Hilbertian fields and Hilbert's irreducibility theorem

Rodney Coleman, Laurent Zwald

Hilbertian fields and Hilbert's irreducibility theorem

Rodney Coleman, Laurent Zwald

September 25, 2018

Abstract

Hilbert's irreducibility theorem plays an important role in inverse Galois theory. In this article we introduce Hilbertian fields and present a clear detailed proof of Hilbert's irreducibility theorem in the context of these fields.

An important result in inverse Galois theory is Hilbert's irreducibility theorem. Unfortunately it is difficult to find a clear proof, probably because such a proof requires many detailed steps. Those that we have seen lack important details or have errors and so make reading difficult. For this reason we set out to write a clear, detailed proof, which a reader with a certain mathematical maturity should not find difficult. We will use some basic results from Galois theory, which we detail in an appendix. (The word Result in the text refers to these results.)

We begin by introducing Hilbertian fields. Let $f(X, Y)$ be a nonzero polynomial in two variables over a field F. Collecting monomials having the same power of Y, we may write

$$f(X, Y) = a_0(X) + a_1(X)Y + a_2(X)Y^2 + \cdots + a_n(X)Y^n,$$

where the $a_i(X)$ are polynomials in X alone and $a_n(X) \neq 0$, i.e., we may consider f as a member of $F[X][Y]$. The number n is the degree of f with respect to Y. We recall that a nonzero element a in an integral domain R is *irreducible* if it is a nonunit and, whenever $a = bc$, either b or c is a unit. As a polynomial ring over an integral domain is an integral domain, $F[X][Y]$ is an integral domain. For reasons which will become obvious further on, we will say that $f \in F[X, Y]$ is irreducible, if f is irreducible as an irreducible element of the ring $F[X][Y]$ and has degree greater than 0 in Y, i.e., the polynomial has at least one monomial containing a power of Y. If a polynomial is not irreducible, then we will say it is reducible.

We may extend this definition to polynomials in more than two variables. If $f \in F[X_1, \ldots, X_k]$, with $k \geq 3$, then we may consider f as an element of $F[X_1, \ldots, X_{k-1}][X_k]$. We will say that f is irreducible if f is irreducible in the polynomial ring $F[X_1, \ldots, X_{k-1}][X_k]$ and has degree greater than 0 in X_k. (This definition is not entirely satisfactory, because it depends on which variable we set in the last position.)

Let $f \in F[X, Y]$ be a polynomial of degree greater than 0 in Y. For every $b \in F$, we may define a polynomial $f_b \in F[Y]$ by setting $f_b(Y) = f(b, Y)$. If $a_n(b) \neq 0$, then f_b has n roots, counted according to their multiplicity. If these roots are distincts, then we say that b is a regular value.

Proposition 1 *Let $f(X, Y)$ be a polynomial of degree greater than 0 in Y over a field F of characteristic 0. Then all but a finite number of values $b \in F$ are regular.*

PROOF If we eliminate those values of b, which are roots of the leading coefficient a_n, then the polynomial f_b has a positive degree. We now consider f as an element of $F(X)[Y]$ and it is

1

not difficult to see that $\Delta(f)(b) = \Delta(f_b)$, where $\Delta(f)$ (resp. $\Delta(f_b)$) denotes the discriminant of f (resp. f_b). As $\Delta(f)$ is a polynomial with coefficients in $F(X)$, there is a finite number of elements u of $F(X)$ for which $\Delta(f)(u) = 0$; in particular, there is a finite number of values of $b \in F$ for which $\Delta(f)(b) = 0$. If exclude these values, then $\Delta(f_b) = \Delta(f)(b) \neq 0$, i.e., b is regular. $\square$

We may now define the notion of a Hilbertian field. If for any $f \in F[X, Y]$ which is irreducible, there exists an infinite number of values of $b \in F$ such that $f_b(Y) = f(b, Y) \in F[Y]$ is irreducible, then we say that the field F is Hilbertian. We say that f_b is a specialization of F. Clearly a finite field cannot be Hilbertian. This is also the case for a field which is algebraically closed. An important example of a Hilbertian field is that of the rational numbers $\mathbf{Q}$. This is known as Hilbert's irreducibility theorem. We will prove this in Section 4. of the article. For the moment we will consider certain important properties of Hilbertian fields.

1. Properties of Hilbertian fields

In this section we present some technical results, which enable us to illustrate how the notion of a Hilbertian field intervenes in inverse Galois theory. In particular, the aim is to arrive at an important result at the end of the section, namely Theorem 1. It could be useful to look at this theorem before reading the section in detail, this in order to appreciate the direction of the section.

lemHILBERTprop1

Lemma 1 *Let R be an integral domain, S a subring of R and $f, h \in S[X]$, with f monic. If $g \in R[X]$ and $fg = h$, then $g \in S[X]$.*

PROOF As f is monic, there exist $q, r \in S[X]$ such that $h = fq + r$, with $\deg r < \deg f$. We have

$$fq + r = fg \implies r = f(g - q).$$

As R is an integral domain,

$$\deg r = \deg f + \deg(g - q) \implies g - q = 0,$$

because $\deg r < \deg f$. Therefore $g = q \in S[X]$. $\square$

The next preliminary result concerns Galois extensions of fields of fractions and is interesting in its own right.

oposHILBERTprop1

Proposition 2 *Suppose that R is an integral domain and F its field of fractions. In addition, let E be a separable extension of F of degree n. Then there exists $\alpha \in E$ such that $E = F(\alpha)$ and $m(\alpha, F) \in R[X]$.*

PROOF From the primitive element theorem we know that there exists $\beta \in E$ such that $E = F(\beta)$. As F is the field of fractions of R, we may multiply $m = m(\beta, F)$ by a nonzero constant $d \in R$ to obtain $dm \in R[X]$. Setting $\alpha = d\beta$, we have $F(\alpha) = F(\beta)$. We now look for $m(\alpha, F)$. If

$$f(X) = d^n b_0 + d^{n-1} b_1 X + \cdots + d b_{n-1} X^{n-1} + X^n,$$

where

$$m(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} + X^n,$$

then $f \in R[X]$ and

$$f(\alpha) = f(d\beta) = d^n m(\beta) = 0.$$

Also, f is monic and
$$[E : F] = [F(\alpha) : F] = [F(\beta) : F] = n$$

and so f is the minimal polynomial of α over F and $f \in R[X]$. This proves the result. $\qquad \square$

At this point we introduce some notation. If R is a subring of the field F and A a subset of an extension E of F, then we will write $R[A]$ for the subring of E generated by R and A. If A is composed of a single element a, then we will write $R[a]$ for $R[\{a\}]$. From now on we will suppose that rings and fields have characteristic 0. The next result is fundamental.

`lemHILBERTprop2` **Lemma 2** *We take R, F, E, α as in Proposition* `proposHILBERTprop1` *2, with $f = m(\alpha, F) \in R[X]$, and A a finite subset of E containing α such that*

$$\forall x \in A \; \forall \sigma \in Gal(E/F), \; \sigma(x) \in A.$$

Then there exists $u \in R$ such that, for any field F' and ring homomorphism $\omega : R \longrightarrow F'$, with $\omega(u) \neq 0$, we may find a Galois extension E' of F' and a ring homomorphism extension $\tilde{\omega} : R[A] \longrightarrow E'$ of ω with the following properties:

- $E' = F'(\alpha')$, where $\alpha' = \tilde{\omega}(\alpha)$;

- *If $f' \in F'[X]$ is the polynomial obtained from f by applying ω to the coefficients of f and f' is irreducible, then $G' = Gal(E'/F')$ is isomorphic to $G = Gal(E/F)$.*

PROOF The proof of this result is rather long, so we will proceed by steps.

1. Definition of u: Let $u = \Delta(f)$, the discriminant of f. (For a definition of the discriminant, see for example [4]). As $\operatorname{char} F = 0$, because $\operatorname{char} R = 0$, and f is irreducible, f has no multiple root. This implies that $u \neq 0$. If F' is a field and $\omega : R \longrightarrow F'$ a ring homomorphism such that $\omega(u) \neq 0$, then $\Delta(f') = \omega(u) \neq 0$, hence f' is strongly separable.

2. A first extension of R and ω: We now construct a ring $\tilde{R}$, containing R and we extend ω to this ring. As $E = F(\alpha)$ and $A \subset E$, for every $x \in A$, there exists $g_x \in F[X]$ such that $x = g_x(\alpha)$. In addition, F is the field of fractions of R, and so there exists $d_x \in R^*$ such that $d_x g_x \in R[X]$. We now set

$$d = \prod_{x \in A} d_x.$$

Then $dg_x \in R[X]$, for all $x \in A$. We now set

$$\tilde{R} = R[d^{-1}] \subset F$$

and extend ω to $\omega_1 : \tilde{R} \longrightarrow F'$ by setting $\omega_1(d^{-1}) = \omega(u)^{-1}$.

It should be noticed that $\tilde{R}[A] = \tilde{R}[\alpha]$. First, $\alpha \in A$ implies that $\tilde{R}[\alpha] \subset \tilde{R}[A]$. On the other hand, if $x \in A$ and $g_x(X) = \sum_{i=0}^{n} a_i X^i$, with $a_0, \ldots, a_n \in F$, then

$$x = g_x(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \Longrightarrow dx = \sum_{i=0}^{n} \left(\prod_{y \in A, y \neq x} d_y \right) (d_x a_i) \alpha^i,$$

which lies in $R[\alpha]$, because $d_x a_i \in R$, for all i, and $d_y \in R$, for all y. However, $R[\alpha] \subset \tilde{R}[\alpha]$ and $x = d^{-1}(dx) \in \tilde{R}[\alpha]$. Hence, $A \subset \tilde{R}[\alpha]$ and so $\tilde{R}[A] \subset \tilde{R}[\alpha]$.

