ACTA ARITHMETICA
180.1 (2017)

On Hilbert's irreducibility theorem

by

Abel Castillo (Chicago, IL) and Rainer Dietmann (London)

1. Introduction. One of the fundamental results in Diophantine geometry is Hilbert's irreducibility theorem [7], stating that if $f(X_1, \dots, X_r, T_1, \dots, T_s) \in \mathbb{Q}[X_1, \dots, X_r, T_1, \dots, T_s]$ is irreducible, then there exists a specialisation $\mathbf{t} = (t_1, \dots, t_s) \in \mathbb{Q}^s$ such that

$$f(X_1, \dots, X_r) = f(X_1, \dots, X_r, t_1, \dots, t_s)$$

as a rational polynomial in $X_1, \dots, X_r$ is still irreducible over $\mathbb{Q}[X_1, \dots, X_r]$. In fact, if $r = 1$ then more is true: Suppose that $f(X, T_1, \dots, T_s) \in \mathbb{Q}[X, T_1, \dots, T_s]$ is irreducible and of degree n in X. Consider f as a polynomial in X over the rational function field $L = \mathbb{Q}(T_1, \dots, T_s)$, having roots $\alpha_1, \dots, \alpha_n$ in the algebraic closure $\overline{L}$. As f is irreducible, these roots are distinct, and we can consider the Galois group G of f over L as a subgroup of the symmetric group S_n. Then there exists a specialisation $\mathbf{t} \in \mathbb{Q}^s$ such that the resulting rational polynomial in X is still irreducible and has Galois group G over $\mathbb{Q}$. In fact, if $\mathbf{t}$ is chosen in such a way that the specialised polynomial in X is still of degree n, and separable, then its Galois group $G_{\mathbf{t}}$ over $\mathbb{Q}$ is a subgroup of G (well-defined up to conjugation, see Lemma 1 for the construction of an embedding of $G_{\mathbf{t}}$ into G) and it turns out that 'almost all' specialisations for $\mathbf{t}$ preserve the Galois group, i.e. $G_{\mathbf{t}} = G$.

In this paper we are interested in getting precise quantitative forms of these statements, so in the setting for $r = 1$ above, for fixed f and any subgroup K of G let

$$N_f(H; K) = \#\{\mathbf{t} \in \mathbb{Z}^s : |\mathbf{t}| \le H \text{ and the splitting field of } f(X, \mathbf{t}) \text{ over } \mathbb{Q} \text{ has Galois group } K\},$$

2010 *Mathematics Subject Classification*: 11C08, 11G35, 11R32, 11R45.
Key words and phrases: Hilbert's irreducibility theorem, quantitative bounds, Galois resolvents, integer points on curves and hypersurfaces.
Received 9 December 2015; revised 24 February 2017.
Published online 9 August 2017.

DOI: 10.4064/aa8380-2-2017 © Instytut Matematyczny PAN, 2017

where we use $|\cdot|$ to denote the maximum norm of a vector. Note that without loss of generality we can assume that f has integer coefficients, and in this arithmetic setting we are counting integer specialisations $\mathbf{t}$ of bounded height H. Our first result is the following.

THEOREM 1. *Let $\varepsilon > 0$. Suppose that $f(X, \mathbf{T}) \in \mathbb{Z}[X, T_1, \dots, T_s]$ is irreducible. Let G be the Galois group of $f(X)$ over $\mathbb{Q}(T_1, \dots, T_s)$, and let K be a subgroup of G. Then*

$$N_f(H; K) \ll_{f,\varepsilon} H^{s-1+|G/K|^{-1}+\varepsilon}, \tag{1}$$

where $|G/K|$ denotes the index of K in G.

In particular, this shows that almost all specialisations for $\mathbf{t}$ preserve the Galois group G of f, and specialisations leading to small subgroups of G are rare. Our result is not the first of its kind; Cohen [2, Theorem 2.1], using the large sieve, obtained a bound in a more general number field setting, but with exponent $s - 1/2$ for $G \neq K$ instead of $s - 1 + |G/K|^{-1}$. The first two bounds in the literature that are sensitive to the size of K are apparently due to the second author [4], who in the special case of the polynomial

$$X^n + T_1 X^{n-1} + \cdots + T_n$$

already obtained (1) (see [11] for very recent improvements in this special case when in addition $n \geq 12$), and due to Zywina [15]. Zywina, like Cohen, works over general number fields rather than the rational numbers, but uses the larger sieve instead of the large sieve and obtains the same bound (1) for the number of all specialisations leading to a polynomial having Galois group contained in K, where K is allowed to be any subset of G stable under conjugation, for example a normal subgroup.

Our work makes use of recent advances on bounding the number of points on curves instead of sieve methods, generalising the approach from [4]; note that a somewhat similar line of attack was also used in a few previous papers (see [12], [14], [3]) discussing the related problem of bounding the smallest admissible specialisation in Hilbert's irreducibility theorem. We restrict our attention to the field of rational numbers; the method should generalise to number fields, provided a suitable analogue of [1] holds, and in principle allows for making the implied O-constants explicit, though this was not our focus. It gives sharper bounds than Cohen's and Zywina's results in most cases, namely as soon as K is any non-normal subgroup of G.

