STNB2025
ON SOME RECENT PROGRESS OF THE SCHINZEL HYPOTHESIS OVER POLYNOMIAL RINGS
SUMMARY OF MAIN RESULTS AND SOME APPLICATIONS

ALBERTO F. BOIX AND DANNY A. J. GÓMEZ-RAMÍREZ

1. General outline of the course

In [SS58, page 188], it was formulated the so–called *Schinzel (H) hypothesis*, which can be stated as follows.

Conjecture 1.1. *Let $P_1, \dots, P_s$ be polynomials in $\mathbb{Z}[x]$, all of degree at least one, satisfying the following condition.*

$$\text{There is no prime } p \in \mathbb{Z} \text{ dividing all values } \prod_{i=1}^{s} P_i(m),\ m \in \mathbb{Z}.$$

Then, there are infinitely many integers $m \in \mathbb{Z}$ such that $P_1(m), \dots, P_s(m)$ are prime numbers.

The conjecture is, of course, known in the case $s = 1$ when P_1 is a polynomial of degree one; this is nothing but the classical Dirichlet's theorem on primes in arithmetic progressions. To the best of our knowledge, the case $s > 1$ is completely open.

The goal of these lectures is to explain how Bodin, Debès and Najib have recently proved [BDN20] the Schinzel hypothesis replacing the ring of integers $\mathbb{Z}$ by a polynomial ring $A[x_1, \dots, x_m]$, where A is, roughly speaking, a ring where the classical Hilbert's irreducibility theorem holds.

Lecture one: review of Dirichlet's theorem on primes in arithmetic progressions

The goal of this first lecture is to briefly review, on the one hand, the main steps in the proof of the classical Dirichlet's theorem on primes in arithmetic progressions, and, on the other hand, a serious and less known attempt done by Murty [MT06] to prove this theorem just generalizing in a suitable form Euclid's argument of the infinitude of prime numbers.

Prelude: Dirichlet's Theorem on prime in arithmetic progressions and generalizations. Recall that Dirichlet's Theorem on primes in arithmetic progressions can be stated as follows.

Theorem 1.2 (Dirichlet, 1837)**.** *Given positive integers $a,\ d$ with $\gcd(a, d) = 1$, there are infinitely many primes of the form $a + nd$, where $n \in \mathbb{N}$.*

In other words, there are infinitely many $n \in \mathbb{N}$ such that $f(n) = a + nd$ is a prime number, where $f(X) = a + dX$.

The first serious attempt to generalize Dirichlet's theorem for primes in arithmetic progressions was given by Bunyakovsky. Bunyakovsky's conjecture was motivated by the following result.

Proposition 1.3. *Let $f \in \mathbb{Z}[X]$ be a non–constant polynomial. Consider the sequence*

$$f_\bullet := \{f(n)\}_{n \in \mathbb{Z}}.$$

If $f_\bullet$ contains infinitely many prime values, then the following assertions hold.

(i) $\mathrm{lc}(f) > 0$*, where* $\mathrm{lc}(f)$ *denotes the leading coefficient of f.*

(ii) f is irreducible over $\mathbb{Q}$.

(iii) There is no prime p such that $p \mid f(n)$ for all $n \in \mathbb{N}$.

Conjecture 1.4 (Bunyakovsky, 1857)**.** *If conditions (i), (ii) and (iii) hold in Proposition 1.3, then $f_\bullet$ contains infinitely many prime values.*

Bunyakovsky's conjecture is equivalent to this a priori weaker statement.

Conjecture 1.5 (Bunyakovsky's weak conjecture)**.** *For any non–constant $f \in \mathbb{Z}[X]$ satisfying conditions (i), (ii) and (iii) of Proposition 1.3, $f(n)$ is prime for at least one positive integer n.*

Proof. Assume that Bunyakovsky's weak conjecture holds. Therefore, there is $n \in \mathbb{N}$ such that $f(n)$ is prime. Now, set $q(X) := f(X+n)$. Since f satisfies conditions (i), (ii) and (iii) of Proposition 1.3, $q(X) = f(X+n)$ also satisfies them. Therefore, by Bunyakovsky's weak conjecture applied to q we have that there is $m > n$ such that $f(m)$ is prime. In this fashion, we can construct infinitely many values on which $f(n)$ is prime, as desired. □

50 years later, Dickson generalized Bunyakovsky's conjecture for the case of more than one polynomial.

Conjecture 1.6 (Dickson, 1904)**.** *Given $f_1, \dots, f_m \in \mathbb{Z}[X]$, with $\deg(f_j) = 1$ for all $1 \leq j \leq n$, assume that each f_j satisfies conditions (i), (ii) and (iii) of Proposition 1.3. Assume, in addition, that, for any prime number p, there is some integer n_0 such that p does not divide the product*

$$\prod_{i=1}^{m} f_i(n_0).$$

Then, there are infinitely many positive integers n such that $f_j(n)$ is prime for all $1 \leq j \leq m$.

