

ROOT QUANTUM NUMBERS OVER HILBERTIAN FIELDS

ELIZABETH TOWNSEND

ABSTRACT. Let $f(x)$ be an irreducible polynomial over a field K , and let α be a root of $f(x)$. The root quantum number is defined to be the number of roots of $f(x)$ in $K(\alpha)$, and it is known that the root quantum number must divide the degree of the polynomial. The main goal of this paper will be to prove that if K is a Hilbertian field, then for every n and for every d dividing n , there exists an irreducible polynomial over K of degree n having root quantum number d with the sole exception $n = 2$ and $d = 1$. The proof is completed first over \mathbb{Q} and then extended to all Hilbertian fields. The paper also discusses the idea of a root quantum number from a variety of different group theoretic perspectives.

1. INTRODUCTION

A. Perlis introduced the idea of a root quantum number of a polynomial. We begin by recalling some important facts that are already known [1].

Definition 1.1. Let $f(x)$ be an irreducible polynomial over K of degree n , and let α be a root of $f(x)$. The *root quantum number*, denoted $r_K(f)$, is the number of roots of $f(x)$ that lie in $K(\alpha)$.

We may also let $s_K(f)$ denote the number of subfields $L \subseteq \overline{K}$ that are K -isomorphic to $K(\alpha)$, where \overline{K} is the algebraic closure of K .

Theorem 1.2 (A. Perlis). *Let $f(x) \in K[x]$ be an irreducible polynomial, and let α be a root of $f(x)$. Then $r_K(f)$ and $s_K(f)$ are independent of the choice of α , and $r_K(f) \cdot s_K(f)$ is the cardinality of the set of roots of $f(x)$. In particular, $r_K(f)$ divides the degree of $f(x)$.*

Note that the cardinality of the set of roots of $f(x)$ is known as the *seperable degree* of $f(x)$, which must divide the degree of the polynomial. For a proof of this theorem and further discussion of root quantum numbers of polynomials, see Perlis [1].

A natural question regarding the classification of root quantum numbers now arises: Which triples (K, n, d) occur that indicate the existence of an

Date: July 26, 2002.

The LSU Research Experience for Undergraduates Program is supported by a National Science Foundation grant, DMS-0097530 and a Louisiana Board of Regents Enhancement grant, LEQSF (2002-2004)-ENH-TR-17.

irreducible polynomial $f(x)$ of degree n over K having root quantum number d ? In Section 4, this problem is completely solved for the case when $K = \mathbb{Q}$, the field of rational numbers. \mathbb{Q} is the primary example of a class of fields called *Hilbertian fields*, and the main result of this paper is the classification of triples where K is a Hilbertian field. Section 5 generalizes the results of Section 4 to arbitrary Hilbertian fields, but the section is logically independent of Section 4.

Main Theorem. *Let K be a Hilbertian field. For any $n \neq 2$ and for any d a divisor of n , there exists an irreducible polynomial $f(x) \in K[x]$ with degree n having root quantum number d .*

The hypothesis $n \neq 2$ is necessary: Suppose $f(x)$ is an irreducible polynomial of degree 2 over, say \mathbb{Q} . Thus $f(x)$ has precisely two roots, say α_1 and α_2 . If we factor $f(x)$ in $\mathbb{Q}(\alpha_1)$, we necessarily have that $f(x) = (x - \alpha_1)(x - \alpha_2)$. Hence, $\alpha_2 \in \mathbb{Q}(\alpha_1)$, and $r_{\mathbb{Q}}(f) = 2$.

The proof of the Main Theorem proceeds in two steps.

- (1) Interpret root quantum numbers group-theoretically and find groups with prescribed root quantum numbers.
- (2) Go from groups back to polynomials by realizing the groups from Step 1 as Galois groups over K . This is the step in which the property that K is Hilbertian is necessary.

2. ROOT QUANTUM NUMBERS OF GROUPS

Let $f(x)$ be an irreducible polynomial of degree n over a field K and let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be the roots of $f(x)$ in a fixed algebraic closure \bar{K} . We are interested in $r_K(f)$, the number of roots of $f(x)$ that lie in $K(\alpha_1)$. We have $K(\alpha_1)|K$, an extension of degree n , and $K(\alpha_1)$ is a subfield of $K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Let $G = \text{Gal}(K(\alpha_1, \alpha_2, \dots, \alpha_n)|K)$ and let $H = \text{Gal}(K(\alpha_1, \alpha_2, \dots, \alpha_n)|K(\alpha_1))$. The roots of $f(x)$ that lie in $K(\alpha_1)$ will be precisely the roots that are fixed by H . Therefore we may recognize H as the set of elements of G that fix $K(\alpha_1)$ pointwise; *i.e.*, H is the G -stabilizer of α_1 , or $H = \text{stab}_G(\alpha_1)$. This gives rise to the following alternate definition of a quantum root number of a polynomial: $r_K(f) = |\{\alpha_j : \text{stab}_G(\alpha_j) = H\}|$.

