ANALOGUES OF THE DIOPHANTINE PROBLEM FOR SUBRINGS OF THE FIELD OF RATIONAL FUNCTIONS

Georgia Kourkounaki

Supervisor
Thanases Pheidas

Master's Thesis

Department of Mathematics and Applied Mathematics
School of Science and Technology
University of Crete
January 2019

To my parents,
Kostas and Paraskevi,
who always stand by me.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, prof. Thanases Pheidas, for the support and guidance he provided me all the way through my studies. The completion of this thesis would have been impossible without his help.

Besides my supervisor, I would like to thank the rest of the commitee: prof. Konstantinos Dimitrakopoulos and prof. Nikolaos G. Tzanakis for the time they spent reading this thesis.

Finally, I am profoundly grateful to my colleagues Iosif and Kostas for their patience and friendship for the last two years. Heartfelt thanks also go to Sotiris for his continuous encouragement in my daily routine.

The commitee of this thesis consists of :

- prof. Konstantinos Dimitrakopoulos, Department of History and Philosophy of Science, National and Kapodistrian University of Athens
- prof. Thanases Pheidas (supervisor), Department of Mathematics and Applied Mathematics, University of Crete
- prof. Nikolaos G. Tzanakis, Department of Mathematics and Applied Mathematics, University of Crete

Contents

Notation

$\mathbb{N}$, $\mathbb{N}_0$	the natural numbers and the natural numbers including zero
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the integer, the rational, the real and the complex numbers
$\lvert n\rvert$	the absolute value of n
$a \mid b$	a divides b
$\vee$, $\wedge$	logical disjunction and conjunction (read as “or”, “and”)
$\rightarrow$	implication (read as “implies”)
$\leftrightarrow$	equivalence (read as “if and only if”)
$\forall$	universal quantification (read as “for all”)
$\exists$	existential quantification (read as “there exists”)
R^*	the multiplicative group of units of the ring R
$R[X_1, \ldots, X_n]$	polynomials in $X_1, \ldots, X_n$ with coefficients in R
$F(t)$	the rational functions over F in t
$R[[t]], R((t))$	the formal power series and formal Laurent series over R
$\mathrm{deg}(P)$	the degree of the polynomial P
$\mathrm{deg}_{\mathrm{min}}(P)$	the minimum degree of the monomials of P with non-zero coefficients
$\mathrm{deg}_+(P), \mathrm{deg}_-(P)$	the positive degree and the negative degree of P respectively
$\mathrm{LC}(P)$	the leading coefficient of P
$\mathrm{char}(R)$	the characteristic of the ring R
$\overline{R}$	the algebraic closure of R
$\mathrm{Q}(R)$	the field of fractions of R
$\mathcal{O}_K$	the ring of integers of a field K

Throughout this thesis R denotes an integral domain and F denotes a field.

Επεκτεταμένη Περίληψη

Η εργασία αυτή πραγματεύεται το Δέκατο Πρόβλημα του Hilbert (HTP εν συντομία), το οποίο διατυπώθηκε από τον Hilbert στο Δεύτερο Παγκόσμιο Συνέδριο Μαθηματικών το 1900 ως εξής

> Δοθείσης διοφαντικής εξίσωσης με οποιονδήποτε αριθμό μεταβλητών και ακέραιους συντελεστές, να βρεθεί μία μέθοδος με την οποία να μπορεί κανείς να αποφανθεί σε πεπερασμένο αριθμό βημάτων για το αν η εξίσωση έχει λύση στους ακεραίους ή όχι.

Ένα υποσύνολο A του $\mathbb{Z}^n$ ονομάζεται **διοφαντικό** αν περιγράφεται ως

$$A = \{(z_1, \ldots, z_n) \in \mathbb{Z}^n : \exists (x_1, \ldots, x_m) \in \mathbb{Z}^m (P(z_1, \ldots, z_n, x_1, \ldots, x_m) = 0)\},$$

όπου P ένα διοφαντικό πολυώνυμο, δηλαδή ένα πολυώνυμο με ακεραίους συντελεστές. Ο Yuri Matijasevič χρησιμοποιώντας την προηγούμενη δουλειά των Martin Davis, Hilary Putnam και της Julia Robinson, έδωσε ύστερα από 70 χρόνια αρνητική απάντηση στο HTP. Για την αρνητική αυτή απάντηση χρειάστηκαν τα παρακάτω αποτελέσματα της θεωρίας υπολογισμού και της λογικής. Οι ορισμοί είναι από το [19].

Ένα υποσύνολο του $\mathbb{Z}$ ονομάζεται **αναδρομικά απαριθμήσιμο** αν υπάρχει αλγόριθμος που να τυπώνει τα στοιχεία του A. Ένα υποσύνολο A του $\mathbb{Z}$ ονομάζεται **αναδρομικό** αν υπάρχει αλγόριθμος που να αποφασίζει αν ένα στοιχείο x ανήκει στο A, δηλαδή δοσμένου ακεραίου x, ο αλγόριθμος τυπώνει ΝΑΙ αν $x \in A$ και ΟΧΙ διαφορετικά. Εύκολα μπορεί να αποδείξει κάποιος ότι κάθε αναδρομικό σύνολο είναι και αναδρομικά απαριθμήσιμο, η ερώτηση είναι αν ισχύει και το αντίστροφο. Η απάντηση είναι αρνητική και προκύπτει από το παρακάτω πρόβλημα.

Πρόβλημα Τερματισμού. Να βρεθεί αλγόριθμος που να δέχεται ως είσοδο ένα πρόγραμμα H και έναν ακέραιο x και να έχει ως έξοδο ΝΑΙ αν το πρόγραμμα τερματίζει με είσοδο το x και ΟΧΙ διαφορετικά.
Ο Alan Turing απέδειξε το 1936 ότι το πρόβλημα τερματισμού είναι μη αποφασίσιμο.

Θεώρημα DPRM (Davis, Putnam, Robinson, Matijasevič). Ένα υποσύνολο των ακεραίων είναι αναδρομικά απαριθμήσιμο αν και μόνο αν είναι διοφαντικό.

Από τη μη αποφασισιμότητα του προβλήματος τερματισμού, μπορούμε να κατασκευάσουμε ένα αναδρομικά απαριθμίσιμο σύνολο το οποίο δεν είναι αναδρομικό. Αυτό είναι ισοδύναμο με το να έχουμε ένα μη αναδρομικό διοφαντικό σύνολο, δηλαδή υπάρχει ένα διοφαντικό πολυώνυμο $P(z, x_1, \ldots, x_m)$ για το οποίο δεν υπάρχει αλγόριθμος για την απόφανση για ποιες τιμές $a \in \mathbb{Z}$ η εξίσωση $P(a, x_1, \ldots, x_m) = 0$ έχει λύση για $x_1, \ldots, x_m \in \mathbb{Z}$. Συνεπώς δεν υπάρχει αλγόριθμος που να αποφασίζει την ύπαρξη ακέραιων λύσεων μίας τυχούσας διοφαντικής εξίσωσης.

Μετά την αρνητική απάντηση του HTP, οι ερευνητές αναρωτήθηκαν αν το ίδιο ίσχυε σε δακτυλίους πέραν των ακεραίων. Έτσι διατυπώθηκε το γενικευμένο HTP το οποίο ζητάει έναν αλγόριθμο που να αποφασίζει αν μία πολυωνυμική εξίσωση, με συντελεστές σε ένα δακτύλιο R', έχει λύση σε ένα δακτύλιο R, όπου R μεταθετικός και $R' \leq R$. Η απάντηση στο HTP πάνω από το R εξαρτάται από τους δακτύλιους R και R'. Τα σπουδαιότερα αποτελέσματα για τις επεκτάσεις του HTP σε δακτυλίους πέραν των ακεραίων είναι τα

- αποφασίσιμα: HTP πάνω από το $\mathbb{R}$, $\overline{\mathbb{Z}}$, και $p-$αδικά σώματα

- μη αποφασίσιμα: HTP υπέρ πολυωνυμικών δακτυλίων, $\mathbb{R}(t)$, $\mathbb{C}(t_1, t_2)$ και $\mathbb{F}_q(t)$

ενώ ανοικτά παραμένουν ακόμα τα προβλήματα HTP υπέρ των ρητών, αριθμητικών σωμάτων και τυπικών σειρών Laurent πάνω από πεπερασμένο σώμα. Παρακάτω θα δούμε κάποιους βασικούς ορισμούς ([13], [16]) που θα χρησιμοποιηθούν στη συνέχεια.

Μία **γλώσσα** $\mathcal{L}$ είναι ένα σύνολο αποτελούμενο από όλα τα λογικά σύμβολα καθώς και από σύμβολα για τις σχέσεις, τις συναρτήσεις και τις σταθερές. Μία **πρωτοτάξια πρόταση** της γλώσσας ενός μοντέλου είναι μία πρόταση φτιαγμένη χρησιμοποιώντας τα σύμβολα της γλώσσας. Μία **υπαρξιακή πρόταση** είναι μία πρόταση της μορφής $\exists x : S$, όπου το S είναι διάζευξη συστημάτων διοφαντικών εξισώσεων και ανισώσεων. Όταν το S αποτελείται μόνο από εξισώσεις, λέμε ότι η πρόταση είναι **θετική υπαρξιακή**. Η **(θετική υπαρξιακή) θεωρία** ενός μοντέλου είναι το σύνολο όλων των (θετικών υπαρξιακών) προτάσεων που είναι αληθείς στο μοντέλο. Λέμε ότι η θεωρία ενός μοντέλου είναι **αποφασίσιμη** αν υπάρχει αλγόριθμος για την απόφανση της αλήθειας τυχούσας πρότασης στο μοντέλο, διαφορετικά η θεωρία λέγεται **μη αποφασίσιμη**.

Στην παρούσα εργασία θα επικεντρωθούμε στο διοφαντικό πρόβλημα πάνω από πολυωνυμικούς δακτυλίους και υποδακτυλίους των ρητών συναρτήσεων. Σχετική εργασία για προβλήματα αποφασισιμότητας είναι η [21].

Έστω, τώρα, ο πολυωνυμικός δακτύλιος $R[t]$ και D μία κλάση διοφαντικών εξισώσεων υπέρ το $R[t]$. Μία σημαντική παρατήρηση είναι ότι το ανάλογο του HTP υπέρ το $R[t]$ για συστήματα διοφαντικών εξισώσεων της κλάσης D είναι ισοδύναμο με το πρόβλημα αποφασισιμότητας της θετικής υπαρξιακής θεωρίας του $R[t]$ στη γλώσσα $\mathcal{L}$ η οποία περιέχει σύμβολα για τις πράξεις, τις σχέσεις και τις σταθερές που εμφανίζονται στους συντελεστές των εξισώσεων της D.

Στο δεύτερο κεφάλαιο ορίζουμε τις σχέσεις $|_n, |^p$ ως εξής, για $n > 1$ και p πρώτο

$$x\,|_n\, y \leftrightarrow \exists q, s \in \mathbb{Z} : y = xqn^s$$

και

$$x\,|^p\, y \leftrightarrow \exists s \in \mathbb{N} : y = \pm xp^s.$$

Αποδεικνύουμε ότι:

Θεώρημα 1. *Η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\mathcal{L}_{div_n} = \{0, 1, =, +, |_n\}$ είναι μη αποφασίσιμη.*

Πόρισμα 1. *Η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα $\mathcal{L}_{div^p} = \{0, 1, =, +, |, |^p\}$ είναι μη αποφασίσιμη.*

Αρχικά, δείχνουμε ότι αν $x\,|_n\, 1$ και $y\,|_n\, 1$, τότε $y = x^2$ αν και μόνο αν

C1) $2nx + 1\,|_n\, 4n^2y - 1$

C2) $2nx - 1\,|_n\, 4n^2y - 1$

C3) $ny - kx\,|_n\, nx - k$, για κάθε k τέτοιο ώστε $|k| < n$.

Στη συνέχεια αποδεικνύουμε ότι αν ισχύουν τα παρακάτω

C4) $nz + nx - 1 \,|_n\, n^2u - (nx-1)^2$

C5) $2nz + 1 \,|_n\, nx - 1$

C6) $2nz - 1 \,|_n\, nx - 1$

C7) $2n^2u + 1 \,|_n\, nx - 1$,

τότε $u = z^2$. Τέλος, δείχνουμε ότι ένας ακέραιος u είναι ίσος με z^2, για κάποιον ακέραιο z, αν και μόνο αν υπάρχουν ακέραιοι x, y τέτοιοι ώστε $x \,|_n\, 1$, $y \,|_n\, 1$, ισχύουν οι υποθέσεις C1)-C3), C5)-C7) και επιπλέον $nz + nx - 1 \,|_n\, n^2u - n^2y + 2nx - 1$.

Σκιαγράφηση απόδειξης Θεωρήματος 1. Έχουμε ότι ισχύουν οι παρακάτω ισοδυναμίες:

$$z = x + y \leftrightarrow 0 \,|_n\, (x + y - z)$$
$$z = x \cdot y \leftrightarrow 4w = (x+y)^2 - (x-y)^2.$$

Συνεπώς, μπορούμε να εκφράσουμε την πρόσθεση στους ακεραίους με ένα θετικό υπαρξιακό τύπο του $\mathbb{Z}$ στη γλώσσα $\mathcal{L}_{div_n}$. Επιπλέον, από προηγούμενες παρατηρήσεις, μπορούμε να εκφράσουμε ότι ο ακέραιος u είναι τετράγωνο με ένα θετικό υπαρξιακό τύπο της γλώσσας $\mathcal{L}_{div_n}$. Επομένως, μπορούμε να εκφράσουμε και τον πολλαπλασιασμό ακεραίων με ένα θετικό υπαρξιακό τύπο της γλώσσας $\mathcal{L}_{div_n}$. Άρα, αν υπήρχε αλγόριθμος που να αποφασίζει την αλήθεια θετικών υπαρξιακών προτάσεων του $\mathbb{Z}$ στη γλώσσα $\mathcal{L}_{div_n}$, θα μπορούσαμε να τον μετατρέψουμε σε αλγόριθμο απόφασης της αλήθειας θετικών υπαρξιακών προτάσεων του $\mathbb{Z}$ στη γλώσσα που περιέχει την πρόσθεση και τον πολλαπλασιασμό, το οποίο έρχεται σε αντίφαση με την αρνητική απάντηση του HTP στο [11]. □

Σκιαγράφηση απόδειξης Πορίσματος 1. Αρχικά δείχνουμε ότι $x \;|_p\; y$ αν και μόνο αν υπάρχει ακέραιος z τέτοιος ώστε $z \;|^p\; y \wedge z \mid z$ ή $y \;|^p\; z \wedge x \mid z$. Συνεπώς, αν υπήρχε αλγόριθμος απόφασης θετικών υπαρξιακών προτάσεων του $\mathbb{Z}$ στη γλώσσα $\mathcal{L}_{div^p}$, θα μπορούσε να μετατραπεί σε αλγόριθμο για την απόφαση θετικών υπαρξιακών προτάσεων του $\mathbb{Z}$ στην γλώσσα $\mathcal{L}_{div_n}$, το οποίο αντιφάσκει στο Θεώρημα 1. □

Το τρίτο κεφάλαιο της εργασίας πραγματεύεται τη μη αποφασισιμότητα της θετικής υπαρξιακής θεωρίας του $R[t]$ στην γλώσσα των πολυωνυμικών δακτυλίων, $\mathcal{L}_t = \{+, \cdot, =, 0, 1, t\}$. Το κύριο θεώρημα αυτού του κεφαλαίου είναι το

Θεώρημα 2. *Το διοφαντικό πρόβλημα για τον πολυωνυμικό δακτύλιο $R[t]$ με συντελεστές στο $\mathbb{Z}[t]$ είναι μη αποφασίσιμο.*

Η απόδειξη αυτού οφείλεται στον J. Denef και παρουσιάστηκε το 1978 στο [4]. Ο συγγραφέας αξιοποιεί την εξίσωση Pell

$$X^2 - (t^2-1)Y^2 = 1$$

υπέρ το $R[t]$, για την οποία αποδεικνύει ότι οι λύσεις της είναι τα πολυώνυμα Chebyshev $\pm(X_n, Y_n)$, $n = 0, 1, 2, \dots$, που ορίζονται από τον αναδρομικό τύπο $X_n + \sqrt{t^2-1}Y_n = (t + \sqrt{t^2-1})^n$. Στη συνέχεια ορίζουμε τις σχέσεις $\sim, Imt$ πάνω από το $R[t]$ έτσι ώστε $V \sim W$ αν και μόνο αν τα πολυώνυμα λαμβάνουν τις ίδιες τιμές για $t = 1$ και η $Imt(Y)$ είναι αληθής αν και μόνο αν υπάρχει

$X \in R[t]$ τέτοιο ώστε $X^2 - (t^2-1)Y^2 = 1$. Παρατηρούμε ότι οι σχέσεις $V \sim 0, Imt(Y)$ είναι διοφαντικές υπέρ το $R[t]$, αφού η πρώτη είναι αληθής αν και μόνο αν υπάρχει $X \in R[t]$ τέτοιο ώστε $V = (t-1)X$, άρα είναι διοφαντική και η δεύτερη εξ ορισμού. Έπειτα αποδεικνύουμε ότι $Y_n \sim n$, για $n = 0, 1, 2, \dots$ και συμπεραίνουμε ότι

1. αν το πολυώνυμο Y ικανοποιεί την $Imt(Y)$ τότε υπάρχει ακέραιος m τέτοιος ώστε $Y \sim m$
2. για κάθε ακέραιο m υπάρχει πολυώνυμο Y που ικανοποιεί την $Imt(Y)$ τέτοιο ώστε $Y \sim m$.

