (and hence $p \nmid n$). First, if n is even but not divisible by 4, then the next candidate $e' = e + 2$ works, since $\gcd(e', n) = 1$ and $p \nmid e'$. (Otherwise, p divides $e' - e = 2$; hence e is even, a contradiction.) Next, if n is divisible by 4, then the first relatively prime to n integer greater than e is $e' = \frac{n}{2} + q$, where q is the smallest prime not dividing n. Had $p \mid e'$, we would have $p \mid (e' - e) = q - 1$. In particular, $p < q$, and hence $p \mid n$ by minimality of q, a contradiction. Finally, if n is odd, the same argument will show that $e' = \frac{n+q}{2}$ is relatively prime to np, where now q is the smallest odd prime not dividing n (if $p = 2$, we have to take $q \equiv n \pmod 4$).

It remains to evaluate q which is a standard exercise in number theory: Let $\omega(n)$ be the number of distinct prime divisors of n. Then q is no more than the $\omega(n)+2$ prime number. Since the k-th prime equals $k \log k(1 + o(1))$ and

$$\omega(n) \leq \frac{\log n}{\log\log n}(1 + o(1))$$

[MV07, Theorem 2.10], we have

$$q \leq \omega(n)\log(\omega(n))(1 + o(1)) = \log n(1 + o(1)).$$

Note that for $n = 4\prod_{2<l<q} l$ (i.e., 4 times the product of all the odd prime numbers less than q) the inequality is in fact equality. Thus the estimation $n > 2m + \log(n)(1 + o(1))$ is the best possible. □

The following result is very well known; however, for the sake of completeness, we give a proof.

Proposition 2.6. *Let F be an algebraically closed field of characteristic $l \geq 0$. Let E/K be a separable extension of degree n of algebraic function fields of one variable over F. Assume that a prime divisor $\mathfrak{p}$ on K decomposes as*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

on E. If $l > 0$, assume further that $\gcd(e_i, l) = 1$, for $i = 1, \dots, r$. Then the Galois group of the Galois closure of E/K (as a subgroup of S_n) contains an element of cyclic type $(e_1, \dots, e_r)$. Moreover, the result holds even if $l = e_r = 2$ (we still assume that $\gcd(e_i, 2) = 1$ for $i = 1, \dots, r-1$).

Proof. The completion $\hat{K}$ of K at $\mathfrak{p}$ is a field of Laurent series over F [Ser79, Theorem 2], say $\hat{K} = F((Y))$. Let x be a primitive element of E/K, integral at $\mathfrak{p}$, and let f be its irreducible polynomial over K. Then f factors over $F((Y))$ into a product of separable irreducible polynomials $f = f_1 \cdots f_r$ such that $\deg f_i = e_i$ for each $i = 1, \dots, r$ [Ser79, II§3].

If either $l = 0$, or $l > 0$ and $\gcd(e_i, l) = 1$, then $F((Y))$ has a unique extension of degree e_i, namely $F((Y^{1/e_i}))$ [Che51, IV§6]. We thus get that the splitting field of f over $F((Y))$ is $F((Y^{1/e}))$, where $e = \operatorname{lcm}(e_1, \dots, e_r)$, unless $l = e_r = 2$, and then the splitting field of f is the compositum of $F((Y^{1/e'}))$ with an extension of degree 2, where $e' = \operatorname{lcm}(e_1, \dots, e_{r-1})$. In both cases the Galois group of f over $F((Y))$ is cyclic of order e. Its generator σ acts cyclicly on the roots of each of the f_i's. Consequently, the cyclic type of σ is $(e_1, \dots, e_r)$, as required. □

Lemma 2.7. *Let F be a field, let $f(X, Y) = a(X) + b(X)Y = \sum_{i=0}^{n} (a_i + b_i Y) X^i \in F[X, Y]$ be irreducible and separable over $F(Y)$, let $E = F(Y)[X]/(f(X, Y))$, and let $\alpha \in F$ such that $a_n + b_n \alpha \neq 0$. Then the decomposition of $\mathfrak{p} = (Y - \alpha)$ on E corresponds to the factorization of $f(X, \alpha)$ over F.*