Now G acts transitively on the set of roots $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$. And H is a subgroup of G of index n . Thus there is a bijection between the set of α_i 's and the left cosets of H in G . That is, $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is G -isomorphic to the G -set G/H where G acts transitively by left multiplication. This motivates the following definition.

Definition 2.1. Let G be a group and H a subgroup. The root quantum number of G acting by left multiplication on G/H is $r(G, G/H) := |\{gH : \text{stab}_G(gH) = H\}|$.

Remark 2.2. When $G = \text{Gal}(K(\alpha_1, \alpha_2, \dots, \alpha_n)|K)$ and $H = \text{Gal}(K(\alpha_1, \alpha_2, \dots, \alpha_n)|K(\alpha_1))$ according to the notation of the first paragraph in this section, then $r(G, G/H) = r_K(f)$.

Remark 2.3. For an arbitrary group G and subgroup H , the root quantum number $r(G, G/H)$ is a group-theoretic concept. That is, the number does not refer to any field.

Even though $r(G, G/H)$ is independent of a field, we may associate the group G with a polynomial. In particular, if G arises as the Galois group of some extension over a field K , then we have the following important lemma.

Main Lemma. *Let $|G : H| = n$ and let $r(G, G/H) = d$. If $N|K$ is a field extension with $G = \text{Gal}(N|K)$, then there is an irreducible polynomial $f(x)$ of degree n in $K(x)$ with root quantum number d .*

Proof. Suppose $|G : H| = n$ and $r(G, G/H) = d$, and let $G = \text{Gal}(N|K)$. We shall construct $f(x)$ in the following manner. Let $L = N^H$ be the fixed field of H . Then $L = K(\alpha)$ for some α . Let $f(x)$ be the minimal polynomial of α over K . Then we have that the degree of $f(x) = |N^H : K| = |G : H| = n$. Let $S = \{\alpha_1, \dots, \alpha_n\}$ be the roots of $f(x)$ in N with, say, $\alpha_1 = \alpha$. Then G acts transitively on S , so we have that $S \approx G/\text{stab}_G(\alpha_1) = G/H$. Thus we see that $r_K(f) = r(G, G/H) = d$, as desired. \square

We have defined the root quantum number of a group acting transitively on a set of cosets. There are other useful methods of interpreting the root quantum number using group theory. We conclude this section with observations about root quantum numbers that are of interest, but will not be used later in the paper. We begin with a well-known lemma.

Lemma 2.4. *Let G act on S , and let $g \in G$ and $s_1, s_2 \in S$. If $gs_1 = s_2$, then $\text{stab}_G(s_1) = g^{-1}\text{stab}_G(s_2)g$.*

Proof. Let $g \in G$ and $s_1, s_2 \in S$, and let $gs_1 = s_2$. Let $\sigma \in \text{stab}_G(s_2)$, which happens if and only if $\sigma(s_2) = s_2$. Substituting for s_2 gives us that $\sigma(gs_1) = gs_1$, and acting by g^{-1} on both sides yields $g^{-1}\sigma g(s_1) = s_1$. This happens exactly when $g^{-1}\sigma g(s_1) \in \text{stab}_G(s_1)$, which occurs if and only if $\sigma \in g \text{stab}_G(s_1)g^{-1}$. \square

Proposition 2.5. $r(G, G/H) = |N_G(H) : H|$.

Proof. G acts transitively on G/H . Thus, for every g_iH there exists a $\gamma_i \in G$ such that $\gamma_i g_1 H = g_i H$. Let $H = \text{stab}_G(g_1 H)$. By Lemma 2.4, we then have that $H = \gamma_i^{-1} \text{stab}_G(g_i H) \gamma_i$ or equivalently that $\text{stab}_G(g_i H) = \gamma_i H \gamma_i^{-1}$. $r(G, G/H) = |\{gH : \text{stab}_G(gH) = H\}|$, so the number of γ_i for which $\gamma_i H \gamma_i^{-1} = H$ will also be the root quantum number. That is, may realize the root quantum number as the index of H in its normalizer in G , or $r(G, G/H) = |N_G(H) : H|$. \square

Note that this proposition combined with Remark 2.2 gives us directly that the root quantum number of a polynomial must divide its degree.

