Pure and Applied Mathematics Quarterly
Volume 4, Number 4
(*Special Issue: In honor of
Jean-Pierre Serre, Part 1 of 2*)
1059—1083, 2008

Bounds for Hilbert's Irreducibility Theorem

Pierre Dèbes and Yann Walkowiak

Abstract: In the context of Hilbert's irreducibility theorem, it is an open question whether there exists a bound for the least hilbertian specialization in $\mathbb{N}$ that is polynomial in the degree d and the logarithmic height $\log(H)$ of the polynomial $P(T,Y)$ in question. A positive answer would be useful, notably for algorithmic applications. We obtain a polynomial bound in $\log(H)$ and $d^{\mathrm{Hi(P)}}$ where Hi(P) — the Hilbert index of P — is a pure group-theoretical invariant we define and which we show to be absolutely bounded for many classes of polynomials. We also discuss further questions related to effectiveness in Hilbert's irreducibility theorem.

2000 MSC. Primary 12E25, 14G05 ; Secondary 11C08, 12E05

1. Introduction

Hilbert's irreducibility theorem is one of the few general powerful tools in Arithmetic Geometry, like Siegel's or Falting's theorems. Its simplest but most essential form asserts that, given an irreducible polynomial $P(T,Y) \in \mathbb{Q}[T,Y]$ with $\deg_Y(P) \geq 1$, a specialization t of the parameter T can be found in $\mathbb{Z}$ such that the specialized polynomial $P(t,Y)$ is still irreducible. The gist of it is that in appropriate situations, rational parameters can be specialized in $\mathbb{Q}$ without changing the algebraic structure. Among many applications, recall its use in the Inverse Galois Problem over $\mathbb{Q}$ ([Se1] section 10): if a finite group G can be realized over $\mathbb{Q}(T)$ then, by specialization, it can be realized over $\mathbb{Q}$ as well. See also [Se1] section 11 where it is explained how Néron [Ne] used it in a similar

Received June 9, 2006.

manner to prove in 1952 that there are elliptic curves of rank ≥ 9 over $\mathbb{Q}$, by first working over $\mathbb{Q}(T)$.

An important task in Arithmetic Geometry is to provide fully effective versions of fundamental theorems. For Hilbert's irreducibility theorem, such effective versions are available, although the first ones were not established before the 90' [De3] [ScZa]. The next and latest improvement appeared in [Wa2]: there is an upper bound for the smallest hilbertian specialization $t \in \mathbb{N}$ that is polynomial in $\deg_T(P)$ and $\log(H)$ (the logarithmic height of P) and exponential in $\deg_Y(P)$. Moreover, a fully polynomial bound can be given in the *Galois case*, that is for the class of polynomials $P(T,Y)$ such that the field generated over $\mathbb{Q}(T)$ by a root of P in $\overline{\mathbb{Q}(T)}$ is a Galois extension of $\mathbb{Q}(T)$. However these bounds are not as good as one can expect.

In this paper we make some further progress towards the main goal which is to find a polynomial bound in $\deg(P)$ and $\log(H)$ in the general case. One motivation comes from a long-standing open question: finding a deterministic algorithm for the factorization of bivariate polynomials in polynomial time. A polynomial bound for Hilbert's theorem would provide such an algorithm (see [Wa1] chapter 5). Building on Walkowiak's method (which we review in section 2) we obtain a polynomial bound in $\log(H)$, $\deg_T(P)$ and $\deg_Y(P)^{\mathrm{Hi}(P)}$ (theorem 3.3) where $\mathrm{Hi}(P)$ — the Hilbert index of P — is a pure group-theoretical invariant which we show to be absolutely bounded for many classes of polynomials, thus achieving the main goal in these cases (theorem 4.1). It is true for example if the Galois group G of $P(T,Y)$ over $\mathbb{Q}(T)$ is solvable and its action on the roots is primitive; it is also true if $\log|G|/\log\deg_Y(P)$ is bounded (in particular in the Galois case). And although it is not in general, we feel that the Hilbert index which encompasses the group-theoretical aspect of the problem is a key to the remaining task. We note however that computing $\mathrm{Hi}(P)$ or even deciding whether the preceding group-theoretical assumptions hold may be algorithmically difficult and so our results are not at this stage so much of a practical gain for the motivating question of factoring polynomials.

There are further questions related to the issue of bounds in Hilbert's theorem. We seize the opportunity to discuss some in the second part of the paper. For example it is plausible that there exists a bound depending only on the degree of the polynomial. We show that this follows from Lang's conjecture on rational points

on varieties and more particularly from its consequence established by Caporaso, Harris and Mazur about the number of rational points over a number field on a curve of genus ≥ 2 (proposition 5.2). This bound could even be polynomial in the degree. Using Siegel's theorem we obtain a result about good specializations in large consecutive integers (proposition 5.5) which is a weak form of this. Consideration of polynomials with more variables is worthwhile too. The problem reduces then to bounding the number of integral points on varieties of high dimension (and not just curves as in the preceding situation) and so, although we have some partial results to offer, it is more difficult in general. Other related comments, variants of the problem are collected in the final section.

Several chapters in Serre's books [Se1] and [Se2] are devoted to Hilbert's irreducibility theorem. The following topics (in addition to the already quoted ones) have been quite influential, to us in particular: the basic notion of *thin subsets* ("ensembles minces") ([Se1] section 9), the group-theoretical aspect ([Se1] section 9), very present in this paper, the connection with Noether's program through Colliot-Thélène's conjecture ([Se2] section 3). The question of bounds is also discussed, in [Se1] section 9 through a diophantine viewpoint and in [Se1] section 13 *via* sieve methods.

2. General approach

2.1. Main questions. Given a class of polynomials $P(T,Y) \in \mathbb{Q}[T,Y]$ irreducible and such that $\deg_Y(P) \geq 2$, we say that for this class there exists a polynomial bound in the degree and the height (resp. a bound depending only on the degree, or any other given type of bound) for the least integral hilbertian specialization if there exists a monomial $C(D,h)$ (resp. a function $C(D)$, or a function C of the given type) such that for each polynomial $P(T,Y)$ in the class, there exists an integer $t > 0$ such that $P(t,Y)$ is irreducible in $\mathbb{Q}[Y]$ and $t \leq C(\deg(P), \log(H(P))$ (resp. $t \leq C(\deg(P))$, or $t \leq C$).

At the moment the best known bound is polynomial in $2^{\deg(P)}$ and $\log(H(P))$ [Wa2].

2.2. Notation. From now on we fix an irreducible polynomial $P(T,Y)$ in $\mathbb{Q}[T,Y]$ with $\deg_Y(P) \geq 2$ and with coefficients in $\mathbb{Z}$ assumed to be relatively prime. We will use the following notation throughout the paper:

- $m = \deg_T(P)$, $n = \deg_Y(P)$ and $D = \deg(P)$
- $H = \max(H(P), e^e)$ where $H(P)$ is the height of P, *i.e.* the maximum of the absolute values of the coefficients of P. With our convention on the coefficients of P, the height $H(P)$ coincides with the Weil height of P.

2.3. Outline of the method. A standard preliminary argument reduces the problem to counting integral points on plane curves. Our version of the argument, which is a basic point of our approach and which we call the *preliminary reduction*, is given in section 3.1. Here is its conclusion. Let $N/\mathbb{Q}(T)$ be the Galois closure of $P(T,Y)$ and G be its Galois group. Denote the set of all proper maximal subgroups M of G by $\mathcal{M}_G$ and consider the corresponding minimal non-trivial sub-extensions $N^M/\mathbb{Q}(T)$ of the Galois closure $N/\mathbb{Q}(T)$. For each $M \in \mathcal{M}_G$ pick a primitive element of $N^M/\mathbb{Q}(T)$ integral over $\mathbb{Z}[T]$ and consider its irreducible polynomial $Q_M(T,Y) \in \mathbb{Z}[T,Y]$.