3

3. $\tilde{R}[X]/(f)$ and $\tilde{R}[\alpha]$ are isomorphic: There is a natural homomorphism from $\tilde{R}[X]$ into $\tilde{R}[\alpha]$:

$$\phi : \tilde{R}[X] \longrightarrow \tilde{R}[\alpha], g \longmapsto g(\alpha).$$

If $h \in \ker \phi$, then there exists $g \in F[X]$ such that $h = fg$, because $f = m(\alpha, F)$. From Lemma 1, $g \in R[X]$, because $\tilde{R}$ is a subring of F. Therefore $\ker \phi \subset (f)$. On the other hand, if $g \in (f)$, then $g(\alpha) = 0$ and so $g \in \ker \phi$. It follows that $\ker \phi = (f)$. As ϕ is surjective, we have an isomorphism

$$\bar{\phi} : \frac{\tilde{R}[X]}{(f)} \longrightarrow \tilde{R}[\alpha].$$

4. Construction of the extension E' of F': Our next task is to construct a Galois extension E' of F' and a ring homomorphism $\tilde{\omega}$ from $\tilde{R}[A]$ into E', extending ω_1 and hence ω. Let g' be an irreducible factor of f' and $\rho : F'[X] :\longrightarrow F'[X]/(g')$ the natural projection. From the homomorphism $\omega_1 : \tilde{R} \longrightarrow F'$ constructed above, we obtain the natural homomorphism $\hat{\omega}_1 : \tilde{R}[X] \longrightarrow F'[X]$. We now compose $\hat{\omega}_1$ with ρ to obtain the homomorphism

$$\rho \circ \hat{\omega}_1 : \tilde{R}[X] \longrightarrow F'[X]/(g')$$

and then use this to define another homomorphism:

$$\gamma : \frac{\tilde{R}[X]}{(f)} \longrightarrow \frac{F'[X]}{(g')}, v + (f) \longmapsto \rho \circ \hat{\omega}_1(v).$$

(As $\rho \circ \hat{\omega}_1(f) = f' + (g')$ and $g'|f'$, we must have $\rho \circ \hat{\omega}_1(v) = 0$, for all $v \in (f)$, hence γ is well-defined.)

Now we set

$$E' = \frac{F'[X]}{(g')} \qquad \text{and} \qquad \tilde{\omega} = \gamma \circ \bar{\phi}^{-1}.$$

As g' is irreducible E' is a field, which is clearly an extension of F'. Also, $\tilde{R}[A] = \tilde{R}[\alpha]$ and so $\tilde{\omega}$ is a homomorphism from $\tilde{R}[A]$ into E'. We need to check that $\tilde{\omega}$ extends ω. If $x \in R \subset \tilde{R}[A]$, then

$$\begin{aligned}
\tilde{\omega}(x) &= \gamma \circ \bar{\phi}^{-1}(x) = \gamma(x + (f)) = \rho \circ \hat{\omega}_1(x) \\
&= \rho(\omega_1(x)) = \rho(\omega(x)) = \omega(x) + (g'),
\end{aligned}$$

therefore $\tilde{\omega}$ extends ω to $\tilde{R}[A]$. If we restrict $\tilde{\omega}$ to $R[A]$, then we have the homomorphism we are looking for, under the conditions that $E' = F'(\alpha')$ and that E' is a Galois extension of F'.

5. $E' = F'(\alpha')$: As

$$\bar{\phi}^{-1}(\alpha) = X + (f)$$

and

$$\gamma(X + (f)) = \rho(\hat{\omega}_1(X)) = \rho(X) = X + (g'),$$

we have

$$\alpha' = \tilde{\omega}(\alpha) = X + (g')$$

and, by Result 2,

$$F'(\alpha') = F'(X + (g')) = \frac{F'[X]}{(g')} = E'.$$

6. E' is a Galois extension of F': As $\mathrm{char}\, F' = 0$, we only need to show that E' is a normal extension of F'. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Since f is irreducible over F and E is a splitting field of f, Theorem 10 ensures that the Galois group $G = G(E/F)$ acts transitively on the roots of f. This implies that the roots of f belong to A, because $\alpha \in A$. Moreover, the roots of f' are $\tilde{\omega}(\alpha_1), \ldots, \tilde{\omega}(\alpha_n)$, since, by the relations between the roots of a polynomial and its coefficients,

$$f'(X) = (-\tilde{\omega}(\alpha_1) + X) \cdots (-\tilde{\omega}(\alpha_n) + X).$$

Consequently,

$$E' = F'(\alpha') = F'(\tilde{\omega}(\alpha_1), \ldots, \tilde{\omega}(\alpha_n))$$

is a splitting field of f' and, by Theorem 7, E' is a normal extension of F'.

7. The special case $g' = f'$: In this case, f' is irreducible. As above, let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. Since $E = F(\alpha)$, from Result 4 there exists a unique $\sigma_i \in G$ such that $\sigma_i(\alpha) = \alpha_i$. Similarly, $\alpha'_1, \ldots, \alpha'_n$ are the conjugates of α' and, since $E' = F'(\alpha')$ and f' is irreducible over F', Result 4 ensures the existence of a unique $\sigma'_i \in G' = Gal(E'/F')$ such that $\sigma'_i(\alpha') = \alpha'_i$.

From Step 1. of our proof (the definition of u), the values of $\alpha_1, \ldots, \alpha_n$ are distinct. Consequently, the automorphisms $\sigma_1, \ldots, \sigma_n$ are different elements of G. Moreover, Result 9 ensures that G has cardinal n. Thus $G = \{\sigma_1, \ldots, \sigma_n\}$. Similarly, since f' is irreducible, G' is of cardinal n and $G' = \{\sigma'_1, \ldots, \sigma'_n\}$.

We now define a mapping Φ from G into G' by setting $\Phi(\sigma_i) = \sigma'_i$. We will prove that this mapping is an isomorphism. First we will show that

$$\forall s \in \tilde{R}[A], \ \forall \sigma_i \in G, \ \ \tilde{\omega}(\sigma_i(s)) = \sigma'_i(\tilde{\omega}(s)). \tag{1}$$

As $\tilde{R}[A] = \tilde{R}[\alpha]$, it is sufficient to prove the identity for α and for the elements of $\tilde{R}$. For α we have

$$\tilde{\omega}(\sigma_i(\alpha) = \tilde{\omega}(\alpha_i) = \alpha'_i = \sigma'_i(\alpha') = \sigma'_i(\tilde{\omega}(\alpha)).$$

If $x \in \tilde{R}$, then $x \in F$, hence

$$\begin{aligned}
\tilde{\omega}(\sigma_i(x)) &= \tilde{\omega}(x) = \gamma \circ \bar{\phi}^{-1}(x) = \gamma(x + (f)) = \rho \circ \hat{\omega}_1(x) \\
&= \hat{\omega}_1(x) + (g') = \hat{\omega}_1(x) + (f'),
\end{aligned}$$

because $g' = f'$. However, $\hat{\omega}_1(x) \in F'$, therefore

$$\hat{\omega}_1(x) + (f') = \sigma'_i(\hat{\omega}_1(x) + (f')).$$

Thus

$$\tilde{\omega}(\sigma_i(x)) = \sigma'_i(\tilde{\omega}(x)).$$

It follows that the identity (1) applies. We now use this identity to prove that Φ is a homomorphism. Since $\sigma_i(\alpha) \in A$, for $i = 1, \ldots, n$, we have

$$\begin{aligned}
(\sigma_i \sigma_j)'(\alpha') &= (\sigma_i \sigma_j)'(\tilde{\omega}(\alpha)) \\
&= \tilde{\omega}((\sigma_i \sigma_j)(\alpha)) \\
&= \tilde{\omega}(\sigma_i(\sigma_j(\alpha))) \\
&= \sigma'_i(\tilde{\omega}(\sigma_j(\alpha))) \\
&= \sigma'_i \sigma'_j(\tilde{\omega}(\alpha)) \\
&= \sigma'_i \sigma'_j(\alpha').
\end{aligned}$$

5

Therefore Φ is a homomorphism. Clearly Φ is surjective. As $|G| = |G'|$, Φ is also injective, hence an isomorphism. This finishes the proof. $\qquad\square$

In inverse Galois theory we are confronted with the problem of determining whether a given group H may be considered as the Galois group of a Galois extension E of a certain field F, usually $\mathbf{Q}$. This may be difficult to decide directly. However, it may be possible to take another field F' and find a Galois extension E' of this field such that H is isomorphic to the Galois group $Gal(E'/F')$, which is in turn isomorphic to the group $Gal(E/F)$. We will now consider this question.

Let F be a Hilbertian field and E a Galois extension of degree n of $F(X)$, the field of fractions of the polynomial ring $F[X]$. From Proposition 2, we know that there is an element $\alpha \in E$, such that $E = F(X)(\alpha)$ and $f(Y) = m(\alpha, F(X)) \in F[X][Y]$. Then f is irreducible in $F[X][Y]$ (in the sense of our definition at the beginning of the article).

| thmHILBERTprop1 |

Theorem 1 *For an infinite number of values $b \in F$, $f_b(Y) = f(b, Y)$ is irreducible in $F[Y]$ and $E' = F[Y]/(f_b)$ is a Galois extension of F, with $G = Gal(E/F(X))$ isomorphic to $G' = Gal(E'/F)$.*

PROOF We apply Lemma 2. If A is the set of roots of f in E, then

$$\forall x \in A \; \forall \sigma \in G = Gal(E/F(X)), \; \sigma(x) \in A$$

and $\alpha \in A$. We choose $b \in F$ and consider the homomorphism

$$\omega_b : F[X] \longrightarrow F, g \longmapsto g(b).$$

From Lemma 2, there exists $u \in F[X]$ such that, if $\omega_b(u) \neq 0$, then there is an isomorphism Φ_b from $Gal(E/F(X))$ onto $Gal(E'/F)$, if f_b is irreducible. Indeed, if $f(X,Y) = \sum_{i=0}^{n} a_i(X)Y^i$, then

$$f'(Y) = \sum_{i=0}^{n} \omega_b(a_i(X))Y^i = \sum_{i=0}^{n} a_i(b)Y^i = f_b(Y),$$

where f' is defined as in Lemma 2. Moreover, in Step 4. of Lemma 2 we saw that $E' = F'[X]/(f')$, which leads to the form of E' in the statement of the theorem. We notice that $u \in F[X]$, so that $u(b) = 0$ for a finite number of values b. Eliminating these values from the infinite number of values b with f_b irreducible leaves us with an infinite number of values b, hence the result.$\square$

Remark Suppose that we have a finite group H and we wish to know whether it can be represented as a Galois group over a given Hilbertian field F, then we may look for a Galois extension E of the field $F(X)$ such that H is isomorphic to the Galois group $G = Gal(E/F(X))$. (As E is a finite extension of a field of functions, we say that E is a function field.) From the theorem, we know that there is a Galois extension E' of F such that H is isomorphic to $G' = Gal(E'/F)$. However, we do not know how to find such an extension.