Lemma 2.6. *Let $\Delta = \{gH : \text{stab}_G(gH) = H\}$. Then $\Delta \cong N_G(H)/H$.*

Proof. First recall that $\text{stab}_G(gH) = H$ if and only if $g \in N_G(H)$. Hence, the identity map is an isomorphism from $N_G(H)/H$ to Δ . \square

Proposition 2.7. *For every $\gamma \in G$, either $\gamma(\Delta) = \Delta$ or $\gamma(\Delta) \cap \Delta = \emptyset$.*

Proof. Assume that $\gamma(\Delta) \cap \Delta \neq \emptyset$. Then there is a $g_0H \in \gamma(\Delta) \cap \Delta$, so $g_0H \in \gamma(\Delta)$ and $g_0H \in \Delta$. Thus we have that g_0H and $\gamma^{-1}g_0H \in \Delta$. Lemma 2.6 implies that g_0 and γ^{-1} are in $N_G(H)$, which means that $g_0(\gamma^{-1}g_0)^{-1} \in N_G(H)$. Thus we also see that $\gamma \in N_G(H)$. But for every $gH \in \Delta$, Lemma 2.6 says that $g \in N_G(H)$, so $\gamma g \in N_G(H)$ as well. Thus, $\gamma gH \in \Delta$, and we have that $\gamma(\Delta) = \Delta$. \square

Recall that a group acts *imprimitively* on a set S if there is a subset $\Omega \subseteq S$ such that $1 \not\leq |\Omega| \leq |S|$ with the following property: for every $g \in G$ either $g(\Omega) = \Omega$ or $g(\Omega) \cap \Omega = \emptyset$. Ω is called a *block* of imprimitivity. So when $\Delta = \{gH : \text{stab}_G(gH) = H\}$ has size $1 \leq |\Delta| \leq |G : H|$, then Δ is a block of imprimitivity. Recall by Lemma 2.6, however, that Δ is also a group, so it is a special kind of block of imprimitivity. Hence, except for the two extreme cases, in which $|\Delta| = 1$ or $|\Delta| = |G : H|$, the root quantum number is the size of a special kind of block of imprimitivity. We record this observation as:

Corollary 2.8. *When $1 \leq r(G, G/H) \leq |G : H|$, then G acts imprimitively on G/H with block size $r(G, G/H)$.*

3. CLASSIFICATION OF ROOT QUANTUM NUMBERS OVER \mathbb{Q}

In this section we shall prove the Main Theorem in the special case where $K = \mathbb{Q}$. In particular, we have the following theorem.

Theorem 3.1. *For any $n \neq 2$ and for any d a divisor of n , there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with degree n having root quantum number d .*

We shall prove Theorem 3.1 using the same two steps discussed in the introduction. First, fix an index n and let d be a divisor of n . We shall find pairs (G, H) such that $|G : H| = n$ and $r(G, G/H) = d$. It is important to recall Remark 2.3, which says that this first step is completely independent of the choice of a base field.

Lemma 3.2. *Let \mathfrak{S}_n be the symmetric group on n elements. Then $r(\mathfrak{S}_n, \mathfrak{S}_n/\mathfrak{S}_{n-1}) = 1$.*

Proof. First, it is obvious that \mathfrak{S}_n acts transitively on $\{1, 2, \dots, n\}$. Now, fix an element in this set, say n . The \mathfrak{S}_n -stabilizer of n is the set of all permutations that fix n but permute the elements $1, 2, \dots, n-1$. Thus, $H = \text{stab}_{\mathfrak{S}_n}(n) = \mathfrak{S}_{n-1}$. And $\mathfrak{S}_n/\mathfrak{S}_{n-1} = (1)$, so there is just one coset. Thus, $r(\mathfrak{S}_n, \mathfrak{S}_n/\mathfrak{S}_{n-1}) = 1$. \square

Lemma 3.3. *Let C_n be the cyclic group of order n . Then $r(C_n, C_n/\{1\}) = n$.*

Proof. This action may be recognized as C_n acting on itself by left multiplication, which is both a transitive and faithful action. Thus, $H = \text{stab}_{C_n}(a) = \{1\}$ for every $a \in C_n$. And the identity fixes every element of C_n , so we have that $r(C_n, C_n/\{1\}) = n$. \square

Now we shall develop the necessary tools to discuss the third type of group, the group that will yield root number d . Let $n = dt$, and let A and B be groups acting on sets Δ and Γ , respectively such that $|\Delta| = d$ and $|\Gamma| = t$. Define $A^\Gamma = \{f \mid f : \Gamma \rightarrow A\}$, which is a group under composition of functions. We may now define an action of B on A^Γ in the following way: for $f \in A^\Gamma, b \in B$, let ${}^b f : \Gamma \rightarrow A$ be such that ${}^b f(\gamma) = f(b\gamma)$. We now have the tools to introduce the following definition.

