Αποφασισιμότητα στην Διαφορική Άλγεβρα

Μαριάνθη Μανιού

Επιβλέπων καθηγητής:
Αθανάσιος Φειδάς

Μεταπτυχιακη εργιασια

Τμημα Μαθηματικων και Εφαρμοσμενων Μαθηματικων
Πανεπιστημιο Κρητης

Ηράκλειο
Δεκέμβριος, 2015

Η παρούσα μεταπτυχιακή εργασία κατατέθηκε στο Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης τον Δεκέμβριο του 2015 στα πλαίσια του μεταπτυχιακού προγράμματος «Μαθηματικά και Εφαρμογές τους» στην κατεύθυνση «Μαθηματικά της Πληροφορικής».

Την επιτροπή αξιολόγησης αποτέλεσαν οι:
Αθανάσιος Φειδάς (επιβλέπων),
Αχιλλέας Τερτίκας,
Xavier Vidaux (Universidad de Concepcion, Chile),
τους οποίους ευχαριστώ για την συμμετοχή τους στην επιτροπή αυτή καθώς και για τη συμβολή τους.

Extended abstract

Summary of Chapter 1 (Introduction)

Our study concerns Decidability in Differential Algebra.

At the beginning we show some proofs of undecidability of theories of various rings and languages. Especially, we prove that the theory of the integer ring $\mathbb{Z}$ in languages with divisibility relations is undecidable. These results are not only interesting by theirselves, but are also useful at the proof of undecidability of polynomial rings, that we also show. These proofs can be found in Chapters 2 and 3.

In the following Chapter we prove the undecidability of the theory of the ring of exponential sums EXP($\mathbb{C}$) (it contains expressions of the form $\sum_{i=1}^{N} \alpha_i e^{\mu_i t}$, where $\alpha_i, \mu_i \in \mathbb{C}, \forall i$) in the language $L = \{+, \cdot, ', 0, 1\}$ ($'$ denotes the derivative in respect to t). We also show similar results for the rings $\mathbb{C}[t]$ (polynomials in the variable t over the complex numbers) and EXP($\mathbb{C}$)[t] (it contains the two above rings).

Then we check the decidability of the rings $\mathbb{C}[t]$ and EXP($\mathbb{C}$)[t] when we consider the above language without the multiplication. We produce some new elimination results for linear differential operators and we set these in the context of existing knowledge. Our new results are those of Chapter 5. (By new we mean that we haven't find it in the existing bibliography.) W e approach to find an elimination of quantifiers in the rings $\mathbb{C}[t]$, EXP($\mathbb{C}$) and EXP($\mathbb{C}$)[t] in the language $L = \{+, ', 0, 1\}$.

Finally we present a possible future application of results of this type; it is Grothendieck's problem for differential equations. The type of application we have in mind is the following: There may exist a language L^{ext}, extending our language L, in which the notions needed to express Grothendieck's problem can be expressed and the theory of EXP($\mathbb{C}$)[t] admits elimination of quantifiers. If the elimination theory over L^{ext} transfers to each ring of power series over a finite field, $F_p[[t]]$, one might be able to transfer theorems between EXP($\mathbb{C}$)[t] to all (or almost all) $F_p[[t]]$. It is then plausible that Grothendieck's question might be among those theorems. Unfortunately, our language L is too poor to express properties, for example it cannot express the property of two functions being linearly independent over the field of constants. Thus our results are only a first step towards the above goal. The corresponding for power series of posiive characteristic. The equivalent for power series of positive characteristic can be found in [PZ04].

Hilbert's tenth problem

Hilbert's tenth problem asks for an algorithm to determine the solvability in integers of diophantine equations over $\mathbb{Z}$, i.e., of polynomials with integer coefficients.
It took seventy years and the work of Martin Davis, Hilary Putnam and Julia Robinson to develop the techniques with which, finally, Yuri Matiyasevich was able to provide a negative answer to Hilbert's tenth problem.
After the proof of Matiyasevich of the unsolvability of Hilbert's tenth problem, it has been asked whether such an algorithm exist if we consider a ring other than the integers.

Positive existential theory

Let S be a structure and L a language.
We define as an existential formula $\alpha(\overline{x})$ a formula of the form

$$\exists y_1 \exists y_2 \ldots \exists y_m \ \phi(\overline{x}, y_1, y_2, \ldots, y_m)$$

where $m \geq 0$ and $\phi(\overline{x}, \overline{y})$ is quantifier-free.
If the formula $\phi(\overline{x}, \overline{y})$ has no negation, then the formula $\alpha(\overline{x})$ is called positive existential.
A (positive) existential sentence is a (positive) existential formula of the form

$$\exists y_1 \exists y_2 \ldots \exists y_m \ \tilde{\phi}(y_1, y_2, \ldots y_m),$$

i.e., a (positive) existential formula without free variables.
A (positive) existential theory of the structure S is the set of (positive) existential sentences that are true in S.
We say that a (positive) existential theory is decidable if there is an algorithm that decides if a given (positive) existential sentence is true in the structure or not - otherwise the theory is undecidable.
The undecidability of a (positive) existential theory T is proved by reducing an other (positive) existential theory T', for which we know that it is undecidable, into T.

Summary of Chapter 2

In this chapter we show that the positive existential theories of $(\mathbb{Z}; +, |_n)$ and $(\mathbb{Z}; +, |, |^p)$ are undecidable. These results are not only interesting by theirselves, but will also be useful in the next chapter to show that Hilbert's tenth problem over polynomial rings is undecidable.

Theorem 1. *Let n be a fixed integer, and $n > 1$. Denote divisibility in $\mathbb{Z}\left[\frac{1}{n}\right]$ by $|_n$, thus for all $x, y \in \mathbb{Z}$*

$$x \mid_n y \leftrightarrow \exists q \in \mathbb{Z}, f \in \mathbb{N} : y = xqn^{-f}.$$

Then the positive existential theory of $(\mathbb{Z}; +, |_n)$ is undecidable, i.e., there is no algorithm to decide formulas of the form

$$\exists x_1, \ldots, \exists x_m \in \mathbb{Z} : \bigwedge_{i=1}^{s} F_i(x_1, \ldots, x_m) \mid_n G_i(x_1, \ldots, x_m)$$

where F_i and G_i are polynomials over $\mathbb{Z}$ of degree one or less.

Idea of proof. *Hilbert's tenth problem is the positive existential theory of $(\mathbb{Z}; +, \cdot)$, thus it is undecidable. To show that the positive existential theory of $(\mathbb{Z}; +, |_n)$ is undecidable, we reduce the positive existential theory of $(\mathbb{Z}; +, \cdot)$ into it. To do that we have to express the relation $z = x \cdot y$ by a positive existential formula in the structure $(\mathbb{Z}; +, |_n)$.*

$$z = x \cdot y \leftrightarrow \exists x_1, \ldots, \exists x_m : \bigwedge_{i=1}^{s} C_i(x_1, \ldots, x_m) \mid_n D_i(x_1, \ldots, x_m),$$

where C_i and D_i are polynomials of degree one or less.

Corollary 1. *Let p be a fixed prime number, $p > 1$. Define the relation $|^p$ by*

$$x \mid^p y \leftrightarrow \exists f \in \mathbb{N} : y = \pm x p^f.$$

Then the positive existential theory of $(\mathbb{Z}; + \mid, \mid^p)$ is undecidable.

Indeed Theorem 1 implies the Corollary since

$$x \mid_p y \leftrightarrow \exists z \in \mathbb{Z} : x \mid z \wedge y \mid^p z$$

Summary of Chapter 3

In this chapter we show Hilbert's tenth problem for polynomial rings $F[t]$ over fields F. In the proof, the characteristic of the ring will be important. We will make a distinction between characteristic other than 2 and characteristic 2. The proofs are based on [Phe94] for rings of characteristic other than 2 and on [Den78b] for rings of characteristic equal to 2.

Polynomial ring of characteristic other than 2

Theorem 2. *If the characteristic of F is other than 2, then $F[t]$ has undecidable positive existential theory in the language $\{+, \cdot, 0, 1, t\}$.*

Idea of proof. *First we prove the undecidability of the positive existential theory of $F[t, t^{-1}]$ when the characteristic of the field F is 0 and when the characteristic is $p > 2$. In the case of characteristic 0 we reduce Hilbert's tenth problem into the positive existential theory of $F[t, t^{-1}]$ and in the case of characteristic $p > 2$ we reduce the positive existential theory of $(\mathbb{Z}; +, \mid, \mid^p)$ into the positive existential theory of $F[t, t^{-1}]$. Having proved the undecidability of the positive existential theory of $F[t, t^{-1}]$ we can reduce it into the positive existential theory of $F[t]$, with $\operatorname{char} F \neq 2$, to prove that the second one is also undecidable.*

Polynomial ring of characteristic 2

Definition 1. *Let F be an integral domain of characteristic $p = 2$. Let $a \in F[t]$ and $a \notin F$. Let $\alpha(a)$ be a root of the equation $x^2 + ax + 1 = 0$. We define two sequences $X_m(a), Y_m(a) \in F[t], m \in \mathbb{Z}$ by*

$$X_m(a) + \alpha(a)Y_m(a) = (\alpha(a))^m = (a + \alpha(a))^{-m}.$$

Theorem 3. *Let F be an integral domain of characteristic $p = 2$. Let $F[t]$ be the ring of polynomials over F in one variable t. Then the positive existential theory of $F[t]$ in the language $\{+, \cdot, 0, 1, t\}$ is undecidable, i.e., there is no algorithm to decide whether or not a polynomial equation with coefficients in $(\mathbb{Z}/2\mathbb{Z})[t]$ has a solution in $F[t]$.*

Idea of proof. *We consider the map $m \mapsto (X_m(t), Y_m(t))$ for $m \in \mathbb{Z}$. With this map we reduce the positive existential theory of $(\mathbb{Z}; +, |, |^2)$, that we have shown to be undecidable, into the positive existential theory of $F[t]$ in the language $\{+, \cdot, 0, 1, t\}$. So we conclude that the latter is also undecidable.*

Summary of Chapter 4

Polynomial ring $\mathbb{C}[t]$

Theorem 4. *$\mathbb{C}[t]$ has undecidable positive existential theory in the language $\{+, \cdot, ', 0, 1, t\}$.*

Idea of proof. *First we show that Hilbert's tenth problem over $\mathbb{Z}$ in the language $L = \{+, \cdot, 0, 1\}$ is equivalent to Hilbert's tenth problem over $\mathbb{N}$ in L. Since the positive existential theory of $\mathbb{Z}$ in L is undecidable, it follows that the positive existential theory of $\mathbb{N}$ in L is undecidable. To show that the positive existential theory of $\mathbb{C}[t]$ is undecidable in the language $\{+, \cdot, ', 0, 1, t\}$, we define the natural numbers in it by an existential formula as follows:*

$$n \in \mathbb{N} \leftrightarrow n' = 0 \ \wedge \ \exists x \ tx' = nx \ \wedge \ \exists y \ (t-1)y = x - 1.$$

Then we can reduce the positive existential theory of $\mathbb{N}$ in the language $\{+, \cdot, 0, 1\}$ into the positive existential theory of $\mathbb{C}[t]$ in the language $\{+, \cdot, ', 0, 1, t\}$. Since the positive existential theory of $(\mathbb{N}; +, \cdot, 0, 1)$ is undecidable, it follows that the positive existential theory of $(\mathbb{C}[t]; +, \cdot, ', 0, 1, t)$ is undecidable.

The rings $\mathrm{EXP}(\mathbb{C})$ and $\mathrm{EXP}(\mathbb{C})[t]$

Let R be any of the rings $\mathrm{EXP}(\mathbb{C})$ and $\mathrm{EXP}(\mathbb{C})[t]$.

Theorem 5. *R has undecidable positive existential theory in the language $\{+, \cdot, ', 0, 1\}$.*

Idea of proof. *To show that the positive existential theory of R is undecidable in the language $\{+, \cdot, ', 0, 1\}$, we define the integers in it by an existential formula as follows:*

$$\lambda \in \mathbb{Z} \leftrightarrow \exists x \exists y \exists h \exists w \exists u \left(x' = x \ \wedge \ y' = \lambda y \ \wedge \ (x-1)h = y - 1 \ \wedge \ xw = 1 \ \wedge \ yu = 1 \right).$$

Then we can reduce the positive existential theory of $\mathbb{Z}$ *in the language* $\{+,\cdot,0,1\}$ *into the positive existential theory of* R *in the language* $\{+,\cdot,',0,1\}$. *Since the positive existential theory of* $(\mathbb{Z};+,\cdot,0,1)$ *is undecidable, it follows that the positive existential theory of* $(R;+,\cdot,',0,1)$ *is undecidable.*

Summary of Chapter 5

In this chapter we will check the decidability of the theory of the rings $\mathbb{C}[t]$ and $\mathrm{EXP}(\mathbb{C})[t]$ if we consider the language without the multiplication, i.e., if we consider the language $L=\{+,',0,1\}$.

The main questions of this chapter are the following:

Question 1. *Is the theory of the polynomial ring* $\mathbb{C}[t]$ *in the language* $\{+,',0,1\}$ *decidable? More precisely, does it admit constructive quantifier elimination?*

Question 2. *Is the theory of the ring of exponential sums and polynomials* $\mathrm{EXP}(\mathbb{C})[t]$ *in the language* $\{+,',0,1\}$ *decidable? More precisely, does it admit constructive quantifier elimination?*

First we check the existence of a solution of linear differential equations in the rings $\mathbb{C}[t]$ and $\mathrm{EXP}(\mathbb{C})[t]$ and we will be referring to the quantifier elimination.

Existence of solution of differential equations

A linear differential equation of degree n with constant coefficients is of the form

$$\mathcal{L}x := \sum_{k=0}^{n} \alpha_k x^{(k)}(t) = f(t)$$

with constants α_k and a function f.
Let x_p be a particular solution, i.e., a solution of the equation $\mathcal{L}x = f(t)$. If $x_p^\star$ is another particular solution, then $x_H = x_p - x_p^\star$ is a solution of the homogeneous equation, $\mathcal{L}x = 0$. Furthermore, for each solution x_H of the homogeneous equation, $x_H + x_p$ is obviously a solution of the initial equation.

We conclude that the set of all the solutions of the initial equation can be found by finding one solution and adding to it the general solution of the homogeneous equation.

Lemma 1. *A differential equation*

$$\alpha_n x^{(n)} + \cdots + \alpha_0 x = f$$

with constant coefficients $\alpha_i \in \mathbb{C}[t], i = 0, \ldots n$ *and* $\alpha_n \neq 0$ *has always a solution in the ring* $\mathbb{C}[t]$ *if* $f \in \mathbb{C}[t] \setminus 0$. *If* $f = 0$ *then the differential equation has a solution if and only if at least one root of the characteristic equation is equal to* 0.

Lemma 2. *A differential equation*

$$\alpha_n x^{(n)} + \cdots + \alpha_0 x = f$$

with constant coefficients $\alpha_i \in EXP(\mathbb{C})[t], i = 0, \ldots n$ *and* $\alpha_n \neq 0$ *has always a solution in the ring* $EXP(\mathbb{C})[t]$ *if* $f \in EXP(\mathbb{C})[t]$.

Quantifier elimination

Definition 2. *Let* T *be a theory in a language* L. T *admits elimination of quantifiers in* L *if and only if every formula* $\phi(\overline{x})$ *of* L *is equivalent in* T *to a quantifier-free* L*-formula* $\psi(\overline{x})$, *i.e., to a finite Boolean combination of atomic formulas.*

Each formula can be written in the form

$$Q_1 x_1 \ldots Q_n x_n \ \phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

where $Q_i \in \{\forall, \exists\}$ and ϕ a quantifier-free formula.
A formula of the form $\forall x \phi$ can be written equivalently as $\neg \exists x \neg \phi$.
We also have that $\exists x(\phi_1 \vee \phi_2) \leftrightarrow \exists x \phi_1 \vee \exists x \phi_2$.
Therefore, a theory T admits quantifier elimination in L if and only if for each formula of the form

$$\exists x \phi(x, \overline{y}),$$

where ϕ is a conjunction of atomic formulas and negations of atomic formulas, exists a T-equivalent quantifier-free formula $\psi(\overline{y})$.

The quantifier elimination can be used as a technique to prove decidability.

We tried to find an elimination of quantifiers in the ring $\mathbb{C}[t]$ and $\mathrm{EXP}(\mathbb{C})[t]$ in the language $L = \{+, ', 0, 1\}$. Our effort isn't complete but we have some results that we present here.
We consider the language $L = \{+, ', 0, 1\}$.

For the quantifier elimination we need the following lemmas:

Lemma 3. *Suppose that $\mathcal{L}_1, \dots \mathcal{L}_n$ are non-zero differential operators and $f_1, \dots, f_n$ terms of L. Then in each of the ring $\mathbb{C}[t]$ and $\mathrm{EXP}(\mathbb{C})[t]$ we have the following equivalence:*

$$\bigwedge_{i=1}^{n} \mathcal{L}_i x = f_i$$
$$\Longleftrightarrow$$
$$\mathcal{L}x = h \wedge \phi_0$$

We show the above equivalence by the following example:

Let $D_j\mathcal{L}_i$ be the jth derivative of $\mathcal{L}_i x$.

$$\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - 4x + 2t = 0$$

$$\begin{aligned}
&\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - 4x + 2t = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x := D_1\mathcal{L}_1 x - \mathcal{L}_2 x = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = (x'' + 2x') - (x'' - 4x + 2t) = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = 2x' + 4x - 2t = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = x' + 2x - t = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x := D_0\mathcal{L}_1 x - \overline{\mathcal{L}}_2 x = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = (x' + 2x + 1) - (x' + 2x - t) = 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = t + 1 = 0
\end{aligned}$$

So we end up with a formula with only one differential equation and a formula that doesn't contain the variable x.

Lemma 4. *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be non-zero linear differential operators and f and g terms of L. In each of the rings $\mathbb{C}[t]$ and $EXP(\mathbb{C})[t]$ we consider the formula*

$$\sigma(x) : \ \mathcal{L}_1 x = f \wedge \mathcal{L}_2 x \neq g$$

The formula $\sigma(x)$ is equivalent to a formula of one of the following forms

1. $$\mathcal{L}_1 x = f \wedge \mathcal{L}x \neq h$$

   where h is a term of L and $\mathcal{L}$ is an operator with order smaller than the order of $\mathcal{L}_1$.

2.

$$\mathcal{L}_1 x = f \wedge \phi_0$$

where ϕ_0 is a quantifier-free formula that doesn't contain the variable x.

We show these equivalences by the following examples:

Let $D_j\mathcal{L}_i$ be the jth derivative of $\mathcal{L}_i x$.
Example 1.

$$\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - x' + 9 \neq 0$$

$$\begin{aligned}
&\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - x' + 9 \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x := D_1\mathcal{L}_1 x - \mathcal{L}_2 x \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = (x'' + 2x') - (x'' - x' + 9) \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = 3x' - 9 \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = x' - 3 \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x := D_0\mathcal{L}_1 x - \overline{\mathcal{L}}_2 x \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = (x' + 2x + 1) - (x' - 3) \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = 2x + 4 \neq 0
\end{aligned}$$

So we end up with a formula at which the order of the differential inequation is smaller than that of the differential equation.

Example 2.

$$\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - 4x + 2t \neq 0$$

$$\begin{aligned}
&\mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \mathcal{L}_2 x = x'' - 4x + 2t \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x := D_1\mathcal{L}_1 x - \mathcal{L}_2 x \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = (x'' + 2x') - (x'' - 4x + 2t) \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = 2x' + 4x - 2t \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \overline{\mathcal{L}}_2 x = x' + 2x - t \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x := D_0\mathcal{L}_1 x - \overline{\mathcal{L}}_2 x \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = (x' + 2x + 1) - (x' + 2x - t) \neq 0 \\
&\quad \Leftrightarrow \mathcal{L}_1 x = x' + 2x + 1 = 0 \ \wedge \ \hat{\mathcal{L}}_2 x = t + 1 \neq 0
\end{aligned}$$

So we end up with one differential equation and a quantifier-free formula that doesn't contain any x.

Lemma 5. *Let R be one of the rings $\mathbb{C}[t]$ or $EXP(\mathbb{C})[t]$. Let $\mathcal{L}$ and $\mathcal{L}_1 \dots \mathcal{L}_n$ be non-zero differential operators and $x_1, \dots x_n$ variables. We suppose that the order of each $\mathcal{L}_i$ is smaller that the order of $\mathcal{L}$. We consider the formula*

$$\theta \ : \ \bigwedge_{i=1}^{n} \mathcal{L}(x) = \mathcal{L}(x_i) \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq \mathcal{L}_i(x_i) \ .$$

If the system $\mathcal{L}x = 0 \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq 0$ has non-zero solutions in R, then the formula $\exists x \ \theta$ is equivalent to $0 = 0$. Otherwise, it is equivalent to $0 = 1$.