To summarise our main result on Hilbert's irreducibility theorem, let us keep the notation above and introduce the quantity

$$E_f(H) = \#\{\mathbf{t} \in \mathbb{Z}^s : |\mathbf{t}| \leq H \text{ and the splitting field of } f(X, \mathbf{t}) \text{ over } \mathbb{Q} \text{ has Galois group different from } G\}.$$

COROLLARY 1. *Keeping the notation and the assumptions from Theorem* 1*, we have*

$$E_f(H) \ll_{f,\varepsilon} H^{s-1+\delta_G+\varepsilon},$$

where

$$\delta_G = \max\{|G/K|^{-1} : K \text{ is a proper subgroup of } G\}.$$

The quantity δ_G in Corollary 1 for many groups can be as large as $1/2$, for example for $G = S_n$, but for many interesting groups it can also be pretty small: for example, if $G = A_n$ and $n \geq 5$, then $\delta_G = 1/n$ (see [5, Theorem 5.2A]). Coming back to the original question of irreducibility, still assuming $r = 1$, let

$$R_f(H) = \#\{\mathbf{t} \in \mathbb{Z}^s : |\mathbf{t}| \leq H \text{ and } f(X, \mathbf{t}) \text{ becomes reducible in } \mathbb{Q}[X]\}.$$

COROLLARY 2. *Keeping the notation and assumptions from Theorem* 1*, we have*

$$R_f(H) \ll_{f,\varepsilon} H^{s-1+\gamma_G+\varepsilon}, \tag{2}$$

where

$$\gamma_G = \max\{|G/K|^{-1} : K \text{ is an intransitive subgroup of } G\}. \tag{3}$$

Of course always $\gamma_G \leq \delta_G$, but often γ_G is much smaller than δ_G. As an example, consider $f(X, T) = X^3 - T$. Clearly, $X^3 - T$ has no root over $\mathbb{Q}(T)$, thus is irreducible, and its discriminant $-27T^2$ is no square in $\mathbb{Q}(T)$, hence $X^3 - T$ has Galois group S_3 over $\mathbb{Q}(T)$, whence $\delta_G = 1/2$ and $\gamma_G = 1/3$. In this example, $f(X, t)$ becomes reducible as soon as t is a third power, so the bound (2) actually turns out to be sharp here.

Let us also remark that in the special case $s = 1$ sometimes more can be done: see for example the papers [6] and [10].

Finally, let us reconsider Hilbert's Irreducibility Theorem in its general form applying to polynomials $F(X_1, \dots, X_r, T_1, \dots, T_s)$ in r variables $X_1, \dots, X_r$. This case can be reduced to the special case $r = 1$ by *Kronecker's specialisation*—see for example [8, Chapter 9, §3], or [2, proof of Theorem 2.5], where it has been shown that if $f(X_1, \dots, X_r, T_1, \dots, T_s) \in \mathbb{Z}[X_1, \dots, X_r, T_1, \dots, T_s]$ is irreducible over $\mathbb{Q}$, then for

$$J_f(H) = \#\{\mathbf{t} \in \mathbb{Z}^s : |\mathbf{t}| \leq H \text{ and } f(X_1, \dots, X_r, \mathbf{t}) \text{ becomes reducible in } \mathbb{Q}[X_1, \dots, X_r]\}$$

one has the upper bound

$$J_f(H) \ll_f H^{s-1/2} \log H. \tag{4}$$

In fact, as in Corollary 2, the exponent $s - 1/2$ in general is sharp, as can be seen for example by considering the polynomial

$$f(X_1, \dots, X_r, T_1, \dots, T_s) = (X_1 + \cdots + X_r)^2 - (T_1 + \cdots + T_s).$$

As in Corollary 2, however, in special cases one can do better.

THEOREM 2. *Let $f(X_1,\dots,X_r,T_1,\dots,T_s) \in \mathbb{Z}[X_1,\dots,X_r,T_1,\dots,T_s]$ be irreducible, and suppose that for some $i \in \{1,\dots,r\}$ the monomial of highest degree in X_i is of the form $X_i^n h$, where $n \geq 1$ and h depends at most on $T_1,\dots,T_s$, but not on any X_j. Moreover, let G be the Galois group of the splitting field of $f(X_i)$, considered as a polynomial over the function field $\mathbb{Q}(X_1,\dots,X_{i-1},X_{i+1},T_1,\dots,T_s)$. Then*

$$J_f(H) \ll_{f,\varepsilon} H^{s-1+\gamma_G+\varepsilon},$$

where γ_G has been defined in (3).

Note that polynomials f not satisfying the assumptions of Theorem 2 regarding the form of the highest degree monomial in one of the variables can be brought into that form after applying a suitable non-singular linear transformation on the variables $X_1,\dots,X_r$ that does not change the property of being reducible or irreducible over the rationals. It seems difficult, though, to control how the relevant G and thus γ_G change in this process.

As we have already remarked, our approach roughly follows [4], using auxiliary varieties based on suitable Galois resolvents, and bounding the number of integral points on these varieties. More care, however, has to be taken in constructing the Galois resolvents in Section 2 to guarantee their irreducibility. In Section 3 we use a result from the literature, stemming itself from an application of the determinant method, to bound the number of integral points on curves, which is enough to deal with the case $s = 1$. For $s > 1$ we use a fibration approach to reduce to this special case of curves. Theorem 1 along with Corollaries 1 and 2 and Theorem 2 will then be proved in Sections 4, 5 and 6.

2. Construction of the Galois resolvents. We will now give a construction of Galois resolvents, polynomials that detect containment of the Galois group of a polynomial in a prescribed group, as given in Lemma 4. To this end we first need some preparations. Keeping the notation from the introduction, we observe that the group G acts on the roots of $f(X,\mathbf{T})$ by permutations, and this gives rise to an injective homomorphism

$$\rho : G \hookrightarrow S_n.$$

For $\mathbf{t} \in \mathbb{Z}^s$, write $G_{\mathbf{t}}$ for the Galois group of the splitting field of $f(X,\mathbf{t})$. To make sense of a comparison between $G_{\mathbf{t}}$ and subgroups of G, we construct an injection of $G_{\mathbf{t}}$ into G that is compatible with the choice of enumeration of roots. In other words, we want the following diagram to commute:

(5)
$$\begin{array}{ccc} G_{\mathbf{t}} & \xhookrightarrow{\ \iota\ } & G \\ & \searrow^{\rho_{\mathbf{t}}} & \downarrow \rho \\ & & S_n \end{array}$$

