Hilbert's irreducibility theorem and its application to the inverse Galois problem

JV van Zyl

University of Pretoria

Submitted in partial fulfillment of the requirements of the degree

Magister Scientiae

in the Department of Mathematics & Applied Mathematics

in the Faculty of Natural & Agricultural Sciences

University of Pretoria

Pretoria

October 2005

Hilbert's irreducibility theorem and its application to the inverse Galois problem

by

Jacobus Visser van Zyl

supervised by

Prof LM Pretorius

in the

Department of Mathematics and Applied Mathematics

for the degree

MSc Mathematics

Abstract

To every polynomial $f(x)$ with rational coefficients one can associate a finite group G_f, the Galois group of the splitting field of f over the rational numbers. The inverse problem of Galois theory asks whether for a given finite group G, there exists a polynomial f such that G is isomorphic to G_f. A Galois extension of $\mathbb{Q}$, with Galois group G, is called a *realisation* of G over $\mathbb{Q}$, and G is said to *occur* over $\mathbb{Q}$. It is known that all abelian groups occur over $\mathbb{Q}$, and Šaferevič showed in 1957 that all solvable groups occur over $\mathbb{Q}$. Almost all other progress with the problem depends on Hilbert's irreducibility theorem, which implies that a realisation of G over $\mathbb{Q}$ exists if and only if a realisation exists over the function field $\mathbb{Q}(x)$. Hence it suffices to find realisations of a particular group G over $\mathbb{Q}(x)$, which enables us to use tools from Riemannian Surface Theory and Algebraic Geometry.

Contents

1 Introduction

Before the 1800s, the main problem in algebra was to solve polynomial equations over the rational numbers. The solution to the quadratic has been known since ± 1700 BC ([1], §3) and the general solutions to the cubic and the quartic were discovered in the 1740s by Dal Ferro, Tartgalia, Cardano and Ferrari ([3], §9.9). For the next 200 years mathematicians struggled to solve the general quintic. It wasn't until 1799 when Ruffini published an incomplete outline of a proof, based on the earlier work of Lagrange, that the general quintic is not solvable by radicals. In 1824 Abel published a complete proof, and the question was finally settled. Two decades later Galois used the language of groups to confirm the result, in the process giving birth to Galois theory.

With every polynomial f of degree n over a field k, one can associate a finite group G_f, the Galois group of the splitting field of f over k, which is a subgroup of S_n, the symmetric group of n elements consisting of all permutations of n elements. Galois proved that f is solvable by radicals over k if and only if the group G_f is solvable. Thus, to gain an understanding of the solvability of polynomials, one needs an understanding of the correspondence between subgroups of S_n and polynomials of degree n over k. Unfortunately it is very difficult in general to compute the Galois group of a polynomial, and the full understanding has only been achieved for small n ([10], [14]).

A natural question for bigger n, first stated by Hilbert in 1892 [6], is if at least every subgroup of S_n corresponds to some polynomial over k. This problem is called the Inverse Problem of Galois Theory, or simply the Inverse

Galois Problem.

While the Inverse Galois Problem is stated for any field k, most of the work done has been over $\mathbb{Q}$. For some fields the problem has been solved: the problem has a negative solution over the finite fields (all Galois extensions are abelian) and p-adic numbers (all Galois extensions are solvable) ([10], §1), and a positive solution over the function field $\mathbb{C}(x)$ ([13], §2.2.2) and in fact, over the function field $k(x)$ for k algebraically closed or k a p-adic field ([7], §0.1).

It is easy to show that every finite abelian group occur as a Galois group over $\mathbb{Q}$ (see Theorem 7.1) and in 1954 Šaferevič [12] proved that all solvable groups occur as a Galois group over $\mathbb{Q}$. Almost all other results depend on Hilbert's Irreducibility theorem - the statement that $\mathbb{Q}$ is a *hilbertian field*, that is, for every irreducible polynomial $f(x, y)$ over $\mathbb{Q}$, there are infinitely many $b \in \mathbb{Q}$ such that the Galois group of $f(b, y)$ over $\mathbb{Q}$ is isomorphic to the Galois group of $f(x, y)$ over $\mathbb{Q}(x)$. Thus it is sufficient to work over the function field $\mathbb{Q}(x)$, which allows the use of methods from Riemannian Surface Theory and Algebraic Geometry. Every finitely generated extension of a hilbertian field is again hilbertian, and Weissauer's Theorem (Theorem 6.2) gives conditions for an infinite extension of a hilbertian field to be hilbertian (of special importance is the full cyclotomic field $\mathbb{Q}_{ab}$).

Of particular interest are the Galois extensions K of $\mathbb{Q}(x)$, with $\mathbb{Q}$ algebraically closed in K (in other words, all the elements of $K \backslash \mathbb{Q}$ are transcendental over $\mathbb{Q}$). Such an extension is called *regular*. The *Regular Inverse Galois Problem* asks whether every finite group G occurs as the Galois group of a regular extension of $\mathbb{Q}(x)$. Regular extensions have the property that if

K is a regular extension of $\mathbb{Q}(x)$ with Galois group G, then G occurs as a Galois group over *every* hilbertian field K of characteristic 0.

This dissertation gives a detailed proof of Hilbert's Irreducibility Theorem and does not deal specifically with finding Galois extensions of $\mathbb{Q}(x)$. For such constructions, see [7], [9], [10] and [12]. The structure of the dissertation is based on the first chapter of Helmut Völklein's book "Groups as Galois Groups - an Introduction" ([13]), and the bulk of the proofs given herein is due to him.

2 Preliminary Results

First we establish a few results. Unless otherwise stated, k will be a field of characteristic 0, and $\overline{k}$ will be an algebraic closure of k. Elementary results from Galois Theory will be used without reference. See [8] for an excellent introduction to Galois Theory.

Theorem 2.1 *Let α be algebraic over the field L, and let R be a ring with L as its field of fractions. Let $f(y) = a_n y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in R[y]$ be a polynomial satisfying $f(\alpha) = 0$. Then the polynomial*

$$g(Y) = Y^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i} Y^i$$

is a monic polynomial of degree n in $R[y]$ satisfying $g(a_n\alpha) = 0$. Also $L(\alpha) = L(a_n\alpha)$.

Proof. Since $f(\alpha) = 0$, it follows that

$$\begin{aligned} & a_n^n\alpha^n + a_n^{n-1}a_{n-1}\alpha^{n-1} + a_n^{n-1}a_{n-2}\alpha^{n-2} + \cdots + a_n^{n-1}a_0 = 0, \\ \text{i.e.} \quad & (a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + \cdots + a_n^{n-1}a_0 = 0, \\ \text{or concisely,} \quad & (a_n\alpha)^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i}(a_n\alpha)^i = 0, \end{aligned}$$

which shows that $a_n\alpha$ is a root of the monic polynomial $g(Y)$. Since $0 \neq a_n \in L$, we have that $L(\alpha) = L(a_n\alpha)$. ■

This result allows us to assume that for a given Galois extension K of k, there exists a monic polynomial over k whose roots generate K over k. This is nicely complemented by the following:

Theorem 2.2 *Let $f(x_1, x_2, \ldots, x_s)$ be a polynomial in $s \geqslant 2$ variables over k. Then f is irreducble as a polynomial in s variables over k if and only if f is irreducible and primitive (i.e., the coefficients of f are relatively prime) as a polynomial in x_s over $k[x_1, x_2, \ldots, x_{s-1}]$.*

Proof. Suppose that f is primitive and irreducible as a polynomial in x_s over $k[x_1, \ldots, x_{s-1}]$. If f is not irreducible as a polynomial in s variables, then f decomposes as $f = gh$ over k. Since f is irreducible as a polynomial in x_s, one of the factors, say g, must be a polynomial in $k[x_1, \ldots, x_{s-1}]$. This means that the coefficients of f, viewed as a polynomial in x_s, are all multiples of g. Hence g is a unit in $k[x_1, \ldots, x_{s-1}]$ implying that $g \in k$. Thus f is irreducible as a polynomial in x_s over $k[x_1, \ldots, x_{s-1}]$.

The converse is clear. ■

In particular, if f is monic in x_s, we are allowed to drop the hypothesis that f is primitive as a polynomial in x_s.

Theorem 2.3 *Let $x_1, x_2, \ldots, x_m$ be algebraically independent over a field k, and let $\mathbf{x} = (x_1, x_2, \ldots, x_m)$. Let $\overline{k}$ be an algebraic closure of k.*

(i) If k' is a finite Galois extension of k, then $k'(\mathbf{x})$ is a finite Galois extension of $k(\mathbf{x})$, and the restriction map $G(k'(\mathbf{x})/k(\mathbf{x})) \to G(k'/k)$ is an isomorphism. In particular, every field between $k(\mathbf{x})$ and $k'(\mathbf{x})$ is of the form $k''(\mathbf{x})$, and $[k''(\mathbf{x}) : k(\mathbf{x})] = [k'' : k]$.

(ii) Let $f(\mathbf{x}, y) \in k(\mathbf{x})[y]$ be irreducible over $k(\mathbf{x})$, and let $K = k(\mathbf{x})[y]/(f) = k(\mathbf{x})(\alpha)$ be the corresponding field extension of $k(\mathbf{x})$,

where α is a root of f over $k(\mathbf{x})$. Then k is algebraically closed in K if and only if f is irreducible over $\overline{k}(\mathbf{x})$. In this case, $f(\mathbf{x}, y)$ is irreducible over $k_1(\mathbf{x})$ for every extension field k_1 of k such that $x_1, x_2, \ldots, x_m, y$ are independent transcendentals over k_1.