Elimination of existential quantifier for formulas with no or one inequation

In each of the rings $\mathbb{C}[t]$ and $EXP(\mathbb{C})[t]$, if we can eliminate the existential quantifier from any formula of the form

$$\exists x \ \phi(x) : \exists x \ \left(\bigwedge_{j=1}^{m} \tilde{\mathcal{L}}_j x = f_j \ \wedge \ \bigwedge_{j=1}^{n} \mathcal{L}_j x \neq g_j \ \wedge \ \phi_0 \right) \ ,$$

where in the quantifier-free formula ϕ_0 the variable x is not appeared, then we have shown that the theory of the ring in the language L admits quantifier elimination.

We have a method to achieve this elimination if the number of inequations is 0 or 1.

We consider a system of one equation and one inequation.

$$\exists x \ \phi(x) : \exists x \ \left(\mathcal{L}x = f \ \wedge \ \mathcal{L}_1 x \neq g_1 \right) . \tag{0.1}$$

From the Lemma 4 we can assume, without loss of generality, that the order of $\mathcal{L}_1$ is smaller than the order of $\mathcal{L}$

The above formula can be written equivalently as

$$\begin{array}{c} \neg \left(\exists y\right) \left(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1 \right) \ \wedge \ \left(\exists x\right) \left(\mathcal{L}x = f \right) \\ \vee \\ \left(\exists y\right) \left[\left(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1 \right) \ \wedge \ \left(\exists x\right) \left(\mathcal{L}x = f \ \wedge \ \mathcal{L}_1 x \neq g_1 \right) \right] . \end{array} \tag{0.2}$$

We consider the formula

$$\neg \left(\exists y\right) \left(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1 \right) \ \wedge \ \left(\exists x\right) \left(\mathcal{L}x = f \right) \tag{0.3}$$

The formula $\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1$, according to the Lemma 3a is equivalent to a formula of the form $\tilde{\mathcal{L}}y = h \ \wedge \ \tilde{\phi}_0$. So we get the equivalent formula

$$\neg\,(\exists y)\left(\tilde{\mathcal{L}}y = h \ \wedge \ \tilde{\phi}_0\right) \ \wedge \ (\exists x)\,(\mathcal{L}x = f)\,.$$

We consider the formula

$$(\exists y)\left[\,(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1) \ \wedge \ (\exists x)\,(\mathcal{L}x = f \ \wedge \ \mathcal{L}_1 x \neq g_1)\,\right] \tag{0.4}$$

which is equivalent to the formula

$$(\exists y)\left[\,(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1) \ \wedge \ (\exists x)\,(\mathcal{L}x = \mathcal{L}y \ \wedge \ \mathcal{L}_1 x \neq \mathcal{L}_1 y)\,\right].$$

According to the Lemma 5 the formula $(\exists x)\,(\mathcal{L}x = \mathcal{L}y \ \wedge \ \mathcal{L}_1 x \neq \mathcal{L}_1 y)$ is equivalent to $0 = 0$ if the system $\mathcal{L}x = 0 \wedge \mathcal{L}_1 x \neq 0$ has non-zero solutions in the ring. Otherwise, it is equivalent to $0 = 1$.
If the formula is equivalent to $0 = 1$, then the formula (0.4) is also equivalent to $0 = 1$. Otherwise, the formula (0.4) is equivalent to $(\exists y)\,(\mathcal{L}y = f \ \wedge \ \mathcal{L}_1 y = g_1)$. According to the Lemma 3b this formula is equivalent to one equation and a quantifier-free formula $\overline{\phi}_0$, i.e., it is equivalent to $(\exists y_j)(\tilde{\mathcal{L}}_j y_j = h \ \wedge \ \overline{\phi}_0)$.

Therefore, in each case we end up with formulas of the form $(\exists z)(\hat{\mathcal{L}}z = \hat{w})$.
If $w \neq 0$ then this formula is equivalent to $0 = 0$ in the rings $\mathbb{C}[t]$ and $EXP(\mathbb{C})[t]$.
If $w = 0$ then this formula is equivalent to $0 = 0$ in the ring $EXP(\mathbb{C})[t]$ and to $\mathcal{L}(1) = 0$ in the ring $\mathbb{C}[t]$.
That means that in each case the formula $(\exists z)(\hat{\mathcal{L}}z = \hat{w})$ is equivalent to a quantifier-free formula.

The negation of a quantifier-free formula remains quantifier-free.

So there exists an equivalent quantifier-free formula for each of the formulas (0.3) and (0.4).

Thus the formula (0.2) is equivalent to the conjunction of quantifier-free formulas, so also the formula (0.1).

Summary of Chapter 6

In this chapter we present Grothendieck's problem.
We denote by K an algebraic number field. For a prime ideal $\mathfrak{p}$ of K, $\overline{K}_{\mathfrak{p}}(x)$ denotes the residue field.
We consider the differential equation:

$$\alpha_0(x)y^{(n)} + \alpha_1(x)y^{(n-1)} + \cdots + \alpha_n(x)y = 0 \tag{1}$$

where $\alpha_i(x) \in K[x], 0 \leq i \leq n$.

Grothendieck's problem. *If, for almost all prime ideals* $\mathfrak{p}$*,* $(1)_{\mathfrak{p}}$ *has* n *solutions in* $\overline{K}_{\mathfrak{p}}(x)$ *which are independent over* $\overline{K}_{\mathfrak{p}}(x^p)$*, are all solutions of* (1) *algebraic functions.*

We present also its proof for first order differential equations, based on [Hon81]. For differential equations of order $n > 1$, it is an open problem.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Το αντικείμενο της εργασίας είναι η Αποφασισιμότητα στην Διαφορική Άλγεβρα.

Αρχικά παρουσιάζουμε αποδείξεις μη αποφασισιμότητας κάποιων θεωριών. Συγκεκριμένα, αποδεικνύουμε ότι η θεωρία του δακτυλίου $\mathbb{Z}$ σε γλώσσες, οι οποίες περιλαμβάνουν σχέσεις διαιρετότητας είναι μη αποφασίσιμη. Τα αποτελέσματα αυτά δεν είναι μόνο ενδιαφέροντα από μόνα τους, αλλά είναι επίσης χρήσιμα στην απόδειξη της μη αποφασισιμότητας των πολυωνυμικών δακτυλίων, την οποία επίσης παρουσιάζουμε. Οι αποδείξεις αυτές βρίσκονται στα Κεφάλαια 2 και 3.

Στο ακόλουθο Κεφάλαιο αποδεικνύουμε την μη αποφασισιμότητα της θεωρίας του δακτυλίου των εκθετικών αθροισμάτων $\mathrm{EXP}(\mathbb{C})$ (περιέχει εκφράσεις της μορφής $\sum_{i=1}^{N} \alpha_i e^{\mu_i t}$, όπου $\alpha_i, \mu_i \in \mathbb{C}, \forall i$) στη γλώσσα $L = \{+, \cdot, ', 0, 1\}$ (το $'$ συμβολίζει την παράγωγο ως προς t). Δείχουμε επίσης ανάλογα αποτελέσματα για τους δακτυλίους $\mathbb{C}[t]$ (πολυώνυμα μιας μεταβλητής t επί των μιγαδικών αριθμών) και $\mathrm{EXP}(\mathbb{C})[t]$ (περιέχει τους δύο παραπάνω δακτυλίους).

Στη συνέχεια, ελέγχουμε την αποφασισιμότητα των δακτυλίων $\mathbb{C}[t]$ και $\mathrm{EXP}(\mathbb{C})[t]$ αν θεωρήσουμε την παραπάνω γλώσσα χωρίς τον πολλαπλασιασμό. Παρουσιάζουμε κάποια νέα αποτελέσματα απαλοιφής για διαφορικούς τελεστές στο Κεφάλαιο 5. (Νέα με την έννοια ότι δεν μπορέσαμε να τα ανακαλύψουμε στην υπάρχουσα βιβλιογραφία.) Έγινε μία προσπάθεια για την δημιουργία απαλοιφής ποσοδεικτών στους δακτυλίους $\mathbb{C}[t]$και $\mathrm{EXP}(\mathbb{C})[t]$ στη γλώσσα $L = \{+, ', 0, 1\}$ επιδέχονται απαλοιφή ποσοδεικτών.

Τέλος παρουσιάζουμε μια πιθανή εφαρμογή τέτοιων αποτελεσμάτων, το πρόβλημα του Grothendieck για διαφορικές εξισώσεις. Η μορφή της εφαρμογής είναι η εξής: Είναι δυνατόν να υπάρχει μια γλώσσα L^{ext}, μια επέκταση της γλώσσας L, στην οποία οι έννοιες που χρειάζονται να εκφράσουμε το πρόβλημα του Grothendieck μπορούν να εκφραστούν και η θεωρία του $\mathrm{EXP}(\mathbb{C})[t]$ επιδέχεται απαλοιφή ποσοδεικτών. Αν η θεωρία απαλοιφής επί της L^{ext} μεταβιβάζεται σε κάθε δακτύλιο δυναμοσειρών επί ενός πεπερασμένου σώματος, $F_p[[t]]$, θα μπορούσαμε να μεταβιβάσουμε τα θεωρήματα του $\mathrm{EXP}(\mathbb{C})[t]$ σε κάθε (ή σχεδόν κάθε) $F_p[[t]]$. Τότε ίσως το Grothendieck να είναι ένα από αυτά τα Θεωρήματα. Δυστυχώς, με

την γλώσσα L δεν μπορούμε να εκφράσουμε ιδιότητες όπως για παράδειγμα την ιδιότητα ότι δύο συναρτήσεις είναι γραμμικά ανεξάρτητς επί του σώματος των σταθερών. Οπότε τα αποτελέσματά μας είναι απλώς ένα πρώτο βήμα προς αυτό το στόχο. Το αντίστοιχο για δυναμοσειρές με θετική χαρακτηριστική έχει γίνει, [PZ04].

1.1 10^o πρόβλημα του Hilbert

Το 10^o πρόβλημα του David Hilbert ήταν το 10^o σε μια λίστα 23 προβλημάτων που έθεσε ο Hilbert στο Παγκόσμιο συνέδριο Μαθηματικών το 1900. Η αρχική του διατύπωση είναι η εξής:

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.
Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Δηλαδή ζητούσε να κατασκευαστεί ένας αλγόριθμος ο οποίος, με είσοδο ένα πολυώνυμο $P(x_1, \ldots, x_n)$ με ακέραιους συντελεστές, αποφασίζει πάντα αν η εξίσωση $P(x_1, \ldots, x_n) = 0$ έχει ακέραια λύση.
Αρκετά αργότερα, το 1970, ο Yuri Matiyasevich βασιζόμενος σε εργασίες των Martin Davis, Hilary Putnam, και Julia Robinson, έλυσε το 10^o πρόβλημα του Hilbert, δίνοντας μια αρνητική απάντηση. Αποδείχθηκε δηλαδή ότι δεν υπάρχει τέτοιος αλγόριθμος.
Μία πληρέστερη αναφορά υπάρχει στο [Mat70] και στο [Dav73] υπάρχουν πληροφορίες για επόμενες εξελίξεις.
Μετά την απόδειξη του Matiyasevich της μη επιλυσιμότητας του $10^{ου}$ προβλήματος του Hilbert, έχει ερωτηθεί αν υπάρχει τέτοιος αλγόριθμος αν αντί τους ακεραίους θεωρήσουμε κάποιον άλλο δακτύλιο. Για παράδειγμα, μπορούμε να θεωρήσουμε εξισώσεις με μιγαδικούς συντελεστές και να εξετάσουμε αν έχουν λύση στο $\mathbb{C}$. Αφού το $\mathbb{C}$ είναι αλγεβρικά κλειστό, κάθε εξίσωση βαθμού τουλάχιστον 1 έχει λύση. Όπως θα δείξουμε παρακάτω, δεν υπάρχει αλγόριθμος που αποφασίζει την επιλυσιμότητα των εξισώσεων με συντελεστές σε ένα σώμα F στον πολυωνυμικό δακτύλιο. Υπάρχουν επίσης αρκετά ανοιχτά προβλήματα. Για παράδειγμα, η απάντηση στο 10^o πρόβλημα του Hilbert δεν είναι γνωστή αν οι λύσεις πρέπει να είναι ρητές και όχι ακέραιες.

1.2 Θετική υπαρξιακή θεωρία

Έστω S μια δομή, για παράδειγμα ένας δακτύλιος, και L μια γλώσσα, ένα σύνολο από σταθερές, σύμβολα συναρτήσεων και σύμβολα σχέσεων.

Ορισμός 1.1. *Ένας υπαρξιακός τύπος (existential formula) $\alpha(\overline{x})$ είναι ένας τύπος της μορφής*

$$\exists y_1 \exists y_2 \ldots \exists y_m \ \phi(\overline{x}, y_1, y_2, \ldots, y_m)$$

όπου $m \geq 0$ και $\phi(\overline{x}, \overline{y})$ ένας τύπος ελεύθερος ποσοδεικτών, δηλαδή δεν περιέχει τους ποσοδείκτες $\exists$ και $\forall$.
Αν ο τύπος $\phi(\overline{x}, \overline{y})$ δεν περιέχει άρνηση, τότε ο τύπος $\alpha(\overline{x})$ ονομάζεται θετικός υπαρξιακός (positive existential).

Ορισμός 1.2. *Μια (θετική) υπαρξιακή πρόταση είναι ένας (θετικός) υπαρξιακός τύπος της μορφής*

$$\exists y_1 \exists y_2 \ldots \exists y_m \ \tilde{\phi}(y_1, y_2, \ldots y_m),$$

δηλαδή είναι ένας (θετικός) υπαρξιακός τύπος χωρίς μεταβλητες ελεύθερες ποσοδεικτών.

Ορισμός 1.3. *Μια (θετική) υπαρξιακή θεωρία μιας δομής S είναι το σύνολο των (θετικών) υπαρξιακών προτάσεων που είναι αληθής στην S.*

Οι (θετικοί) υπαρξιακοί τύποι είναι κλειστοί ως προς την ένωση ($\vee$) και την τομή ($\wedge$).

$$(\exists x \ \phi(t,x)) \vee (\exists y \ \psi(u,y)) \leftrightarrow \exists x \exists y \ (\phi(t,x) \vee \psi(u,y))$$
$$(\exists x \ \phi(t,x)) \wedge (\exists y \ \psi(u,y)) \leftrightarrow \exists x \exists y \ (\phi(t,x) \wedge \psi(u,y))$$

Το ίδιο ισχύει και για (θετικές) υπαρξιακές προτάσεις οπότε και για (θετικές) υπαρξιακές θεωρίες.

Ορισμός 1.4. *Μια (θετική) υπαρξιακή θεωρία είναι αποφασίσιμη αν υπάρχει αλγόριθμος ο οποίος θα αποφασίζει, μετά από πεπερασμένο αριθμό βημάτων, αν μια δεδομένη (θετική) υπαρξιακή πρόταση είναι αληθής στη δομή ή όχι-διαφορετικά η θεωρία είναι μη αποφασίσιμη.*

Η μη αποφασισιμότητα μιας (θετικής) υπαρξιακής θεωρίας T αποδεικνύεται συνήθως ανάγοντας μια άλλη (θετική) υπαρξιακή θεωρία T', για την οποία γνωρίζουμε ότι είναι μη αποφασίσιμη, στην T ως εξής:

- Υποθέτουμε ότι η T είναι αποφασίσιμη.
- Μεταφράζουμε το σύνολο της T' στην (θετική) υπαρξιακή θεωρία της T, δηλαδή βρίσκουμε έναν αλγόριθμο ο οποίος, δεδομένης μιας (θετικής) υπαρξιακής πρότασης ϕ της T', παράγει μια (θετική) υπαρξιακή πρόταση ψ της T έτσι ώστε η ϕ είναι αληθής στην T' αν και μόνο αν η ψ είναι αληθής στην T.
- Εφ'όσον η (θετική) υπαρξιακή θεωρία T' είναι μη αποφασίσιμη, δηλαδή δεν υπάρχει αλγόριθμος ο οποίος απαντάει σε (θετικές) υπαρξιακές ερωτήσεις στην T', καταλήγουμε σε άτοπο.

ΚΕΦΑΛΑΙΟ 2

Θετική υπαρξιακή θεωρία των $(\mathbb{Z}; +, |_n)$ και $(\mathbb{Z}; +, |, |^p)$

Στο κεφάλαιο αυτό θα δείξουμε ότι οι θετικές υπαρξιακές θεωρίες των $(\mathbb{Z}; +, |_n)$ και $(\mathbb{Z}; +, |, |^p)$ είναι μη αποφασίσιμες.
Τα αποτελέσματα αυτά δεν είναι μόνο ενδιαφέροντα από μόνα τους, αλλά θα είναι επίσης χρήσιμα στο επόμενο κεφάλαιο για να δείξουμε ότι το 10^o πρόβλημα του Hilbert επί των πολυωνυμικών δακτυλίων είναι μη αποφασίσιμο.

Ορισμός 2.1. *Με $|_n$ συμβολίζουμε την διαιρετότητα στο $\mathbb{Z}\left[\frac{1}{n}\right]$, οπότε για κάθε $x, y \in \mathbb{Z}$ έχουμε*

$$x \mid_n y \leftrightarrow \exists q \in \mathbb{Z}, f \in \mathbb{N} : y = xqn^{-f}.$$

Παρατήρηση 2.1. *Αν $(x, n) = 1$, τότε $x \mid_n y \leftrightarrow x \mid y$.*

Ορισμός 2.2. *Έστω p ένας πρώτος αριθμός, $p > 1$. Ορίζουμε την σχέση $|^p$ ως εξής*

$$x \mid^p y \leftrightarrow \exists f \in \mathbb{N} : y = \pm xp^f.$$

Θεώρημα 2.1. *Έστω n ένας ακέραιος, και $n > 1$. Τότε η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση και την σχέση $|_n$ είναι μη αποφασίσιμη, δηλαδή δεν υπάρχει αλγόριθμος ο οποίος αποφασίζει κατά πόσον ισχύουν οι τύποι της μορφής*

$$\exists x_1, \ldots, \exists x_m \in \mathbb{Z} : \bigwedge_{i=1}^{s} F_i(x_1, \ldots, x_m) \mid_n G_i(x_1, \ldots, x_m)$$

όπου F_i και G_i είναι πολυώνυμα πάνω από το $\mathbb{Z}$ βαθμού το πολύ 1.

Πόρισμα 2.1. *Έστω p ένας πρώτος αριθμός, $p > 1$. Τότε η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $|^p$ είναι μη αποφασίσιμη.*

Απόδειξη. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $|^p$ είναι αποφασίσιμη, δηλαδή ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $(\mathbb{Z}; +, |, |^p)$.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση και την σχέση $|_n$ στην θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρτότητα και την σχέση $|^p$.
Η απεικόνιση της αναγωγής είναι $n \mapsto n$.
Τότε το $+$ αντιστοιχεί στο $+$.
Επίσης έχουμε ότι

$$\begin{aligned} x \mid_p y &\leftrightarrow \exists q, f \in \mathbb{Z} : yp^f = xq \\ &\leftrightarrow \exists f \in \mathbb{Z} : x \mid yp^f \\ &\leftrightarrow \exists z, f \in \mathbb{Z} : x \mid z \quad \wedge \quad z = \pm yp^f \\ &\leftrightarrow \exists z \in \mathbb{Z} : x \mid z \quad \wedge \quad y \mid^p z. \end{aligned}$$

Οπότε μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, |, |^p)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, |_n)$.
Εφ'όσον όμως η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση και την σχέση $|_n$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $|^p$ είναι μη αποφασίσιμη. □

Στο υπόλοιπο του κεφαλαίου θα αποδείξουμε το Θεώρημα 2.1. Θα ανάγουμε την υπαρξιακή θεωρία του $(\mathbb{Z}; +, \cdot)$ στην θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, |_n)$ μέσω της απεικόνισης $n \mapsto n$.

Ορισμός 2.3. *Έστω $n, x, y \in \mathbb{Z}$ με $n > 1$. Για κάθε πρώτο αριθμό p, ορίζουμε το $h(p)$ ως εξής*

$$h(p) = \begin{cases} 0 & \text{αν } v_p(ny) = v_p(x) \\ 1 & \text{διαφορετικά .} \end{cases}$$

Λήμμα 2.1. *Έστω $h \equiv h(p) \pmod p$ και $i > 0$. Αν $p^i \mid ny - hx$, τότε $p^i \mid x$.*

Απόδειξη. Αν $h(p) = 0$ τότε $p \mid h$ και $v_p(x) = v_p(ny)$. Τότε $v_p(hx) > v_p(ny)$. Εφόσον $p^i \mid ny - hx$ έχουμε ότι $i \leq v_p(ny - hx) = \min\{v_p(ny), v_p(hx)\} = v_p(ny) = v_p(x)$. Άρα, $p^i \mid x$.