(1) *The preliminary reduction shows how to construct a set $\mathcal{M}_P \subset \mathcal{M}_G$ such that for all but finitely many $t \in \mathbb{Q}$, if $P(t,Y)$ is reducible in $\mathbb{Q}[Y]$, then $Q_M(t,Y)$ has a root in $\mathbb{Q}$, for some $M \in \mathcal{M}_P$.*

Furthermore, based on [Wa2], the primitive elements of $N^M/\mathbb{Q}(T)$ can be chosen in such a way that the polynomials $Q_M(T,Y)$ be of manageable size ($M \in \mathcal{M}_P$); more specifically [Wa2] section 4.2 provides the following estimates:

$$(2) \qquad \begin{cases} \deg_Y(Q_M) = n(M) = [G:M] \leq 2^n \\ \deg_T(Q_M) \leq m\, n(M)^2 \\ \deg(Q_M) \leq 2m\, n(M)^2 \\ H(Q_M) \leq 2^{3n(M)^3}(m+1)^{n(M)^2} H^{n(M)^2} \end{cases}$$

As to the finitely many exceptional t in (1) they are roots of the discriminant of P viewed as a polynomial in Y and so their number is $\leq 2nm$.

We can then develop two strategies.

2.4. Strategy one. The first one improves upon the one in [Wa2] and will be the main line of the paper. Consider the positive integers t less than or equal to some positive number B. Denote the number of those such that $P(t,Y)$ is reducible in $\mathbb{Q}[Y]$ by $S(P,B)$ and the number of those such that $Q_M(t,Y)$ has a root in $\mathbb{Z}$ by $N_T(Q_M,B)$ ($M \in \mathcal{M}_G$). From (1) we have

$$S(P,B) \leq \sum_{M \in \mathcal{M}_P} N_T(Q_M,B) \ + \ 2nm \tag{3}$$

Each number $N_T(Q_M,B)$ can be evaluated by using Heath-Brown results [H-B] on the density of rational points on projective curves. Adapting them to affine curves and making them fully effective, Walkowiak obtained the following estimate ([Wa2] section 2.4): given a polynomial $F(T,Y) \in \mathbb{Z}[T,Y]$ irreducible over $\mathbb{Q}$, we have

$$N_T(F,B) \leq C_1 \, B^{1/2} \log^5 B \tag{4}$$

where $C_1 = 2^{88} \deg(F)^{45} \log^{19}(H_F)$ (with $H_F = \max(H(F), e^e)$). One deduces

$$S(P,B) \leq C_2 \, B^{1/2} \log^5(B) \tag{5}$$

for a new constant C_2 given by

$$C_2 = 2^{165} m^{64} \log^{19}(H) \sum_{M \in \mathcal{M}_P} [G:M]^{147}$$

By choosing B large enough the right-hand side term in (5) can be made $< B$. Specifically take $B = [(1+C_2)^4]$ (which satisfies in particular $\log^5 B \leq B^{1/4}$) to conclude that there exists an integer t such that $P(t,Y)$ is irreducible and

$$0 \leq t \leq (1+C_2)^4 \tag{6}$$

In order to get a good bound C_2, the problem comes down to controlling the quantity $\sum_{M \in \mathcal{M}_P} [G:M]$. In section 3.2 we introduce a parameter – the Hilbert index – that encodes this problem. Bounding this Hilbert index becomes a pure

group-theoretical question. In section 4.2 we explain how we can reach our goal in some situations thanks to some results on finite groups.

2.5. Strategy two. Our second strategy rests on the observation that the contribution of $\mathcal{M}_P$ in the estimates can be big but depends only on the degree $\deg(P)$ and not on the height $H(P)$. The idea is to look for results of the same type for the diophantine part of the problem concerned with the solutions of the equations $Q_M(t,y) = 0$ ($M \in \mathcal{M}_P$). However improving estimate (4) in this direction is hopeless. On the other hand it looks more reasonable if instead of working with all integers t *a priori*, some extra condition is imposed on t and one tries to find some small t (in terms of the degree only) such that $Q_M(t,Y)$ has no root in $\mathbb{Q}$ ($M \in \mathcal{M}_P$) and satisfying this condition.

In section 5.1 for example, we give an argument based on Lang's conjectures which shows how to construct two integers a and $k > 0$ such that $P(t,Y)$ can be reducible only for finitely many integers t of the form $a + b^k$ ($b \in \mathbb{Z}$). Furthermore, a, k and the number of the exceptional integers depend only on $\deg(P)$, thus showing that a bound depending only on $\deg(P)$ for the least hilbertian specialisation for P is conjecturally expected.

In section 5.2, we work with suitably large consecutive integers. We show that there is at least one hilbertian specialization out of $2\deg(P)^8$ consecutive integers provided they are suitably large; the lower bound however is not effective as the argument uses Siegel's theorem.

3. Hilbert index

We first review the preliminary reduction to explain how the set $\mathcal{M}_P$ from section 2.3 can be best chosen. The Hilbert index is derived from this reduction.

3.1. The preliminary reduction. In addition to the notation from section 2, let $\mathcal{Y}_1(T), \dots, \mathcal{Y}_n(T)$ be the $n = \deg_Y(P)$ roots of $P(T,Y)$ in the Galois closure N of $P(T,Y)$ over $\mathbb{Q}(T)$. For all but finitely many $t \in \mathbb{Q}$, there is a specialization morphism $v_t : \mathbb{Q}[T, \mathcal{Y}_1, \dots, \mathcal{Y}_n] \to \overline{\mathbb{Q}}$ extending the specialization $T \to t$ and such that the corresponding values $\mathcal{Y}_1(t), \dots, \mathcal{Y}_n(t)$ are all distinct.

For such $t \in \mathbb{Q}$, a divisor $D(Y)$ of $P(t,Y)$ in $\mathbb{Q}[Y]$ is determined by the subset $J \subset \{1,\dots,n\}$ of indices j for which $D(\mathcal{Y}_j(t)) = 0$ (modulo a multiplicative constant). Consider then the corresponding polynomial $F_J(Y) = \prod_{j\in J}(Y - \mathcal{Y}_j(T)) \in N[Y]$ and denote the subfield of N generated over $\mathbb{Q}(T)$ by its coefficients by $\mathbb{Q}(T,\{\mathcal{Y}_J\})$ [1]. If $D(Y)$ is a non trivial divisor of $P(t,Y)$ (*i.e.* $0 < \deg(D) < n$), then $\mathbb{Q}(T,\{\mathcal{Y}_J\})$ is different from $\mathbb{Q}(T)$ (as $P(T,Y)$ is irreducible in $\mathbb{Q}(T)[Y]$) but becomes equal to $\mathbb{Q}$ *via* the specialization v_t. And so does every minimal non trivial sub-extension N^M of N contained in $\mathbb{Q}(T,\{\mathcal{Y}_J\})$.

Conclusion 3.1 — *For all but finitely many $t \in \mathbb{Q}$, if it can be guaranteed that, for all possible subsets $J \subset \{1,\dots,n\}$ with $0 < \mathrm{card}(J) < n$, there is at least one minimal non trivial sub-extension $N^M \subset N$ contained in $\mathbb{Q}(T,\{\mathcal{Y}_J\})$ such that $Q_M(t,Y)$ has no root in $\mathbb{Q}$, then the polynomial $P(t,Y)$ is irreducible in $\mathbb{Q}[Y]$.*

Also observe, first, that as $\mathbb{Q}(T,\{\mathcal{Y}_J\}) = \mathbb{Q}(T,\{\mathcal{Y}_{J^c}\})$ (with J^c the complement of J in $\{1,\dots,n\}$), condition above only needs to be checked for all $J \subset \{1,\dots,n\}$ with $0 < \mathrm{card}(J) \le [n/2]$, and second, that the containment $N^M \subset \mathbb{Q}(T,\{\mathcal{Y}_J\})$ only needs to be satisfied up to conjugation by some $\gamma \in G$ (indeed the same polynomial $Q_M(T,Y)$ can be attached to two conjugate extensions $N^M/\mathbb{Q}(T)$). Finally note that the Galois group of the extension $N/\mathbb{Q}(T,\{\mathcal{Y}_J\})$ is the subgroup

$$G_J = \{g \in G \mid g(J) = J\}$$

of G viewed as a subgroup of S_n *via* its action on $\mathcal{Y}_1(T),\dots,\mathcal{Y}_n(T)$.

Conclusion 3.1 (continued) — *The set $\mathcal{M}_P$ from display* (1) *of section 2.3 can be taken to be any subset of $\mathcal{M}_G$ with the following property:*

(7) *for all $J \subset \{1,\dots,n\}$ with $0 < \mathrm{card}(J) \le [n/2]$, there exists $M \in \mathcal{M}_P$ such that for some $\gamma \in G$, the maximal subgroup M^γ contains the subgroup G_J.*

The subset $\mathcal{M}_P$ is then said to cover all possible non trivial factorizations of $P(T,Y)$.