Proof.

(i) The Galois group G of k'/k extends naturally to $k'(\mathbf{x})$ by fixing $x_1, \ldots, x_m$. Let G' be the group of such extensions of G. It is clear that G and G' are isomorphic. The fixed field of G is, by definition, k, and so the fixed field of G' is $k(\mathbf{x})$. Thus, by Artin's Theorem, $k'(\mathbf{x})$ is Galois over $k(\mathbf{x})$ with Galois group G'. If F' is any field between $k(\mathbf{x})$ and $k'(\mathbf{x})$, let H' be the subgroup of G' such that F' is the fixed field of H'. Let H be the corresponding subgroup of G, with fixed field F, where F is a field between k and k'. Then, by the definition of G', it follows that $F' = F(\mathbf{x})$.

(ii) Suppose k is not algebraically closed in K, and let $\hat{k}$ be the algebraic closure of k in K. Since $k \subset \hat{k} \subset K$, there exist an irreducible polynomial $\hat{f} \in \hat{k}(\mathbf{x})[y]$ such that $\hat{f}(\mathbf{x}, \alpha) = 0$ and $\hat{f}$ divides f. Now, since $\hat{k} \neq k$, $[\hat{k} : k] > 1$, and so $[K : k(\mathbf{x})] = [K : \hat{k}(\mathbf{x})][\hat{k}(\mathbf{x}) : k(\mathbf{x})] > [K : \hat{k}(\mathbf{x})]$ implying that the degree of $\hat{f}$ is less than the degree of f, which means that f is not irreducible over $\hat{k}(\mathbf{x})$, and hence not over $\overline{k}(\mathbf{x})$.

Conversely, assume that k is algebraically closed in K. Let k' be any finite Galois extension of k. Let $K' = k'(\mathbf{x})(\alpha)$ be the compositum of K and $k'(\mathbf{x})$ inside some algebraic closure of $k'(\mathbf{x})$. Now, $K \cap k'(\mathbf{x}) \subset k'(\mathbf{x})$

and hence, by (i), $K \cap k'(\mathbf{x}) = k''(\mathbf{x})$ for some field $k \subset k'' \subset k'$. Let $\beta \in k'' \subset K$, and let $g(y)$ be the irreducible polynomial of β over k (it exists, since k'' is a finite extension of k). Since k is closed in K and $\beta \in K$, $\beta \in k$. Since $\beta \in k''$ was arbitrary, it follows that $k = k''$. Hence $K \cap k'(\mathbf{x}) = k(\mathbf{x})$. Since $k'(\mathbf{x})$ and K are finitely generated over $k(\mathbf{x})$ by (i) and K' is the compositum of K and $k'(\mathbf{x})$, it follows that $[K' : k'(\mathbf{x})] = [K : k(\mathbf{x})]$. This means that the irreducible polynomial of α over $k'(\mathbf{x})$ has the same degree as f, showing that f is irreducible over $k'(\mathbf{x})$. Since k' was arbitrary, f is irreducible over $\overline{k}(\mathbf{x})$.

Let k_1 be an extension field of k such that $x_1, \ldots, x_m, y$ are independent transcendentals over k_1 and suppose that $f(\mathbf{x}, y)$ is not irreducible over $k_1(\mathbf{x})$, i.e. $f = gh$ for some $g, h \in k_1(\mathbf{x})[y]$. We may assume that g is monic in y. We may also assume that k_1 is generated over k by the coefficients of g (where g is viewed as a rational function in $x_1, \ldots, x_m, y$) and that one of these coefficients, call it t, is transcendental over k (if not, then $k_1 \subset \overline{k}$ and the result follows immediately since f is irreducible over $\overline{k}(\mathbf{x})$).

Now, k_1 is a finite extension of some field $k_2 = k(t_1, t_2, \ldots, t_s)$, where $t_1, \ldots, t_s$ are independant transcendentals over k with $t_1 = t$ ([8], Chapter 8, Theorem 2.1) . Now, for each $\beta \in k$, the function $a_\beta : k_2 \to k_2$ mapping $t \to t + \beta$ and fixing k and the other t_i is an automorphism of k_2 over k. Each automorphism a_β can be extended to an embedding of k_1 into $\overline{k_2}$, which can be extended to an embedding of $k_1(\mathbf{x})[y]$ into $\overline{k_2}(\mathbf{x})[y]$.

Apply each such a_β to the equation $f = gh$. Since $f \in k(\mathbf{x})[y]$, f is

fixed by a_β. On the other hand, applying a_β to g for each β yields distinct monic polynomials in $\overline{k_2}(\mathbf{x})[y]$ each dividing f, contradiction. Thus f is irreducible over $k_1(\mathbf{x})$.

■

We say that a group G *occurs* over k, or G is realised over k, if there exists a Galois extension of k with Galois group G. Part (i) of the above result states that if G occurs over k, then it also occurs over $k(x)$. It is reasonable to ask for which k the converse will also hold. In the next section, we attempt to answer that question.

3 Specialising coefficients of a polynomial

Recall that the discriminant of a monic polynomial $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ is defined to be equal to $\prod_{i<j}(\alpha_j - \alpha_j)^2$. Note that this expression is symmetric in the α_is. By the Fundemental Theorem of Symmetric Polynomials, the determinant can be written as a polynomial over $\mathbb{Z}$ in the coefficients of f ([1], §13). The determinant is nonzero if and only if if and only if f is separable, i.e. if and only if f has no repeated roots.

Theorem 3.1 *Let K be a finite Galois extension of F with Galois group G. Let R be a subring of F having F as a field of fractions. Let $\alpha \in K$ be a generator of K over F, satisfying $f(\alpha) = 0$ for some polynomial $f(y) \in R[y]$ of degree $n = [K : F]$ (we may assume f monic by Theorem 2.2). Let $A \subset K$ be a finite set containing α and invariant under G. Let $S = R[A]$.*

Then there exists a $0 \neq u \in R$ such that for each ring-homomorphism ω from R into some field F' satisfying $\omega(u) \neq 0$, the following holds:

(i) ω extends to a homomorphism $\overline{\omega} : S \to K'$, where K' is a finite field extension of F'.

(ii) for each such $\overline{\omega}$, the field K' is Galois over F', generated by $\alpha' = \overline{\omega}(\alpha)$ over F'. We have $f'(\alpha') = 0$, where $f' \in F'[y]$ is the polynomial obtained by applying ω to the coefficients of f. Thus $[K' : F'] = [K : F]$ if and only if f' is irreducible, in which case K' is $F' - isomorphic$ to $F'[y]/(f')$.

(iii) Now suppose that f' is irreducible. Then for each $\overline{\omega}$ as in (1), there is a unique isomorphism from G to $G(K'/F')$ mapping σ to σ', such that

$\overline{\omega}(\sigma(s)) = \sigma'(\overline{\omega}(s))$ *for all* $\sigma \in G$, $s \in S$.

Proof. Since K/F is Galois, $f(y)$ is seperable, hence its discriminant D_f is a nonzero element of R. Also, $\omega(D_f)$ is the discriminant of the polynomial f' obtained by applying ω to the coefficients of f. Consider only those ω for which $\omega(D_f)$ is nonzero and thus f' is separable.

Consider the natural map between $R[y]$ and $R[\alpha]$. Let I be the kernel of this map. If $h \in I$, then $h(\alpha) = 0$, hence $h = fg$ for some polynomial $g \in F[y]$. Let $f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0$ and $g(y) = b_m y^m + b_{m-1}y^{m-1} + \cdots + b_0$, where $a_i \in R$ and $b_i \in F$. Then

$$h(y) = b_m y^{m+n} + (b_{m-1} + b_m a_{n-1})y^{m+n-1} + \cdots + a_0 b_0.$$

Since $h \in I \subset R[y]$, the coefficient b_m of y^{m+n} lies in R. Similarly, $b_{m-1} + b_m a_{n-1} \in R$, implying that $b_{m-1} \in R$. Continuing in this way, we see that $b_i \in R$ for each i, and hence $g \in R[y]$. Thus $h \in fR[y]$, the ideal of $R[y]$ generated by f. Conversely, if h is in this ideal, then $h(\alpha) = 0$ hence $h \in I$. This yields the isomorphism

$$\phi : R[y]/I \to R[\alpha].$$

Case 1: $R[A] = R[\alpha]$

Extend ω to $R[y] \to F'[y]$ by fixing y. This map sends f to f' and thus induces the ring-homomorphism

$$\varphi : R[y]/I = R[y]/(f) \to F'[y]/(f')$$

by applying ω to the coefficients of the polynomials in $R[y]/I$. Let $\xi = \varphi \circ \phi^{-1}$ by a ring-homomorphism from $R[\alpha]$ to $F'[y]/(f')$.

(i) Let g' be an irreducible factor of f', and set $K' = F'[y]/(g')$. K' is then a finite field extension of F'. Composing ξ with the natural map $F'[y]/(f') \to F'[y]/(g')$ gives a homomorphism from $S = R[\alpha]$ to K', which extends ω as desired.

(ii) The image of α under $\overline{\omega}$ is the polynomial y in $F'[y]/(g')$, which is a root, say α', of g' in the field $K' = F'[y]/(g')$, which is thus generated by α' over F'.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of α under G. By hypothesis, $\alpha_i \in A$ for each i. Let $\alpha_i' = \overline{\omega}(\alpha_i) \in K'$. Applying ω to $f = \prod_{i=1}^{n}(y - \alpha_i)$ yields $f' = \prod_{i=1}^{n}(y - \alpha_i')$. Since each $\alpha_i' \in K'$, the conjugates of α' (which are the roots of g') all lie in K', hence K' is normal over F' (since $K' = F'[\alpha']$). Also, since f' is seperable, so is g', and hence K' is seperable over F', and thus Galois.

f' is seperable if and only if $[K : F] = \deg(f) = \deg(f') = \deg(g') = [K' : F']$, in which case $K' = F'[y]/(f')$.