Αν $h(p) = 1$ τότε $p \nmid h$ και $v_p(x) \neq v_p(ny)$. Τότε $v_p(hx) = v_p(x)$. Εφ'όσον $p^i \mid ny - hx$ έχουμε ότι $i \leq v_p(ny - hx) = \min\{v_p(ny), v_p(hx)\} = \min\{v_p(ny), v_p(x)\} \leq v_p(x)$. Άρα, $p^i \mid x$. □

Λήμμα 2.2. *Έστω $n > 1$. Υποθέτουμε ότι οι ακέραιοι x και y ικανοποιούν τις σχέσεις $x \mid_n 1$ και $y \mid_n 1$. Τότε $y = x^2$ αν και μόνο αν ισχύουν οι παρακάτω συνθήκες:*

$$2nx + 1 \mid_n 4n^2y - 1 \tag{2.1}$$

$$2nx - 1 \mid_n 4n^2y - 1 \tag{2.2}$$

$$ny - kx \mid_n nx - k, \text{ για κάθε } k \text{ με } |k| < n \tag{2.3}$$

Απόδειξη. Έστω $y = x^2$. Τότε $4n^2y - 1 = 4n^2x^2 - 1 = (2nx - 1)(2nx + 1)$. Οπότε $2nx - 1 \mid 4n^2y - 1$ και $2nx + 1 \mid 4n^2y - 1$. Εφ'όσον $(2nx \pm 1, n) = 1$, από την Παρατήρηση 2.1 έχουμε ότι $2nx - 1 \mid_n 4n^2y - 1$ και $2nx + 1 \mid_n 4n^2y - 1$.
Επίσης έχουμε ότι $ny - kx = nx^2 - kx = x(nx - k)$. Από την σχέση $x \mid_n 1$ έχουμε ότι $xq = n^f$. Άρα,

$$q(ny - kx) = xq(nx - k) \Rightarrow q(ny - kx) = n^f(nx - k) \Rightarrow nx - k = q(ny - kx)n^{-f}$$
$$\Rightarrow ny - kx \mid_n nx - k.$$

Αντίστροφα, υποθέτουμε ότι ισχύουν οι σχέσεις (2.1), (2.2), (2.3). Εφ'όσον $(2nx \pm 1, n) = 1$, από τις σχέσεις (2.1) και (2.2) έχουμε ότι $2nx+1 \mid 4n^2y-1$ και $2nx-1 \mid 4n^2y-1$. Άρα, αφού $(2nx + 1, 2nx - 1) = 1$, έχουμε ότι $(2nx + 1)(2nx - 1) \mid 4n^2y - 1$. Εφ'όσον $4n^2y - 1 \neq 0$, έχουμε ότι

$$|(2nx + 1)(2nx - 1)| \leq |4n^2y - 1|$$

Άρα,

$$\begin{aligned} 4n^2x^2 - 1 &= (2nx + 1)(2nx - 1) \\ &\leq |(2nx + 1)(2nx - 1)| \\ &\leq |4n^2y - 1| \\ &\leq 4n^2|y| + 1. \end{aligned}$$

Οπότε,

$$4n^2x^2 \leq 4n^2|y| + 2 \Rightarrow x^2 \leq |y| + \frac{1}{2n^2}.$$

Εφ'όσον οι x και y είναι ακέραιοι, ισχύει $x^2 \leq |y|$.
Έστω $n = q_1^{a_1} \cdots q_k^{a_k}$ η παραγοντοποίηση του n.
Από το Κινέζικο Θεώρημα Υπολοίπων, υπάρχει $h \pmod n$ έτσι ώστε $h \equiv h(q_j) \pmod q_j$, για κάθε πρώτο $q_j \in \{q_1, \ldots, q_k\}$.
Διαλέγουμε το h έτσι ώστε $|h| < n$ και $hx \geq 0$. Οπότε, από την σχέση (2.3) έχουμε ότι $ny - h \mid_n nx - h$, οπότε υπάρχουν $q, f \in \mathbb{Z}$ έτσι ώστε

$$(ny - hx)q = (nx - h)n^f. \tag{2.4}$$

Έστω i_j έτσι ώστε $q_j^{i_j} \mid ny - hx$ με $0 \leq i_j \leq a_j, \forall j \in \{1, \ldots, k\}$ και $q_j \in \{q_1, \ldots, q_k\}$.

Τότε

$$q_1^{i_1}\cdots q_k^{i_k} \mid ny-hx$$
$$\Leftrightarrow$$
$$ny-hx = q_1^{i_1}\cdots q_k^{i_k}\alpha, \text{ με } (\alpha,n)=1. \tag{2.5}$$

Εφ'όσον $\alpha \mid ny-hx$, από την σχέση (2.4) έχουμε $\alpha \mid (nx-h)n^f$ και αφού $(\alpha,n^f)=(\alpha,n)=1$ συμπεραίνουμε ότι

$$\alpha \mid nx-h. \tag{2.6}$$

Σύμφωνα με το Λήμμα 2.1 έχουμε ότι $q_j^{i_j} \mid x$. Άρα

$$q_1^{i_1}\cdots q_k^{i_k} \mid x. \tag{2.7}$$

Από τις σχέσεις (2.5), (2.6), (2.7) έχουμε ότι $ny-hx \mid x(nx-h)$, άρα $|ny-hx| \leq |x(nx-h)|$. Εφ'όσον $|h|<n$ και $x\neq 0$ (αφού $x \mid_n 1$) έχουμε ότι $x(nx-h)>0$, άρα $|ny-hx| \leq x(nx-h) = nx^2-hx$. Οπότε

$$n|y|-hx = n|y|-|hx| = |n|y|-|hx|| \leq |ny-hx| \leq |x(nx-h)| = x(nx-h) = nx^2-hx.$$

Επομένως, $n|y| \leq nx^2 \Rightarrow |y| \leq x^2$.
Άρα, από τις σχέσεις $x^2 \leq |y|$ και $|y| \leq x^2$ έπεται ότι $|y|=x^2 \Rightarrow y=\pm x^2$.
Αν $y=-x^2$ τότε από την σχέση $2nx+1 \mid 4n^2y-1$ έχουμε ότι $2nx+1 \mid -4n^2x^2-1$. Ισχύει ότι $2nx+1 \mid (2nx)^2-1^2 \Rightarrow 2nx+1 \mid 4n^2x^2-1$. Άρα $2nx+1 \mid (-4n^2x^2-1)+(4n^2x^2-1) \Rightarrow 2nx+1 \mid -2$. Άτοπο.
Οπότε $y=x^2$. □

Λήμμα 2.3. *Έστω $n>1$ και $x,u,z\in\mathbb{Z}$. Υποθέτουμε ότι ισχύουν οι εξής συνθήκες:*

$$nz+nx-1 \mid_n n^2u-(nx-1)^2 \tag{2.8}$$
$$2nz+1 \mid_n nx-1 \tag{2.9}$$
$$2nz-1 \mid_n nx-1 \tag{2.10}$$
$$2n^2u+1 \mid_n nx-1 \tag{2.11}$$

Τότε $u=z^2$.

Απόδειξη. Εφ'όσον $(nz+nx-1,n)=(2nz\pm 1,n)=(2n^2u+1,n)=1$, από την Παρατήρηση 2.1 έχουμε ότι $nz+nx-1 \mid n^2u-(nx-1)^2$, $2nz+1 \mid nx-1$, $2nz-1 \mid nx-1$, $2n^2u+1 \mid nx-1$. Οπότε

$$n^2u-(nx-1)^2 \equiv 0 \pmod{nz+nx-1}. \tag{2.12}$$

Ισχύει $nz+nx-1 \equiv 0 \pmod{nz+nx-1} \Rightarrow nx-1 \equiv -nz \pmod{nz+nx-1}$. Άρα (2.12) $\Rightarrow n^2u-(-nz)^2 \equiv \pmod{nz+nx-1} \Rightarrow nz+nx-1 \mid n^2u-n^2z^2$.
Υποθέτουμε ότι $u\neq z^2$. Τότε

$$|nx-1|-n|z| \leq |nz+nx-1| \leq |n^2u-n^2z^2| \leq n^2|u|+n^2z^2 \tag{2.13}$$

Αφού $(2nz+1, 2nz-1) = 1$, έχουμε ότι $(2nz+1)(2nz-1) \mid nx-1 \Rightarrow 4n^2z^2-1 \mid nx-1$. Έχουμε ότι $nx-1 \neq 0$, αφού $n \neq 1$, άρα

$$4n^2z^2 - 1 = |4n^2z^2 - 1| \leq |nx-1|. \tag{2.14}$$

Όμοια, από την σχέση (2.11) έχουμε ότι

$$2n^2|u| - 1 \leq |2n^2u + 1| \leq |nx-1|. \tag{2.15}$$

Προσθέτοντας τις σχέσεις (2.14) και (2.15) παίρνουμε $4n^2z^2 + 2n^2|u| - 2 \leq 2|nx-1| \Rightarrow 2n^2z^2 + n^2|u| - 1 \leq |nx-1| \Rightarrow 2n^2z^2 + n^2|u| - n|z| - 1 \leq |nx-1| - n|z|$.
Από την σχέση (2.13) έχουμε ότι

$$2n^2z^2 + n^2|u| - n|z| - 1 \leq n^2|u| + n^2z^2 \Rightarrow n^2z^2 - n|z| - 1 \leq 0.$$

Εφόσον οι ρίζες του πολυωνύμου $t^2 - t - 1$ είναι $\frac{1\pm\sqrt{5}}{2}$, από την παραπάνω ανισότητα προκύπτει ότι

$$-1 \leq \frac{1-\sqrt{5}}{2} \leq n|z| \leq \frac{1+\sqrt{5}}{2} \leq 2 \tag{2.16}$$

Αν $z \neq 0$, τότε αφού $n > 1$ θα πρέπει να ισχύει $n|z| \geq 2$, αλλά τότε δεν ισχύει η ανισότητα (2.16). Άρα $z = 0$. Τότε από τις σχέσεις (2.13) και (2.15) έχουμε ότι $2n^2|u| - 1 \leq n^2|u| \Rightarrow n^2|u| \leq 1 \Rightarrow u = 0$.
Οπότε ισχύει $u = z = 0$ ή $u = z^2$. Δηλαδή σε κάθε περίπτωση ισχύει $u = z^2$. □

Λήμμα 2.4. *Για κάθε μη μηδενικό ακέραιο d υπάρχει ένας ακέραιος x που ικανοποιεί τις σχέσεις $x \mid_n 1$ και $d \mid_n nx-1$.*

Απόδειξη. Γράφουμε το d ως $d = d_0d_1$ όπου $d_0 \mid_n 1$ και το d_1 είναι σχετικά πρώτο ως προς το n. Ορίζουμε $x = n^{\phi(d_1)-1}$, όπου ϕ είναι η συνάρτηση Euler. Τότε έχουμε ότι $x \mid_n 1$.
Εφ'όσον $(d_1, n) = 1$, από το Θεώρημα Euler έχουμε ότι $n^{\phi(d_1)} \equiv 1 \pmod{d_1}$. Οπότε $nx-1 = n^{\phi(d_1)} - 1 \equiv 0 \pmod{d_1}$, άρα $d_1 \mid nx-1$ και αφού $(d_1, n) = 1$ ισχύει $d_1 \mid_n nx-1$.
Άρα από τις σχέσεις $d_0 \mid_n 1$ και $d_1 \mid_n nx-1$ παίρνουμε ότι $d \mid_n nx-1$. □

Λήμμα 2.5. *$u = z^2$ αν και μόνο αν υπάρχουν ακέραιοι x και y έτσι ώστε $x \mid_n 1$ και $y \mid_n 1$ και ισχύουν οι σχέσεις (2.1) - (2.3), (2.9) - (2.11) και*

$$nz + nx - 1 \mid_n n^2u - n^2y + 2nx - 1. \tag{2.17}$$

Απόδειξη. Έστω $u = z^2$. Σύμφωνα με το Λήμμα 2.4 με $d = (2nz+1)(2nz-1)(2n^2u+1)$ υπάρχει ένας ακέραιος x που ικανοποιεί τις σχέσεις (2.9), (2.10), (2.11) και $x \mid_n 1$. Παίρνουμε $y = x^2$. Τότε έχουμε ότι $y \mid_n 1$ και τότε σύμφωνα με το Λήμμα 2.2 ισχύουν οι σχέσεις (2.1), (2.2), (2.3). Εφ'όσον $n^2u - n^2y + 2nx - 1 = n^2z^2 - n^2x^2 + 2nx - 1 = (nz)^2 - (nx-1)^2 = (nz - nx + 1)(nz + nx - 1)$ έχουμε ότι ισχύει και η σχέση (2.17).

Αντίστροφα, υποθέτουμε ότι υπάρχουν x και y έτσι ώστε οι σχέσεις (2.1) - (2.3), (2.9) - (2.17), $x \mid_n 1$ και $y \mid_n 1$ ισχύουν. Σύμφωνα με το Λήμμα 2.2 έχουμε ότι $y = x^2$. Αντικαθιστώντας το στην σχέση (2.17) καταλήγουμε στην σχέση (2.8). Οπότε, αφού ισχύουν όλες οι προϋποθέσεις του Λήμματος 2.3, έχουμε ότι $u = z^2$. □

Απόδειξη του Θεωρήματος 2.1. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση και την σχέση $|_n$ είναι αποφασίσιμη, δηλαδή υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $(\mathbb{Z}; +, |_n)$.
Θα ανάγουμε το 10^o πρόβλημα του Hilbert, δηλαδή την υπαρξιακή θεωρία του $(\mathbb{Z}; +, \cdot)$ στην θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, |_n)$.
Η απεικόνιση της αναγωγής είναι $n \mapsto n$.
Τότε το $+$ αντιστοιχεί στο $+$.
Σύμφωνα με το Λήμμα 2.5 υπάρχουν πολυώνυμα A_i και B_i πάνω από το $\mathbb{Z}$ βαθμού το πολύ 1 έτσι ώστε

$$u = z^2 \leftrightarrow \exists x, y : \bigwedge_{i=1}^{s} A_i(x, y) \mid_n B_i(x, y).$$

Επίσης έχουμε τις ισοδυναμίες

$$z = x + y \leftrightarrow 0 \mid_n x + y - z$$
$$z = x \cdot y \leftrightarrow 4z = (x + y)^2 - (x - y)^2.$$

Οπότε μπορούμε να ορίσουμε το $\cdot$ ως εξής

$$z = x \cdot y \leftrightarrow \exists x_1, \ldots, \exists x_m : \bigwedge_{i=1}^{s} C_i(x_1, \ldots, x_m) \mid_n D_i(x_1, \ldots, x_m),$$

όπου C_i και D_i πολυώνυμα πάνω από το $\mathbb{Z}$ βαθμού το πολύ 1.
Οπότε μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, |_n)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, \cdot)$.
Εφ΄όσον η θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, \cdot)$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, |_n)$ είναι μη αποφασίσιμη. □

ΚΕΦΑΛΑΙΟ 3

Θετική υπαρξιακή θεωρία των πολυωνύμων

Στο κεφάλαιο αυτό θα αποδείξουμε το 10^o πρόβλημα του Hilbert για πολυωνυμικούς δακτυλίους $F[t]$ επί σωμάτων F. Στην απόδειξη, η χαρακτηριστική του δακτυλίου θα είναι σημαντική. Θα κάνουμε μια διάκριση μεταξύ χαρακτηριστικής διάφορη του 2 και χαρακρητιστικής 2. Οι αποδείξεις είναι βασισμένες στο [Phe94] για δακτυλίους με χαρακτηριστική διάφορη του 2 και στο [Den78b] για δακτυλίους με χαρακτηριστική 2.

3.1 Πολυωνυμικός δακτύλιος με χαρακτηριστική διάφορη του 2

Θεωρούμε τον δακτύλιο $F[t, t^{-1}]$, ο οποίος περιέχει τα πολυώνυμα ως προς t και t^{-1} με συντελεστές στο σώμα F.

Θεώρημα 3.1. *Αν η χαρακτηριστική του F είναι διάφορη του 2, τότε το $F[t]$ έχει μη αποφασίσιμη θετική υπαρξιακή θεωρία στη γλώσσα $\{+, \cdot, 0, 1, t\}$.*

Ιδέα της απόδειξης. *Αρχικά θα αποδείξουμε την μη αποφασισιμότητα της θετικής υπαρξιακής θεωρίας του $F[t, t^{-1}]$ όταν η χαρακτηριστική του σώματος F είναι 0 και όταν η χαρακτηριστική είναι $p > 2$. Στην περίπτωση που η χαρακτηριστική είναι 0 θα ανάγουμε το 10^o πρόβλημα του Hilbert στην θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ και στην περίπτωση που η χαρακτηριστική είναι $p > 2$ θα ανάγουμε την θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, |, |^p)$ στην θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$. Έχοντας αποδείξει την μη αποφασισιμότητα της θετικής υπαρξιακής θεωρίας του $F[t, t^{-1}]$ μπορούμε να την ανάγουμε στην θετική υπαρξιακή θεωρία του $F[t]$, με $\operatorname{char} F \neq 2$, για να δείξουμε ότι και η δεύτερη είναι μη αποφασίσιμη.*

Λήμμα 3.1. *Για κάθε $x \in F[t, t^{-1}]$, το x είναι μια δύναμη του t, $x = t^n$ αν και μόνο αν το x διαιρεί το 1 και το $t - 1$ διαιρεί το $x - 1$.*

Απόδειξη. Αν $x = t^n$, τότε $xt^{-n} = 1$. Οπότε $x \mid 1$.
Επίσης

$$x = t^n \Rightarrow x - 1 = t^n - 1 = (t-1)(t^{n-1} + \cdots + 1) \Rightarrow t - 1 \mid x - 1.$$

Αντίστροφα, υποθέτουμε ότι $t - 1 \mid x - 1$ και ότι $x \mid 1$, δηλαδή το x είναι αντιστρέψιμο. Ένα στοιχείο $x \in F[t, t^{-1}]$ είναι ένα πολυώνυμο ως προς t και t^{-1}. Οπότε

$$x = a_{-u}t^{-u} + \ldots a_{-1}t^{-1} + a_0 + a_1 t + \cdots + a_v t^v$$

με $u, v \geq 0$. Πολλαπλασιάζοντας με t^u παίρνουμε $xt^u = f(t)$ το οποίο είναι ένα πολυώνυμο του $F[t]$, οπότε $x = \frac{f(t)}{t^u}$.
Εφόσον το x είναι αντιστρέψιμο, υπάρχει $y \in F[t, t^{1-}]$ έτσι ώστε $xy = 1$. Έχουμε ότι $y = \frac{g(t)}{t^m}$ με $m \geq 0$ και $g(t) \in F[t]$.
Από την σχέση $xy = 1$ έχουμε $f(t)g(t) = t^{m+u}$. Οπότε έχουμε ότι $f(t) = at^i$ με $a \in F \setminus \{0\}$ και $i \geq 0$, δηλαδή $x = at^n$. Εφόσον $t - 1 \mid x - 1$ έχουμε ότι

$$t - 1 \mid at^n - 1 = at^n - a + a - 1 = a(t^n - 1) + a - 1 = a(t-1)(t^{n-1} + \cdots + 1) + a - 1.$$

Οπότε πρέπει $a - 1 = 0 \Rightarrow a = 1$.
Δηλαδή $x = t^n$. □

Λήμμα 3.2.

$$(t^n - 1)/(t-1) \equiv n \pmod{t-1}$$

Απόδειξη.

$$\begin{aligned}
(t^n - 1)/(t-1) - n &= (t-1)(t^{n-1} + t^{n-2} + \cdots + t + 1)/(t-1) - n \\
&= t^{n-1} + t^{n-2} + \cdots + t + 1 - n \\
&= t^{n-1} + t^{n-2} + \cdots + t + 1 - \underbrace{(1 + \cdots + 1)}_{n\text{-φορές}} \\
&= (t^{n-1} - 1) + (t^{n-2} - 1) + \cdots + (t-1) + (1-1) \\
&= (t-1)(t^{n-2} + \cdots + 1) \\
&\equiv 0 \pmod{t-1}
\end{aligned}$$

Οπότε,

$$(t^n - 1)/(t-1) \equiv n \pmod{t-1}.$$

□

Λήμμα 3.3. *Υποθέτουμε ότι η χαρακτηριστική του F είναι μηδέν. Τότε για κάθε $n \in F[t, t^{-1}]$, το n είναι μη μηδενικός ακέραιος αν και μόνο αν*

- *το n διαιρεί το 1*
- *είτε το $n-1$ διαιρεί το 1 ή το $n+1$ διαιρεί το 1*
- *υπάρχει δύναμη x του t έτσι ώστε $(x-1)/(t-1) \equiv n \pmod{t-1}$.*

Απόδειξη. Έστω $n \in \mathbb{Z} \setminus \{0\}$, τότε $n \mid 1$, αφού το F είναι σώμα.
Επίσης ισχύει $n-1 \mid 1$ ή $n+1 \mid 1$, διαφορετικά θα ίσχυε ταυτόχρονα $n = 1$ και $n = -1$.
Από το Λήμμα 2 έχουμε ότι $\frac{t^n-1}{t-1} \equiv n \pmod{t-1}$ οπότε υπάρχει δύναμη x του t έτσι ώστε $\frac{x-1}{t-1} \equiv n \pmod{t-1}$.