Proof. Let $R = F[Y, (a_n + b_n Y)^{-1}]$. Then $S = R[X]/(f(X, Y)) \subseteq E$ is integral over R. Moreover, as $Y = -a(X)b^{-1}(X)$ in E, we have that S is a localization of the polynomial ring $F[X]$ at $-b(X)a^{-1}(X)$ and at $a_n - b_n a(X)b^{-1}(X)$. Hence S is integrally closed [AM69, Proposition 5.12], and the assertion follows from [Ser79, I§4 Proposition 10]. □

2.2. **Proof of Proposition B.** Let $f(X, Y) = a(X) + b(X)Y \in F[X, Y]$ be an irreducible polynomial. For a large integer n we need to find $c(X) \in F[X]$ such that $f(X, c(X)Y) = a(X) + b(X)c(X)Y$ is irreducible of degree n and the Galois group of $f(X, c(X)Y)$ over $\tilde{F}(Y)$ is S_n.

Lemma 2.5 with $m = \max\{\deg a(X), 2 + \deg b(X)\}$ and $p = \operatorname{char}(F)$ gives (for $n > 2m + \log n(1 + o(1))$) a positive integer e such that

$$n - m > e > \frac{n}{2} \text{ (in particular, } e > m), \tag{3}$$

$$\gcd(e, np) = 1 \text{ (or } \gcd(e, n) = 1, \text{ if } p = 0). \tag{4}$$

Let $\alpha_1 \neq \alpha_2$ and $\gamma_1 \neq \gamma_2$ be elements of F such that α_i is nonzero and γ_i is not a root of $a(X)b(X)$, $i = 1, 2$. In Lemma 2.3 we constructed (for a, b, $p_1 = (X - \gamma_1)^e$, $p_2 = (X - \gamma_2)^2$, α_1, and α_2) a polynomial $c(X) \in F[X]$ of degree $\deg c = n - \deg b(X)$ which is relatively prime to $a(X)$ such that

$$f(X, c(X)\alpha_1) = a(X) + \alpha_1 b(X)c(X) = (X - \gamma_1)^e h_1(X), \tag{5}$$

$$f(X, c(X)\alpha_2) = a(X) + \alpha_2 b(X)c(X) = (X - \gamma_2)^2 h_2(X). \tag{6}$$

Here $h_1(X), h_2(X) \in F[X]$ are separable polynomials which are relatively prime to $(X - \gamma_1)a(X)$, $(X - \gamma_2)a(X)$, respectively. In particular $\gcd(a, c) = 1$, and hence $f(X, c(X)Y)$ is irreducible (Lemma 2.1). By (3), $\deg_X f(X, c(X)Y) = \deg b(X) + \deg c(X) = n$. Keeping (4), (5), and (6) in mind, Lemma 2.7 and Proposition 2.6

with $\mathfrak{p} = (Y - \alpha_1)$ give us an e-cycle in $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y))$, and with $\mathfrak{p} = (Y - \alpha_2)$ give a transposition. Thus $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y)) = S_n$ (Lemma 2.4). □

3. Dirichlet's theorems

3.1. **Proof of Theorem A.** We actually prove a stronger statement.

Theorem 3.1. *Let M/F be a PAC extension. Then Dirichlet's theorem holds for $F[X]$ and $\mathcal{N}(M)$.*

Proof. The field F is an infinite field, since M/F is a PAC extension ([JR94, Remark 1.2]) and $f(X, Y) = a(X) + b(X)Y$ is irreducible (Lemma 2.1). Proposition B gives a polynomial $c(X) \in F[X]$ for which $f(X, c(X)Y)$ is an irreducible polynomial of degree n in X and $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y)) = S_n$. Now the assertion follows from Corollary 1.4. □

Remark 3.2. The above proves a stronger statement than stated; namely, for large n there exists $c(X) \in F[X]$ such that every separable extension N/M of degree n is generated by a root of $f(X, c(X)\alpha)$, for infinitely many $\alpha \in F$.

In Theorem A and Proposition B we have considered only linear polynomials. We pose the natural generalization to general polynomials (cf. [FJ05, Lemma 10.3.1]).

Problem 3.3. Let $f(X, Y) \in F[X, Y]$ be an absolutely irreducible polynomial. For large n, is there a polynomial $c(X) \in F[X]$ for which $f(X, c(X)Y)$ is an X-stable polynomial of degree n? For which $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y)) \cong S_n$?

