Chapter 4
Hilbert Irreducibility Theorem

4.1 Hilbert Irreducibility Theorem

In this section we shall be interested in discussing proofs, generalizations and geometric formulations of the so-called Hilbert Irreducibility Theorem (HIT in the sequel).

Here is the original statement, proved by Hilbert in 1894:

Theorem 4.1.1 (Hilbert Irreducibility Theorem)**.** *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a polynomial, of degree ≥ 1 in Y, irreducible in the ring $\mathbb{Q}[X,Y]$. Then there exist infinitely many integers $n \in \mathbb{Z}$ such that the specialized polynomial $F(n,Y) \in \mathbb{Z}[Y]$ is irreducible in the ring $\mathbb{Q}[Y]$.*

In the case when $\deg_Y F \geq 2$, the only interesting one, as a corollary we obtain that:

Under the above hypothesis on the polynomial $F(X,Y)$, for infinitely many $n \in \mathbb{Z}$ the specialized polynomial $F(n,Y)$ has no rational root.

Consider the plane algebraic curve of equation $\mathcal{C} : F(x,y) = 0$; it is endowed with a map $\mathcal{C} \to \mathbb{A}^1$ defined by the x function: $\mathcal{C} \ni (x,y) \mapsto x \in \mathbb{A}^1$. The above weak conclusion of HIT asserts that the map $x : \mathcal{C}(\mathbb{Z}) \to \mathbb{Z}$ is not surjective. The full HIT predicts that for infinitely many points $n \in \mathbb{Z} = \mathbb{A}^1(\mathbb{Z})$, the pre-image $x^{-1}(n)$ is irreducible, i.e. forms a single orbit for the natural action of the Galois group.

A natural generalization to several variables and arbitrary number fields reads as follows:

Theorem 4.1.2. *Let κ be a number field, $d \geq 1$ a positive integer, $F(X_1,\ldots,X_d,Y) \in k[X_1,\ldots,X_d,Y]$ an irreducible polynomial of degree ≥ 1 in Y. Then for a Zariski-dense set of rational points $(a_1,\ldots,a_d) \in \kappa^d$ the specialized polynomial $F(a_1,\ldots,a_d,Y) \in \kappa[Y]$ is irreducible.*

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in Mathematics, DOI 10.1007/978-981-10-2648-5_4

We provide an equivalent geometric formulation:

Theorem 4.1.3. *Let V be an irreducible affine algebraic variety of dimension $d \geq 1$, $\pi : V \to \mathbb{A}^d$ a dominant morphism, all defined over a number field κ; there exists a Zariski-dense subset of rational points $(a_1, \ldots, a_d) \in \mathbb{A}^d(\kappa) = \kappa^d$ such that each of their fibre $\pi^{-1}(a_1, \ldots, a_d)$ is irreducible.*

By irreducible, we mean of course irreducible over κ; it will be a finite set of points of $V(\bar{\kappa})$, all conjugate over κ to a single point.

The link between Theorems 4.1.2 and 4.1.3 is clear: a polynomial $F(X_1, \ldots, X_d, Y) \in \kappa[X_1, \ldots, X_d, Y]$ defines the affine variety in $\mathbb{A}^{d+1}$ of equation $F = 0$, which is naturally endowed with a dominant morphism to the affine space $\mathbb{A}^d$ (projection on the first d coordinates). If the polynomial F is monic in Y, such a projection is also a finite map; we then speak of ramified covering of the affine space.

Remark. Since the affine spaces are simply connected, each covering of degree > 1 of $\mathbb{A}^d$ must ramify somewhere, actually over a codimension one subvariety.

Hilbert Irreducibility Theorem (H.I.T.) is in a sense a converse to the Chevalley-Weil Theorem discussed in the previous section. While the Chevalley-Weil theorem applies in the situation where an unramified covering of algebraic varieties is given (and it predicts a sort of surjectivity over the set of rational points) H.I.T. holds for certain coverings of rational varieties, which do ramify. A weak conclusion of H.I.T. is the non-surjectivity of the set-theoretic map between the sets of rational points.