Αντίστροφα, υποθέτουμε ότι $n \in F[t, t^{-1}]$ και $n \mid 1$ και $(n-1 \mid 1$ ή $n+1 \mid 1)$ και $\frac{t^k-1}{t-1} \equiv n \pmod{t-1}, k \in \mathbb{Z}$.
Εφ'όσον το $n \in F[t, t^{-1}]$ είναι αντιστρέψιμο ($n \mid 1$) έχουμε ότι $n = at^i$, όπου $a \in F \setminus \{0\}$ και $i \in \mathbb{Z}$.
Εφ'όσον και το $n-1$ ή το $n+1$ είναι αντιστρέψιμο ($n-1 \mid 1$ ή $n+1 \mid 1$) έχουμε ότι

$$n-1 = b_1 t^{j_1}, b_1 \in F \setminus \{0\}, j_1 \in \mathbb{Z} \Rightarrow at^i - 1 = b_1 t^{j_1}$$
$$\text{ή}$$
$$n+1 = b_2 t^{j_2}, b_2 \in F \setminus \{0\}, j_2 \in \mathbb{Z} \Rightarrow at^i + 1 = b_2 t^{j_2}$$

Για $i \neq 0$, το $at^i \pm 1$ έχει μια μη μηδενική ρίζα σε μια επέκταση του F, η οποία όμως δεν είναι ρίζα του $bt^j, j \in \{j_1, j_2\}, b \in \{b_1, b_2\}$.
Άρα, $i = 0$.
Οπότε, $n = a \in F \setminus \{0\}$. Δηλαδή το n είναι μη μηδενικό σταθερό πολυώνυμο του $F[t, t^{-1}]$.
Από την τρίτη συνθήκη, $\frac{t^k-1}{t-1} \equiv \pmod{t-1}, k \in \mathbb{Z}$ και από το Λήμμα 2 έχουμε ότι

$$k \equiv n \pmod{t-1} \Rightarrow n-k \equiv 0 \pmod{t-1} \Rightarrow \exists y \in F[t, t^{-1}] : n-k = y(t-1)$$
$$\Rightarrow n = k + y(t-1)$$

Εφ'όσον το n είναι μη μηδενικό σταθερό πολυώνυμο, πρέπει $y = 0$.
Οπότε, $n = k \in \mathbb{Z} \setminus \{0\}$. □

Θεώρημα 3.2. *Υποθέτουμε ότι η χαρακτηριστική του F είναι μηδέν. Τότε η θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$ είναι μη αποφασίσιμη.*

Απόδειξη. Θέλουμε να δείξουμε ότι δεν υπάρχει αλγόριθμος, ο οποίος, δεδομένης μιας θετικής υπαρξιακής πρότασης γ, μας απαντάει αν η γ ισχύει στον δακτύλιο $F[t, t^{-1}]$ ή όχι.
Σύμφωνα με το Λήμμα 1, ένα στοιχείο $x \in F[t, t^{-1}]$ είναι μια δύναμη του t αν και μόνο αν

- $x \mid 1 \quad : \quad (\exists y)(xy = 1)$

- $t-1 \mid x-1 \quad : \quad (\exists z)(x-1=(t-1)z)$

Οπότε μπορούμε να εκφράσουμε το γεγονός ότι ένα στοιχείο $x \in F[t,t^{-1}]$ είναι μια δύναμη του t με τον θετικό υπαρξιακό τύπο

$$\phi(x) \quad : \quad \exists y \exists z((xy=1) \wedge (x-1=(t-1)z))$$

Σύμφωνα με το Λήμμα 3, το n είναι μη μηδενικός ακέραιος αν και μόνο αν

- $n \mid 1 \quad : \quad (\exists z)(nz=1)$
- $n-1 \mid 1 \vee n+1 \mid 1 \quad : \quad (\exists w)((n+1)w=1 \text{ or } (n-1)w=1)$
- υπάρχει μια δύναμη x του $t \quad : \quad (\exists x)\phi(x)$
- $(x-1)/(t-1) \equiv n \pmod{t-1} \quad : \quad (\exists y)((x-1)/(t-1)-n=y(t-1)) \Rightarrow (\exists y)(x-1-n(t-1)=y(t-1)^2) \Rightarrow (\exists y)(x-1=n(t-1)+y(t-1)^2)$

Οπότε μπορούμε να εκφράσουμε το γεγονός ότι ένα στοιχείο $n \in F[t.t^{-1}]$ είναι ένας ακέραιος με τον θετικό υπαρξιακό τύπο

$$\begin{aligned} \psi(n) \quad : \quad & (\exists x)(\exists y)[\phi(x) \wedge x-1=(t-1)n+y(t-1)^2] \wedge \\ & (\exists z)(\exists w)(nz=1 \wedge ((n+1)w=1 \text{ or } (n-1)w=1) \end{aligned}$$

Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $F[t,t^{-1}]$ είναι αποφασίσιμη, δηλαδή υπάρχει αλγόριθμος που αποφασίζει αν μια θετική υπαρξιακή πρόταση είναι αληθής στο $F[t,t^{-1}]$.
Τότε το πρόβλημα αν μια διοφαντική εξίσωση έχει ακέραια λύση είναι αποφασίσιμο:
η διοφαντική εξίσωση $P(x_1,\ldots,x_n)=0$ έχει ακέραια λύση αν και μόνο αν η θετική υπαρξιακή πρόταση

$$(\exists x_1)\ldots(\exists x_n)((\psi(x_1)\wedge\cdots\wedge\psi(x_n))\wedge P(x_1,\ldots,x_n)=0)$$

είναι αληθής στο $F[t,t^{-1}]$.
Αλλά η απάντηση στο 10^o πρόβλημα του Hilbert, δηλαδή αν υπάρχει αλγόριθμος που αποφασίζει αν μια διοφαντική εξίσωση έχει ακέραια λύση, είναι αρνητική.
Οπότε καταλήγουμε σε άτοπο.
Δηλαδή η θετική υπαρξιακή θεωρία του $F[t,t^{-1}]$ είναι μη αποφασίσιμη. □

Λήμμα 3.4. *Το t^n-1 διαιρεί το t^m-1 στο $F[t,t^{-1}]$ αν και μόνο αν το n διαιρεί το m στο $\mathbb{Z}$.*

Απόδειξη. Υποθέτουμε ότι $n \mid m$, τότε $m=kn, k \in \mathbb{Z}$.

$$t^m-1=t^{kn}-1=(t^n)^k-1=(t^n-1)(t^{n(k-1)}+\cdots+1)$$

Οπότε, $t^n-1 \mid t^m-1$.

Αντίστροφα, από την ευκλείδεια διαίρεση έχουμε ότι $m = nq + r, \quad q, r \in \mathbb{Z}, 0 \leq r < n$.
Εφ'όσον $t^n - 1 \mid t^m - 1$ έχουμε ότι $t^m - 1 \equiv 0 \pmod{t^n - 1} \Rightarrow t^m \equiv 1 \pmod{t^n - 1}$.
Επίσης έχουμε ότι $t^n - 1 \mid t^n - 1$, οπότε $t^n \equiv 1 \pmod{t^n - 1}$.
Επομένως έχουμε ότι

$$t^m \equiv t^{nq+r} \pmod{t^n - 1} \Rightarrow 1 \equiv (t^n)^q\, t^r \pmod{t^n - 1} \Rightarrow 1 \equiv t^r \pmod{t^n - 1}.$$

Οπότε $t^n - 1 \mid t^r - 1$.
Αν $r \neq 0$, τότε $n \leq r$. Άτοπο.
Οπότε, $r = 0$. Επομένως, $m = nq$.
Συνεπώς, $n \mid m$. □

Λήμμα 3.5. *Υποθέτουμε ότι η χαρακτηριστική του F είναι p και $p > 2$. Τότε το $t^m - 1)/(t^n - 1)$ είναι ένα τετράγωνο στο $F[t, t^{-1}]$ αν και μόνο αν $(\exists s \in \mathbb{Z})m = np^s$.*

Απόδειξη. Υποθέτουμε ότι το $\frac{t^m-1}{t^n-1}$ είναι ένα τετράγωνο στο $F[t, t^{-1}]$, οπότε $\exists a \in F[t, t^{-1}]$ τέτοιο ώστε $\frac{t^m-1}{t^n-1} = a^2$.
Εφόσον ένα στοιχείο του $F[t, t^{-1}]$ είναι της μορφής $\frac{f(t)}{t^k}$ όπου $f(t) \in F[t]$, έχουμε ότι

$$\frac{t^m - 1}{t^n - 1} = \left(\frac{f(t)}{t^k}\right)^2 \Rightarrow \frac{t^m - 1}{t^n - 1} = \frac{f^2(t)}{t^{2k}} \Rightarrow t^{2k}(t^m - 1) = f^2(t)(t^n - 1) \qquad (*)$$

Έστω $m = m_1 p^l$, όπου $p \nmid m_1$. Τότε

$$t^m - 1 = t^{m_1 p^l} - 1 = (t^{m_1} - 1)^{p^l}.$$

Έστω $n = n_1 p^r$, όπου $p \nmid n_1$. Τότε

$$t^n - 1 = t^{n_1 p^r} - 1 = (t^{n_1} - 1)^{p^n}.$$

Οπότε,

$$(*) \Rightarrow t^{2k}(t^{m_1} - 1)^{p^l} = f^2(t)(t^{n_1} - 1)^{p^r} \qquad (**)$$

Υποθέτουμε ότι το $t^{m_1} - 1$ έχει μια μη μηδενική ρίζα, έστω u, σε μια επέκταση του F η οποία δεν είναι ρίζα του $t^{n_1} - 1$. Τότε

$$0 = u^{2k}(u^{m_1} - 1)^{p^l} = f^2(u)(u^{n_1} - 1)^{p^r} \Rightarrow f^2(u) = 0.$$

Οπότε το u είναι ρίζα του $f^2(t)$ με άρτια πολλαπλότητα. Στο αριστερό μέρος της εξίσωσης (**), το u είναι ρίζα του $(t^{m_1} - 1)^{p^l}$, οπότε είναι ρίζα με περιττή πολλαπλότητα, αφού το p^l είναι περιττό.
Άτοπο.
Οπότε, το σύνολο ριζών του $t^{n_1} - 1$ συμπίπτει με το σύνολο ριζών του $t^{m_1} - 1$.
Εφ'όσον $m_1 \nmid p$ και $n_1 \nmid p$ έχουμε ότι οι ρίζες των πολυωνύμων $t^{m_1} - 1$ και $t^{n_1} - 1$ είναι διακριτές.

Άρα το πλήθος των ριζών ισούται με το βαθμό του πολυωύμου. Οπότε $n_1 = m_1$.
Τότε

$$\left.\begin{array}{c} m = m_1 p^l \\ n = n_1 p^r \end{array}\right\} \Rightarrow \left.\begin{array}{c} m = m_1 p^l \\ n = m_1 p^r \end{array}\right\} \Rightarrow \left.\begin{array}{c} m = m_1 p^l \\ m_1 = np^{-r} \end{array}\right\} \Rightarrow m = np^{-r}p^l \Rightarrow m = np^{l-r}$$

Οπότε $\exists s = l - r : m = np^s$.

Αντίστροφα, αν $m = np^s$, τότε

$$\frac{t^m - 1}{t^n - 1} = \frac{t^{np^s} - 1}{t^n - 1} = \frac{(t^n - 1)^{p^s}}{t^n - 1} = (t^n - 1)^{p^s - 1}$$

το οποίο είναι τετράγωνο, αφού $2 \mid p^s - 1$. □

Θεώρημα 3.3. *Υποθέτουμε ότι η χαρακτηριστική του F είναι $p > 2$. Τότε η θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ είναι μη αποφασίσιμη.*

Απόδειξη. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ είναι αποφασίσιμη, δηλαδή ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $F[t, t^{-1}]$.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $(\exists s \in \mathbb{Z})m = p^s n$ στην θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$. Δηλαδή θέλουμε να 'μεταφράσουμε' τους φυσικούς αριθμούς με την πρόσθεση, την διαιρετότητα και την σχέση $(\exists s \in \mathbb{Z})m = p^s n$, στην υπαρξιακή θεωρία του $F[t, t^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$.
Η απεικόνιση της αναγωγής είναι $n \mapsto t^n$. Οι δυνάμεις του t εκπροσωπούν τους ακέραιους. Σύμφωνα με το Λήμμα 1, μπορούμε να εκφράσουμε το γεγονός ότι ένα στοιχείο $x \in F[t, t^{-1}]$ είναι μια δύναμη του t με τον θετικό υπαρξιακό τύπο

$$\phi(x) : (\exists y)(\exists z)((xy = 1)) \wedge (x - 1 = (t - 1)z)).$$

Άρα το σύνολο των δυνάμεων του t είναι θετικά υπαρξιακά ορισμένο.
Έχουμε ότι $m + n \mapsto t^{m+n} = t^m t^n$, δηλαδή η πρόσθεση των ακεραίων αντιστοιχεί στον πολλαπλασιαμό των αντίστοιχων δυνάμεων του t.
Από το Λήμμα 4 έχουμε ότι $n \mid m \Leftrightarrow t^n - 1 \mid t^m - 1$ και εφόσον $t^n - 1 \mid t^m - 1 \Leftrightarrow \exists a \in F[t, t^{-1}] : a(t^n - 1) = t^m - 1$ έχουμε ότι η σχέση $n \mid m$ μπορει να οριστεί θετικά υπαρξιακά.
Από το Λήμμα 5 έχουμε ότι $(\exists s \in \mathbb{Z})m = np^s \Leftrightarrow (t^m - 1)/(t^n - 1)$ είναι τετράγωνο στο $F[t, t^{-1}] \Leftrightarrow \exists b \in F[t, t^{-1}] : t^m - 1 = b^2(t^n - 1)$.
Δηλαδή η σχέση $(\exists s \in \mathbb{Z})m = p^s n$ μπορεί να οριστεί θετικά υπαρξιακά.
Οπότε, μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $F[t, t^{-1}]$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $(\exists s \in \mathbb{Z})m = p^s n$.
Εφ'όσον όμως η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $(\exists s \in \mathbb{Z})m = p^s n$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του $F[t, t^{-1}]$ είναι μη αποφασίσιμη. □

Απόδειξη του Θεωρήματος 3.1. Γνωρίζουμε ότι η θετική υπαρξιακή θεωρία του $F[u, u^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, u\}$ είναι μη αποφασίσιμη.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $F[u, u^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, u\}$ στην θετική υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$, για να δείξουμε ότι και η δεύτερη είναι μη αποφασίσιμη.
Για τον σκοπό αυτό κάνουμε τα παρακάτω:
Θέτουμε $u = t + \sqrt{t^2 - 1}$. Άρα έχουμε $u^{-1} = t - \sqrt{t^2 - 1}$.
Δηλαδή $F[u, u^{-1}] = F[t, \sqrt{t^2 - 1}]$.
Άρα το $F[u, u^{-1}]$ είναι μια επέκταση του $F[t]$.
Κάθε στοιχείο x του $F[u, u^{-1}]$ μπορεί να γραφεί ως $x = a + b\sqrt{t^2 - 1}$, όπου $a, b \in F[t]$.
Οπότε η απεικόνιση της αναγωγής είναι $x \mapsto (a, b)$.

$$\begin{aligned} x_1 + x_2 &= a_1 + b_1\sqrt{t^2-1} + a_2 + b_2\sqrt{t^2-1}[t] \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{t^2 - 1} \\ x_1 + x_2 &\mapsto (a_1 + a_2, b_1 + b_2) \end{aligned}$$

$$\begin{aligned} x_1 \cdot x_2 &= (a_1 + b_1\sqrt{t^2-1})(a_2 + b_2\sqrt{t^2-1}) \\ &= a_1 \cdot a_2 + a_1 \cdot b_2\sqrt{t^2-1} + a_2 \cdot b_1\sqrt{t^2-1} + b_1 \cdot b_2(t^2-1) \\ &= (a_1 \cdot a_2 + b_1 \cdot b_2(t^2-1)) + (a_1 \cdot b_2 + a_2 \cdot b_1)\sqrt{t^2-1} \\ x_1 \cdot x_2 &\mapsto (a_1 \cdot a_2 + b_1 \cdot b_2(t^2-1), a_1 \cdot b_2 + a_2 \cdot b_1) \end{aligned}$$

$u \mapsto u - t =: v$. Γράφουμε όλες τις εξισώσεις στην μορφή $fv = g$ όπου $f.g \in F[t]$ και αν τετραγωνίσουμε τις εξισώσεις αυτές παίρνουμε $f^2v^2 = g^2 \Rightarrow f^2(t^2 - 1) = g^2$, άρα όλες αυτές οι εξισώσεις είναι στο $F[t]$, όπου $t = \frac{u+u^{-1}}{2}$.

Οπότε αφού η θετική υπαρξιακή θεωρία του $F[u, u^{-1}]$ στη γλώσσα $\{+, \cdot, 0, 1, u\}$ είναι μη αποφασίσιμη, συμπεραίνουμε ότι η θετική υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$ είναι μη αποφασίσιμη. □

3.2 Πολυωνυμικός δακτύλιος με χαρακτηριστική 2

Θεώρημα 3.4. *Έστω F μια ακέραια περιοχή με χαρακτηριστική $p = 2$. Έστω $F[t]$ ο δακτύλιος των πολυωνύμων πάνω από το F σε μια μεταβλητή t. Τότε η θετική υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$ είναι μη αποφασίσιμη, δηλαδή δεν υπάρχει αλγόριθμο ο οποίος αποφασίζει αν μια πολυωνυμική εξίσωση με συντελεστές στο $(\mathbb{Z}/2\mathbb{Z})[t]$ έχει λύση στο $F[t]$ ή όχι.*

Ορισμός 3.1. *Έστω F μια ακέραια περιοχή με χαρακτηριστική $p = 2$. Έστω $a \in F[t]$ και $a \notin F$. Έστω $\alpha(a)$ μια ρίζα της εξίσωσης $x^2 + ax + 1 = 0$. Ορίζουμε τις δύο ακολουθίες $X_m(a), Y_m(a) \in F[t], m \in \mathbb{Z}$ ως εξής*

$$X_m(a) + \alpha(a)Y_m(a) = (\alpha(a))^m = (a + \alpha(a))^{-m}. \tag{3.1}$$

Λήμμα 3.6. *Έστω F μια ακέραια περιοχή με χαρακτηριστική $p = 2$. Έστω $a \in F[t], a \notin F$. Για κάθε $m, n \in \mathbb{Z}$ έχουμε:*

i. Το $X_m(a)$ (αντ. $Y_m(a)$) ισούται με το πολυώνυμο το οποίο παίρνουμε αν αντικαταστήσουμε το t με a στο $X_m(t)$ (αντ. $Y_m(t)$).

Ο βαθμός του πολυωνύμου $X_m(t)$ είναι $m - 2$, αν $m \geq 2$.

Ο βαθμό του πολυωνύμου $Y_m(t)$ είναι $m - 1$, αν $m \geq 2$.

$X_{-m}(a) = X_m(a) + aY_m(a)$

$Y_{-m}(a) = Y_m(a)$

ii. Όλες οι λύσεις $X, Y \in F[t]$ της εξίσωσης

$$X^2 + aXY + Y^2 = 1 \tag{3.2}$$

δίνονται από $X_m(a), Y_m(a)$, με $m \in \mathbb{Z}$.

iii. $X_{m+n}(a) = X_m(a)X_n(a) + Y_m(a)Y_n(a)$
$Y_{m+n}(a) = X_m(a)Y_n(a) + Y_n(a)X_n(a) + aY_m(a)Y_n(a)$

iv. $n \mid m \Leftrightarrow Y_n(a) \mid Y_m(a)$

v. $Y_{m2^n}(a) = \frac{a^{2^n}}{a} \left(Y_m(a)\right)^{2^n}$ *και* $Y_{2^n}(a) = \frac{a^{2^n}}{a}$, *αν* $n \geq 0$

vi. $(a + 1)Y_m(a + 1) = aY_m(a) + 1 \Leftrightarrow m = \pm 2^n$ *για κάποιο* $n \in \mathbb{N}$.