Definition 3.4. The *wreath product* is defined to be $A \wr B = \{(f, b) : f \in A^\Gamma, b \in B\}$ with the following operation: $(f_1, b_1)(f_2, b_2) = (f_1({}^{b_1}f_2), b_1 b_2)$.

It is easily verifiable that $(f, b)^{-1} = (F, b^{-1})$ where $F(\gamma) = (f({}^{b^{-1}}\gamma))^{-1}$, the inverse taken in the group A .

Remark 3.5. One might recognize the wreath product as the semidirect product of A^Γ and B . That is, $A \wr B = A^\Gamma \rtimes B$.

Let A act on itself by left multiplication and B act on itself by left multiplication. Then $A \wr B$ acts transitively on the set of cosets $(A \wr B)/H$, where $H = \text{stab}_G(f, b)$ for a fixed $(f, b) \in A \wr B$. In particular, if $n = dt$, we can let C_d and C_t be the cyclic groups of order d and t , respectively. Let e_d denote the identity of C_d and e_t the identity of C_t . Consider $C_d \wr C_t$. Let C_t act on itself by left multiplication, and let C_d act on itself by left multiplication.

Lemma 3.6. Let $G = C_d \wr C_t$ and let $H = \{(g, e_t) : g(\tau_0) = e_d\}$ for a fixed $\tau_0 \in C_t$. Then $r(G, G/H) = d$.

Proof. First note that $|H| = d^{t-1}$ since the function g is free to take any $\tau \in C_t$ different from τ_0 to any element in C_d . And $|G| = d^t t$, so H is a subgroup of index $dt = n$ in G . We wish to determine $|\{gH : \text{stab}_G(gH) = H\}|$. But H stabilizes $(f, \tau)H$ if and only if $(f, \tau)H(f, \tau)^{-1} = H$. Thus we wish to find out how many elements $(f, \tau) \in G$ are such that $(f, \tau)H(f, \tau)^{-1} = H$. That is, we must find conditions on (f, τ) such that $(f, \tau)(g, e_t)(f, \tau)^{-1} \in H$ for every $(g, e_t) \in H$. Hence we want $(f, \tau)(g, e_t)(F, \tau^{-1}) \in H$, where F is defined as above. Simplifying this expression yields $(f({}^\tau g)f^{-1}, e_t) \in H$. Thus we need only find out which functions $f({}^\tau g)f^{-1}$ send τ_0 to e_d . Applying the function to τ_0 yields $f(\tau_0)g(\tau\tau_0)f^{-1}(\tau_0)$. But these are all elements of C_d , an abelian group, so we may write $f(\tau_0)f^{-1}(\tau_0)g(\tau\tau_0) = g(\tau\tau_0)$. And $g(\tau\tau_0) = e_d$ precisely when $\tau = e_t$ since for every $\tau \neq e_t$ there is a g such that $g(\tau_0) = e_d$, but $g(\tau\tau_0) \neq e_d$. Thus we have that elements in cosets that are fixed by H are of the form (f, e_t) where f is an arbitrary function in $(C_d)^t$.

We have just determined the set of all elements in G representing cosets whose stabilizer is H . Now we must determine the number of cosets of

H represented by these elements. Now, $(f_1, e_t)H = (f_2, e_t)H$ if and only if $(f_1, e_t) = (f_2, e_t)(g, e_t)$ for some g such that $g(\tau_0) = e_d$. That is, we have that $f_1(\tau) = f_2(\tau)g(\tau)$ and consequently, $f_1(\tau_0) = f_2(\tau_0)$. There are d choices for the value of $f_1(\tau_0)$. Thus to find representatives of different cosets, we should have that $f_i(\tau_0) \neq f_j(\tau_0)$ for every $i \neq j$. There are d different choices for values of $f(\tau_0)$, so we see that there are exactly d cosets formed by these representative elements. Hence we have that $r(G, G/H) = d$. \square

We now have that symmetric groups, cyclic groups, and wreath products of cyclic groups yield root quantum numbers for every divisor d of a fixed index n . Now we proceed to Step 2, in which we must show that each of these three groups arise as Galois groups for some extension of \mathbb{Q} . There are a few well-known theorems that we must recall to prove this remaining fact.