[1] The notation $\{\mathcal{Y}_J\}$ is meant to suggest the unordered set of roots $\mathcal{Y}_j$ with $j\in J$ whose field of definition is precisely the field generated by the coefficients of $F_J(Y)$. We would use the notation $\mathbb{Q}(T,\mathcal{Y}_j\,|\,j\in J)$ for the field generated by all individuals $\mathcal{Y}_j$ with $j\in J$.

Remark 3.2. The whole set $\mathcal{M}_G$ obviously satisfies this property, and actually satisfies more. Namely, for all but finitely many $t \in \mathbb{Q}$, the following conditions are equivalent:

(i) $Q_M(t,Y)$ has no root in $\mathbb{Q}$ for all $M \in \mathcal{M}_G$,

(ii) $\widehat{P}(t,Y)$ irreducible in $\mathbb{Q}[Y]$,

where $\widehat{P}(T,Y)$ denotes the irreducible polynomial of some primitive element over $\mathbb{Q}(T)$ of the Galois closure N of $P(T,Y)$; implication (i) $\Rightarrow$ (ii) follows from the preliminary reduction applied to $\widehat{P}(T,Y)$ and the converse is clear.

Condition (ii) is strictly stronger than condition "(iii) $P(t,Y)$ irreducible", which is what we want: take for example $P(T,Y) = Y^4 - 2Y^2 - T + 1$; the Galois closure of P contains the four roots $\pm\sqrt{1 \pm \sqrt{T}}$ and so also $\sqrt{1-T^2}$; for $t = 3/5$, $P(t,Y)$ is irrreducible, but as $\sqrt{1-t^2} \in \mathbb{Q}$, condition (i) above does not hold. The converse (iii) $\Rightarrow$ (ii) however does hold if the function field $\mathbb{Q}(T, \mathcal{Y}_1(T))$ contains the compositum of all minimal sub-extensions of N, that is if the subgroup $\Gamma_P \subset G$ fixing one given root $\mathcal{Y}(T)$ of P is contained in the Frattini subgroup $\Phi(G)$ of G [2].

3.2. The Hilbert index. A better choice can be made for the set $\mathcal{M}_P$ than the whole set $\mathcal{M}_G$ which is too big for the estimates we have in view[3]. Observe that the condition on $\mathcal{M}_P$ that it covers all possible non trivial factorizations of P, *i.e.* condition (7) above, is a pure group-theoretical condition on the group G embedded in S_n *via* its action on the roots of P. Given a transitive subgroup $G \subset S_n$, we will denote by $\Sigma(G,n)$ the minimum of the quantities $\sum_{M \in \mathcal{M}}[G:M]$ (which are those to optimize for our strategy to work best) where $\mathcal{M}$ ranges over the subsets of $\mathcal{M}_G$ satisfying condition (7). The *Hilbert index* of $G \subset S_n$ is then defined by

$$\mathrm{Hi}(G,n) = \frac{\log(\Sigma(G,n))}{\log(n)}$$

[2] The subgroup Γ_P is defined up to conjugation in G but the condition itself is well-defined as $\Phi(G)$ is a normal subgroup of G.

[3] Even when conditions (ii) and (iii) from remark 3.2 are equivalent and all minimal non-trivial sub-extensions of N do contribute to the reducibility set of $P(T,Y)$, these contributions have overlaps and a subset of them suffices to cover all possible non trivial factorizations.

We will use the following practical variants. For each subset $J \subset \{1, \dots, n\}$ with $0 < \mathrm{card}(J) \leq [n/2]$, consider all maximal subgroups containing the subgroup G_J (defined in section 3.1) of maximal order. Let J vary and denote the resulting subset of $\mathcal{M}_G$ by $\mathcal{M}(G,n)^\flat$ and a set of representatives of their conjugacy classes by $\mathcal{M}(G,n)^\sharp$. The *flat* and *sharp* variants of the Hilbert index are defined from $\Sigma(G,n)^\flat = \sum_{M \in \mathcal{M}(G,n)^\flat} [G:M]$ and $\Sigma(G,n)^\sharp = \sum_{M \in \mathcal{M}(G,n)^\sharp} [G:M]$ by

$$\mathrm{Hi}(G,n)^\flat = \frac{\log(\Sigma(G,n)^\flat)}{\log(n)} \qquad \text{and} \qquad \mathrm{Hi}(G,n)^\sharp = \frac{\log(\Sigma(G,n)^\sharp)}{\log(n)}$$

Clearly we have $\mathrm{Hi}(G,n) \leq \mathrm{Hi}(G,n)^\sharp \leq \mathrm{Hi}(G,n)^\flat$.

For some specific groups there may be better choices for $\mathcal{M}$ than the set $\mathcal{M}(G,n)^\sharp$ to approach $\mathrm{Hi}(G,n)$. For example it may happen that a maximal subgroup M in $\mathcal{M}(G,n)^\sharp$ contains several groups G_J (up to conjugacy) in which case this only group M can be kept to cover all factorizations associated to these G_J. However handling these possibilities in order to find the best possible choice for $\mathcal{M}$ seems to be an intricate problem in general.

The *Hilbert index* $\mathrm{Hi}(P)$ of some irreducible polynomial $P(T,Y) \in \mathbb{Q}[T,Y]$ with $n = \deg_Y(P) \geq 2$ is defined to be the Hilbert index of its Galois group embedded in S_n *via* its action on the $n = \deg_Y(P)$ roots of P in $\overline{\mathbb{Q}(T)}$ (and similarly for its flat and sharp variants $\mathrm{Hi}(P)^\flat$ and $\mathrm{Hi}(P)^\sharp$).

3.3. General conclusion. With these definitions, strategy one from section 2.4 leads to the following result. Recall $P(T,Y)$ is an irreducible polynomial in $\mathbb{Q}[T,Y]$ with $\deg_Y(P) \geq 2$ and with coefficients in $\mathbb{Z}$ assumed to be relatively prime.

Theorem 3.3 — *Let $S(P,B)$ be the number of positive integers t less than or equal to some number $B \geq 2$ and such that $P(t,Y)$ is reducible in $\mathbb{Q}[Y]$. Then we have*

$$S(P,B) \leq 2^{165}\, m^{64}\, n^{147\mathrm{Hi}(P)}\, \log^{19}(H)\, B^{1/2}\, \log^5(B)$$

Consequently there exists a polynomial bound for the least integral hilbertian specialization for each class of irreducible polynomials $F(T,Y) \in \mathbb{Q}[T,Y]$ with $\deg_Y(F) \geq 2$ and with Hilbert index bounded by an absolute constant $A > 0$.

Proof. This readily follows from inequality (5) by choosing $\mathcal{M}_P$ so that $\sum_{M\in\mathcal{M}_P}[G : M] = \Sigma(G,n)$ and noting that $\Sigma(G,n) = n^{\mathrm{Hi}(P)}$. $\square$

The bounds from [Wa2] are recovered as follows. Form a subset $\mathcal{M} \subset \mathcal{M}_G$ consisting, for each $J \subset \{1,\dots,n\}$ with $0 < \mathrm{card}(J) \le [n/2]$, of exactly one proper maximal subgroup M_J of G containing G_J; in particular $[G : M_J] \le [G : G_J] \le 2^n$. By construction $\mathcal{M}$ automatically covers all possible non trivial factorisations of P. Therefore we have the following rough estimate which yields the desired polynomial bounds in 2^n, $\log(H)$ and B for $S(P,B)$:

$$n^{\mathrm{Hi}(P)} = \Sigma(G,n) \le \mathrm{card}(\mathcal{M}) \max_{M\in\mathcal{M}}[G : M] \le 2^n \cdot 2^n = 2^{2n}$$

Bounding $\mathrm{Hi}(P)$ by an absolute constant would be the ultimate goal. As the following remark shows, this is not always possible but in section 4.2 we will give new large classes of polynomials for which it is and so for which there exists a polynomial bound for the least integral hilbertian specialization.

Remark 3.4. For $G = S_n$ embedded in itself, the subgroups G_J with $0 < \mathrm{card}(J) < [n/2]$ are maximal (they are of the form $S_k \times S_{n-k}$ where $\mathrm{card}(J) = k$) and two such subgroups with different values of $\mathrm{card}(J)$ are non-conjugate. So $\Sigma(G,n) \ge 2^{n-1} - 1$ is exponential in this case and $\mathrm{Hi}(G,n) \gg n/\log(n)$. The desirable estimate $\mathrm{Hi}(G,n) \le A$ is false in general.