Σκιαγράφηση απόδειξης Θεωρήματος 2. Για να αποδείξουμε το θεώρημα, αρκεί να βρούμε ένα αλγόριθμο ο οποίος δοσμένου διοφαντικού πολυωνύμου P, n μεταβλητών, βρίσκει πολυώνυμο $\tilde{P}$ με συντελεστές στο $\mathbb{Z}[t]$ έτσι ώστε

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t] : \tilde{P}(Z_1, \dots, Z_n) = 0.$$

Λαμβάνοντας υπ' όψην τα παραπάνω συμπεράσματα, εύκολα αποδεικνύουμε ότι

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t] : \bigwedge_{i=1}^{n} (Imt(Z_i)) \land P(Z_1, \dots, Z_n) \sim 0.$$

Επειδή οι σχέσεις $\sim, Imt$ είναι διοφαντικές υπέρ το $R[t]$ μπορούμε να κατασκευάσουμε το ζητούμενο $\tilde{P}$. Συνεπώς, αν το διοφαντικό πρόβλημα υπέρ το $R[t]$ με συντελεστές στο $\mathbb{Z}[t]$ ήταν αποφασίσιμο, τότε και το διοφαντικό πρόβλημα υπέρ το $\mathbb{Z}$ θα ήταν αποφασίσιμο, το οποίο έρχεται σε αντίφαση με την αρνητική απάντηση του HTP. □

Στη συνέχεια παρουσιάζεται το διοφαντικό πρόβλημα πολυωνυμικού δακτυλίου $R[t, t^{-1}]$ με συντελεστές στο $\mathbb{Z}[t]$ το οποίο αποδείχθηκε μη αποφασίσιμο από τον Peter Pappas στο [12]. Το αποτέλεσμα ήταν αναμενόμενο, το ενδιαφέρον, όμως, σε αυτόν το δακτύλιο είναι ότι οι λύσεις της εξίσωσης Pell $X^2 - (t^2-1)Y^2 = 1$ υπέρ το $R[t, t^{-1}]$ είναι τα ζεύγη

- $\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right)$, $(m, n) \in \mathbb{N}_0^2, j = 1, 2, 3, 4$ αν $i \in R$
- $\left(X^{(j)}_{(m,0)}, Y^{(j)}_{(m,0)}\right)$, $m \in \mathbb{N}_0, j = 1, 2, 3, 4$ αν $i \notin R$,

όπου οι ακολουθίες $X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)} \in \mathbb{Z}[i][t, t^{-1}]$, για $(m, n) \in \mathbb{N}_0^2$ και $j = 1, 2, 3, 4$ ορίζονται από τους αναδρομικούς τύπους

$$\begin{aligned}
X^{(1)}_{(m,n)} + uY^{(1)}_{(m,n)} &= (t+u)^m \left(\frac{1-iu}{t}\right)^n, \\
X^{(2)}_{(m,n)} + uY^{(2)}_{(m,n)} &= (t+u)^m \left(\frac{1+iu}{t}\right)^n, \\
X^{(3)}_{(m,n)} + uY^{(3)}_{(m,n)} &= (t-u)^m \left(\frac{1-iu}{t}\right)^n, \\
X^{(4)}_{(m,n)} + uY^{(4)}_{(m,n)} &= (t-u)^m \left(\frac{1+iu}{t}\right)^n.
\end{aligned}$$

Για τον ίδιο δακτύλιο, αποδεικνύουμε επίσης ότι:

Θεώρημα 3.*Η θετική υπαρξιακή θεωρία του δακτυλίου $R[t, t^{-1}]$ στη γλώσσα $\mathcal{L}_{div} = \{0, 1, =, +, | , t\}$ είναι μη αποφασίσιμη.*

Πόρισμα 2. *Έστω t_1, t_2 διακεκριμένες μεταβλητές. Τότε η θετική υπαρξιακή θεωρία του $R[t_1, t_2]$ στη γλώσσα $\{0, 1, =, +, |, t_1, t_2\}$ είναι μη αποφασίσιμη.*

Θεώρημα 4.*Αν ο δακτύλιος R περιέχει το σώμα των ρητών αριθμών, τότε η δομή του δακτυλίου του $\mathbb{Z}$ είναι θετικά υπαρξιακά περιγράψιμη στη γλώσσα $\mathcal{L}_{div}$ υπέρ το $R[t, t^{-1}]$.*

Τα παραπάνω αποτελέσματα οφείλονται στον Θ. Φειδά και παρουσιάζονται στο [14]. Αποδεικνύουμε ότι αν $2 \in R^*$ (αντίστοιχα $2 \notin R^*$) τότε υπάρχει θετικός υπαρξιακός τύπος ϕ_1 (αντίστοιχα ϕ_2) της $\mathcal{L}_{\text{div}}$ τέτοιος ώστε για κάθε $x, y, z \in \{t^n, n \in \mathbb{Z}\}$ έχουμε ότι $\phi_1(x, y, z)$ (αντίστοιχα $\phi_2(x, y, z)$) είναι αληθής στο $R[t, t^{-1}]$ αν και μόνο αν $z = x \cdot y$. Για κάθε $P, Q \in R[t, t^{-1}]$ ορίζουμε τη σχέση $\sim$ έτσι ώστε $t - 1 \,|\, P - Q$.

Σκιαγράφηση απόδειξης Θεωρήματος 3. Ορίζουμε $y_n = \dfrac{t^n - 1}{t - 1}$ και $D = \{y_n \in R[t, t^{-1}] : n \in \mathbb{Z}\}$. Τότε, από προηγούμενη παρατήρηση, η σχέση $x = z \cdot w$, για $z, w \in D$, είναι περιγράψιμη από θετικό υπαρξιακό τύπο του $R[t, t^{-1}]$ στη γλώσσα $\mathcal{L}_{\text{div}}$. Επίσης, η σχέση $P \sim 0$ (δηλαδή $P \equiv 0 (\text{mod}\, t - 1)$) είναι επίσης περιγράψιμη από θετικό υπαρξιακό τύπο του $R[t, t^{-1}]$ στη γλώσσα $\mathcal{L}_{\text{div}}$. Έστω $P(X_1, \ldots, X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$ και $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ ρίζα του P. Τότε δείχνουμε ότι υπάρχουν $Y_1, \ldots, Y_m \in D$ τέτοια ώστε

$$P(x_1 \ldots, x_m) \equiv P(Y_1, \ldots, Y_m) (\text{mod}\, t - 1),$$

συνεπώς $P(Y_1, \ldots, Y_m) \sim 0$. Αντίστροφα, αν υπάρχουν $Y_1, \ldots, Y_m \in D$ τέτοια ώστε $P(Y_1, \ldots, Y_m) \sim 0$ τότε δείχνουμε ότι υπάρχουν $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ τέτοια ώστε $P(x_1, \ldots, x_m) = 0$. Επομένως καταλήγουμε στην ισοδυναμία

$$\exists x_1, \ldots, x_m \in \mathbb{Z} : P(x_1, \ldots, x_m) = 0 \leftrightarrow \exists Y_1, \ldots, Y_m \in R[t, t^{-1}] : \bigwedge_{i=1}^{m} Y_i \in D \wedge P(Y_1, \ldots, Y_m) \sim 0.$$

Άρα αν υπήρχε αλγόριθμος για την απόφανση της αλήθειας θετικών υπαρξιακών προτάσεων του $R[t, t^{-1}]$ στη γλώσσα $\mathcal{L}_{\text{div}}$, θα μπορούσε να μετατραπεί σε αλγόριθμο για την απόφανση αν μία τυχούσα διοφαντική εξίσωση έχει λύση στους ακεραίους ή όχι, το οποίο είναι άτοπο λόγω της αρνητικής απάντησης του HTP από τον Matijasevič στο [11].

Σκιαγράφηση απόδειξης Πορίσματος 2. Θεωρούμε την απεικόνιση

$$\begin{array}{rccc} \sigma : & R[t_1, t_2]/\langle 1 - t_1 t_2 \rangle & \longrightarrow & R[t, t^{-1}] \\ & t_1 & \longmapsto & t \\ & t_2 & \longmapsto & t^{-1}. \end{array}$$

Τότε η σ είναι ισομορφισμός δακτυλίων και άρα $R[t_1, t_2]/\langle 1 - t_1 t_2 \rangle \cong R[t, t^{-1}]$. Για κάθε $x, y \in R[t, t^{-1}]$ έχουμε

$$\sigma(x) \,|\, \sigma(y) \text{ στο } R[t, t^{-1}] \leftrightarrow \exists z \in R[t_1, t_2] : x \,|\, y + z(1 - t_1 t_2) \text{ στο } R[t_1, t_2].$$

Συνεπώς αν η θετική υπαρξιακή θεωρία του $R[t_1, t_2]$ στη γλώσσα $\{0, 1, =, +, |, t_1, t_2\}$ ήταν αποφασίσιμη, τότε θα ήταν και η θετική υπαρξιακή θεωρία του $R[t, t^{-1}]$ στη γλώσσα $\mathcal{L}_{\text{div}}$, το οποίοι είναι άτοπο λόγω του Θεωρήματος 3. □

Στη συνέχεια αποδεικνύουμε ότι υπάρχει θετικός υπαρξιακός τύπος ϕ_{unit} της $\mathcal{L}_{\text{div}}$ τέτοιος ώστε για κάθε $x \in R[t, t^{-1}]$, ο $\phi_{\text{unit}}(x)$ είναι αληθής αν και μόνο αν το x είναι αντιστρέψιμο στοιχείο του R. Επίσης, δείχνουμε ότι υπάρχει θετικός υπαρξιακός τύπος ϕ_{mult} της $\mathcal{L}_{\text{div}}$ τέτοιος ώστε για κάθε $x, y, z \in R[t, t^{-1}]$, ο $\phi_{\text{mult}}(x, y, z)$ είναι αληθής αν και μόνο αν το $z = x \cdot y$.

Σκιαγράφηση απόδειξης Θεωρήματος 4. Αποδεικνύουμε ότι ισχύει η ισοδυναμία

$$\mu \in \mathbb{Z} \leftrightarrow \mu \in R \wedge \exists x \in R[t, t^{-1}] : x \,|\, 1 \wedge t - 1 \,|\, x - 1 \wedge (t-1)^2 \,|\, x - 1 - \mu(t-1).$$

Αν το R περιέχει το $\mathbb{Q}$ τότε μπορούμε να αντικαταστήσουμε τον τύπο $\mu \in R$ με τον τύπο ϕ_{unit} που προαναφέρθηκε. Επιπλέον, ο πολλαπλασιασμός των ακεραίων μπορεί να περιγραφθεί από τον θετικό υπαρξιακό τύπο της $\mathcal{L}_{\text{div}}$, $\phi_{\text{mult}}|_{\mathbb{Z}}$. □

Εν συνεχεία, γίνεται μία διαφορετική προσέγγιση της μη αποφασισιμότητας της θετικής υπαρξιακής θεωρίας του πολυωνυμικού δακτυλίου $F[t]$ και $F[t, t^{-1}]$, όπου F σώμα, από τον Θ. Φειδά στο [13]. Τα κύρια αποτελέσματα της ενότητας είναι

Θεώρημα 5. *Η υπαρξιακή θεωρία του $F[t, t^{-1}]$ στη γλώσσα $\{0, 1, =, +, \cdot, t\}$ είναι μη αποφασίσιμη.*

Θεώρημα 6.*Η υπαρξιακή θεωρία του $F[t]$ στη γλώσσα $\{0, 1, =, +, \cdot, t\}$ είναι μη αποφασίσιμη.*

Στην περίπτωση που το σώμα F είναι χαρακτηριστικής 0, αποδεικνύουμε ότι ένα στοιχείο $x \in F[t, t^{-1}]$ είναι $m-$οστή δύναμη του t, $m \in \mathbb{Z}$, αν και μόνο αν το x είναι αντιστρέψιμο στοιχείο και το $t-1$ διαιρεί το $x-1$ στο $F[t, t^{-1}]$. Έπειτα δείχνουμε ότι ένα στοιχείο $n \in F[t, t^{-1}]$ είναι μη μηδενικός ακέραιος αν και μόνο αν το n είναι αντιστρέψιμο, το $n-1$ είτε το $n+1$ είναι αντιστρέψιμο και υπάρχει στοιχείο $x = t^m$ τέτοιο ώστε $\dfrac{x-1}{t-1} \equiv n (\text{mod}\, t-1)$.

Στη περίπτωση που το σώμα F είναι θετικής χαρακτηριστικής $p > 2$, αποδεικνύουμε ότι

- $t^n - 1 \,|\, t^m - 1$ στο $F[t, t^{-1}]$ αν και μόνο αν $n \,|\, m$ στο $\mathbb{Z}$ και
- το $\dfrac{t^m - 1}{t^n - 1}$ είναι τετράγωνο στο $F[t, t^{-1}]$ αν και μόνο αν υπάρχει ακέραιος s ώστε $m = np^s$ (ισοδύναμα $n \,|^p\, m$).

Σκιαγράφηση απόδειξης Θεωρήματος 5.

- *Περίπτωση char$(F) = 0$.* Έχουμε ότι η σχέση "το $x \in F[t, t^{-1}]$ είναι δύναμη του t" περιγράφεται από τον υπαρξιακό τύπο (έστω $\phi(x)$)

  $$\exists n \in \mathbb{Z} : x = t^n \leftrightarrow \exists y, z \in F[t, t^{-1}] : xy = 1 \wedge x - 1 = (t-1)z.$$

  Άρα η σχέση "το $n \in F[t, t^{-1}]$ είναι μη μηδενικός ακέραιος" μπορεί να περιγραφεί από τον υπαρξιακό τύπο (έστω $\psi(n)$)

  $$\begin{gathered}\exists\, x, y \in F[t, t^{-1}] : nx = 1 \wedge ((n+1)y = 1 \vee (n-1)y = 1) \\ \wedge \exists\, z, w \in F[t, t^{-1}] : \phi(x) \wedge x - 1 = (t-1)n + (t-1)^2 w.\end{gathered}$$

  Συνεπώς, δοσμένου διοφαντικού πολυωνύμου $P(X_1, \ldots, X_n)$ έχουμε ότι

$$\exists z_1,\dots,z_n \in \mathbb{Z} : P(z_1,\dots,z_n) = 0 \leftrightarrow$$
$$\exists x_1,\dots,x_n \in F[t,t^{-1}] : P(x_1,\dots,x_n) = 0 \wedge \psi(x_1) \wedge \dots \wedge \psi(x_n).$$

Επομένως, αν υπήρχε αλγόριθμος που απαντάει στην ερώτηση αν ο τελευταίος τύπος είναι αληθής στο $F[t,t^{-1}]$ τότε θα υπήρχε αλγόριθμος που θα μπορεί να απαντήσει στην ερώτηση αν η εξίσωση $P = 0$ έχει λύση στους ακεραίους, το οποίο έρχεται σε αντίφαση με την αρνητική απάντηση του HTP.

- *Περίπτωση char*$(F) = p$, $p > 2$. Αναπαριστούμε τους ακέραιους αριθμούς από δυνάμεις του t, δηλαδή το t^n αναπαριστά τον ακέραιο n. Έχουμε ότι το σύνολο των δυνάμεων του t είναι περιγράψιμο από υπαρξιακό τύπο. Έτσι μπορούμε να αντιστοιχίσουμε την υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα που περιλαμβάνει την πρόσθεση, τη διαιρετότητα και την τοπική διαιρετότητα, με την υπαρξιακή θεωρία του $F[t,t^{-1}]$ ως εξής

  1) Η πρόσθεση στους ακεραίους $m+n$ αντιστοιχεί στο γινόμενο $t^m t^n$.
  2) Η σχέση διαιρετότητας $n \mid m$ στους ακεραίους αντιστοιχεί στο $t^n - 1 \mid t^m - 1$ στο $F[t,t^{-1}]$.
  3) Η σχέση της τοπικής διαιρετότητας $n|^p m$ αντιστοιχεί στον υπαρξιακό τύπο $\exists d \in F[t,t^{-1}]$: $\dfrac{t^m-1}{t^n-1} = d^2$.