We shall see in a moment that actually this seemingly weaker statement asserting non-surjectivity over rational points is in fact equivalent to the full H.I.T. provided one admits coverings by possibly reducible varieties. The following statement will be regarded as the general Hilbert Irreducibility Theorem, and will be proved to be equivalent to Theorem 4.1.2:

Theorem 4.1.4. *Let κ be a number field, X be an algebraic variety defined over κ of dimension d and $\pi : X \dashrightarrow \mathbb{A}^d$ a dominant rational map, also defined over κ. Suppose that π admits no section $\theta : \mathbb{A}^d \dashrightarrow X$. Then the set $\mathbb{A}^d(\kappa) = \kappa^d$ is not contained in the image $\pi(X(\kappa))$ of the rational points of X. Moreover, the set $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is Zariski-dense on $\mathbb{A}^d$.*

Remarks. (1) If X is irreducible, then the rational map π admits no section if and only if it has degree > 1; in general, the existence of a section is equivalent to the existence of an irreducible component of X where the restriction of π is a birational isomorphism to $\mathbb{A}^d$. (2) Due to the birational invariance of the above statement, the affine space $\mathbb{A}^d$ could be replaced by any κ-rational variety.

Following Serre [48] we call *thin* the sets of rational points which are images of morphisms admitting no section. Precisely:

Definition. Let Y be an algebraic variety defined over a field κ. A subset $A \subset Y(\kappa)$ is said to be *thin* with respect to κ if there exists an algebraic variety X with $\dim X \leq \dim Y$ and a rational map $\pi : X \dashrightarrow Y$ defined over κ such that π admits no sections and A is contained in the image $\pi(X(\kappa))$ of the rational points of X.

We can always decompose the variety X as $X = X' \cup X''$, for two closed subvarieties X', X'', where X' is of pure dimension $d = \dim X = \dim Y$ or is empty and every component of X'' (which might also be empty) has dimension $< d$. Now a rational map $\pi : X \to Y$ admits a section if and only if it is of degree one when restricted to a suitable irreducible component of X'. Also, note that the image of X'' is contained in a hypersurface of $\mathbb{A}^d$.

Hence thin sets in $\mathbb{A}^d$ according to Serre's definition above are union of sets of two kinds: (1) sets of rational points contained in a proper closed subvariety; (2) images of rational points of a variety of pure dimension d under a map admitting no rational section. Again, type (2) sets could be alternatively defined as finite union of images of rational dominant maps of degree > 1 defined on an *irreducible variety* of the same dimension.

We shall prove that those of type (1) are in fact contained in sets of type (2). This is the content of the following lemma (compare with [12], Lemma 5.2)

Lemma 4.1.5. *Let $Y \subset \mathbb{A}^d$ be a proper closed subvariety defined over a field κ. There exists an irreducible algebraic variety X of dimension d and a finite map $\pi : X \to \mathbb{A}^d$ of degree > 1 such that $Y(\kappa) \subset \pi(X(\kappa))$.*

Proof. Let $P(X_1, \dots, X_d) \in k[X_1, \dots, X_d]$ be a non-zero squarefree polynomial vanishing identically on Y. Let $X \subset \mathbb{A}^{d+1}$ to be the variety defined by the equation $Y^2 = P(X_1, \dots, X_d)$. Then X is irreducible (since P is square-free, in particular not a square); projection $\pi : X \to \mathbb{A}^d$ onto the x-coordinates provides a finite map such that $Y(\kappa) \subset \pi(X(\kappa))$. □

In view of the above lemma, we could rephrase the definition of thin set by saying that a subset $Z \subset \mathbb{A}^d(k)$ is thin with respect to κ if it is contained in the image $\pi(X(\kappa))$ where X is a union of irreducible varieties each of dimension d and $\pi : X \to \mathbb{A}^d$ is dominant of degree > 1 on each component of X.

In view of the above consideration, Theorem 4.1.4 becomes equivalent to the statement where "variety of dimension d" is replaced by "variety of pure dimension d". Also, it is equivalent to the following statement: *the set $\mathbb{A}^d(\kappa)$ is not thin.* To justify that this last statement does imply also the last sentence of Theorem 4.1.4, namely that $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is Zariski-dense, note that if it were not, up to adding a type (1) subset to $\pi(X(\kappa))$ (which is possible by Lemma 4.1.5), we would obtain the emptiness of $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$, contrary to the fact that $\mathbb{A}^d(\kappa)$ is not thin.