2. A characterization of Hilbertian fields

In this section we continue our discussion of extensions of Hilbertian fields and find a useful characterization of Hilbertian fields. As in Theorem 1, we consider a Hilbertian field F and E a Galois extension of degree n of $F(X)$ and we take an element $\alpha \in E$, such that $E = F(X)(\alpha)$ and let $f(X,Y) = m(\alpha, F(X)) \in F[X][Y]$.

`propHILBERText1`

Proposition 3 *Let L be a finite extension of F such that $L(X) \subset E$ and $h \in L[X][Y]$ irreducible with roots in E. Up to a finite number of the values $b \in F$ such that $f_b(Y)$ is irreducible $h_b(Y)$ is irreducible in $L[Y]$.*

PROOF Let $\beta'_1, \ldots, \beta'_m$ be the roots of h_b in an extension E' of L, where f_b is irreducible in $F[Y] \subset L[Y]$. If h_b is reducible, then we can write $h_b = u_b v_b$, with $u_b, v_b \in L[Y]$ and $\deg u_b > 0$, $\deg v_b > 0$. Without loss of generality we may write

$$
\begin{aligned}
u_b(Y) &= \gamma(-\beta'_1 + Y) \cdots (-\beta'_s + Y) \\
v_b(Y) &= \delta(-\beta'_{s+1} + Y) \cdots (-\beta'_m + Y),
\end{aligned}
$$

with $\gamma, \delta \in L$. If $\sigma \in Gal(E'/L)$, then σ permutes the roots of u_b and of v_b, which cannot be possible if $Gal(E'/L)$ acts transitively on the roots. It follows that, if $Gal(E'/L)$ acts transitively on the roots of h_b, then h_b is irreducible. We will show that, with the exception of a finite set of values of b, there is an extension E' of L containing the roots of h_b and such that the Galois group $Gal(E'/L)$ acts transitively on these roots.

As L is a finite extension of F and $\mathrm{char}\,F = 0$, by the primitive element theorem, there exists $x \in L$ such that $L = F(x)$. We notice that

$$ F \subset F(x) = L \Longrightarrow F(X) \subset L(X) \subset E. $$

In addition, as $x \in L$, we have $x \in L(X)$, so we may consider the conjugates of x over $F(X)$. The roots $\beta_1, \ldots, \beta_m$ of $h(X, Y)$ are, by hypothesis, in E. We let A be the subset of E composed of x, with its conjugates over $F(X)$, α, with its conjugates over $F(X)$, and the roots of $h(X, Y)$. If $\sigma \in Gal(E/F(X))$ and $a \in A$, then clearly $\sigma(a) \in A$. We notice that the roots of h_b are distinct if the discriminant $\Delta(h_b) \neq 0$. However, $\Delta(h_b) = \Delta(h)(b)$, which has the value 0 for a finite number of values of b. Therefore, if we exclude these values, we can be sure that the roots of h_b are distinct.

As in Theorem `thmHILBERTprop1` 1, we consider the valuation homomorphism

$$ \omega_b : F[X] \longrightarrow F, g \longmapsto g(b), $$

where $b \in F$. Lemma `lemHILBERTprop2` 2 ensures the existence of $u \in F[X]$ such that, if $\omega_b(u) \neq 0$, we may extend ω_b to a homomorphism

$$ \tilde{\omega}_b : F[X][A] \longrightarrow E', $$

where E' is a Galois extension of F. Moreover, $u(b) = 0$ for a finite number of values b, so we may suppose that $\omega_b(u) \neq 0$. As a generator of L over F is included in A, we have $L \subset F[X][A]$. Also, $\tilde{\omega}_b$ restricted to F is the identity and so $\tilde{\omega}_b$ restricted to L is not trivial. Given that a ring homomorphism of a field into another field is either trivial or injective, it must be so that $\tilde{\omega}_b$ restricted to L is injective. We will note $\tilde{L}$ the image of L under $\tilde{\omega}_b$ in E'. As $\tilde{L}$ is isomorphic to L, E' is an extension of L.

We now let χ_b be the natural homomorphism from $F[X][A][Y]$ into $E'[Y]$ generated by $\tilde{\omega}_b$. We may identify $F[A][X]$ and $F[X][A]$. To see this it is sufficient to notice that, If $A = \{a_1, \ldots, a_n\}$, then $F[A][X]$ is composed of sums of expressions of the form $c a_1^{s_1} \ldots a_n^{s_n} X^t$ and $F[X][A]$ of sums of expressions of the form $c X^t a_1^{s_1} \ldots a_n^{s_n}$, where $c \in F$ and $s_1, \ldots s_n, t \in \mathbf{N}$. Thus we may consider that $L[X] = F(x)[X]$ is included in $F[X][A]$, because $x \in A$. We may write

$$ h(X, Y) = \sum_{i=0}^{m} h_i(X) Y^i, $$

7

where the coefficients $h_i(X)$ lie in $L[X]$, a subset of $F[X][A]$. We are interested in finding the form of $\chi_b(h)$. We may write

$$h_i(X) = \sum_{j=1}^{n} a_{ij} X^j,$$

with $a_{ij} \in L$. As $L = F(x)$, we can express each a_{ij} in the form

$$a_{ij} = \sum_{k=1}^{m} u_k^{ij} x^k,$$

with $u_k^{ij} \in F$. Hence,

$$
\begin{aligned}
\tilde{\omega}_b \left(\sum_{j=1}^{n} a_{ij} X^j \right) &= \sum_{j=1}^{n} \tilde{\omega}_b(a_{ij}) \tilde{\omega}_b(X^j) \\
&= \sum_{j=1}^{n} \tilde{\omega}_b \left(\sum_{k=1}^{m} u_k^{ij} x^k \right) b^j \\
&= \sum_{j=1}^{n} \left(\sum_{k=1}^{m} u_k^{ij} \tilde{\omega}_b(x)^k \right) b^j.
\end{aligned}
$$

Therefore, if we identify $\tilde{L}$ and L and consider the polynomial $\tilde{h} \in \tilde{L}[X][Y]$ corresponding to $h \in L[X][Y]$, then we find an expression for the coefficients of $\tilde{h}_b$ by replacing x with $\tilde{\omega}_b(x)$. Let us write $\tilde{h}_b$ for this polynomial. Then we have

$$\chi_b(h(X,Y)) = \tilde{h}_b(Y).$$

We notice that the roots of h lie in A so their images under $\tilde{\omega}_b$ are in E'. We have

$$h(X,Y) = h_m(X)(-\beta_1 + Y) \cdots (-\beta_m + Y) \implies \tilde{h}_b(Y) = \tilde{h}_m(b)(-\beta_1' + Y) \cdots (-\beta_m' + Y),$$

where $\beta j' = \chi_b(\beta_i)$, for some i. So we have found expressions for the roots of $\tilde{h}_b$.

From our work at the beginning of the proof, to show that $\tilde{h}_b$ is irreducible, it is sufficient to prove that the Galois group $Gal(E'/\tilde{L})$ acts transitively on the roots β_j' (for any b in the infinite set we have retained). This we will now do. As $h(X,Y)$ is irreducible in $L[X][Y]$, from Gauss's lemma, $h(X,Y)$ is also irreducible in $L(X)[Y]$. E is a normal extension of $F(X)$ containing $L(X)$, hence, by Result 6, E is a normal extension of $L(X)$. Moreover, by Result 7, E is the splitting field of a polynomial $g \in L(X)[Y]$. From Result 10, the Galois group $G_1 = Gal(\bar{E}/L(X))$, where $\bar{E}$ is a splitting field of h included in E, acts transitively on the roots β_i. Now, Result 3, with $F = F' = \bar{E}$ and $f = f^* = g$, implies that any element $\sigma \in G_1$ may be extended to an element $\tilde{\sigma} \in G_2 = Gal(E/L(X))$. This implies that G_2 acts transitively on the roots β_i. Supposing that f_b is irreducible, then, from Theorem 1, $G = Gal(E/F(X))$ is isomorphic to $G' = Gal(E'/F)$, where $E' = F[Y]/(f_b)$. (This is the same E' as that obtained earlier in the proof after applying Lemma 2.)

If we restrict the isomorphism from G onto G' to the subgroup G_2, then we obtain a subgroup G_2' of G'. We claim that G_2' is a subgroup of the Galois group $G'' = Gal(E'/\tilde{L})$. To prove this we need to show that the automorphisms of G_2' fix the elements of $\tilde{L}$. We use the identity (1) and the explicit form of the isomorphism Φ from G onto G'. If $\tilde{z} \in \tilde{L}$, $\sigma \in G_2$ and σ' the corresponding automorphism in G_2', then

$$\sigma'(\tilde{z}) = \sigma'(\tilde{\omega}_b(z)) = \tilde{\omega}_b(\sigma(z)) = \tilde{\omega}_b(z) = \tilde{z}.$$

This proves that $G_2' \subset G''$ and so the claim.

We now show that G'' acts transitively on the roots β_j'. There exists $\sigma \in G_2$ such that $\sigma(\beta_i) = \beta_j$, because G_2 acts transitively on the roots β_i. Let σ' be the element of G_2' corresponding to σ. Then, using the identity (1) again, we have

$$\sigma'(\beta_i') = \sigma'(\tilde{\omega}_b(\beta_i)) = \tilde{\omega}_b(\sigma(\beta_i)) = \tilde{\omega}_b(\beta_j) = \beta_j'.$$

Therefore G'' acts transitively on the roots β_j'. This finishes the proof. □

We can now establish the characterization of Hilbert fields, which we referred to at the beginning of the section.