LEMMA 1. *Suppose that* $\mathbf{t} \in \mathbb{Z}^s$ *satisfies the conditions*

$$\deg f(X, \mathbf{t}) = n \quad \textit{and} \quad \Delta(\mathbf{t}) \neq 0, \tag{6}$$

where $\Delta(\mathbf{T})$ *is the discriminant of* $f(X, \mathbf{T})$ *viewed as a polynomial in* X. *Then there exist injective homomorphisms* ι *and* $\rho_{\mathbf{t}}$ *such that the diagram in* (5) *commutes.*

Proof. Consider the Dedekind domain $\mathbb{Z}(T_1, \ldots, T_{s-1})[T_s]$; the conditions (6) imply that the prime $(T_s - t_s)$ is unramified in the splitting field of $f(X, \mathbf{T})$. Choose a prime $\mathfrak{p}$ in the splitting field of $f(X, \mathbf{t})$ lying above $(T_s - t_s)$, and the injection of the decomposition group of this prime into G gives rise to an injection of the Galois group of $f(X, T_1, \ldots, T_{s-1}, t_s)$ over $\mathbb{Q}(T_1, \ldots, T_{s-1})$ (see for instance [13, Section 1.7, pp. 20–21]). Since the prime $\mathfrak{p}$ is unramified and the reduction $f(X, \mathbf{T})$ modulo $\mathfrak{p}$ has degree n in X, reduction mod $\mathfrak{p}$ sends $\alpha_i(\mathbf{T})$ to $\alpha_i(T_1, \ldots, T_{s-1}, t_s)$. Now suppose that σ is an element of the Galois group of $f(X, T_1, \ldots, T_{s-1}, t_s)$ over $\mathbb{Q}(T_1, \ldots, T_{s-1})$, and suppose that the above injection sends $\sigma \mapsto \overline{\sigma}$ with $\overline{\sigma}(\alpha_i(\mathbf{T})) = \alpha_j(\mathbf{T})$. The injection described above has the property that

$$\sigma(\alpha_i(\mathbf{T}) \pmod{\mathfrak{p}}) = \alpha_j(\mathbf{T}) \pmod{\mathfrak{p}},$$

So we can inject the Galois group of $f(X, T_1, \ldots, T_{s-1}, t_s)$ into S_n by its action on the roots of $f(X, \mathbf{T})$, which is precisely what we need for the diagram to commute. The proof is completed by repeating this procedure one parameter at a time. ∎

LEMMA 2. *Let* $n \in \mathbb{N}$ *and* $z_1, \ldots, z_n, w_1, \ldots, w_n \in \mathbb{C}$. *Suppose that*

$$z_1^k + \cdots + z_n^k = w_1^k + \cdots + w_n^k$$

for all $k \in \{1, \ldots, n\}$. *Then* $\{z_1, \ldots, z_n\} = \{w_1, \ldots, w_n\}$, *i.e. the* z_i *are a permutation of the* w_i *and vice versa.*

Proof. This is a well known result going back to Newton. ∎

LEMMA 3. *Let* $n \in \mathbb{N}$, *let* K *be a subgroup of* S_n, *and let* $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ *be distinct. Further, let* $\{\sigma_1, \ldots, \sigma_m\}$ *be a set of coset representatives for* S_n/K, *where* $m = |S_n/K|$. *Then there exist* $e_1, \ldots, e_n \in \mathbb{N}$, $d_1, \ldots, d_{|K|} \in \mathbb{N}$ *and* $\gamma \in \mathbb{Z}$ *such that all complex numbers*

$$z_i = \sum_{k=1}^{|K|} d_k \sum_{\tau \in K} (\alpha_{\sigma_i(\tau(1))} + \gamma)^{ke_1} \cdots (\alpha_{\sigma_i(\tau(n))} + \gamma)^{ke_n} \qquad (1 \leq i \leq m) \tag{7}$$

are distinct.

Proof. For convenience, let us introduce the notation

$$\begin{aligned}\mathbf{e} &= (e_1, \dots, e_n),\\ w_{i,\tau,\mathbf{e},k,\gamma} &= (\alpha_{\sigma_i(\tau(1))}+\gamma)^{ke_1}\cdots(\alpha_{\sigma_i(\tau(n))}+\gamma)^{ke_n},\\ w_{i,\tau,\mathbf{e},\gamma} &= w_{i,\tau,\mathbf{e},1,\gamma}.\end{aligned}$$

We now show that it is possible to choose $\gamma \in \mathbb{Z}$ and $e_1, \dots, e_n \in \mathbb{N}$ in such a way that

$$w_{i,\tau_1,\mathbf{e},\gamma} \neq w_{j,\tau_2,\mathbf{e},\gamma} \tag{8}$$

for all (i,τ_1) and (j,τ_2) where $i \neq j$ and $\tau_1, \tau_2 \in K$. The condition

$$w_{i,\tau_1,\mathbf{e},\gamma} = w_{j,\tau_2,\mathbf{e},\gamma}$$

is equivalent to

$$\left(\frac{\alpha_{\sigma_i(\tau_1(1))}+\gamma}{\alpha_{\sigma_j(\tau_2(1))}+\gamma}\right)^{e_1}\cdots\left(\frac{\alpha_{\sigma_i(\tau_1(n))}+\gamma}{\alpha_{\sigma_j(\tau_2(n))}+\gamma}\right)^{e_n} = 1,$$

providing all denominators are different from zero. Since $i \neq j$, at least one exponent e_ℓ must be attached to a fraction of the form $\frac{\alpha_s+\gamma}{\alpha_t+\gamma}$ where $s \neq t$ and thus $\alpha_s \neq \alpha_t$. Suppose that all the other exponents e_m where $m \neq \ell$ are fixed. Then we are left with an equation of the form