Finally, it remains to us to prove Theorem 4.1.4 in some of its equivalent formulations discussed above and to prove that it formally implies the apparently stronger Theorem 4.1.3.

Proof of Theorem 4.1.4. We start by proving its 1-dimensional analogue:

Theorem 4.1.6. *Let $\mathcal{C}$ be an algebraic curve defined over a number field κ, $\pi : \mathcal{C} \dashrightarrow \mathbb{A}^1$ be a rational dominant map admitting no section. Then $\mathbb{A}^1(\kappa) \not\subset \pi(\mathcal{C}(\kappa))$.*

Proof. We easily reduce to the case where $\mathcal{C}$ is smooth and $\pi : \mathcal{C} \to \mathbb{A}^1$ is a finite morphism; this might affect the set $\pi(\mathcal{C}(\kappa))$ only by a finite set. Then decompose $\mathcal{C}$ into the union $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$ of its irreducible components. We know by hypothesis that the restriction $\pi_{|\mathcal{C}_i}$ has degree > 1 for each $i = 1, \ldots, r$ and we have to prove that $\mathbb{A}^1(\kappa) \not\subset \bigcup_{i=1}^r \pi(\mathcal{C}_i(\kappa))$. Let us choose a finite set S of places of κ containing the archimedean ones. Since the ring extension $\kappa[\mathcal{C}]/\pi^*\kappa[\mathbb{A}^1]$ is integral, after enlarging if necessary the set S, we can suppose that the ring extension $\mathcal{O}_S[\mathcal{C}]/\pi^*\mathcal{O}_S[\mathbb{A}^1]$ is also integral. By this we mean that the each component $\mathcal{C}_i$ is defined by an equation $P_i(X, Y) = 0$, where $P_i(X, Y) \in \mathcal{O}_S[X, Y]$ has S-integral coefficients, is monic in Y and the map $\pi : \mathcal{C} \to \mathbb{A}^1$ is the projection on the X-coordinate. Clearly, it suffices to prove that $\mathbb{A}^1(\mathcal{O}_S) \not\subset \pi(\mathcal{C}(\kappa))$, but in view of the integrality of the ring extension $\mathcal{O}_S[\mathcal{C}]/\pi^*\mathcal{O}_S[\mathbb{A}^1]$, each κ-rational pre-image of an S-integer is necessarily an S-integer point of $\mathcal{C}$. If $\mathcal{C}(\mathcal{O}_S)$ is finite, we are done, since $\mathbb{A}^1(\mathcal{O}_S) = \mathcal{O}_S$ is an infinite set. Otherwise, consider the different components $\mathcal{C}_i$ of $\mathcal{C}$ endowed with maps $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$, for $i = 1, \ldots, r$. By hypothesis, for each $i \in \{1, \ldots, r\}$, the map $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$ has degree > 1. Now, consider a non-constant polynomial $p(t) \in \mathcal{O}_S[t]$, which will be chosen later; it defines a finite morphism $p : \mathbb{A}^1 \to \mathbb{A}^1$. We can construct for each $i \in \{1, \ldots, r\}$ the *fiber product* $\mathcal{C}'_i \to \mathbb{A}^1$ of $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$ and $p : \mathbb{A}^1 \to \mathbb{A}^1$, namely the curve

$$\mathcal{C}'_i := \{(\alpha, \beta) \in \mathcal{C}_i \times \mathbb{A}^1 \, : \, \pi_i(\alpha) = p(\beta)\},$$

endowed with its natural projection on $\mathbb{A}^1$, sending $(\alpha, \beta) \mapsto \beta$. Let us choose the polynomial $p(t)$ in such a way that each corresponding curve $\mathcal{C}'_i$ is irreducible and has positive genus. It suffices for this to choose $p(t) = t^3 + c$, where $c \in \mathcal{O}_S$ is chosen outside the zero branch locus of any of the π_i. Hence we have a choice working for all components $\mathcal{C}_i$. Now, the points of $\mathbb{A}^1$ which are both of the form $p(\beta)$ for $\beta \in \mathcal{O}_S$ and $\pi_i(\alpha)$, for $\alpha \in \mathcal{C}_i(\mathcal{O}_S)$, are images of S-integral points of $\mathcal{C}'_i$, by our construction of $\mathcal{C}'_i$. However, by Siegel's Theorem all the curves $\mathcal{C}'_i$ have only finitely many S-integral points; hence only finitely many of the points of the set $p(\mathcal{O}_S) \subset \mathbb{A}^1(\mathcal{O}_S)$ can be images of S-integral points of $\mathcal{C}$, so infinitely many of them lie outside $\pi(\mathcal{C}(\mathcal{O}_S))$. □