For this reason, Schinzel hypothesis is sometimes referred as *generalized Dickson's conjecture*.

Looking for an Euclidean's proof of Dirichlet's Theorem. In order to illustrate the headline of this part, we plan to develop first a couple of examples.

Example 1.7. We claim that there are infinitely many prime numbers that are congruent to 1 modulo 4. Indeed, suppose, to reach a contradiction, that there are finitely many ones, namely $p_1, \dots, p_k$, where $k \geq 1$. Consider the polynomial $f(X) = 4x^2 + 1$, and look at the number $N := f(p_1 \cdots p_k)$. By the Fundamental Theorem of Arithmetic, there is a prime number q dividing N. Fix one q prime dividing N. Since $q \mid N$, we have that -1 is a square modulo q. This implies, by Gauss quadratic reciprocity's law, that $q \equiv 1 \pmod 4$.

Summing up, we have two options. Either N is prime, and therefore is congruent to 1 modulo 4, or N is not prime. In both cases, we get a contradiction because $q \notin \{p_1, \dots, p_k\}$. In any case, this gives an infinitude of primes $\equiv 1 \pmod 4$ provided we have at least one. But of course $5 \equiv 1 \pmod 4$, so we are done. Notice that $1^2 \equiv 1 \pmod 4$.

Example 1.8. We claim that there are infinitely many primes that are congruent to 3 modulo 4. In this case, we repeat the same previous argument, but now with the polynomial $g(X) := 4X - 1$. Indeed, assume, to reach a contradiction, that there are finitely many ones, namely $p_1, \dots, p_k$, where $k \geq 1$. Since $N := g(p_1 \cdots p_k)$ is odd, N has only two types of prime factors: primes that are 1 modulo 4, and primes that are 3 modulo 4. Since not all of its prime factors are 1 modulo 4, there is a prime number q dividing N which is 3 modulo 4 and $q \notin \{p_1, \dots, p_k\}$. Again, this gives an infinitude of primes provided there is one, which is of course true because $7 \equiv 3 \pmod 4$.

Notice that $3^2 \equiv 1 \pmod 4$.

So, keeping in mind the above examples, it seems that one way to prove the infinitude of primes in a concrete arithmetic progression is to use Euclid's argument for the infinitude of primes, but choosing first a polynomial which contains these primes, roughly speaking, as divisors.

We formalize this idea by introducing the following classical notion.

Definition 1.9 (Prime divisors of a polynomial)**.** Let $f \in \mathbb{Z}[X]$, and let p be a prime number. We say that p is a *prime divisor of* f if p divides $f(n)$ for some $n \in \mathbb{N}$. In this case, we denote by $P(f)$ the set of prime divisors of the polynomial f.

The following result, obtained by Schur in [Sch12], may be regarded as a generalization of Euclid's argument for the infinitude of prime numbers. A proof can be found for instance in [Hua82, Chapter 5, Theorem 4.2]. See also [MT06, Theorem 2].

Theorem 1.10 (Schur's Theorem)**.** *If $f \in \mathbb{Z}[X]$ is non–constant, then $P(f)$ is an infinite set.*

The next question one might ask is what happens in case we intersect the prime divisors of two polynomials. This is solved by the following theorem by Nagell. The interested reader in a proof may like to consult [Nag69, Theorem 3].

Theorem 1.11 (Nagell)**.** *If $f,\ g \in \mathbb{Z}[X]$ are non–constant polynomials, then $P(f) \cap P(g)$ is infinite.*

Remark 1.12. As pointed out in [MT06], since the prime divisors of the k–th cyclotomic polynomial consists of the prime divisors of k jointly with the primes that are 1 modulo k we have, as consequence of Nagell's Theorem, that for any $k \geq 1$, any polynomial has infinitely many prime divisors that are 1 modulo k.

Keeping in mind Remark 1.12, the following notion seems the best one can expect.

Definition 1.13 (Murty)**.** A *Euclidean proof* for the arithmetic progression $\ell \pmod k$ is the existence of an irreducible polynomial $f \in \mathbb{Z}[X]$ such that all prime divisors of f, except for finitely many ones, are either 1 modulo k or ℓ modulo k.

In this way, the main result obtained by Murty was the following one. It characterizes the arithmetic progressions that admit an Euclidean proof in the above sense.