  Συνεπώς αν υπήρχε αλγόριθμος που να αποφασίζει την αλήθεια μίας υπαρξιακής πρότασης του $F[t,t^{-1}]$ θα μπορούσε να μετατραπεί σε αλγόριθμο που να αποφασίζει την αλήθεια μίας υπαρξιακής πρότασης του $\mathbb{Z}$ στη γλώσσα που περιλαμβάνει την πρόσθεση, τη διαιρετότητα και την τοπική διαιρετότητα, το οποίο αντιφάσκει το Πόρισμα 1. □

Σκιαγράφηση απόδειξης Θεωρήματος 6. Έστω $s = t + \sqrt{t^2-1}$. Τότε $s^{-1} = t - \sqrt{t^2-1}$ και $F[s,s^{-1}] = F[t,\sqrt{t^2-1}]$. Θεωρούμε το δακτύλιο $F[s,s^{-1}]$ ως module υπέρ το $F[t] = F[s+s^{-1}]$, με βάση $\mathcal{B} = \{1, s+s^{-1}\}$. Έστω πολυώνυμο P n μεταβλητών υπέρ το $F[s,s^{-1}]$. Τότε το P γράφεται ως προς τη βάση $\mathcal{B}$ ως $P = P_1 + (s+s^{-1})P_2$, όπου $P_1, P_2 \in F[t]$. Άρα έχουμε

$$\exists x_1,\dots,x_n \in F[s,s^{-1}] : P(x_1,\dots,x_n) = 0 \leftrightarrow$$
$$\exists X_1,\dots,X_n \in F[t] : P_1(X_1,\dots,X_n) + (s+s^{-1})P_2(X_1,\dots,X_n) = 0 \wedge s+s^{-1} = 2t \leftrightarrow$$
$$\exists X_1,\dots,X_n \in F[t] : P_1(X_1,\dots,X_n) = 0 \wedge P_2(X_1,\dots,X_n) = 0$$

διότι $\mathcal{B}$ είναι βάση. Συνεπώς, αν υπήρχε αλγόριθμος που να αποφασίζει αν η τελευταία πρόταση είναι αληθής στο $F[t]$, θα υπήρχε αλγόριθμος που να απαντάει στην ερώτηση αν η εξίσωση $P = 0$ έχει λύση στο $F[s,s^{-1}]$, το οποίο είναι άτοπο λόγω του Θεωρήματος 3. □

Στο τέταρτο κεφάλαιο παρουσιάζονται τα διοφαντικά προβλήματα των δακτυλίων $R[t]$ και $F[t,t^{-1}]$ στη “γεωμετρική γλώσσα”, $\mathcal{L}_T = \{+,\cdot,=,0,1,T\}$, όπου η σχέση $T(a)$ υποδηλώνει ότι το a είναι μη σταθερό στοιχείο του δακτυλίου $R[t]$. Ο λόγος που ονομάζουμε την $\mathcal{L}_T$ “γεωμετρική γλώσσα” είναι διότι συνδέεται με επεκτάσεις του HTP γεωμετρικής φύσεως, οι οποίες είναι και το θέμα της πρώτης ενότητας.

Έστω F σώμα και πολυώνυμα $f_1,\dots,f_m \in F[X_1,\dots,X_n]$. Ορίζουμε **αφινική πολλαπλότητα** $\mathbb{V}$ το σύνολο

$$\mathbb{V} = \{(a_1,\dots,a_n) \in F^n : f_1(a_1,\dots,a_n) = \dots = f_m(a_1,\dots,a_n) = 0\}.$$

Ερώτηση 1. Έστω F σώμα και $\mathbb{V}$ μία αφινική πολλαπλότητα ορισμένη πάνω από το πρώτο σώμα του F. Υπάρχει αλγόριθμος που να αποφασίζει αν η $\mathbb{V}$ περιέχει κάποια καμπύλη που να παραμετρικοποιείται από ρητές συναρτήσεις με συντελεστές στο F;

Το παραπάνω ερώτημα παραμένει ανοιχτό και συνδέεται με τη θετική υπαρξιακή θεωρία των ρητών συναρτήσεων στη γλώσσα $\mathcal{L}_T$. Πράγματι, έστω $\mathbb{V}$ αφινική πολλαπλότητα που ορίζεται από

$$f_1(x_1,\ldots,x_n) = \cdots = f_m(x_1,\ldots,x_n) = 0,$$

με $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$. Τότε η $\mathbb{V}$ δέχεται ρητή παραμετρικοποίηση αν και μόνο αν το σύστημα των εξισώσεων που ορίζουν τη $\mathbb{V}$ περιέχει ένα $F(t)-$ρητό σημείο χωρίς όλες του οι συντεταγμένες να ανήκουν στο F. Συνεπώς, η Ερώτηση 1 διατυπώνεται ισοδύναμα ως εξής

Ερώτηση 2. Υπάρχει αλγόριθμος για την απόφανση της αλήθειας τύπων της μορφής

$$\exists \mathrm{x} = (x_1,\ldots,x_n) \in F(t)^n : f_1(\mathrm{x}) = \cdots = f_m(\mathrm{x}) = 0 \wedge \left(\bigvee_{i=1}^{n} T(x_i)\right)$$

πάνω από το $F(t)$;

Η παραπάνω έκφραση είναι ένας θετικός υπαρξιακός τύπος του $F(t)$ στη γλώσσα $\mathcal{L}_T$. Επομένως, αν η θετική υπαρξιακή θεωρία του $F(t)$ στη $\mathcal{L}_T$ είναι αποφασίσιμη τότε το γεωμετρικό πρόβλημα της Ερώτησης 1 θα έχει θετική απάντηση, ενώ αν η θετική υπαρξιακή θεωρία του $F(t)$ στη $\mathcal{L}_T$ είναι μη αποφασίσιμη, τότε θα έχουμε ένα πρώτο βήμα προς την αρνητική απάντηση του προβλήματος της Ερώτησης 1. Προσπάθειες επίλυσης του γεωμετρικού προβλήματος έχουν γίνει στο [8] και περισσότερα γεωμετρικά προβλήματα που αντιστοιχούν σε ανάλογα του HTP παρουσιάζονται στα [17] (ενότητα 2) και [18] (ενότητα 12).

Παρόλο που το γεωμετρικό πρόβλημα της Ερώτησης 1 παραμένει ανοιχτό, έχει δοθεί αρνητική απάντηση για τον πολυωνυμικό δακτύλιο $R[t]$, όπου R ακέραια περιοχή, από τους Θ. Φειδά και Κ. Zahidi στο [15]. Το κύριο Θεώρημα της ενότητας είναι το

Θεώρημα 7. *Ο δακτύλιος $R[t]$ έχει μη αποφασίσιμη υπαρξιακή θεωρία στη γλώσσα $\mathcal{L}_T$.*

Έστω R ακέραια περιοχή. Αρχικά θεωρούμε ένα στοιχείο $a \in R[t]$, τέτοιο ώστε $T(a)$. Δουλεύουμε με την εξίσωση Pell $X^2-(a^2-1)Y^2 = 1$ και ορίζουμε τις αναδρομικές ακολουθίες $X_n(a), Y_n(a), n \in \mathbb{N}_0$, με αρχικές τιμές $X_0 = 1, Y_0 = 0$ και τύπο

$$X_{n+1} = aX_n + (a^2-1)Y_n$$

και

$$Y_{n+1} = X_n + aY_n.$$

Επεκτείνουμε τον ορισμό στους ακεραίους, θέτοντας $X_{-n} = X_n$ και $Y_{-n} = -Y_n$, $n \in \mathbb{N}_0$, και παρατηρούμε ότι τα ζεύγη (X_n, Y_n) αποτελούν λύσεις της εξίσωσης Pell για $n \in \mathbb{Z}$. Στη συνέχεια αποδεικνύουμε ότι το a^2-1 δεν είναι τέλειο τετράγωνο στον δακτύλιο $R[t]$ και ορίζουμε στοιχείο $u \in \mathrm{Q}(R)(t)$ τέτοιο ώστε $u^2 = a^2-1$. Τότε τα ζεύγη (X_n, Y_n) ικανοποιούν τις εξής σχέσεις

- $X_n + uY_n = (X_1 + uY_1)^n$
- $X_{n+m} = X_nX_m + u^2Y_nY_m$
- $Y_{n+m} = Y_nX_m + X_nY_m$,

για $n, m \in \mathbb{Z}$. Έπειτα αποδεικνύουμε ότι οι λύσεις της εξίσωσης Pell είναι τα ζεύγη $(\pm X_n, Y_n)$, $n \in \mathbb{Z}$, δείχνοντας αρχικά ότι το (X_0, Y_0) αποτελεί λύση και ύστερα, αν υποθέσουμε τυχούσα λύση (X, Y), κάνοντας επαγωγή στο βαθμό του πολυωνύμου X, καταλήγουμε ότι αυτή ισούται με $(\pm X_k, Y_k)$ για κάποιο $k \in \mathbb{Z}$. Στη συνέχεια αποδεικνύουμε ότι για τυχαίους ακέραιους n, m, ο n διαιρεί τον m στο $\mathbb{Z}$ αν και μόνο αν το Y_n διαιρεί το Y_m στο $R[t]$.

Θεωρούμε, τώρα, την περίπτωση που ο δακτύλιος R έχει θετική χαρακτηριστική $p > 2$. Τότε για κάθε $n \neq 0$ έχουμε $n|^p m$ αν και μόνο αν

$$\exists Z_1, Z_2, W_1, W_2 \in R[t] : Z_1^2 - (X_n(a)^2 - 1)W_1^2 = 1 \wedge Z_2^2 - ((X_n(a) + 1)^2 - 1)W_2^2 = 1 \wedge \\ Z_1 = X_m(a) \wedge Z_2 = Z_1 + 1.$$

Έπειτα ορίζουμε τη σχέση $Z \sim 0$ που δηλώνει ότι το $a - 1$ διαιρεί το πολυώνυμο Z στον $R[t]$ και δείχνουμε ότι περιγράφεται από την θετική υπαρξιακή πρόταση στη γλώσσα $\mathcal{L}_T$. Επίσης παρατηρούμε ότι $Y_n \equiv n(\text{mod } a - 1)$.

Σκιαγράφηση απόδειξης Θεωρήματος 7.

- *Περίπτωση char(F)=0.* Θεωρούμε τυχαίο διοφαντικό πολυώνυμο P και $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ λύση της εξίσωσης $P = 0$. Τότε έχουμε ότι

  $$P(Y_{z_1}, \ldots, Y_{z_n}) \equiv P(z_1, \ldots, z_n)(\text{mod } a - 1) \equiv 0(\text{mod } a - 1).$$

  Άρα $P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$. Αντίστροφα, αν υποθέσουμε ότι $P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$, για κάποια $z_1, \ldots, z_n \in \mathbb{Z}$, έχουμε ότι

  $$P(Y_{z_1}, \ldots, Y_{z_n}) \equiv 0(\text{mod } a - 1) \Leftrightarrow \\ P(z_1, \ldots, z_n) \equiv 0(\text{mod } a - 1)$$

  και αφού το $P(z_1, \ldots, z_n)$ είναι σταθερά έχουμε ότι $P(z_1, \ldots, z_n) = 0$. Συνεπώς καταλήγουμε ότι

  $$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Y_{z_1}, \ldots, Y_{z_n} \in R[t] : P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$$

  και η σχέση $\sim$ περιγράφεται από θετικό υπαρξιακό τύπο στη γλώσσα $\mathcal{L}_T$. Άρα, αν υπήρχε αλγόριθμος που να μπορεί να αποφασίσει την αλήθεια θετικών υπαρξιακών προτάσεων πάνω από το $R[t]$ στη γλώσσα $\mathcal{L}_T$, θα μπορούσαμε να τον μετατρέψουμε σε αλγόριθμο που να αποφασί- ζει εάν μία τυχούσα διοφαντική εξίσωση έχει λύση στους ακεραίους ή όχι, το οποίο έρχεται σε αντίφαση με την αρνητική απάντηση στο HTP.

- *Περίπτωση char(F)=p>2.* Αναπαριστούμε τους ακεραίους με τα ζεύγη (X_n, Y_n), δηλαδή το ζεύγος (X_n, Y_n) αναπαριστά τον ακέραιο n. Τότε μπορούμε να αντιστοιχίσουμε την θετική υπαρξιακή θεωρία του $R[t]$ στη γλώσσα $\mathcal{L}_T$ με τη θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα που περιέχει τη πρόσθεση, τη διαιρετότητα και την τοπική διαιρετότητα ως εξής

1) Η πρόσθεση $m+n$ στους ακεραίους αντιστοιχεί στο ζεύγος (X_{m+n}, Y_{m+n}).

2) Η σχέση της διαιρετότητας $n\,|\,m$ αντιστοιχεί στη σχέση $Y_n\,|\,Y_m$.

3) Η σχέση της τοπικής διαιρετότητας $n|^p m$ περιγράφεται από θετική υπαρξιακή πρότασης της γλώσσας $\mathcal{L}_T$ στο δακτύλιο $R[t]$, όπως είδαμε παραπάνω.

Συνεπώς, αν η θετική υπαρξιακή θεωρία του δακτυλίου $R[t]$ στη γλώσσα $\mathcal{L}_T$ ήταν αποφασίσιμη, τότε θα ήταν και η θετική υπαρξιακή θεωρία του $\mathbb{Z}$ στη γλώσσα που περιέχει την πρόσθεση, τη διαιρετότητα και την τοπική διαιρετότητα, πράγμα το οποίο είναι άτοπο λόγω του Πορίσματος 1. □

Στη συνέχεια γίνεται μία προσπάθεια να δοθεί απάντηση για την αποφασισιμότητα του δακτυλίου $F[t,t^{-1}]$ στη γλώσσα $\mathcal{L}_T$, όπου F σώμα χαρακτηριστικής 0. Αρχικά ορίζουμε το θετικό βαθμό $\deg_+(P)$ και τον αρνητκό βαθμό $\deg_-(P)$ ενός πολυωνύμου $P = \sum_{i=r}^{r'} \alpha_i t^i$ του $F[t,t^{-1}]$ ως εξής

$$\deg_+(P) = \begin{cases} r', & \text{αν } r' \geq 0 \\ -\infty, & \text{αν } r' < 0 \end{cases}$$

και

$$\deg_-(P) = \begin{cases} r, & \text{αν } r \leq 0 \\ +\infty, & \text{αν } r > 0. \end{cases}$$

Δουλεύουμε με την εξίσωση Pell $X^2 - (a^4-1)Y^2 = 1$ και ορίζουμε τις αναδρομικές ακολουθίες $X_n, Y_n, n \in \mathbb{N}$, ως εξής

$$X_{n+1}(a) = a^2 X_n(a) + (a^4-1)Y_n(a)$$

και

$$Y_{n+1}(a) = X_n(a) + a^2 Y_n(a),$$

με αρχικές τιμές $X_0 = 1$ και $Y_0 = 0$. Επεκτείνουμε τον ορισμό στους ακεραίους θέτοντας $X_{-n} = X_n$ και $Y_{-n} = -Y_n$ κι έπειτα αποδεικνύουμε ότι το $a^4 - 1$ δεν είναι τέλειο τετράγωνο στο $F[t,t^{-1}]$.

Λήμμα 8. *Έστω $a \in F[t,t^{-1}]$, τέτοιο ώστε να ισχύει $T(a)$ και a μη αντιστρέψιμο. Τότε οι λύσεις της εξίσωσης $X^2 - (a^4-1)Y^2 = 1$ είναι της μορφής $(X,Y) = (\pm X_n, Y_n)$ για $n \in \mathbb{Z}$.*

Αν υποθέσουμε ότι το παραπάνω λήμμα ισχύει, τότε η θετική υπαρξιακή θεωρία του $F[t,t^{-1}]$ στη γλώσσα $\mathcal{L}_T$ είναι μη αποφασίσιμη ακολουθώντας την ίδια απόδειξη όπως προηγουμένως, η οποία παρουσιάζεται στο [15]. Επομένως, το πρόβλημα ανάγεται στην απόδειξη του λήμματος 8.

Σκιαγράφηση της προσπάθειας απόδειξης λήμματος 8.
Η μέθοδος που χρησιμοποιούμε παρουσιάζεται στο [15] από τους Φειδά και Zahidi.

Εύκολα διαπιστώνουμε ότι τα ζεύγη $(\pm X_n, Y_n)$ ικανοποιούν την εξίσωση Pell, δηλαδή είναι λύσεις της. Αντίστροφα, έστω (X,Y) λύση της Pell. Θα κάνουμε επαγωγή στο βαθμό του Y. Παρατηρούμε ότι αν $Y = 0$ τότε $X = \pm 1$, άρα σε αυτή την περίπτωση έχουμε $(X,Y) = (\pm X_0, Y_0)$. Έστω $\deg_+(Y) = \deg_-(Y) = 0$, τότε αποδεικνύουμε ότι $(X,Y) = (\pm X_1, Y_1)$ ή $(\pm X_{-1}, Y_{-1})$. Υποθέτουμε ότι το λήμμα ισχύει για λύσεις (Z,W) της Pell τέτοιες ώστε

$$\deg_+(W) < \deg_+(Y).$$

Αν υποθέσουμε ότι $\deg_+(a) \leq 0$, τότε μέσω του αυτομορφισμού ϕ του $F[t, t^{-1}]$ που στέλνει το t στο t^{-1}, αποδεικνύουμε ότι $(X(t^{-1}), Y(t^{-1}))$ επίσης λύση της Pell με $\deg_+(a) > 0$. Επομένως, χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $\deg_+(a) > 0$. Ορίζουμε

$$\begin{array}{c} Z_1 = a^2X + (a^4 - 1)Y, W_1 = X + a^2Y \\ Z_2 = a^2X - (a^4 - 1)Y, W_2 = X - a^2Y. \end{array}$$

Θεωρούμε τις εξής περιπτώσεις:

1) *Περίπτωση* $\deg_+(Y) > 0$. Έχουμε ότι $\deg_+(W_1W_2) = \deg_+(1-Y^2) = \deg_+(Y^2)$. Αποδεικνύουμε ότι η περίπτωση $\deg_+(W_1) = \deg_+(W_2) = \deg_+(Y)$ είναι αδύνατη, συνεπώς $\deg_+(W_i) < \deg_+(Y)$ για $i = 1$ ή 2.