End of the proof of Theorem 4.1.4. Let us assume that $\pi : X \dashrightarrow \mathbb{A}^d$ is as above; again, one easily reduces to the case where $\pi : X \to \mathbb{A}^d$ is actually a morphism. Suppose by contradiction that $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is not Zariski-dense, so it is contained in a hypersurface $Z \subset \mathbb{A}^d$. Let us choose a line $l \subset \mathbb{A}^d$, defined over κ such that: (1) $l \not\subset Z$; (2) the pre-image $\pi^{-1}(l)$ is a curve; (3) $\mathcal{C}$ and $\pi_{|\mathcal{C}} : \mathcal{C} \to l$ admits no section. The existence of such a line can be proved by standard application of Bertini's theorem. Then Theorem 4.1.6 provides the desired contradiction. □

Proof of Theorem 4.1.3. As promised, we now prove Theorem 4.1.3, by deducing it from Theorem 4.1.4. Recall that we are given an irreducible affine variety V of dimension d and a dominant rational map $\pi : V \dashrightarrow \mathbb{A}^d$ of degree > 1. We want to prove that for a Zariski-dense set of rational points in $\mathbb{A}^d(\kappa)$, each pre-image is irreducible over κ. Again, it is easy to reduce to the case of dimension 1 and of a finite morphism $\pi : V \to \mathbb{A}^1$ (here V is an irreducible curve). We note at once that if the degree of π is two or three, then Theorem 4.1.4 immediately implies our conclusion: actually, if the pre-image of a point, which consists of two or three algebraic points, contains no rational point, it means that such pre-image is made of Galois conjugate elements (in other words: if a polynomial in one variable of degree two or three has no roots, then it is irreducible). To explain the strategy of our proof, let us consider the case of a map $\pi : V \to \mathbb{A}^1$ of degree four. Then, for a point $\alpha \in \mathbb{A}^1(\kappa)$, having a rational pre-image is not equivalent to having a reducible pre-image: it may be that the pre-image is made of two Galois orbits of quadratic points. Let us define the *fibered square* $V \times_\pi V$ of V with respect to π as

$$V \times_\pi V := \{(x, y) \in V \times V \, : \, \pi(x) = \pi(y)\};$$

it is a curve, endowed with a natural projection to $\mathbb{A}^1$; let us also define its symmetric fibered square as the quotient of the variety $V \times_\pi V$ by the natural involution interchanging x and y, and denote it by $V^{(2)}$; it is a reducible curve, contains canonically V via the diagonal embedding $V \hookrightarrow V \times_\pi V$. The reducible curve $V^{(2)}$ is still endowed with a natural projection to $\mathbb{A}^1$, which we denote by π_2. If π has degree 4, which we are assuming, then $\deg(\pi_2) = 4 + 6 = 10$. Now, for a point $\alpha \in \mathbb{A}^1(\kappa)$, the existence of a rational point in the pre-image $\pi_2^{-1}(\alpha)$ is equivalent to the reducibility of the pre-image $\pi^{-1}(\alpha) \subset V(\bar{\kappa})$. So, Theorem 4.1.4 implies the conclusion of Theorem 4.1.3 in this case.