Theorem 1.14 (Murty)**.** *A Euclidean proof exists for the arithmetic progression $\ell \pmod k$ if and only if $\ell^2 \equiv 1 \pmod k$.*

Lecture two: basics on Hilbertian fields

Hilbert's irreducibility theorem says that if $f \in \mathbb{Q}[T_1, \ldots, T_r, X]$ is an irreducible polynomial, then there are $(a_1, \ldots, a_r) \in \mathbb{Q}^r$ such that $f(a_1, \ldots, a_r, X) \in \mathbb{Q}[x]$ remains irreducible. The goal of this lecture is to formally introduce the so–called *Hilbertian fields*, namely, fields where the above statement is also valid. The main reference for this lecture will be [FJ23, Chapter 13].

What is Hilbert's irreducibility about?

Question 1.15. Let $\mathbb{K}$ be a field, let $\underline{T} = T_1, \ldots, T_r$, $\underline{X} = X_1, \ldots, X_n$, and let $f \in \mathbb{K}[\underline{T}, \underline{X}]$ irreducible. Are there infinitely many values $\underline{t} = t_1, \ldots, t_r$ such that $f(\underline{t}, \underline{X}) \in \mathbb{K}[\underline{X}]$ is irreducible?

One quickly understands that, in order to obtain some positive answers to the above question, some restrictions are needed.

(i) At least, $r \geq 1$. For instance, take $f(T, X) = c \in \mathbb{K}$ a constant polynomial.
(ii) At least, $n \geq 1$. For instance, take $f(T, X) = T^2 + T + 2 \in \mathbb{Z}[T, X]$. For any $t_1 \in \mathbb{Z}$, $f(t_1, X)$ is an even number, so $f(t_1, X) \in \mathbb{Z}[X]$ is reducible.
(iii) Since we want infinite values of the parameters, we need to require that $\mathbb{K}$ is infinite.

Keeping in mind the above restrictions, we are ready to introduce the notion of Hilbertian field.

Definition 1.16. Let $\mathbb{K}$ be a field, let $\underline{X} = X_1, \ldots, X_n$ be variables and $\underline{T} = T_1, \ldots, T_r$ be parameters, ($r \geq 1$ and $n \geq 1$). Let $\underline{f} = (f_1, \ldots, f_m) \in \mathbb{K}(\underline{T})[\underline{X}]^m$ ($m \geq 1$), where $f_j \in \mathbb{K}(\underline{T})[\underline{X}]$ is irreducible for all j, and let $g \in \mathbb{K}[\underline{T}]$.

(i) Set
$$H_{\mathbb{K}}(\underline{f}, g) := \{\underline{a} = (a_1, \dots, a_r) \in \mathbb{K}^r \mid \ g(\underline{a}) \neq 0, \ f_j(\underline{a}, \underline{X}) \text{ irreducible } \forall j\}.$$
We say that $H_{\mathbb{K}}(\underline{f}, g)$ is a *Hilbert subset* of $\mathbb{K}^r$.

If, in addition, $n = 1$, and for any $1 \leq j \leq m$, f_j is separable in X, we say that $H_{\mathbb{K}}(\underline{f}, g)$ is a *separable Hilbert subset* of $\mathbb{K}^r$.

(ii) A *Hilbert set* of $\mathbb{K}$ is a Hilbert subset of $\mathbb{K}^r$ for some $r \geq 1$.

(iii) A *separable Hilbert set* of $\mathbb{K}$ is a separable Hilbert subset of $\mathbb{K}^r$ for some $r \geq 1$.

(iv) We say that $\mathbb{K}$ is *Hilbertian* provided any separable Hilbert set of $\mathbb{K}$ is non–empty.

(v) We say that $\mathbb{K}$ is *strongly Hilbertian* provided any Hilbert set of $\mathbb{K}$ is non–empty.

The first thing we plan to exhibit is a large family of fields that are not Hilbertian; namely, Henselian fields. For more information about Henselian fields, the reader can consult for instance [EP05, Chapter IV].

Proposition 1.17 (Geyer)**.** *No Henselian field is Hilbertian.*

Proof. Let $(\mathbb{K}, v)$ be a Henselian field with valuation ring $(R, \mathfrak{m})$, and choose $0 \neq \lambda \in \mathfrak{m}$, and a prime number $p \neq \text{char}(\mathbb{K})$. Consider the irreducible polynomials in $\mathbb{K}(T)[X]$
$$f(T, X) = X^p + \lambda \cdot T - 1, \ g(T, X) = X^p + \frac{1}{T} - 1.$$
Assume, to reach a contradiction, that $\mathbb{K}$ is Hilbertian. Therefore, there is $0 \neq a \in \mathbb{K}$ such that both $f(a, X)$ and $g(a, X)$ are irreducible as elements of $\mathbb{K}[X]$. In particular, none of them has a zero in $\mathbb{K}$.