4. Group-theoretical bounds

As before, $P(T,Y)$ is an irreducible polynomial in $\mathbb{Q}[T,Y]$ with $n = \deg_Y(P) \ge 2$ and its Galois group embedded in S_n *via* its action on the $n = \deg_Y(P)$ roots of P in $\overline{\mathbb{Q}(T)}$ is denoted by $G \subset S_n$.

4.1. Three invariants of finite groups. Let $\nu(G)^\flat$ be the number of proper maximal subgroups of G, $\nu(G)^\sharp$ be the number of their conjugacy classes and n_G^+ be the maximal index of a proper maximal subgroup of G. We have

$$\Sigma(G,n)^\flat \le \nu(G)^\flat\, n_G^+ \quad \text{and} \quad \Sigma(G,n)^\sharp \le \nu(G)^\sharp\, n_G^+$$

Thus condition $\mathrm{Hi}(G,n)^\flat \le A$ (resp. $\mathrm{Hi}(G,n)^\sharp \le A$) holds under condition (8-i) below (resp. under condition (8-ii) below): for some absolute constant $a > 0$,

$$(8) \qquad \text{(i) } \max(\nu(G)^\flat, n_G^+) \le n^a \qquad\qquad \text{(ii) } \max(\nu(G)^\sharp, n_G^+) \le n^a$$

As for $M \in \mathcal{M}(G,n)^\flat$ we have $[G:M] \le 2^n$ (since M contains some group G_J), the numbers $\nu(G)^\flat$, $\nu(G)^\sharp$ and n_G^+ can be replaced by the analogous numbers where only the proper maximal subgroups of G of index $\le 2^n$ are taken into account, which can be advantageous in some circumstances.

The following is known about these invariants. According to a theorem of Pyber (see [LuSe] theorem 11.3.4), $\nu(G)^\flat \le |G|^\kappa$ for some absolute constant $\kappa \ge 1$. We have *a fortiori* $\nu(G)^\sharp \le |G|^\kappa$. It is conjectured that $\nu(G)^\flat \le |G|$ [Wal] and that $\nu(G)^\sharp$ is at most the number of conjugacy classes of G [AsGu1]; and both are proved for solvable groups (in the same respective papers) and asymptotically for simple groups [LiSh2] [AsGu1].

Using Pyber's theorem and the inequality $n \ge \sqrt{\log|G|}$ (which follows from $|G| \le n!$), we obtain the following upper bounds for the Hilbert index $\mathrm{Hi}(G,n)$:

$$\mathrm{Hi}(G,n)^\flat \le (\kappa+1)\frac{\log|G|}{\log(n)} \le (2\kappa+2)\frac{\log|G|}{\log\log|G|}$$

4.2. Main result. We give below some group-theoretical situations where we have better. Our list is not exhaustive.

Theorem 4.1 — *The Hilbert index* $\mathrm{Hi}(G,n)$ *is absolutely bounded in each of the following situations, where* α *and* β *denote some positive absolute constants:*

(a) $|G| \leq n^{\alpha}$ *(e.g. in the Galois case).*

(b) $G \subset S_n$ *is a primitive action and one of the following conditions holds:*

1. G *is solvable,*

2. G *does not not involve* A_d *as a section for some fixed integer* $d > 0$*,*

3. G *is almost simple and* $G \subset S_n$ *is a non-standard primitive action in the sense of* [LiSh1].

(c) $G \subset S_n$ *is a primitive action of maximal degree and* $\nu(G)^{\sharp} \leq (\log |G|)^{\alpha}$*. The latter condition holds for example if* $G = S_d$*.*

(d) G *is a* p*-group of order* p^r *such that* $\nu(G)^{\sharp} \leq (rp)^{\beta}$*.*

Consequently in each of these situations there exists a polynomial bound for the least hilbertian specialization for the class of irreducible polynomials in $\mathbb{Q}[T,Y]$ *with* n *roots in* $\overline{\mathbb{Q}(T)}$ *and with an action of the Galois group on the* n *roots given by a permutation group* $G \subset S_n$ *satisfying the assumptions of the situation in question.*

Proof. From Pyber's theorem and the inequality $n \geq \sqrt{\log |G|}$, condition (8-i) and (8-ii) hold under the following respective conditions, where $\alpha > 0$ is an absolute constant:

$$(9) \qquad \text{(i) } |G| \leq n^{\alpha}, \qquad \text{(ii) } n \geq (n_G^+)^{1/\alpha} \text{ and } \nu(G)^{\sharp} \leq (\log |G|)^{\alpha}$$

Condition (9-i) holds in situations (a) and (b). It is obvious for (a). For (b) it follows from the literature on finite groups (see [LiSh1] for a survey of this type of results). Namely for primitive groups, the following bounds are known. If G is solvable then $|G| < 24^{-1/3} n^{3.244}$ [Pá] [Wo] whence (b-1). Under the assumption of (b-2), $|G| < n^{f(d)}$ with $f(d)$ depending only on d [BaCaPá]. Finally under the assumption of (b-3), $|G| < n^9$ [Li].

A primitive action $G \subset S_n$ of maximal degree is equivalent to the action by left translation on left cosets modulo a maximal subgroup of maximal index. Therefore $n = n_G^+$ and condition (9-ii) holds in situation (c). From corollary 5.3

of [LiMaSh] we have $\nu(S_d)^\sharp = [d/2] + d^{o(1)}$ and so $\nu(G)^\sharp \leq (\log |G|)^\beta$ holds in this case.

Finally let $G \subset S_n$ be a transitive p-group of order p^r. Maximal proper subgroups of G are of index p in G. Using the assumption on $\nu(G)^\sharp$ we obtain $\Sigma(G,n)^\sharp \leq p(rp)^\beta$. Furthermore p^r divides $n!$. Using that the p-adic valuation of $n!$ is $\leq n/(p-1)$ (*e.g.* [Am] Lemme 3.5.6), we obtain $n \geq (p-1)r$ [4]. For $p > 2$, this gives $n^{2\beta+2} \geq p^{\beta+1} r^{2\beta+2} \geq \Sigma(G,n)^\sharp$. For $p = 2$, we get $n^{2\beta+2} \geq r^{2\beta+2} \geq \Sigma(G,n)^\sharp$ if $r \geq 2$, while for $r = 1$, we obviously have $\Sigma(G,n)^\sharp = p$. In all cases, the Hilbert index of G is $\leq 2\beta + 2$, which proves (d). □

Remark 4.2. The number of maximal subgroups of a p-group G is determined by the abelianization G^{ab}. However G^{ab} can be big with many maximal subgroups and with G embedded in S_n with a small n. Indeed, from [KoNe] there exist transitive 2-groups $G \subset S_n$ which cannot be generated by fewer than $n/\sqrt{\log n}$ elements and so have at least $2^{n/\sqrt{\log(n)}}$ non conjugate maximal subgroups. For these groups, we have $\nu(G)^\sharp \geq 2^{n/\sqrt{\log(n)}}$ and in particular the assumption of (d) does not hold. A similar example with $\nu(G)^\sharp \sim 2^{n/(2\log_2(n))}$ is given in [AsGu2].

5. Strategy two

We follow here the second strategy explained in section 2.5.

5.1. Removing the dependence in the height. We keep the notation from section 2. Our motivation is to investigate whether a bound depending only in the degree can be found for the least integral hilbertian specialization. A partial answer to this question was given by Yasumoto: according to [Ya] this is true if one restricts to the class of all irreducible polynomials $P(x,T,Y)$ obtained by specializing X in $\mathbb{Q}$ in a polynomial $P(X,T,Y) \in \mathbb{Q}[X,T,Y]$. The proof uses non-standard methods. The general case seems difficult though plausible. As we will now see it is a consequence of Lang's conjecture on rational points on varieties.

[4] The example below in remark 4.2 shows one cannot expect much better in general.

Lang conjectured that if V is a variety of general type defined over a number field K then the set $V(K)$ of K-rational points is not Zariski-dense in V. Caporaso, Harris and Mazur [CHarM] showed Lang's conjecture implies the following statement (see also [Pa]):

Conjecture 5.1 (CHarM) — *For every number field K and every integer $g > 1$ there exists a finite integer $B(g, K)$ such that* $\mathrm{card}(C(K)) < B(g, K)$ *for every curve of genus g defined over K.*

Proposition 5.2 — *Assume the CHarM conjecture holds. Then there exists a bound depending only on the degree for the least integral hilbertian specialization for polynomials in two variables and with coefficients in $\mathbb{Q}$.*

Proof. The first author discussed the following argument with U. Zannier. The strategy is to assure *via* some change of variable that the curves $Q_i(t, y) = 0$ associated to the polynomial $P(T, Y)$ in the preliminary reduction are of genus ≥ 2 and so have only finitely many rational points. Then, using the conjecture, one can bound in terms of $\deg(P)$ the total number of rational points on these curves, and so the number of $t \in \mathbb{Q}$ such that $P(t, Y)$ is reducible in $\mathbb{Q}[Y]$.

