CAMBRIDGE

Cambridge University Press
978-0-521-06503-0 - Groups as Galois Groups: An Introduction
Helmut Volklein
Excerpt
More information

Part One

The Basic Rigidity Criteria

1
Hilbert's Irreducibility Theorem

The definition and basic properties of hilbertian fields are given in Section 1.1. Section 1.2 contains the proof of Hilbert's irreducibility theorem (which says that the field $\mathbb{Q}$ is hilbertian). We give the elementary proof due to Dörge [Do] (see also [La]).

Section 1.3 is not necessary for someone interested only in Galois realizations over $\mathbb{Q}$. It centers around Weissauer's theorem, which shows that many infinite algebraic extensions of a hilbertian field are hilbertian. As our main application we deduce that the field $\mathbb{Q}_{\text{ab}}$ generated by all roots of unity is hilbertian. Next to $\mathbb{Q}$ itself, this field is the one that has attracted the most attention in the recent work on the Inverse Galois Problem. This is due to Shafarevich's conjecture (see Chapter 8).

In this chapter, k denotes a field of characteristic 0. (Most results remain true in positive characteristic, with suitable modifications; see [FJ], Chs. 11 and 12.) We let $x, y, x_1, x_2, \ldots$ denote independent transcendentals over k. Thus $k[x_1, \ldots, x_m]$ is the polynomial ring, and $k(x_1, \ldots, x_m)$ the field of rational functions over k in $x_1, \ldots, x_m$.

1.1 Hilbertian Fields

1.1.1 Preliminaries

We will use elementary Galois theory, as developed in most introductory algebra books, without further reference. (See, e.g., [Jac], I, Ch. 4). The most useful single result will be Artin's theorem (saying that if G is a finite group of automorphisms of a field K then K is Galois over the fixed field F of G and $G(K/F) = G$).

If K is a field with subfield k, we say K is *regular over* k if k is algebraically closed in K.

Lemma 1.1 *Suppose $x_1, \dots, x_m$ are algebraically independent over k, and set $\mathbf{x} = (x_1, \dots, x_m)$. Let $\bar{k}$ be an algebraic closure of k.*

(i) If k'/k is finite Galois, then $k'(\mathbf{x})/k(\mathbf{x})$ is finite Galois, 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 $K = k(\mathbf{x})[y]/(f)$ be the corresponding field extension of $k(\mathbf{x})$. Then K is regular over k if and only if f is irreducible over $\bar{k}(\mathbf{x})$. If this holds, then $f(\mathbf{x}, y)$ is irreducible over $k_1(\mathbf{x})$ for every extension field k_1 of k such that $x_1, \dots, x_m, y$ are independent transcendentals over k_1.

Proof. (i) The group $G = G(k'/k)$ acts naturally on $k'(\mathbf{x})$ (fixing $x_1, \dots, x_m$), with fixed field $k(\mathbf{x})$. By Artin's theorem, $k'(\mathbf{x})/k(\mathbf{x})$ is Galois with group G. The last part of (i) follows now by using the Galois correspondence.

(ii) Let $\hat{k}$ be the algebraic closure of k in K, and let α be the image of y in K (thus $f(\alpha) = 0$). Then α satisfies a polynomial $\hat{f}(y) \in \hat{k}(\mathbf{x})[y]$ of degree $[K : \hat{k}(\mathbf{x})]$, and $\hat{f}$ divides f. It follows that if $\hat{k} \neq k$ then f is not irreducible in $\hat{k}(\mathbf{x})[y]$, hence not in $\bar{k}(\mathbf{x})[y]$.