It is classically known that the symmetric group arises as a Galois group over \mathbb{Q} for polynomials of any degree n . This fact is a result of the work of many mathematicians, one of whom is Van der Waerden. Van der Waerden's Theorem says that the Galois group for most polynomials over \mathbb{Q} is \mathfrak{S}_n .

Theorem 3.7. *Every abelian group is the Galois group for some extension over \mathbb{Q} .*

Proof. Consider any abelian group which is of the form $C_{q_1} \oplus C_{q_2} \oplus \cdots \oplus C_{q_t}$. Choose a prime $p_1 \equiv 1 \pmod{q_1}$. Then we have that $C_{p_1-1} \cong \text{Gal}(\mathbb{Q}(\omega_{p_1})|\mathbb{Q})$ where ω_{p_1} is a primitive p_1^{th} root of unity. Now q_1 divides $p_1 - 1$, and thus C_{q_1} is a subgroup of C_{p_1-1} . There is a corresponding subfield $\mathbb{Q}(\pi_1)$ such that $C_{q_1} \cong \text{Gal}(\mathbb{Q}(\pi_1)|\mathbb{Q})$. Now choose a prime $p_2 \equiv 1 \pmod{q_2}$ and $p_2 > p_1$. We can make this choice because of Dirichlet's Theorem. We will have that $C_{p_2-1} \cong \text{Gal}(\mathbb{Q}(\omega_{p_2})|\mathbb{Q})$ where ω_{p_2} is a primitive p_2^{th} root of unity. Then q_2 divides $p_2 - 1$, and thus C_{q_2} is a subgroup of C_{p_2-1} . There is a corresponding subfield $\mathbb{Q}(\pi_2)$ such that $C_{q_2} \cong \text{Gal}(\mathbb{Q}(\pi_2)|\mathbb{Q})$. But since the intersection of $\mathbb{Q}(\omega_{p_1})$ and $\mathbb{Q}(\omega_{p_2})$ is \mathbb{Q} , then we necessarily have that the intersection of $\mathbb{Q}(\pi_1)$ and $\mathbb{Q}(\pi_2)$ is \mathbb{Q} . Thus we have that $\text{Gal}(\mathbb{Q}(\pi_1, \pi_2)|\mathbb{Q}) \cong C_{q_1} \oplus C_{q_2}$. We may continue this construction, choosing $p_i > p_{i-1}$ and $p_i \equiv 1 \pmod{q_i}$, and we will eventually have that $\text{Gal}(\mathbb{Q}(\pi_1, \pi_2, \dots, \pi_t)|\mathbb{Q}) \cong C_{q_1} \oplus C_{q_2} \oplus \cdots \oplus C_{q_t}$. \square

This theorem immediately implies that C_n arises as a Galois group for some extension over \mathbb{Q} , and the construction in the proof actually tells us an extension for which C_n is the Galois group.

Theorem 3.8 (Shafarevich). *Every solvable group arises as the Galois group of some extension of \mathbb{Q} . [3]*

Note, of course, that a corollary to Theorem 3.8 is Theorem 3.7 since all abelian groups are solvable.

Thus we need only show that $C_d \wr C_t$ is a solvable group. That $C_d \wr C_t$ is solvable is an immediate consequence of the following well-known theorem.

Theorem 3.9. *Let G be a group and $N \triangleleft G$. If N and G/N are both solvable, then G is solvable.*

Recalling Remark 3.5, we may write $G = C_d \wr C_t = (C_d)^t \rtimes C_t$. Thus we have that $(C_d)^t \triangleleft G$ and $G/(C_d)^t \cong C_t$, a solvable group. And $(C_d)^t$ is solvable as well, giving us that G is also solvable. Hence Theorem 3.9 tells us that $C_d \wr C_t$ arises as the Galois group for some extension of \mathbb{Q} .