(iii) If f' is irreducible, the conjugates of α' over F' are all the α_i'. Since f' is seperable, the α_i' are distinct. Thus, for each α_i', there exists a unique $\sigma_i \in G'$ such that $\sigma_i(\alpha') = \alpha_i'$. Similarly, there exists a unique $\sigma_i \in G$ such that $\sigma_i(\alpha) = \alpha_i$. This yields a bijection $\theta : \sigma_i \to \sigma_i'$ between G and G'. If $\overline{\omega}(\sigma(\alpha)) = \sigma'(\overline{\omega}(\alpha))$ for all $\sigma \in G$, then for each $\sigma, \tau \in G$, we

have:

$$\begin{aligned}
(\sigma\tau)'(\alpha') &= (\sigma\tau)'(\overline{\omega}(\alpha)) \\
&= \overline{\omega}(\sigma\tau(\alpha)) \qquad \text{(by assumption)} \\
&= \overline{\omega}(\sigma(\tau(\alpha))) \\
&= \sigma'(\overline{\omega}(\tau(\alpha))) \qquad \text{(by assumption)} \\
&= \sigma'\tau'(\overline{\omega}(\alpha)) \qquad \text{(by assumption)} \\
&= \sigma'\tau'(\alpha').
\end{aligned}$$

Thus the bijection θ is also a homomorphism, and hence an isomorphism.

Let $s \in S$ be arbitrary, and $\sigma_i \in G$ be arbitrary. Since $S = R[\alpha]$, we can write $s = h(\alpha)$ for some $h \in R[y]$. Let $h' \in F'[y]$ be obtained by applying ω to the coefficients of h. Then

$$\begin{aligned}
\sigma_i'(\overline{\omega}(s)) &= \sigma_i'(\overline{\omega}(h(\alpha))) \\
&= \sigma_i'(h'(\alpha')) \qquad \text{(definition of } h' \text{ and } \alpha') \\
&= h'(\alpha_i') \qquad (\sigma_i' \text{ fixes } F') \\
&= \overline{\omega}(h(\alpha_i)) \\
&= \overline{\omega}(\sigma_i(h(\alpha)) \\
&= \overline{\omega}(\sigma_i(s)).
\end{aligned}$$

Since $\alpha \in S$, we are done.

Case 2: $R[A] \neq R[\alpha]$

Since $A \subset K = F[\alpha]$, we can write $a = \sum_{i=0}^{n-1} b_i\alpha^i$ with $b_i \in F$ for each $a \in A$. Let B be the set of all b_i as a ranges over all the elements of A. Since

A is finite, so is B, and since F is the field of fractions of R, there exists a nonzero $v \in R$ such that $vb_i \in R$ for each $b_i \in B$.

Set $u = vD_f$ and $\tilde{R} = R[u^{-1}]$. Then for each $b_i \in B$, we have

$$vb_i = r_i \in R \implies \frac{ub_i}{D_f} = r_i \implies b_j = \frac{r_j D_f}{u} \in \tilde{R}.$$

Hence $A \subset \tilde{R}[\alpha]$ and so $\tilde{R}[A] = \tilde{R}[\alpha]$.

If $\omega : R \to F'$ is a homomorphism with $\omega(u) \neq 0$, extend if to $\tilde{R}$ by setting $\omega(\frac{r}{u}) = \frac{\omega(r)}{\omega(u)}$. This extesion is unique, since for ω to be a homomorphism on $\tilde{R}$, $\omega(\frac{r}{u})\omega(u) = \omega(\frac{r}{u}u) = \omega(r)$.

Now, ω and $\tilde{R}$ satisfy the original hypotheses, so we can apply Case 1. ■

The next result may be viewed as a weak analogue of Hilbert's Irreducibility Theorem (replacing "irreducible" with "separable", and noting that in characteristic 0 irreducible polynomials are separable). Recall that "for almost all" means "for all but finitely many".

Theorem 3.2 *Let L be a field and let $f(x, y) \in L[x, y]$ be separable as a polynomial in y over $L(x)$. Then the specialised polynomial $f(b, y) \in L[y]$ is seperable for almost all $b \in L$.*

Proof. We may assume that f is monic in y. Since f is seperable over $L(x)$, its discriminant $D(x)$ is a nonzero element of $L[x]$. The specialised polynomial $f(b, y)$ has discriminant $D(b)$, which is nonzero except for the finitely many roots of $D(x)$. Hence, $f(b, y)$ is seperable for all those b such that $D(b) \neq 0$. ■

Theorem 3.3 *Let K be a Galois extension of $k(x)$ of finite degree $n > 1$. Then there exists a polynomial $f(x, y) \in k[x, y]$ monic and of degree n in y, and a generator α of K over $k(x)$ such that $f(x, \alpha) = 0$. Furthermore:*

(i) For almost all $b \in k$, the following holds: If the polynomial $f_b(y) := f(b, y)$ is irreducible over k, then $k[y]/(f_b)$ is Galois over k with Galois group isomorphic to $G = G(K/k(x))$.

(ii) There is a finite collection of polynomials $p_I(x, y) \in k[x, y]$, irreducible and of degree greater than 1 in y over $k(x)$, such that for almost all $b \in k$, the following holds: If none of the specialised polynomials $p_I(b, y) \in k[y]$ has a root in k, then $f(b, y)$ is irreducible over k.

(iii) Suppose ℓ is a finite extension of k contained in K. Let $h(x, y) \in \ell[x, y]$ be irreducible over $\ell(x)$ and assume that its roots lie in K. Then, for almost all $b \in k$ the following holds: If $f_b(y)$ is irreducible over k, then $h(b, y)$ is irreducible over ℓ.

Proof. For each generator α of K over $k(x)$, there exists a polynomial $f(x, y)$ of degree n in y satisfying $f(x, \alpha) = 0$. By multipling f by a suitable element of $k[x]$, me may assume that $f \in k[x, y]$. Furthermore, by Theorem 2.1 we may assume that f is monic in y. Thus $f(x, y) = \prod_{i=1}^{n}(y - \alpha_i)$, where the α_i are the conjugates of α over $k(x)$.

For each $b \in k$, let $\omega_b : k[x] \to k$ be the evaulation homomorphism sending $h \in k[x]$ to $h(b)$. Let $F = k(x)$, $\omega = \omega_b$, $R = k[x]$ and $F' = k$. Then $f'(y) = f_b(y)$.

(i) Suppose $f_b(y)$ is irreducible over k and let $K' = k[y]/(f_b) = k[\beta]$ where β is a root of f_b. Let A be a finite subset of K containing α and its conjugates over k. Then $S = k[x][\beta]$. Now apply Theorem 3.1. There exists a $0 \neq u(x) \in k[x]$ such that for all $b \in k$ satisfying $\omega_b(u(x)) = u(b) \neq 0$ (in other words, all $b \in k$ except the finitely many roots of u), ω_b can be extended to the homomorphism $\overline{\omega_b} : S \to K'$ with $\overline{\omega_b}(\alpha) = \beta$. By (ii) $k[\beta]$ is Galois over k, and by (iii), $G(k[\beta]/k)$ is isomorphic to $G(K/k(x)$.

(ii) Let I be a proper, non-empty subset of $\{1, \ldots, n\}$. Since f is irreducible over $k(x)$, the product $\prod_{i\in I}(y - \alpha_i)$ cannot lie in $k(x)[y]$. Thus is has a coefficient d_I with $d_I \notin k(x)$. However, since all the α_i lie in K and d_I is a polynomial function of the α_i, $d_I \in K = k(x)[\alpha]$. Thus there exists an irreducible polynomial $p_I(x, y) \in k(x)[y]$ of degree greater than 1 in y satissying $p_I(x, d_I) = 0$. By multiplying p_I with a suitable element of $k[x]$, we may assume that $p_I \in k[x, y]$.

Now suppose f_b is not irreducible over k. Then there is some I as above such that the product $\prod_{i\in I}(y - \alpha'_i)$ lies in $k[y]$, where $\alpha'_i = \overline{\omega_b}(\alpha_i)$. Thus the coefficient $c = \overline{\omega_b}(d_I)$ lies in k. Applying $\overline{\omega_b}$ to the equation $p_I(x, s_I) = 0$, we obtain $p_I(b, c) = 0$, showing that $p_I(b, y)$ has a root $c \in k$.

(iii) Suppose f_b is irrudicible over k, and let $h(x, y) = h_0(x)\prod_{i=1}^{t}(y - \beta_i)$ where $h_0(x) \in \ell[x]$ and $\beta_i \in K$.

Let A be a finite set as in Theorem 3.1 containing β_i and a generator of ℓ over k. Let $S = k[x][A]$, such that $\ell \subset S$. Then $\overline{\omega_b}$ maps ℓ to a

subfield ℓ' of K'. Under this map we get $h(b, y) = h_0(b) \prod_{i=1}^{t}(y - \beta_i')$. Furthermore, the isomorphism in (iii) of Theorem 3.1 maps a subgroup H of G to s subgroup H' of G'.

Since h is irreducible over $k(x)$ and k has characteristic 0, h is seperable, and the group $H = G(K/\ell(x))$ permutes its roots transitively. Thus H' permutes the roots β_i' transitively. Exclude the finitely many $b \in k$ such that $h_0(b) = 0$ and $h(b, y)$ is not seperable (Theorem 3.2). Then $h(b, y)$ is seperable, and the subgroup H' of $G(k'/\ell)$ permutes its roots transitively, hence $h(b, y)$ is irreducible over ℓ.