Απόδειξη.

i. **Βάση επαγωγής** : Για $m = 2$ έχουμε $X_2(a) + \alpha(a)Y_2(a) = (\alpha(a))^2 = a\alpha(a) + 1$. Άρα $X_2(a) = 1, Y_2(a) = a$. Δηλαδή $\deg(X_2) = 0 = 2 - 2$ και $\deg(Y_2) = 1 = 2 - 1$.

Επαγωγική υπόθεση : Υποθέτουμε ότι ισχύει για $m = k$, δηλαδή $\deg(X_k) = k-2$ και $\deg(Y_k) = k - 1$. (Ε.Υ.)

Επαγωγικό βήμα : Θα δείξουμε ότι ισχύει για $m = k+1$, δηλαδή $\deg(X_{k+1}) = k-1$ και $\deg(Y_{k+1}) = k$.

$$\begin{aligned} X_{k+1} + \alpha Y_{k+1} =& (a + \alpha(a))^{-(k+1)} = (a + \alpha(a))^{-k}(a + \alpha(a))^{-1} \\ =& (X_k + \alpha(a)Y_k)(a + \alpha(a))^{-1} = (X_k + \alpha(a)Y_k)\alpha(a) \\ =& \alpha(a)X_k + \alpha(a)^2 Y_k = \alpha(a)X_k + (a\alpha(a) + 1)Y_k \\ =& Y_k + \alpha(a)[X_k + aY_k] \end{aligned}$$

$$\Rightarrow X_{k+1} = Y_k \ , \ Y_{k+1} = X_k + aY_k$$

Άρα έχουμε ότι

$$\begin{aligned}\deg(X_{k+1}) = \deg(Y_k) &\overset{\text{Ε.Υ.}}{=} k-1\\ \deg(Y_{k+1}) = \max\{\deg(X_k), \deg(aY_k)\} &= \max\{\deg(X_k), \deg(a)+\deg(Y_k)\}\\ &\overset{\text{Ε.Υ.}}{=} \max\{k-2, 1+k-1\} = \max\{k-2, k\} = k\end{aligned}$$

Για κάθε ρίζα z της εξίσωσης $x^2+ax+1=0$ ισχύει $X_m(a)+zY_m(a)=z^m$. Μια ρίζα είναι η $z=\alpha(a)$. Από τους τύπους του Vieta έχουμε ότι η δεύτερη ρίζα είναι η $z=a+\alpha(a)$. Οπότε έχουμε $X_m(a)+(a+\alpha(a))Y_m(a)=(a+\alpha(a))^m$. Άρα,

$$\begin{aligned}X_{-m}(a)+\alpha(a)Y_{-m}(a) =&(a+\alpha(a))^m = X_m(a)+(a+\alpha(a))Y_m(a)\\ =&X_m(a)+aY_m(a)+\alpha(a)Y_m(a)\\ \Rightarrow X_{-m}(a) = X_m(a)+aY_m(a) \;\;,&\;\; Y_{-m}(a)=Y_m(a)\end{aligned}$$

ii. Αρχικά θα δείξουμε ότι το $(X,Y)=(X_m(a),Y_m(a))$ είναι λύση της εξίσωσης $X^2+aXY+Y^2=1$.

$$\begin{aligned}&(X_m(a))^2+aX_m(a)Y_m(a)+(Y_m(a))^2\\ &\quad=(X_m(a))^2+((\alpha(a))^{-1}+\alpha(a))X_m(a)Y_m(a)+(Y_m(a))^2\\ &\quad=(X_m(a))^2+(\alpha(a))^{-1}X_m(a)Y_m(a)+\alpha(a)X_m(a)Y_m(a)+(Y_m(a))^2\\ &\quad=X_m(a)[X_m(a)+(\alpha(a))^{-1}Y_m(a)]+Y_m(a)[\alpha(a)X_m(a)+Y_m(a)]\\ &\quad=X_m(a)[X_m(a)+\alpha(a))^{-1}Y_m(a)+\alpha(a)Y_m(a)[X_m(a)+(\alpha(a))^{-1}Y_m(a)]\\ &\quad=[X_m(a)+\alpha(a)Y_m(a)][X_m(a)+\alpha(a))^{-1}Y_m(a)]\\ &\quad=(\alpha(a))^m(\alpha(a))^{-m}=1\end{aligned}$$

Άρα το $(X_m(a),Y_m(a))$ είναι λύση της εξίσωσης (3.2).

Έστω (X,Y) μια λύση της εξίσωσης (3.2). Παραμετρικοποιούμε την καμπύλη $(\alpha(a))^2+a\alpha(a)+1=0$ ως εξής:

$$\alpha(a)=s \;\;,\;\; a=s+\frac{1}{s}.$$

Τότε οι συναρτήσεις $X+\alpha(a)Y$ και $X+(\alpha(a))^{-1}Y$ έχουν πόλο μόνο στο $s=0$, και αφού

$$(X+\alpha(a)Y)(X+(\alpha(a))^{-1}Y)=X^2+aXY+Y^2=1 \tag{3.3}$$

έχουμε ότι οι συναρτήσεις αυτές έχουν ρίζα μόνο στο $s=0$. Οπότε $X+\alpha(a)Y=cs^m$ για κάποιο $m\in\mathbb{Z}$. Άρα $X+\alpha(a)Y=cs^m=c(\alpha(a))^m$. Αντικαθιστώντας στην σχέση (3.3) έχουμε $c(\alpha(a))^mc(\alpha(a))^{-m}=1\Rightarrow c^2=1$. Οπότε

$$\begin{aligned}&X+\alpha(a)Y=(\alpha(a))^m=X_m(a)+\alpha(a)Y_m(a)\\ &\Rightarrow X=X_m(a) \;\;,\;\; Y=Y_m(a).\end{aligned}$$

iii.

$$\begin{aligned}X_{m+n}(a)+\alpha(a)Y_{m+n}(a) &= (a+\alpha(a))^{-(m+n)}\\ &=(a+\alpha(a))^{-m}(a+\alpha(a))^{-n}(X_m(a)+\alpha(a)Y_m(a))(X_n(a)+\alpha(a)Y_n(a))\\ &=X_m(a)X_n(a)+\alpha(a)X_m(a)Y_n(a)+\alpha(a)X_n(a)Y_m(a)+(\alpha(a))^2Y_m(a)Y_n(a)\\ &=X_m(a)X_n(a)+\alpha(a)X_m(a)Y_n(a)+\alpha(a)X_n(a)Y_m(a)+(a\alpha(a)+1)Y_m(a)Y_n(a)\\ &=[X_m(a)X_n(a)+Y_m(a)Y_n(a)]+\alpha(a)[X_m(a)Y_n(a)+X_n(a)Y_m(a)+aY_m(a)Y_n(a)]\end{aligned}$$

Οπότε

$$\begin{aligned}X_{m+n}(a) &= X_m(a)X_n(a)+Y_m(a)Y_n(a)\\ Y_{m+n}(a) &= X_m(a)Y_n(a)+Y_m(a)X_n(a)+aY_m(a)Y_n(a)\end{aligned}$$

iv. Αρκεί να το αποδείξουμε για $n, m \geq 0$.
Αρχικά, υποθέτουμε ότι $n \mid m$, δηλαδή $m = nq$, με $q \in \mathbb{N}$. Από την σχέση (3.1) προκύπτει

$$\begin{aligned}X_{nq}(a)+\alpha(a)Y_{nq}(a) =&(\alpha(a))^{nq} = ((\alpha(a))^n)^q = (X_n(a)+\alpha(a)Y_n(a))^q\\ =&\sum_{i=0}^{q}\binom{q}{i}X_n(a)^{q-i}(\alpha(a)Y_n(a))^i\\ =&\sum_{\substack{i=0\\ i\ \text{άρτιος}}}^{q}\binom{q}{i}X_n(a)^{q-i}(\alpha(a))^iY_n(a)^i+\sum_{\substack{i=1\\ i\ \text{περιττός}}}^{q}\binom{q}{i}X_n(a)^{q-i}(\alpha(a))^iY_n(a)^i.\end{aligned}$$

Αφού $(\alpha(a))^i = \alpha(a)(\alpha(a))^{i-1} = \alpha(a)((\alpha(a))^2)^{\frac{i-1}{2}} = \alpha(a)(a\alpha(a)+1)^{\frac{i-1}{2}}$ έχουμε

$$\begin{aligned}&X_{nq}(a)+\alpha(a)Y_{nq}(a)\\ &=\sum_{\substack{i=0\\ i\ \text{άρτιος}}}^{q}\binom{q}{i}X_n(a)^{q-i}(\alpha(a)Y_n(a))^i+\sum_{\substack{i=1\\ i\ \text{περιττός}}}^{q}\binom{q}{i}X_n(a)^{q-i}\alpha(a)(a\alpha(a)+1)^{\frac{i-1}{2}}Y_n(a)^i\\ &=\sum_{\substack{i=0\\ i\ \text{άρτιος}}}^{q}\binom{q}{i}X_n(a)^{q-i}(\alpha(a)Y_n(a))^i+\alpha(a)\sum_{\substack{i=1\\ i\ \text{περιττός}}}^{q}\binom{q}{i}X_n(a)^{q-i}(a\alpha(a)+1)^{\frac{i-1}{2}}Y_n(a)^i.\end{aligned}$$

Οπότε

$$Y_m(a) = Y_{nq}(a) = \sum_{\substack{i=1\\ i\ \text{περιττός}}}^{q}\binom{q}{i}X_n(a)^{q-i}(a\alpha(a)+1)^{\frac{i-1}{2}}Y_n(a)^i.$$

Δηλαδή $Y_n(a) \mid Y_m(a)$.

Αντίστροφα, υποθέτουμε ότι $Y_n(a) \mid Y_m(a)$.
Αν $n = 0$ τότε

$$X_n(a)+\alpha(a)Y_n(a) = (\alpha(a))^n = 1 \Rightarrow X_n(a) = 1, Y_n(a) = 0.$$

Άρα $Y_m(a) = 0$. Τότε $X_m(a) = X_{-m}(a) \Rightarrow (\alpha(a))^m = (\alpha(a)^{-m} \Rightarrow (\alpha(a))^m = ((\alpha(a))^{-1})^m \Rightarrow (\alpha(a))^m = (a + \alpha(a))^m$.
Αν $m \neq 0$ τότε $a = 0$. Άτοπο, αφού $a \notin F$. Άρα $m = 0$. Δηλαδή $n \mid m$.
Οπότε υποθέτουμε ότι $n > 0$. Από την ευκλείδεια διαίρεση έχουμε ότι $m = nq + r$, με $q, r \in \mathbb{N}$ και $0 \leq r < n$. Τότε

$$Y_m(a) = Y_{nq+r}(a) = X_{nq}(a)Y_r(a) + Y_{nq}(a)X_r(a) + aY_{nq}(a)Y_r(a)$$

Εφ'όσον $Y_n(a) \mid Y_m(a)$ και $Y_n(a) \mid Y_{nq}(a)$ έχουμε ότι $Y_n(a) \mid X_{nq}(a)Y_r(a)$ και άρα $Y_n(a) \mid X_{nq}(a)^2 Y_r(a)$. Αφού το $(X_{nq}(a), Y_{nq}(a))$ είναι λύση της εξίσωσης (3.2), έχουμε

$$\begin{aligned} & X_{nq}(a)^2 + aX_{nq}Y_{nq}(a) + Y_{nq}(a)^2 = 1 \\ \Rightarrow & X_{nq}(a)^2 = 1 + aX_{nq}(a)Y_{nq}(a) + Y_{nq}(a)^2 \\ \Rightarrow & X_{nq}(a)^2 Y_r(a) = (1 + aX_{nq}(a)Y_{nq}(a) + Y_{nq}(a)^2)Y_r(a) \end{aligned}$$

Δηλαδή $Y_n(a) \mid (1 + aX_{nq}(a)Y_{nq}(a) + Y_{nq}(a)^2)Y_r(a)$ άρα $Y_n(a) \mid Y_r(a)$.
Αν $r \neq 0$, τότε $Y_r(a) \neq 0$.
Οπότε $\deg(Y_n(a)) \leq \deg(Y_r(a)) \Rightarrow n - 1 \leq r - 1 \Rightarrow n \leq r$. Άτοπο.
Άρα, $r = 0$ και τότε $m = nq$. Συνεπώς, $n \mid m$.

v. • $Y_{m2^n}(a) = \frac{a^{2^n}}{a}(Y_m(a))^{2^n}$:

Βάση επαγωγής : Για $n = 0$ έχουμε $Y_m(a) = Y_m(a)$.

Επαγωγική υπόθεση : Υποθέτουμε ότι ισχύει για $n = k$, δηλαδή $Y_{m2^k}(a) = \frac{a^{2^k}}{a}(Y_m(a))^{2^k}$. (Ε.Υ.)

Επαγωγικό βήμα : Θα δείξουμε ότι ισχύει για $n = k+1$, δηλαδή $Y_{m2^{k+1}}(a) = \frac{a^{2^{k+1}}}{a}(Y_m(a))^{2^{k+1}}$.

$$\begin{aligned} Y_{m2^{k+1}}(a) =& Y_{m2^k 2}(a) = Y_{m2^k + m2^k}(a) \\ =& X_{m2^k}(a)Y_{m2^k}(a) + Y_{m2^k}(a)X_{m2^k}(a) + aY_{m2^k}(a)Y_{m2^k}(a) \\ =& a(Y_{m2^k}(a))^2 \overset{\text{Ε.Υ.}}{=} a\left(\frac{a^{2k}}{a}(Y_m(a))^{2^k}\right)^2 = a\frac{a^{2^{k+1}}}{a^2}(Y_m(a))^{2^{k+1}} \\ =& \frac{a^{2^{k+1}}}{a}(Y_m(a))^{2^{k+1}} \end{aligned}$$

• $Y_{2^n}(a) = \frac{a^{2^n}}{a}$:

Βάση επαγωγής : Για $n = 0$ έχουμε $Y_1(a) = 1$.
Από την σχέση (3.1) για $m = 1$ έχουμε

$$X_1(a) + \alpha(a)Y_1(a) = \alpha(a) \Rightarrow X_1(a) = 0, Y_1(a) = 1.$$

Επαγωγική υπόθεση : Υποθέτουμε ότι ισχύει για $n = k$, δηλαδή $Y_{2^k}(a) = \frac{a^{2^k}}{a}$. (Ε.Υ.)

Επαγωγικό βήμα : Θα δείξουμε ότι ισχύει για $n = k+1$, δηλαδή $Y_{2^{k+1}}(a) = \frac{a^{2^{k+1}}}{a}$.

$$\begin{aligned} Y_{2^{k+1}}(a) =& Y_{2^k 2}(a) = Y_{2^k+2^k}(a) \\ =& X_{2^k}(a) + Y_{2^k}(a) + Y_{2^k} X_{2^k}(a) + a Y_{2^k}(a) Y_{2^k}(a) \\ =& a(Y_{2^k}(a))^2 \overset{\text{Ε.Υ.}}{=} a\left(\frac{a^{2^k}}{a}\right)^2 = a\frac{a^{2^{k+1}}}{a^2} \\ =& \frac{a^{2^{k+1}}}{a} \end{aligned}$$

vi. Υποθέτουμε ότι $m = \pm 2^n$. Τότε $Y_m(a) = Y_{2^n}(a)$ για κάθε a. Άρα $Y_m(a+1) = Y_{2^n}(a+1)$. Από το (v) έχουμε ότι

$$Y_m(a+1) = \frac{(a+1)^{2^n}}{a+1} \Rightarrow (a+1)Y_m(a+1) = (a+1)^{2^n} = a^{2^n} + a = aY_{2^n}(a) + 1$$

Αντίστροφα, υποθέτουμε ότι $(a+1)Y_m(a+1) = aY_m(a) + 1$. Παρατηρούμε ότι $m \neq 0$, άρα αφού $Y_{-m}(a) = Y_m(a)$, μπορούμε να υποθέσουμε ότι $m > 0$. Γράφουμε $m = 2^n q$, με q περιττό. Τότε

$$\begin{aligned} (a+1)Y_m(a+1) =& (a+1)Y_{2^n q}(a+1) = (a+1)\frac{(a+1)^{2^n}}{a+1}(Y_q(a+1))^{2^n} \\ =& (a+1)^{2^n}(Y_q(a+1))^{2^n}. \end{aligned}$$

Άρα

$$\begin{aligned} ((a+1)Y_q(a+1))^{2^n} =& (a+1)Y_m(a+1) = aY_m(a) + 1 = aY_{2^n q}(a) + 1 \\ =& a\frac{a^{2^n}}{a}(Y_q(a))^{2^n} + 1 = a^{2^n}(Y_q(a))^{2^n} + 1 = (aY_q(a)+1)^{2^n}. \end{aligned}$$

Οπότε $(a+1)Y_q(a+1) = aY_q(a)+1$. Υποθέτουμε ότι $q \geq 3$. Τότε το $Y_q(a)$ είναι πολυώνυμο βαθμού $q-1$, οπότε $Y_q(a) = \gamma a^{q-1} + \beta a^{q-2} +$ (όροι μικρότερου βαθμού ως προς a) με $\gamma \neq 0$. Αλλά τότε

$$\begin{aligned} (a+1)Y_q(a+1) =& (a+1)\gamma(a+1)^{q-1} + (a+1)\beta(a+1)^{q-2} + \dots \\ =& \gamma(a+1)^q + \beta(a+1)^{q-1} + \dots \\ =& \gamma a^q + (a\gamma + \beta)a^{q-1} + \dots \end{aligned}$$

και $aY_q(a) + 1 = \gamma a^q + \beta a^{q-1} + \dots$.
Οπότε $a\gamma + \beta = \beta \Rightarrow a\gamma = 0$. Άτοπο, αφού $\gamma \neq 0$ και $a \notin F$ άρα $a \neq 0$. Οπότε $q = 1$ και $m = 2^n$.