Conversely, assume $\hat{k} = k$, and let k' be any finite Galois extension of k. Let K' be the composite of K and $k'(\mathbf{x})$ inside some algebraic closure of $k(\mathbf{x})$. By (i) we have $K \cap k'(\mathbf{x}) = k''(\mathbf{x})$ for some k'' between k and k'. Then $k'' \subset \hat{k}$, hence $k'' = k$. Thus $K \cap k'(\mathbf{x}) = k(\mathbf{x})$. Since $k'(\mathbf{x})/k(\mathbf{x})$ is Galois (by (i)), it follows that $[K' : k'(\mathbf{x})] = [K : k(\mathbf{x})]$. But $K' = k'(\mathbf{x})[\alpha]$, hence f is irreducible over $k'(\mathbf{x})$. Since k' was an arbitrary finite Galois extension of k, it follows that f is irreducible over $\bar{k}(\mathbf{x})$.

For the last claim, suppose f decomposes as $f = gh$ for $g, h \in k_1(\mathbf{x})[y]$, of degree ≥ 1 in y. Without loss, g is monic in y. We may assume that k_1 is generated over k by the coefficients of g (where g is viewed as a rational function in $x_1, \dots, x_m, y$), and that one such coefficient, call it t, is transcendental over k. By Remark 1.2 below, k_1 is finite over a field $k_2 = k(t_1, \dots, t_s)$, where $t_1, \dots, t_s$ are independent transcendentals over k, and $t = t_1$. There is an infinite subset $A \subset \mathrm{Aut}(k_2/k)$ such that all $\alpha \in A$ take distinct values on t (e.g., $\alpha(t) = t + c$, $c \in k$, and $\alpha(t_i) = t_i$ for $i > 1$). These α can be extended to embeddings of k_1 into $\bar{k}_2$, and further to embeddings of $k_1(\mathbf{x})[y]$ into $\bar{k}_2(\mathbf{x})[y]$ (fixing $x_1, \dots, x_m, y$). Applying these embeddings to g we obtain infinitely many (distinct) divisors of f in $\bar{k}_2(\mathbf{x})[y]$, all of them monic in y. This contradiction completes the proof. □

Remark 1.2 Suppose $k_1 = k(a_1, \dots, a_r)$ is a finitely generated extension of k. If $t_1, \dots, t_s$ is a collection of elements among $a_1, \dots, a_r$, maximal with respect to being algebraically independent over k, then k_1 is finite over the purely transcendental extension $k(t_1, \dots, t_s)$ of k. (Indeed, k_1 is finitely generated and algebraic, hence finite over $k(t_1, \dots, t_s)$.)

Lemma 1.3 *Let α be algebraic over the field L. Let $f(y) = \sum_{i=0}^{n} a_i y^i$ be a polynomial over L of degree $n > 0$ with $f(\alpha) = 0$. Then*

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

is a monic polynomial of degree n with $g(a_n\alpha) = 0$. Clearly, $L(\alpha) = L(a_n\alpha)$.

Proof. Clear. □

Let $f(y) \in D[y]$ be a polynomial over the factorial domain D of degree ≥ 1. Recall that $f(y)$ is irreducible in $D[y]$ if and only if it is irreducible in $F[y]$, where F is the field of fractions of D. Further, $f(y)$ is called primitive if it is nonzero, and the g.c.d. of its nonzero coefficients is 1. If $g(y)$ is a nonzero polynomial over F, then there is $d \in F$, unique up to multiplication by units of D, such that $d \cdot g(y)$ is primitive. Further, a polynomial ring in any (finite) number of variables over a field is factorial. (For all this, see, e.g., [Jac], I, Ch. 2.)

Lemma 1.4 *Let $f(x_1, \dots, x_s)$ be a polynomial in $s \geq 2$ variables over k, of degree ≥ 1 in x_s. Then f is irreducible as polynomial in s variables if and only if f is irreducible and primitive when viewed as polynomial in x_s over the ring $D = k[x_1, \dots, x_{s-1}]$. Note that f is irreducible over D if and only if f is irreducible over $F = k(x_1, \dots, x_{s-1})$.*

Proof. First assume f is irreducible and primitive when viewed as polynomial in x_s over D. If then $f = gh$ for polynomials g, h in $x_1, \dots, x_s$ then one of these polynomials, say g, must actually be a polynomial in $x_1, \dots, x_{s-1}$. Since f is primitive, it follows that g is a unit in D, hence $g \in k$. This proves that f is irreducible as a polynomial in s variables. The converse is clear. For the last statement in the Lemma, see above. □

1.1.2 Specializing the Coefficients of a Polynomial

First a basic lemma about specializing a Galois extension. This lemma will be used several times, in particular in Chapter 10 for a problem in positive characteristic. Therefore we allow fields of any characteristic (just in this Lemma 1.5).