■

We are now ready to provide a restriction on k that will guarantee that if a group G occurs over $k(x)$, then it also occurs over k. Note that part (i) of the above result almost answers our question. In fact, if there exists a $b \in k$ such that $f(b, y)$ is irreducible over k and b is not one of the finitely many elements of k for which part (i) does not hold, then $k[y]/(f_b)$ is the required extension. A sufficient condition for the existence of such an element is if there are *infinitely* many $b \in k$ such that $f(b, y)$ is irreducible over k. This gives rise to the definition of a *hilbertian field*.

4 Hilbertian fields

Definition 4.1 *A field k is called* hilbertian *if for each irreducible polynomial $f(x,y) \in k[x,y]$ of positive degree in y, there are infinitely many $b \in k$ such that $f(b,y)$ is irreducible over k.*

Parts (ii) and (iii) of Theorem 3.3 give rise to two equivalent definitions for k to be hilbertian:

Theorem 4.2 *The following conditions on k are equivalent:*

(i) For each irreducible polynomial $f(x,y) \in k[x,y]$ of positive degree in y, there are infinitely many $b \in k$ such that the specialised polynomial $f(b,y)$ is irreducible over k.

(ii) For any $p_1(x,y), \ldots, p_t(x,y) \in k[x,y]$ that are irreducible over $k(x)$ and of degree greater than 1 in y, there are infinitely many $b \in k$ such that none of the specialised polynomials $p_1(b,y), \ldots, p_t(b,y)$ has a root in k.

(iii) Given a finite extension ℓ/k and $h_1(x,y), \ldots, h_m(x,y) \in \ell[x,y]$ that are irreducible over $\ell(x)$, there are infinitely many $b \in k$ such that the specialised polynomials $h_1(b,y), \ldots, h_m(b,y)$ are irreducible over ℓ.

Proof.

(iii) $\Longrightarrow$ (i): Let $f(x,y)$ be as in the hypothesis. Then f is irreducible over $k(x)$ by Theorem 2.2. By (iii), with $\ell = k$, $m = 1$ and $h_1 = f$, there are infinitely many $b \in k$ such that $f(b,y)$ is irreducible over k.

(i) $\Longrightarrow$ (iii): Let ℓ and $h_i(x, y)$ be as in the hypotheses. Let S be the (finite) set of all roots of $h_i(x, y)$ over $\ell(x)$. Let K be a finite Galois extension of $\ell(x)$ containing S and let $f(x, y) \in k[x, y]$ be a polynomial, monic in y and irreducible over $k(x)$ (hence irreducible as a polynomial in two variables, by Theorem 2.2) as in Theorem 3.3. By (i), there are infinitely many $b \in k$ such that $f(b, y)$ is irreducible over k. Then by part (iii) of Theorem 3.3, for all these b except finitely many, $h_i(x, y)$ is irreducible over ℓ. Hence there are infinitely many $b \in k$ such that all the polynomials $h_i(b, y)$ are irreducible over ℓ.

(iii) $\Longrightarrow$ (ii): Let $p_i(x, y)$ be as in the hypothesis. By (iii), with $\ell = k$, $m = t$ and $h_i = p_i$, there are infinitely many $b \in k$ such that the specialised polynomials $p_i(b, y)$ are irreducible over k, and since each of the p_i are of degree greater than 1 in y, none of these polynomials has a root in k.

(ii) $\Longrightarrow$ (iii) Let ℓ and $h_i(x, y)$ be as in the hypotheses. Let S be the (finite) set of all roots of $h_i(x, y)$ over $\ell(x)$. Let K be a finite Galois extension of $\ell(x)$ containing S and let $f(x, y) \in k[x, y]$ be a polynomial, monic in y and irreducible over $k(x)$ (hence irreducible as a polynomial in two variables, by Theorem 2.2) as in Theorem 3.3. Let $p_1(x, y), \ldots, p_t(x, y)$ be a collection of polynomials, irreducible and of degree greater than 1 when viewed as polynomials in y, as in part (ii) of Theorem 3.3. Then, by (ii) there are infinitely many $b \in k$ such that none of the specialised polynomials $p_i(b, y)$ has a root in k. Then, by (ii) of Theorem 3.3, for almost all of these b, $f(b, y)$ is irreducible over k. By part (iii) of Theorem 3.3, it follows that for each i, $h_i(b, y)$ is irreducible over ℓ for

almost all of the remaining b. Hence there are infinitely many $b \in k$ such that all of the polynomials $h_i(b, y)$ are irreducible over ℓ.

■

Part (iii) of the above result shows that every fininte extension of a hilbertian field is also hilbertian.

It can be shown that if k is hilbertian, then so is $k(x_1, x_2, \ldots, x_m)$. Hence, if a group G occurs over $k(x_1, x_2, \ldots, x_m) = k(x_1, x_2, \ldots, x_{m-1})(x_m)$, it also occurs over $k(x_1, x_2, \ldots, x_{m-1})$ by Theorem 3.3(i) and proceeding inductively, G occurs over k. For a proof of these results, see [13], §1.1.3.

Definition 4.3 *A finite group* G occurs regularly *over* k *if for some* $m \geqslant 1$, k *is algebraically closed in some Galois extension of* $k(x_1, \ldots, x_m)$ *with Galois group* G.

In the above definition we may actually replace "some $m \geqslant 1$" with "all $m \geqslant 1$" ([13], §1.3.2). Regular realisations are also invariant under extensions of k, as the next theorem shows.

Theorem 4.4 *Suppose* G *occurs regularly over* k. *Then* G *occurs regularly over every extension field* k_1 *of* k.

Proof. Let G occur regularly over k, and let K be a Galois extension of $k(x_1, \ldots, x_m) = k(\mathbf{x})$, generated by α over $k(\mathbf{x})$, with k algebraically closed in K. We may assume that $x_1, x_2, \ldots, x_m$ are independent transcendentals over k_1, by the remarks following Theorem 4.2 and [8], Chapter 8, Theorem 2.1. Hence $x_1, \ldots, x_m$ are independent transcendentals over $\overline{k_1}$.

Let $f(\mathbf{x}, y) \in k(\mathbf{x})[y]$ be the irreducible polynomial of α over $k(\mathbf{x})$. Then $K = k(\mathbf{x})[y]/(f)$, and since k is algebraiclly closed in K, it follows from Theorem 2.3(ii) that f is irreducible over $\overline{k_1}(\mathbf{x})$, and hence over $k_1(\mathbf{x})$. Thus $K_1 = k_1(\mathbf{x})[y]/(f)$ is an extension field of $k_1(\mathbf{x})$ with $[K : k(\mathbf{x})] = [K_1 : k_1(\mathbf{x})]$. Since K is galois over $k(\mathbf{x})$, $K \subset K_1$ contains all the roots of f. Hence K_1 is Galois over $k_1(\mathbf{x})$, and k_1 is algebriacally closed in K_1 by Theorem 2.3(ii).

The Galois group of K_1 over $k_1(x)$ embeds into G via restriction, and the two groups have the same order, hence they are isomorphic. Thus G occurs regularly over k_1. ■

If k_1 in the above result happens to be hilbertian, then G occurs as a Galois group over k_1 by the remarks preceding Definition 4.3. Hence, if G occurs regularly over $\mathbb{Q}$, then G occurs as a Galois group over *every* hilbertian field of characteristic 0 (since every field of characteristic 0 contains $\mathbb{Q}$ as a subfield).

5 Hilbert's Irreducibility Theorem

We will show that $\mathbb{Q}$ is hilbertian, using the equivalent definition given by Theorem 4.2(ii). The concept of a *sparse* set will be useful.

Definition 5.1 *Let $M \subset \mathbb{N}$. We say that M is* sparse *if there is a real number $\epsilon < 1$ such that*

$$|M \cap \{1, \ldots, N\}| \leqslant N^{\epsilon}$$

for almost all N.

The next theorem gives a few properties of sparse sets. Property (iii) is particularly useful, as it shows that the complement of a sparse set is infinite.

Theorem 5.2 *The following holds:*

(i) Finite sets are sparse.

(ii) Finite unions of sparse sets are sparse.

(iii) If M is sparse, then $M^c := \mathbb{N} \backslash M$ is not sparse.

Proof.

(i) Clear.

(ii) Let $U_1, \ldots, U_n$ be sparse and let $\epsilon_1, \ldots, \epsilon_n < 1$ be corresponding real numbers as in the definition. Let $U = \cup_{i=1}^{n} U_i$. Then, for almost all N,

$$\begin{aligned} |U \cap \{1, \ldots, N\}| &= |\cup_{i=1}^{n} (U_i \cap \{1, \ldots, N\}| \\ &\leqslant \sum_{i=1}^{n} |U_i \cap \{1, \ldots, N\}| \\ &\leqslant \sum_{i=1}^{n} N^{\epsilon_i} \\ &\leqslant nN^{\alpha} \end{aligned}$$

where $\alpha = \max_i\{\epsilon_i\}$. Now, if $N > n^{\frac{2}{1-\alpha}}$, then

$$\begin{aligned} N^{\frac{1-\alpha}{2}} &> n \\ \implies N^{\alpha} N^{\frac{1-\alpha}{2}} &> nN^{\alpha} \\ \implies N^{\frac{1+\alpha}{2}} &> nN^{\alpha}, \end{aligned}$$

showing that U is sparse, with $\epsilon = \frac{1+\alpha}{2} < 1$.