Proof of Theorem 3.1. Fix $n \neq 2$. Then for every d dividing n , Lemmas 3.2, 3.3, and 3.6 give pairs (G, H) where $|G : H| = n$ and $r(G, G/H) = d$. In each pair, G is either \mathfrak{S}_n , C_n , or $C_d \wr C_t$ where $n = dt$. \mathfrak{S}_n occurs as a Galois group over \mathbb{Q} . Theorems 3.7 and 3.8 guarantee that all cyclic groups and wreath products of cyclic groups arise as Galois groups for some extension of \mathbb{Q} . We may now apply the Main Lemma, and we have that for every $n \neq 2$ and for every d dividing n , we can construct a polynomial of degree n over \mathbb{Q} having root quantum number d . \square

4. CLASSIFICATION OF ROOT QUANTUM NUMBERS OVER HILBERTIAN FIELDS

The goal of this section will be to show that Theorem 3.1 holds for fields other than just the field of rationals. In particular, we shall show that the theorem is true for all *Hilbertian fields*. There are several ways to formulate the definition of a Hilbertian field, but we shall use the following definition.

Definition 4.1. Let $\mathbf{t} = (t_1, t_2, \dots, t_k)$ be a set of transcendental elements and $\mathbf{x} = (x_1, x_2, \dots, x_l)$ be indeterminates. A field K is *Hilbertian* if for any finitely many irreducible polynomials $f_1(\mathbf{t}, \mathbf{x}), \dots, f_m(\mathbf{t}, \mathbf{x}) \in K(\mathbf{t})[\mathbf{x}]$ and any finitely many non-zero polynomials $g_1(\mathbf{t}), \dots, g_n(\mathbf{t}) \in K[\mathbf{t}]$ there exists a vector $\mathbf{a} \in K^r$ for every r such that $f_1(\mathbf{a}, \mathbf{x}), \dots, f_m(\mathbf{a}, \mathbf{x}) \in K[\mathbf{x}]$ are well-defined and irreducible and $g_1(\mathbf{a}), \dots, g_n(\mathbf{a})$ are non-zero.

So for example, \mathbb{Q} , all algebraic number fields, and any field that is finitely generated over its prime subfield are examples of Hilbertian fields. Finite fields, \mathbb{R} , and \mathbb{C} are not Hilbertian. The major benefit of a field being Hilbertian is the ability to perform the process of *specialization*, or finding a vector \mathbf{a} that satisfies the above criteria. This procedure is important because it gives us the following crucial theorem.

Theorem 4.2 (Hilbert Irreducibility Theorem). *Let K be a Hilbertian field and $\mathbf{t} = (t_1, t_2, \dots, t_n)$ be a set of transcendental elements. If $f(\mathbf{t}, x) \in K(\mathbf{t})[x]$ is an irreducible polynomial, then there are infinitely many $\mathbf{a} = (a_1, a_2, \dots, a_n) \in K^n$ such that the specialization $f(\mathbf{a}, x) \in K[x]$ is well-defined and irreducible over K . The specialization can be chosen such that $\text{Gal}(f(\mathbf{t}, x)|K(\mathbf{t})) \cong \text{Gal}(f(\mathbf{a}, x)|K)$. [2]*

Hilbert's Irreducibility Theorem is useful because it yields the following proposition.

Proposition 4.3. *Let K be a Hilbertian field. If a finite group G occurs as a Galois group over $K(\mathbf{t})$, it occurs over K as well. [2, p. 87]*

The previous discussion motivates the following extension of Theorem 3.1 to all Hilbertian fields, and this result is the Main Theorem of the paper.

Main Theorem. *Let K be a Hilbertian field. For any $n \neq 2$ and for any d a divisor of n , there exists an irreducible polynomial $f(x) \in K[x]$ with degree n having root quantum number d .*

Step 1 of the proof has been completed in Section 3 since computing $r(G, G/H)$ does not require reference to a field. In light of Proposition 4.3, we recognize that in order to prove the Main Theorem we need only show that symmetric groups, cyclic groups, and wreath products of cyclic groups occur as Galois groups over $K(\mathbf{t})$ where K is Hilbertian. Chapter 3 of *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem* by Jensen, Ledet, and Yui was focused largely on this end, so we shall reference this work heavily throughout this discussion. We must now introduce some terminology.

Definition 4.4. A finite Galois extension $L|K(\mathbf{t})$ is called *regular* over K , if K is relatively algebraically closed in L , i.e., if no element in $L|K$ is algebraic over K .

Definition 4.5. Let K be a field and G a finite group. A Galois extension $S|R$ with group G is called a *generic G -extension* over K , if

- (1) R is of the form $K[\mathbf{t}, 1/t]$ for some number d of indeterminates $\mathbf{t} = (t_1, \dots, t_d)$, and an element $t \in K[\mathbf{t}] \setminus (0)$; and
- (2) whenever L is an extension field of K and T/L is a Galois algebra with group G , there is a K -algebra homomorphism $\phi : R \rightarrow L$, such that $S \otimes_{\phi} L|L$ and $T|L$ are isomorphic as Galois extensions.