□

Λήμμα 3.7. *Έστω F μια ακέραια περιοχή με χαρακτηριστική $p = 2$. Για κάθε $m, q \in \mathbb{Z}$ έχουμε*

$$m \mid^2 q \leftrightarrow (Y_m(t) = Y_q(t) = 0) \ \vee \ (\exists a \in F[t] \exists t, s \in \mathbb{Z} : atY_m(t) \wedge tY_q(t) = aY_t(a) \\ \wedge (a+1)Y_s(a+1) = aY_t(a) + 1).$$

Απόδειξη. Υποθέτουμε ότι $m \mid^2 q$, οπότε $q = m2^n$ για κάποιο $n \in \mathbb{N}$.
Αν $m = 0$, τότε $q = 0$ και $Y_m(t) = Y_q(t) = 0$.
Άρα υποθέτουμε ότι $m \neq 0$. Θέτουμε $a = tY_m(t)$. Τότε $a \notin F$. Επιλέγουμε $t = s = 2^n$, τότε από το Λήμμα 3.1(vi) έχουμε $(a+1)Y_s(a+1) = aY_t(a) + 1$. Από το Λήμμα 3.1$(v)$ συμπεραίνουμε ότι

$$tY_q(t) = tY_{m2^n}(t) = t\frac{t^{2^n}}{t}(Y_m(t))^{2^n} = t^{2^n}(Y_m(t))^{2^n} = (tY_m(t))^{2^n} = a^{2^n} = aY_{2^n}(a) = aY_t(a).$$

Αντίστροφα, αν $Y_m(t) = Y_q(t) = 0$ τότε $m = q = 0$, άρα $m \mid^2 q$.
Διαφορετικά, έστω $a \in F[t]$ και $t, s \in \mathbb{Z}$ έτσι ώστε

$$a = tY_m(t) \wedge tY_q(t) = aY_t(a) \wedge (a+1)Y_s(a+1) = aY_t(a) + 1.$$

Αν $m = 0$, τότε $a = tY_0(t) = 0$, και τότε $tY_q(t) = 0$, άρα $q = 0$ και $m \mid^2 q$.
Αν $m \neq 0$, τότε $a = tY_m(t) \notin F$. Αφού τα $(a+1)Y_s(a+1)$ και $aY_t(a) + 1$ έχουν τον ίδιο βαθμό, από το Λήμμα 3.1(i) έχουμε ότι $s = \pm t$, και άρα $(a+1)Y_s(a+1) = aY_s(a) + 1$. Σύμφωνα με το Λήμμα 3.1(vi) έχουμε ότι $s = \pm t = \pm 2^n$ για κάποιο $n \in \mathbb{N}$, άρα από το Λήμμα 3.1(v) έχουμε

$$aY_t(a) = aY_{\pm 2^n}(a) = aY_{2^n}(a) = a\frac{a^{2^n}}{a} = a^{2^n} = (tY_m(t))^{2^n} = t^{2^n}(Y_m(t))^{2^n} = tY_{m2^n}(t)$$

Άρα $tY_q(t) = aY_t(a) = tY_{m2^n}(t)$. Εφ'όσον τα $Y_q(t)$ και $Y_{m2^n}(t)$ έχουν τον ίδιο βαθμό έχουμε ότι $q = \pm m2^n$. Οπότε $m \mid^2 q$. □

Απόδειξη του Θεωρήματος 3.4. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $F[t]$ είναι αποφασίσιμη, δηλαδή ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $F[t]$.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ εφοδιασμένο με την πρόσθεση, την διαιρετότητα και την σχέση $\mid^2$ στην θετική υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$.
Η απεικόνιση της αναγωγής είναι $m \mapsto (X_m(t), Y_m(t))$ για $m \in \mathbb{Z}$.
Από το Λήμμα 3.6 (iii) και (iv) συμπεραίνουμε ότι η πρόσθεση και η διαιρετότητα μπορούν να οριστούν θετικά υπαρξιακά πάνω στο $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$.
Από το Λήμμα 3.7 συμπεραίνουμε ότι η σχέση $\mid^2$ μπορεί να οριστεί θετικά υπαρξιακά πάνω στο $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$.
Οπότε μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $F[t]$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιαές ερωτήσεις στο

$(\mathbb{Z}; +, |, |^2)$.
Εφ΄όσον η θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, |, |^2)$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{+, \cdot, 0, 1, t\}$ είναι μη αποφασίσιμη. □

ΚΕΦΑΛΑΙΟ 4

Θετική υπαρξιακή θεωρία στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$

4.1 Πολυωνυμικός δακτύλιος $\mathbb{C}[t]$

Θεώρημα 4.1. *Το $\mathbb{C}[t]$ έχει μη αποφασίσιμη θετική υπαρξιακή θεωρία στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$.*

Ιδέα της απόδειξης. *Για να δείξουμε ότι η θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ είναι μη αποφασίσιμη στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$, θα δείξουμε ότι μπορούμε να ορίσουμε τους φυσικούς αριθμούς στην δομή αυτή με έναν θετικό υπαρξιακό τρόπο. Τότε μπορούμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$. Αφού, όπως θα δείξουμε στη συνέχεια, η θετική υπαρξιακή θεωρία του $(\mathbb{N}; +, \cdot, 0, 1)$ είναι μη αποφασίσιμη, έπεται ότι η θετική υπαρξιακή θεωρία του $(\mathbb{C}[t]; +, \cdot, ', 0, 1, t)$ είναι μη αποφασίσιμη.*

Λήμμα 4.1. *Το 10^o πρόβλημα του Hilbert επί του $\mathbb{Z}$ στη γλώσσα $L = \{+, \cdot, 0, 1\}$ είναι ισοδύναμο με το 10^o πρόβλημα του Hilbert επί του $\mathbb{N}$ στην L.*

Απόδειξη. Υποθέτουμε ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $\mathbb{N}$.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$.
Δηλαδή θέλουμε να μεταφράσουμε τους ακεραίους στην θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$.

$$x \in \mathbb{Z} \leftrightarrow \exists x_1, x_2 \in \mathbb{N} : x = x_1 - x_2$$

Αφού το $\mathbb{Z}$ ορίζεται με έναν θετικό υπαρξιακό τύπο στη δομή $(\mathbb{N}; +, \cdot, 0, 1)$ μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{N}; +, \cdot, 0, 1)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, \cdot, 0, 1)$.

Αντίστροφα, υποθέτουμε ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $\mathbb{Z}$.

Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$.
Δηλαδή θέλουμε να μεταφράσουμε τους φυσικούς αριθμούς στην θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$.
Σύμφωνα με το Θεώρημα του Lagrange, ένας ακέραιος είναι μη μηδενικός, δηλαδή φυσικός αν και μόνο αν είναι το άθροισμα τεσσάρων τετραγώνων.

$$x \in \mathbb{N} \leftrightarrow \exists x_1, x_2, x_3, x_4 \mathbb{Z} : x = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

Αφού το $\mathbb{N}$ ορίζεται με έναν θετικό υπαρξιακό τύπο στη δομή $(\mathbb{Z}; +, \cdot, 0, 1)$ μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, \cdot, 0, 1)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{N}; +, \cdot, 0, 1)$. □

Αφού η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ είναι μη αποφασίσιμη, έπεται ότι η θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ είναι μη αποφασίσιμη.

Λήμμα 4.2. *Έστω x λύση της διαφορικής εξίσωσης $tx' = nx$ τότε $x(1) = 1 \Leftrightarrow \exists y\ (t-1)y = x - 1$.*

Απόδειξη. Αφού το x είναι λύση της $tx' = nx$ έχουμε ότι $x = \lambda t^n$. Αν $x(1) = 1$ τότε $\lambda = 1$, δηλαδή $x = t^n$, τότε

$$x - 1 = t^n - 1 = (t-1)(t^{n-1} + \cdots + 1) \Rightarrow t - 1 \mid x - 1.$$

Οπότε $\exists y\ (t-1)y = x - 1$.

Αντίστροφα, υποθέτουμε ότι $\exists y\ (t-1)y = x - 1$, δηλαδή $t - 1 \mid x - 1$. Τότε

$$\begin{aligned} t - 1 \mid \lambda t^n - 1 \Rightarrow t - 1 \mid \lambda t^n - \lambda + \lambda - 1 \Rightarrow t - 1 \mid \lambda(t^n - 1) + \lambda - 1 \\ \Rightarrow t - 1 \mid \lambda(t-1)(t^{n-1} + \cdots + 1) + \lambda - 1. \end{aligned}$$

Άρα πρέπει $\lambda - 1 = 0 \Rightarrow \lambda = 1$. Οπότε $x(1) = 1$. □

Λήμμα 4.3. *$n \in \mathbb{N}$ αν και μόνο αν στο $\mathbb{C}[t]$ ισχύουν τα εξής:*

$$n' = 0 \quad \wedge \quad \exists x\ tx' = nx \quad \wedge \quad \exists y\ (t-1)y = x - 1.$$

Απόδειξη. Αν το n είναι ένας φυσικός αριθμός, τότε είναι σταθερός και άρα η παράγωγος n' είναι 0. Αν $x = t^n$, τότε $x' = nt^{n-1} \Rightarrow tx' = nt^n \Rightarrow tx' = nx$.

Αντίστροφα, υποθέτουμε ότι $n \in \mathbb{C}$ και ότι υπάρχει ένα $x \in \mathbb{C}[t]$ με $tx' = nx$ και $\exists y(t-1)y = x - 1$, δηλαδή σύμφωνα με το Λήμμα (4.2) $x(1) = 1$. Η λύση της διαφορικής εξίσωσης $tx' = nx$ είναι $x = \lambda t^n$. Από την συνθήκη $x(1) = 1$ έχουμε $x = t^n$. Αφού $x = t^n \in \mathbb{C}[t]$, πρέπει $n \in \mathbb{N}$. □

Απόδειξη του Θεωρήματος 4.1. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ είναι αποφασίσιμη, δηλαδή ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο $\mathbb{C}[t]$.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{N}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$.
Δηλαδή θέλουμε να μεταφράσουμε τους φυσικούς αριθμούς στην θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$.
Σύμφωνα με το Λήμμα 4.3 μπορούμε να ορίσουμε το $\mathbb{N}$ με έναν υπαρξιακό τύπο στην δομή $(\mathbb{C}[t]; +, \cdot, ', 0, 1, t)$.
Οπότε μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{C}[t]; +, \cdot, ', 0, 1, t)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{N}; +, \cdot, 0, 1)$.
Εφ'όσον η θετική υπαρξιακή θεωρία του $(\mathbb{N}; +, \cdot, 0, 1)$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του $\mathbb{C}[t]$ στη γλώσσα $\{+, \cdot, ', 0, 1, t\}$ είναι μη αποφασίσιμη. □

4.2 Δακτύλιοι $\mathrm{EXP}(\mathbb{C})$ και $\mathrm{EXP}(\mathbb{C})[t]$

Έστω R οποιοσδήποτε από τους δακτυλίους $\mathrm{EXP}(\mathbb{C})$ και $\mathrm{EXP}(\mathbb{C})[t]$.

Θεώρημα 4.2. *Ο δακτύλιος R έχει μη αποφασίσιμη θετική υπαρξιακή θεωρία στη γλώσσα $\{+, \cdot, ', 0, 1\}$.*

Ιδέα της απόδειξης. *Για να δείξουμε ότι η θετική υπαρξιακή θεωρία του R είναι μη αποφασίσιμη στη γλώσσα $\{+, \cdot, ', 0, 1\}$, θα δείξουμε ότι μπορούμε να ορίσουμε τους ακεραίους στην δομή αυτή με έναν θετικό υπαρξιακό τρόπο. Τότε μπορούμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του R στη γλώσσα $\{+, \cdot, ', 0, 1\}$. Αφού η θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, \cdot, 0, 1)$ είναι μη αποφασίσιμη, έπεται ότι η θετική υπαρξιακή θεωρία του $(R; +, \cdot, ', 0, 1)$ είναι μη αποφασίσιμη.*

Λήμμα 4.4. *Στον δακτύλιο R ισχύει ότι, υπάρχουν $c, d \neq 0$ έτσι ώστε*

$$\lambda \in \mathbb{Z} \Leftrightarrow ce^t - 1 \mid de^{\lambda t} - 1.$$

Απόδειξη. Υποθέτουμε ότι $\lambda \in \mathbb{Z}$.
Επιλέγουμε $d = c^\lambda$.

- $\lambda = 0$: Τότε έχουμε $c^\lambda e^{\lambda t} - 1 = 1 - 1 = 0$. Οπότε $ce^t - 1 \mid c^\lambda e^{\lambda t} - 1$.
- $\lambda > 0$:

$$\sum_{i=0}^{\lambda-1} (ce^t)^i = \frac{(ce^t)^\lambda - 1}{ce^t - 1} \Rightarrow (ce^t)^\lambda - 1 = (ce^t - 1) \sum_{i=0}^{\lambda-1} (ce^t)^i.$$

Οπότε αν το λ είναι ένας θετικός ακέραιος έχουμε ότι $ce^t - 1 \mid c^\lambda e^{\lambda t} - 1$.

- $\lambda < 0$:

$$\sum_{i=0}^{k-1}((ce^t)^{-1})^i = \frac{\left(\frac{1}{ce^t}\right)^\lambda - 1}{\frac{1}{ce^t} - 1} = \frac{\frac{1-(ce^t)^\lambda}{(ce^t)^\lambda}}{\frac{1-ce^t}{ce^t}} = \frac{ce^t}{(ce^t)^\lambda}\frac{1-(ce^t)^\lambda}{1-ce^t} = \frac{1}{(ce^t)^{\lambda-1}}\frac{(ce^t)^\lambda - 1}{ce^t - 1}$$

$$\Rightarrow (ce^t)^\lambda - 1 = (ce^t - 1)(ce^t)^{\lambda-1}\sum_{i=0}^{\lambda-1}((ce^t)^{-1})^i$$

Οπότε αν το λ είναι ένας αρνητικός ακέραιος έχουμε ότι $ce^t - 1 \mid c^\lambda e^{\lambda t} - 1$.

Επομένως, σε κάθε περίπτωση έχουμε ότι $ce^t - 1 \mid c^\lambda e^{\lambda t} - 1$.

Αντίστροφα, υποθέτουμε ότι $ce^t - 1 \mid de^{\lambda t} - 1$. Αφού κάθε μη μηδενικός μιγαδικός αριθμός μπορεί να γραφεί σε εκθετική μορφή, θέτουμε $c = e^{-\beta}$ και $d = e^{-\gamma}$, όπου $\beta, \gamma \in \mathbb{C}$. Οπότε

$$ce^t - 1 = e^{-\beta}e^t - 1 = e^{-\beta}\left(e^t - e^\beta\right)$$
$$de^{\lambda t} - 1 = e^{-\gamma}e^{\lambda t} - 1 = e^{-\gamma}\left(e^{\lambda t} - e^\gamma\right)$$

Άρα

$$ce^t - 1 \mid de^{\lambda t} - 1 \iff e^t - e^\beta \mid e^{\lambda t} - e^\gamma$$

Από την διαιρετότητα έχουμε ότι κάθε λύση της $e^t - e^\beta = 0$ είναι επίσης λύση της $e^{\lambda t} - e^\gamma = 0$. Παρατηρούμε οτι τα $\alpha = \beta$ και $\alpha = \beta + 2\pi i$ είναι λύσεις της εξίσωσης $e^t - e^\beta = 0$.
Αφού το $\alpha = \beta$ είναι επίσης λύση της $e^{\lambda t} - e^\gamma$ έχουμε

$$e^{\lambda\alpha} - e^\gamma = 0 \text{ άρα } e^{\lambda\beta} - e^\gamma = 0$$
$$\text{άρα } e^{\lambda\beta} = e^\gamma \ .$$

Αφού το $\alpha = \beta + 2\pi i$ είναι επίσης λύση της $e^{\lambda t} - e^\gamma$ έχουμε

$$e^{\lambda\alpha} - e^\gamma = 0 \text{ άρα } e^{\lambda(\beta+2\pi i)} - e^\gamma = 0$$
$$\text{άρα } e^{\lambda\beta}e^{2\lambda\pi i} - e^\gamma = 0$$
$$\text{άρα } e^\gamma e^{2\lambda\pi i} - e^\gamma = 0$$
$$\text{άρα } e^\gamma(e^{2\lambda\pi i} - 1) = 0$$
$$\text{άρα } e^{2\lambda\pi i} = 1$$
$$\text{άρα } \lambda \in \mathbb{Z} \ .$$

□

Απόδειξη του Θεωρήματος 4.2. Υποθέτουμε ότι η θετική υπαρξιακή θεωρία του R είναι αποφασίσιμη, δηλαδή ότι υπάρχει αλγόριθμος ο οποίος απαντάει σε θετικές υπαρξιακές ερωτήσεις πάνω στο R.
Θέλουμε να ανάγουμε την θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\{+, \cdot, 0, 1\}$ στην θετική υπαρξιακή θεωρία του R στη γλώσσα $\{+, \cdot, ', 0, 1\}$.
Δηλαδή θέλουμε να μεταφράσουμε τους ακεραίους στην θετική υπαρξιακή θεωρία του R στη γλώσσα $\{+, \cdot, ', 0, 1\}$.
Σύμφωνα με το Λήμμα 4.4 έχουμε ότι $\lambda \in \mathbb{Z}$ αν και μόνο αν $ce^t - 1 \mid de^{\lambda t} - 1$, δηλαδή αν και μόνο αν $(\exists h)\left((ce^t - 1)h = de^{\lambda t} - 1\right)$.
Μπορούμε να ορίσουμε το ce^t ως λύση της διαφορικής εξίσωσης $x' = x$ και το $de^{\lambda t}$ ως λύση της διαφορικής εξισωσης $y' = \lambda y$. Εξασφαλίζουμε ότι τα x και y είναι μη μηδενικά με τον τύπο $(\exists w)(xw = 1) \ \wedge \ (\exists u)(yu = 1)$.
Οπότε έχουμε

$$\lambda \in \mathbb{Z} \leftrightarrow \exists x \exists y \exists h \exists w \exists u \left(x' = x \ \wedge \ y' = \lambda y \ \wedge \ (x-1)h = y - 1 \ \wedge \ xw = 1 \ \wedge \ yu = 1\right).$$

Δηλαδή μπορούμε να ορίσουμε το $\mathbb{Z}$ με έναν υπαρξιακό τύπο στην δομή $(R; +, \cdot, ', 0, 1)$.
Οπότε μπορούμε να μετατρέψουμε τον αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(R; +, \cdot, ', 0, 1)$ σε έναν αλγόριθμο που απαντάει σε θετικές υπαρξιακές ερωτήσεις στο $(\mathbb{Z}; +, \cdot, 0, 1)$.
Εφ'όσον η θετική υπαρξιακή θεωρία του $(\mathbb{Z}; +, \cdot, 0, 1)$ είναι μη αποφασίσιμη, καταλήγουμε σε άτοπο.
Οπότε η θετική υπαρξιακή θεωρία του R στη γλώσσα $\{+, \cdot, ', 0, 1\}$ είναι μη αποφασίσιμη. $\square$

ΚΕΦΑΛΑΙΟ 5

Υπαρξιακή θεωρία στη γλώσσα $\{+,', 0, 1\}$

Στο κεφάλαιο αυτό θα εξετάσουμε την αποφασισιμότητα της θεωρίας των δακτυλίων $\mathbb{C}[t]$ και $\mathrm{EXP}(\mathbb{C})[t]$ αν έχουμε τη γλώσσα $L = \{+,', 0, 1\}$.

Ερώτηση 5.1. *Είναι αποφασίσιμη η θεωρία του πολυωνυμικού δακτυλίου $\mathbb{C}[t]$ στη γλώσσα $\{+,', 0, 1\}$; Για την ακρίβεια, επιδέχεται κατασκευαστική απαλοιφή ποσοδεικτών;*

Ερώτηση 5.2. *Είναι αποφασίσιμη η θεωρία του δακτυλίου των εκθετικών αθροισμάτων και πολυωνύμων $\mathrm{EXP}(\mathbb{C})[t]$ στη γλώσσα $\{+,', 0, 1\}$; Για την ακρίβεια, επιδέχεται κατασκευαστική απαλοιφή ποσοδεικτών;*

Αρχικά θα εξετάσουμε την ύπαρξη λύσης των γραμμικών διαφορικών εξισώσεων στους δακτυλίους $\mathbb{C}[t]$ και $\mathrm{EXP}(\mathbb{C})[t]$ και θα αναφερθούμε στην έννοια της απαλοιφής ποσοδεικτών.

5.1 Ύπαρξη λύσης διαφορικών εξισώσεων

Μια γραμμική διαφορική εξίσωση βαθμού n με σταθερούς συντελεστές είναι της μορφής

$$\mathcal{L}x := \sum_{k=0}^{n} \alpha_k x^{(k)}(t) = f(t)$$

με σταθερές α_k και μια συνάρτηση f.
Έστω x_p μια ειδική λύση, δηλαδή μια λύση της εξίσωσης $\mathcal{L}x = f(t)$. Αν $x_p^\star$ μια άλλη ειδική λύση, τότε η $x_H = x_p - x_p^\star$ είναι λύση της ομογενούς εξίσωσης, $\mathcal{L}x = 0$. Επιπλέον, για κάθε λύση x_H της ομογενούς εξίσωσης, η $x_H + x_p$ είναι προφανώς λύση της αρχικής εξίσωσης.

Συμπεραίνουμε ότι το σύνολο όλων των λύσεων της αρχικής εξίσωσης μπορεί να βρεθεί βρίσκοντας μια λύση και προσθέτοντας σε αυτήν την γενική λύση της ομογενούς εξίσωσης.

Στον δακτύλιο $\mathbb{C}[t]$ η συνάρτηση f θα έχει τη μορφή $\sum_{\ell=1}^{m} C_\ell t^\ell$, όπου $C_\ell \in \mathbb{C}$.
Στον δακτύλιο $\mathrm{EXP}(\mathbb{C})[t]$ η συνάρτηση f θα έχει τη μορφή $\sum_{\beta,\ell} C_{\beta,\ell} t^\ell e^{\beta t}$, όπου ο υποδείκτης ℓ διατρέχει ένα πεπερασμένο σύνολο μη αρνητικών ακεραίων και το β ένα πεπερασμένο σύνολο μιγαδικών.

5.1.1 Λύση της ομογενούς γραμμικής εξίσωσης με σταθερούς συντελεστές

Θεωρούμε την ομογενή γραμμική εξίσωση με σταθερούς συντελεστές

$$\sum_{k=0}^{n} \alpha_k x^{(k)}(t) = 0 \tag{5.1}$$

την οποία θα συμβολίσουμε ως $\mathcal{L}x = 0$. Η γενική λύση αυτής της εξίσωσης εξαρτάται από τις ρίζες $\lambda_1, \ldots, \lambda_n$ της χαρακτηριστικής εξίσωσης $\sum_{k=0}^{n} \alpha_k \lambda^k = 0$.
Για κάθε ρίζα λ με πολλαπλότητα $M(\lambda) \geq 1$, οι

$$e^{\lambda t}, te^{\lambda t}, t^2 e^{\lambda t}, \ldots, t^{M(\lambda)-1} e^{\lambda t}$$

είναι $M(\lambda)$ γραμμικώς ανεξάρτητες λύσεις της $Lx(t) = 0$. Για κάθε $\lambda \in \{\lambda_1, \ldots, \lambda_n\}$ θεωρούμε τη συνάρτηση $x^{[\lambda]} = \sum_{i=0}^{M(\lambda)-1} c_{\lambda,i} t^i e^{\lambda t}$. Τότε η γενική λύση της (5.1) είναι

$$x_H(t) = \sum_{\lambda} x^{[\lambda]}.$$

Πολυωνυμικός δακτύλιος $\mathbb{C}[t]$

Η διαφορική εξίσωση (5.1) στον δακτύλιο $\mathbb{C}[t]$ έχει λύση αν και μόνο αν τουλάχιστον μία ρίζα της χαρακτηριστικής εξίσωσης είναι ίση με 0.