(iii) Suppose that both M and M^c are sparse and let $\epsilon_1, \epsilon_2 < 1$ be such that $|M \cap \{1, \ldots, N\}| \leqslant N^{\epsilon_1}$ and $|M^c \cap \{1, \ldots, N\}| = N - |M \cap \{1, \ldots, N\}| \leqslant N^{\epsilon_2}$. Adding the inequalities gives $N \leqslant N^{\epsilon_1} + N^{\epsilon_2}$, which is false for all $N > 3^{\frac{1}{1-\epsilon}}$, where $\epsilon = \max\{\epsilon_1, \epsilon_2\}$. Hence M^c is not sparse, and in particular, by part (i), M^c is infinite.

■

Thus, for given polynomials $p_i(x, y)$ over $\mathbb{Q}$ (as in Theorem 4.2(ii)), we have to find infinitely many rational b such that $p_i(b, y)$ have no rational roots. By the above theorem it will suffice to show that the set of all $b \in \mathbb{Q}$ such that some $p_i(b, y)$ has a rational root, is sparse. Theorem 5.5 reduces

the problem to counting rational points on certain analytic curves, which will be addressed by the next theorem.

Recall that any analytic function can be expressed as a Laurant series over $\mathbb{C}$ ([11], §5.5). The theorem uses a generalised mean value theorem by H. A. Schwarz, which is proved in the appendix (Theorem 5.3).

Theorem 5.3 *Let $i_0 \in \mathbb{Z}$ and let*

$$\phi(t) = \sum_{i=i_0}^{\infty} a_i t^i$$

be a Laurant series with complex coefficients, converging for all nonzero t in a neighbourhood of 0 in $\mathbb{C}$. Let $B(\phi)$ be the set of all $b \in \mathbb{N}$ for which $\phi(\frac{1}{b})$ is an integer. Then $B(\phi)$ is a sparse set unless ϕ is a Laurant polynomial.

Proof. Assume that $\phi(t)$ is not a Laurant polynomial. If $B(\phi)$ is finite, we are done, so assume that it is infinite.

Now, the series defined by

$$\overline{\phi}(t) = \sum_{i=i_0}^{\infty} \overline{a_i} t^i$$

has the same radius of convergence as ϕ. Also, for each $b \in B(\phi)$, $\phi(\frac{1}{b}) = \overline{\phi}(\frac{1}{b})$. Since $B(\phi)$ is infinite and $i_0 \in \mathbb{Z}$, $\phi = \overline{\phi}$. Hence the coefficients of ϕ are real.

Thus the function $f(s) := \phi(\frac{1}{s}) = \sum_{i=i_0}^{\infty} a_i s^{-i}$ is real-valued and defined for large values of s.

Recall that $B(\phi)$ consists of all integers b such that $\phi(\frac{1}{b}) = f(b)$ is an integer. To show that $B(\phi)$ is sparse, we will show that it is a union of sparse sets, and the result will follow from Theorem 5.2. A step in this direction

is the observation that if $b_1 < b_2 < \dots$ is an infinite sequence of positive integers with $b_{i+1} - b_i \geqslant b_i^\lambda$ for some $\lambda > 0$, then the set $B = \{b_1, b_2, \dots\}$ is sparse.

Indeed, for each positive integer N, let N_0 be the number of integers $b \in B$ with $\sqrt{N} < b \leqslant N$. For a particular N, let $b_{\alpha+1}, \dots, b_{\alpha+N_0}$ be the elements b of B satisfying $\sqrt{N} < b \leqslant N$. Then

$$\begin{aligned} b_{\alpha+2} - b_{\alpha+1} &\geqslant b_{\alpha+1}^\lambda > \sqrt{N}^\lambda \\ b_{\alpha+3} - b_{\alpha+2} &\geqslant b_{\alpha+2}^\lambda > \sqrt{N}^\lambda \\ \vdots &\quad \vdots \\ b_{\alpha+N_0} - b_{\alpha+N_0-1} &\geqslant b_{\alpha+N_0-1}^\lambda > \sqrt{N}^\lambda. \end{aligned}$$

Adding the $N_0 - 1$ inequalities yield

$$(N_0 - 1)\sqrt{N}^\lambda < b_{\alpha+N_0} - b_{\alpha+1} < N.$$

Hence $N_0 < N^{1-\frac{\lambda}{2}} + 1$. Thus

$$|B \cap \{1, \dots, N\}| \leqslant \sqrt{N} + N_0 < N^{\frac{1}{2}} + N^{1-\frac{\lambda}{2}} + N^0,$$

implying that B is sparse.

While all the elements of $B(\phi)$ may not satisfy the above requirement, we can split it up into a finite number of sets which do. Indeed, there exists a positive λ and natural numbers m and S such that the following holds: Whenever $s_0, \dots, s_m \in \mathbb{Z}$ such that $f(s_0), \dots, f(s_m) \in \mathbb{Z}$ and $S < s_0 < \dots < s_m$, then $s_m - s_0 \geqslant s_0^\lambda$.

For m large enough the series $f^{(m)}(s) = \sum_{i=\mu}^{\infty} d_i s^{-i}$ has only terms with negative powers of s,i.e., $\mu > 0$. Since ϕ is not a Laurant polynomial, we

may assume that $d_\mu \neq 0$. Then $s^\mu f^{(m)}(s)$ tends to d_μ as s goes to infinity. Hence there exists an $S > 0$ such that $0 < |s^\mu f^{(m)}(s)| < 2|d_\mu|$ for all $s > S$.

Now assume that $s_0, \ldots, s_m$ are as in the hypothesis. Let σ be a real number as in Theorem A.2 satisfying $S < s_0 \leqslant \sigma \leqslant s_m$. Then $\frac{V_m f^{(m)}(\sigma)}{m!}$ is the determinant of a matrix with integral entries, hence a nonzero integer (nonzero since $|\sigma^\mu f^{(m)}(\sigma)| > 0$). It follows that $V_m \geqslant \frac{m!}{|f^{(m)}(\sigma)|}$, and so

$$\begin{aligned}
(s_m - s_0)^{\frac{m(m+1)}{2}} &\geqslant \prod_{i>j}(s_i - s_j) \\
&= V_m \\
&\geqslant \frac{m!}{|f^{(m)}(\sigma)|} \\
&\geqslant \frac{m!\sigma^\mu}{2|d_{mu}|} \qquad \text{(since } |\sigma^\mu f^{(m)}(\sigma)| < 2|d_\mu|\text{)} \\
&\geqslant \frac{m!s_0^\mu}{2|d_\mu|}.
\end{aligned}$$

Hence

$$s_m - s_0 \geqslant \left(\frac{m!}{2|d_\mu|}\right)^{\frac{2}{m(m+1)}} s_0^{\frac{2\mu}{m(m+1)}}.$$

Thus any $\lambda < \frac{2\mu}{m(m+1)}$ is sufficient (possibly having to choose a larger S).

Now, $B(\phi)$ is the union of the finite (hence sparse) set of elements less than S, and m infinite sparse sets. Hence $B(\phi)$ is sparse. ■

We now show that the roots of a seperable polynomial are (locally) analytic functions of its coefficients. First we prove a little lemma that will be used in the main result.

Lemma 5.4 *If $g(x, y) = \sum_{i,j\geqslant 0}^{\infty} a_{ij}x^i y^j$ is a Taylor series with no constant term and no y term (i.e. $a_{00} = a_{01} = 0$) with complex coefficients such that*

$|a_{ij}| < C$ for some positive constant C, then there exists a Taylor series $\varphi(t) = \sum_{i=1}^{\infty} b_i t^i$ with complex coefficients such that $g(t, \varphi(t)) = \varphi(t)$ for all t in a neighbourhood of 0.

Proof. Since g has no constant and y term, the equation $g(t, \varphi(t)) = \varphi(t)$ allows us to solve for the coefficients b_i recursively (remember that $a_{00} = a_{01} = 0$):

$$\begin{aligned} \varphi(t) &= g(t, \varphi(t)) \\ \implies \sum_{i=1}^{\infty} b_i t^i &= \sum_{i,j \geqslant 0} a_{ij} t^i \left(\sum_{k=1}^{\infty} b_k t^k \right)^j \\ \implies b_1 &= a_{10} \\ b_2 &= a_{11} b_1 \\ b_3 &= a_{11} b_2 + a_{12} b_1^2 + a_{21} b_1, \end{aligned}$$

and so on. Hence φ exists, and we need to prove that it has a positive radius of convergence.

Note that each b_i is a polynomial, *with positive integer coefficients*, in the coefficients a_{ij} and b_j with $j < i$, and since $b_1 = a_{10}$, it follows inductively that each b_i is a polyniomial, with positive integer coefficients, in the coefficients of g.

Hence, if we apply the above the the specific polynomial g_0 with $a_{ij} = C$ for all $i, j \geqslant 0$ (other than $a_{00} = a_{01} = 0$ to solve for the function $\varphi_0(t) = \sum_{i=1}^{\infty} c_i t^i$, we will have that $|b_i| \leqslant |c_i|$ for each i. Hence, if φ_0 has a positive radius of convergence, so will φ.