$$\left(\frac{\alpha_s+\gamma}{\alpha_t+\gamma}\right)^{e_\ell} = c \tag{9}$$

for some $c \in \mathbb{C}$. Now choose $\gamma \in \mathbb{Z}$ large enough, in terms of $\alpha_1, \dots, \alpha_n$ and a sufficiently large parameter H only depending on n, such that (9) always has at most one solution $e_\ell \in \mathbb{N}$ with $e_\ell \leq H$, for all possible choices of $\alpha_s \neq \alpha_t$, ℓ and $c \in \mathbb{C}$. For this fixed γ, we have shown that for all tuples (i,τ_1) and (j,τ_2) where $i \neq j$, we have

$$\#\{e_1, \dots, e_n \in \mathbb{N} : e_\ell \leq H\,(1 \leq \ell \leq n) \text{ and } w_{i,\tau_1,\mathbf{e},\gamma} = w_{j,\tau_2,\mathbf{e},\gamma}\} \ll H^{n-1}.$$

Since there are only $O_n(1)$ possibilities to choose (i,τ_1) and (j,τ_2) with $i \neq j$, but there are $\gg H^n$ vectors $\mathbf{e} \in \mathbb{N}^n$ where $e_\ell \leq H$ $(1 \leq \ell \leq n)$, by choosing H sufficiently large we certainly can find such an exponent vector $\mathbf{e} \in \mathbb{N}^n$ for which (8) holds true. Now fix that vector $\mathbf{e} \in \mathbb{N}^n$ and γ, and write

$$v_{i,k} = \sum_{\tau \in K} w_{i,\tau,\mathbf{e},k,\gamma} \quad (1 \leq i \leq m,\ 1 \leq k \leq |K|).$$

If $i \neq j$, then there exists at least one $k \in \{1, \dots, |K|\}$ such that $v_{i,k} \neq v_{j,k}$: By Lemma 2 the conditions $v_{i,k} = v_{j,k}$ $(1 \leq k \leq |K|)$ would imply

$$\{w_{i,\tau,\mathbf{e},\gamma} : \tau \in K\} = \{w_{j,\tau,\mathbf{e},\gamma} : \tau \in K\},$$

contradicting (8). The complex numbers in (7) are now exactly of the form

$$z_i = \sum_{k=1}^{|K|} d_k v_{i,k} \quad (1 \le i \le m).$$

To make them distinct, it is enough to choose $d_1, \dots, d_{|K|} \in \mathbb{N}$ in such a way that

$$\sum_{k=1}^{|K|} d_k (v_{i,k} - v_{j,k}) \neq 0 \tag{10}$$

whenever $i \neq j$. As shown above, for $i \neq j$ there is at least one non-zero coefficient on the left hand side of (10), whence

$$\#\Big\{d_1, \dots, d_{|K|} \in \mathbb{N}^{|K|} : \sum_{k=1}^{|K|} d_k (v_{i,k} - v_{j,k}) = 0 \text{ and } d_k \le H \ (1 \le k \le |K|)\Big\} \ll H^{|K|-1}.$$

We can now conclude in a similar way as above: Since there are $O_n(1)$ possibilities to choose i and j where $i \neq j$, but there are $\gg H^{|K|}$ vectors $\mathbf{d} \in \mathbb{N}^{|K|}$ where $d_k \le H$ $(1 \le k \le |K|)$, by choosing H sufficiently large we can find a vector $\mathbf{d} \in \mathbb{N}^{|K|}$ such that (10) is true whenever $i \neq j$. This finishes the proof. ∎

The following result generalises [4, Lemma 5] ([1]).

LEMMA 4. *Let $n \in \mathbb{N}$, and let*

$$f(X, \mathbf{T}) = X^n + g_1(\mathbf{T}) X^{n-1} + \cdots + g_n(\mathbf{T})$$

where $g_i \in \mathbb{Z}[T_1, \dots, T_s]$ $(1 \le i \le n)$. Suppose that $f(X) = f(X, \mathbf{T})$, considered as a polynomial in the ring $\mathbb{Q}(\mathbf{T})[X]$, has distinct roots $\alpha_1 = \alpha_1(\mathbf{T}), \dots, \alpha_n = \alpha_n(\mathbf{T})$ in the algebraic closure $\overline{\mathbb{Q}(\mathbf{T})}$ of $\mathbb{Q}(\mathbf{T})$, and let G be the Galois group of the corresponding splitting field operating on $\alpha_1(\mathbf{T}), \dots, \alpha_n(\mathbf{T})$. Moreover, let K be a subgroup of G. Then there exists a Galois resolvent $\Phi_{f,K}$ with the following properties:

(i) *$\Phi_{f,K}$ is a polynomial of the form*

$$\Phi_{f,K}(Z, \mathbf{T}) = Z^m + h_1(\mathbf{T}) Z^{m-1} + \cdots + h_m(\mathbf{T}), \tag{11}$$

where $m = |S_n/K|$ and $h_i \in \mathbb{Z}[T_1, \dots, T_s]$ $(1 \le i \le m)$.

(ii) *If one specialises the parameters $T_1, \dots, T_s$ in $f(X, \mathbf{T})$ to any s-tuple of integers $\mathbf{t} = (t_1, \dots, t_s)$ such that the polynomial $f(X) = f(X, \mathbf{t})$ is separable and its splitting field has Galois group K over $\mathbb{Q}$, then $\Phi_{f,K}(Z) = \Phi_{f,K}(Z, \mathbf{t})$ has an integer root z.*

([1]) Note that in case of $K = \mathbb{Q}$ in that lemma, the additional assumption $a_1, \dots, a_n \in \mathbb{Z}$ is needed, which of course is satisfied in the later application of Lemma 5 in [4].