Recall that a polynomial (in one variable) is called separable if it has no multiple roots. The discriminant of a monic polynomial $p(y)$ is a polynomial function (over $\mathbb{Z}$) in the coefficients of p. It is nonzero if and only if p is separable.

Lemma 1.5 *Let K/F be a finite Galois extension with Galois group G. Let R be a subring of F, having F as a field of fractions. Let α be a generator for K over F, satisfying $f(\alpha) = 0$ for some monic polynomial $f(y) \in R[y]$ of degree $n = [K : F]$. Finally, let A be a finite subset of K containing α, and invariant under G. Let $S = R[A]$ (the subring of K generated by R and A). Then there is $u \neq 0$ in R such that for each (ring-) homomorphism ω from R to a field F' satisfying $\omega(u) \neq 0$ the following holds:*

1. *ω extends to a homomorphism $\tilde{\omega} : S \to K'$, where K' is a finite field extension of F'. We may assume that K' is generated over F' by $\tilde{\omega}(S)$.*
2. *For each such $\tilde{\omega}$, the field K' is Galois over F', and is generated over F' by $\alpha' = \tilde{\omega}(\alpha)$. We have $f'(\alpha') = 0$, where $f'(y) \in F'[y]$ 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 this case, K' is F'-isomorphic to $F'[y]/(f')$.*
3. *Now suppose f' is irreducible. Then for each $\tilde{\omega}$ as in (1), there is a unique isomorphism $G \to G' = G(K'/F')$, $\sigma \mapsto \sigma'$, such that $\tilde{\omega}(\sigma(s)) = \sigma'(\tilde{\omega}(s))$ for all $\sigma \in G$, $s \in S$.*

Proof. Since K/F is Galois, the polynomial $f(y)$ is separable, hence its discriminant D_f is a nonzero element of R. Further, $\omega(D_f)$ is the discriminant of the polynomial $f'(y)$ obtained by applying ω to the coefficients of f. We will only consider such ω with $\omega(D_f) \neq 0$. Then $f'(y)$ is separable.

The ideal I of $R[y]$ generated by f is the kernel of the natural map $R[y] \to R[\alpha]$, $h \mapsto h(\alpha)$. Indeed, if $h \in R[y]$ with $h(\alpha) = 0$ then by elementary field theory we have $h = gf$ for some $g \in F[y]$. Write $f = \sum_{i=0}^{n} a_i y^i$, $g = \sum_{j=0}^{m} b_j y^j$ with $a_i \in R$, $b_j \in F$. Since f is monic in y, it follows that $b_m \in R$ (because it equals the highest y-coefficient of h). The second highest y-coefficient of h equals $b_{m-1} + b_m a_{n-1}$, hence $b_{m-1} \in R$. Continuing like this, we see that all $b_j \in R$. Hence $g \in R[y]$, and thus $h \in I$. This yields a natural isomorphism

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

Step 1 We first consider the special case that $R[A] = R[\alpha]$. We show that (1)–(3) hold for each homomorphism $\omega : R \to F'$ with $\omega(D_f) \neq 0$.

Extend ω to a map $R[y] \to F'[y]$ (fixing y). This map sends f to f', hence induces a homomorphism

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

Let

$$\chi = \psi \circ \phi^{-1} : R[\alpha] \to F'[y]/(f').$$

(1). Set $K' = F'[y]/(g')$, where g' is an irreducible factor of f'. Then K' is a finite field extension of F'. Composing χ with the natural map $F'[y]/(f') \to F'[y]/(g') = K'$ we obtain a homomorphism $S = R[\alpha] \to K'$ that extends ω. This proves (1).