Now,

$$\begin{aligned} g_0(t,u) = C(t + t^2 + tu + u^2 + \dots) & \\ &= C\left(\sum_{i,j\geqslant 0} t^i u^j - 1 - u\right) \\ &= C\left[\left(\sum_{i=0}^{\infty} t^i\right)\left(\sum_{j=0}^{\infty} u^j\right) - 1 - u\right] \\ &= C\left(\frac{1}{(1-t)(1-u)} - 1 - u\right) \end{aligned}$$

for all $|t| < 1$ and $|u| < 1$. We now solve the equation $g_0(t,u) = u$ for u to obtain

$$u(t) = \frac{1}{2(C+1)}\left(1 \pm \frac{\sqrt{(1+2C)^2t^2 - (1+(1+2C)^2)t + 1}}{1-t}\right).$$

Since $\varphi_0(0) = 0$, it follows that

$$\varphi_0(t) = \frac{1}{2(C+1)}\left(1 - \frac{\sqrt{(1+2C)^2t^2 - (1+(1+2C)^2)t + 1}}{1-t}\right)$$

solves the equation $\varphi_0(t) = g_0(t, \varphi_0(t))$ for all $|t| < 1$, $|\varphi(t)| < 1$. Since $\varphi_0(0) = 0$, φ_0 has a positive radius of convergence. ■

The next theorem actually follows directly from its complex-analytic analogue on implicit functions, but we present a more algebraic proof, due to Cauchy ([2], Chapter 3, §1).

Theorem 5.5 *Let $f(x,y)$ be a polynomial of positive degree n in y over $\mathbb{C}$. Let $c_0 \in \mathbb{C}$ be such that the polynomial $f(c_0,y)$ is seperable. Then there exist analytic functions $\varphi_1, \dots, \varphi_n$ defined in a neighbourhood U of c_0 such that for each $c \in U$, the polynomial $f(c,y)$ has the n distinct roots $\varphi_1(c), \dots, \varphi_n(c)$.*

Proof. Let α be a root of $f(c_0, y)$. By replacing x with $x - c_0$ and y with $y - \alpha$ we can assume that $c_0 = \alpha = 0$. Thus we need to show that there exists an analytic function φ with $\varphi(0) = 0$ and $f(t, \varphi(t)) = 0$ for all t in some neighbourhood of 0.

By hypothesis, $f(0, 0) = 0$, so f has no constant term. Since $f(0, y)$ is seperable $f_y(0, 0)$ is nonzero, implying that f has a y term with non-zero coefficient. Dividing through by this coefficient, we can assume that f has a y term with coefficient 1.

Let $g(x, y) = y - f(x, y)$. Then g has no constant term and no y term. The condition $f(t, \varphi(t)) = 0$ is equivalent to $g(t, \varphi(t)) = \varphi(t)$. By Lemma 5.4, a unique solution for φ exists in some neighbourhood of 0.

If we apply the above for each root of $f(c_0, y)$, we obtain n analytic functions, and since $f(c_0, y)$ is seperable, its roots are distinct, hence for c close enough to c_0, the n functions will all have distinct values on c (since they are analytic). These n functions satisfy the claim. ■

We now set up a situation that will allow use to use the preceding results to prove that $\mathbb{Q}$ is hilbertian.

Theorem 5.6 *Let $p(x, y) \in \mathbb{Q}[x, y]$ be irreducible over $\mathbb{Q}(x)$ and of degree $r > 1$ in y. Then for almost all $x_0 \in \mathbb{Q}$ the following holds:*

(i) There are $\epsilon > 0$ and analytic functions $\varphi_1(t), \ldots, \varphi_r(t)$ defined for complex t with $|t| < \epsilon$ such that $\varphi_1(t), \ldots, \varphi_r(t)$ are the roots of the polynomial $p(x_0 + t, y)$.

(ii) If some $\varphi_i(t)$ is a rational function of t with complex coefficients, then

there are only finitely many $q \in \mathbb{Q}$ such that $\varphi_i(q) \in \mathbb{Q}$.

(iii) Let $B(p, x_0)$ be the set of all $b \in \mathbb{N}$ such that $p(x_0 + \frac{1}{b}, y)$ has a rational root. Then $B(p, x_0)$ is a sparse set.

Proof. The polynomial p is irreducible, hence seperable over $\mathbb{Q}(x)$, and hence, by Theorem 3.2, $p(x_0, y)$ is seperable for almost all $x_0 \in \mathbb{Q}$. Consider only such x_0 in the following.

(i) Follows from Theorem 5.5, by replacing t with $t - x_0$.

(ii) Suppose $\varphi := \varphi_i$ is a rational function of t. Then $p(x_0 + t, \varphi(t))$ is identically zero in $\mathbb{C}(t)$. Hence $p(x_0 + x, \varphi(x))$ is identically zero in $\mathbb{C}(x)$, for x transcendental over $\mathbb{C}$. Thus $\varphi(x)$ is a root of the polynomial $p(x_0 + x, y) \in \mathbb{Q}(x)[y]$, showing that $\varphi(x)$ is algebraic over $\mathbb{Q}(x)$, hence over $\overline{\mathbb{Q}}(x)$. By Theorem 2.3(ii), with $k = \mathbb{Q}$ and $k_1 = \mathbb{C}$, any irreducible polynomial over $\overline{\mathbb{Q}}(x)$ is also irreducible over $\mathbb{C}(x)$. Hence $\overline{\mathbb{Q}}(x)$ is algebraically closed in $\mathbb{C}(x)$.

Now, for each $\tau \in G(\overline{\mathbb{Q}}/\mathbb{Q})$, consider the rational function φ^τ obtained by applying τ to the coefficients ofφ. For each $b \in \mathbb{Q}$ with $\varphi(b) \in \mathbb{Q}$, $\varphi^\tau(b) = \varphi(b)$. If there are infinitely many such b, then $\varphi^\tau = \varphi$ for all τ, hence φ has rational coefficients. Then $\varphi(x - x_0) \in \mathbb{Q}(x)$ is a root of the polynomial $p(x, y)$, contradicing that p is irreducible over $Q(x)$.

(iii) By multiplying p with a suitable integer, we may assume that $p(x, y) \in \mathbb{Z}[x, y]$. Write $p(x, y) = \sum_{i=1}^{r} p_i(x) y^i$. For sufficiently large R, the

expression

$$x^R p\left(x_0 + \frac{1}{x}, y\right) = \sum_{i=1}^{r} x^R p_i\left(x_0 + \frac{1}{x}\right) y^i$$

is a polynomial with integer coefficients. Let its y^i coefficient be denoted by $q_i(x) = x^R p_i\left(x_0 + \frac{1}{x}\right)$. Then q_r is a nonzero element of $\mathbb{Z}[x]$.

Define

$$q(x, Y) = Y^r + \sum_{i=0}^{r-1} q_i(x) q_r(x)^{r-i-1} Y^i \in \mathbb{Z}[x, Y]$$

in the same fashion as in Theorem 2.1.

Now suppose that for some $c \in \mathbb{Q}$ and $b \in \mathbb{N}$, $p(x_0 + \frac{1}{b}, c) = 0$. Then, as in the proof of Theorem 2.1, $q(b, q_r(b)c) = 0$. Hence $q_r(b)c$ is a rational root of the monic polynomial $q(b, Y) \in \mathbb{Z}[Y]$, implying that $q_r(b)c \in \mathbb{Z}$.

If we assume that $\frac{1}{b} < \epsilon$, then $c = \varphi_i(\frac{1}{b})$ for some i, by (i). Thus $q_r(b)\varphi_i(\frac{1}{b}) \in \mathbb{Z}$.

Let $\phi_i(t) = q_r(\frac{1}{t})\varphi_i(t)$. By the above, if $b \in B(p, x_0)$, then $\phi_i(\frac{1}{b}) \in \mathbb{Z}$ for some i. Let $B(\phi_i)$ be the set of all $b \in \mathbb{N}$ such that $\phi_i(\frac{1}{b}) \in \mathbb{Z}$, as in Theorem 5.3 (note that ϕ_i can be expressed as a Laurant series as in Theorem 5.3, since $\varphi_i(t)$ is analytic and $q_r(\frac{1}{t})$ is a rational function in t, by [11], §5.6). Then $B(p, x_0)$ lies in the union of the sets $B(\phi_i)$. By Theorem 5.3, $B(\phi_i)$ is sparse, unless ϕ_i is a Laurant polynomial, hence a rational function of t. If so, φ_i is also a rational function, hence $B(\phi_i)$ is finite by (ii). Theorem 5.2 now shows that $B(p, x_0)$ is sparse.

■

Finally, we prove the main result:

Theorem 5.7 (Hilbert's Irreducibility Theorem) *The field $\mathbb{Q}$ is hilbertian.*

Proof. Let $p_i(x, y) \in \mathbb{Q}[x, y]$ be as in condition (iii) of Theorem 4.2. By Theorem 5.6, we can choose $x_0 \in \mathbb{Q}$ such that (i)-(iii) of Theorem 5.6 hold for all p_i. Let C be the set of all $b \in \mathbb{N}$ such that none of the specialised polynomials $p_i(x_0 + \frac{1}{b}, y)$ has a root in $\mathbb{N}$. We will show that C is infinite.

Let $B = \mathbb{N} \backslash C$. Then B contains all $b \in \mathbb{N}$ such that for some i, $p_i(x_0 + \frac{1}{b}, y)$ has a rational root, hence B is the union of the sets $B(p_i, x_0)$ as in Theorem 5.6(iii). These sets are sparse, hence by Theorem 5.2 B is sparse, and so C is infinite. ■

6 Weissauer's Theorem

By the remarks preceding definition 4.3, every finitely generated extension of a hilbertian field is also hilbertian. This is complemented by Weissauer's theorem, which addresses infinite extensions of a hilbertian field. We present the outline of a proof given by Fried in [4], which is more algebraic than the original proof of Weissauer in [15].

The next theorem is used in the proof of Weissauer's theorem. We omit the proof, as it is similar to the proof of Theorem 3.3.