Πράγματι, η (5.1) έχει λύση στο $\mathbb{C}[t]$ αν και μόνο αν $x_H(t) = \sum_{\lambda} \sum_{i=0}^{M(\lambda)-1} c_{\lambda,i} t^i e^{\lambda t} \in \mathbb{C}[t]$. Αυτό συμβαίνει αν και μόνο αν $\lambda = 0$ για τουλάχιστον ένα λ, δηλαδή $\alpha_0 = 0$.

Δακτύλιος $\mathrm{EXP}(\mathbb{C})[t]$

Η διαφορική εξίσωση (5.1) στον δακτύλιο $\mathrm{EXP}(\mathbb{C})[t]$ έχει πάντα n, γραμμικώς ανεξάρτητες λύσεις.

Είναι γνωστό ότι:
Πρόταση: Η γραφή μίας συνάρτησης του $\mathrm{EXP}(\mathbb{C})[t]$ στη μορφή της $\sum_{\lambda,i} c_{\lambda,i} t^i e^{\lambda t}$, για λ ανα δύο διαφορετκά, είναι μοναδική.

Το εξής Λήμμα έπεται εύκολα από τα παραπάνω:
Αλγοριθμική επιλυσιμότητα συστημάτων ομογενών εξισώσεων και ανισώσεων

Λήμμα 5.1. *Έστω R ένας από τους δακτυλίους $\mathbb{C}[t]$, $\mathrm{EXP}(\mathbb{C})[t]$. Υπάρχει αλγόριθμος ο οποίος, δεδομένων εξίσωσης $\mathcal{L}x = 0$ και ανισώσεων $\mathcal{L}_j x \neq 0$ για $j = 1, \ldots, n$, αποφασίζει το κατά πόσον το σύστημα $\mathcal{L}x = 0 \wedge \mathcal{L}_j x \neq 0$ έχει ή δεν έχει μη μηδενικές λύσεις στον R.*

5.1.2 Λύση της μη-ομογενούς γραμμικής εξίσωσης με σταθερούς συντελεστές

Θεωρούμε την μη-ομογενή γραμμική εξίσωση

$$\sum_{k=0}^{n} \alpha_k x^{(k)}(t) = f \ . \tag{5.2}$$

Έστω ότι $f = \sum_{\ell=1}^{m} f_\ell$, όπου f_ℓ συναρτήσεις έτσι ώστε η παρακάτω m μη-ομογενείς εξισώσεις

$$\mathcal{L}x = f_\ell, \quad \ell = 1, 2, \ldots, m.$$

έχουν λύσεις $x_1, x_2, \ldots, x_m$, αντιστοίχως. Τότε μια ειδική λύση x_p της (5.2) είναι η $x_1 + x_2 + \cdots + x_m$.

Πολυωνυμικός δακτύλιος $\mathbb{C}[t]$

Θεωρούμε την εξίσωση

$$\mathcal{L}x = t^\ell \tag{5.3}$$

όπου ℓ μη αρνητικός ακέραιος. Διακρίνουμε τις εξής περιπτώσεις:

i. Το $\lambda = 0$ δεν είναι ρίζα της χαρακτηριστικής εξίσωσης της ομογενούς εξίσωσης.
   Υπάρχει λύση της μορφής
   $$x(t) = \sum_{i=0}^{\ell} \gamma_i t^i.$$

ii. Το $\lambda = 0$ είναι ρίζα της χαρακτηριστικής εξίσωσης της ομογενούς εξίσωσης με πολλαπλότητα M.

Υπάρχει λύση της μορφής

$$x(t) = t^M \sum_{i=0}^{\ell} \gamma_i t^i.$$

Σε κάθε περίπτωση, αντικαθιστούμε στην (5.3) και εξισώνοντας τους αντίστοιχους συντελεστές προκύπτει ένα γραμμικό σύστημα εξισώσεων, το οποίο μπορεί να γραφεί σε μορφή πίνακα.
Ο πίνακας συντελεστών για τους αγνώστους γ_i είναι ένας διαγώνιος πίνακας, ο οποίος δεν έχει μηδενικά στη διαγώνιο. Οπότε τα γ_i μπορούν να καθοριστούν μονοσήμαντα.

Συνεπώς, μια διαφορική εξίσωση $\mathcal{L}x = f$ στον δακτύλιο $\mathbb{C}[t]$ έχει πάντα μία ειδική λύση αν $f \neq 0$.

Δακτύλιος $\mathrm{EXP}(\mathbb{C})[t]$

Θεωρούμε την εξίσωση

$$\mathcal{L}x = t^d e^{\beta t}. \tag{5.4}$$

όπου d είναι ένας μη αρνητικός ακέραιος και $\beta \in \mathbb{C}$. Διακρίνουμε τις εξής περιπτώσεις:

i. Το β δεν είναι ρίζα της χαρακτηριστικής εξίσωσης της ομογενούς εξίσωσης.

Υπάρχει λύση της μορφής

$$x(t) = e^{\beta t} \sum_{i=0}^{\ell} \gamma_i t^i.$$

ii. Το β είναι ρίζα της χαρακτηριστικής εξίσωσης της ομογενούς εξίσωσης με πολλαπλότητα M.

Υπάρχει λύση της μορφής

$$x(t) = e^{\beta t} t^M \sum_{i=0}^{\ell} \gamma_i t^i.$$

Σε κάθε περίπτωση, αντικαθιστούμε στην (5.4) και εξισώνοντας τους αντίστοιχους συντελεστές προκύπτει ένα γραμμικό σύστημα εξισώσεων, το οποίο μπορεί να γραφεί σε μορφή πίνακα.
Ο πίνακας συντελεστών για τους αγνώστους γ_i είναι ένας διαγώνιος πίνακας, ο οποίος δεν έχει μηδενικά στη διαγώνιο. Οπότε τα γ_i μπορούν να καθοριστούν μονοσήμαντα.

Συνεπώς, μια διαφορική εξίσωση στον δακτύλιο $\mathrm{EXP}(\mathbb{C})[t]$ έχει πάντα μία ειδική λύση.

Έχουμε αποδείξει ότι:

Λήμμα 5.2. *Μια διαφορική εξίσωση*

$$\alpha_n x^{(n)} + \cdots + \alpha_0 x = f$$

με σταθερούς συντελεστές $\alpha_i \in \mathbb{C}[t], i = 0, \ldots n$ *και* $\alpha_n \neq 0$ *έχει πάντα λύση στον δακτύλιο* $\mathbb{C}[t]$ *αν* $f \in \mathbb{C}[t] \setminus \{0\}$. *Αν* $f = 0$ *τότε η διαφορική εξίσωση έχει λύση αν και μόνο αν τουλάχιστον μία ρίζα της χαρακτηριστικής εξίσωσης είναι ίση με* 0.

Λήμμα 5.3. *Μια διαφορική εξίσωση*

$$\alpha_n x^{(n)} + \cdots + \alpha_0 x = f$$

με σταθερούς συντελεστές $\alpha_i \in EXP(\mathbb{C})[t], i = 0, \ldots n$ *και* $\alpha_n \neq 0$ *έχει πάντα λύση στον δακτύλιο* $EXP(\mathbb{C})[t]$ *αν* $f \in EXP(\mathbb{C})[t]$.

5.2 Η έννοια της απαλοιφής ποσοδεικτών

Έστω L μια γλώσσα. Ένα σύνολο απαλοιφής για την θεωρία T είναι ένα σύνολο F από τύπους που ορίζονται από την L τέτοιο ώστε κάθε τύπος $\phi(\overline{x})$ της L είναι ισοδύναμος στην T με έναν κατάλληλο λογικό (Boolean) συνδυασμό από τύπους του F.

Προφανώς το σύνολο όλων των τύπων της L είναι ένα σύνολο απαλοιφής για την T.

Ορισμός 5.1. *Έστω* T *μια θεωρία στη γλώσσα* L. HT *επιδέχεται απαλοιφή ποσοδεικτών στην* L *αν και μόνο αν κάθε τύπος* $\phi(\overline{x})$ *της* L *είναι ισοδύναμος στην* T *με έναν τύπο* $\psi(\overline{x})$ *της* L, *ο οποίος είναι ελεύθερος ποσοδεικτών, δηλαδή με έναν κατάλληλο λογικό συνδυασμό ατομικών τύπων.*

Κάθε τύπος μπορεί να γραφεί στη μορφή

$$Q_1 x_1 \ldots Q_n x_n \ \phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

όπου $Q_i \in \{\forall, \exists\}$ και ϕ ένας τύπος ελεύθερος ποσοδεικτών.
Ένας τύπος της μορφής $\forall x \phi$ γράφεται ισοδύναμα ως $\neg \exists x \neg \phi$.
Επίσης έχουμε ότι $\exists x(\phi_1 \vee \phi_2) \leftrightarrow \exists x \phi_1 \vee \exists x \phi_2$.
Οπότε μια θεωρία T επιδέχεται απαλοιφή ποσοδεικτών στην L αν και μόνο αν για κάθε τύπο της μορφής

$$\exists x \phi(x, \overline{y}),$$

όπου ϕ μια σύζευξη ατομικών τύπων και άρνηση ατομικών τύπων, υπάρχει ένας ισοδύναμος τύπος $\psi(\overline{y})$, ο οποίος είναι ελεύθερος ποσοδεικτών.

Η απαλοιφή ποσοδεικτών μπορεί να χρησιμοποιηθεί ως τεχνική απόδειξης της αποφασισιμότητας. Έχουμε ότι μια θεωρία T είναι αποφασίσιμη αν υπάρχει αλγόριθμος ο οποίος

ελέγχει σε πεπερασμένα βήματα, για κάθε πρόταση α στη γλώσσα L της T, αν η α ανήκει στην T ή όχι. Υποθέτουμε ότι το F είναι ένα σύνολο απαλοιφής για την T και υπάρχουν τα παρακάτω:

1. μια διαδικασία η οποία μεταφράζει κάθε πρόταση της L σε έναν ισοδύναμο λογικό συνδυασμό προτάσεων του F στην T (ή ακόμα μια αναγωγή κάθε τύπου της L σε έναν ισοδύναμο λογικό συνδυασμό τύπων του F στην T)

2. ένας αλγόριθμος ο οποίος αποφασίζει, για κάθε λογικό συνδυασμό α από προτάσεις του F, αν το α ανήκει ή όχι στην T.

Τότε η T είναι αποφασίσιμη. Εφαρμόζοντας διαδοχικά τις δύο προηγούμενες διαδικασίες έχουμε έναν αλγόριθμο απόφασης.

5.2.1 Ορισμένα αποτελέσματα απαλοιφής στους δακτυλίους $\mathbb{C}[t]$, $EXP(\mathbb{C})[t]$ στη γλώσσα $\{+,', 0, 1\}$

Προσπαθήσαμε να βρούμε μια απαλοιφή ποσοδεικτών στους δακτυλίους $\mathbb{C}[t]$ και $EXP(\mathbb{C})[t]$ στη γλώσσα $L = \{+,', 0, 1\}$. Η προσπάθειά μας δεν ολοκληρώθηκε αλλά έχουμε ορισμένα αποτελέσματα τα οποία παρουσιάζουμε εδώ.

Εργαζόμαστε στη γλώσσα $L = \{+,', 0, 1\}$.

Με τον όρο "διαφορικός τελεστής" θα εννούμε γραμμικώς ομογενής διαφορικός τελεστής που είναι όρος της γλώσσας L.

Λήμμα 5.4. *Έστω οτι $\mathcal{L}_1, \dots \mathcal{L}_n$ είναι μη μηδενικοί διαφορικοί τελεστές και $f_1, \dots, f_n$ όροι της L. Τότε υπάρχει ένας μη μηδενικός διαφορικός τελεστής $\mathcal{L}$, με τάξη μικρότερη ή ίση προς το μέγιστο του συνόλου $\{$τάξη του $\mathcal{L}_1, \dots,$ τάξη του $\mathcal{L}_n\}$, ένας όρος h της L και τύπος ϕ_0, χωρίς ποσοδείκτες και στον οποίο δεν εμφανίζεται η μεταβλητή x τέτοια ώστε, σε καθέναν από τους δακτυλίους $\mathbb{C}[t]$, $EXP(\mathbb{C})[t]$, οι εξής τύποι είναι ισοδύναμοι:*

$$\bigwedge_{i=1}^{n} \mathcal{L}_i x = f_i$$

και

$$\mathcal{L}x = h \wedge \phi_0 \ .$$

Επιπλέον, υπάρχει ένας αλγόριθμος γιά την κατασκευή των $\mathcal{L}$, h και ϕ_0 από τα $\mathcal{L}_i$, για $i = 1, \dots, n$, f και g.

Λήμμα 5.5. *Έστω οτι $\mathcal{L}_1$ και $\mathcal{L}_2$ είναι μη μηδενικοί διαφορικοί τελεστές και f και g όροι της L. Σε καθέναν από τους δακτυλίους $\mathbb{C}[t]$, $EXP(\mathbb{C})[t]$, θεωρούμε τον τύπο*

$$\sigma(x): \ \mathcal{L}_1 x = f \wedge \mathcal{L}_2 x \neq g$$

όπου f και g όροι της γλώσσας L. Ο τύπος $\sigma(x)$ είναι ισοδύναμος με έναν τύπο μιας των παρακάτω μορφών

(α)

$$\mathcal{L}_1 x = f \wedge \mathcal{L} x \neq h$$

όπου h ένας όρος της L και $\mathcal{L}$ είναι ένας τελεστής με τάξη μικρότερη της τάξης του $\mathcal{L}_1$.

(β)

$$\mathcal{L}_1 x = f \wedge \phi_0$$

όπου ϕ_0 ένας τύπος χωρίς ποσοδείκτες, στον οποίο δεν εμφανίζεται η μεταβλητή x.

Επιπλέον, υπάρχει ένας αλγόριθμος γιά την κατασκευή των $\mathcal{L}$, h και ϕ_0 από τα $\mathcal{L}_1$, $\mathcal{L}_2$, f και g.

Λήμμα 5.6. *Έστω R οποιοσδήποτε από τους δακτυλίους $\mathbb{C}[t]$ ή $EXP(\mathbb{C})[t]$. Έστωσαν μη μηδενικοί διαφορικοί τελεστές $\mathcal{L}$ και $\mathcal{L}_1 \dots \mathcal{L}_n$ και έστωσαν $x_1, \dots x_n$ μεταβλητές. Έστω οτι η τάξη κάθε $\mathcal{L}_i$ είναι μικρότερη της τάξης του $\mathcal{L}$. Θεωρούμε τον τύπο*

$$\theta \ : \ \bigwedge_{i=1}^{n} \mathcal{L}(x) = \mathcal{L}(x_i) \ \wedge \ \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq \mathcal{L}_i(x_i) \ .$$

Αν το σύστημα $\mathcal{L}x = 0 \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq 0$ έχει μη μηδενικές λύσεις στον R, τότε ο τύπος $\exists x \ \theta$ είναι ισοδύναμος με $0 = 0$. Αλλοιώς, είναι ισοδύναμος με $0 = 1$.

5.2.2 Απαλοιφή υπαρξιακού ποσοδείκτη για τύπους με καμία ή μια ανίσωση

Σε καθέναν από τους δακτυλίους $\mathbb{C}[t]$ και $EXP(\mathbb{C})[t]$, αν μπορούμε να απαλείψουμε τον υπαρξιακό ποσοδείκτη από έναν, οποιονδήποτε, τύπο της μορφής

$$\exists x \ \phi(x) : \exists x \ \left(\bigwedge_{j=1}^{m} \tilde{\mathcal{L}}_j x = f_j \ \wedge \ \bigwedge_{j=1}^{n} \mathcal{L}_j x \neq g_j \ \wedge \ \phi_0 \right) \ ,$$

όπου στο ϕ_0 δεν εμφανίζεται η μεταβλητή x και είναι ελεύθερο ποσοδεικτών, τότε θα έχουμε δείξει ότι η θεωρία του δακτυλίου στη γλώσσα L επιδέχεται απαλοιφή ποσοδεικτών.

Έχουμε μια μέθοδο για να πετύχουμε αυτή την απαλοιφή αν ο αριθμός των ανισώσεων είναι 0 ή 1. Η μέθοδός μας δεν γενικεύεται για περισσότερες ανισώσεις με προφανή τρόπο.

Θεωρούμε το παραπάνω σύστημα για $n = 1$, δηλαδή

$$\exists x \ \phi(x) : \exists x \ \left(\bigwedge_{j=1}^{m} \tilde{\mathcal{L}}_j x = f_j \ \wedge \ \mathcal{L}_1 x \neq g_1 \ \wedge \ \phi_0 \right) \ .$$

Με βάση το Λήμμα 5.4 μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, οτι το σύστημα, εκτός από μία ανίσωση, έχει μόνο μία εξίσωση, δηλαδή $m = 1$ και ένα καινούριο ϕ_0.

Ο νέος ισοδύναμος τύπος είναι

$$\exists x \ \phi(x) : \exists x \ \left(\mathcal{L}x = f \ \wedge \ \mathcal{L}_1 x \neq g_1 \ \wedge \ \phi_0 \right) . \tag{5.5}$$

Σύμφωνα με το Λήμμα 5.5 μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι η τάξη του $\mathcal{L}_1$ είναι μικρότερη από την τάξη του $\mathcal{L}$.

Ο τύπος $\exists x\ (\mathcal{L}x = f\ \wedge\ \mathcal{L}_1 x \neq g_1)$ γράφεται ισοδύναμα ως

$$\begin{gathered}\neg\,(\exists y)\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)\ \wedge\ (\exists x)\,(\mathcal{L}x = f)\\ \vee\\ (\exists y)\left[\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)\ \wedge\ (\exists x)\,(\mathcal{L}x = f\ \wedge\ \mathcal{L}_1 x \neq g_1)\,\right]\end{gathered} \tag{5.6}$$

Θεωρούμε τον τύπο

$$\neg\,(\exists y)\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)\ \wedge\ (\exists x)\,(\mathcal{L}x = f)\ . \tag{5.7}$$

Ο τύπος $\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1$, σύμφωνα με το Λήμμα 5.4 ισοδυναμεί με έναν τύπο της μορφής $\tilde{\mathcal{L}}_j y = h\ \wedge\ \tilde{\phi}_0$. Δηλαδή προκύπτει ο ισοδύναμος τύπος

$$\neg\,(\exists y)\left(\tilde{\mathcal{L}}_j y = h\ \wedge\ \tilde{\phi}_0\right)\ \wedge\ (\exists x)\,(\mathcal{L}x = f)\,.$$

Στη συνέχεια, θεωρούμε τον τύπο

$$(\exists y)\left[\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)\ \wedge\ (\exists x)\,(\mathcal{L}x = f\ \wedge\ \mathcal{L}_1 x \neq g_1)\,\right],$$

ο οποίος είναι ισοδύναμος με τον τύπο

$$(\exists y)\left[\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)\ \wedge\ (\exists x)\,(\mathcal{L}x = \mathcal{L}y\ \wedge\ \mathcal{L}_1 x \neq \mathcal{L}_1 y)\,\right]. \tag{5.8}$$

Σύμφωνα με το Λήμμα 5.6 ο τύπος $(\exists x)\,(\mathcal{L}x = \mathcal{L}y\ \wedge\ \mathcal{L}_1 x \neq \mathcal{L}_1 y)$ είναι ισοδύναμος με $0 = 0$ αν το σύστημα $\mathcal{L}x = 0 \wedge \mathcal{L}_1 x \neq 0$ έχει μη μηδενικές λύσεις στον δακτύλιο. Διαφορετικά, είναι ισοδύναμος με $0 = 1$.
Αν είναι ισοδύναμος με $0 = 1$, τότε και ο τύπος (5.8) είναι ισοδύναμος με $0 = 1$. Διαφορετικά, ο τύπος (5.8) είναι ισοδύναμος με $(\exists y)\,(\mathcal{L}y = f\ \wedge\ \mathcal{L}_1 y = g_1)$. Σύμφωνα με το Λήμμα 5.4 ο τύπος αυτός ισοδυναμεί με μία εξίσωση και έναν τύπο $\bar{\phi}_0$, ο οποίος είναι ελεύθερος ποσοδεικτών και δεν περιέχει η μεταβλητή x, δηλαδή ισοδυναμεί με τον τύπο $(\exists y)(\tilde{\mathcal{L}}_1 y = h\ \wedge\ \bar{\phi}_0)$.