(2). We have $K' = F'[\tilde{\omega}(S)] = F'[\tilde{\omega}(\alpha)] = F'[\alpha']$ (because $S = R[\alpha]$ by hypothesis in Step 1).

The conjugates $\alpha_1, \dots, \alpha_n$ of α over F all lie in $A \subset S$ (by hypothesis). Let $\alpha'_1, \dots, \alpha'_n$ be their $\tilde{\omega}$-images. Applying $\tilde{\omega}$ to $f(y) = (y - \alpha_1)\cdots(y - \alpha_n)$ we get $f'(y) = (y - \alpha'_1)\cdots(y - \alpha'_n)$. Hence K' contains all conjugates of α' over F', and therefore is normal over F'. Also, K'/F' is separable (since f' is), hence K'/F' is Galois. The rest of (2) is clear.

(3). Assume f' is irreducible. Then $\alpha'_1, \dots, \alpha'_n$ are all conjugate over F' (and are pairwise distinct since f' is separable). Thus for each $i = 1, \dots, n$ there is a unique $\sigma'_i \in G' = G(K'/F')$ mapping α' to α'_i. Also, there is a unique $\sigma_i \in G = G(K/F)$ mapping α to α_i. Thus $\sigma_i \mapsto \sigma'_i$ is a bijection from G to G'.

Now fix some s in $S = R[\alpha]$. We can write it in the form $s = h(\alpha)$ with $h(y) \in R[y]$. Let $h'(y) \in F'[y]$ be obtained by applying ω to the coefficients of h. Then $\sigma'_i(\tilde{\omega}(s)) = \sigma'_i(\tilde{\omega}(h(\alpha))) = \sigma'_i(h'(\alpha')) = h'(\alpha'_i) = \tilde{\omega}(h(\alpha_i)) = \tilde{\omega}(\sigma_i(h(\alpha))) = \tilde{\omega}(\sigma_i(s))$. This proves that $\sigma'(\tilde{\omega}(s)) = \tilde{\omega}(\sigma(s))$ for all $s \in S$ and $\sigma \in G$. In particular, $(\sigma\tau)'(\alpha') = (\sigma\tau)'(\tilde{\omega}(\alpha)) = \tilde{\omega}(\sigma\tau(\alpha)) = \sigma'(\tilde{\omega}(\tau(\alpha))) = \sigma'\tau'(\alpha')$. Thus the map $\sigma \mapsto \sigma'$ is homomorphic, hence isomorphic. This proves (3).

Step 2 The general case.

Each $a \in A$ can be written as

$$a = \sum_{i=0}^{n-1} b_i \alpha^i$$

with $b_i \in F$. Choose $v \neq 0$ in R such that $vb_i \in R$ for all occurring b_i (as a ranges over A). This is possible because F is the field of fractions of R. Set $u = vD_f$ and $\tilde{R} = R[u^{-1}]$. Then all $b_i \in \tilde{R}$, hence $A \subset \tilde{R}[\alpha]$ and so $\tilde{R}[A] = \tilde{R}[\alpha]$.

If $\omega : R \to F'$ is a homomorphism with $\omega(u) \neq 0$, then ω extends uniquely to a homomorphism $\tilde{R} \to F'$. Now apply Step 1 to $\tilde{R}$, and we are done. □

The next Lemma can be viewed as a very weak analogue of Hilbert's irreducibility theorem (noting that an irreducible polynomial in characteristic 0 is separable). We use the phrase "for almost all" to mean "for all but finitely many."