2) *Περίπτωση* $\deg_+(Y) = 0$. Έχουμε ότι $\deg_+(W_1W_2) \leq 0$ επομένως είτε $\deg_+(W_1) = \deg_+(W_2) = 0$ ή κάποιο εκ των W_1, W_2 έχει θετικό βαθμό ίσο με $-\infty$. Στην πρώτη περίπτωση καταλήγουμε σε άτοπο, άρα $\deg_+(W_i) < 0$ δηλαδή $\deg_+(W_i) < \deg_+(Y)$, για $i = 1$ ή 2.

Η μόνη περίπτωση που παραμένει ακόμα αναπόδεικτη είναι $\deg_+(Y) = -\infty$.

Abstract

Our aim in this thesis is to give a presentation of extensions of Hilbert's Tenth Problem, focusing on polynomial rings and subrings of rational functions. More precisely, we deal with the positive existential theory of $R[t]$ in the languages $\mathcal{L}_t$ and $\mathcal{L}_T$, as well as the positive existential theory of the Laurent polynomial ring in $\mathcal{L}_t$. We also attempt to prove the undecidability of the positive existential theory of the Laurent polynomial ring in $\mathcal{L}_T$.

Chapter 1

Introduction

Hilbert's Tenth Problem. Hilbert, in 1900, gave a lecture in which he listed 23 problems to be solved in the next century. More pricesely, his tenth problem stated that:

> Suppose we are given a diophantine equation with an arbitrary number of unknowns and with integer coefficients. Give a process by which it is possible to determine after a finite number of operations whether or not this equation is solvable in integer numbers.

In particular, "... a way in which it is possible to determine after a finite number of operations ..." is what we call now an "algorithm". At the moment Hilbert gave the lecture, the theory of recursive functions and algorithms was in an early stage. In contemporary mathematics, Hilbert's Tenth Problem (HTP for short) asks for an algorithm that takes as an imput a multivariant diophantine polynomial $f(X_1, \ldots, X_n)$ and gives as an output YES if there exist integers $z_1, \ldots, z_n$ such that $f(z_1, \ldots, z_n) = 0$ and NO otherwise.

Definition 1.0.1. A subset A of $\mathbb{Z}^n$ is called **diophantine** if it can be described as

$$A = \{(z_1, \ldots, z_n) \in \mathbb{Z}^n : \exists (x_1, \ldots, x_m) \in \mathbb{Z}^m \, (P(z_1, \ldots, z_n, x_1, \ldots, x_m) = 0)\},$$

where P is a **diophantine polynomial** (that is a polynomial of multiple variables with integer coefficients). Equivalently, A is diophantine if

$$z_1, \ldots, z_n \in A \leftrightarrow \exists (x_1, \ldots, x_m) \in \mathbb{Z}^m \, (P(z_1, \ldots, z_n, x_1, \ldots, x_m) = 0)$$

for some diophantine polynomial P.

Example 1.0.2. Let A be the set of *nonnegative integers*. Then by Lagrange's four-square theorem we have that

$$z \in A \leftrightarrow \exists x_1, x_2, x_3, x_4 \in \mathbb{Z} : z = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Thus A is diophantine.

Lemma 1.0.3. *The union and intersection of diophantine sets are diophantine.*

Proof. Let A, B be diophantine sets. Then A, B are the zero sets for some diophantine polynomials P, Q respectively. Therefore $A \cap B$ is the zero set of $P^2 + Q^2$ and $A \cup B$ is the zero set of $P \cdot Q$. □

Note: The complement of a diophantine set is not necesserily diophantine.

Yuri Matijasevič using the previous work of Martin Davis, Hilary Putnam and Julia Robinson, gave the last step for a negative answer to HTP in 1970. For his proof, Matijasevič combined results of elementary computability theory and logic. The definitions are from [19].

Definition 1.0.4. A subset A of $\mathbb{Z}$ is recursively enumerable if there exists an algortithm that prints the elements of A.

Definition 1.0.5. A set $A \subseteq \mathbb{Z}$ is recursive if there exists an algorithm that decides the membership in A, i.e. given an integer x, prints YES if $x \in A$ and NO otherwise.

It is easy to see that every recursive set is recursive enumerable, since given an algorithm for deciding membership in A, one can apply it with imput $0, 1, -1, 2, -2, \dots$ and print each number for which the algorithm returns YES. The question is whether the converse sentence holds, that is whether every recursive enumerable set is recursive or not.

Halting Problem asks for an algorithm that takes as an input a program P and an integer x and gives as an output YES if the program halts with the input x and NO otherwise.

Alan Turing in 1936 prooved that the halting problem is undecidable, meaning there is no Turing machine that can solve it[1]. Using the undecidability of the halting problem, one can constract a recursive enumerable set that is not recursive[2].

DPRM Theorem (Davis, Putnam, Robinson, Matijasevič). A subset A of $\mathbb{Z}$ is recursively enumerable if and only if it is diophantine.

We know that there exists a recursive enumerable set A that is not recursive. By the DPRM theorem, this is equivalent to having a diophantine set that is not recursive. Thus, there exists a diophantine polynomial $P(z, x_1, \dots, x_m)$ such that there is no algortithm for deciding for which values $a \in \mathbb{Z}$ the equation $P(a, x_1, \dots, x_m) = 0$ has a solution in $x_1, \dots, x_m \in \mathbb{Z}$. Consequently, one cannot find an algorithm that can decide the existence of integer solutions to all diophantine polynomial equations. Matijasevič's final step for the proof can be found in [11] and for the full proof, the reader is advised to see [1].

After the negative answer to HTP, researchers start to ask the same question as Hilbert for rings other than the integers. Let R be a commutative ring with unity and R' be a subring of R. We say that the **diophantine problem for *R*** (or HTP over R) with coefficients in R' is decidable if there exists an algorithm to decide whether or not a polynomial equation with coefficients in R' has a solution in R; otherwise we say it is undecidable. The question of whether the diophantine problem for R is decidable or undecidable depends on the ring R. We will now see some definitions (from [13], [16]), that we will use throughout the thesis.

A **language** $\mathcal{L}$ is a set consisting of all logical symbols and perhaps some symbols for relations, functions and constants. A **first-order sentence** of the language of a structure (model) is a sentence built using the symbols of the language. For example, if we take the language of rings $\mathcal{L}_r = \{+, \cdot, =, 0, 1\}$ and the structure of real numbers $\mathbb{R}$ then $\forall x, y \exists z : (x < z < y)$ is a first-order sentence.

[1] For details on Halting Problem and Turing machines, see Chapter 7 of [10]

[2] For details see Corollary 4 of [19]

An **existential sentence** is a sentence of the form $\exists x : S$, where S is a disjunction of systems of diophantine equations and inequations. When S involves only equations we say that the sentence is **positive existential**. The **(positive existential) theory** of a structure is the set of true (positive existential) sentences in the structure. We say that the theory of a structure is **decidable** if there exists an algorithm which can decide whether any given sentence is true or false in the structure; otherwise we say that the theory is **undecidable**.

Here is a brief list of results on the diophantine problem of varius rings and their theory. We mark YES for a decidable problem, NO for undecidable and ? for an open problem.

Ring	HTP	Theory
$\mathbb{Z}$	NO (Y. Matijasevič)	NO (K. Gödel)
$\mathbb{Q}$	?	NO (J. Robinson)
$\mathbb{R}$	YES (A. Tarski)	YES (A. Tarski)
$\mathbb{C}$	YES	YES (A. Robinson)
$\overline{\mathbb{Z}}$	YES (R. Rumely)	YES (L. van den Dries)
$\mathbb{F}_q$	YES	YES
$p-$adic fields	YES (A. Nerode)	YES (A. Macintyre, Ax-Kochen)
number field	?	NO (J. Robinson)
$\mathcal{O}_K$	?	NO (J.Robinson)
$R[t]$	NO (J. Denef)	NO
$\mathbb{R}(t)$	NO (J. Denef)	NO
$\mathbb{C}(t)$	?	?
$\mathbb{C}(t_1, \dots, t_n)$, $n \geq 2$	NO (K.H. Kim, F.W. Roush)	NO
$\mathbb{F}_q(t)$	NO (T. Pheidas, C. Videla)	NO (J. L. Eršov, J. G. Penzin)
$\mathbb{F}_q((t))$	?	?

For an extensive survey and more details, see [16]. In this master's thesis, we will focus on the diophantine problem for polynomial rings and subrings of rational functions. Let $R[t]$ be a polynomial ring and D a class of diophantine equations over $R[t]$. Notice that the analogue of HTP for $R[t]$ for the class D, asked for systems of diophantine equations (rather than a single one), is equivalent to the question of decidability of the positive existential theory of $R[t]$ in the lanuage $\mathcal{L}$ which contains symbols for the operations, relations and constants for the coefficients of the equations in D. For example, the analogue of HTP for $\mathbb{R}[t]$ with coefficients in $\mathbb{Z}$ is equivalent to the question of positive existential theory of $\mathbb{R}[t]$ in the language $\mathcal{L} = \{+, \cdot, =, 0, 1\}$, while the analogue with coefficients in $\mathbb{Z}[t]$ is equivalent to the question of decidability of the positive existential theory of $\mathbb{R}[t]$ in the language $\mathcal{L} = \{+, \cdot, =, 0, 1, t\}$.

Chapter 2

The diophantine problem for addition and localized divisibility

In this chapter we will introduce two relations, namely $|_n$ and $|^p$, that we will use later. In particular we will prove that the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}_{div_n} = \{0, 1, =, +, |_n\}$ is undecidable and as a corollary yields the undecidability of the positive existential theory of $\mathbb{Z}$ in the language that contains the addition, the divisibility and $|^p$. These results are due to J. Denef and can be found in [5].

Definition 2.0.1. Fix $n \in \mathbb{Z}$, $n > 1$ and p a prime number. We define the relations $|_n$, $|^p$ over $\mathbb{Z}$ by

$$x \,|_n\, y \leftrightarrow \exists q, s \in \mathbb{Z} : y = xqn^s$$

and

$$x \,|^p\, y \leftrightarrow \exists s \in \mathbb{N} : y = \pm x p^s.$$

The last relation is often referred to as **localized divisibility**.

Definition 2.0.2. Let $n, x, y \in \mathbb{Z}$ with $n > 1$. For every prime number p, we define $h(p)$ by

$$h(p) = \begin{cases} 0, \text{if } ny \text{ and } x \text{ are divisible by the same powers of } p \\ 1, \text{otherwise} \end{cases}$$

Lemma 2.0.3. *Let $n, x, y \in \mathbb{Z}$ with $n > 1$. If $h \equiv h(p) (mod\, p)$ then*

$$\forall s > 0 (p^s \,|\, ny - hx \rightarrow p^s \,|\, x).$$

Proof. If $h(p) = 0$ then ny and x are divisible by the same powers of p. Let p^r divide ny and x, for some $r \in \mathbb{N}_0$. Since $p^s \,|\, ny - hx$, we obtain that $p^s \,|\, p^r$, therefore $p^s \,|\, x$. If $h(p) = 1$, then ny and x are not divisible by the same powers of p. Let $r \in \mathbb{N}_0$ be the greater power of p that divides both ny and x. If $p^s \,|\, ny - hx$, for some $s \in \mathbb{N}$, then $p^s \,|\, p^r$, thus $p^s \,|\, x$. □

Lemma 2.0.4. *Let $n > 1$ and suppose $x|_n 1$ and $y|_n 1$. Then $y = x^2$ if and only if*

C1) $2nx + 1 \,|_n\, 4n^2y - 1$

C2) $2nx - 1 \,|_n\, 4n^2y - 1$

C3) $ny - kx \,|_n\, nx - k$*, for all* k *such that* $|k| < n$.

Proof. If $y = x^2$, then $4n^2y - 1 = 4n^2x^2 - 1 = (2nx + 1)(2nx - 1)$, so conditions C1), C2) hold. Since $x \,|_n\, 1$, there exist $q, s \in \mathbb{Z}$ such that $xqn^s = 1$. Therefore

$$\begin{aligned} nx - k &= (nx - k)xqn^s \\ &= (nx^2 - kx)qn^s \\ &= (ny - kx)qn^s. \end{aligned}$$

Thus condition C3) holds.

Conversely, assume that conditions C1)-C3) hold. Conditions C1) and C2) yield

$$\begin{aligned} 4n^2y - 1 = (2nx + 1)q_1n^{s_1} \\ 4n^2y - 1 = (2nx - 1)q_2n^{s_2}, \end{aligned}$$

for some $q_1, q_2, s_1, s_2 \in \mathbb{Z}$. Since $2nx + 1, 2nx - 1, n$ are pairwise relatively prime, we obtain that $(2nx+1)(2nx-1)$ divides $4n^2y-1$. In addition, we have that $n > 1$, thus $4n^2y-1 \neq 0$, therefore the last relation implies

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

Furthermore, we have that

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

thus we obtain that

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

Since x, y are both integers, we obtain that

$$x^2 \leq |y|.$$

To obtain the other direction inequality we will use condition C3). Let $n = p_1^{r_1} \cdots p_k^{r_k}$ be the factorization of n. By Chinese Remainder Theorem, there exist $h(\text{mod } n)$ such that $h \equiv h(p_i)(\text{mod } p_i)$, for every $i = 1, \ldots, k$. Choose h such that $|h| < n$ and $hx \geq 0$. Let a_j be the largest integer in $\{0, \ldots, r_j\}$ such that $p_j^{a_j} \,|\, ny - hx$, for each $j \in \{1, \ldots, k\}$. Then $p_1^{a_1} \cdots p_k^{a_k} \,|\, ny - hx$, so

$$ny - hx = p_1^{a_1} \cdots p_k^{a_k} l, \tag{2.0.1}$$

for some $l \in \mathbb{Z}$ with gcd$(l, p_j) = 1$, for each $j = 1, \ldots, k$. By lemma 2.0.3 we obtain that $p_j^{a_j} \,|\, x$, for each $j \in \{1, \ldots, k\}$, thus

$$p_1^{a_1} \cdots p_k^{a_k} \,|\, x. \tag{2.0.2}$$

Condition C3) yields $nx - h = (ny - hx)qn^s$, for some $q, s \in \mathbb{Z}$. Since $l \,|\, ny - hx$, we obtain that

$$l \,|\, nx - h. \tag{2.0.3}$$

Therefore, relations (2.0.1), (2.0.2),(2.0.3) yield

$$ny - hx \,|\, x(nx - h).$$

Thus $|ny - hx| \leq |x(nx - h)|$. Since $|h| < n$ and $x \neq 0$ (by $x \,|_n\, 1$), we have that $x(nx - h) > 0$. Hence,

$$\begin{aligned} |ny - hx| &\leq |x(nx - h)| \\ &= x(nx - h) \\ &= nx^2 - hx. \end{aligned}$$

Furthermore,

$$\begin{aligned} |ny - hx| &\geq |n|y| - |hx|| \\ &\geq n|y| - |hx| \\ &= n|y| - hx. \end{aligned}$$

Consequently, we obtain that $n|y| - hx \leq nx^2 - hx$, thus $|y| \leq x^2$. Therefore, we have that $y = \pm x^2$. Suppose that $y = -x^2$, then condition C1) yields $2nx + 1 \,|_n\, -4n^2x^2 - 1$, we obtain $2nx+1 \,|\, -4n^2x^2-1$. Since $2nx+1 \,|\, 4n^2x^2-1$, we conclude that $2nx+1 \,|\, (-4n^2x^2-1)+(4n^2x^2-1)$. So $2nx + 1 \,|\, -2$, which is a contradiction (since $n > 1$). Hence, the lemma follows. □

Lemma 2.0.5. *Let $x, u, z \in \mathbb{Z}$ and $n > 1$. Suppose that the following conditions hold:*

C4) $nz + nx - 1 \,|_n\, n^2u - (nx - 1)^2$

C5) $2nz + 1 \,|_n\, nx - 1$

C6) $2nz - 1 \,|_n\, nx - 1$

C7) $2n^2u + 1 \,|_n\, nx - 1$.

Then $u = z^2$.