The general case is analogous: if n denotes the degree of the map π, it suffices to consider the union of the curves $V^{(i)}$, where each $V^{(i)}$ is the i-th fold symmetric fiber product of V with itself (with respect to π), for $i = 1, \ldots, [n/2]$. □

4.2 Universal Hilbert Sequences

Let us consider the simplest case treated by Hilbert himself, namely that of a polynomial $P(X, Y) \in \mathbb{Z}[X, Y]$, irreducible of degree ≥ 1 in Y. By Hilbert Irreducibility Theorem 4.1.1, there exists an infinite sequence $x_0 < x_1 < x_2, < \ldots$ of integers such that the polynomial $P(x_n, Y)$ is irreducible in $\mathbb{Q}[Y]$ for every n. One can ask whether there exists a single sequence working for all irreducible polynomials: of course, we must neglect a finite set depending on the given polynomial, namely the precise question is: *does there exist a sequence* $x_0 < x_1 < x_2, < \ldots$ *of integers such that for every irreducible polynomial* $P(X, Y) \in \mathbb{Z}[X, Y]$ *of positive degree in* Y *there exists an index* $n_0(P)$ *such that for every* $n > n_0(P)$ *the specialized polynomial* $P(x_n, Y)$ *is irreducible in* $\mathbb{Q}[Y]$*?* A positive answer to this question can be given via a diagonalization argument, starting from the original result of Hilbert. It is however tempting to search for explicit sequences with the above property. They are commonly called *Universal Hilbert Sequences.* The first examples, to our knowledge, have been provided by Sprindzuk [53]; other examples have been constructed by Bilu [5] and Dèbes and Zannier [24].

We shall content to show one example, drawn from the paper [14], which classifies Universal Hilbert Sequences among power sums. By a power sum we mean in this context a function $\mathbb{N} \to \mathbb{Q}$ of the form

$$n \mapsto u(n) = b_1 a_1^n + \ldots + b_k a_k^n,$$

where $k \in \mathbb{N}$ and $a_1, \ldots, a_k$ are natural number and $b_1, \ldots, b_k$ are rational numbers. Theorem 4 of [14] reads as follows:

Theorem 4.2.1. *Let $u : \mathbb{N} \to \mathbb{Q}$ be a power sum as above. The following are equivalent:*

(1) the sequence $u(0), u(1), \ldots$ is a Universal Hilbert Sequence;

(2) there exist no integer $d \geq 2$, polynomial $P(X) \in \mathbb{Q}[X]$ of degree d and power sum $v : \mathbb{N} \to \mathbb{Q}$ such that identically $u(nd) = P(v(n))$.

As an example, the sequence $n \mapsto 2^n + 3^n$ is a U.H.S.. Clearly, it is not the case for the sequence $n \mapsto u(n) := 2^n$, or any other geometric progression; actually for the last sequence u, note that putting $P(X) = X^2$ one has $u(2n) = P(u(n))$, so condition (2) is not satisfied.

We now give a sketch of the proof that the sequence $u(n) := 2^n + 3^n$ is a U.H.S.; the general proof of Theorem 4.2.1 is obtained by following the same path.

As in the deduction of Theorem 4.1.3 from Theorem 4.1.4, we reduce to proving the following:

Proposition 4.2.2. *Let $P(X, Y) \in \mathbb{Z}[X, Y]$ be an irreducible polynomial of degree $d \geq 2$ in Y. Then the equation $P(2^n + 3^n, y) = 0$ has only finitely many solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$.*

Proof. Suppose by contradiction that the equation $P(2^n + 3^n, y) = 0$ has infinitely many integral solutions. Then by Siegel's finiteness theorem on integral points (Theorem 3.3.1), the curve of equation $P(X, Y) = 0$ must have genus zero and only one or two points at infinity. In algebraic language, there exist two non-constant rational functions $f(t), g(t)$ such that $P(f(t), g(t)) \equiv 0$, and such that for infinitely many $n \in \mathbb{N}$, $2^n + 3^n = f(t_n)$ for a suitable $t_n \in \mathbb{Q}$. Moreover, the degree of $f(t)$ equals $d = \deg_Y P$ and $f(t), g(t)$ can have only one or two poles (all together). In the first case, after a change of variables, we obtain that $f(t), g(t) \in \mathbb{Q}[t]$ are polynomials. We then have, again by our assumptions on the infinitude of the integral solutions to the original equation, that the equation $2^n + 3^n = f(t)$ has infinitely many solutions $(n, t) \in \mathbb{N} \times \mathbb{Q}$. After a translation of the form $t \mapsto t + c$, we can suppose that the polynomial $f(t) \in \mathbb{Q}[t]$ is of the form $f(t) = at^d + a_2 t^{d-2} + \ldots + a_d$. Since the denominators of t must be bounded, we can suppose after another change of variable that t is in fact an integer, so the equation $2^n + 3^n = f(t)$ has infinitely many integral solutions, where $f(t)$ has degree d and no term of degree $d - 1$. In particular, for infinitely many pairs $(n, t) \in \mathbb{N} \times \mathbb{Z}$ we shall have