Let then $\{Q_1(T, Y), \ldots, Q_N(T, Y)\} \subset \mathbb{Q}[T, Y]$ be a set of irreducible polynomials as given by the preliminary reduction: for each $t \in \mathbb{Q}$ but in a finite set F, if $Q_1(t, Y), \ldots, Q_N(t, Y)$ have no root in $\mathbb{Q}$, then $P(t, Y)$ is irreducible. From previous sections, the number N can be bounded by 2^n, the degrees of the polynomials $Q_1, \ldots, Q_N$ by $d = m2^{2n+1}$ and the cardinality of the finite set F by $2nm$. Furthermore, up to enlarging the finite set F, one may assume that $Q_1, \ldots, Q_N$ in $\mathbb{Q}[T, Y]$ are absolutely irreducible: indeed for a polynomial Q_i that is irreducible in $\mathbb{Q}[T, Y]$ but not absolutely irreducible, if for some $t \in \mathbb{Q}$ we have $Q_i(t, y) = 0$ for some $y \in \mathbb{Q}$, then $(\partial Q_i/\partial Y)(t, y) = 0$, and so the number of such t is less than or equal to the degree of the discriminant of Q_i vith respect to Y.

For $i = 1, \ldots, N$, denote a smooth projective model of the affine curve $Q_i(t, y) = 0$ by C_i. Branch points $t \in \mathbb{Q}$ of the T-projection map $C_i \to \mathbb{P}^1$ induced by $(t, y) \to t$ are among roots of the discriminant $\Delta_i(T)$ of Q_i with respect to T. Thus if $\delta = \sum_{1 \leq i \leq N} \deg(\Delta_i(T))$, then there exists $a \in \{0, 1, \ldots, \delta\}$ that is not a branch point of any of these T-projections. Fix such an a. Each polynomial $Q_i(a + T, Y)$ is absolutely irreducible and has a root in $\overline{\mathbb{Q}}((T))$, $i = 1, \ldots, N$.

From [De2], for every integer $k \geq 1$, $Q_i(a + T^k, Y)$ is absolutely irreducible, $i = 1, \ldots, N$.

For each index $i \in \{1, \ldots, N\}$ and each integer $k \geq 1$, denote the smooth projective model of the affine curve $Q_i(a+t^k, y) = 0$ by $C_{i,k}$ and its genus by $g_{i,k}$. For every $t \in \overline{\mathbb{Q}}$, $t \neq 0$, t is a branch point of the T-projection map $C_{i,1} \to \mathbb{P}^1$ if and only if every kth root of t is a branch point of the T-projection map $C_{i,k} \to \mathbb{P}^1$, $i = 1, \ldots, N$; furthermore the ramification indices are the same. So each branch point $t \neq \infty$ [5] of $T : C_{i,1} \to \mathbb{P}^1$ gives rise to k branch points $\mathcal{P}$ of $T : C_{i,k} \to \mathbb{P}^1$ with the same ramification indices $e_{\mathcal{P}}$. The Riemann-Hurwitz formula yields

$$\begin{aligned} 2g_{i,k} - 2 &= -2 \deg_Y Q_i + \textstyle\sum_{t \in \mathbb{P}^1(\overline{\mathbb{Q}})} \sum_{\mathcal{P}/t} (e_{\mathcal{P}} - 1) \\ &\geq -2 \deg_Y Q_i + k \end{aligned}$$

Set $d = \max_{1 \leq i \leq N}(\deg_Y Q_i)$ and $k = 2 + 2d$. For $i = 1, \ldots, N$, we obtain $g_{i,k} \geq 2$ and it follows from $2g_{i,k} - 2 \leq 2k\delta d$ that for $g_\infty = k\delta d + 1$, we have $g_{i,k} \leq g_\infty$. Denote the maximum of the bounds $B(g, \mathbb{Q})$ given by the CHarM conjecture for $2 \leq g \leq g_\infty$ by $\mathcal{N}(g_\infty)$. Then if $S \subset \mathbb{Q}$ is any subset such that $|S| > N\mathcal{N}(g_\infty) + \mathrm{card}(F)$, there exists $t \in S$ such that $Q_i(a + t^k, Y)$ has no root in $\mathbb{Q}$, $i = 1, \ldots, N$, and so $P(a + t^k, Y)$ is irreducible in $\mathbb{Q}[Y]$. □

Remark 5.3. Suppose given a polynomial $Q(T, Y) \in \mathbb{Q}[T, Y]$, which as the polynomials $Q_1(T + a, Y), \ldots, Q_N(T + a, Y)$ from the proof above, is absolutely irreducible and has a root in $\overline{\mathbb{Q}}((T))$. For each $k \geq 1$, denote a smooth projective model of the affine curve $Q(t^k, y) = 0$ by C_k. Assume further that the genus of $\mathcal{C}_1$ is at least 2 (or replace $Q(T, Y)$ by $Q(T^{k_0}, Y)$ for some suitably large integer k_0 to reduce to this case as explained in the proof above). For integers $k, h \geq 1$, the correspondences $(t, y) \to (t^h, y)$ induce maps $\varphi_{hk,k} : C_{hk} \to C_k$, making the infinite collection $(C_k)_{k \geq 1}$ a projective system of curves. It follows from Faltings' theorem (resp. Siegel's theorem) that

(10) *for k suitably large, say $k \geq k_F$ (resp. $k \geq k_S$), there are no rational points $M \in C_k(\mathbb{Q})$ (resp. no rational points $M \in C_k(\mathbb{Q})$ with $T(M) \in \mathbb{Z}$) unless $T(M) \in \{0, 1, \infty\}$.*

[5] 0 need not be excluded since by construction it is not a branch point.

An alternative to using the CHarM conjecture to get a bound depending only in the degree in Hilbert's theorem would be to prove an effective version of this profinite version of Faltings' theorem (resp. Siegel's theorem) with k_F (resp. k_S) depending only of $\deg(Q)$.

5.2. Good specializations in large consecutive integers. Going even further than proposition 5.2, one can ask whether the bound for the least hilbertian specialization could be *polynomial* in $\deg(P)$. More specifically: do there exist absolute constants μ and ν such that for any polynomial $P(T,Y) \in \mathbb{Q}[T,Y]$ irreducible and with $\deg_Y(P) \geq 1$, it is always possible to find a hilbertian specialization among any $\mu \deg(P)^\nu$ consecutive integers? We do not have any counter-example and in fact we do not have any essentially better example than the following one of some irreducible polynomial $P(T,Y) \in \mathbb{Q}[T,Y]$ with many small "bad" specialisations. Producing such polynomials seems difficult just as it is difficult to produce curves with many rational points.

Example 5.4. Given an integer $d \geq 1$, pick a polynomial $p(Y) \in \mathbb{Z}[Y]$ and an integer a such that both polynomials $p(y)$ and $p(y) - ad!$ are reducible in $\mathbb{Q}[Y]$. Set then $P(T,Y) = p(y) - at(t-1)...(t-d+1)$. The polynomial $P(t,Y)$ is reducible for $t = 0, 1, \ldots, d$.

Next we note that while the preceding question seems quite hard, it can be answered positively if "among any $\mu \deg(P)^\nu$ consecutive integers" is replaced by "among any *suitably large* $\mu \deg(P)^\nu$ consecutive integers".

Proposition 5.5 — *Let $P(T,Y) \in \mathbb{Q}[T,Y]$ irreducible with $\deg_Y(P) \geq 1$. Then for all suitably large integers m, at least one of the polynomials $P(m+k,Y)$, $k = 1, \ldots, 2\deg(P)^8$ is irreducible in $\mathbb{Q}[Y]$.*

The proof however uses Siegel's theorem and does not provide an effective lower bound for the good integers m. Similar effective results are proved in [De3;corollary 2.5] but under the assumption that $P(T,Y)$ is absolutely irreducible and unramified above ∞.