Definition 4.6. Let M be the splitting field of a polynomial $p(\mathbf{t}, x) \in K(\mathbf{t})[x]$ over $K(\mathbf{t})$, and let G be a finite group. The polynomial $p(\mathbf{t}, x)$ is said to be *generic* for G over K if

- (1) $M|K(\mathbf{t})$ is Galois with $\text{Gal}(M|K(\mathbf{t})) \cong G$
- (2) every Galois extension $M|K$ with $G \cong \text{Gal}(M|K)$ is the splitting field of a polynomial $p(\mathbf{a}, x)$ for some $\mathbf{a} = (a_1, \dots, a_n) \in K^n$, and
- (3) $p(\mathbf{t}, x)$ satisfies (1) and (2) for G -extensions over any field containing K .

Note that if a generic polynomial exists for a group G over a field K , then the group G obviously arises as a Galois group over K .

Proposition 4.7. *The polynomial $x^n + t_1x^{n-1} + \dots + t_n$ is generic for \mathfrak{S}_n -extensions for any field and any n . [2, p. 3]*

Proposition 4.7 is a classical result in Galois Theory, and it tells us that the symmetric group of any order arises as a Galois group over any field.

We shall now show that cyclic groups of any order arise as Galois groups over all Hilbertian fields. Note that it is sufficient to show that cyclic groups of prime powers occur as Galois groups, since if G and H both arise as Galois groups over a field K , then so does $G \oplus H$.

First we shall describe the construction that yields the cyclic group of order $q = p^n$ where p is odd. Let K be a field of characteristic $\neq p$. Let $K(\mu_q)$ denote the q^{th} cyclotomic field over K , and let $d = |K(\mu_q) : K|$. Then we have that $C_d \cong \text{Gal}(K(\mu_q)|K)$ with generator κ . That is, $\kappa : \xi \mapsto \xi^e$ where ξ is a primitive q^{th} root of unity and $e \in \mathbb{Z}$ has order $d \pmod q$. It is possible to choose e to have order $pd \pmod{pq}$ so that $p \nmid (e^d - 1)/q$. Now we shall define a map Φ by

$$\Phi(x) = x^{e^{d-1}} \kappa x^{e^{d-2}} \cdot \dots \cdot \kappa^{d-1} x.$$

Define $\mathbf{x} = (x_1, \dots, x_d)$ such that $x_i = \kappa^i x_1$, and let $x = x_1 \cdot \dots \cdot x_d$. Now let $R = K[\mathbf{y}, 1/x]$ where $\mathbf{y} = (y_1, \dots, y_d)$ are indeterminates. Also let $R_q = K(\mu_q)[\mathbf{y}, 1/x] = K(\mu_q)[\mathbf{x}, 1/x]$ so that R_q is the scalar extension of R to $K(\mu_q)$. Now let $S_q = R_q[\theta]$, where $\theta^q = \Phi(x_1)$. Define $S = S_q^{C_d}$.

Proposition 4.8. *$S|R$ is a generic C_q -extension over K . [2, p. 122]*

This proposition gives us all cyclic groups of odd order over any field with characteristic $\neq p$.

Now we cite a result of A. Yakovlev that implies the occurrence of cyclic groups of order $q = 2^n$ over all fields of characteristic $\neq 2$.

Proposition 4.9. *Let K be a field of characteristic $\neq 2$, and let $a \in K^* \setminus (K^*)^2$ be a norm in the cyclotomic extension $K(\mu_q)/K$ where $q = 2^n$. Then $K(\sqrt{a})/K$ can be embedded in a cyclic extension of degree q . [2, p. 126]*

Thus we may obtain a regular C_q -extension over K via the following construction. Let t be an indeterminate. Then the regular quadratic extension $K(t, \sqrt{1+t^{2^{n-1}}})/K(t)$ can be embedded in a C_q -extension.

We have the following important corollary to Propositions 4.8 and 4.9.

Corollary 4.10. *Let K be a field and A a finite abelian group. Then there is a regular A -extension $M|K(\mathbf{t})$ over K . [2, p.126]*

Hence all cyclic groups arise as Galois groups over fields of the form $K(\mathbf{t})$.

Now we show that wreath products of cyclic groups arise as Galois groups over fields of the form $K(\mathbf{t})$. We cite a theorem of Ikeda that implies this fact.