Lemma 1.6 *Let L be a field, and $f(x, y) \in L[x, y]$ separable as polynomial in y over $L(x)$. Then the specialized polynomial $f(b, y) \in L[y]$ is separable for almost all $b \in L$.*

Proof. By Lemma 1.3 we may assume f is monic as polynomial in y. Its discriminant is an element $D(x) \in L[x]$, nonzero because f is separable (in y). For each $b \in L$, the polynomial $f(b, y) \in L[y]$ has discriminant $D(b)$. Thus $f(b, y)$ is separable for all $b \in L$ different from the roots of $D(x)$. □

Proposition 1.7 *Let K be a Galois extension of $k(x)$ of finite degree $n > 1$. Then there is a polynomial $f(x, y) \in k[x, y]$, monic and of degree n in y, and a generator α of K over $k(x)$ with $f(x, \alpha) = 0$. Further:*

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

(ii) Suppose ℓ is a finite extension of k contained in K. Let $h(x, y) \in \ell[x, y]$ be irreducible as polynomial in y over $\ell(x)$, and assume the roots of this polynomial are contained in K. Then for almost all $b \in k$ the following holds: If $f(b, y)$ is irreducible in $k[y]$, then $h(b, y)$ is irreducible in $\ell[y]$.

(iii) There is a finite collection of polynomials $p_I(x, y) \in k[x][y]$, irreducible and of degree >1 when viewed as polynomial in y over $k(x)$, such that for almost all $b \in k$ the following holds: If none of the specialized polynomials $p_I(b, y) \in k[y]$ has a root in k, then $f(b, y)$ is irreducible in $k[y]$.

Proof. Each generator α of K over $k(x)$ satisfies some polynomial $f(y)$ of degree n over $k(x)$. Multiplying f by some element of $k[x]$ we may view $f = f(x, y)$ as polynomial in two variables over k. By Lemma 1.3 we may assume that f is monic in y. Thus $f(y) = (y - \alpha_1) \cdots (y - \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α over $k(x)$.

For $b \in k$ let $\omega_b : k[x] \to k$ be the evaluation homomorphism $h(x) \mapsto h(b)$. We apply Lemma 1.5 with $F = k(x)$, and with $\omega = \omega_b : R = k[x] \to F' = k$. Then $f'(y)$ (obtained by applying ω to the coefficients of $f(y)$) equals the polynomial $f_b(y) = f(b, y)$. Let $u = u(x) \in R = k[x]$ be as in Lemma 1.5. Then $\omega_b(u) = u(b)$, hence assertions (1) to (3) in Lemma 1.5 hold for all $b \in k$ different from the finitely many roots of u. Assertions (2) and (3) imply claim (i).

Assume from now on that $b \in k$ is not a root of u. Then ω_b extends to $\tilde{\omega} : S \to K'$ where S is a subring of K containing $k[x][\alpha_1, \ldots, \alpha_n]$, and K' a finite Galois extension of k generated by $\tilde{\omega}(S)$. Let $\alpha'_1, \ldots, \alpha'_n$ be the $\tilde{\omega}$-images of $\alpha_1, \ldots, \alpha_n$. Then $f_b(y) = (y - \alpha'_1) \cdots (y - \alpha'_n)$.

(iii). Let I be a proper, nonempty subset of $\{1, \ldots, n\}$. Since f is irreducible as polynomial in y over $k(x)$, the partial product $\prod_{i \in I}(y - \alpha_i)$ cannot lie in $k(x)[y]$. Thus it has some coefficient d_I with $d_I \notin k(x)$. This d_I lies in S (since the α_i are in S), and it satisfies some irreducible polynomial p_I over $k(x)$ of degree >1. We may choose p_I to have coefficients in $k[x]$.

Now assume that f_b is not irreducible. Then there is some I as above such that the polynomial $\prod_{i \in I}(y - \alpha'_i)$ lies in $k[y]$. It follows that $c := \tilde{\omega}(d_I)$ lies in k (since it is a coefficient of this polynomial). Applying $\tilde{\omega}$ to the equation $p_I(x, d_I) = 0$ we obtain $p_I(b, c) = 0$. This proves (iii).

(ii). Assume f_b is irreducible, and write h as

$$h(x, y) = h_0(x) \prod_{i=1}^{t} (y - \beta_i) \tag{1.1}$$

with $h_0(x) \in \ell[x]$ and $\beta_i \in K$. We may assume that the β_i lie in the finite set A from Lemma 1.5, hence in S. Set $\beta'_i = \tilde{\omega}(\beta_i)$.