Οπότε σε κάθε περίπτωση καταλήγουμε σε τύπους της μορφής $(\exists z)(\hat{\mathcal{L}}z = \hat{w})$.
Αν $w \neq 0$ τότε ο τύπος αυτός στους δακτυλίους $\mathbb{C}[t]$ και $EXP(\mathbb{C})[t]$ είναι ισοδύναμος με $0 = 0$.
Αν $w = 0$ τότε ο τύπος αυτός στον δακτύλιο $EXP(\mathbb{C})[t]$ είναι ισοδύναμος με $0 = 0$. Στον δακτύλιο $\mathbb{C}[t]$ είναι ισοδύναμος με $\mathcal{L}(1) = 0$.
Δηλαδή σε κάθε περίπτωση ο τύπος $(\exists z)(\hat{\mathcal{L}}z = \hat{w})$ είναι ισοδύναμος με έναν τύπο ελεύθερο ποσοδεικτών.

Η άρνηση ενός τύπου χωρίς ποσοδείκτες παραμένει ελεύθερη ποσοδεικτών.

Οπότε για τους τύπους (5.7) και (5.8) υπάρχει ένας ισοδύναμος τύπος, ο οποίος είναι ελεύθερος ποσοδεικτών.

Επομένως ο τύπος (5.6) είναι ισοδύναμος με την διάζευξη τύπων ελεύθερων ποσοδεικτών.

Οπότε στους δακτυλίους $\mathbb{C}[t]$, $EXP(\mathbb{C})[t]$ κάθε υπαρξιακός τύπος της L, με μία ή καμία ανισότητα, είναι ισοδύναμος με έναν τύπο ο οποίος είναι ελεύθερος ποσοδεικτών.

Απόδειξη του Λήμματος 5.4. Αναγωγή δύο εξισώσεων σε μία εξίσωση και έναν τύπο ελεύθερο ποσοδεικτών:
Υποθέτουμε ότι έχουμε τον τύπο

$$\mathcal{L}_1 x = f \ \wedge \ \mathcal{L}_2 x = g$$

με n και m η τάξη του $\mathcal{L}_1$ και $\mathcal{L}_2$ αντίστοιχα.
Αφού μπορούμε πάντα να διαιρέσουμε με τον συντελεστή του μεγιστοτάξιου όρου, μπορούμε να υποθέσουμε ότι οι συντελεστές των μεγιστοτάξιων όρων είναι 1.
Ορίζουμε τους διαφορικούς τελεστές $\tilde{\mathcal{L}}_1$ και $\tilde{\mathcal{L}}_2$ έτσι ώστε

$$\tilde{\mathcal{L}}_1 := \mathcal{L}_1 x - f = 0 \ \wedge \ \tilde{\mathcal{L}}_2 := \mathcal{L}_2 x - g = 0 \tag{5.9}$$

Έστω $D_j \tilde{\mathcal{L}}_i$ η j-οστή παράγωγος του $\tilde{\mathcal{L}}_i x$.
Έστω $n < m$, τότε ορίζουμε την διαφορική εξίσωση $D_{m-n}\tilde{\mathcal{L}}_1 x - \tilde{\mathcal{L}}_2 x = 0$ η τάξη της οποίας είναι μικρότερη από την τάξη της $\tilde{\mathcal{L}}_2 x$.
Άρα ο τύπος (5.9) είναι ισοδύναμος με τον τύπο

$$\tilde{\mathcal{L}}_1 x = 0 \wedge D_{m-n}\tilde{\mathcal{L}}_1 x - \tilde{\mathcal{L}}_2 x = 0$$

δηλαδή με έναν τύπο χαμηλότερης τάξης.
Επαναλαμβάνουμε την διαδικασία αυτή μέχρις ότου ο τύπος που προκύπτει να είναι της μορφής

$$\tilde{\mathcal{L}} x = 0 \wedge \phi_0$$

όπου ο τύπος ϕ_0 είναι ελεύθερος ποσοδεικτών και δεν περιέχει τη μεταβλητή x.

Υποθέτουμε ότι έχουμε τον τύπο

$$\bigwedge_{j=1}^{n} \mathcal{L}_j x = f_j$$

και ισχυριζόμαστε ότι μπορεί να γραφεί ισοδύναμα ως $\mathcal{L} x = h \wedge \phi_0$, όπου το ϕ_0 είναι ένας τύπος ελεύθερος ποσοδεικτών ο οποίος δεν περιέχει τη μεταβλητη x.

Επαγωγή στον αριθμό των εξισώσεων, n.

Βάση επαγωγής : Για $n = 1$ έχουμε μια εξίσωση, άρα είναι στη μορφή $\mathcal{L}x = h \wedge \phi_0$.

Επαγωγική υπόθεση : Υποθέτουμε ότι ισχύει για $n = k$, δηλαδή αν έχουμε k εξισώσεις τότε μπορούμε να τις ανάγουμε στη μορφή

$$\tilde{\mathcal{L}}_k x = \tilde{f}_k \wedge \bigwedge_{j=1}^{k} \phi_j.$$

Επαγωγικό βήμα : Θα δείξουμε ότι ισχύει για $n = k + 1$, δηλαδή αν έχουμε $k + 1$ εξισώσεις μπορούμε να τις ανάγουμε στη μορφή

$$\mathcal{L}x = h.$$

Από την επαγωγική υπόθεση ξέρουμε ότι μπορούμε να ανάγουμε τις k πρώτες εξισώσεις στην παραπάνω μορφή. Οπότε έχουμε δύο εξισώσεις, τις $\tilde{\mathcal{L}}_k x = \tilde{f}_k \wedge \bigwedge_{j=1}^{k} \phi_j$ και $\mathcal{L}_{k+1} x = f_{k+1}$. Από την παραπάνω διαδικασία προκύπτει ότι ο τύπος

$$\tilde{\mathcal{L}}_k x = \tilde{f}_k \wedge \mathcal{L}_{k+1} x = f_{k+1}$$

γράφεται ισοδύναμα ως

$$\tilde{\mathcal{L}}_{k+1} x = \tilde{f}_{k+1} \wedge \phi_{k+1}.$$

Οπότε

$$\begin{aligned}
\bigwedge_{j=1}^{k+1} \mathcal{L}_j x = f_j \Leftrightarrow \tilde{\mathcal{L}}_k x = \tilde{f}_k \ \wedge \ \bigwedge_{j=1}^{k} \phi_j \ \wedge \ \mathcal{L}_{k+1} x = f_{k+1} \\
\Leftrightarrow \tilde{\mathcal{L}}_{k+1} x = \tilde{f}_{k+1} \ \wedge \ \phi_{k+1} \ \wedge \ \bigwedge_{j=1}^{k} \phi_j \\
\Leftrightarrow \tilde{\mathcal{L}}_{k+1} x = \tilde{f}_{k+1} \ \wedge \ \bigwedge_{j=1}^{k+1} \phi_j.
\end{aligned}$$

□

Απόδειξη του Λήμματος 5.5. Υποθέτουμε ότι έχουμε τον τύπο

$$\mathcal{L}_1 x = f \ \wedge \ \mathcal{L}_2 x \neq g$$

με n και m η τάξη του $\mathcal{L}_1$ και $\mathcal{L}_2$ αντίστοιχα.
Αφού μπορούμε πάντα να διαιρέσουμε με τον συντελεστή του μεγιστοτάξιου όρου, μπορούμε

να υποθέσουμε ότι οι συντελεστές των μεγιστοτάξιων όρων είναι 1.
Ορίζουμε τους διαφορικούς τελεστές $\tilde{\mathcal{L}}_1$ και $\tilde{\mathcal{L}}_2$ έτσι ώστε

$$\tilde{\mathcal{L}}_1 := \mathcal{L}_1 x - f = 0 \ \wedge \ \tilde{\mathcal{L}}_2 := \mathcal{L}_2 x - g \neq 0 \tag{5.10}$$

Έστω $D_j \tilde{\mathcal{L}}_i$ η j-οστή παράγωγος του $\tilde{\mathcal{L}}_i x$.
Έστω $n < m$, τότε ορίζουμε την διαφορική ανίσωση $D_{m-n}\tilde{\mathcal{L}}_1 x - \tilde{\mathcal{L}}_2 x \neq 0$ η τάξη της οποίας είναι μικρότερη από την τάξη της $\tilde{\mathcal{L}}_2 x$.
Άρα ο τύπος (5.10) είναι ισοδύναμος με τον τύπο

$$\tilde{\mathcal{L}}_1 x = 0 \ \wedge \ D_{m-n}\tilde{\mathcal{L}}_1 x - \tilde{\mathcal{L}}_2 x \neq 0.$$

Επαναλαμβάνουμε την διαδικασία αυτή μέχρις ότου η τάξη του τελεστή της ανίσωσης να είναι μικρότερη της τάξης του τελεστή της εξίσωσης.
Αν η τάξη της ανίσωσης μηδενιστεί μετά από κάποια βήματα τότε ο τύπος (5.10) είναι ισοδύναμος με τον τύπο

$$\tilde{\mathcal{L}}_1 x = 0 \ \wedge \ \phi_0 \neq 0.$$

□

Απόδειξη του Λήμματος 5.6. Θεωρούμε τον τύπο

$$\theta \ : \ \bigwedge_{i=1}^{n} \mathcal{L}(x) = \mathcal{L}(x_i) \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq \mathcal{L}_i(x_i) \ ,$$

ο οποίος γράφεται ισοδύναμα ως

$$\theta \ : \ \bigwedge_{i=1}^{n} \mathcal{L}(x - x_i) = 0 \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x - x_i) \neq 0 \ .$$

Η ανίσωση $\mathcal{L}_i(x - x_i) \neq 0$ ισχύει όταν $x - x_i \neq 0$. Δηλαδή ο τύπος $\exists x \ \theta$ είναι ισοδύναμος με $0 = 0$ αν το σύστημα $\mathcal{L}x = 0 \wedge \bigwedge_{i=1}^{n} \mathcal{L}_i(x) \neq 0$ έχει μη μηδενικές λύσεις. Διαφορετικά, είναι ισοδύναμος με $0 = 1$. □

ΚΕΦΑΛΑΙΟ 6

Πρόβλημα του Grothendieck

Στο κεφάλαιο αυτό θα αναφερθούμε στο πρόβλημα του Grothendieck.

Έστω K ένα αλγεβρικό σώμα αριθμών, $\mathfrak{p}$ ένα πρώτο ιδεώδες του K και $\overline{K}_{\mathfrak{p}}$ το σώμα υπολοίπων.

Θεωρούμε την διαφορική εξίσωση

$$\alpha_0(x)y^{(n)} + \alpha_1(x)y^{(n-1)} + \cdots + \alpha_n(x)y = 0,\ \alpha_i(x) \in K[x],\ i = 1, \ldots, n \qquad (1)$$

Συμβολίζουμε με $(1)_{\mathfrak{p}}$ την αναγωγή της (1) modulo $\mathfrak{p}$.

Πρόβλημα του Grothendieck. *Αν, σχεδόν για κάθε πρώτο ιδεώδες $\mathfrak{p}$, το $(1)_{\mathfrak{p}}$ έχει n λύσεις στο $\overline{K}_{\mathfrak{p}}(x)$ οι οποίες είναι ανεξάρτητες επί του $\overline{K}_{\mathfrak{p}}(x^p)$, όλες οι λύσεις της (1) είναι αλγεβρικές συναρτήσεις.*

Θα αποδείξουμε το πρόβλημα $n = 1$, χρησιμοποιώντας το Θεώρημα πυκνότητας του Tchebotarev.
Για $n > 1$ το πρόβλημα είναι άλυτο.

Θεωρούμε μια διαφορική εξίσωση τάξης 1.

Το Θεώρημα πυκνότητας του Tchebotarev είναι το εξής:

Θεώρημα 6.1. *Έστω K ένα αλγεβρικό σώμα αριθμών πεπερασμένου βαθμού. Αν σχεδόν όλα τα πρώτα ιδεώδη του K είναι βαθμού ένα, τότε το K είναι το ρητό σώμα αριθμών.*

Απόδείξη του Προβλήματος Grothendieck για $n = 1$. Θεωρούμε την ακόλουθη διαφορική εξίσωση πρώτης τάξης:

$$\begin{aligned} &\alpha_0(x)y' + \alpha_1(x) = 0,\ \alpha_0(x), \alpha_1(x) \in K[x] \\ &\Rightarrow y' = -\frac{\alpha_1(x)}{\alpha_0(x)}y \\ &\Rightarrow y' = P(x)y,\ P(x) \in K(x) \end{aligned} \tag{6.1}$$

Από υπόθεση έχουμε ότι η $(6.1)_{\mathfrak{p}}$ έχει μία λύση στο $\overline{K}_{\mathfrak{p}}(x)$, έστω $y_{\mathfrak{p}} = \prod_i (x - \alpha_i)^{\gamma_i}$, $\gamma_i \in \mathbb{Z} \setminus 0$.
Η εξίσωση είναι γραμμική και οι λύσεις σχηματίζουν ένα module επί του $\overline{K}_{\mathfrak{p}}[x^p]$:

1. αν y_1, y_2 είναι λύσεις της εξίσωσης, τότε και τα $y_1 \pm y_2$ είναι λύσεις.
2. αν το y_1 ίναι λύση της εξίσωσης, τότε και το $y_2 : x^p y_1$ είναι λύση.

Δηλαδή δεδομένων $f \in \overline{K}_{\mathfrak{p}}$ και λύσης y_1, το $y_2 := f \cdot y_1$ είναι επίσης λύση.
Για κάθε $n > 0$ ισχύει $(x - \alpha_i)^{p^n} = x^{p^n} - \alpha_i^{p^n} \in \overline{K}_{\mathfrak{p}}[x^p]$.
Οπότε μπορούμε να πολλαπλασιάσουμε κάθε λύση με $(x - \alpha_i)^{p^{n_i}}$, με κατάλληλο n_i ώστε να απαλείψουμε τον παρονομαστή, παίρνοντας ξανά μια λύση, η οποία ανήκει στο $\overline{K}_{\mathfrak{p}}[x]$.
Θέτουμε $y_{\mathfrak{p}} = \prod_i (x - \overline{\alpha}_i)^{c_i},\ c_i \in \mathbb{Z}_{\geq 0}$. Αντικαθιστώντας στην εξίσωση προκύπτει

$$P(x) \mod \mathfrak{p} = \frac{y'_{\mathfrak{p}}}{y_{\mathfrak{p}}} = \sum_i \frac{c_i}{x - \overline{\alpha}_i}\ .$$

Η εξίσωση αυτή ισχύει για σχεδόν κάθε $\mathfrak{p}$ στο K.
Σε μια κατάλληλη επέκταση του K έχουμε

$$P(x) \mod \mathfrak{p} = \sum_i \frac{\beta_i}{x - \alpha_i}\ .$$

δηλαδή

$$\beta_i \equiv (\text{ ακέραιος }) \pmod{\mathfrak{p}}$$

Για να χρησιμοποιήσουμε το Θεώρημα πυκνότητας παίρνοντας ως αλγεβρικό σώμα αιθμών το $\mathbb{Q}(\beta_i)$, αρκεί να δείξουμε ότι όλα τα πρώτα ιδεώση του $\mathbb{Q}(\beta_i)$ είναι βαθμού 1.
Έστω το σώμα $F = \mathbb{Q}(\beta_i)$.
Για να δείξουμε ότι σχέδον όλα τα πρώτα ιδεώση του F ελιναι βαθμού 1, αρκεί να δείξουμε ότι

$$\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_p.$$

Σε μια κατάλληλη επέκταση του K, K_{ext}, έχουμε $\beta \in K_{ext}$. Οπότε έχουμε $F \subseteq K_{ext}$
Από το Θεώρημα Lying-Over έχουμε $\mathfrak{p}_F = F \cap \mathfrak{p}_K$, Αφού η απεικόνιση $\mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_K/\mathfrak{p}_K$ διατηρεί το β_i, δηλαδή $\beta_i + \mathfrak{p}_F \mapsto \beta_i + \mathfrak{p}_K$, το β_i είναι επίσης ακέραιος modulo $\mathfrak{p}_F$.

Κάθε στοιχείο $\alpha \in F$ και συγκεκριμένα κάθε στοιχείο του $\mathcal{O}_F$ μπορεί να γραφεί στη μορφή $a = \sum_{i=0}^{n} a_i \beta^i$. Το άθροισμα αυτό modulo $\mathfrak{p}_F$ γίνεται άθροισμα ακεραίων, δηλαδή $\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_p$.

Επόμένως έχουμε ότι $\mathbb{Q}(\beta_i) = \mathbb{Q} \Rightarrow \beta_i \in \mathbb{Q}$.

Θέτουμε

$$y = c \prod_i (x - \alpha_i)^{\beta_i}$$

τότε η λύση αυτή της (6.1) είναι μία αλγεβρική συνάρτηση. □

Bibliography

[AM03] Carlo Toffalori (auth.) Annalisa Marcja. *A Guide to Classical and Modern Model Theory*. Trends in Logic 19. Springer Netherlands, 1 edition, 2003.

[Bod09] Esther Bod. Hilbert's tenth problem and some generalizations. Master's thesis, Utrecht University, Netherlands, 2009.

[Dav73] Martin Davis. Hilbert's Tenth Problem is Unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

[Den78a] Jan Denef. The Diophantine problem for polynomial rings and fields of rational functions. *Transactions of the American Mathematical Society*, 242:391–399, 1978.

[Den78b] Jan Denef. The diophantine problem for polynomial rings of positive characteristic. *Logic Colloquium*, 78(North-Holland(1979)):131–145, 1978.

[Hed04] Shawn Hedman. *A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity*. Oxford Texts in Logic, Volume 1. Oxford University Press, 2004.

[Hon81] Taira Honda. Algebraic differential equations. *Symposia Mathematica*, XXIV:169–204, Academic Press, London-New York, 1981.

[Kap57] Irving Kaplansky. *An Introduction to Differential Algebra*. Actualites Scientifiques Et Industrielles, 1251. Hermann, 1st edition, 1957.

[Mat70] Yuri Matiyasevich. Enumerable sets are diophantine. *Dkl. Akad. Nauk SSSR*, 191:279–282, 1970. English translation Soviet Math. Dokl., 11:354-358, 1970.

[Maz94] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, 1994.

[Phe94] Thanases Pheidas. Extensions of Hilbert's Tenth Problem. *The Journal of Symbolic Logic*, 59(2):372–397, 1994.

[Poo08] Bjorn Poonen. Undecidability in Number Theory. *Notices A.M.S.*, 55(3):344–350, 2008.

[Pri] David Pritchard. Hilbert's Tenth Problem.

[PZ] Thanases Pheidas and Karim Zahidi. Decision problems in Algebra and analogues of Hilbert's tenth problem.

[PZ00] Thanases Pheidas and Karim Zahidi. Undecidability of existential theories of rings and fields: A survey. *Contemporary Mathematics*, 270:49–106, 2000.

[PZ04] Thanases Pheidas and Karim Zahidi. Elimination theory for addition and the Frobenius map in polynomial rings. *The Journal of Symbolic Logic*, 69(4):1006–1026, 2004.

[Shl06] Alexandra Shlapentokh. Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields. *Leiden : Cambridge University Press*, 2006.

[Tar98] Alfred Tarski. *A decision method for elementary algebra and geometry, in Quantifier Elimination and Cylindrical Algebraic Decomposition.* Texts and Monographs in Symbolic Computation. Springer-Verlag Wien, 1 edition, 1998.

Πίνακας συμβόλων

Σύμβολο	Περιγραφή
$\mathbb{N}$	Σύνολο φυσικών
$\mathbb{Z}$	Σύνολο ακεραίων
$\mathbb{C}$	Σύνολο μιγαδικών
$EXP(\mathbb{C})$	Δακτύλιος εκθετικών αθροισμάτων
$\mathbb{C}[t]$	Πολυωνυμικός δακτύλιος επί του $\mathbb{C}$
$EXP(\mathbb{C})[t]$	Πολυωνυμικός δακτύλιος επί του $EXP(\mathbb{C})$
$'$	Παράγωγος ως προς τη μεταβλητή t
$\|_n$	Διαιρετότητα στο $\mathbb{Z}\left[\frac{1}{n}\right]$
$\|^p$	Ισότητα με δυνάμεις του p
$\mathcal{L}$	Γραμμικός διαφορικός τελεστής