Proof. Since n and $nz + nx - 1$ are relatively prime, condition C4) yields $nz + nx - 1$ divides $n^2u - (nx - 1)^2$. We have $nz + nx - 1 \,|\, (nz + nx - 1)(-nz + nx - 1)$, that is $nz + nx - 1 \,|\, (nx - 1)^2 - n^2z^2$. Consequently,

$$nz + nx - 1 \,|\, (n^2u - (nx - 1)^2) - ((nx - 1)^2 - n^2z^2) \Rightarrow nz + nx - 1 \,|\, n^2u - n^2z^2.$$

Suppose that $u \neq z^2$. Then

$$|nx - 1| - n|z| \leq |nz + nx - 1| \leq |n^2u - n^2z^2| \leq n^2|u| + n^2z^2. \tag{2.0.4}$$

Since $n, 2nz+1, 2nz-1$ are relatively prime to one another, C5) and C6) imply $(2nz+1)(2nz-1) \mid nx-1$ and since $nx-1 \neq 0$, we obtain that

$$4n^2z^2 - 1 \leq |nx-1|. \tag{2.0.5}$$

In the same way, since $\gcd(2n^2u+1, n) = 1$, we can replace the relation $|_n$ in C7) with the relation $|$. Hence

$$2n^2|u| - 1 \leq |2n^2u+1| \leq |nx-1|. \tag{2.0.6}$$

By (2.0.5),(2.0.6) yields

$$\begin{gathered} 4n^2z^2 - 1 + 2n^2|u| - 1 \leq 2|nx-1| \Rightarrow \\ 2n^2z^2 + n^2|u| - 1 \leq |nx-1| \Rightarrow \\ 2n^2z^2 + n^2|u| - n|z| - 1 \leq |nx-1| - n|z|. \end{gathered}$$

By (2.0.4) we have that

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

Suppose that $z \neq 0$. Since the roots of the polynomial $X^2 - X - 1$ are $\dfrac{1 \pm \sqrt{5}}{2}$, we obtain that $-1 < n|z| < 2$. However, $n > 1$ and $z \neq 0$, thus the previous inequation cannot hold. Hence, either $z = 0$ or $u = z^2$. If $z = 0$, from (2.0.4) and (2.0.6) we have that

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

Since $n > 1$, the above inequation holds only when $u = 0$. Hence the proof follows. □

Recall that $\varphi(n)$ denotes the *Euler's totient function*, that is the number of integers that are relatively prime to a given integer n.

Lemma 2.0.6. *For any nonzero integer d there exists an integer x such that $x \,|_n\, 1$ and $d \,|_n\, nx-1$.*

Proof. We write $d = d_0d_1$, where $d_0 \,|_n\, 1$ and $\gcd(d_1, n) = 1$. Set $x = n^{\varphi(d_1)-1}$. Then by Euler's Theorem we have that $n^{\varphi(d_1)} \equiv 1 (\text{mod } d_1)$. Therefore

$$nx - 1 \equiv nn^{\varphi(d_1)-1} - 1 \equiv 0 (\text{mod } d_1),$$

so $d_1 \mid nx-1$. Hence, from the previous relation and from $d_0 \,|_n\, 1$ we can easily deduce that $d \,|_n\, nx-1$. □

Lemma 2.0.7. *Let $n > 1$ and $u, z \in \mathbb{Z}$. Then $u = z^2$ if and only if there exist integers x, y such that $x \,|_n\, 1$, $y \,|_n\, 1$, conditions C1)-C3), C5)-C7) hold and*

$$nz + nx - 1 \,|_n\, n^2u - n^2y + 2nx - 1. \tag{2.0.7}$$

Proof. Suppose that $u = z^2$ and set $d = (2nz+1)(2nz-1)(2n^2u+1)$. Then, by lemma 2.0.6 there exists an integer x such that $x\,|_n\,1$ and $(2nz+1)(2nz-1)(2n^2u+1)\ |_n\, nx-1$. Hence, conditions C5)-C7) hold. Set $y = x^2$. Then $y\,|_n\,1$ and by lemma 2.0.4, conditions C1)-C3) hold. Furthermore, condition C4) implies

$$nz + nx - 1\,|_n\, n^2u - n^2x^2 + 2nx - 1 = n^2u - n^2y + 2nx - 1.$$

Conversely, suppose that there exist integers x, y that satisfy the conditions of the lemma. Then, by lemma 2.0.4 we obtain that $y = x^2$. Thus, (2.0.7) implies condition C4). Therefore, by lemma 2.0.7 we obtain that $u = z^2$ and the proof follows. □

Theorem 2.0.8. *Let $n > 1$. Then the positive existential theory of $\mathbb{Z}$ in $\mathcal{L}_{div_n}$ is undecidable, i.e. there is no algorithm for deciding the truth of positive existential formulas of $\mathbb{Z}$ in the language $\mathcal{L}_{div_n}$.*

Proof. We have the following equivalences:

$$\begin{aligned} z = x + y &\leftrightarrow 0\,|_n\,(x+y-z)\\ z = x\cdot y &\leftrightarrow 4w = (x+y)^2 - (x-y)^2. \end{aligned}$$

Therefore, we can express the addition of integers with a positive existential formula of $\mathbb{Z}$ in the language $\mathcal{L}_{div_n}$. By lemma 2.0.7, we can express the fact that an integer u is a square by a positive existential formula of $\mathbb{Z}$ in the language $\mathcal{L}_{div_n}$. Thus, we can also express the multiplication of integers by a positive existential formula of $\mathbb{Z}$ in $\mathcal{L}_{div^n}$. Consequently, if there was an algorithm that could decide the truth of positive existential sentences of $\mathbb{Z}$ in $\mathcal{L}_{div_n}$, we could convert it into an algorithm that could decide the truth of positive existential sentences of $\mathbb{Z}$ in the language $\{0, 1, =, +, \cdot\}$, which is a contradiction according to the negative answer of HTP in [11]. □

Corollary 2.0.9. *Let p a prime number. Then the positive existential theory of $\mathbb{Z}$ in the language $\{0, 1, =, +, |, |^p\}$ is undecidable.*

Proof. We have that

$$\begin{aligned} x\,|_p\,y &\leftrightarrow \exists q, s \in \mathbb{Z} : y = xqp^s\\ &\leftrightarrow \exists s, z \in \mathbb{Z} : x\,|\,z \wedge y = \pm zp^s\\ &\leftrightarrow \begin{cases} \exists z \in \mathbb{Z} : z\,|^p\,y \wedge x\,|\,z, \text{if } s \geq 0\\ \exists z \in \mathbb{Z} : y\,|^p\,z \wedge x\,|\,z, \text{otherwise} \end{cases} \end{aligned}$$

Therefore, if there was an algorithm for deciding the truth of positive existential sentences of $\mathbb{Z}$ in the language $\{0, 1, =, +, |, |^p\}$, we could convert it into an algorithm for deciding the truth of positive existential sentences of $\mathbb{Z}$ in the language $\mathcal{L}_{div_n}$, which is a contradiction according to theorem 2.0.8. □

Chapter 3

Positive existential theories of polynomial rings

Our purpose in this chapter is to examine the diophantine problem of polynomial ring $R[t]$ and Laurent polynomial ring $R[t, t^{-1}]$ with coefficients in $\mathbb{Z}[t]$. In particular, we will prove that both of them have undecidable positive existential theories using the Pell equation $X^2 - dY^2 = 1$ over $R[t]$ in various forms. For an extensive look on Pell equation, see [1]. For the algebraic background we use [7] and [9].

3.1 Main theorem

In August of 1978, J. Denef prooved in [4] that the diophantine problem of $R[t]$ (i.e. the ring of polynomials over R with the variable t) with coefficients lay in $\mathbb{Z}[t]$ is undecidable. Here we present his proof.

Throughout this section we consider R be an integral domain, with $\text{char}(R) = 0$. Note that the diophantine problem for $R[t]$ with coefficients in $\mathbb{Z}$ is solvable if and only if the diophantine problem for R with coefficients in $\mathbb{Z}$ is solvable. Because of that we examine the diophantine problem for $R[t]$ with coefficients in $\mathbb{Z}[t]$.

Now, we consider the Pell equation

$$X^2 - (t^2 - 1)Y^2 = 1 \tag{3.1.1}$$

over $R[t]$. Let $u \in \overline{R[t]}$ such that

$$u^2 = t^2 - 1. \tag{3.1.2}$$

Our aim is to find the solutions $(X, Y) \in R[t]^2$ of (3.1.1). To do so, we define two sequences $X_n, Y_n \in \mathbb{Z}[t]$, $n = 0, 1, 2, \dots$ by setting

$$X_n + uY_n = (t + u)^n. \tag{3.1.3}$$

Remark 3.1.1. From the above definition we observe that X_n, uY_n represent the rational and the irrational parts, respectively, of $(t + u)^n$ over $R[t]$.

So we have the following

Lemma 3.1.2. *The solutions* (X, Y) *of* (3.1.1) *are given by* $(\pm X_n, \pm Y_n)$, $n = 0, 1, 2, \ldots$.

Proof. First we will show that $(\pm X_n, \pm Y_n)$, $n = 0, 1, 2, \ldots$ satisfy (3.1.1). We have that (3.1.1) is equivalent to

$$(X + uY)(X - uY) = 1. \tag{3.1.4}$$

From (3.1.2) it becomes clear that the inverse of $(t + u)$ is $(t - u)$. Hence we have

$$\begin{aligned} X_n - uY_n &= (t - u)^n \\ &= ((t + u)^{-1})^n \\ &= (t + u)^{-n}. \end{aligned}$$

So $(X_n + uY_n, X_n - uY_n)$ satisfy (3.1.4), hence they are solutions of (3.1.1).

Conversely, suppose $(X, Y) \in R[t]^2$ a solution of (3.1.1). We parametrise the curve (3.1.2) by

$$t = \frac{s^2 + 1}{s^2 - 1}, \; u = \frac{2s}{s^2 - 1}.$$

Now, the rational functions $X(t) + uY(t), X(t) - uY(t)$ have poles only at $s = \pm 1$. The fact that the inverse of $X + uY$ is $X - uY$ implies that they have also zeroes at $s = \pm 1$. Therefore,

$$X + uY = c\frac{(s + 1)^{m_1}}{(s - 1)^{m_2}}, \; c \in R, m_1, m_2 \in \mathbb{Z}. \tag{3.1.5}$$

We will show that $m_1 = m_2$. Suppose (without the loss of generality) that $m_2 < m_1$. Then (3.1.5) is equivalent to

$$X + uY = c\left(\frac{s + 1}{s - 1}\right)^{m_2} (s + 1)^{m_1 - m_2} = c(t + u)^{m_2}(s + 1)^{m_1 - m_2}$$

hence $X - uY = c(t - u)^{m_2}(s + 1)^{m_1 - m_2}$. Thus, by (3.1.2) and (3.1.4) we have

$$c^2(s + 1)^{2(m_1 - m_2)} = 1$$

which means that $m_1 = m_2$ and $c^2 = 1$. Therefore by the definition (3.1.3), the pair (X, Y) either equals to (X_{m_1}, Y_{m_1}) or to $(-X_{m_1}, -Y_{m_1})$ (according to whether $c = 1$ or $c = -1$ respectevily), which completes the proof of the lemma. □

Definition 3.1.3. Let R be a commutative ring with unity and let $D(X_1, \ldots, X_n)$ be a relation in R. We say that $D(X_1, \ldots, X_n)$ is diophantine over R if there exists a polynomial $P(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ such that

$$\forall X_1, \ldots, X_n \in R\, [D(X_1, \ldots, X_n) \leftrightarrow \exists Y_1, \ldots, Y_m \in R : P(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = 0].$$

Lemma 3.1.4. *Let* R *be an integral domain. If the relations* D_1, D_2 *are diophantine over* $R[t]$ *with coefficients in* $\mathbb{Z}[t]$ *then the relations* $D_1 \vee D_2$ *and* $D_1 \wedge D_2$ *are also diophantine.*

Proof. Since D_1, D_2 are diophantine over $R[t]$ with coefficients in $\mathbb{Z}[t]$ then there exist polynomials P_1, P_2 over $R[t]$ as described in the definition. Then

$$D_1 \vee D_2 \leftrightarrow P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 P_2 = 0$$

and

$$D_1 \wedge D_2 \leftrightarrow P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + tP_2^2 = 0.$$

□

Example 3.1.5. Let D be the *ordering relation* on positive integers, that is $D(x, y) \leftrightarrow x < y$. We have already seen at the example 1.0.2 that the expression $x > 0$ is diophantine. So we have

$$D(x, y) \leftrightarrow \exists z \in \mathbb{Z} : z > 0 \wedge (x + z = y).$$

Thus D is diophantine.

We define the relation $\sim$ over $R[t]$ such that

$$V \sim W \leftrightarrow V|_{t=1} = W|_{t=1}.$$

Remark 3.1.6. Notice that $V \sim 0$ is diophantine over $R[t]$ with coefficients in $\mathbb{Z}[t]$ since

$$V \sim 0 \leftrightarrow \exists X \in R[t] : V = (t-1)X.$$

Lemma 3.1.7. $Y_n \sim n$ *for* $n = 0, 1, 2, \ldots$.

Proof. By (3.1.3) we have that

$$X_n + uY_n = \sum_{i=0}^{n} \binom{n}{i} u^i t^{n-i}.$$

By Remark 3.1.1 we have that Y_n is the irrational part of u in the sum $\sum_{i=0}^{n} \binom{n}{i} u^i t^{n-i}$ and (3.1.2) implies that u to an even power lays in $R[t]$. Hence the irrational part is

$$\begin{aligned} Y_n &= \sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i} u^{i-1} t^{n-i} \\ &= \sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i} (t^2-1)^{\frac{i-1}{2}} t^{n-i}. \end{aligned}$$

By substituting $t = 1$ the lemma follows. □

We define the relation Imt over $R[t]$ by

$$Imt(Y) \leftrightarrow Y \in R[t] \wedge \exists X \in R[t] : X^2 - (t^2-1)Y^2 = 1.$$

So we have the following

Lemma 3.1.8. 1. *The relation $Imt(Y)$ is diophantine over $R[t]$ with coefficients in $\mathbb{Z}[t]$.*

2. *If Y satisfies $Imt(Y)$, then there exists an integer m such that $Y \sim m$.*

3. *For every integer m there exists a polynomial Y satisfying $Imt(Y)$ and $Y \sim m$.*

Proof. 1. It follows directly from definition of the relation Imt.

2. If Y satisfies $Imt(Y)$ then there exists a polynomial $X \in R[t]$ such that (X, Y) satisfy (3.1.1). Therefore, by lemma 3.1.2 we have that $Y = \pm Y_m$, for some $m = 0, 1, 2, \dots$ hence by lemma 3.1.7 the proof follows.

3. We take $Y = Y_m$ if $m > 0$ and $Y = -Y_{-m}$ if $m < 0$. Therefore by lemmas 3.1.2, 3.1.7 the proof follows.

□

Theorem 3.1.9. *The diophantine problem for $R[t]$ with coefficients in $\mathbb{Z}[t]$ is undecidable.*

Proof. To prove this we need to find an algorithm which given a polynomial $P(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ is able to find a polynomial $\tilde{P}(X_1, \dots, X_n) \in (\mathbb{Z}[t])[X_1, \dots, X_n]$ such that

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t] : \tilde{P}(Z_1, \dots, Z_n) = 0. \quad (3.1.6)$$

Let P be a polynomial of n variables and with coefficients lay in $\mathbb{Z}$. By lemma 3.1.8(2,3) we have that

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t] : \bigwedge_{i=1}^{n}(Imt(Z_i)) \wedge P(Z_1, \dots, Z_n) \sim 0.$$

The fact that the relations $\sim$ and Imt are diophantine over $R[t]$ with coefficients in $\mathbb{Z}[t]$, along with lemma 3.1.4, gives us a polynomial $\tilde{P}$ satisfying (3.1.6). Hence if the diophantine problem for $R[t]$ with coefficients in $\mathbb{Z}[t]$ was solvable, then the diophantine problem for $\mathbb{Z}$ would be solvable, which is a contradiction to HTP as Matijasevič has shown in [11]. □

3.2 Laurent polynomial ring

Let R be an integral domain, with $\text{char}(R) = 0$. We define the **Laurent polynomial ring** as the ring $R[t, t^{-1}]$, that is the polynomials in the variables t, t^{-1} with coefficients lay in R.

Notation 3.2.1. Let $P = \sum_{i=r}^{r'} \alpha_i t^i$ an element of $R[t, t^{-1}]$, with $r, r' \in \mathbb{Z}$ and $r \leq r'$. We define $\deg_{\text{min}}(P) = r$ and $\deg(P) = r'$.

3.2.1 The diophantine problem of Laurent polynomial ring

Using the same ideas and methods as Denef's, Peter Pappas proved in [12] that the diophantine problem for the Laurent polynomial ring $R[t, t^{-1}]$ with coefficients in $\mathbb{Z}[t]$ is undecidable. The result is not unexpected but the interesting difference here is that we consider two cases; namely $i \notin R$ and $i \in R$. For the proof we need the following result from Denef in [3] (its generalization is in [6]).