Theorem 2 *The field F is Hilbertian if and only if, for every finite extension L of F and finite set of irreducible polynomials $h_1, \ldots, h_k \in L[X, Y]$, there is an infinite number of values $b \in F$ such that $h_{i,b}(Y) = h_i(b, Y) \in L[Y]$ is irreducible, for $i = 1, \ldots, k$.*

PROOF Let F be an Hilbertian field, L a finite extension of F and $h_1, \ldots, h_k$ irreducible polynomials in $L[X, Y] = L[X][Y]$. (From Gauss's Lemma, these polynomials are irreducible in $L(X)[Y]$.) Adding the roots of the polynomials h_i to $L(X)$, we obtain a finite extension M of $L(X)$. From Result 5, $L(X)$ is a finite extension of $F(X)$, so M is a finite extension of $F(X)$. Now let E be a normal closure of M over $F(X)$. Then E is finite Galois extension of $F(X)$ (Result 8). From Result 2, we may find $\alpha \in E$ such that $E = F(\alpha)$ and $m(\alpha, F(X)) \in F[X][Y]$. As usual, we write $f(X)$ for $m(\alpha, F(X))$. In addition, $L(X) \subset E$ and the roots of each h_i are in E. From Proposition 3, for each i, for all but a finite number of the $b \in F$ such that $f_b(Y)$ is irreducible, $h_{i,b}(Y)$ is irreducible. It follows that $h_{i,b}(Y)$ is irreducible, for all i, for an infinite number of values of b.

The converse is elementary. We only need to choose $L = F$ and $k = 1$. □

We know that $\mathbf{Q}$ is a Hilbertian field. The next two results will show us that there are many other such fields.

Theorem 3 *If F is a Hilbertian field, then any finite extension E of F is also Hilbertian.*

PROOF Let E be a finite extension of the Hilbertian field F and $f \in E[X, Y]$ irreducible. From Theorem 2, there are infinitely many $b \in F$, such that f_b is irreducible. As $F \subset E$, there are infinitely many $b \in E$ such that f_b is irreducible. Hence E is Hilbertian. □

We recall that a number field is a finite extension in $\mathbf{C}$ of the field $\mathbf{Q}$.

Corollary 1 *Number fields are Hilbertian.*

3. The Kronecker specialization

We have considered extensions of fields of fractions of polynomials in one variable. In this section we aim to consider the case of polynomials in several variables. We use a tool known as the Kronecker specialization. We fix an integer $d > 1$. For a field F and an integer $k > 2$, we define a mapping S_d from $F[X_1, \ldots, X_k]$ into $F[X, Y]$ by

$$S_d(f)(X, Y) = f(X, Y, Y^d, Y^{d^2}, \ldots, Y^{d^{k-2}}).$$

The mapping S_d is called a Kronecker specialization. We note V_d the collection of polynomials in $F[X_1, \ldots, X_k]$ whose degree is less than d in each variable $X_2, \ldots, X_k$ and W_d the collection of polynomials in $F[X, Y]$ whose degree is inferior to d^{k-1} in the variable Y.

Proposition 4 *The mapping S_d defines a bijection from V_d onto W_d.*

PROOF First let $f \in V_d$ be a monomial. Then f has the form $aX_1^{\alpha_1} \cdots X_k^{\alpha_k}$ and so

$$S_d(f) = aX^{\alpha_1}Y^{\alpha_2 + \alpha_3 d + \alpha_4 d^2 + \ldots + \alpha_k d^{k-2}}.$$

If $g \in V_d$, with $g = bX_1^{\beta_1} \cdots X_k^{\beta_k}$, and $S_d(g) = S_d(f)$, then

$$b = a \qquad \beta_1 = \alpha_1 \qquad \beta_2 + \beta_3 d + \beta_4 d^2 + \ldots + \beta_k d^{k-2} = \alpha_2 + \alpha_3 d + \alpha_4 d^2 + \ldots + \alpha_k d^{k-2}.$$

As the representation in base d is unique, we must have $\alpha_i = \beta_i$, for all $i \geq 2$. Hence $g = f$ and S_d defines an injection from the monomials in V_d into the monomials in W_d. Also, any integer $s < d^{k-1}$ has a unique representation in base d:

$$s = \alpha_2 + \alpha_3 d + \alpha_4 d^2 + \cdots + \alpha_k d^{k-2},$$

which implies that S_d restricted to the monomials of V_d defines a bijection onto the monomials of W_d. As

$$S_d(m_1 + \cdots + m_k) = S_d(m_1) + \cdots + S_d(m_k),$$

for monomials $m_1, \ldots, m_k$, the mapping S_d defines a bijection from V_d onto W_d $\qquad \square$

Remark It is not difficult to see that, if the product fg is in V_d, then

$$S_d(fg) = S_d(f)S_d(g).$$

We now see that the Hilbertian property "carries over" to multivariable polynomials. (We advise the reader to return to the beginning of the article to revise the definition of an irreducible polynomial in several variables.)

Theorem 4 *If F is a Hilbertian field and $f \in F[X_1, \ldots, X_k]$ is irreducible, then there exists an infinite number of values $b \in F$ such that $f(b, X_2, \ldots, X_k) \in F[X_2, \ldots, X_k]$ is irreducible.*

PROOF Let d be an integer superior to the degree of each variable X_i in f. We can write

$$S_d(f)(X,Y) = g(X) \prod_{i \in C} g_i(X,Y), \tag{2}$$

where the g_i are irreducible polynomials in $F[X][Y]$ and C is a finite index set. As F is Hilbertian, from Theorem 2, for an infinite number of values of $b \in F$, $g_{i,b}(Y) = g_i(b,Y)$ is irreducible in $F[Y]$. If we exclude the values b which are roots of g, then we still have an infinite number of values of $b \in F$ such that $g_i(b,Y)$ is irreducible, for all $i \in C$. For any b in the remaining set, we have the factorization into prime factors in $F[Y]$:

$$S_d(f)(b,Y) = g(b) \prod_{i \in C} g_i(b,Y).$$

For any such b, suppose now that $f_b = f(b, X_2, \ldots, X_k)$ is reducible, i.e., $f_b = uv$, with u and v nonconstant. We may consider f_b, u and v as members of $F[X_1, \ldots, X_k]$. As $f_b \in V_d$, we have $u, v \in V_d$ and

$$S_d(u)S_d(v) = S_d(uv) = S_d(f_b) = S_d(f)(b,Y) = g(b) \prod_{i \in C} g_i(b,Y).$$

10

We now have a partition $\{A, B\}$ of C, with A and B nonempty, since u and v are nonconstant, and $\alpha, \beta \in F$ such that $g(b) = \alpha\beta$ and

$$S_d(u) = \alpha \prod_{i \in A} g_i(b, Y) \qquad \text{and} \qquad S_d(v) = \beta \prod_{i \in B} g_i(b, Y).$$

At this point we set

$$U(X, Y) = \prod_{i \in A} g_i(X, Y) \qquad \text{and} \qquad V(X, Y) = \prod_{i \in B} g_i(X, Y).$$

As $U, V \in W_d$, there exist unique $\tilde{u}, \tilde{v} \in V_d$ such that $S_d(\tilde{u}) = U$ and $S_d(\tilde{v}) = V$. Then

$$S_d(\tilde{u}_b) = S_d(\tilde{u})(b, Y) = U(b, Y) = \prod_{i \in A} g_i(b, Y) = \alpha^{-1} S_d(u) = S_d(\alpha^{-1} u),$$

which implies that $\tilde{u}_b = \alpha^{-1} u$. In the same way, $\tilde{v}_b = \beta^{-1} v$ and so

$$\tilde{u}_b \tilde{v}_b = \alpha^{-1} \beta^{-1} uv = g(b)^{-1} f_b.$$

Our next step is to show that $\tilde{u}\tilde{v} \notin V_d$. If this is not the case, then

$$S_d(g\tilde{u}\tilde{v}) = g S_d(\tilde{u}) S_d(\tilde{v}) = gUV = S_d(f),$$

from which we deduce that

$$g\tilde{u}\tilde{v} = f,$$

which contradicts the irreducibility of f, since $\tilde{u}$ and $\tilde{v}$ are nonconstant. Hence $\tilde{u}\tilde{v} \notin V_d$.

We are now in a position to prove that f_b is irreducible for an infinite number of values of b. We may consider f as a polynomial in $F[X_1][X_2, \ldots, X_k]$. Thus a monomial is of the form $a(X_1)X^{n_2} \cdots X^{n_k}$. As $\tilde{u}\tilde{v} \notin V_d$ and $\tilde{u}_b \tilde{v}_b = g(b)^{-1} f_b$, to avoid a contradiction, b must be a root of $a(X_1)$, whenever there is an i such that the power n_i of X_i is greater than $d - 1$. We can eliminate these values of b for each such monomial. As the number of these monomials is finite, we are left with an infinite number of values of b for which f_b is irreducible. $\qquad\square$

Corollary 2 *Let F be a Hilbertian field and $f \in F[X_1, \ldots, X_k]$, with $k \geq 2$, irreducible. For every polynomial $p \in F[X_1, \ldots, X_{k-1}]$, there exist elements $b_1, \ldots, b_{k-1} \in F$ such that $p(b_1, \ldots, b_{k-1}) \neq 0$ and the polynomial $f(b_1, \ldots, b_{k-1}, X_k)$ is irreducible.*

PROOF Let $f \in F[X_1, \ldots, X_k]$ be irreducible. We aim to prove by induction on n that, for every polynomial $p \in F[X_1, \ldots, X_n]$, with $n < k$, there exist $b_1, \ldots, b_n \in F$ such that $p(b_1, \ldots, b_n) \neq 0$ and $f(b_1, \ldots, b_n, X_{n+1}, \ldots, X_k)$ is irreducible. First, let $p \in F[X_1]$. From Theorem 4, there is an infinite number of values of $b \in F$ such that $f(b, X_2, \ldots, X_k)$ is irreducible. If we take one such b which is not a root of p, then we have a value of b satisfying the required conditions. Thus the result is true for $n = 1$.