Proof. Let $\{Q_1(T,Y),\dots,Q_N(T,Y)\} \subset \mathbb{Q}[T,Y]$ be a set of irreducible and monic (in Y) polynomials as given by the preliminary reduction (section 3.1); as recalled in the proof of proposition 5.2 one may further assume they are absolutely irreducible. Fix an integer D which will be chosen later. Let $\Delta(T) \in \mathbb{Q}[T]$ be the discriminant of $P(T,Y)$ with respect to Y and $a > 0$ be an integer not in the finite set $\{|t-t'|/i \mid \Delta(t) = \Delta(t') = 0 \text{ and } i = 1,\dots,D-1\}$. As $\deg(\Delta) \le 2\deg(P)^2$, such an integer a can be found with $a \le 2D\deg(P)^4$. We will show the following holds for $D = \deg_Y(P)^2$, which is more precise than the announced result:

(11) for all suitably large integers m, for at least one integer $i = 0,\dots,D-1$, none of the polynomials $Q_j(m+ia,Y)$ has a root in $\mathbb{Q}$, $j = 1,\dots,N$; consequently $P(m+ia,Y)$ is irreducible in $\mathbb{Q}[Y]$.

If (11) does not hold, there exists a D-tuple $\mathbf{j} = (j_0,\dots,j_{D-1})$ such that for infinitely many integers m, each of the polynomials $Q_{j_i}(m+ia,Y)$ has a root in $\mathbb{Q}$, $i = 0,\dots,D-1$. Fix an algebraic closure of $\mathbb{Q}(T)$ and fix inside it, for $i = 0,\dots,D-1$, some representative E_i of the function field isomorphism class of the affine curve $Q_{j_i}(t+ia,y) = 0$ over $\overline{\mathbb{Q}}$. Let $E_{\mathbf{j}}$ be the compositum of all these functions fields and denote by $C_{\mathbf{j}}$ a smooth projective model of the field $E_{\mathbf{j}}$; it is defined over some number field K. From above, if (11) does not hold, then (for some choice of the representatives $E_i \subset \overline{\mathbb{Q}(T)}$) there are infinitely many points $M \in C_{\mathbf{j}}(K)$ such that $T(M) \in \mathbb{Z}$. We show below that the function T on $C_{\mathbf{j}}$ has at least 3 distinct poles, which contradicts Siegel's theorem.

For each $i = 0,\dots,D-1$, E_i is contained in the Galois closure N_i over $\overline{\mathbb{Q}}(T)$ of the polynomial $P(T+ia,Y)$ (from the construction of the polynomials $Q_1,\dots,Q_N$). From the choice of a, it follows that the branch point sets of any two extensions $E_i/\overline{\mathbb{Q}}(T)$ and $E_{i'}/\overline{\mathbb{Q}}(T)$ $(i \ne i')$ can have no finite common point. Therefore the extensions $E_i/\overline{\mathbb{Q}}(T)$ are pairwise linearly disjoint and $[E_{\mathbf{j}} : \overline{\mathbb{Q}}(T)] \ge 2^D$. Observe next, again as a consequence of $E_i \subset N_i$, that the compositum of all the fields of definition of the poles of the function T on (a smooth projective model of) the curve $Q_{j_i}(t+ia,y) = 0$ is contained in the compositum $E_{i,\infty}$ of all the fields of definition of the poles of the function T on the curve $P(t+ia,y) = 0$. Now all the fields $E_{i,\infty}$ $(i = 0,\dots,D-1)$ are actually the same field, say E_∞ (as the isomorphism $t \to t+ia$ fixes ∞) and so we have $[E_\infty : \mathbb{Q}] \le \deg_Y(P)!$. The result follows as for $D = \deg_Y(P)^2$, we have $2^D > 2\deg_Y(P)!$ $\square$

The proof extends to the more general situation where n polynomials $P_1(T, Y), \dots, P_n(T, Y)$ are given instead of the single polynomial $P(T, Y)$ and the ground field is a number field (instead of $\mathbb{Q}$).

6. Further perspectives

6.1. Extension to several variables. We consider here polynomials $P(T_1, \dots, T_r, Y)$ with r parameters and one variable and are interested in "small" specialisations $(t_1, \dots, t_r)$ preserving irreducibility. There are classical reductions to the preceding case of one parameter but they are not economic in terms of constants. We discuss here a direct approach based on the strategy used in [Wa2] and on results of Heath-Brown [H-B] in the higher dimensional situation.

6.1.1. General approach. The preliminary reduction (section 3.1) readily extends to the several variable situation to provide the following estimate

$$S(P, B) \leq \sum_{M \in \mathcal{M}_P} N_T(Q_M, B)$$

where $\mathcal{M}_P$ is some suitable subset of $\mathcal{M}_G$ and for each $B \geq 2$, $S(P, B)$ is the number of r-tuples $\mathbf{t} = (t_1, \dots, t_r)$ of positive integers $\leq B$ such that $P(\mathbf{t}, Y)$ is reducible in $\mathbb{Q}[Y]$ and $\mathrm{Disc}_Y(P)(\mathbf{t}) \neq 0$ (with $\mathrm{Disc}_Y(P)$ the discriminant of P with respect to Y) and $N_T(Q_M, B)$ is the number of those such that $Q_M(\mathbf{t}, Y)$ has a root $y_{\mathbf{t}}$ in $\mathbb{Z}$ (with the polynomials Q_M defined similarly as in section 2.3). Bounding the root $y_{\mathbf{t}}$ using Liouville's inequality reduces then the problem to estimate the number of integral points with coordinates $\leq (1 + m)^r H(Q_M) B^m$ (with $m = \deg_{T_1, \dots, T_r}(P)$) on the hypersurfaces $Q_M(t_1, \dots, t_r, y) = 0$.

Denote the number of integral points on the hypersurface $F(x_1, \dots, x_s) = 0$ with coordinates $\leq B$ by $N(F, B)$. It is more difficult to efficiently control the quantities $N(F, B)$ for high dimensional hypersurfaces than it is for curves (as in [Wa2]). For curves the estimate we had for $N(F, B)$ was in $B^{1/d}$ (with $d = \deg(F)$). For surfaces for example, the problem is that, because surfaces may contain lines, one may have $N(F, B) \gg B$: take for example $F(x_1, x_2, x_3) = x_1^d - x_2^d + x_3^d - 1$ for which we have $F(a, a, 1) = 0$ for all $a \in [0, B] \cap \mathbb{Z}$. When this happens, the derived upper bound for $S(P, B)$ may be of order B^m, and so there is no hope to obtain $S(P, B) < B^2$ unless $m = 1$, which is a strong condition.

This strategy however, conjoined with an effective version of theorem 9 of [H-B] (which can be obtained in the same way as theorem 3 of [H-B] is treated in [Wa2]) does lead to some explicit bound for a hilbertian specialization for polynomials $P(T_1, T_2, Y)$ with $\deg_{T_1,T_2}(P) = 1$.

6.1.2. Towards some improvements. Heath-Brown's paper also provides sharper estimates in the case of surfaces for the number of integral points not lying on a line contained in the surface in question. We can then improve the estimates of $N_T(Q_M, B)$ under the assumption that the surfaces $Q_M(t_1, t_2, y) = 0$ contain only finitely many lines, that is are non ruled surfaces.

Namely consider in general a polynomial $F(T_1, T_2, Y) \in \mathbb{Z}[T_1, T_2, Y]$ irreducible, monic in Y and defining a non ruled surface. Using Liouville's inequality, for every point $(t_1, t_2) \in \mathbb{Z}^2$ such that $\max(|t_1|, |t_2|) \leq B$, the integral roots y of $F(t_1, t_2, Y) = 0$ can be bounded by $(1 + m)^2 H(F) B^m$. Then the evaluation of $N_T(F, B)$ can be done in two steps: first count the number, which we denote by $N_1(F, (1 + m)^2 H(F) B^m)$, of points $(t_1, t_2, y) \in \mathbb{Z}^3$ with coordinates $\leq (1 + m)^2 H(F) B^m$, such that $F(t_1, t_2, y) = 0$ but are not lying on a line in the surface; second, count the points $(t_1, t_2) \in \mathbb{Z}^2$ with $\max(|t_1|, |t_2|) \leq B$ such that there is a point $(t_1, t_2, y) \in \mathbb{Z}^3$ lying on a line in the surface $F(t_1, t_2, y) = 0$. For the second count, note that the involved roots y can be bounded by cB where c is a constant depending only on F (and more precisely on the finitely many lines in the surface). Thus we obtain:

$$N_T(F, B) \leq N(F, cB) + N_1(F, (1 + m)^2 H B^m)$$

and we can improve our previous estimate for $N_T(F, B)$ by using the following result of Heath-Brown[6] (theorem 7 and theorem 9 of [H-B]):

For any absolutely irreducible polynomial $F \in \overline{\mathbb{Q}}[X_1, X_2, X_3]$ of degree d, if $N_1(F, B)$ is the number of integral points on the hypersurface $F(x_1, x_2, x_3) = 0$ not lying on any line contained in F, we have $N_1(F, B) \ll_\varepsilon B^{1/2+3/2\sqrt{d}+\varepsilon}$. Counting also points lying on lines, we have $N(F, B) \ll_\varepsilon B^{1+\varepsilon}$ if $d \geq 2$.