3.2. **PAC extensions.** Theorem A makes it interesting to calculate $\mathcal{N}(F)$ for a PAC field F. Its generalization, Theorem 3.1, raises the following questions. When does a given field have a PAC extension M? What positive integers can occur as degrees of separable extensions of such M's?

Examples (PAC fields which have separable extensions of arbitrary degrees)**.** Let M be a PAC field. If M is Hilbertian or more generally RG-Hilbertian (i.e., M has the irreducible specialization property for regular Galois extensions), then every finite group occurs as a Galois group over M [FV92]. In particular, $\mathcal{N}(M) = \mathbb{Z}^+$ (where $\mathbb{Z}^+$ denotes the set of all positive integers).

In general, $n \in \mathcal{N}(M)$ if and only if some Galois group over M has a subgroup of index n. For example, if a cyclic group of order n (or alternatively the symmetric group of degree n) occurs as a Galois group over M, then $n \in \mathcal{N}(M)$. In particular, if $\mathrm{Gal}(M)$ is a finitely generated free profinite group (and hence M is "far" from being Hilbertian), then $\mathcal{N}(M) = \mathbb{Z}^+$.

The succeeding result asserts that for a PAC field M, the set $\mathcal{N}(M)$ is finite only if $M = M_s$, where M_s is a fixed separable closure of M.

Lemma 3.4. *Let M be a PAC field and assume $M \neq M_s$. Then $\mathcal{N}(M)$ is infinite.*

Proof. Artin-Schreier Theorem implies that if $[M_s : M]$ is finite, then $[M_s : M] = 2$ and M is real closed. However a PAC field cannot be real, since the curve defined by $X^2 + Y^2 + 1$ has an M-rational point. □

In contrast to PAC fields which have been studied since the late 1960s, PAC extensions first appeared in 1994 and have not yet been well understood. In what follows we describe all the known PAC extensions. Also we give some new explicit interesting examples of PAC extensions and deduce for them corollaries to Theorem 3.1.

A profinite group is compact; hence it is equipped with a normalized Haar measure (see [FJ05, Chapter 18]). In particular, if K is a field and e is a positive integer, then $\mathrm{Gal}(K)^e$ is equipped with a normalized Haar measure. Let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ be an e-tuple of Galois automorphisms. Then $\langle \boldsymbol{\sigma} \rangle$ denotes the subgroup generated by $\sigma_1, \ldots, \sigma_e$, and $K_s(\boldsymbol{\sigma})$ denotes the fixed field of $\langle \boldsymbol{\sigma} \rangle$ in a fixed separable closure K_s of K. The phrase "for almost all" means "for all but a set of measure zero".

Clearly (and uninteresting for us), a separably closed field is a PAC extension of any infinite subfield of the field itself. In [JR94], Razon and Jarden prove the following:

(1) Let K be a countable Hilbertian field and let $e \geq 1$. Then $K_s(\boldsymbol{\sigma})/K$ is PAC (as an extension) for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.
(2) Let L/K be a PAC extension and let F/K be an algebraic extension. Then FL/F is a PAC extension.

So far these are all the known PAC extensions. We shall use these properties to construct some explicit PAC extensions M/F (for non-Hilbertian F). Before doing that, we emphasize that there are restrictions on a field extension to be PAC; e.g., it is known that no Galois extension of a finitely generated field (except for the separable closure) is PAC [BSJ]. In particular, since there is a Galois extension M of $\mathbb{Q}$ such that M is a PAC field [FJ05, Theorem 18.10.2], we get that for an extension M/F to be PAC (as an extension) it does not suffice that M is PAC (as a field).

Given a countably Hilbertian field K, (1) and (2) yield abundance of separable extensions F/K such that Dirichlet's theorem holds for $F[X]$ (and some infinite set $\mathcal{N}$ which we omit from now on):

Corollary 3.5. *Let K be a countable Hilbertian field and let F/K be a separable algebraic extension. Assume that the set $\{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid FK_s(\boldsymbol{\sigma}) \neq K_s\}$ has a positive measure for some positive integer e. Then, Dirichlet's theorem holds for $F[X]$.*

Proof. By the assumption, (1), and (2) we get that there is $\boldsymbol{\sigma}$ (actually a positive measure set of $\boldsymbol{\sigma}$'s) for which the extension $FK_s(\boldsymbol{\sigma})/F$ is PAC and $FK_s(\boldsymbol{\sigma}) \neq K_s$. Therefore Lemma 3.4 and Theorem 3.1 imply the assertion. □

For almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the group $\langle \boldsymbol{\sigma} \rangle$ is isomorphic to the free profinite group on e generators [FJ05, Theorem 18.5.6]. Also, by Galois correspondence, if F/K is Galois and $FK_s(\boldsymbol{\sigma}) = K_s$, then $\langle \boldsymbol{\sigma} \rangle$ is isomorphic to a subgroup of $\mathrm{Gal}(F/K)$. Therefore we have

Corollary 3.6. *Let K be a countable Hilbertian field, let $e \geq 1$, let F/K be a Galois extension, and assume that $\mathrm{Gal}(F/K)$ does not have a free subgroup of rank e. Then Dirichlet's theorem holds for $F[X]$.*

In particular, since a pro-solvable group cannot have a noncyclic free profinite group as a subgroup, we get

Corollary 3.7. *Let F be a pro-solvable extension of a countable Hilbertian field K. Then Dirichlet's theorem holds for $F[X]$.*

In light of the above corollaries we suggest two open problems:

Problem 3.8. Let K be a Hilbertian field. Classify all separable algebraic extensions F of K such that the measure of $\{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid FK_s(\boldsymbol{\sigma}) \neq K_s\}$ is positive for some positive integer e.

Problem 3.9. Let K be a Hilbertian field. Classify extensions F of K which have a PAC extension which is not separably closed.

Remark 3.10. There are fields which do not have any separable extension which is PAC, other than the separable closure, e.g., $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$. In general, if a field is henselian, then it has no separable extension which is a PAC field other than the separable closure [FJ05, Corollary 11.5.5]. Note that over $\mathbb{C}$ or over $\mathbb{R}$ Dirichlet's theorem obviously does not hold, since every polynomial of degree greater than two is reducible.

Acknowledgments

I would like to thank Moshe Jarden for raising the question that initiated this work and for many helpful suggestions and Peter Müller for his help in the second chapter. I would also like to thank Dan Haran, Joseph Bernstein, and Sasha Sodin. I gratefully thank the anonymous referee for valuable comments which improved this work. Special thanks are directed to my friends Dubi Kelmer and Ilya Surding and to my wife, Hamutal, for carefully reading the manuscript.

This work was partially carried out while the author was at the Max-Planck-Institut für Mathematik in Bonn. It is part of the author's Ph.D. thesis done at Tel Aviv University, supervised by Professor Dan Haran.

References

[AM69] Michael F. Atiyah and Ian. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802 (39:4129)

[BSJ] Lior Bary-Soroker and Moshe Jarden, *PAC fields over finitely generated fields*, to appear in Math. Z.

[Che51] Claude Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, no. 6, American Mathematical Society, New York, 1951. MR0042164 (13:64a)

[DM96] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR1409812 (98m:20003)

[FHJ84] Michael D. Fried, Dan Haran, and Moshe Jarden, *Galois stratification over Frobenius fields*, Adv. in Math. **51** (1984), no. 1, 1–35. MR728998 (86c:12007)

[FJ05] Michael D. Fried and Moshe Jarden, *Field arithmetic*, second ed., revised and enlarged by Moshe Jarden, Ergebnisse der Mathematik (3) **11**, Springer-Verlag, Heidelberg, 2005. MR2102046 (2005k:12003)

[FV92] Michael D. Fried and Helmut Völklein, *The embedding problem over a Hilbertian PAC-field*, Ann. of Math. (2) **135** (1992), no. 3, 469–481. MR1166641 (93f:12005)

[JR94] Moshe Jarden and Aharon Razon, *Pseudo algebraically closed fields over rings*, Israel J. Math. **86** (1994), no. 1-3, 25–59. MR1276130 (95c:12006)

[Kor19] Heinrich Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Mathematische Zeitschrift **5** (1919), 100–111.

[MM99] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. MR1711577 (2000k:12004)

[MV07] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, Cambridge, 2007. MR2378655

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002. MR1876657 (2003d:11171)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, New York, 1979. MR554237 (82e:12016)

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, **1**, Jones and Bartlett Publishers, Boston, 1992. MR1162313 (94d:12006)

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978 Israel

Current address: Department of Mathematics, The Hebrew University, Givat Ram, Jerusalem 91904, Israel

E-mail address: barylior@post.tau.ac.il