(iii) *If one factorises $\Phi_{f,K}(Z,\mathbf{T})$ over $\mathbb{Q}[Z,T_1,\dots,T_s]$ into irreducible factors, then each factor has degree at least $|G|/|K|$ in Z.*

Proof. Since the roots $\alpha_1(\mathbf{T}),\dots,\alpha_n(\mathbf{T})$ are distinct, it is possible to specialise $T_1,\dots,T_s$ to an s-tuple $\mathbf{t}$ of complex numbers such that the complex roots $\alpha_1=\alpha_1(\mathbf{t}),\dots,\alpha_n=\alpha_n(\mathbf{t})$ of $f(X)=f(X,\mathbf{t})$ are all distinct. We are therefore in a position to invoke Lemma 3. Keeping the notation from that lemma, we find $e_1,\dots,e_n\in\mathbb{N}$ and $d_1,\dots,d_{|K|}\in\mathbb{N}$, and a $\gamma\in\mathbb{Z}$, such that all the numbers z_i in (7) are distinct. Now since replacing the variable X by $X-\gamma$ does not change the splitting field and thus does not change the Galois group of $f(X,\mathbf{T})$ over $\mathbb{Q}(\mathbf{T})$, and also for fixed $\mathbf{t}\in\mathbb{Z}^s$ does not change the Galois group of $f(X,\mathbf{t})$ over $\mathbb{Q}$, we can without loss of generality assume that $\gamma=0$.

We now define

$$\Phi_{f,K}(Z,\mathbf{T})=\prod_{i=1}^{m}(Z-z_i)=\prod_{i=1}^{m}\Big(Z-\sum_{k=1}^{|K|}d_k\sum_{\tau\in K}\alpha_{\sigma_i(\tau(1))}^{ke_1}\cdots\alpha_{\sigma_i(\tau(n))}^{ke_n}\Big),\tag{12}$$

where $\{\sigma_1,\dots,\sigma_m\}$ is a set of coset representatives for S_n/K.

It is important to keep in mind that by construction the $z_i=z_i(\mathbf{T})$ are distinct, since we can specialise $\mathbf{T}$ so as to end up with distinct complex z_i. By expanding the expression (12), it becomes transparent that $\Phi_{f,K}(Z,\mathbf{T})$ is of the form (11), where the h_i are symmetric polynomials in the z_i with integer coefficients. Any permutation of the α_i just permutes the z_i, so the h_i are symmetric polynomials in the α_i as well, with integer coefficients. Hence, by the fundamental theorem on symmetric functions, the h_i are integer polynomials in the elementary symmetric polynomials in $\alpha_1,\dots,\alpha_n$, which in turn by Vieta's Theorem are of the form $\pm g_i$. This shows that the h_i are integer polynomials in $T_1,\dots,T_s$ and confirms (i).

For (ii) and (iii), we first note that the symmetric group S_n operates on the z_i via

$$\varrho(z_i)=\sum_{k=1}^{|K|}d_k\sum_{\tau\in K}\alpha_{\varrho(\sigma_i(\tau(1)))}^{ke_1}\cdots\alpha_{\varrho(\sigma_i(\tau(n)))}^{ke_n}$$

for all $\varrho\in S_n$.

To show (ii), fix any $\mathbf{t}\in\mathbb{Z}^s$ and consider

$$\tilde{z}=\sum_{k=1}^{|K|}d_k\sum_{\tau\in K}\alpha_{\tau(1)}^{ke_1}\cdots\alpha_{\tau(n)}^{ke_n}.$$

Choosing the σ_i in the same coset of S_n/K as the identity map, one finds that $\tilde{z}$ is one of the z_i occurring on the left hand side of (12). Now suppose that $f(X)=f(X,\mathbf{t})$ has Galois group K over $\mathbb{Q}$. Clearly, $\tau(\tilde{z})=\tilde{z}$ for all $\tau\in K$. This shows that $\tilde{z}\in\mathbb{Q}$. Moreover, $\tilde{z}$ is a root of the monic integer

polynomial $\Phi_{f,K}(Z, \mathbf{t})$, whence the stronger conclusion $\tilde{z} \in \mathbb{Z}$ follows. This finishes the proof of (ii).

For (iii), it is useful to work over the function field $\mathbb{Q}(\mathbf{T})$ rather than over $\mathbb{Q}$. As observed above, the $z_i = z_i(\mathbf{T})$ are then *distinct* elements of the algebraic closure $\overline{\mathbb{Q}(\mathbf{T})}$ of $\mathbb{Q}(\mathbf{T})$. As a consequence,

$$\mathrm{Stab}(z_i) = \{\varrho \in S_n : \varrho(z_i) = z_i\} = \sigma_i K \sigma_i^{-1} \quad (1 \le i \le m),$$

which implies that

$$\{\varrho \in S_n : \varrho(z_i) = z_j\} = \sigma_j \sigma_i^{-1} \mathrm{Stab}(z_i) = \sigma_j K \sigma_i^{-1} \quad (1 \le i, j \le m). \tag{13}$$

These observations are crucial for the following argument: Suppose that $\Phi_{f,K}(Z, \mathbf{T})$ factorises over $\mathbb{Q}$ into $\Phi_1, \Phi_2 \in \mathbb{Q}[Z, T_1, \dots, T_s]$, i.e.

$$\Phi_{f,K}(Z, \mathbf{T}) = \Phi_1(Z, \mathbf{T}) \Phi_2(Z, \mathbf{T}). \tag{14}$$