We now suppose that the result is true for $n < k - 1$ and consider the case $n + 1$. Let $p \in F[X_1, \ldots, X_{n+1}]$. We may consider p as an element of $F[X_{n+1}][X_1, \ldots, X_n]$. Each coefficient has a finite number of roots. If c is not one of these roots, then $p(X_1, \ldots, X_n, c)$ is a nonzero polynomial in $F[X_1, \ldots, X_n]$. From the induction hypothesis, there exist $b_1, \ldots, b_n$ such that $p(b_1, \ldots b_n, c) \neq 0$ and $f(b_1, \ldots, b_n, X_{n+1}, \ldots, X_k)$ is irreducible. Using Theorem 4, we know that there is an infinite number of values of b, such that $f(b_1, \ldots, b_n, b, X_{n+2}, \ldots, X_k)$ is irreducible. As $p(b_1, \ldots, b_n, X_{n+1}) \in F[X_{n+1}]$, if we eliminate any b which is a root of this

11

polynomial, then we have $p(b_1, \ldots, b_n, b) \neq 0$. Therefore the result is true for $n+1$. This finishes the induction step. $\qquad\square$

To prove the next theorem, which will provide us with more Hilbertian fields, we will need Result 1.

ufd

thHILBERTkron2 **Theorem 5** *If F is Hilbertian field, then $F(X_1, \ldots, X_k)$ is Hilbertian field, for any $k \in \mathbf{N}^*$.*

PROOF Let $f \in F(X_1, \ldots, X_k)[X, Y]$ be irreducible. There exists $g \in F(X_1, \ldots, X_k)^*$ such that $gf \in F[X_1, \ldots X_k, X][Y]$. We may write $gf = c(gf)h$, where $c(h) = 1$. We have

$$h = \frac{g}{c(gf)}f \qquad \text{and} \qquad \frac{g}{c(gf)} \in F(X_1, \ldots, X_k, X)^*.$$

We notice that $h \in F(X_1, \ldots, X_k, X)[Y]$ is primitive and irreducible. From Gauss's Lemma, h is also irreducible in $F[X_1, \ldots, X_k, X][Y]$. Now, using Theorem 4, we see that there are infinitely many values of $b \in R$ such that $h(X_1, \ldots, X_k, b, Y)$ is irreducible in $F[X_1, \ldots, X_k][Y]$. Using Gauss's Lemma again, we see that $h(X_1, \ldots, X_k, b, Y)$ is irreducible in $F(X_1, \ldots, X_k)[Y]$. To finish, we notice that

$$f(X_1, \ldots, X_k, b, Y) = \frac{c(gf)_b}{g} h(X_1, \ldots, X_k, b, Y),$$

where $c(gf)_b$ is the polynomial in $F[X_1, \ldots, X_k]$ obtained by replacing the variable X by b. Now $c(fg) \in F(X_1, \ldots X_k)[X]$, so there can only be a finite number of values of b such that $c(gf)_b = 0$. If we exclude these values, then $\frac{c(gf)_b}{g}$ is a unit in $F(X_1, \ldots, X_k)$ and so $f(X_1, \ldots, X_k, b, Y)$ is irreducible in $F(X_1, \ldots X_k)[Y]$. We have shown that $F(X_1, \ldots, X_k)$ is Hilbertian. $\qquad\square$

We may now extend Theorem 1.

thmHILBERTprop1

HREDthm1a **Theorem 6** *If F is an Hilbertian field and E a Galois extension of $F(X_1, \ldots, X_k)$, then there exists a Galois extension E' of F such that $Gal(E/F(X_1, \ldots, X_k))$ is isomorphic to $Gal(E'/F)$.*

PROOF We prove this result by induction on k. For $k = 1$, it is sufficient to apply Theorem 1. Suppose now that the result is true for k and let us consider the case $k + 1$. E is a Galois extension of $F(X_1, \ldots, X_k, X_{k+1})$. From Theorem 5, $F(X_1, \ldots, X_k)$ is Hilbertian and so there is a Galois extension E' of $F(X_1, \ldots, X_k)$ such that

$$Gal(E/F(X_1, \ldots, X_k, X_{k+1})) \simeq Gal(E'/F(X_1, \ldots, X_k)).$$

From the induction hypothesis there is an extension E'' such that

$$Gal(E'/F(X_1, \ldots, X_k)) \simeq Gal(E''/F),$$

therefore

$$Gal(E/F(X_1, \ldots, X_k, X_{k+1})) \simeq Gal(E''/F).$$

This finishes the induction step and the proof. $\qquad\square$

Remark We recall that the general polynomial of degree k over a field F has the form

$$f(Y) = Y^n - X_1 Y^{n-1} + X_2 Y^{n-2} + \cdots + (-1)^{n-1} X_{n-1} Y + (-1)^n X_n \in F(X_1, \ldots, X_k)[Y],$$

where $F(X_1, \ldots, X_k)$ is the rational function field over F in k variables. The Galois group of f is the symmetric group S_k (see [5]). In particular, this is the case if $F = \mathbf{Q}$. Writing E for the splitting field of f over $\mathbf{Q}(X_1, \ldots, X_k)$ and using the fact that $\mathbf{Q}$ is a Hilbertian field, from Theorem 6 we deduce that S_k is realizable as a Galois group over $\mathbf{Q}$.

4. **Proof of Hilbert's irreducibility theorem**

Above we stated without proof Hilbert's irreducibility theorem, namely that the field of rational numbers $\mathbf{Q}$ is a Hilbertian field, i.e., for any $f \in \mathbf{Q}[X, Y]$, which is irreducible, there exists an infinite number of values $b \in \mathbf{Q}$ such that $f(b, Y) \in \mathbf{Q}[Y]$ is irreducible. We aim now to provide a detailed proof of this result. Our proof is based on that given in [1], with modifications. We now suppose that our field is $\mathbf{C}$, the complex numbers. For any $z \in \mathbf{C}$, the polynomial $f(z, Y)$ has n roots which may or may not be distinct. For any z, we may write $u_1(z), \ldots, u_n(z)$ for these roots. Thus we obtain n functions defined on $\mathbf{C}$. If b is a regular value, then the roots $u_1(b), \ldots, u_n(b)$ are distinct. We can say more.

Lemma 3 *If b is a regular value of the polynomial $f(X, Y)$ over $\mathbf{C}$, then there is a neighbourhood N of b in $\mathbf{C}$ such that the functions $u_1(z), \ldots, u_n(z)$ are analytic on N.*

PROOF We will suppose that the functions u_i exist and find the possible forms, then we will show that the functions so obtained satisfy the conditions. Let $u(z)$ be one such function and, to begin, we will suppose that $b = 0$ and $u(0) = 0$. We seek a power series

$$u(z) = \sum_{k=1}^{\infty} b_k z^k,$$

with $b_k \in \mathbf{C}$, which converges on some set $N = \{z \in \mathbf{C} : |z| < R\}$, with $R > 0$, within which

$$f(z, u(z)) = 0.$$

We may write $f(z, u(z))$ in the form

$$f(z, u) = a_{10} z + a_{01} u + \sum_{i+j \geq 2} a_{ij} z^i u^j.$$

The sum on the right is finite, because f is a polynomial. Let f_u be the derivative of f with respect to the variable u. As $z = 0$ is a regular value, $f_u(0, 0) = a_{01} \neq 0$, so we may write

$$f(z, u) = -a_{01} \left(-\frac{a_{10}}{a_{01}} z - u + \sum_{i+j \geq 2} -\frac{a_{ij}}{a_{01}} z^i u^j \right) = -a_{01} \left(a'_{10} z - u + \sum_{i+j \geq 2} a'_{ij} z^i u^j \right). \quad (3)$$

From this we deduce

$$f_u(z, u) = -a_{01} \left(-1 + g(z, u) \right),$$

where every monomial of g has degree at least 1.

We now substitute $u(z) = \sum_{k=1}^{\infty} b_k z^k$ in the equation $f(z, u(z)) = 0$:

$$f(z, u(z)) = -a_{01} \left(a'_{10} z - \sum_{k \geq 1} b_k z^k + \sum_{i+j \geq 2} a'_{ij} z^i \left(\sum_{k \geq 1} b_k z^k \right)^j \right) = 0.$$

As this is a power series in z, which we suppose convergent on a neighbourhood of 0, the coefficient of z, namely $a'_{10} - b_1$, has the value 0, which implies that $b_1 = a'_{10}$.

Our next step is to take a Taylor expansion of the polynomial $f(z, u)$ in u, around the point $u_0 = \sum_{i=1}^{k-1} b_i z^i$. For $u(z) = \sum_{k \geq 1} b_k z^k$, we obtain

$$f(z, \sum_{i=1}^{\infty} b_i z^i) \quad = \quad f(z, \sum_{i=1}^{k-1} b_i z^i) + \left(-a_{01} \left(-1 + g(z, \sum_{i=1}^{k-1} b_i z^i) \right) \right) \sum_{i=k}^{\infty} b_i z^i$$
$$+ \text{ terms of degree at least } 2k.$$

The value of this expression is 0, so the coefficient of each power of z must be 0. In particular, the coefficient of z^k is $a_{01} b_k$ plus the coefficient c_k of z^k in the expression of the polynomial $f(z, \sum_{i=1}^{k-1} b_i z^i)$. Therefore $b_k = -\frac{c_k}{a_{01}}$. With this rule and the initial value $b_1 = a'_{10}$ the entire sequence of b_is is determined. We now have a candidate for the series $\sum_{k=1}^{\infty} b_k z^k$. We must show that it has a positive radius of convergence. We will do this by constructing a power series $\sum_{k=1}^{\infty} A_k z^k$ with positive radius of convergence R and such that, for every k, $A_k \geq |b_k|$.

For each k, there is a polynomial in several variables with positive integer coefficients, which we note p_k, such that b_k is is the value of p_k evaluated at the set of coefficients a'_{ij}. We will write $b_k = p_k(a'_{ij})$. Let A be an element of $\mathbf{Z}$ such that $A \geq |a'_{ij}|$, for all a'_{ij}. If we replace a'_{ij} by A in the equation (3), then we obtain

$$h(z, v) = Az - v + A \sum_{i+j \geq 2} z^i v^j = 0.$$

Now, redoing the calculations which we did on the equation (3), we obtain a solution of the form $\sum_{k=1}^{\infty} A_k z^k$, where A_k is the polynomial expression derived from $p_k(a'_{ij})$ by replacing the a'_{ij}s by A. Clearly $A_k \geq |b_k|$, for every k, since the coefficients of the p_k are positive. For $|z| < 1$ and $|u| < 1$, we have

$$0 \quad = \quad Az - v + Az^0 \sum_{j=2}^{\infty} v^j + Az^1 \sum_{j=1}^{\infty} v^j + A \sum_{i=2}^{\infty} z^i \left(\sum_{j=0}^{\infty} v^j \right)$$
$$= \quad Az - v + A \frac{v^2}{1-v} + A \frac{zv}{1-v} + A \left(\frac{z^2}{1-t} \frac{1}{1-z} \right).$$

Multiplying by $1 - v$ we obtain

$$0 = Az(1-v) - v(1-v) + Av^2 + Azv + A \frac{z^2}{1-z} = (A+1)v^2 - v + \frac{Az}{1-z}, \qquad (4)$$

which is a quadratic equation in v. If we set, for z sufficiently small,

$$v(z) = \frac{1 - \left(1 - 4(A+1)\frac{Az}{1-z} \right)^{\frac{1}{2}}}{2(A+1)},$$

then $v(z)$ is the solution of the equation (4), with $v(0) = 0$, where the square root in the expression is the principal value (for example, see [2]). We would like to show that $v(z)$ is analytic for z sufficiently small. However, the principal value of the function $w_1(z) = (1-z)^{\frac{1}{2}}$ is analytic, which is also the case for the function $w_2(z) = \frac{z}{1-z}$. Moreover, for z sufficiently small, $|w_2(z)| < 1$. Therefore, given that the composition of analytic functions is analytic, we see that

$v(z)$ is analytic in a neighbourhood of 0. It now follows that $u(z)$ is analytic in a neighbourhood of 0.