However, since $\mathbb{K}$ is a valued field, either $a \in R$ or $1/a \in \mathfrak{m}$. On the one hand, if $a \in R$, then we have that
$$f(a, 1) = \lambda \cdot a \equiv 0 \pmod{\mathfrak{m}}, \ \frac{\partial f}{\partial X}(a, 1) = p \not\equiv 0 \pmod{\mathfrak{m}}.$$
Therefore, since $\mathbb{K}$ is Henselian, we have that $f(a, X)$ has a zero in $\mathbb{K}$, which is a contradiction.

On the other hand, if $a^{-1} \in \mathfrak{m}$, then we have that
$$g(a, 1) = a^{-1} \equiv 0 \pmod{\mathfrak{m}}, \ \frac{\partial g}{\partial X}(a, 1) = p \not\equiv 0 \pmod{\mathfrak{m}}.$$
Therefore, since $\mathbb{K}$ is Henselian, we have that $g(a, X)$ has a zero in $\mathbb{K}$, which is also a contradiction.

In any case, we end up with a contradiction, hence $\mathbb{K}$ can not be Hilbertian. □

Hilbert's irreducibility theorem: main steps in the proof. The main result of this lecture is the following:

Theorem 1.18 (Hilbert's Irreducibility Theorem (HIT))**.** *$\mathbb{Q}$ is Hilbertian.*

Actually, HIT can be deduced from the a priori weaker form of it.

Theorem 1.19 (HIT in one variable)**.** *Let $f \in \mathbb{Q}[T, X]$ irreducible. Then, there are infinitely many rational numbers t_0 such that $f(t_0, X) \in \mathbb{Q}[X]$ is irreducible.*

Actually, this statement can be formulated over the ring of integers, keeping in mind the following version of Gauss Lemma for polynomials. The reader is referred to [VGR18, Lemma 15].

Lemma 1.20 (Gauss polynomial Lemma)**.** *The following assertions hold.*

(i) If a monic polynomial in $\mathbb{Z}[Y]$ factors in $\mathbb{Q}[Y]$, then it factors in $\mathbb{Z}[Y]$.

(ii) A polynomial $\psi(Y)$ divides $f \in \mathbb{Z}[X, Y]$ if and only if, upon writing
$$f(X, Y) = \sum_{j=0}^{n} a_j(Y) X^j,$$
we have that $\psi(Y)$ is a factor of each $a_j(Y)$.

(iii) If $\psi(Y)$ is irreducible and divides $f \cdot g$, where $g \in \mathbb{Z}[X,Y]$ is written as

$$g(X,Y) = \sum_{j=0}^{m} b_j(Y)X^j,$$

then either ψ is a factor of all the a_j's or it is a factor of all the b_j's.

(iv) If $f(X,Y) = g_1(X,Y) \cdot g_2(X,Y)$, where $g_j \in \mathbb{Q}(Y)[X]$, then it can be factored into the product of two polynomials in $\mathbb{Z}[X,Y]$.

In this way, keeping in mind Gauss Lemma, Theorem 1.19 can be deduced from the following:

Proposition 1.21. *Let $f \in \mathbb{Z}[T,X]$, $f \notin \mathbb{Z}[T]$ be irreducible. Then, for an infinite number of $t_1 \in \mathbb{Z}$, $f(t_1,X) \in \mathbb{Z}[X]$ is irreducible.*

One can prove Proposition 1.21 by contrapositive. The formulation is as follows.

Proposition 1.22 (Main Ingredient)**.** *Let $g(T,Y) \in \mathbb{Z}[T,Y]$, $g \notin \mathbb{Z}[T]$. Assume that there is $t_0 \in \mathbb{Z}$ such that, for any $t_1 \geq t_0$, $g(t_1,Y)$ is monic and reducible in $\mathbb{Z}[Y]$. Then, $g \in \mathbb{Q}[T,Y]$ is reducible.*

We plan to show here that Proposition 1.22 implies Proposition 1.21. The argument is as follows.