We can consider $\Phi_{f,K}(Z) = \Phi_{f,K}(Z, \mathbf{T})$ as a monic rational polynomial in Z over $\mathbb{Q}(\mathbf{T})$, and analogously for $\Phi_1(Z) = \Phi_1(Z, \mathbf{T})$. Now (12) provides a factorisation of $\Phi_{f,K}(Z)$ over $\overline{\mathbb{Q}(\mathbf{T})}$ into factors of the form $Z - z_i$. Suppose that Φ_1 has degree $k \ge 1$ in Z. Then by (12), (14) and uniqueness of factorisation, Φ_1 must be of the form

$$\Phi_1(Z) = c \cdot \prod_{j=1}^{k} (Z - z_{i_j})$$

for suitable $c \in \mathbb{Q}$ and distinct $i_j \in \{1, \dots, m\}$. As shown in (13), we have

$$\{\varrho \in S_n : \varrho(z_{i_1}) = z_{i_l}\} = \sigma_{i_l} K \sigma_{i_1}^{-1}$$

for all $l \in \{1, \dots, k\}$. In particular, for given $l \in \{1, \dots, k\}$ there are exactly $|K|$ elements in S_n that map z_{i_1} to z_{i_l}, hence there are at most $k|K|$ elements in S_n that map z_{i_1} to any root z_{i_l} of Φ_1. Therefore, if $|G| > k|K|$, then we can find an element $\varrho \in G$ such that

$$\varrho(z_{i_1}) \notin \{z_{i_1}, \dots, z_{i_k}\}, \tag{15}$$

so $\varrho(z_{i_1})$ is not a root of Φ_1, as all the z_i are distinct elements of $\overline{\mathbb{Q}(\mathbf{T})}$. Now the operation of G on the z_i is that of field automorphisms of the splitting field of $\Phi_{f,K}(Z)$ over $\mathbb{Q}(\mathbf{T})$. Such field automorphisms fix all elements of the ground field $\mathbb{Q}(\mathbf{T})$, and therefore necessarily map any root of a polynomial over $\mathbb{Q}(\mathbf{T})$ to another root of that polynomial. As $\Phi_1(Z) = \Phi_1(Z, \mathbf{T})$ has coefficients in $\mathbb{Q}(\mathbf{T})$, we conclude that $\varrho(z_{i_1}) \in \{z_{i_1}, \dots, z_{i_k}\}$. This contradicts (15). Consequently, $|G| > k|K|$ is impossible. This way we obtain the lower bound

$$k \ge |G|/|K|$$

for the degree in Z of any factor Φ_1 of $\Phi_{f,K}$. ∎

3. Bounding the number of integer points on curves and hypersurfaces

LEMMA 5. *Let $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$ where $a_0 \neq 0$. Then all roots $z \in \mathbb{C}$ of the equation $f(z) = 0$ satisfy the inequality*

$$|z| \leq \frac{1}{\sqrt[n]{2}-1} \cdot \max_{1\leq k\leq n} \sqrt[k]{\left|\frac{a_k}{a_0\binom{n}{k}}\right|}.$$

Proof. This is [9, Theorem 3 in §27]. ∎

LEMMA 6. *Let $F \in \mathbb{Z}[X_1, X_2]$ be irreducible and of degree d. Further, let P_1, P_2 be real numbers such that $P_1, P_2 \geq 1$, and let*

$$N(F; P_1, P_2) = \#\{\mathbf{x} \in \mathbb{Z}^2 : F(\mathbf{x}) = 0 \text{ and } |x_i| \leq P_i \ (1 \leq i \leq 2)\}.$$

Moreover, let

$$Y = \max\Big\{\prod_{i=1}^{2} P_i^{e_i}\Big\}$$

with the maximum taken over all integer 2-tuples (e_1, e_2) for which the corresponding monomial $X_1^{e_1}X_2^{e_2}$ occurs in $F(X_1, X_2)$ with non-zero coefficient. Then

$$N(F; P_1, P_2) \ll_{d,\epsilon} \max\{P_1, P_2\}^{\epsilon} \exp\left(\frac{\log P_1 \log P_2}{\log Y}\right). \tag{16}$$

Proof. This is [1, Theorem 1]; see also [4, Lemma 8] for more details. ∎

It is crucial for our application of Lemma 6 in proving the following result that the bound (16) only depends on the degree d of F, but not on its coefficients.

LEMMA 7. *Let $F(Z; T_1, \dots, T_s) \in \mathbb{Z}[Z; T_1, \dots, T_s]$ be irreducible, and suppose that F is monic of degree m in Z. Further, let*

$$M_F(H) = \#\{\mathbf{t} \in \mathbb{Z}^s : |\mathbf{t}| \leq H \text{ and } F(Z; t_1, \dots, t_s) = 0 \text{ has an integer root } z\}.$$

Then for every $\varepsilon > 0$ we have

$$M_F(H) \ll_{F,\varepsilon} H^{s-1+1/m+\varepsilon}. \tag{17}$$

Proof. Without loss of generality we may assume that $H \geq 2$. Then by Lemma 5, there exists a constant $\alpha \geq 1$, depending at most on F, such that whenever $\mathbf{t} \in \mathbb{C}^s$ with $|\mathbf{t}| \leq H$ and $F(z; t_1, \dots, t_s) = 0$ for some $z \in \mathbb{C}$, then $|z| \leq H^{\alpha}$. We proceed by induction on s.

For $s = 1$, Lemma 6 gives

$$M_F(H) \le \#\{(z, t_1) \in \mathbb{Z}^2 : |z| \le H^\alpha,\ |t_1| \le H,\ F(z; t_1) = 0\}$$
$$\ll_{F,\varepsilon} H^\varepsilon \exp\left(\frac{\alpha(\log H)^2}{\log Y}\right).$$

Now $F(Z; T_1)$ contains the monomial Z^m, whence $Y \ge H^{\alpha m}$, and we obtain

$$M_F(H) \ll_{F,\varepsilon} H^{1/m+\varepsilon},$$

as claimed.

Next, let us discuss the case $s > 1$, assuming that the lemma has already been proved for $s - 1$.