We have supposed that $u(0) = 0$. If we have $u(0) = a$, where a is not necessarily 0, then, writing $y(z) = u(z) - a$, we have $y(0) = 0$ and so we have $y(z)$ analytic for z sufficiently small, which implies that $u(z)$ is analytic for z sufficiently small. Finally, if we suppose that $u(b) = a$, then writing $y(z) = u(b - z)$, we have $y(0) = a$ and $y(z)$ is analytic for z sufficiently close to 0, which implies that $u(z)$ is analytic for u sufficiently close to b.

For each root a_i of f_b we can find an analytic root function $u_i(z)$, with $u_i(b) = a_i$, defined on a neighbourhood N_i of b. As the a_i are distincts, by continuity, we may choose a neighbourhood N of b such that the functions $u_i(z)$ are analytic on N and, for any $z \in N$, distinct. This finishes the proof. $\qquad\square$

Remark For $z \in N$, we may write

$$f(z, Y) = a_n(z) \prod_{i=1}^{n} \left(-u_i(z) + Y \right),$$

where $a_n(z)$ is a polynomial in z and the u_n are analytic functions defined on N.

We need another preliminary result. We take $m + 1$ increasing values of the real variable t: $t_0 < t_1 < t_2 < \cdots < t_m$ and we write V_m for the Vandermonde determinant of the t_is, i.e.,

$$V_m = \begin{vmatrix} 1 & t_0 & t_0^2 & \dots & t_0^{m-1} & t_0^m \\ 1 & t_1 & t_1^2 & \dots & t_1^{m-1} & t_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & t_m & t_m^2 & \dots & t_m^{m-1} & t_m^m \end{vmatrix}.$$

Now let $f : [t_0, t_m] \longrightarrow \mathbf{R}$ be an m times differentiable function. We set

$$W_m = \begin{vmatrix} 1 & t_0 & t_0^2 & \dots & t_0^{m-1} & f(t_0) \\ 1 & t_1 & t_1^2 & \dots & t_1^{m-1} & f(t_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & t_m & t_m^2 & \dots & t_m^{m-1} & f(t_m) \end{vmatrix}.$$

lemHILBIRRED2

Lemma 4 *There exist $u \in (t_0, t_m)$ such that*

$$\frac{W_m}{V_m} = \frac{f^{(m)}(u)}{m!}.$$

PROOF Suppose that $g : [t_0, t_m] \longrightarrow \mathbf{R}$ is an m times differentiable function and that $g(t_i) = f(t_i)$, for all i. By Rolle's theorem, in each interval (t_i, t_{i+1}), there exists a_i such that $g^{(1)}(a_i) = f^{(1)}(a_i)$. So we have m points $a_0 < a_1 < \cdots < a_{m-1}$ such that $g^{(1)}(a_i) = f^{(1)}(a_i)$, for all i. We now apply Rolle's theorem again and obtain $m-1$ points $b_0 < b_1 < \cdots < b_{m-2}$ such that $g^{(2)}(b_i) = f^{(2)}(b_i)$, for all i. Continuing in the same way, we finally obtain a point u such that $g^{(m)}(u) = f^{(m)}(u)$

We now consider the system

$$\begin{pmatrix} 1 & t_0 & \dots & t_0^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_m & \dots & t_m^m \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} f(t_0) \\ \vdots \\ f(t_m) \end{pmatrix}.$$

This system has a unique solution and so there exists a unique polynomial $g(X)$ of degree less than m in $\mathbf{R}[X]$ such that $g(t_i) = f(t_i)$, for all i. From what we have just seen, there exists an element $u \in (t_0, t_m)$ such that

$$f^{(m)}(u) = g^{(m)}(u) = m!a_m \Longrightarrow a_m = \frac{f^{(m)}(u)}{m!}.$$

Using Cramer's rule, we obtain

$$a_m = \frac{W_m}{V_m} \Longrightarrow \frac{W_m}{V_m} = \frac{f^{(m)}(u)}{m!}.$$

This ends the proof. □

The next preliminary result is interesting in that it shows that we often only need know that two functions have the same values at a limited number of points to establish that they have the same values at all points.

lemHILBIRRED3 **Lemma 5** *Let G be a connected open subset of $\mathbf{C}$ and f, g analytic functions from G into $\mathbf{C}$. Suppose that there exists a sequence $(z_n)_{n=1}^{\infty}$ in G and $z_0 \in G$ such that*

- *for all $n \geq 1$, $z_n \neq z_0$;*

- *$\lim_{n \to \infty} z_n = z_0$;*

- *for all $n \geq 1$, $f(z_n) = g(z_n)$.*

Then, for all $z \in G$, $f(z) = g(z)$.

PROOF As f and g are analytic on G, for all $z \in G$, we may find $r > 0$ (depending on z) such that, for any $\tilde{z}$ with $|\tilde{z} - z| < r$, we have

$$f(\tilde{z}) = \sum_{n=0}^{\infty} a_n(\tilde{z} - z^n)^n \qquad \text{and} \qquad g(\tilde{z}) = \sum_{n=0}^{\infty} b_n(\tilde{z} - z^n)^n,$$

where the coefficients a_n and b_n are in $\mathbf{C}$. Let H be the subset of points $z \in G$ where the Taylor series of f and g coincide, i.e., $a_n = b_n$, for all $n \geq 0$. We aim to show that $H = G$, which is sufficient to prove the result. First we show that $z_0 \in H$ and so H is nonempty. As f and g are analytic, we may find $r > 0$ such that, for $|z - z_0|$, we have

$$f(z) = \sum_{n=0}^{\infty} a_n(z - z_0)^n \quad \text{and} \quad \sum_{n=0}^{\infty} b_n(z - z_0)^n,$$

where the coefficients a_n and b_n are in $\mathbf{C}$. We will use an induction argument to show that, for all n, $a_n = b_n$. To see this, we first notice that f and g are continuous at z_0, hence

$$a_0 = f(z_0) = \lim_{n \to \infty} f(z_n) = \lim_{n \to \infty} g(z_n) = g(z_0) = b_0.$$

Suppose now that we have established that $a_m = b_m$ up to a certain m. We set, for all $|z - z_0| \leq r$,

$$f^*(z) = a_{m+1} + a_{m+2}(z-z_0) + a_{m+3}(z-z_0)^2 + \cdots \quad \text{and} \quad g^*(z) = b_{m+1} + b_{m+2}(z-z_0) + b_{m+3}(z-z_0)^2 + \cdots.$$

Then, for $0 < |z - z_0| < r$, we have

$$f^*(z) = \frac{1}{(z - z_0)^{m+1}} \left(f(z) - (a_0 + a_1(z - z_0) + \cdots + a_m(z - z_0)^m) \right)$$

and

$$g^*(z) = \frac{1}{(z - z_0)^{m+1}} \left(g(z) - (b_0 + b_1(z - z_0) + \cdots + b_m(z - z_0)^m) \right)$$

and so, for all $n \geq 1$, $f^*(z_n) = g^*(z_n)$, since $z_n \neq z_0$ and $f(z_n) = g(z_n)$, for all $n \geq 1$. It follows that $a_{m+1} = b_{m+1}$, because f^* and g^* are continuous at z. By induction, for all n, $a_n = b_n$. Hence the Taylor series of f and g coincide at z_0, which implies that $H \neq \emptyset$

The statement that $z \in H$ is equivalent to saying that $f^{(n)}(z) = g^{(n)}(z)$ for all $n \geq 0$. As the functions $f^{(n)}$ and $g^{(n)}$ are continuous, H is closed in G. If $z \in H$, then there exists $r > 0$ such that $f = g$ on the open disk $D(z, r)$. For any $\zeta \in D(z, r)$, there is a neighbourhood N of ζ on which $f = g$ and so have the same Taylor series at ζ. Therefore $D(z, r) \subset H$ and it follows that H is open in G. Since G is connected, we must have $H = G$ and so $f(z) = g(z)$, for all $z \in G$.$\square$

In proving Hilbert's irreducibility theorem which follows (Theorem $\overset{\texttt{thmHILBIRRED1}}{7}$), we will use two more preliminary results whose proofs we leave as exercises.

exerHILBIRRED1 **Exercise 1** *Suppose that $g \in \mathbf{C}[X]$, with $\deg g = m$, and $m + 1$ integers t_i such that $g(t_i) \in \mathbf{Q}$. Show that $g \in \mathbf{Q}[X]$.*

exerHILBIRRED2 **Exercise 2** *Let $m \geq 1$ and $f(X) = \sum_{i=0}^{m} a_i X^i \in \mathbf{Z}[X]$. Show that, if $\alpha = \frac{p}{q}$, with $(p, q) = 1$, is a root of f, then $p|a_0$ and $q|a_m$. Deduce that, if f is monic, then any rational root of f is an integer.*

We now turn to the proof of Hilbert's result.

thmHILBIRRED1 **Theorem 7** *(Hilbert's irreducibility Theorem) If $f(X, Y) \in \mathbf{Q}[X, Y]$ is irreducible, then there exists an infinite number of rational numbers b such that $f_b(Y) = f(b, Y)$ is irreducible in $\mathbf{Q}[Y]$.*

PROOF The proof is rather long and detailed, so we will proceed by steps.