Proof. First of all, writing

$$f(T,X) = \sum_{j=0}^{n} a_j(T)X^{n-j},$$

set

$$g(T,Y) := a_0(T)^{n-1} f\left(T, \frac{Y}{a_0(T)}\right).$$

Let $t_1 \geq t_0$ be given by Proposition 1.22. Since, by assumption, $f(t_1,X)$ factors in $\mathbb{Z}[X]$, $g(t_1,Y)$ factors in $\mathbb{Q}[Y]$. Since $g(t_1,Y)$ is monic, we can apply part (i) of Gauss polynomial lemma to conclude that $g(t_1,Y)$ also factors in $\mathbb{Z}[Y]$. Therefore, by applying Proposition 1.22, we have

$$g(T,Y) = \Psi_1(T,Y) \cdot \Psi_2(T,Y), \ \Psi_j(T,Y) \in \mathbb{Q}[T,Y].$$

Substituting back $Y = a_0(T) \cdot X$, we obtain

$$f(T,X) = \frac{\Phi_1(T,X) \cdot \Phi_2(T,X)}{A \cdot a_0(T)^{n-1}},$$

where $\Phi_j \in \mathbb{Z}[T,X]$, $A \in \mathbb{Z}$ and $a_0(T) \in \mathbb{Z}[T]$. In this way, the conclusion finally follows by part (iv) of Gauss polynomial Lemma. □

Now, the reader may ask how to prove Proposition 1.22. The whole details can be found in [Lan83, Chapter 9]. Let us just mention two ingredients necessary for the proof. The first one is a Mean value Theorem for more than two points; the statement reads as follows.

Theorem 1.23 (Mean Value Theorem for several points)**.** *Let $\varphi \in \mathcal{C}^m([t_i, t_{i+m}])$, where*

$$t_i < t_{i+1} < \ldots < t_{i+m}$$

are real numbers. Then, there is $t_i < \tau < t_{i+m}$ such that

$$\frac{\varphi^{(m)}(\tau)}{m!} = \frac{\begin{vmatrix} 1 & t_i & t_i^2 & \ldots & t_i^{m-1} & \varphi(t_i) \\ 1 & t_{i+1} & t_{i+1}^2 & \ldots & t_{i+1}^{m-1} & \varphi(t_{i+1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & t_{i+m} & t_{i+m}^2 & \ldots & t_{i+m}^{m-1} & \varphi(t_{i+m}) \end{vmatrix}}{V_m},$$

where V_m is the Vandermonde determinant attached to the points $t_i < t_{i+1} < \ldots < t_{i+m}$.

Building upon this Mean Value Theorem for more than two points, one can prove the following result for Puiseux expansions and density of points, which is the key point to obtain a proof of Hilbert's irreducibility Theorem.

Proposition 1.24 (Puiseux expansions and density of points)**.** *Let*

$$\varphi(t) = at^{n/e} + \ldots + b + \frac{c}{t^{1/e}} + \ldots,$$

where $a, b, c \in \mathbb{R}$*. Assume that:*

(i) φ *converges for all sufficiently large values of* t*.*
(ii) $\varphi \notin \mathbb{R}[t]$*.*
(iii) There are infinitely many positive integers $\{t_i\}_{i\geq 0}$ *such that* $\varphi(t_i) \in \mathbb{Z}$*.*

Then, there is $i_0 \in \mathbb{Z}$*, a natural number* $m \geq 1$ *and a real number* $\lambda \in (0, +\infty)$ *such that, for any* $i > i_0$*, we have*

$$t_{i+m} - t_i > t_i^{\lambda}.$$

Remark 1.25. As we have already explained, a detailed account of the proof of Hilbert's irreducibility theorem is given in [Lan83, Chapter 9], see also [Ser97, Chapter 8]. A different approach, based on Hilbert's original proof, is given in [VGR18].

Lecture three: classic Hilbertian fields and Hilbertian rings

The goal of this lecture is to review the known fact that number fields are Hilbertian. Along the way, we also to see how the Hilbertian property behaves under algebraic field extensions. The main reference for this lecture will also be [FJ23, Chapter 13], where the reader can find full details.

Reduction Lemmata. Our first goal is to explain some basics reduction results involving Hilbert sets.

Lemma 1.26 (First reduction Lemma)**.** *Each Hilbert subset* $H_{\mathbb{K}}(f_1, \ldots, f_m; g) \subset \mathbb{K}^r$ *contains a Hilbert subset of the form* $H_{\mathbb{K}}(f_1', \ldots, f_m'; g') \subset \mathbb{K}^r$*, with, for any* $1 \leq i \leq m$*,* $f_i' \in \mathbb{K}[\underline{T}, \underline{X}]$ *irreducible and* $f_i' \notin \mathbb{K}[\underline{T}]$*.*

The main reason to look at the First reduction lemma is because of the following statement, which roughly says that, in order to prove that a field is either Hilbertian or strongly Hilbertian, it is enough to reduce to the case of one single parameter. The precise statement reads as follows.

Proposition 1.27. *Assume that any Hilbert subset* $H_{\mathbb{K}}(f_1, \ldots, f_m; g) \subset \mathbb{K}$ *with* $f_i \in \mathbb{K}[T, \underline{X}]$ *irreducible, is non–empty. Then, any Hilbert set of* $\mathbb{K}$ *is non–empty.*

Next, we come to the following reduction lemma, which roughly says that one can reduce to one single variable.