Let us first consider those $t_2, \dots, t_s \in \mathbb{Z}$ bounded in modulus by H such that $F(Z; T_1) = F(Z; T_1, t_2, \dots, t_s)$ is still irreducible over the rationals, as a polynomial in Z and T_1. Then as above the number of permissible z and t_1 can be bounded by $O_{F,\varepsilon}(H^{1/m+\varepsilon})$, since the term Z^m is still present. Taking into account $O(H^{s-1})$ choices for $t_2, \dots, t_s$, we end up with a contribution of $O_{F,\varepsilon}(H^{s-1+1/m+\varepsilon})$, which is compatible with (17).

Next, let us discuss those $t_2, \dots, t_s \in \mathbb{Z}$ bounded in modulus by H such that $F(Z; T_1)$ becomes reducible over $\mathbb{Q}$. As $F(Z; T_1, \dots, T_s)$ is irreducible over $\mathbb{Q}$, by (4) the number of such exceptional specialisations $t_2, \dots, t_s$ can be bounded by $O_{F,\varepsilon}(H^{s-3/2+\varepsilon})$. Now if $F(Z; T_1)$ becomes reducible over $\mathbb{Q}$, each irreducible factor must be at least linear in Z, since $F(Z; T_1)$ is monic in Z. If each irreducible factor is at least quadratic in Z, then by the same argument as above we get a contribution of $O_{F,\varepsilon}(H^{1/2+\varepsilon})$ for the number of zeros of $F(Z; T_1)$, and together with $O_{F,\varepsilon}(H^{s-3/2+\varepsilon})$ possible choices for $t_2, \dots, t_s$ we again end up with a bound compatible with (17).

It remains to discuss those $t_2, \dots, t_s \in \mathbb{Z}$ bounded in modulus by H for which $F(Z; T_1)$ splits off a linear factor in Z. Let U denote the number of such $t_2, \dots, t_s$. We can bound U by the following 'fibration argument': Since F is an integer polynomial, monic in Z, any linear factor of $F(Z; T_1)$ can be assumed to have integer coefficients and being monic in Z. Given a tuple $(t_2, \dots, t_s)$ counted by U, every choice of $t_1 \in \mathbb{Z}$ gives rise to a monic integer one-variable polynomial $F(Z) = F(Z; t_1, t_2, \dots, t_s)$ of degree m having an integer root z. But $F(Z; T_1, \dots, T_s)$ is irreducible over $\mathbb{Q}$, so by Hilbert's irreducibility theorem we can choose $t_1 \in \mathbb{Z}$ such that the specialized polynomial $G(Z; T_2, \dots, T_s) = F(Z; t_1, T_2, \dots, T_s)$ is still irreducible over $\mathbb{Q}$. Then G still is an integer polynomial, only depending on F, and monic of degree m in z. Therefore our inductive assumption is applicable to G, yielding

$$M_G(H) \ll_{F,\varepsilon} H^{s-2+1/m+\varepsilon}.$$

On the other hand, as observed above,

$$M_G(H) \geq U,$$

since all $(t_2, \dots, t_s)$ counted by U, for all $t_1 \in \mathbb{Z}$, in particular our special choice, give rise to a specialized $F(Z)$ having an integer root z. Combining the last two bounds, we obtain

$$U \ll_{F,\varepsilon} H^{s-2+1/m+\varepsilon}.$$

Once $(t_2, \dots, t_s)$ have been fixed, we use the trivial bound $O(H)$ for the t_1's and get a total contribution of $O_{F,\varepsilon}(H^{s-1+1/m+\varepsilon})$, which again is compatible with (17). ∎

4. Proof of Theorem 1. Let us first briefly remark that without loss of generality we may restrict to $f(X, \mathbf{T})$ that are monic in X: For suppose that $f(X, \mathbf{T}) \in \mathbb{Z}[X, T_1, \dots, T_s]$ of degree n in X is given. Then

$$f(X, \mathbf{T}) = g_0(\mathbf{T})X^n + g_1(\mathbf{T})X^{n-1} + \cdots + g_n(\mathbf{T})$$

for suitable $g_0, \dots, g_n \in \mathbb{Z}[T_1, \dots, T_s]$. As f is of degree n in X, the polynomial $g_0(\mathbf{T})$ is not identically zero and will be zero for at most $O_f(H^{n-1})$ values of $\mathbf{t} \in \mathbb{Z}^s$ when $|\mathbf{t}| \leq H$, which is of negligible order of magnitude with respect to Theorem 1. Now consider the polynomial

$$\begin{aligned} h(X, \mathbf{T}) &= g_0(\mathbf{T})^{n-1} f(X/g_0(\mathbf{T}), \mathbf{T}) \\ &= X^n + g_1(\mathbf{T})X^{n-1} + g_0(\mathbf{T})g_2(\mathbf{T})X^{n-2} + \cdots + g_0(\mathbf{T})^{n-1}g_n(\mathbf{T}) \end{aligned}$$

in $\mathbb{Z}[X, T_1, \dots, T_s]$, which shares all relevant properties with $f(X, \mathbf{T})$. Considered over $\mathbb{Q}(T_1, \dots, T_s)$, both f and h have the same splitting field and hence the same Galois group, and for fixed $\mathbf{t} \in \mathbb{Z}^s$ with $g_0(\mathbf{t}) \neq 0$, again f and h over $\mathbb{Q}$ have the same splitting field and hence the same Galois group. In particular, as $f(X, \mathbf{T})$ is irreducible over $\mathbb{Q}$, the same is true for $h(X, \mathbf{T})$. With respect to Theorem 1, we may therefore without loss of generality assume that f is monic in X, i.e. $g_0(T) \equiv 1$.