Theorem 3.2.2. *The diophantine problem for the ring of Gaussian integers $\mathbb{Z}[i]$ with coefficients in $\mathbb{Z}$ is undeciable.*

Let R be an integral domain, with $\mathrm{char}(R) = 0$. In this section we will use the same notation as in the previous one, meaning we will work with the Pell equation (3.1.1) over $R[t, t^{-1}]$ and we define $u \in \overline{R[t, t^{-1}]}$ as in (3.1.2). Let $X, Y \in R[t, t^{-1}]$ which satisfy (3.1.1). Now, $X + uY$ is an algebraic function of t, so it can be written as

$$\frac{g(t)}{t^r} + \frac{\sqrt{t^2-1}f(t)}{t^k},$$

with $f(t), g(t) \in R[t]$. We parametrize the curve (3.1.2) by

$$t = \frac{s^2+1}{s^2-1},\ u = \frac{2s}{s^2-1}.$$

As rational functions of s, $X + uY$, $X - uY$ have poles only at $s = \pm 1$ and $s = \pm i$. From (3.1.4) we can see that they also have zeros at $s = \pm 1, \pm i$. Following the same argument as in the proof of lemma 3.1.2 one can easily see that

$$X + uY = c\left(\frac{s-1}{s+1}\right)^m \left(\frac{s-i}{s+i}\right)^n,$$

for some $c \in R$, $m, n \in \mathbb{Z}$. Observe that $(X + uY)(-s) = (X - uY)(s)$ and since $X + uY$ is the inverse of $X - uY$ by (3.1.4), we conclude that

$$X - uY = c\left(\frac{s-1}{s+1}\right)^{-m} \left(\frac{s-i}{s+i}\right)^{-n}.$$

By substituting the above expressions in (3.1.4), yields $c^2 = 1$. Suppose that $c = 1$ (the case $c = -1$ can be treated the exact same way). Therefore, $X + uY$ takes the form

$$\begin{aligned} X + uY &= c\left(\frac{s-1}{s+1}\right)^m \left(\frac{s-i}{s+i}\right)^n \\ &= c\left(\frac{s-1}{s+1}\right)^m \left(\frac{s-i}{s+i}\frac{s-i}{s-i}\right)^n \\ &= c\,(t+u)^m \left(\frac{s^2-1}{s^2+1} - i\frac{2s}{s^2+1}\right)^n \\ &= (t+u)^m \left(\frac{1-iu}{t}\right)^n. \end{aligned}$$

Since $(t+u) = (t-u)^{-1}$, we conclude $(t+u)^m = (t-u)^{-m}$ and $\left(\frac{1+iu}{t}\right)^n = \left(\frac{1-iu}{t}\right)^{-n}$. Hence, we can rewrite $X + uY$, $X - uY$ as expressions involving exponents $m, n \in \mathbb{N}_0$. Therefore, if $(X, Y) \in R[t, t^{-1}]^2$ is a solution of (3.1.1), we have one of the following outcomes with $m, n \in \mathbb{N}_0$

- $X + uY = (t+u)^m \left(\dfrac{1-iu}{t}\right)^n$

  $X - uY = (t-u)^m \left(\dfrac{1+iu}{t}\right)^n$

- $X + uY = (t+u)^m \left(\dfrac{1+iu}{t}\right)^n$

  $X - uY = (t-u)^m \left(\dfrac{1-iu}{t}\right)^n$

- $X + uY = (t-u)^m \left(\dfrac{1-iu}{t}\right)^n$

  $X - uY = (t+u)^m \left(\dfrac{1+iu}{t}\right)^n$

- $X + uY = (t-u)^m \left(\dfrac{1+iu}{t}\right)^n$

  $X - uY = (t+u)^m \left(\dfrac{1-iu}{t}\right)^n$

Let $S = \mathbb{Z}[i][t, t^{-1}]$, then by (3.1.2) $S[u]$ is a quadratic ring extension of S. We define two sequences $X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)} \in S$, for $j = 1, 2, 3, 4$ and $(m, n) \in \mathbb{N}_0^2$ by

$$\begin{aligned}
X^{(1)}_{(m,n)} + uY^{(1)}_{(m,n)} &= (t+u)^m \left(\frac{1-iu}{t}\right)^n, \\
X^{(2)}_{(m,n)} + uY^{(2)}_{(m,n)} &= (t+u)^m \left(\frac{1+iu}{t}\right)^n, \\
X^{(3)}_{(m,n)} + uY^{(3)}_{(m,n)} &= (t-u)^m \left(\frac{1-iu}{t}\right)^n, \\
X^{(4)}_{(m,n)} + uY^{(4)}_{(m,n)} &= (t-u)^m \left(\frac{1+iu}{t}\right)^n.
\end{aligned}$$

Applying the ring automorphism of $S[u]$, which fixes the elements of S and sends u to $-u$, along with (3.1.2), we have

$$\begin{aligned}
X^{(1)}_{(m,n)} - uY^{(1)}_{(m,n)} &= (t-u)^m \left(\frac{1+iu}{t}\right)^n = (t+u)^{-m} \left(\frac{1-iu}{t}\right)^{-n}, \\
X^{(2)}_{(m,n)} - uY^{(2)}_{(m,n)} &= (t-u)^m \left(\frac{1-iu}{t}\right)^n = (t+u)^{-m} \left(\frac{1+iu}{t}\right)^{-n}, \\
X^{(3)}_{(m,n)} - uY^{(3)}_{(m,n)} &= (t+u)^m \left(\frac{1+iu}{t}\right)^n = (t-u)^{-m} \left(\frac{1-iu}{t}\right)^{-n}, \\
X^{(4)}_{(m,n)} - uY^{(4)}_{(m,n)} &= (t+u)^m \left(\frac{1-iu}{t}\right)^n = (t-u)^{-m} \left(\frac{1+iu}{t}\right)^{-n}.
\end{aligned}$$

Therefore, the pair $\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right)$ is a solution of (3.1.1), for every $(m, n) \in \mathbb{N}_0^2$ and each $j = 1, 2, 3, 4$. Hence we have the following lemma.

Lemma 3.2.3. *The solutions of the equation* (3.1.1) *over* $R[t,t^{-1}]$ *are of the form*

a) $\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right)$, $(m,n)\in\mathbb{N}_0^2, j=1,2,3,4$, *if* $i\in R$

b) $\left(X^{(j)}_{(m,0)}, Y^{(j)}_{(m,0)}\right)$, $m\in\mathbb{N}_0, j=1,2,3,4$, *if* $i\notin R$.

Proof. In the case $i\in R$ we have already seen that $(X,Y)\in R[t,t^{-1}]$ is a solution of (3.1.1) if and only if it is of the form a). For the case $i\notin R$ it remains to show that for every $m\in\mathbb{N}_0, n\in\mathbb{N}$ and $j=1,2,3,4$

$$\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right)\notin R[t,t^{-1}]^2.$$

We fix $x=X^{(j)}_{(m,n)}, y=Y^{(j)}_{(m,n)}$ for some $m\in\mathbb{N}_0, n\in\mathbb{N}, j\in\{1,2,3,4\}$. Assume that $(x,y)\in R[t,t^{-1}]$. Let $\sigma: S[u]\to S[u]$ be the ring automorphism, which fixes u and t and sends i to $-i$. Then $\sigma(x+uy)=x+uy$, which by the definitions of $X^{(j)}_{(m,n)}+uY^{(j)}_{(m,n)}$ for $j=1,2,3,4$, implies that

$$\left(\frac{1+iu}{t}\right)^n=\left(\frac{1-iu}{t}\right)^n,$$

which is possible only for $n=0$. This contradicts with the assumption that n belongs to $\mathbb{N}$, hence the lemma follows. □

Next we define the relations $\sim, Imt(Y)$ as in the previous section, i.e. for $V,W\in R[t,t^{-1}]$

$$V\sim W\leftrightarrow V|_{t=1}=W|_{t=1} \text{ and}$$
$$Imt(Y)\leftrightarrow Y\in R[t,t^-1]\wedge\exists X\in R[t,t^{-1}]: X^2-(t^2-1)Y^2=1.$$

Notice that the relations $Z\sim 0, Imt(Y)$ are diophantine over $R[t,t^{-1}]$ with coefficients in $\mathbb{Z}[t]$, as shown in remark 3.1.6 and in lemma 3.1.8 respectively.

Lemma 3.2.4. *Let* $A=\{Y|_{t=1}: Imt(Y) \text{ holds}\}$.

a) If $i\in R$ *then* $A=\mathbb{Z}[i]$.

b) If $i\notin R$ *then* $A=\mathbb{Z}$.

Proof. We will use the same ideas as in the proof of lemma 3.1.7. Note that

$$Y^{(j)}_{(m,n)}=\frac{\left(X^{(j)}_{(m,n)}+uY^{(j)}_{(m,n)}\right)-\left(X^{(j)}_{(m,n)}-uY^{(j)}_{(m,n)}\right)}{2u}.$$

Applying the definitions of $X^{(j)}_{(m,n)}+uY^{(j)}_{(m,n)}$ for $j=1,2,3,4$ in the above form, yields $Y^{(2)}_{(m,n)}=-Y^{(3)}_{(m,n)}$ and $Y^{(1)}_{(m,n)}=-Y^{(4)}_{(m,n)}$. Therefore

- If $m > 0, n > 0$,

$$t^n Y^{(2)}_{(m,n)} = \frac{1}{2u}((t+u)^m(1+iu)^n - (t-u)^m(1-iu)^n)$$

$$= \frac{1}{2u}\left(\left(\sum_{j=0}^{m}\binom{m}{j}t^{m-j}u^j\right)\left(\sum_{j=0}^{n}\binom{n}{j}(iu)^j\right) - \left(\sum_{j=0}^{m}\binom{m}{j}t^{m-j}(-u)^j\right)\left(\sum_{j=0}^{n}\binom{n}{j}(-iu)^j\right)\right)$$

$$= \frac{1}{2u}2\left(\left(\sum_{\substack{j=0\\ j \text{ odd}}}^{m}\binom{m}{j}t^{m-j}u^j\right)\left(\sum_{\substack{j=0\\ j \text{ even}}}^{n}\binom{n}{j}(iu)^j\right) - \left(\sum_{\substack{j=0\\ j \text{ even}}}^{m}\binom{m}{j}t^{m-j}u^j\right)\left(\sum_{\substack{j=0\\ j \text{ odd}}}^{n}\binom{n}{j}(-iu)^j\right)\right)$$

$$= \left(\sum_{\substack{j=0\\ j \text{ odd}}}^{m}\binom{m}{j}t^{m-j}u^{j-1}\right)\left(\sum_{\substack{j=0\\ j \text{ even}}}^{n}\binom{n}{j}(iu)^j\right) - \left(\sum_{\substack{j=0\\ j \text{ even}}}^{m}\binom{m}{j}t^{m-j}u^j\right)\left(\sum_{\substack{j=0\\ j \text{ odd}}}^{n}\binom{n}{j}(-i)^j u^{j-1}\right)$$

$$= t^n Y^{(1)}_{(m,n)}.$$

- If $m > 0, n = 0$

$$t^n Y^{(2)}_{(m,0)} = \sum_{\substack{j=0\\ j \text{ odd}}}^{m}\binom{m}{j}t^{m-j}u^{j-1} = t^n Y^{(1)}_{(m,0)}.$$

- If $m = 0, n > 0$

$$t^n Y^{(1)}_{(0,n)} = \sum_{\substack{j=0\\ j \text{ odd}}}^{n}\binom{n}{j}(-i)^j u^{j-1}$$

and

$$t^n Y^{(2)}_{(0,n)} = \sum_{\substack{j=0\\ j \text{ odd}}}^{n}\binom{n}{j}i^j u^{j-1}.$$

Substituting u with $(t^2-1)^{\frac{1}{2}}$ and setting $t = 1$, the result for the first case is $m - n, (m,n) \in \mathbb{N}$, for the second $m, m \in NN_0$ and for the third $n, n \in \mathbb{N}_0$. Hence the lemma follows. □

Theorem 3.2.5. *The diophantine problem for $R[t, t^{-1}]$ with coefficients in $\mathbb{Z}[t]$ is undecidable.*

Proof. a) *Case $i \in R$.* By lemma 3.2.4 we have

$$\exists z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Z_1, \ldots, Z_n \in R[t, t^{-1}] : \\ \bigwedge_{j=1}^{n}(Imt(Z_j)) \wedge P(Z_1, \ldots, Z_n) \sim 0.$$

Since $\sim$ and Imt are diophantine, we can construct an algorithm which given a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ is able to find a plynomial $\tilde{P} \in \mathbb{Z}[t][X_1, \ldots, X_n]$ such that

$$\exists z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Z_1, \ldots, Z_n \in R[t, t^{-1}] : \tilde{P}(Z_1, \ldots, Z_n) = 0.$$

Thus, if the diophantine problem for $R[t,t^{-1}]$ with coefficients in $\mathbb{Z}[t]$ was decidable, then so would be the diophantine problem for $\mathbb{Z}[i]$ with coefficiens in $\mathbb{Z}$, which contradicts theorem 3.2.2, in [3].

b) *Case* $i \notin R$. In the exact same way as in the previous case, by lemma 3.2.4 we have

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t,t^{-1}] : \\ \bigwedge_{j=1}^{n}(Imt(Z_j)) \wedge P(Z_1, \dots, Z_n) \sim 0.$$

Therefore, we can construct an algorithm which given a polynomial $P \in \mathbb{Z}[x_1, \dots, x_n]$ is able to find a plynomial $\tilde{P} \in \mathbb{Z}[t][X_1, \dots, X_n]$ such that

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Z_1, \dots, Z_n \in R[t,t^{-1}] : \tilde{P}(Z_1, \dots, Z_n) = 0.$$

Thus, if the diophantine problem for $R[t,t^{-1}]$ with coefficients in $\mathbb{Z}[t]$ was decidable, then so would be the HTP, which contradicts the negative answer of HTP in [11].

□

3.2.2 Undecidability for addition and divisibility

Let R be an integral domain, with $\text{char}(R) = 0$. We will study the diophantine problem for addition and devisibility in the Laurent polynomial ring $R[t,t^{-1}]$, i.e the positive existential theory of $R[t,t^{-1}]$ in the language $\mathcal{L}_{\text{div}} = \{0, 1, =, +, |, t\}$. The results are due to T. Pheidas and can be found in [14].

Proposition 3.2.6. *The set of units of* $R[t,t^{-1}]$ *is* $R[t,t^{-1}]^* = \{ct^m : c \in R^*, m \in \mathbb{Z}\}$.

Proof. Assume x a unit of the ring $R[t,t^{-1}]$. Then there exists $y \in R[t,t^{-1}]$ such that $xy = 1$. Let $r, s \in \mathbb{Z}$ so that $\deg_{\text{min}}(x) = r$, $\deg_{\text{min}}(y) = s$. Therefore, $x = t^r f_1(t)$ and $y = t^s f_2(t)$ for some polynomials $f_1, f_2 \in R[t]$. Since $xy = 1$ we have that

$$f_1(t)f_2(t) = t^{-(r+s)}. \tag{3.2.1}$$

Observe that if the product of two polynomials of $R[t]$ is a monomial, then the factors have to be monomials[1]. Indeed, assume $r_0 = \deg_{\text{min}}(f_1), s_0 = \deg_{\text{min}}(f_2)$ and r_1, s_1 the degree of f_1, f_2, respectively. Then $\deg_{\text{min}}(f_1 f_2) = r_0 + s_0$ and $\deg(f_1 f_2) = r_1 + s_1$. Thus, by (3.2.1) we have $r_0 + s_0 = r_1 + s_1$. We have that $r_0 \leq r_1$ and $s_0 \leq s_1$. Suppose that $r_0 < r_1$, then

$$r_0 + s_0 < r_1 + s_0 \leq r_1 + s_1 \Leftrightarrow r_0 + s_0 < r_1 + s_1$$

which is a contradiction. Therefore, $r_0 = r_1$ so we also obtain that $s_0 = s_1$. Consequently, $x = ct^m$, $c \in R^*$, $m \in \mathbb{Z}$. □

Lemma 3.2.7. $t^n - 1 \,|\, t^m - 1$ *in* $R[t,t^{-1}]$ *if and only if* $n \,|\, m$ *in* $\mathbb{Z}$.

Proof. Assume that $t^n - 1 \,|\, t^m - 1$ in $R[t,t^{-1}]$. Then $t^m - 1 = P(t^n - 1)$, for some $P \in R[t,t^{-1}]$. Hence, we have

[1] The observation also holds for polynomials in $R[t,t^{-1}]$.

$$\begin{gathered}\frac{t^m-1}{t-1}=P\frac{t^n-1}{t-1}\Rightarrow\\ t^{m-1}+\cdots+t+1=P(t^{n-1}+\cdots+t+1)\Rightarrow\\ t^{m-1}+\cdots+t+1\equiv P(t^{n-1}+\cdots+t+1)(\text{mod}\,t-1)\Rightarrow\\ m\equiv kn(\text{mod}\,t-1)\end{gathered}$$

for some $k\in\mathbb{Z}$. Since m,n,k are constants we have $m=kn$, thus n divides m in $\mathbb{Z}$. Conversely, suppose that n divides m in $\mathbb{Z}$,thus $m=kn$, for some $k\in\mathbb{Z}$. Then

$$\begin{aligned}t^m-1&=t^{kn}-1\\&=(t^n-1)(t^{(k-1)n}+\cdots+t^n+1).\end{aligned}$$

Therefore, t^n-1 divides t^m-1 in $F[t,t^{-1}]$. □

Lemma 3.2.8. *If $k\in\mathbb{Z}^*$ and $n\in\mathbb{Z}$ then*

$$\frac{t^{kn}-1}{t^k-1}\equiv n(mod\,t^k-1)$$

Proof. If $n=0$, then the result is obvious. Suppose $n>0$, so

$$\frac{t^{kn}-1}{t^k-1}=1+t^k+t^{2k}+\cdots+t^{(n-1)k}\equiv n(\text{mod}\,t^k-1).$$

□

Lemma 3.2.9. *If $k\in\mathbb{Z}$ then $\dfrac{t^k-1}{t-1}\equiv 1(mod\,t+1)$ if and only if k is odd.*

Proof. Suppose that $k>0$ (the case $k\leq 0$ is similar), then

$$\frac{t^k-1}{t-1}=1+t+\cdots+t^{k-1}=\begin{cases}0\,(\text{mod}\,t+1), & \text{if } k \text{ is even}\\ 1\,(\text{mod}\,t+1), & \text{if } k \text{ is odd.}\end{cases}$$

□

Lemma 3.2.10. *For any $x\in R[t,t^{-1}]$, $x=t^m$, $m\in\mathbb{Z}$ if and only if x divides 1 and $t-1$ divides $x-1$ in $R[t,t^{-1}]$.*

Proof. If $x=t^m$, $m\in\mathbb{Z}$ then $t^mt^{-m}=1$ so $x\,|\,1$ and $t^m-1=(t-1)(t^{m-1}+\cdots+t+1)$ so $t-1|x-1$.