Lemma 1.28 (Second Reduction Lemma)**.** *Any Hilbert subset of* $\mathbb{K}$ *contains a Hilbert set of the form* $H_{\mathbb{K}}(f_1, \ldots, f_m; g)$*, with* $f_i \in \mathbb{K}[T, X]$ *and* $\deg_X(f_i) \geq 1$ *for any* $1 \leq i \leq m$*.*

We do not plan to give a full proof of the Second Reduction Lemma, instead we plan to recall a key ingredient in its proof, the so–called *Kronecker substitution*, which may be interesting in its own right.

Definition 1.29. Let R be a unique factorization domain (UFD) with fraction field $\mathbb{K}$, and let $d \geq 1$ be an integer. We consider the map of monoids $\mathbb{N}_0^n \longrightarrow \mathbb{N}_0$ given by multiplication by matrix

$$\begin{pmatrix} 1 & d & d^2 & \ldots & d^{n-1} \end{pmatrix}.$$

As usual, this map of free monoids induces the corresponding map of R–algebras

$$R[\mathbb{N}_0^n] = R[X_1, \dots, X_n] \longrightarrow R[\mathbb{N}_0] = R[Y]$$
$$X_j \longmapsto Y^{d^{j-1}} \quad 1 \leq j \leq n.$$

Now, we restrict this map to the set

$$S_R(n,d) := \{f \in R[X_1, \dots, X_n] : \deg_{X_j}(f) < d \text{ for any } 1 \leq j \leq n\}.$$

This restriction gives rise to the map $S_R(n,d) \xrightarrow{S_d} S_R(1,d^n)$, which we call the *Kronecker substitution*.

Full details and properties of the Kronecker substituion can be found for instance in [FJ23, Chapter 12, §13].

The next reduction lemma says, roughly speaking, that we can remove the polynomial that pops up in a Hilbert set which only involves the parameters. The precise statement reads as follows.

Lemma 1.30 (Third Reduction Lemma)**.** *Let $H := H_{\mathbb{K}}(g_1, \dots, g_m; h) \subset \mathbb{K}^r$ with $g_i \in \mathbb{K}[\underline{T}, X]$, irreducible and $\deg_X(g_i) \geq 1$. Then, H contains a Hilbert set of the form $H_{\mathbb{K}}(f_1, \dots, f_m)$ such that each $f_j \in \mathbb{K}[\underline{T}, X]$ is monic in X, irreducible and $\deg_X(f_i) \geq 2$. In addition, the following assertions hold.*

(i) If $g_1, \dots, g_m$ are separable in X, then so are $f_1, \dots, f_m$.
(ii) If $g_1, \dots, g_m$ are absolutely irreducible in X, then so are $f_1, \dots, f_m$.
(iii) If there is $\underline{a} \in \mathbb{K}^r$ such that $f_i(\underline{a}, X)$ has no root in $\mathbb{K}$ for all i, then $g_i(\underline{a}, X)$ also has no root in $\mathbb{K}$.

The main reason to consider the Third Reduction Lemma is given by the following statement.

Proposition 1.31. *Suppose that any Hilbert subset of the form $H_{\mathbb{K}}(f_1, \dots, f_m)$, with $f_j \in \mathbb{K}[T, X]$ monic in X, and $\deg_X(f_j) \geq 2$ is non–empty. Then, any Hilbert set of $\mathbb{K}$ is non–empty.*

Hilbertian fields and algebraic extensions. *The question we want to tackle now is the following:*

Question 1.32. Let $\mathbb{K} \subset \mathbb{L}$ be an algebraic field extension. Assume that $\mathbb{K}$ is Hilbertian. Under which conditions we can guarantee that $\mathbb{L}$ is Hilbertian?

The first answer is given by the following:

Proposition 1.33 (Hilbertianity and finite separable field extensions)**.** *Let $\mathbb{K} \subset \mathbb{L}$ ba a finite, separable field extension. Then, any separable Hilbert subset of $\mathbb{L}^r$ contains a separable Hilbert subset of $\mathbb{K}^r$. In particular, if $\mathbb{K}$ is Hilbertian, then so is $\mathbb{L}$.*

Actually, Proposition 1.33 is a particular case of the following more general statement.

Theorem 1.34. *Let $\mathbb{K} \subset \mathbb{L}$ be an algebraic field extension with finite separable degree. Then, any separable Hilbert subset of $\mathbb{L}^r$ contains a separable Hilbert subset of $\mathbb{K}^r$. In particular, if $\mathbb{K}$ is Hilbertian, then so is $\mathbb{L}$.*

Relation between Hilbertianity and strong Hilbertianity. Our last goal in this part is to explain the relation between Hilbertian fields and strongly Hilbertian fields. Of course, the two notions coincide when $\mathbb{K}$ is of characteristic zero, so the only difference pops up when $\mathbb{K}$ is of prime characteristic p. Then answer to this question is given by Uchida's Theorem.