Now let $\Phi_{f,K}(Z, \mathbf{T})$ be the Galois resolvent from Lemma 4. Then for given $\mathbf{t} \in \mathbb{Z}^s$, if the polynomial $f(X, \mathbf{t})$ has Galois group K over $\mathbb{Q}$, then $\Phi_{f,K}(Z, \mathbf{t})$ has an integer root z. If we factor $\Phi_{f,K}(Z, \mathbf{T})$ over $\mathbb{Q}$, each irreducible factor can be assumed to have integer coefficients, being monic in Z, and having degree at least $|G|/|K| = |G/K|$ in Z. Applying Lemma 7 to each such factor, we immediately obtain Theorem 1.

5. Proof of Corollaries 1 and 2. Let n be the degree of X in $f(X, \mathbf{T})$, so $f(X, \mathbf{T}) = g_0(\mathbf{T})X^n + O(X^{n-1})$ for a suitable $g_0(\mathbf{T}) \in \mathbb{Z}[T_1, \dots, T_s]$. The two corollaries then follow from Theorem 1 on noting that, by Lemma 1, if $f(X, \mathbf{t})$ for some specialisation $\mathbf{t} \in \mathbb{Z}^s$ still is of degree n in X, and separable, then the Galois group K of f over $\mathbb{Q}$ will be a subgroup of G. The exceptional

$\mathbf{t} \in \mathbb{Z}^s$ with $|\mathbf{t}| \leq H$ such that $f(X, \mathbf{t})$ has degree less than n or becomes inseparable are easily seen to be of order or magnitude $O_f(H^{s-1})$ and can therefore be neglected, as they must satisfy $g_0(\mathbf{t}) = 0$ or $\Delta(\mathbf{t}) = 0$, where $\Delta(\mathbf{t})$ is the discriminant of $f(X, \mathbf{t})$. Since f was assumed to be of degree n, the polynomial $g_0(\mathbf{T})$ is not identically zero, and since f was assumed to be irreducible, $\Delta(\mathbf{T})$ cannot be identically zero, whence the bound $O(H^{s-1})$ for those exceptional $\mathbf{t}$ immediately follows.

6. Proof of Theorem 2. We follow the 'fibration approach' from the proof of Lemma 7 to reduce the problem to the special case $r = 1$: Suppose that $\mathbf{t} \in \mathbb{Z}^s$ is counted by $J_f(H)$. Then for this fixed $\mathbf{t}$, the specialised polynomial $f(X_1, \ldots, X_r)$ factorises over $\mathbb{Q}[X_1, \ldots, X_r]$. Now by assumption, f has the monomial of highest degree in X_i of the form $X_i^n h$, where h is not identically zero and depends at most on $T_1, \ldots, T_s$, but not on any X_j. As there are only $O_f(H^{s-1})$ many $\mathbf{t} \in \mathbb{Z}^s$ with $|\mathbf{t}| \leq H$ and $h(\mathbf{t}) = 0$, which is a negligible quantity with respect to Theorem 2, we may without loss of generality assume that $h(\mathbf{t}) \neq 0$. Hence the polynomial f factorises in the form $f = g_1 g_2$, where g_1 and g_2 are rational polynomials of degree less than n in X_i. This remains true for the resulting one-variable polynomial $f(X_i)$ after specialising all the X_j where $j \neq i$ to any rational numbers. Hence, using Hilbert's irreducibility theorem to choose integer specialisations for the variables x_j with $j \neq i$ such that $f(X_i)$ as a polynomial over $\mathbb{Q}(T_1, \ldots, T_s)$ keeps its Galois group G, we then find that any $\mathbf{t} \in \mathbb{Z}^s$ counted by $J_f(H)$ leads to a specialised $f(X_i)$ that becomes reducible. Using Corollary 2 we therefore find that $J_f(H) \ll_{f,\varepsilon} H^{s-1+\gamma_G+\varepsilon}$.

Acknowledgements. The authors would like to thank the anonymous referees for several useful comments. The first author also wants to thank the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago and his Ph.D. supervisor A. C. Cojocaru for funding and guidance, and both authors want to thank the NSF for funding the 2012 Number Theory Summer School at Göttingen.

References

[1] T. D. Browning and D. R. Heath-Brown, *Plane curves in boxes and equal sums of two powers*, Math. Z. 251 (2005), 233–247.

[2] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. 43 (1981), 227–250.

[3] P. Dèbes and Y. Walkowiak, *Bounds for Hilbert's irreducibility theorem*, Pure Appl. Math. Quart. 4 (2008), 1059–1083.

[4] R. Dietmann, *On the distribution of Galois groups*, Mathematika 58 (2012), 35–44.

[5] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer, New York, 1996.
[6] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory 6 (1974), 211–231.
[7] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coeffizienten*, J. Reine Angew. Math. 110 (1892), 104–129.
[8] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
[9] M. Marden, *Geometry of Polynomials*, 2nd ed., Math. Surveys 3, Amer. Math. Soc., 1966.
[10] P. Müller, *Hilbert's irreducibility theorem for prime degree and general polynomials*, Israel J. Math. 109 (1999), 319–337.
[11] I. Rivin, *Galois groups of generic polynomials*, arXiv:1511.06446 (2015).
[12] A. Schinzel and U. Zannier, *The least admissible value of the parameter in Hilbert's irreducibility theorem*, Acta Arith. 69 (1995), 293–302.
[13] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, New York, 1979.
[14] Y. Walkowiak, *Théorème d'irréductibilité de Hilbert effectif*, Acta Arith. 116 (2005), 343–362.
[15] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1011.6465 (2010).

Abel Castillo
Department of Mathematics, Statistics,
and Computer Science
University of Illinois at Chicago
851 S Morgan St
Chicago, IL 60607, U.S.A.
E-mail: acasti8@uic.edu

Rainer Dietmann
Department of Mathematics
Royal Holloway
University of London
TW20 0EX Egham, United Kingdom
E-mail: Rainer.Dietmann@rhul.ac.uk