Theorem 6.1 *Let k be a hilbertian field, and let ℓ be a finite extension of k. Let $A(y), B(y) \in \ell[x_1, x_2][y]$ be monic polynomials in y, where x_1 and x_2 are algebraically independant over ℓ. Suppose that A has no root in a splitting field of B over $\ell(x_1, x_2)$. Then for any nonzero $v \in \ell[x_1, x_2]$, there exist $b_1, b_2 \in k$ with $v(b_1, b_2) \neq 0$ such that $A(b_1, b_2, y)$ has no root in a splitting field of $B(b_1, b_2, y)$ over ℓ.*

Theorem 6.2 (Weissauer's Theorem) *Let k be hilbertian, let N be a (possibly infinite) Galois extension of k, and let M be a finite non-trivial extension of N. Then M is hilbertian.*

Outline of proof. We use condition (ii) in Theorem 4.2. Let $p_i(x, y) \in M[x, y]$ be distinct polynomials, monic and of degree greater than 1 in y (we may assume each p_i monic by Theorem 2.1). Let $p(x, y)$ be the product of all the p_i. We thus need to show that there are infinitely many $b \in M$ such that $p(b, y)$ has no root in M.

If some $p_i(x,y)$ has a root $g(x) \in \overline{M}(x)$, then all its roots lie in $\overline{M}(x)$ (since $\overline{M}(x)$ is Galois over $M(x)$), and hence we may write $p_i(x,y) = \prod_i (y - g_i(x))$ with each $g_i \in \overline{M}(x) \backslash M(x)$ (since p_i is irreducible over $M(x)$). Using the same argument as in Theorem 5.6(ii), there are only finitely many $b \in M$ such that $g_i(b) \in M$, hence there are only finitely many $b \in M$ such that the root $g_i(b)$ of $p_i(b,y)$ lie in M. Thus we may assume such a $g(x)$ doesn't exist for any of the p_i and so we may assume that $p(x,y)$ doesn't have a root in $\overline{M}(x)$.

Let α be a generator of M over N, and let ℓ be a finite Galois extension of k containing α and the coefficients of p over M. Let β be a conjugate of α over $\ell \cap N$. Now consider the polynomials $A(y) = p(x_1 + \alpha x_2, y)$ and $B(y) = p(x_1 + \beta x_2, y)$ over $\ell[x_1, x_2]$. Using the assumption that p doesn't have a root in $\overline{M}(x) = \overline{\ell}(x)$, we show that $A(y)$ doesn't have a root in a splitting field of $B(y)$.

Next, let $\mathbb{M}$ be the composite of N and ℓ. Then, if F is a finite Galois extension of ℓ contained in $\mathbb{M}$, then F is galois over $N \cap \ell$. For each $b_1, b_2 \in k$, consider the polynomials $A_{b_1 b_2} = p(b_1 + \alpha b_2, y)$ and $B_{b_1 b_2} = p(b_1 + \beta b_2, y)$, and suppose that $A_{b_1 b_2}$ has the roots $\gamma_1, \ldots, \gamma_m$ in $\mathbb{M}$. Using the fact that $\ell(\gamma_1, \ldots, \gamma_m)$ is Galois over $N \cap \ell$, we conclude that the roots $\gamma_1, \ldots, \gamma_m$ lie in a splitting field of $B_{b_1 b_2}$ over ℓ.

Finally, using Theorem 6.1 and the above, we conclude that there are infinitely many $b_1, b_2 \in k$ such that $A_{b_1 b_2}$ has no root in the splitting field of $B_{b_1 b_2}$. In those cases, the polynomial $A_{b_1 b_2} = p(b_1 + \alpha b_2, y)$ cannot have any roots in $\mathbb{M} \supset M$. Hence there are infinitely many elements $b = b_1 + \alpha b_2$ such that $p(b,y)$ has no root in M, as desired.

A result similar to Weissauer's theorem was proved in 1991 by Haran and Jarden [5]:

Theorem 6.3 *If N and L are (possibly infinte) Galois extensions of a hilbertian field k such that none of the two is contained in the other, then the compositum of N and L over k is hilbertian.*

7 Examples & applications

7.1 Realisations over $\mathbb{Q}$

Finite abelian groups

Theorem 7.1 *Every finite abelian group G occurs as a Galois group over $\mathbb{Q}$. In fact, G is realised as the Galois group of some subfield of the cyclotomic extension $\mathbb{Q}(\omega_n)$, where ω_n is an n^{th} root of unity, for some natural number n.*

Proof. Let $\mathbb{Z}_n$ be a cyclic group of order n. Let $p > 4$ be a prime number of the form $an + 1$, where a is some positive integer (such a prime exists, by Dirichelet's theorem, which states that every arithmetic progression $an + b$, with a and b relatively prime, contains infinitely many primes). Let $f(x) = \frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i$ be the p^{th} cyclotomic polynomial. It is known that f is irreducible over $\mathbb{Q}$. Indeed, the polynomial

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{\sum_{i=0}^{p} \binom{p}{i} x^i - 1}{x} \\ &= \sum_{i=1}^{p} \binom{p}{i} x^{i-1} \\ &= x^{p-1} + px^{p-2} + \sum_{i=2}^{p-2} \binom{p}{i} x^{i-1} + p \end{aligned}$$

is irreducible by Eisenstein's Criterion ([8], Chapter 4, Theorem 3.1).

Let ω_p be a primitive p^{th} root of unity. Since p is prime, all the p^{th} roots of unity are given by the first p powers of ω_p, hence the cyclotomic extension

$F = \mathbb{Q}(\omega_p)$ contains all the roots of f. Thus F is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_{p-1}$ ([8], Chapter 6, Theorem 3.1). Since n divides $p-1$, there exists a cyclic subgroup H of $\mathbb{Z}_{p-1}$ with order $\frac{p-1}{n}$. Let E be the fixed field of H, which is certainly normal in $\mathbb{Z}_{p-1}$. Hence E is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_{p-1}/H$ ([8], Chapter 6, Theorem 1.1), which is isomorphic to $\mathbb{Z}_n$

If p and q are relatively prime integers, then $\mathbb{Q}(\omega_p) \cap \mathbb{Q}(\omega_q) = \mathbb{Q}$. Hence, for any given m and n, one can construct infinitely many Galois extensions K and L of $\mathbb{Q}$ with Galois groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively, such that $K \cap L = \mathbb{Q}$. By the above construction, K and L are subfields of $\mathbb{Q}(\omega_p)$ and $\mathbb{Q}(\omega_q)$ for some relatively primes integers p and q, respectively, and thus the compositum of K and L is contained in the compositum of $\mathbb{Q}(\omega_p)$ and $\mathbb{Q}(\omega_q)$, which is contained in the field $\mathbb{Q}(\omega_{pq})$.

By theorem 1.14 in chapter 6 of [8], the compositum KL is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_m \times \mathbb{Z}_n$, contained in the cyclotomic extension $\mathbb{Q}(\omega_{pq})$.

By the Fundemental Theorem of Finitely Generated Abelian Groups ([3], Theorem 2.4.12) every finite abelian group can be written as a direct product of finitely many cyclic groups. Iterating the above construction shows that every finite abelian group occurs over $\mathbb{Q}$ as the Galois group of some subfield of $\mathbb{Q}(\omega_n)$ over $\mathbb{Q}$, for some natural number n. ■

The permutation group S_n

Let $\mathbb{Q}(\mathbf{x}) = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ where $x_1, \ldots, x_n$ are independant transcendentals over $\mathbb{Q}$. Consider the polynomial

$$f(y) = y^n + x_1 y^{n-1} + \cdots + x_{n-1} y + x_n \in \mathbb{Q}(\mathbf{x})[y],$$

with roots $t_1, t_2, \ldots, t_n$. Every element $\sigma \in S_n$ can be seen as an automorphism of the field $\mathbb{Q}(t_1, t_2, \ldots, t_n)$, by fixing $\mathbb{Q}$ and permuting the t_i. Let F be the fixed field of S_n in $\mathbb{Q}(t_1, \ldots, t_n)$.

Note that since each x_i is a symmetric polynomial in the t_i, $x_i \in F$ for each i, hence $\mathbb{Q}(\mathbf{x}) \subset F$.

Now, by Artin's theorem, $\mathbb{Q}(t_1, \ldots, t_n)$ is a Galois extension of F with Galois group S_n, hence $[\mathbb{Q}(t_1, \ldots, t_n) : F] = |S_n| = n!$. Since $t_1, \ldots, t_n$ are the roots of a polynomial of degree n, it follows that $[\mathbb{Q}(t_1, \ldots, t_n) : \mathbb{Q}(\mathbf{x})] \leqslant n!$. Now, since F is an extension of $\mathbb{Q}(\mathbf{x})$, we have that

$$[\mathbb{Q}(t_1, \ldots, t_n) : F][F : \mathbb{Q}(\mathbf{x})] = [\mathbb{Q}(t_1, \ldots, t_n) : \mathbb{Q}(\mathbf{x})],$$

implying that $[F : \mathbb{Q}(\mathbf{x})] \leqslant 1$, hence $F = \mathbb{Q}(\mathbf{x})$. Thus S_n occurs regularly over $\mathbb{Q}$, and since $\mathbb{Q}$ is hilbertian, S_n occurs over $\mathbb{Q}$.

7.2 Hilbertian fields

The field $\mathbb{Q}^{\mathrm{ab}}$ is hilbertian

Let $N = \mathbb{Q}^{\mathrm{ab}} \cap \mathbb{R}$, where $\mathbb{Q}^{\mathrm{ab}}$ is the field generated over $\mathbb{Q}$ by all the primitive n^{th} roots of unity, for all $n \in \mathbb{N}$.