Theorem 1.35 (Uchida)**.** *Let $p := \mathrm{char}(\mathbb{K}) > 0$. Then, $\mathbb{K}$ is strongly Hilbertian if and only if it is Hilbertian and $\mathbb{K} \neq \mathbb{K}^p$.*

Sketch of proof. We only plan to show one of the two implications. Indeed, assume that $\mathbb{K}$ is strongly Hilbertian, and let $f(T,X) = X^p - T$. Since $\mathbb{K}$ is strongly Hilbertian, there is $0 \neq a \in \mathbb{K}$ such that $X^p - a$ is irreducible. In particular, a can not be a p–th power of an element of $\mathbb{K}$, hence $\mathbb{K} \neq \mathbb{K}^p$, as claimed. For full details, see [FJ23, 13.4.3]. □

We end up this section by introducing what a Hilbertian ring is.

Definition 1.36 (Hilbertian rings)**.** Let R be an integral domain with fraction field $\mathbb{K}$. We say that R is *Hilbertian* if every separable Hilbert subset of $\mathbb{K}^r$ contains elements all of whose coordinates are in R.

Remark 1.37. Notice that, by definition, any overring of a Hilbertian ring is also Hilbertian.

Lecture four: the Schinzel hypothesis for some polynomial rings

The goal of this lecture is to explain the main steps followed by Bodin, Debès and Najib to prove Schinzel's hypothesis for some polynomial rings.

Some preliminary notations. In what follows, R will always denote a UFD with fraction field $\mathbb{K}$, and let $\underline{f} = f_1, \ldots, f_m \in R[\underline{X}, T]$ be irreducible of degree ≥ 1 in T. Moreover, set

$$\mathrm{Irr}_n(R, \underline{f}) := \{M \in R[\underline{X}] : \ f_j(\underline{X}, M(\underline{X})) \text{ irreducible for all } j\}.$$

On the other hand, given $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$, set

$$\mathrm{Pol}_{R,n,\underline{d}} := \{M \in R[\underline{X}] : \ \deg_{X_i}(M) \leq d_i \text{ for any } 1 \leq i \leq n\}.$$

Finally, we set

$$\mathrm{Irr}_{n,\underline{d}}(R, \underline{f}) := \mathrm{Irr}_n(R, \underline{f}) \cap \mathrm{Pol}_{R,n,\underline{d}}\,.$$

Fields with the product formula. Our plan now is to review fields having a product formula.

Definition 1.38. Let $\mathbb{K}$ be a field, and let $\emptyset \neq S$ be a set of primes $\mathfrak{p}$ of $\mathbb{K}$ with attached absolute values $|\cdot|_{\mathfrak{p}}$. We say that $\mathbb{K}$ *has the product formula with respect to* S if, for any $\mathfrak{p} \in S$, there is a real number $\beta_{\mathfrak{p}} > 0$ such that, for any $0 \leq a \in \mathbb{K}$, $|\{\mathfrak{p} \in S : \ |a|_{\mathfrak{p}} \neq 1\}| < \infty$, and

$$\prod_{\mathfrak{p} \in S} |a|_{\mathfrak{p}}^{\beta_{\mathfrak{p}}} = 1.$$

We say that $\mathbb{K}$ *has a product formula* if there is a non–empty set of primes S satisfying the above conditions.

Our reason to look at fields with the product formula in this context is the following result, proved by Weissauer in his thesis. The interested reader may like to consult either [FJ23, 17.3.3] or [BDN20, Theorem 4.6] for details.

Theorem 1.39 (Weissauer)**.** *Let R be an integral domain such that its quotient field $\mathbb{K}$ has a product formula. Then, R is a Hilbertian ring.*

Main results. Now, we are ready to establish some of the main results concerning the Schinzel hypothesis for polynomials. The first one involves fields with a product formula [BDN20, Theorem 1.1].

Theorem 1.40. *Let R be a UFD such that its quotient field $\mathbb{K}$ satisfies a product formula, and is imperfect if $p = \mathrm{char}(\mathbb{K}) > 0$. Let $\underline{f} = f_1, \ldots, f_m \in R[\underline{X}, T]$ be irreducible of degree ≥ 1 in T. Then, for any $\underline{d} \in \mathbb{N}_0^n$ such that*

$$d_1 + \ldots + d_n \geq \left(\max_{1 \leq i \leq m} \deg_{\underline{X}}(f_i) \right) + 2,$$

we have that $\mathrm{Irr}_{n,\underline{d}}(R, \underline{f})$ is Zariski dense in $\mathrm{Pol}_{R,n,\underline{d}}$.