Theorem 4.11 (Ikeda). *Let K be a Hilbertian field, and let $L|K$ be a Galois extension with Galois group $B = \text{Gal}(L|K)$. Let A be a finite abelian group and assume that B acts on A . Then there is an $A \rtimes B$ -extension of K having $L|K$ as its B -subextension. [2, p.129]*

Of course, since cyclic groups are abelian and since the wreath product may be realized as a semidirect product, then an immediate corollary of Ikeda's Theorem is that wreath products of cyclic groups arise as Galois groups over Hilbertian fields. We shall discuss the construction of the extension, however, according to the development of Ikeda's Theorem in *Generic Polynomials* [2, p.128-129].

Let K be a Hilbertian field and let $M|K(\mathbf{t})$ be a regular A -extension where A is a finite abelian group. Also let $L|K$ be finite Galois with $B = \text{Gal}(L|K)$. Assume that B acts on A . Consider $t = |B|$ copies of the A -extension $ML|L(\mathbf{t})$ and denote them $M_1|L(\mathbf{t}_1), \dots, M_n|L(\mathbf{t}_n)$. The composite $N = M_1 \cdots M_n$ over $L(\mathbf{t}_1, \dots, \mathbf{t}_n)$ is a regular A^t -extension.

Now let B act transitively on $\{1, 2, \dots, t\}$ and let $b \in B$. If $bi = j$, then there is a field isomorphism $L(\mathbf{t}_i) \cong L(\mathbf{t}_j)$ given by $b(lt_{ik}) = (bl)(bt_{ik}) = blt_{jk}$ where $l \in L, k = 1, \dots, r$. This isomorphism extends to $b : M_i \cong M_j$ and so B acts on the composite N .

Now let $W = L[\mathbf{t}_1, \dots, \mathbf{t}_n]$. Then B acts on W , and in particular, if $l \in L, \mathbf{w} \in W, b \in B$, then $b(l\mathbf{w}) = (bl)(b\mathbf{w})$. That is, B acts *semi-linearly* on the L -vector space of linear forms in $L[\mathbf{t}_1, \dots, \mathbf{t}_n]$.

Lemma 4.12 (Invariant Basis Lemma). *Let $L|K$ be a finite Galois extension of fields with $B = \text{Gal}(L|K)$ and let W be a finite-dimensional L -vector space on which B acts semi-linearly. Then W has an invariant basis; i.e., an L -basis of vectors in the K subspace W^B of B -invariant elements. [2, p.27]*

We have all of the necessary conditions to apply the Invariant Basis Lemma, and we thus have $L(\mathbf{t}_1, \dots, \mathbf{t}_n)^B = K(\mathbf{s})$ for basis elements $\mathbf{s} = (s_1, \dots, s_u)$. Finally we have the following proposition.

Proposition 4.13. *$N|K(\mathbf{s})$ is an $A \wr B$ -extension of $K(\mathbf{s})$.*

Proof of Main Theorem. Fix $n \neq 2$. Then for every d dividing n , Lemmas 3.2, 3.3, and 3.6 say that the symmetric group, cyclic groups, and wreath products of cyclic groups yield pairs (G, H) where $|G : H| = n$ and $r(G, G/H) = d$. Proposition 4.7 ensures that \mathfrak{S}_n arises as a Galois group over any field. Corollary 4.10 says that cyclic groups occur as Galois groups over fields of the form $K(\mathbf{t})$. Proposition 4.13 indicates that wreath products of cyclic groups are Galois groups over fields of the form $K(\mathbf{t})$. Thus we may apply Proposition 4.3 to Corollary 4.10 and Proposition 4.13, and we have that cyclic groups and wreath products of cyclic groups arise as Galois groups over all Hilbertian fields. Let K be a Hilbertian field. We may now apply the Main Lemma, and we have that for every $n \neq 2$ and for every d dividing n , we can construct a polynomial of degree n over K having root quantum number d . \square

ACKNOWLEDGEMENTS

The author would like to thank Robert Perlis for his guidance and assistance in the research and writing processes. A special thanks is also offered to all persons involved in coordinating the REU 2002 at Louisiana State University.

REFERENCES

- [1] Perlis, Alexander, *Roots Appear in Quanta*, preprint 2002 available at <http://grad.math.arizona.edu/aprl>.
- [2] Jensen, Christian, Arne Ledet, and Noriko Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, Cambridge University Press, manuscript, 2002.
- [3] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

MATHEMATICS DEPARTMENT, WASHINGTON & LEE UNIVERSITY, LEXINGTON, VIRGINIA, 24450

E-mail address: `townsende@wlu.edu`