Now, if $z = a + ib \in \mathbb{Q}^{\text{ab}}$, then $\overline{z} = a - ib \in \mathbb{Q}^{\text{ab}}$ (since if ω is a primitive root of unity, then so is $\overline{\omega}$), and certainly $i \in \mathbb{Q}^{\text{ab}}$. Hence $a = \frac{z+\overline{z}}{2}$ and $b = \frac{z-\overline{z}}{2i}$ are in $\mathbb{Q}^{\text{ab}}$. Hence $\mathbb{Q}^{\text{ab}} = N(i)$. To apply Weissauer's theorem, we need to show that N is a Galois extension of $\mathbb{Q}$.

However, $\mathbb{Q}^{\text{ab}}$ is an abelian Galois extension of $\mathbb{Q}$ ([8], §14). Hence every subfield of $\mathbb{Q}^{\text{ab}}$, in particular N, is Galois over $\mathbb{Q}$.

The algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ is not hilbertian

Let $f(x, y)$ be any irreducible polynomial over $\overline{\mathbb{Q}}(x)$ with degree greater than 2 in y (e.g. $f(x, y) = y^n - x$. Since $\overline{\mathbb{Q}}$ is algebraically closed, $f(b, y)$ splits into linear factors for every $b \in \overline{\mathbb{Q}}$. Hence $\overline{\mathbb{Q}}$ is not hilbertian.

This example shows that the condition $N \neq M$ in Weissauer's Theorem cannot be omitted.

The solvable closure $\mathbb{Q}^{\text{solv}}$ of $\mathbb{Q}$ is not hilbertian

Since $\mathbb{Q}^{\text{solv}}$ is the compositum of all finite solvable extensions over $\mathbb{Q}$, it consists of all iterated radicals over the rationals. Hence, if $b \in \mathbb{Q}^{\text{solv}}$, then so is $\sqrt[n]{b}$ for each n. The polynomial $f(x, y) = y^n - x$ is irreducible over $\mathbb{Q}^{\text{solv}}(x)$, but $f(b, y)$ has a root in $\mathbb{Q}^{\text{solv}}$ for each $b \in \mathbb{Q}^{\text{solv}}$. Hence $\mathbb{Q}^{\text{solv}}$ is not hilbertian.

The field M generated over $\mathbb{Q}$ by the set $\{\sqrt{n}\}_{n>1}$ is hilbertian

Let N be the field generated over $\mathbb{Q}$ by the set $\{\sqrt{p}\}$, where p ranges over the odd primes. Then $M = N(\sqrt{2})$, hence to apply Wieissauer's theorem, I

need to show that N is Galois over $\mathbb{Q}$. But N is the splitting field of the set of polynomials $\{f(x) = x^2 - p\}$, where p ranges over the odd primes, hence it is Galois over $\mathbb{Q}$.

A Appendix

A few of the results used in this dissertation have non-algebraic proofs, which we present here.

Theorem A.1 *For $m \geqslant 1$ and complex numbers $s_0, s_1, \ldots, s_m$, define the* Vandermonde determinant V_m *by*

$$V_m = \begin{vmatrix} 1 & s_0 & s_0^2 & \ldots & s_0^m \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & s_m & s_m^2 & \ldots & s_m^m \end{vmatrix}. \tag{1}$$

Then we have the equality

$$V_m = \prod_{0 \leqslant j < i \leqslant m} (s_i - s_j). \tag{2}$$

Proof. We prove the assertion by induction on m. We have

$$\begin{aligned} V_1 &= \begin{vmatrix} 1 & s_0 \\ 1 & s_1 \end{vmatrix} \\ &= s_1 - s_0 \\ &= \prod_{0 \leqslant j < i \leqslant 1} (s_i - s_j), \end{aligned}$$

hence the statement is true for $m = 1$. Now, for some $m > 1$, suppose that the assertion is true for all integers less than m.

If $s_i = s_j$ for any $i \neq j$, then rows i and j in (1) are equal, and hence $V_m = 0$. This implies that $(s_i - s_j)$ divides V_m for each $i \neq j$, and thus the expression in (2) divides V_m.

Next, write both expressions as polynomials in s_m. Firstly, we see that the degree of the polynomial in (1) is m. In (2), the degree of the polynomial is

equal to the number of brackets containing s_m, which is equal to the number of integers $0 \leqslant j < m$, which is also m. Hence expression (2) is a constant multiple of V_m.

Now, by the induction hypothesis,

$$\begin{aligned}\prod_{0\leqslant j<i\leqslant m}(s_i - s_j) &= \left[\prod_{0\leqslant j<i\leqslant m-1}(s_i - s_j)\right](s_m - s_0)(s_m - s_1)\dots(s_m - s_{m-1}) \\ &= V_{m-1}(s_m - s_0)(s_m - s_1)\dots(s_m - s_{m-1}),\end{aligned}$$

which shows that the coefficient of s_m^m in (2) is equal to V_{m-1}. Developing V_m by the last row (or column) shows that the coefficient of s_m^m in (1) is also equal to V_m. Hence the required equality. ■

Theorem A.2 *Let $s_0 < s_1 < \cdots < s_m$ be real numbers, where $m \geqslant 1$. Let $f(x)$ be a real-valued function defined function defined for $s_0 \leqslant x \leqslant s_m$ and m times continuously differentiable. Let V_m be the Vandermonde determinant*

$$V_m = \begin{vmatrix} 1 & s_0 & s_0^2 & \dots & s_0^m \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & s_m & s_m^2 & \dots & s_m^m \end{vmatrix} = \prod_{j<i}(s_i - s_j).$$

Then there exists a number σ with $s_0 < \sigma < s_m$ such that

$$\frac{f^{(m)}(\sigma)}{m!} = \frac{1}{V_m}\begin{vmatrix} 1 & s_0 & \dots & s_0^{m-1} & f(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_m & \dots & s_m^{m-1} & f(s_m) \end{vmatrix}.$$

Proof. Let $F(s)$ be the function

$$F(s) = \begin{vmatrix} 1 & s_0 & \dots & s_0^{m-1} & f(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_{m-1} & \dots & s_{m-1}^{m-1} & f(s_{m-1}) \\ 1 & s & \dots & s^{m-1} & f(s) \end{vmatrix}.$$

Let

$$c = \frac{F(s_m)}{(s_m - s_0)\dots(s_m - s_{m-1})}$$

and

$$G(s) = F(s) - c(s - s_0)\dots(s - s_{m-1}).$$

The function $G(s)$ is zero at the $m+1$ points $s_0, \dots, s_m$. Hence $G^{(m)}(s)$ is zero at least at one point σ between s_0 and s_m. Hence $G^{(m)}(\sigma) = F^{(m)}(\sigma) - m!c = 0$, giving $F^{(m)}(\sigma) = m!c$.

On the other hand, expanding the determinant $F(s)$ by the last row, we get

$$F(s) = \sum_{i=0}^{m-1} c_i s^i + V_{m-1} f(s),$$

where the c_i are constants depending on the s_i. Hence $F^{(m)}(\sigma) = V_{m-1} f^{(m)}(\sigma)$. Comparing the two expressions for $F^{(m)}(\sigma)$, we obtain

$$\frac{f^{(m)}(\sigma)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0)\dots(s_m - s_{m-1})V_{m-1}} = \frac{F(s_m)}{V_m}.$$

The results follows from the definition of $F(s_m)$. ■

References

[1] EDWARDS, H. M., *Galois Theory*, Springer, 1984

[2] EICHLER, M., *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, New York, 1966

[3] FRALEIGH, J. B., *A First Course in Abstract Algebra*, Addison Wesley Longman, sixth edition, 1998

[4] FRIED, M., On the Sprindzuk-Weissauer approach to universal Hilbert subsets. *Isreal J. Math.* **51**, 347 - 363 (1985)

[5] HARAN, D., JARDEN, M., Compositum of Galois extensions of hilbertian fields. *Ann. scient. Éc. Norm. Sup.* **24**, 739 - 748 (1991)

[6] HILBERT, D., Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. *J. reine angew. Math.* **110**, 104-129 (1892)

[7] JENSEN, C. U., LEDET, A., YUI, N., *Generic Polynomials - Constructive Aspects of the Inverse Galois Problem*, Cambridge University Press, 2002

[8] LANG, S., *Algebra*, Springer, third edition, 2002

[9] MALLE, G., Multi-parameter Polynomials with Given Galois Group, *Journal of Symbolic Computation*, **30**, no 6, 675 - 716 (2000)

[10] MATZAT, B. H., Computational Methods in Constructive Galois Theory, *Trends in computer algebra, Int. Symp., Bad Neuenahr/FRG 1987, Lect. Notes Comput. Sci.* **296**, 137-155 (1988).

[11] SAFF, E. B., SNIDER, D., *Fundementals of Complex Analysis*, Pearson Education, third edition, 2003

[12] ŠAFEREVIČ, I. R., Constructions of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk. SSSR Ser. Mat.* **18**, 525-578 (1954), Amer. Math. Soc. Transl. **4**, 185-237 (1956)

[13] VÖLKEIN, H., *Groups as Galois Groups - an Introduction*, Cambridge University Press, 1996

[14] VÖLKLEIN, H., Inverse Galois Theory - review, *Bull. Amer. Math. Soc.* **38**, 235-243 (2001)

[15] WEISSAUER, R., Der Hilbertsche Irreduzibilitätssatz, *J. reine angew. Math.* **334**, 203-220 (1982)