[6] As before, Heath-Brown's results concern rational points on a projective variety and should be first adapted to our affine situation.

We obtain $N_T(F,B) \ll_\varepsilon B^{1+\varepsilon} + B^{m/2+3m/2\sqrt{d}+\varepsilon}$ and can further give the conjectural bound $N_T(F,B) \ll_\varepsilon B^{1+\varepsilon} + B^{m/2+\varepsilon}$ under the conjecture of Heath-Brown that $N_1(F,B) \ll_\varepsilon B^{1/2+\varepsilon}$. One can also hope to extend this type of results to polynomials defining a surface not containing a curve of degree less than a fixed number.

6.2. Miscellaneous comments.

6.2.1. Improving on strategy one. The key estimates for theorem 3.3 are inequalities (4) and (5) from §2.4; and what really counts for the final result are the constants C_1 and C_2. Indeed even if the term $B^{1/2}\log^5(B)$ could be disregarded in (4) (which is conceivable in the positive genus case but would be a strong effective form of Siegel's theorem), the bound for the least hilbertian specialization would still remain polynomial in C_2. Improving on C_2 would then mean for example replacing the power $\deg_T(F)^{64}$ by some term with slower growth. This seems difficult: such polynomial term is needed in C_2 due to the mere constraint of working with integers not among the roots of the discriminant $\Delta(T)$ of F in Y. Then there is also in C_2 the group-theoretical term $\sum_{M\in\mathcal{M}_P}[G:M]$ which we know can be exponential in $\deg_Y(P)$ in some cases (see remark 3.4). Improving on theorem 3.3 seems to require a better analysis, both diophantine and group-theoretical, of the arithmetic of the (minimal) function fields contained in the Galois closure of the polynomial P.

6.2.2. The Eichler-Fried method. This is another classical method in the context of Hilbert's irreducibility theorem ([Ei], [Fr] or [Wa1] chapitre 3). Here is a sketch of it. Let $\{Q_1(T,Y),\dots,Q_N(T,Y)\} \subset \mathbb{Q}[T,Y]$ be a set of irreducible and monic (in Y) polynomials as given by the preliminary reduction (section 3.1). Again one may reduce to the case they are absolutely irreducible. From Ostrowski's theorem, for all but finitely many primes p the reduction of Q_i modulo p, denoted by $\overline{Q_i}$, is still absolutely irreducible, $i=1,\dots,N$. One can then show that for infinitely many of these primes p, there exists an integer t_i such that the equation $Q_i(t_i,Y)=0 \ [\mathrm{mod}\ p]$ has no root in $\mathbb{Z}$, $i=1,\dots,N$. This uses Weil's inequalities for rational points on curves over finite fields and the classical fact that infinitely many primes split in any given finite Galois extension $L/\mathbb{Q}$ (a consequence of Tchebotarev's density theorem). For each $i=1,\dots,N$, fix such a prime p_i in such a way that $p_1,\dots,p_N$ are distinct. Thanks to the chinese remainder

theorem one can then construct an arithmetic progression $(t_0 + kp_1 \dots p_N)_k$ of specializations t such that no equation $Q_i(t, Y) = 0$ $(i = 1, \dots, N)$ has a solution in $\mathbb{Z}$, and so $P(t, Y)$ is irreducible in $\mathbb{Q}[Y]$.

This method is algorithmically simple but does not provide good bounds. The main obstacle is that known effective bounds for Ostrowski's theorem are rather big: according to [Za], it is for primes $p > e^{12m^2n^2}(4n^2m)^{8n^2m}H^{2(2n-1)^2m}$ that an absolutely irreducible polynomial $F(T, Y) \in \mathbb{Z}[T, Y]$ with degrees m, n with respect to T and Y and with height H remains absolutely irreducible modulo p. Furthermore bounding the primes $p_1, \dots, p_N$ cannot seem to be done efficiently.

The following example shows further one cannot hope removing the dependence on the height by this method.

Example 6.1. For each $N > 0$ let $p(N)$ be the product of all primes less than N and $P_N(T, Y) = Y^2 - T^2 - p(N)$. This polynomial is absolutely irreducible and the least prime such that it remains absolutely irreducible modulo p is $\geq N$.

6.2.3. A special assumption. In addition to the usual hypotheses on $P(T, Y)$, assume that $P(0, Y)$ has a simple root in $\mathbb{Q}$. Then from [De1] corollaire 2, there exists a constant h_0 depending only P such that for any $t \in \mathbb{Q}$ of the form $t = 1/m$ or $t = p^m$ with $m \in \mathbb{Z}$, $m > 0$ and p a prime number, if $|\log(t)| > h_0$ then $P(t, Y)$ is irreducible in $\mathbb{Q}[Y]$. The constant h_0 has precisely been computed in [De3]: it can be taken to be $5000D^{12}H^2$. The good specializations t provided by this result are big compared to the bounds of this paper: their height, *i.e.* m or p^m, is at least in $\exp(5000D^{12}H^2)$. The advantage of this result though is that one does not have to test irreducibility of $P(t, Y)$: it is guaranteed that these t are good specializations. In terms of algorithmic speed, this result is better than those of this paper for finding good hilbertian specializations. It however has a strong arithmetic assumption.

As explained in [De3] there is a trick to get rid of this assumption. There is however a price to pay: instead of a specific good specialization as above, the conclusion is that there exists one among several explicitly given rational numbers. The number of these possible candidates is rather limited but because it is > 1, one has to test the irreducibility of the corresponding specialized polynomials (using classical irreducibility tests for polynomials in one variable). And this cannot be done in polynomial time because the specializations are too big.

6.3. A variant. It is an exercise to show that, given $P(T,Y) \in \mathbb{Q}[T,Y]$, if for some $b(Y) \in \mathbb{Q}[Y]$ such that $\deg(b) > \deg_Y(P)$, the polynomial $P(b(Y),Y)$ is irreducible in $\mathbb{Q}[Y]$, then P is irreducible in $\mathbb{Q}[T,Y]$ (use the uniqueness of the $b(Y)$-adic decomposition of $P(b(Y),Y)$). The converse is also true:

Proposition 6.2 — *Given a polynomial $P(T,Y) \in \mathbb{Q}[T,Y]$ irreducible, there exist infinitely many polynomials $b(Y) \in \mathbb{Q}[Y]$ with $\deg(b) > \deg_Y(P)$ such that $P(b(Y),Y)$ is irreducible in $\mathbb{Q}[Y]$.*

The difference with Hilbert's irreducibility theorem is that T is specialized in $\mathbb{Q}[Y]$ instead of $\mathbb{Q}$. For applications this new variant can be as useful.

Proposition 6.2 actually follows from Hilbert's irreducibility theorem, applied to the polynomial

$$\mathcal{P}(T,T_1,\dots,T_d,Y) = P(T+T_1Y+\cdots+T_dY^d,Y)$$

where $d > \deg_Y(P)$ is some integer and $T_1,\dots,T_d$ are variables. One only needs to check that

(12) *the polynomial $\mathcal{P}$ is irreducible in $\mathbb{Q}(T,T_1,\dots,T_d)[Y]$.*

The proof of (12) is given below. The statement can then be made more precise: given an integer $d > \deg_Y(P)$, the set of polynomials $b(Y)$ of degree $\le d$ satisfying the desired conclusion, viewed as a subset of $\mathbb{Q}^{d+1}$, is a hilbertian set and in particular is Zariski-dense.

However as we know available bounds in the several variable case of Hilbert's irreducibility theorem are big. As far as effectiveness is concerned it would be interesting to find an alternate approach of proposition 6.2 (which could let d vary and thereby offer more room where to specialize).

Proof of (12)**.** We will more generally prove (12) with $\mathbb{Q}$ replaced by any infinite field K.