Conversely, suppose that $x\mid 1$ and $t-1\mid x-1$. Then x is a unit of $R[t,t^{-1}]$, therefore by proposition 3.2.6 we have that $x=ct^m$ for some $c\in R^*$, $m\in\mathbb{Z}$. Furthermore,

$$\begin{aligned}t-1|x-1&\Leftrightarrow ct^m-1\equiv 0\,(\text{mod}\,t-1)\\&\Leftrightarrow ct^m\equiv 1\,(\text{mod}\,t-1)\\&\Leftrightarrow c\equiv 1\,(\text{mod}\,t-1)\end{aligned}$$

Since c is a constant we obtain that $c=1$. □

Lemma 3.2.11. *i) If $2 \in R^*$, then for any $n \in \mathbb{Z}$, $t^n \neq 1$ if and only if there exist an integer k and $a, b \in R[t, t^{-1}]$ such that the following formula $\psi_1(t^n, t^k, a, b)$ is true:*

$$t^k - 1 \,|\, t^n - 1 \wedge t^2 - 1 \,|\, (t^k - 1) - (t - 1) \wedge \\ t^n - 1 \,|\, a \wedge (t - 1)(t^k - 1) \,|\, b \wedge a + b = t^k - 1.$$

ii) If $2 \notin R^*$ then for any $n \in \mathbb{Z}$, $t^n \neq 1$ if and only if there exist an integer k and $a, b \in R[t, t^{-1}]$ such that the following formula $\psi_2(t^n, t^k, a, b)$ is true:

$$(t^3 - 1 \,|\, t^{k+1} - 1 \vee t^3 - 1 \,|\, t^k - t) \wedge t^k - 1 \,|\, t^n - 1 \wedge \\ (t - 1)(t^k - 1) \,|\, a \wedge t^k - 1 \,|\, b \wedge t^n - 1 = t^k - 1 + a + 2b.$$

iii) For any $m, n \in \mathbb{Z}$, $m \neq n$ if and only if there exists an integer r such that the following formula $\psi_3(t^r, t^m, t^n)$ is true:

$$r \neq 0 \wedge t^m - t^n \,|\, t^r - 1.$$

Proof. i) Suppose that $t^n \neq 1$, so $n \neq 0$. Let $n = 2^s k$, with $s \in \mathbb{Z}$ and k odd. By lemma 3.2.7 we obtain the relation $t^k - 1 \mid t^n - 1$. Since k is odd, by lemma 3.2.9 we have that $t+1 \left| \frac{t^k - 1}{t - 1} - 1 \right.$, so $t^2 - 1 \,|\, (t^k - 1) - (t - 1)$. Lemma 3.2.8 implies $\frac{t^n - 1}{t^k - 1} \equiv 2^s (\bmod\, t^k - 1)$, therefore $\frac{t^n - 1}{t^k - 1} \equiv 2^s (\bmod\, t - 1)$. Thus, there exists a $z \in R[t, t^{-1}]$ such that $\frac{t^n - 1}{t^k - 1} = z(t - 1) + 2^s$. Since 2 is a unit of R, we have that

$$2^{-s}(t^n - 1) - 2^{-s} z(t - 1)(t^k - 1) = t^k - 1. \tag{3.2.2}$$

Let $a = 2^{-s}(t^n - 1)$ and $b = -2^{-s} z(t - 1)(t^k - 1)$. Thus, $t^n - 1 \,|\, a$, $(t - 1)(t^k - 1) \,|\, b$ and by (3.2.2) $a + b = t^k - 1$. Hence $\psi_1(t^n, t^k, a, b)$ holds. Conversely, suppose that there exist $k \in \mathbb{Z}$ and $a, b \in R[t, t^{-1}]$ such that $\psi_1(t^n, t^k, a, b)$ holds true. We have that

$$t^2 - 1 \,|\, (t^k - 1) - (t - 1) \Leftrightarrow \\ t + 1 \left| \frac{t^k - 1}{t - 1} - 1 \right. ,$$

thus by lemma 3.2.9 we obtain that k is odd. Assume that $n = 0$. By the relation $t^n - 1 \,|\, a$ we obtain that $a = 0$. Since $a + b = t^k - 1$, we conclude that $b = t^k - 1$. Therefore, $(t - 1)(t^k - 1) \mid t^k - 1$. Since k is odd number we have that $k \neq 0$, thus $t - 1 \mid 1$ which contradicts Proposition 3.2.6. Hence $n \neq 0$ and $t^n \neq 1$.

ii) Suppose that $t^n \neq 1$. Let $n = 3^s k$, with $s \in \mathbb{Z}$ and $k \not\equiv 0 (\bmod\, 3)$. If $k \equiv 1 (\bmod\, 3)$, then $k = 3m + 1$ for some $m \in \mathbb{Z}$. Hence $t^k - t = t(t^{3m} - 1)$, so $t^3 - 1 \,|\, t^k - t$. If $k \equiv 2 (\bmod\, 3)$, then $k = 3m' + 2$ for some $m' \in \mathbb{Z}$. Hence $t^{k+1} - 1 = t^{3(m'+1)} - 1$, so $t^3 - 1 \,|\, t^{k+1} - 1$. Furthermore, $t^k - 1 \,|\, t^n - 1$ and by lemma 3.2.8 we obtain

$$\frac{t^n - 1}{t^k - 2} \equiv 3^s (\bmod\, t^k - 1).$$

Thus $\dfrac{t^n-1}{t^k-1} \equiv 3^s (\bmod\, t-1)$, so there exists $z \in R[t,t^{-1}]$ such that $\dfrac{t^n-1}{t^k-1} = z(t-1)+3^s$. Let $3^s = 2l+1$, for some $l \in R$. Then

$$\frac{t^n-1}{t^k-1} = z(t-1)+2l+1. \tag{3.2.3}$$

Let $a = z(t-1)(t^k-1)$ and $b = l(t^k-1)$. Then $(t-1)(t^k-1)\,|\,a$, $t^k-1\,|\,b$ and by relation (3.2.3) we obtain that $t^n-1 = t^k-1+a+2b$. Thus $\psi_2(t^n,t^k,a,b)$ holds. Conversely, suppose that there exist $k \in \mathbb{Z}$ and $a,b \in R[t,t^{-1}]$ such that $\psi_2(t^n,t^k,a,b)$ is true. Assume that $n=0$. If the relation $t^3-1\,|\,t^{k+1}-1$ holds, then $k+1=3m$ for some $m \in \mathbb{Z}$, thus $k \equiv 2(\bmod\, 3)$. If the relation $t^3-1\,|\,t(t^{k-1}-1)$ holds, then $k-1=3m'$ for some $m' \in \mathbb{Z}$, thus $k \equiv 1(\bmod\, 3)$. In either case we obtain $k \neq 0$. Relations $(t-1)(t^k-1)\,|\,a$ and $t^k-1\,|\,b$ imply that there exist $z,w \in R[t,t^{-1}]$ such that $a=(t^k-1)(t-1)z$ and $b=(t^k-1)w$. Therefore, the relation $t^n-1 = t^k-1+a+2b$ yields $0=(t^k-1)(1+(t-1)z+2w)$ and since $k \neq 0$ we obtain

$$1+(t-1)z+2w=0.$$

Hence, $1+2w \equiv 0(\bmod\, t-1) \Rightarrow 1+2l \equiv 0(\bmod\, t-1)$, for some $l \in \mathbb{Z}$. Since $1+2l$ is a constant, we have that $2l+1=0$, thus $2 \in R^*$, which cantradicts to our hypothesis. Consequently, $n \neq 0$ and $t^n \neq 1$.

iii) Suppose that $m \neq n$ and (without the loss of generality) $m > n$. Let $r = m-n$. Then $t^m = t^r t^n \equiv t^n (\bmod\, t^r-1)$. Therefore, $t^m - t^n\,|\,t^r-1$ and $r \neq 0$. Conversely, suppose that $\psi_3(t^r,t^m,t^n)$ holds for some $r \in \mathbb{Z}$. Assume that $m=n$. Then $0\,|\,t^r-1$, so $t^r-1=0$, which contradicts with the fact that $r \neq 0$. Hence $m \neq n$.

□

Lemma 3.2.12. *i) If $m,n,k \in \mathbb{Z}^*$ and $n \neq k$ then $m=n+k$ if and only if the following formula $\tau(t^n,t^k,t^m)$ is true:*

$$t^n-1|t^m-t^k \wedge t^m-t^k|t^n-1 \wedge t^k-1|t^m-t^n \wedge t^m-t^n|t^k-1.$$

ii) If $m,n \in \mathbb{Z}^*$ and $m \neq n$ then $m=-n$ if and only if

$$t^m-1|t^n-1 \wedge t^n-1|t^m-1.$$

Proof. i) Suppose that $m=n+k$. Then $t^n-1\,|\,t^k(t^n-1)$, so the first divisibility relation holds. We have that $t^n-1 = t^k t^{-k}(t^n-1)$, so $t^k(t^n-1) = t^m-t^k$ divides t^n-1. Furthermore, $t^k-1\,|\,t^n(t^k-1)$ so $t^k-1\,|\,t^m-t^n$. We have that $t^k-1 = t^n t^{-n}(t^k-1)$, thus $t^m-t^n\,|\,t^k-1$. Hence $\tau(t^n,t^k,t^m)$ is true. Conversely, suppose that $\tau(t^n,t^k,t^m)$ holds. By the first two divisibility relations and by lemma 3.2.7 we obtain that $n\,|\,m-k$ and $m-k\,|\,n$, thus $m-k=\pm n$. Similarly, by the latter two divisibility relations and by lemma 3.2.7 we obtain that $m-n=\pm k$. If $m-k=-n$ then $m=k-n$, so by the relation $m-n=\pm k$ we obtain that $k-2n=\pm k$. So either $n=0$ or $n=k$, both of which contradict with our hypothesis. Hence $m=n+k$.

ii) If $m = -n$ then $t^n - 1 = -t^{-n}(t^n - 1)$ and $t^{-n} - 1 = -t^n(t^{-n} - 1)$, so the divisibility relations hold. Conversely, if $t^m - 1 \,|\, t^n - 1$ and $t^n - 1 \,|\, t^m - 1$, then by lemma 3.2.7 we obtain that $m = \pm n$ and since $m \neq n$ we have that $m = -n$.

□

Lemma 3.2.13. *i) Assume that $2 \in R^*$. Then there exists a positive existential formula ϕ_1 of $\mathcal{L}_{div}$ such that for any $x, y, z \in \{t^n, n \in \mathbb{Z}\}$ we have $\phi_1(x, y, z)$ is true in $R[t, t^{-1}]$ if and only if $z = x \cdot y$.*

ii) Assume that $2 \notin R^*$. Then there exists a positive existential formula ϕ_2 of $\mathcal{L}_{div}$ such that for any $x, y, z \in \{t^n, n \in \mathbb{Z}\}$ we have $\phi_2(x, y, z)$ is true in $R[t, t^{-1}]$ if and only if $z = x \cdot y$.

Proof. By lemma 3.2.10 we have that $x = t^n, n \in \mathbb{Z}$ if and only if the following formula of $\mathcal{L}_{\text{div}}$ is true

$$\theta_0(x) : \quad x \,|\, 1 \wedge t - 1 \,|\, x - 1.$$

From now on, we will write formulas of the language $\mathcal{L}_{\text{div}}$ with the index i; $i = 1$ will correspond to the case $2 \in R^*$ and $i = 2$ will correspond to the case $2 \notin R^*$. By lemma 3.2.11i),ii) we have that $x \in \{t^n : n \in \mathbb{Z}^*\}$ if and only if the following formula of $\mathcal{L}_{\text{div}}$ is true

$$\theta_i(x) : \quad \theta_0(x) \wedge \exists w, a, b : [\theta_0(w) \wedge \psi_i(x, w, a, b)].$$

By lemma 3.2.11iii) we obtain that $x, y \in \{t^n : n \in \mathbb{Z}\}$ and $x \neq y$ if and only if the following formula of $\mathcal{L}_{\text{div}}$ is true

$$\zeta_i(x, y) : \quad \theta_0(x) \wedge \theta_0(y) \wedge \exists w[\theta_i(w) \wedge x - y \,|\, w - 1].$$

By lemma 3.2.12 we have that $x, y, z \in \{t^n : n \in \mathbb{Z}^*\}$ and $x \neq y$ and $z = x \cdot y$ if and only if the following formula of $\mathcal{L}_{\text{div}}$ holds

$$\xi_i(x, y, z) : \quad \theta_i(x) \wedge \theta_i(y) \wedge \theta_i(z) \wedge \zeta(x, y) \wedge \tau(x, y, z).$$

We define the formulas ϕ_i of $\mathcal{L}_{\text{div}}$ as

$$\phi_i(x, y, z) : \theta_0(x) \wedge \theta_0(y) \wedge \theta_0(z) \wedge [(x = 1 \wedge y = z) \vee (y = 1 \wedge x = z) \vee \xi_i(x, y, z) \vee \xi_i(x, ty, tz)].$$

Let $x, y, z \in \{t^n : n \in \mathbb{Z}\}$ that satisfy $\phi_i(x, y, z)$ and let $x = t^k, y = t^l, z = t^m$ for some $k, l, m \in \mathbb{Z}$. If either k or l equals to zero then $x = 1 \wedge y = z$ or $y = 1 \wedge x = z$ holds true respectively, so $z = x \cdot y$. If $k, l \neq 0$ and $x = y$ then $\xi_i(x, y, z)$ cannot hold true, so $\xi_i(x, ty, tz)$ is true thus $tz = x \cdot ty \Rightarrow z = x \cdot y$. In the other case $\xi_i(x, y, z)$ holds, so $z = x \cdot y$. Therefore, the $\phi_i(x, y, z)$, for $i = 1, 2$, have the required properties. Conversely, suppose that $x, y, z \in \{t^n : n \in \mathbb{Z}\}$ and $z = x \cdot y$. Obviously $\theta_0(x), \theta_0(y), \theta_0(z)$ are true. If x or y equal to 1, then either $x = 1 \wedge y = z$ or $y = 1 \wedge x = z$ holds true. If $x, y \neq 1$ and $x \neq y$ then by previous observations $\xi_i(x, y, z)$ holds. If $x, y \neq 1$ and $x = y$ then $\xi_i(x, ty, tz)$ is true. Therefore $\phi_i(x, y, z)$ is true in $R[t, t^{-1}]$. □

For any $P, Q \in R[t, t^{-1}]$ we define the relation $\sim$ to mean $t - 1 \,|\, P - Q$.

Theorem 3.2.14. *The positive existential theory of $R[t, t^{-1}]$ in the language $\mathcal{L}_{div}$ is undecidable.*

Proof. Define $y_n = \dfrac{t^n - 1}{t - 1}$. Let $D = \{y_n \in R[t, t^{-1}] : n \in \mathbb{Z}\}$. Then, by lemma 3.2.13 the relation $x = z \cdot w$, for $z, w \in D$, is positive existentially definable in $\mathcal{L}_{\text{div}}$ over $R[t, t^{-1}]$ (i.e can be expressed by a positive existential formula of $R[t, t^{-1}]$ in the language $\mathcal{L}_{\text{div}}$). Also, the relation $P \sim 0$ (that is $P \equiv 0(\text{mod}\, t - 1)$) is positive existentially definable over $R[t, t^{-1}]$ in $\mathcal{L}_{\text{div}}$. Let $P(X_1, \ldots, X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$. Suppose that $P(x_1, \ldots, x_m) = 0$, for some $x_1, \ldots, x_m \in \mathbb{Z}$. Then, by lemma 3.2.8 (for $k = 1$) there exist $Y_1, \ldots, Y_m \in D$ such that

$$0 = P(x_1, \ldots, x_m) \equiv P(Y_1, \ldots, Y_m)(\text{mod}\, t - 1).$$

Hence $P(Y_1, \ldots, Y_m) \sim 0$. Conversely, if there exist $Y_1, \ldots, Y_m \in D$ such that $P(Y_1, \ldots, Y_m) \sim 0$, then lemma 3.2.8 yields

$$0 \equiv P(Y_1, \ldots, Y_m)(\text{mod}\, t - 1) \equiv P(x_1, \ldots, x_m)(\text{mod}\, t - 1),$$

for some $x_1, \ldots, x_m \in \mathbb{Z}$. Since $\deg P(x_1, \ldots, x_m) = 0$ and $\deg(t - 1) = 1$ in t, we have $P(x_1, \ldots, x_m) = 0$. Therefore, we have shown the equivalence

$$\exists x_1, \ldots, x_m \in \mathbb{Z} \colon P(x_1, \ldots, x_m) = 0 \leftrightarrow \exists Y_1, \ldots, Y_m \in R[t, t^{-1}] \colon \bigwedge_{i=1}^{m} Y_i \in D \wedge P(Y_1, \ldots, Y_m) \sim 0.$$

Hence, if there was an algorithm that could decide the truth of positive existential sentences of $R[t, t^{-1}]$ in the language $\mathcal{L}_{\text{div}}$, we could convert it into an algorithm for deciding whether a diophantine equation has a solution in integers or not, which is impossible according to the negative answer of HTP in [11]. □

Corollary 3.2.15. *Let t_1, t_2 be distinct variables. Then the positive existential theory of $R[t_1, t_2]$ in the language $\{0, 1, =, +, |, t_1, t_2\}$ is undecidable.*

Proof. We consider the map

$$\begin{array}{rccc} \sigma : & R[t_1, t_2] / \langle 1 - t_1 t_2 \rangle & \longrightarrow & R[t, t^{-1}] \\ & t_1 & \longmapsto & t \\ & t_2 & \longmapsto & t^{-1}. \end{array}$$

Then σ is an isomorphism, thus $R[t_1, t_2] / \langle 1 - t_1 t_2 \rangle \cong R[t, t^{-1}]$. For any $x, y, \in R[t, t^{-1}]$ we have

$$\sigma(x) \,|\, \sigma(y) \text{ in } R[t, t^{-1}] \leftrightarrow \exists z \in R[t_1, t_2] : x \,|\, y + z(1 - t_1 t_2) \text{ in } R[t_1 t_2].$$

Hence, if the positive existential theory of $R[t_1, t_2]$ in the language $\{0, 1, =, +, |, t_1, t_2\}$ was decidable, then the analogue problem of $R[t, t^{-1}]$ in the language $\mathcal{L}_{\text{div}}$ would be decidable as well, which contradicts theorem 3.2.14. □

Lemma 3.2.16. *i) There exists a formula ϕ_{unit} of $\mathcal{L}_{div}$ such that for any $x \in R[t, t^{-1}]$ we have that $\phi_{unit}(x)$ is true if and only if x is a unit of R.*

ii) There exists a formula ϕ_{mult} of $\mathcal{L}_{div}$ such that for any $x, y, z \in R$ we have that $\phi_{mult}(x, y, z)$ is true if and only if $z = x \cdot y$.