We may further assume that A contains a generator of ℓ over k. Then $\ell \subset S$. Thus $\tilde{\omega}$ maps the field ℓ isomorphically to a subfield of K' that we identify with ℓ (via $\tilde{\omega}$). Under this identification we get

$$h(b, y) = h_0(b) \prod_{i=1}^{t} (y - \beta'_i)$$

(applying $\tilde{\omega}$ to (1.1)). Further, the map in assertion (3) of Lemma 1.5 maps the subgroup $H = G(K/\ell(x))$ of G onto a subgroup H' of $G(K'/\ell)$.

Since h is irreducible as polynomial in y over $\ell(x)$, it is separable (since $\mathrm{char}(k) = 0$) and the group $H = G(K/\ell(x))$ permutes its roots β_i transitively. Then H' permutes the β'_i transitively. Exclude those finitely many b with $h_0(b) = 0$, and those for which $h(b, y)$ is not separable (see Lemma 1.6). Then the polynomial $h(b, y)$ is separable, and the group $H' \subset G(K'/\ell)$ permutes its roots β'_i transitively. Hence $h(b, y)$ is irreducible over ℓ. □

Corollary 1.8 *The following conditions on k are equivalent:*

(1) For each irreducible polynomial $f(x, y)$ in two variables over k, of degree ≥ 1 in y, there are infinitely many $b \in k$ such that the specialized polynomial $f(b, y)$ (in one variable) is irreducible.
(2) Given a finite extension ℓ/k, and $h_1(x, y), \ldots, h_m(x, y) \in \ell[x][y]$ that are irreducible as polynomials in y over the field $\ell(x)$, there are infinitely many $b \in k$ such that the specialized polynomials $h_1(b, y), \ldots, h_m(b, y)$ are irreducible in $\ell[y]$.
(3) For any $p_1(x, y), \ldots, p_t(x, y) \in k[x][y]$ that are irreducible and of degree >1 when viewed as polynomial in y over $k(x)$, there are infinitely many $b \in k$ such that none of the specialized polynomials $p_1(b, y), \ldots, p_t(b, y)$ has a root in k.

Proof. Clearly, (2) implies (1) and (3) (cf. Lemma 1.4). It remains to prove that each of (1) and (3) implies (2).

Let $h_1(x, y), \ldots, h_m(x, y) \in \ell[x][y]$ be as in (2). Let S_0 be the set of all roots of these polynomials in some algebraic closure of $\ell(x)$. Choose a finite extension K of $\ell(x)$ that contains S_0, and is Galois over $k(x)$.

Now apply the above Proposition: Part (ii) shows the implication (1) $\Rightarrow$ (2). (Note that the polynomial $f(x, y)$ from the Proposition (defining the extension $K/k(x)$) is irreducible as polynomial in two variables by Lemma 1.4.) For the implication (3) $\Rightarrow$ (2), use additionally part (iii). □

Definition 1.9 *A field k is called* **hilbertian** *if it satisfies (one of) the 3 equivalent conditions (1), (2), (3).*

Using (1) and (2) we see that every finite extension of a hilbertian field is hilbertian. In the next section we prove that the field $\mathbb{Q}$ is hilbertian. Thus every algebraic number field (of finite degree over $\mathbb{Q}$) is hilbertian.

1.1.3 Basic Properties of Hilbertian Fields

Lemma 1.10 *Suppose k is hilbertian, and $f(x_1, \ldots, x_s)$ is an irreducible polynomial in $s \geq 2$ variables over k, of degree ≥ 1 in x_s.*

(i) Then there are infinitely many $b \in k$ such that the polynomial $f(b, x_2, \ldots, x_s)$ (in $s - 1$ variables) is irreducible over k.
(ii) For any nonzero $p \in k[x_1, \ldots, x_{s-1}]$ there are $b_1, \ldots, b_{s-1} \in k$ such that $p(b_1, \ldots, b_{s-1}) \neq 0$ and $f(b_1, \ldots, b_{s-1}, x_s)$ is irreducible (as polynomial in one variable).