Suppose $\mathcal{P}(T,T_1,\dots,T_d,Y) = \mathcal{Q}(T,T_1,\dots,T_d,Y)\,\mathcal{R}(T,T_1,\dots,T_d,Y)$ for some polynomials $\mathcal{Q},\mathcal{R} \in K[T,T_1,\dots,T_d,Y]\backslash K[T,T_1,\dots,T_d]$. Specializing $(T_1,\dots,T_d)$ to any fixed d-tuple $\mathbf{t} = (t_1,\dots,t_d) \in K^d$ yields

$$P(T + t_1Y + \cdots + t_dY^d, Y) = \mathcal{Q}(T, t_1, \ldots, t_d, Y)\,\mathcal{R}(T, t_1, \ldots, t_d, Y)$$

Set $\varphi_{\mathbf{t}}(Y) = t_1Y + \cdots + t_dY^d$. Changing (T, Y) for $(T - \varphi_{\mathbf{t}}(Y), Y)$ in the previous identity yields $P(T, Y) = \mathcal{Q}(T - \varphi_{\mathbf{t}}(Y), t_1, \ldots, t_d, Y)\,\mathcal{R}(T - \varphi_{\mathbf{t}}(Y), t_1, \ldots, t_d, Y)$. As $P(T, Y)$ is irreducible in $K[T, Y]$, one of the two polynomials on the right-hand side is in K. But changing (T, Y) to $(T + \varphi_{\mathbf{t}}(Y), Y)$ then gives that $\mathcal{Q}(T, t_1, \ldots, t_d, Y)$ or $\mathcal{R}(T, t_1, \ldots, t_d, Y)$ is in K. As this holds for every d-tuple $\mathbf{t} = (t_1, \ldots, t_d) \in K^d$, we obtain a contradiction with the assumption that neither $\mathcal{Q}$ nor $\mathcal{R}$ is in $K[T, T_1, \ldots, T_d]$. Note further that $\deg_Y(\mathcal{P}) \geq 1$ (as $\mathcal{P}(T, 0, \ldots, 0, Y) = P(T, Y)$) to conclude that $\mathcal{P}$ is irreducible in $K(T, T_1, \ldots, T_d)[Y]$. □

Remark 6.3. The argument actually shows $\mathcal{P}$ is irreducible in $K(T_1, \ldots, T_d)[T, Y]$ and it is in fact also irreducible in $K[T_1, \ldots, T_d, T, Y]$. To obtain this extra conclusion, we are left with showing that $\mathcal{P}$ does not factor as $\mathcal{P} = \mathcal{Q}(T_1, \ldots, T_d)\mathcal{R}(T, T_1, \ldots, T_d, Y)$ with $\mathcal{Q} \in K[T_1, \ldots, T_d] \backslash K$ and $\mathcal{R} \in K[T, T_1, \ldots, T_d, Y]$. Assume the contrary holds. Plugging in $T = T_2 = \ldots = T_d = 0$ yields $P(T_1Y, Y) = \mathcal{Q}(T_1, 0, \ldots, 0)\mathcal{R}(0, T_1, 0, \ldots, 0, Y)$. Set $U = T_1Y$ to rewrite it as $P(U, Y) = \mathcal{Q}(U/Y, 0, \ldots, 0)\mathcal{R}(0, U/Y, 0, \ldots, 0, Y)$. Irreducibility of P in $K[U, Y]$ then gives $\deg_{T_1}(\mathcal{Q}) = 0$. More generally substitute 0 for T and for all parameters $T_1, \ldots, T_d$ but the i-th one T_i to get that $\deg_{T_i}(\mathcal{Q}) = 0$, $i = 1, \ldots, d$.

Acknowledgments. We wish to thank R. Guralnick and M. Liebeck for their help in the group-theoretical part of the paper.

References

[Am] Y. Amice, *Les nombres p-adiques*, Collection Sup. Le Mathématicien **14**, P.U.F., (1975)

[AsGu1] M. Aschbacher and R. Guralnick, "Solvable generation of groups and Sylow subgroups of the lower central series", *J. Algebra*, **77**, (1982), no. 1, 189–201.

[AsGu2] M. Aschbacher and R. Guralnick, "On abelian quotients of primitive groups", *Proc. Amer. Math. Soc.*, **107**, (1989), no. 1, 89–95.

[BaCaPá] L. Babai, P. J. Cameron and P. Pálfy, "On the orders of primitive groups with restricted nonabelian composition factors", *J. Algebra*, **79**, (2002), 95–113.

[CHarM] L. Caporaso, J. Harris and B. Mazur, "Uniformity of rational points", *J. Amer. Math. Soc.* , **10**, (1997), 1–35.

[De1] P. Dèbes, "G-fonctions et Théorème d'irréductibilité de Hilbert", *Acta Arithmetica*, **47**, n^o 4, (1986), 371–402.

[De2] P. Dèbes, "On the irreducibility of the polynomials $P(t^m, Y)$", *J. Number Theory*, **42**, n^o 2 (1992), 141–157.

[De3] P. Dèbes, "Hilbert subsets and s-integral points", *Manuscripta Mathematica*, **89**, (1996), 107–137.

[Ei] M. Eichler, "Zum Hilbertschen Irreduzibilittssatz", *Math. Ann., Berlin*, **116**, (1939), 742-748.

[Fr] M. Fried, "On Hilbert's irreducibility theorem", J. Number Theory, **6**, (1974), 211–231.

[FrJa] M. Fried and M. Jarden, *Field Arithmetic*, Springer Verlag, First Edition (1986).

[H-B] D. R. Heath-Brown, "The density of rational points on curves and surfaces", *Ann. of Math.*, **155**, (2002), 553–595.

[KoNe] L. G. Kovacs and M. F. Newman, "Generating transitive permutation groups", *Quart. J. Math. Oxford Ser.*, (2) **39**, (1988), 361–372.

[Li] M. W. Liebeck, "On minimal degrees and base sizes of primitive permutation groups", *Arch. Math.*, **43**, (1984), 11–15.

[LiMaSh] M. W. Liebeck, "On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function", *Duke Math. J.*, (to appear).

[LiSh1] M. W. Liebeck and A. Shalev, "Bases of permutation groups", preprint

[LiSh2] M. W. Liebeck and A. Shalev, paper in preparation.

[LuSe] A. Lubotsky and D. Segal, "Subgroup growth", *Prog. Math.*, **212**, Birkhäuser (2003).

[Ne] A. Néron, "Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps", *Bull. Soc. Math. France*, **80**, (1952), 101–166.

[Pa] P. Pacelli, "Uniform boundedness for rational points", *Duke Math. J.* , **88**, n^o 1, (1997), 77–102.

[Pá] P. P. Pálfy, "A polynomial bound for the orders of primitive solvable groups", *J. Algebra*, **77**, (1982), 127–137.

[ScZa] A. Schinzel and U. Zannier, "The least admissible value of the parameter in Hilbert's Irreducibility Theorem", *Acta Arith.*, **69**, n3 (1995), 293–302.

[Se1] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, translated by M.Brown from notes by M.Waldschmidt, Vieweg, (1990).

[Se2] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett Publ., Boston, (1992).

[Wa1] Y. Walkowiak, "Effectivité dans le théorème d'irréductibilité de Hilbert", Thèse de Doctorat, Univ. Lille1, (2004).

[Wa2] Y. Walkowiak, "Théorème d'irréductibilité de Hilbert effectif", *Acta Arithmetica*, **116**, n^o 4, (2005), 343–362.

[Wal] G. E. Wall, "Some applications of the Eulerian functions of a finite group", *J. Austral. Math. Soc.*, **2**, 1961/1962, 35–59.

[Wo] T. R. Wolf, "Solvable and nilpotent subgroups of $\mathrm{GL}(n, q^m)$", *Canad. J. Math.*, **34**, n^o 4, (1982), 1097–1111.

[Ya] M. Yasumoto, "Algebraic extensions of non-standard models and Hilbert's irreducibility theorem", *Journal of Symbolic Logic*, **53** (1988), n^o 4, 470–480.

[Za] U. Zannier, "On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$, *Archiv. Math.*, **68**, (1997), 129–138.

Pierre Dèbes
Université Lille 1, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France
E-mail: Pierre.Debes@univ-lille1.fr

Yann Walkowiak
IUT de Laval - Département Informatique, 52 rue des docteurs Calmette et Guérin, 53000 Laval Cedex 9, France
E-mail: yann.walkowiak@univ-lemans.fr