1. The coefficient functions y_j: From Proposition $\overset{\texttt{propHILBERTreduc1}}{1}$, we know that all but a finite number number of values $b \in \mathbf{Q}$ are regular values of f. Consequently, we may choose $s_0 \in \mathbf{Q}$, a regular value of f. Lemma $\overset{\texttt{lemHILBIRRED1}}{3}$ guarantees the existence of n roots $u_1(s), \ldots, u_n(s)$ of $f(s, Y)$, which are analytic functions on a $\mathbf{C}$-neighbourhood N of s_0, which we may suppose to be connected. (This is of importance later.) As usual we write

$$f(X, Y) = a_0(X) + a_1(X)Y + a_2(X)Y^2 + \cdots + a_n(X)Y^n,$$

where the $a_i \in \mathbf{Q}[X]$, for $i = 0, 1, \ldots, n$, and $a_n(X) \neq 0$. Let us now consider

$$f(Y) = a_0 + a_1 Y + a_2 Y^2 + \cdots + a_n Y^n,$$

where, for $i = 0, 1, \ldots, n$, a_i is the polynomial function (with coefficients in $\mathbf{Q}$) associated with the polynomial $a_i(X)$. These functions are defined on N. Clearly, $f \in \mathcal{F}[Y]$, where $\mathcal{F}$ is the ring of polynomial functions defined on N, with coefficients in $\mathbf{Q}$. Moreover, it is clear that the functions $u_1, \ldots, u_n$ are roots of f and belong to the ring $\mathcal{A}$ of analytic functions defined on N. We have

$$f(Y) = a_n \prod_{i=1}^{n} (-u_i + Y).$$

17

We now let S be a proper subset of $\mathbf{N}_n = \{1, \ldots, n\}$, i.e., $S \neq \emptyset, \mathbf{N}_n$ and write

$$\alpha(Y) = \prod_{i=1}^{n}(-u_i + Y) \qquad \beta(Y) = \prod_{i \in S}(-u_i + Y) \qquad \gamma(Y) = \prod_{i \notin S}(-u_i + Y).$$

Then $\alpha, \beta, \gamma \in \mathcal{A}[Y]$ and $\alpha = \beta\gamma$. If the coefficients of both β and γ are in $\mathcal{F}$, then the polynomial $f(X, Y)$ can be written as a product of polynomials of degree at least one in $\mathbf{Q}[X][Y]$. To see this, it is sufficient to write the equalities satisfied by the coefficients $a_0, a_1, \ldots, a_n$ in the equality $f(Y) = a_n\beta\gamma$, where $a_n \neq 0$. Indeed, let

$$\beta(Y) = \prod_{i=0}^{k} b_i Y^i \qquad \text{and} \qquad \gamma(Y) = \prod_{j=0}^{l} c_j Y^j,$$

where $b_0, \ldots, b_k, c_0, \ldots c_l \in \mathcal{F}$. Then

$$a_0(s) = a_n(s)b_0(s)c_0(s),$$

for an infinite number of rational numbers s, hence

$$a_0(X) = a_n(X)b_0(X)c_0(X).$$

Also,

$$a_1(s) = a_n(s)\left(b_0(s)c_1(s) + b_1(s)c_0(s)\right),$$

for an infinite number of rational numbers s, hence

$$a_1(X) = a_n(X)\left(b_0(X)c_1(X) + b_1(X)c_0(X)\right).$$

Continuing in the same way, we find that

$$a_k(X) = a_n(X) \sum_{i+j=k} b_i(X)c_j(X),$$

for $k = 0, 1, \ldots, n$. If we set

$$\beta(X, Y) = \sum_{i=0}^{k} b_i(X)Y^i \qquad \text{and} \qquad \gamma(X, Y) = \sum_{j=0}^{l} c_j(X)Y^j,$$

then

$$f(X, Y) = a_n(X)\beta(X, Y)\gamma(X, Y),$$

which implies that $f(X, Y)$ is not irreducible, a contradiction. It follows that, for any proper subset S of $\mathbf{N}_n$, either β or γ has a coefficient y which is not a polynomial function with rational coefficients.

If we replace the b_i and c_j with quotients of polynomial functions with rational coefficients, then analogous calculations to those which we have just employed show that $f(X, Y)$ is reducible in $F(X)[Y]$, which from Gauss's Lemma is not possible, because $f(X, Y)$ is irreducible in $F[X][Y]$. Therefore we may assume that y is not even a quotient of polynomial functions with rational coefficients. We number the distinct functions functions $y_1, \ldots, y_{2^n-2}$. (We do not say that these functions are distinct; certain of them may be the same.)

2. A condition for the irreducibility of $f(s, Y)$: Suppose that $s \in N \cap \mathbf{Q}$ and that $y_1(s), \ldots, y_{2^n-2}(s)$ are all in $\mathbf{C} \setminus \mathbf{Q}$. We claim that $f(s, Y)$ is irreducible in $\mathbf{Q}[Y]$. Indeed, we can always write

$$f(s, Y) = a_n(s) \prod_{i \in S} (-u_i(s) + Y) \prod_{i \notin S} (-u_i(s) + Y),$$

for any proper subset S of $\mathbf{N}_n$. As s is rational, $a_n(s)$ is also rational. If we evaluate the coefficients of β and γ at s, we obtain the coefficients of $\prod_{i \in S} (-u_i(s) + Y)$ and $\prod_{i \notin S} (-u_i(s) + Y)$. By the choice of s, at least one of these coefficients is not rational. Thus, $f(s, Y)$ is irreducible in $\mathbf{Q}[Y]$. In order to prove our theorem, it is sufficient to obtain an infinite number of elements $s \in N \cap \mathbf{Q}$ such that $y_1(s), \ldots, y_{2^n-2}(s)$ are all in $\mathbf{C} \setminus \mathbf{Q}$.

3. Studying the functions y_j: We aim to look at the functions y_j in more detail. To simplify the notation, let us write y for y_j. We notice that there exists $T' > 0$ such that $s_0 + \frac{1}{t} \in N$, if $t > T'$. We define the function δ on (T', ∞) by

$$\delta(t) = y(s_0 + \frac{1}{t}).$$

Let us denote $\mathcal{G}$ the set of functions defined on (T', ∞) by

$$\xi(t) = \frac{h(t)}{g(t)},$$

where h and g are polynomial functions with rational coefficients and g is not the zero function. Clearly, $\mathcal{G}$ is a field. We claim that δ is algebraic over $\mathcal{G}$. To see this, first let us define the function v_i on (T', ∞) by

$$v_i(t) = u_i(s_0 + \frac{1}{t}).$$

Then, for all $t > T'$, we have

$$a_0(s_0 + \frac{1}{t}) + a_1(s_0 + \frac{1}{t})v_i(t) + a_2(s_0 + \frac{1}{t})v_i(t)^2 + \cdots + a_n(s_0 + \frac{1}{t})v_i(t)^n = 0.$$

Multiplying by the appropriate power of t, we obtain the expression

$$h_0(t) + h_1(t)v_i(t) + h_2(t)v_i(t)^2 + \cdots + h_n(t)v_i(t)^n,$$

where $h_0, \ldots, h_n$ are polynomial functions defined on (T', ∞), with coefficients in $\mathbf{Q}$. Hence,

$$h_0 + h_1 v_i + h_2 v_i^2 + \cdots + h_n v_i^n$$

is the zero function and so v_i is algebraic over $\mathcal{G}$. As the algebraic elements over a field form a field, δ is algebraic over $\mathcal{G}$ and so is the root of an equation

$$d_0 + d_1 H \ldots + \ldots d_m H^m = 0,$$

where $d_0, \ldots, d_m \in \mathcal{G}$ and 0 denotes the zero function. We may suppose that the d_i are polynomial functions. (It is sufficient to multiply by the product of the denominators of the d_i, if necessary.) We may even suppose that the coefficients of the polynomial functions d_i are integers. We now multiply the coefficients of the equation satisfied by δ by d_m^{m-1} to obtain

$$d_0 d_m^{m-1} + d_1 d_m^{m-2} d_m \delta + d_2 d_m^{m-3}(d_m \delta)^2 + \cdots + d_{m-1}(d_m \delta)^{m-1} + (d_m \delta)^m = 0.$$

19

Thus $z = d_m \delta$ is a root of the polynomial

$$g(Z) = b_0 + b_1 Z + \cdots + b_{m-1} Z^{m-1} + Z^m, \qquad (5) \qquad \boxed{\texttt{eqnHILBIRRED2}}$$

where $b_j = d_j d_m^{m-j-1}$, for $j = 0, 1, \ldots, m-1$. Clearly, the coefficients of $g(Z)$ are integers. We claim that, if $t \in \mathbf{Z}$, with $t > T'$, and $\delta(t) \in \mathbf{Q}$, then $z(t) \in \mathbf{Z}$. Indeed, $z(t) = d_m(t)\delta(t)$ implies that $z(t) \in \mathbf{Q}$. Also, $z(t)$ is a root of the equation

$$b_0(t) + b_1(t)Z + \cdots + b_{m-1}(t)Z^{m-1} + Z^m,$$

which is a monic polynomial with coefficients in $\mathbf{Z}$. From Exercise $\overset{\texttt{exerHILBIRRED2}}{2,}$ $z(t)$ is an integer.

4. Studying the functions z_j: To simplify the notation, we will write z for z_j: Our next step is to show that there are relatively few integers $t > T'$ such that $z(t)$ is an integer. If this is the case, then we may find many integers t such that $z(t)$ is not an integer. For such t, $\delta(t)$ cannot be rational, which implies that $y(s_0 + \frac{1}{t})$ is not rational.

Lemma $\overset{\texttt{lemHILBIRRED1}}{3}$ ensures us that, for $i = 1, \ldots, n$, u_i is an analytic function on the neighbourhood N of s_0. As sums and products of analytic functions are analytic, for $j = 1, \ldots, 2^n - 2$, y_j is analytic on N. Reducing the size of N to a neighbourhood N' of s_0 if necessary, for $s_0 + x \in N'$, we may write

$$y(s_0 + x) = e_0 + e_1 x + e_2 x^2 + \ldots + e_k x^k + \ldots,$$

where the coefficients $e_i \in \mathbf{C}$. There exists $T'' \geq T'$ such that, if $t > T''$, then $y(s_0 + \frac{1}{t}) \in N'$ and so

$$y(s_0 + \frac{1}{t}) = e_0 + e_1 \frac{1}{t} + e_2 \left(\frac{1}{t}\right)^2 + \ldots + e_k \left(\frac{1}{t}\right)^k + \ldots.$$

As d_m is a polynomial, we may write

$$z(t) = d_m(t)\delta(t) = d_m(t)y(s_0 + \frac{1}{t}) = c_l t^l + \cdots + c_1 t + c_0 + c_{-1} t^{-1} + \cdots + c_{-k} t^{-k} + \cdots,$$

with $c_i \in \mathbf{C}$.