$$|2^n + 3^n - at^d| \ll |t|^{d-2}.$$

Working on each arithmetic progression modulo d and writing $n = md + r$, we can say that for at least one value of $r \in \{0, \dots, d-1\}$ and a positive real number c_1, the Diophantine inequality

$$|2^r 2^{md} + 3^r 3^{md} - at^d| < c_1 |t|^{d-2}$$

has infinitely many integral solutions $(m, t) \in \mathbb{N} \times \mathbb{Z}$. □

Now we can rewrite the above inequality as

$$\left| \frac{2^r 2^{md} + 3^r 3^{md}}{t^d} - a \right| < c_1 |t|^{-2},$$

so

$$\left| \frac{3^{r/d} 3^m \sqrt[d]{1 + 2^r 2^{md} 3^{-r} 3^{-md}}}{t} - a^{1/d} \right| < c_2 |t|^{-2},$$

for a suitable constant c_2. Here $3^{r/d}$ and $a^{1/d}$ denote suitable real d-th roots of 3^r and a. Now let us express by Taylor development $\sqrt[d]{1+u}$ as $1 + \delta_1 u + \delta_2 u^2 + O(u^3)$ where δ_1, δ_2 are the rational numbers $\delta_1 = \binom{1/d}{1} = \frac{1}{d}, \delta_2 = \binom{1/d}{2} = \frac{1-d}{2d^2}$. Putting $\alpha_i = \delta_i \cdot \frac{2^{ri}}{3^{ri}}$ for $i = 1, 2$ and noting that $\frac{2^{6m}}{3^{6m}} \ll t^{-2}$ (since t tends to infinity as 3^m), we obtain from the above displayed inequality that

$$\left| \left(\frac{3^{r/d} 3^m}{t} \right) \left(1 + \alpha_1 \frac{2^{md}}{3^{md}} + \alpha_2 \frac{4^{md}}{9^{md}} \right) - a^{1/d} \right| < c_2 \frac{1}{t^2}.$$

Observe that the term $\frac{3^{r/d} 3^m}{t}$ converges to a non-zero limit for $m \to \infty$; so after multiplying both sides by $9^{md} \cdot \frac{t}{3^{r/d} 3^m}$ we obtain we obtain that the inequality

$$|9^{md} + \alpha_1 6^{md} + \alpha_2 4^{md} - a^{1/d} 3^{-r/d} t 3^m| < c_3 9^{(d-1)m} \tag{4.2.3}$$

holds for infinitely many positive integers m. Note that the left-hand side is a linear combination, with algebraic coefficients, of S-units and an S-integer: namely, it is the value of a homogeneous linear form at the point

$$\mathbf{x} = (9^{md}, 6^{md}, 4^{md}, t3^m) \in \mathcal{O}_S^{*\,3} \times \mathcal{O}_S,$$

where $\mathcal{O}_S = \mathbb{Z}[1/6]$. We now proceed to apply the Subspace Theorem, with $\kappa = \mathbb{Q}$, $N = 4$, S consisting of the archimedean absolute value and the 2-adic and 3-adic ones. Let us define the following linear forms: for the archimedean place, denoted by ∞, put $L_{\infty,1}(X_1, \dots, X_4) = X_1 + \alpha_1 X_2 + \alpha_2 X_3 - a^{1/d} 3^{-r/d} X_4$, then complete to a basis by putting $L_{\infty,i}(X_1, \dots, X_4) = X_i$ for $i = 2, 3, 4$. For each p-adic place ($p = 2, 3$), put $L_{p,i} = X_i$. The double product appearing in the statement of the Subspace Theorem becomes

$$\prod_{i=1}^{4} \prod_{\nu \in \{\infty, 2, 3\}} |L_{i,\nu}(\mathbf{x})|_\nu \leq 9^{-md} \cdot t \cdot c_3 9^{(d-1)m} \leq c_4 3^{-m}.$$