Actually, more can be said in the field case.

Theorem 1.41. *The set* $\mathrm{Irr}_{n,\underline{d}}(R,\underline{f})$ *is Zariski dense in* $\mathrm{Pol}_{R,n,\underline{d}}$ *for any* $\underline{d}\in\mathbb{N}_0^n$ *if either one of the below assertions hold.*

(i) $R=\mathbb{K}$ *is a strongly Hilbertian field.*
(ii) $R=\mathbb{K}$ *is a Hilbertian field and* $\deg_T(f_j)=1$ *for any* $1\leq j\leq m$.

Bonus lecture: applications

One of the interesting applications obtained by Bodin, Dèbes and Najib as consequence of their results on the Schinzel hypothesis for polynomials is the following polynomial version of the Goldbach's problem, the interested reader may like to consult [BDN20, Corollary 1.5] for details.

Theorem 1.42 (Goldbach's conjecture for polynomials)**.** *Let* R *be a UFD such that its quotient field* $\mathbb{K}$ *satisfies a product formula, and is imperfect if* $p=\mathrm{char}(\mathbb{K})>0$. *Then, every non–constant polynomial* $Q\in R[\underline{X}]$ *is the sum of two irreducible polynomials* $F,G\in R[\underline{X}]$ *with* $F=a+bX_1^{d_1}\cdots X_n^{d_n}$ *(*$a,\ b\in R$*) a binomial of degree* $d_1+\ldots+d_n\leq\deg(Q)$.

Remark 1.43. Unfortunately, the proof of Theorem 1.42 presented in [BDN20] is not constructive, and it does not provide an explicit description of the Goldbach's decomposition. We want to mention here that, in [BGR, Theorem 1.7] we provide an explicit and algorithmic way to express a polynomial in at least two variables over any field as a sum of at most $2r$ absolutely irreducible polynomials, where r is the number of monomials of the polynomial we start with.

Acknowledgments

The contents of these lectures are based on a short course given in the framework of the Barcelona Number Theory Seminar (STNB2025) celebrated in Barcelona from 3 to 7 February of 2025. Both authors want to express the gratitude to the organizers: Francesc Bars, Bernat Plans and Artur Travesa. On the other hand, we also want to thank the feedback received for a large number of participants along the lectures. Danny A. J. Gomez-Ramirez sincerely thanks Sandra Miller for all the sincere support, friendship and support.

Alberto F. Boix received partial support by grant PID2022–137283NB–C22 funded by MICIU/AEI/10.13039/501100011033.

References

[BDN20] A. Bodin, P. Dèbes, and S. Najib. The Schinzel hypothesis for polynomials. *Trans. Amer. Math. Soc.*, 373(12):8339–8364, 2020. 1, 8, 9

[BGR] A. F. Boix and D. A. J. Gómez-Ramírez. On some algebraic and geometric extensions of Goldbach's conjecture. Available at https://arxiv.org/pdf/2312.16524.pdf. 9

[EP05] A. J. Engler and A. Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005. 4

[FJ23] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer, Cham, fourth edition, 2023. 3, 6, 7, 8

[Hua82] L. K. Hua. Introduction to number theory. Transl. from the Chinese by Peter Shiu. Berlin-Heidelberg-New York: Springer-Verlag. xviii, 572 p., 14 figs., 1982. 3

[Lan83] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983. 5, 6

[MT06] M. Ram Murty and N. Thain. Prime numbers in certain arithmetic progressions. *Funct. Approx. Comment. Math.*, 35:249–259, 2006. 1, 3

[Nag69] T. Nagell. Sur les diviseurs premiers des polynômes. *Acta Arith.*, 15:235–244, 1969. 3

[Sch12] I. Schur. Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. Sitzungsber. Berl. Math. Ges. 11, 40-50., 1912. 3

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Edited by Martin Brown and Michle Waldschmidt. With a foreword by Brown and Serre. 6

[SS58] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, 4:185–208; erratum 5 (1958), 259, 1958. 1

[VGR18] M. B. Villarino, W. Gasarch, and K. W. Regan. Hilbert's proof of his irreducibility theorem. *Amer. Math. Monthly*, 125(6):513–530, 2018. 4, 6

Department of Mathematics, Universitat Politècnica de Catalunya BarcelonaTech, Av. Eduard Maristany 16, 08019, Barcelona, Spain.
Email address: alberto.fernandez.boix@upc.edu

Visión Real Cognitiva (Cognivisión) S.A.S. Itaguí, Colombia.
Email address: daj.gomezramirez@gmail.com