There are three possibilities:

- **a.** z is a polynomial function;

- **b.** z is not a polynomial function and has at least one coefficient $c_i \in \mathbf{C} \setminus \mathbf{R}$;

- **c.** z is not a polynomial function and all the coefficients of z are real.

We consider the first case. We claim that at least one of the coefficients must be in $\mathbf{C} \setminus \mathbf{Q}$. If this is not the case, then $\delta(t) = \frac{z(t)}{d_m(t)}$, for $t > T''$. Let (t_n) be sequence of values of $t > T''$ converging to ∞. If we set $s_n = s_0 + \frac{1}{t_n}$, then the numbers s_n converge to s_0 and

$$y(s_n) = y(s_0 + \frac{1}{t_n}) = \delta(t_n) = \frac{z(t_n)}{d_m(t_n)} = \frac{z((s_n - s_0)^{-1})}{d_m((s_n - s_0)^{-1})}.$$

If we multiply both z and d_m by an appropriate power of $s_n - s_0$, then we may find polynomial functions with rational coefficients $\hat{z}$ and $\hat{d}_m$ such that

$$\frac{z((s_n - s_0)^{-1})}{d_m((s_n - s_0)^{-1})} = \frac{\hat{z}(s_n)}{\hat{d}_m(s_n)}.$$

20

From Lemma 5, we obtain that $y = \frac{\hat{z}}{d_m}$, a contradiction. (We can apply Lemma 5, because y and $\frac{\hat{z}}{d_m}$ are defined on the connected set N.) This proves our claim. Thus at least one coefficient of z belongs to the set $\mathbf{C} \setminus \mathbf{Q}$. Consequently, from Exercise 1, there can only be a finite number of integers t such that $z(t)$ is an integer. In this case we may choose $T''' > T''$ such that $z(t)$ is not an integer, if $t > T'''$.

Let us now consider the second case. Suppose that i_0 is the largest subscript i for which $c_i \in \mathbf{C} \setminus \mathbf{R}$. Then

$$\lim_{t \to \infty} \frac{\operatorname{Im} z(t)}{t^{i_0}} = \operatorname{Im} c'_{i_0} \neq 0.$$

Hence, we may find $T''' \geq T''$ such that $\frac{z(t)}{t^{i_0}} \notin \mathbf{R}$, for $t > T'''$. This implies that $z(t) \notin \mathbf{R}$ and so is not an integer, for $t > T'''$.

The third case is more difficult to handle. Here all the coefficients c_i are real and at least one coefficient c_i, with i negative, is nonzero. By differentiating z a sufficient number of times we can eliminate all nonnegative powers of t to obtain

$$z^{(m)}(t) = pt^{-q} + \cdots,$$

where p is a nonzero real number, q a positive integer greater than m and the dots represent terms of higher powers of t^{-1}. As

$$\lim_{t \to \infty} t^q z^{(m)}(t) = p,$$

there exists $T''' \geq T''$ such that

$$t > T''' \implies 0 < |z^{(m)}(t)| \leq 2|p|t^{-q}.$$

Now we use Lemma 4. Let $t_0 < t_1 < \cdots < t_m$ be integers such that $t_i \geq T'''$ and $z(t_i) \in \mathbf{Z}$, for all i. For a certain number $u \in (t_0, t_m)$ we have

$$\frac{2|p|}{m! t_0^q} > \frac{2|p|}{m! u^q} \geq \frac{|z^{(m)}(u)|}{m!} = \frac{|W_m|}{|V_m|}.$$

As $z^{(m)}(u) \neq 0$, $W_m \neq 0$, which implies that W_m is a positive integer and so $|W_m| \geq 1$. Therefore

$$\frac{m!}{2|p|} t_0^q < |V_m| = \prod_{i>j}(t_i - t_j) < (t_m - t_0)^{\frac{m(m-1)}{2}}.$$

This implies that there are positive constants α and β such that $\alpha t_0^\beta < t_m - t_0$.

Now let r be the number of distinct functions z_j in this third case. Without loss of generality, let us suppose that these are the functions $z_1, \ldots, z_r$. For each j, we have m_j, α_j and β_j such that, if we have integers $t_0 < t_1 < \ldots < t_{m_j}$, with $z_j(t_i) \in \mathbf{Z}$, for $i = 0, 1, \ldots, m_j$, then $\alpha_j t_0^{\beta_j} < t_{m_j} - t_0$. We set $\bar{m} = \max m_j$ and take $U \in \mathbf{Z}$ such that $\alpha_j U^{\beta_j} \geq rm$. We now consider the interval $I = [U, U + rm]$. If $t_0 < t_1 < \ldots < t_{m_j}$ is a sequence of $m_j + 1$ integers in I, then

$$\alpha_j t_0^{\beta_j} \geq \alpha_j U^{\beta_j} \geq rm = (t_0 + rm) - t_0.$$

This implies that I contains at most m_j integers t such that $z_j(t) \in \mathbf{Z}$.

If we now consider all the z_j in the third case, we see that the interval contains at most $m_1 + \ldots + m_r$ integers t such that $z_j(t) \in \mathbf{Z}$ for some $j = 1, \ldots, r$, i.e., at most rm integers t

such that $z_j(t) \in \mathbf{Z}$, for some $j = 1, \ldots, r$. However, I contains $nm + 1$ integers, so there is at least one integer $t \in I$ such that $z_j(t) \notin \mathbf{Z}$, for $j = 1, \ldots, r$. We may find an infinite number of such t by taking a sequence of intervals $I_k = [U_k, U_k + rm]$, with $U_{k+1} > U_k + rm$.

5. The final step: Using ou previous work, we show that there is an infinite sequence of integers t such that $z_j(t)$ is not an integer, for all z_j. As we have seen, there are three possibilities for z_j. For those which fall in the categories **a** or **b.**, there is a number T''' such that, if $t > T'''$, then $z_j(t) \notin \mathbf{Z}$. If we take T'''' equal to be the maximum of all such T''', then $z_j(t) \notin \mathbf{Z}$, for those $z_j(t)$, where z_j is in either category **a.** or **b.** If the category **c.** is empty, then we have finished.

If this is not the case and $z_1, \ldots, z_r$ belong to the third case, then we can find a sequence of integers t such that $z_j(t) \notin \mathbf{Z}$, for $j = 1, \ldots, r$. We may take these integers greater than T'''' and so we have an infinite sequence of integers t such that $z_j(t) \notin \mathbf{Z}$ for all j. This finishes the proof.$\square$

Remark The rational numbers b, which we have found, such that $f_b(Y)$ is irreducible are of the form $s_0 + t^{-1}$, where t is a positive integer. Of course, there are certainly others: we only need to take s_0' sufficiently far from s_0.

Exercise 3 *In section 4 of the above proof, we assumed that W_m is an integer. Why is this so?*

Remark In this article we have been concerned with irreducible specializations. We have not considered reducible specializations. For many number fields K the number of reducible specializations of irreducible polynomials in $K[X,Y]$ is infinite. However, there are number fields with irreducible polynomials for which this is not the case. For a recent discussion of this question see [3].

Basic results from Galois theory

`ufd` **Result 1** *Let R be a unique factorization domain, with quotient field F, and $f \in R[X]$. Then, if f is nonconstant and irreducible in $R[X]$, then f is irreducible in $F[X]$. On the other hand, if f is primitive and irreducible in $F[X]$, then f is irreducible in $R[X]$.*

`lemSPLIT1` **Result 2** *Let $f \in F[X]$ be irreducible and E an extension of F which contains a root α of f. Then there is an isomorphism*

$$\Phi : F[X]/(f) \longrightarrow F(\alpha)$$

which fixes F, i.e., for g constant, $\Phi(g + (f)) = g$, and such that $\Phi(X + (f)) = \alpha$.

`thSPLIT2` **Result 3** *Let F and F' be fields, $\sigma : F \longrightarrow F'$ an isomorphism, $f \in F[X]$ and $f^* \in F'[X]$ the polynomial corresponding to f. If E is a splitting field of f and E' a splitting field of f^*, then there is an isomorphism $\tilde{\sigma} : E \longrightarrow E'$ extending σ.*

`propSPLIT2` **Result 4** *Let $\sigma : F \longrightarrow F'$ be an isomorphism and $f \in F[X]$ irreducible. If E (resp. E') is an extension of F (resp. F') and α (resp. α') a root of f (resp. f^*) in E (resp. E'), then there is an isomorphism $\hat{\sigma} : F(\alpha) \longrightarrow F'(\alpha')$ extending σ, with $\hat{\sigma}(\alpha) = \alpha'$. This isomorphism is unique.*

`thSEPext4` **Result 5** *Let E be a finite separable extension of a field F of degree n. Then the field of fractions $E(X)$ is a finite extension of degree n of the field of fractions $F(X)$.*

NORMALprop2 · **Result 6** *Suppose that K/F and E/K, with E normal over F. Then E is normal over K.*

NORMALth1 · **Result 7** *The finite extension E of F is normal if and only if E is the splitting field of a polynomial $f \in F[X]$.*

NormalClos1 · **Result 8** *If E is finite extension of the field F and N the normal closure of E over F, then N is a finite extension of F.*

thGALGRP1 · **Result 9** *If E is a finite Galois extension of F, then we have $|Gal(E/F)| = [E : F]$.*

thGALPOLYirred1 · **Result 10** *Let f be a separable polynomial in $F[X]$ of degree n with Galois group $G = Gal(E/F)$. If $f \in F[X]$ is irreducible, then the action of G on the set of roots of f is transitive.*

References

hadlock · [1] C.R. Hadlock, *Field theory and its classical problems*, Math. Assoc. America, 1978.

henrici · [2] P. Henrici, *Applied and computational complex analysis, Vol 1*, Wiley, 1974.

muller · [3] P. Müller, *Finiteness results for Hilbert's irreducibility theorem*, arXiv:math/010907v1, 2018.

rotman · [4] J. Rotman, *Galois theory 2nd edition*, Springer, 1998.

spindler · [5] K. Spindler, *Abstract algebra with applications vol 2*, 1994, Marcel Dekker.