Since the height of the point $\mathbf{x}$ is $\ll 9^{md}$, the Subspace Theorem 2.2.4, applied with any $\epsilon < 1/(2d)$, implies that all but finitely many solutions to the inequality (4.2.3) satisfy finitely many linear dependence relations with integral coefficients. But now, this would yield that a relation like $t = b_1 3^m + b_2 2^{md} 3^{(1-d)m} + b_3 4^{md} 3^{-(2d-1)m}$, for suitable rational numbers b_1, b_2, b_3, would hold infinitely often; this is impossible: by integrality considerations, b_2, b_3 would vanish, and we would have $t = b_1 3^m$; however, an equation like

$$P(2^r 2^{md} + 3^r 3^{md}, 3^{md}) = 0$$

can have only finitely many solutions $m \in \mathbb{N}$.

The case where the rational functions f and g parametrizing the curve $P(X, Y) = 0$ have two poles is similar; details can be found in [14], [60] and [6].

4.3 Hilbert Irreducibility over algebraic groups

In this section, where we give no proofs at all, we shall connect Hilbert irreducibility theory with algebraic groups. Let us start from the original version given by Hilbert himself. Recall that it can be rephrased by saying that given a curve $\mathcal{C}$ and a morphism $\pi : \mathcal{C} \to \mathbb{A}^1$ from the curve to the line, the set $\mathbb{N}$ of natural numbers cannot be contained in the image $\pi(\mathcal{C}(\mathbb{Q}))$ of the rational points on $\mathcal{C}$ (unless the map $\pi : \mathcal{C} \to \mathbb{A}^1$ admits a section).

Now, observe that the line $\mathbb{A}^1$ is the underling algebraic variety of the additive group $\mathbb{G}_a$ and that the set $\mathbb{N}$ of natural numbers is a Zariski-dense sub-semigroup. It is then natural to try to ask the following: *given an algebraic group G defined over a number field κ, a variety V of the same dimension as G and a dominant map $\pi : V \to G$ admitting no section, and given a Zariski-dense sub-semigroup $\Gamma \subset G(\kappa)$, the set Γ cannot be contained in the image $\pi(V(\kappa))$ of the rational points of V.*

Actually, the above statement does not hold, as shown by the simple example below:

Example. Choose $\kappa = \mathbb{Q}$ and $G = V = \mathbb{G}_m$ to be the multiplicative group, and $\pi : \mathbb{G}_m \to \mathbb{G}_m$ be the degree-2 isogeny: $\pi(x) = x^2$. Letting $\Gamma = \{4^n : n \in \mathbb{N}\}$, say, we have that Γ is entirely contained into $\pi(\mathbb{G}_m(\kappa))$.

More generally, whenever V is itself an algebraic group and $\pi : V \to G$ an isogeny, one can construct a counterexample by choosing first a Zariski-dense subgroup in $V(\kappa)$ taking for Γ its image. Starting with the group $\mathbb{G}_a$ this will not be possible, since the latter is simply connected.

It is then natural to ask if such counterexamples are in a sense the only possible ones. In the case of linear algebraic groups, this is the content of the following result, proved in [12]:

Theorem 4.3.1. *Let G be a connected linear algebraic group defined over a number field κ; let V be an algebraic variety with* $\dim V = \dim G$ *and* $\pi : V \dashrightarrow$

G a rational dominant map, all defined over κ. Let $\Gamma \subset G(\kappa)$ be a Zariski-dense sub-semigroup. If $\Gamma \subset \pi(V(\kappa))$ then there exists an algebraic group G', an isogeny $p : G' \to G$ and a rational map $\theta : G' \dashrightarrow V$, all defined over κ, such that $\pi \circ \theta = p$.

Let us see that a particular but significant case is connected with Theorem 4.2.1: consider the case where $G = \mathbb{G}_m^2$ is the two-dimensional torus, Γ is the semigroup generated by the pair $(2,3) \in \mathbb{G}_m^2$; it is Zariski-dense, since the two numbers 2 and 3 are multiplicatively independent. Take any irreducible polynomial $P(X,Y) \in \mathbb{Q}[X,Y]$ of degree ≥ 2 in Y. Then the surface $V \subset \mathbb{G}_m^2 \times \mathbb{A}^1$ defined by the equation $P(X_1+X_2,Y)=0$, provided with the projection $\pi : (X_1,X_2,Y) \mapsto (X_1,X_2)$, gives an example of a ramified covering of $\mathbb{G}_m^2$ admitting no section. Theorem 4.2.1 assures that only finitely many points of Γ have a rational pre-image in V, so in particular $\pi(V(\mathbb{Q}))$ does not contain Γ.