Proof. First we derive (ii) from (i). We use induction on s. The case $s = 2$ is just (i). Now assume $s > 2$, and the claim holds for $s - 1$. Write p as a polynomial in $x_2, \dots, x_{s-1}$, with certain coefficients $c_j(x_1) \in k[x_1]$. By (i) there is $b_1 \in k$ such that $f'(x_2, \dots, x_s) := f(b_1, x_2, \dots, x_s)$ is irreducible, and $c_j(b_1) \neq 0$ for some j. Then $p'(x_2, \dots, x_{s-1}) := p(b_1, x_2, \dots, x_{s-1})$ is nonzero. Now the induction hypothesis yields $b_2, \dots, b_{s-1} \in k$ such that $p'(b_2, \dots, b_{s-1}) \neq 0$ and $f'(b_2, \dots, b_{s-1}, x_s)$ is irreducible. Thus $(b_1, \dots, b_{s-1})$ is as desired.

It remains to prove (i). Let d be an integer bigger than the highest power of any variable occurring in f. Kronecker's specialization of f is defined as $S_d f(x, y) = f(x, y, y^d, \dots, y^{(d^{s-2})})$ (a polynomial in two variables). Write

$$S_d f(x, y) = g(x) \prod_i g_i(x, y)$$

a product of irreducible polynomials $g_i(x, y)$, of degree ≥ 1 in y, and $g(x) \in k[x]$. Since k is hilbertian, there are infinitely many $b \in k$ such that all $g_i(b, y)$ are irreducible. (Use condition (2) and Lemma 1.4.) Consider only such b from now on. We may additionally assume that $g(b) \neq 0$.

Now assume that $f(b, x_2, \dots, x_s)$ is reducible, say $f(b, x_2, \dots, x_s) = h(x_2, \dots, x_s)h'(x_2, \dots, x_s)$, where h and h' are both not constant. The Kronecker specializations $S_d h(y)$ and $S_d h'(y)$ are defined similarly as above. We have $S_d f(b, y) = S_d h(y) S_d h'(y)$, hence $S_d h(y)$ and $S_d h'(y)$ are each a product of certain $g_i(b, y)$ (up to factors from k). Let $H(x, y)$ and $H'(x, y)$ be the product of the corresponding $g_i(x, y)$. Then $S_d f(x, y) = g(x) H(x, y) H'(x, y)$.

Because of the uniqueness of the d-adic expansion of an integer, there are unique polynomials $\tilde{h}(x_1, \dots, x_s)$, $\tilde{h}'(x_1, \dots, x_s)$ with $S_d \tilde{h} = gH$, $S_d \tilde{h}' = H'$, such that the highest power of $x_2, \dots, x_s$ occurring in $\tilde{h}, \tilde{h}'$ is less than d. If the latter would also hold for $\tilde{f} := \tilde{h}\tilde{h}'$ then we would have $\tilde{f} = f$ because of the uniqueness of the d-adic expansion. This contradicts the irreducibility of f because $\tilde{f} = \tilde{h}\tilde{h}'$ with $\tilde{h}, \tilde{h}'$ not constant.

Thus $\tilde{f}$, when written as polynomial in $x_2, \dots, x_s$, contains a monomial $\kappa(x_1) x_2^{i_2} \dots x_s^{i_s}$ where some $i_\nu \geq d$, and $\kappa \neq 0$. Note that $\tilde{h}(b, x_2, \dots, x_s)$ is a scalar multiple of $h(x_2, \dots, x_s)$. (Compare their Kronecker specializations.) Similarly for h'. It follows that $\tilde{f}(b, x_2, \dots, x_s)$ is a (nonzero) scalar multiple of $f(b, x_2, \dots, x_s)$. This implies that $\kappa(b) = 0$.

There are only finitely many possibilities for κ (up to multiplication with elements of k), corresponding to all decompositions $S_d f = gHH'$. If we choose b distinct from the (finitely many) zeroes of all these κ, then $f(b, x_2, \dots, x_s)$ is irreducible. This proves (i). □