More generally, one can consider Diophantine equations involving linear recurrent sequences. We recall that a linear recurrent sequence is a sequence $u : \mathbb{N} \to \kappa$ which can be expressed in the form

$$u(n) = \sum_{i=1}^{h} p_i(n)\alpha_i^n,$$

where $p_1(T),\ldots,p_h(T)$ are polynomial in $\bar{\kappa}[T]$ and $\alpha_1,\ldots,\alpha_h \in \bar{\kappa}^*$, called *roots* of the recurrence, are non-zero scalars.

Consider the simple-looking Diophantine equation like $u(n) = y^2$, to be solved in $(n,y) \in \mathbb{N} \times \kappa$, which consists in finding perfect squares (in a given number field) in a linear recurrent sequence. We shall show how this equation can be viewed as a problem on integral points on covers of algebraic groups. Namely, let d be the multiplicative rank of the group generated by the roots, which we suppose for simplicity to be torsion-free (we can however always reduce to this case); let $\beta_1,\ldots,\beta_d$ be a basis for this multiplicative group. Put $G = \mathbb{G}_a \times \mathbb{G}_m^d$ and let Γ be the cyclic group generated by $\gamma := (1,\beta_1,\ldots,\beta_d)$. For simplicity, we suppose that each α_i, so each β_i, is κ-rational (so the same holds for the polynomials p_i); in that case Γ consists of κ-rational points of G and the sequence u can be expressed as $u(n) = f(\gamma^n)$, where $f \in \kappa[G]$ is a regular function on G. Now, let $V \subset \mathbb{G}_m^d \times \mathbb{A}^1$ be defined by the equation $Y^2 = f(X_1,\ldots,X_d)$. Projection $\pi : V \to \mathbb{G}_m^2$ onto the X coordinates provides a dominant map without sections, unless the given linear recurrent sequence is identically a square (i.e. a square in the ring of linear recurrent sequences). One can then conjecture finiteness of integral solutions to the original equation, which would follow (via an elementary reasoning) from the degeneracy of integral points on V.

A theorem of Zannier [59] (previously a conjecture of Pisot) proves that the sequence cannot take *always* perfect square values in a given number field, thus proving that the projection $\pi(V(\kappa))$ cannot contain Γ; this is exactly the content of Theorem 4.3.1 in that case. More generally, Ferretti and Zannier [32] proved Theorem 4.3.1 for variety V and map $\pi : V \to \mathbb{G}_a \times \mathbb{G}_m^d$, at least whenever Γ is cyclic. The extension to arbitrary linear algebraic groups, provided in Theorem 4.3.1, is based on that result, and carried out in [12].

As mentioned, at least when G is a torus, and $\pi : V \to G$ is a finite map, admitting ramification (which prevents V to be a torus itself) one could conjecture that in fact $V(\mathcal{O}_S)$ is degenerate. This would follow from Vojta's conjecture, and would e.g. imply the finiteness of the solutions to equations of the form $y^d = 2^a + 3^b + 1$, which we already mentioned (and will be reconsidered again in the next chapter). For $d = 2$ and $\kappa = \mathbb{Q}$, the above equation has been solved completely by Leitner [36], using *ad hoc* methods.

Of course, it is worthwhile to consider also the case of non-linear algebraic groups. Whenever G is a simple abelian variety, and V is an irreducible algebraic variety provided with a dominant morphism $V \to G$, then either V is itself is an abelian variety (which happens if and only if the morphism is unramified), or V is of general type. In the second case its integral (i.e. rational) points should be degenerate. This particular case of Lang-Vojta conjecture, however, is far from being proved at present. A weaker statement, suggested by Serre, is that whenever $G(\kappa)$ is Zariski-dense, $\pi(V(\kappa))$ should not coincide with $G(\kappa)$, or even should be sparse in some sense. Partial results in this direction are the object of the paper [62].