Proof. i) Define

$$\phi_{\text{unit}}: \quad x \,|\, 1 \wedge [x-1 \,|\, 1 \vee x+1 \,|\, 1].$$

If $x \in R[t, t^{-1}]$ satisfy ϕ_{unit}, then by proposition 3.2.6 we have that $x = ct^r$, for some $c \in R^*$ and $r \in \mathbb{Z}$. We have that $x-1 \,|\, 1$ or $x+1 \,|\, 1$, hence $x \in R^*$. If $x \in R^*$ then trivially $\phi_{\text{unit}}(x)$ holds true.

ii) Define

$$\phi_{\text{mult}}(x, y, z): \quad t - x \,|\, ty - z.$$

If $x, y, z \in R$ satisfy $\phi_{\text{mult}}(x, y, z)$, then $ty - z = P(t-x)$ for some polynomial $P \in R[t, t^{-1}]$. By equalizing the degrees of the equation we obtain that $P = c$, for some $c \in R$. Thus $y = c$ and $z = x \cdot y$. Conversely, if $z = x \cdot y$ then trivially $\phi_{\text{mult}}(x, y, z)$ is true.

□

Theorem 3.2.17. *If R contains the field of rational numbers $\mathbb{Q}$ then the ring-structure of $\mathbb{Z}$ is positive existentially definable in $\mathcal{L}_{div}$ over $R[t, t^{-1}]$.*

Proof. Let $\mu \in R$. By lemma 3.2.8 we obtain $\mu \in \mathbb{Z}$ if and only if there is a $x \in \{t^n : n \in \mathbb{Z}\}$ such that $\mu \equiv \dfrac{x-1}{t-1} (\text{mod}\, t-1)$. The last relation can be written equivalently as $x - 1 - \mu(t-1) = k(t-1)^2$, for some $k \in R[t, t^{-1}]$. Thus, for any $R[t, t^{-1}]$ we have

$$\mu \in \mathbb{Z} \leftrightarrow \mu \in R \wedge \exists x \in R[t, t^{-1}] : x \,|\, 1 \wedge t - 1 \,|\, x - 1 \wedge (t-1)^2 \,|\, x - 1 - \mu(t-1).$$

Since R contains $\mathbb{Q}$, we can replace the subformula $\mu \in R$ with the formula ϕ_{unit} of lemma 3.2.16 to obtain a positive existential description of $\mathbb{Z}$ over $R[t, t^{-1}]$ in $\mathcal{L}_{\text{div}}$. In addition, the relation $\phi_{\text{mult}}|_{\mathbb{Z}}$ of lemma 3.2.16 gives a positive existential description of the multiplication in $\mathbb{Z}$. Hence the lemma follows. □

Note: The fact that the positive existential theory of a ring R in a specific language is undecidable does not imply that the ring-structure of $\mathbb{Z}$ can be defined over R in that language. In particular, the latter implies the former, thus theorem 3.2.14 can be seen as a corollary of theorem 3.2.17.

3.3 A different approach

In 1994, T. Pheidas published a paper [13] in which he proves that the positive existential theories of the rings $F[t]$ and $F[t, t^{-1}]$, where F denotes a field, in the language $\mathcal{L}_t = \{0, 1, =, +, \cdot, t\}$ are undecidable. These results were not new but the proofs are different than those used before.

Lemma 3.3.1. $\dfrac{t^n - 1}{t - 1} = t^{n-1} + \cdots + t + 1 \equiv n \, (\text{mod}\, t-1).$

Proof. It follows from lemma 3.2.8 for $k = 1$. □

Lemma 3.3.2. *If $char(F) = 0$, then for any $n \in F[t, t^{-1}]$, n is a nonzero integer if and only if n divides 1, either $n - 1$ divides 1 or $n + 1$ divides 1 and there is a power x of t, so that $\dfrac{x-1}{t-1} \equiv n \, (mod\, t-1)$.*

Proof. The direct implication is trivial. Conversely, since n divides 1, by proposition 3.2.6 we obtain that $n = ct^r$, for some $c \in F^*, r \in \mathbb{Z}$. Suppose that $n-1$ divides 1 (the other case is similar). Then $ct^r - 1 = \tilde{c}t^{r'}$, so $ct^r - \tilde{c}t^{r'} = 1$ and this happens only when $r, r' = 0$. Therefore, $n \in F^*$. Furthermore, there exists $m \in \mathbb{Z}$ such that

$$\frac{t^m - 1}{t-1} \equiv n \,(\text{mod}\, t-1) \overset{3.3.1}{\Longleftrightarrow}$$
$$m \equiv n \,(\text{mod}\, t-1).$$

Since m, n are both constants, we have that $m = n$, hence n is a nonzero integer. □

Theorem 3.3.3. *If* $char(F) = 0$*, then the existential theory of* $F[t, t^{-1}]$*, in the language* $\mathcal{L}_t = \{0, 1, =, +, \cdot, t\}$ *is undecidable.*

Proof. By lemma 3.2.10 we have that

$$x = t^n \leftrightarrow \exists y, z \in F[t, t^{-1}] : xy = 1 \wedge x - 1 = (t-1)z.$$

Call the right part $\phi(x)$. By lemma 3.3.2 we can express the fact that an element $n \in F[t, t^{-1}]$ is a nonzero integer by the following existential formula (call it $\psi(n)$)

$$\exists\, x, y \in F[t, t^{-1}] : nx = 1 \wedge ((n+1)y = 1 \vee (n-1)y = 1)$$
$$\wedge \exists\, z, w \in F[t, t^{-1}] : \phi(x) \wedge x - 1 = (t-1)n + (t-1)^2 w.$$

Therefore, given a diophantine polynomial $P(X_1, \ldots, X_n)$ we obtain that

$$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0 \leftrightarrow$$
$$\exists x_1, \ldots, x_n \in F[t, t^{-1}] : P(x_1, \ldots, x_n) = 0 \wedge \psi(x_1) \wedge \cdots \wedge \psi(x_n).$$

Hence, the question whether the last formula is true in $F[t, t^{-1}]$ is equivalent to whether the diophantine equation $P = 0$ has integer solutions, which contradicts to the negative answer of HTP by Matijasevič in [11]. □

The case char(F)=p, p>2. Assume that $\text{char}(F) = p$, for some $p > 2$.

Lemma 3.3.4. *Assume that* F *has positive characteristic* p*, other than two. Then* $\frac{t^m - 1}{t^n - 1}$ *is a square in* $F[t, t^{-1}]$ *if and only if there exists an integer* s *such that* $m = np^s$.

Proof. Suppose that $\frac{t^m - 1}{t^n - 1}$ is a square in $F[t, t^{-1}]$. Then $\frac{t^m - 1}{t^n - 1} = d^2$, for some $d \in F[t, t^{-1}]$. Therefore, $d = \frac{f(t)}{t^k}$, for some $k \in \mathbb{N}_0$ and $f(t) \in F[t]$. Thus

$$\frac{t^m - 1}{t^n - 1} = \left(\frac{f(t)}{t^k}\right)^2 \Rightarrow t^{2k}(t^m - 1) = f^2(t)(t^n - 1). \tag{3.3.1}$$

Let $m = \tilde{m}p^a, n = \tilde{n}p^b$, where $p \nmid \tilde{m}, p \nmid \tilde{n}$, then we have

$$t^m - 1 = (t^{\tilde{m}} - 1)^{p^a}$$

and

$$t^n - 1 = (t^{\tilde{n}} - 1)^{p^b}.$$

Hence, relation (3.3.1) implies

$$t^{2k}(t^{\tilde{m}} - 1)^{p^a} = f^2(t)(t^{\tilde{n}} - 1)^{p^b}. \tag{3.3.2}$$

Let $u \neq 0$ be root of $t^{\tilde{m}} - 1$ that lies in an algebraic closure of F and is not a root of $t^{\tilde{n}} - 1$. Then

$$\begin{aligned} u^{2k}(u^{\tilde{m}} - 1)^{p^a} &= 0 \Rightarrow \\ f^2(u)(u^{\tilde{n}} - 1)^{p^b} &= 0 \Rightarrow \\ f^2(u) &= 0. \end{aligned}$$

Thus, in the left-hand side of (3.3.2) u is a root of odd multiplicity, while in the right-hand side of (3.3.2) u is a root of even multiplicity, which is a contradiction. Hence the set of the roots of $t^{\tilde{m}} - 1$ is equal to the set of the roots of $t^{\tilde{n}} - 1$. Since the number of the roots is equal to the degree of the polynomial (the roots lie in an algebraically closed field), we obtain that $\tilde{m} = \tilde{n}$. Thus $m = np^{a-b}$ which proves the required.

Conversely, if $m = np^s$ for some integer s, then

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

which is a square in $F[t, t^{-1}]$ since $2 \,|\, p^s - 1$. □

Theorem 3.3.5. *Assume that F has characteristic $p > 2$. Then the existential theory of $F[t, t^{-1}]$ in the language $\mathcal{L}_t$ is undecidable.*

Proof. The integers can be represented by the set of powers of t, i.e. t^n represents n. By lemma 3.2.10 the set of powers of t is existentially definable. Addition of integers $m + n$ corresponds to the multiplication $t^m t^n$. The relations $n \,|\, m$, and $|^p$ are existentially definable by lemma 3.2.7 and lemma 3.3.4 respectively. Hence, if there was an algorithm that could decide the truth of existential sentences over $F[t, t^{-1}]$, we could convert it to an algorithm that could decide the truth of existential sentences over $\mathbb{Z}$ in the language $\{0, 1, +, |, |^p\}$, which contradicts corollary 2.0.9. □

Theorem 3.3.6. *The polynomial ring $F[t]$ has undecidable positive existential theory in the language $\mathcal{L}_t$.*

Proof. Assume $s = t + \sqrt{t^2 - 1}$. Then $s^{-1} = t - \sqrt{t^2 - 1}$ and $F[s, s^{-1}] = F[t, \sqrt{t^2 - 1}]$. We consider the ring $F[s, s^{-1}]$ as a module over $F[t] = F[s + s^{-1}]$, with the base $\mathcal{B} = \{1, s + s^{-1}\}$. So now we can interprete the positive existential theory of $F[s, s^{-1}]$ to $F[t]$ in the following way: if $x \in F[s, s^{-1}]$ then x can be written as a pair (a, b) with respect to the base $\mathcal{B}$. Assume a diophantine polynomial P of n variables over $F[s, s^{-1}]$. We write P with respect to the base $\mathcal{B}$, so it takes the form $P = P_1 + (s + s^{-1})P_2$, where $P_1, P_2 \in F[t]$. So we obtain that

$$\begin{gathered}\exists x_1, \ldots, x_n \in F[s, s^{-1}] : P(x_1, \ldots, x_n) = 0 \leftrightarrow \\ \exists X_1, \ldots, X_n \in F[t] : P_1(X_1, \ldots, X_n) + (s + s^{-1})P_2(X_1, \ldots, X_n) = 0 \wedge s + s^{-1} = 2t \leftrightarrow \\ \exists X_1, \ldots, X_n \in F[t] : P_1(X_1, \ldots, X_n) = 0 \wedge P_2(X_1, \ldots, X_n) = 0\end{gathered}$$

because $\mathcal{B}$ is a base. So if there was an algorithm to decide whether the last existential formula is true in $F[t]$ there would be an algorithm to answer whether the equation $P = 0$ has solutions in $F[s, s^{-1}]$, which is a contadiction by Theorem 3.3.3 (in the case char$(F) = 0$) and by Theorem 3.3.5 (in the case char$(F) > 2$). □

Chapter 4

The geometric language

Our aim is to enlarge the language of the rings $\mathcal{L}_r = \{+, \cdot, =, 0, 1\}$ by some extra constants or predicates without reducing the decidability of the existential theory to the ground field F. In the previous chapter we saw such an example, the extension $\mathcal{L}_r \cup \{t\}$. In this chapter we will examine the decidability of positive existential theories of the rings $R[t]$ and $F[t, t^{-1}]$ in the language $\mathcal{L}_T = \mathcal{L}_r \cup \{T\}$, where $T(x)$ denotes that the element x is not a constant element of $R[t]$. We call $\mathcal{L}_T$ "geometric" language because it is connected with a more geometric analogue of HTP (see 4.1.2).

First, observe that whenever the existential theory of a field F in the language of rings is undecidable, then so is the existential theory of $F(t)$ (and its subrings $F[t], F[t, t^{-1}]$) in $\mathcal{L}_T$. Indeed, F is quantifier-free definable in $\mathcal{L}_T$ by

$$x \in F \leftrightarrow \neg T(x).$$

Now we ask the question: when can T be defined by a positive existential formula of $\mathcal{L}_r$ over $F(t)$? The following lemma provides the answer.

Lemma 4.0.1. *Let $F(t)$ be a function field. Then T is positive existentially definable in $\mathcal{L}_r$ if and only if F is a finite field.*

Proof. Suppose that $F = \mathbb{F}_q$, $q = p^n$, for some prime number p. Then we have

$$T(x) \leftrightarrow \exists y \in \mathbb{F}_q(t) : y(x^q - x) = 1.$$

Indeed, if $x \notin \mathbb{F}_q$, then $x^q - x$ is invertible. If $x^q - x$ is invertible and $x \in \mathbb{F}_q$, then $x^q = x$. Thus $x^q - x = 0$, which is a contradiction.

Conversely, assume that F is infinite and $T(x)$ is definable by positive existential formula of $\mathcal{L}_r$. Then the definition is of the form

$$T(x) \leftrightarrow \exists y_1, \ldots, y_n \in F(t) : P(x, y_1, \ldots, y_n) = 0,$$

with P a polynomial with coefficients in F or a prime field of F. Choose an element $a \in F$, such that a is not a pole of any of x and $y_1, \ldots, y_n$ (which is possible since F is infinite). Then $x(a), y_1(a), \ldots, y_n(a)$ lie in F. In addition, $P(x(a), y_1(a), \ldots, y_n(a)) = 0$, thus we obtain $T(x(a))$, which contradicts with the fact that $x(a) \in F$. □

4.1 The geometric problem

The purpose of this section is to discuss the significance of the geometric language $\mathcal{L}_T$ and its connection with geometric problems. It is based on section 4 of [16].

Definition 4.1.1. Let F be a field and polynomials $f_1, \ldots, f_m \in F[X_1, \ldots, X_n]$. We define an affine variety $\mathbb{V}$ to be the set

$$\mathbb{V} = \{(a_1, \ldots, a_n) \in F^n : f_1(a_1, \ldots, a_n) = \cdots = f_m(a_1, \ldots, a_n) = 0\}.$$

Question 4.1.2. Let F be a field and $\mathbb{V}$ be an affine variety defined over the prime field [1] of F. Is there an algorithm to decide whether $\mathbb{V}$ contains some curve which is parametrizable by rational functions with coefficients in F? Equivalently, is there an algorithm to decide whether there is a non-constant rational map from the affine line to $\mathbb{V}$?

The above question is still open and it is connected with the question of the decidability of a rational function field in the language $\mathcal{L}_T$. Indeed, let $\mathbb{V}$ be a affine variety defined by

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0,$$

with $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$. Then $\mathbb{V}$ contains a curve which admits a rational parametrization if and only if the system of equations which defines $\mathbb{V}$ has a $F(t)-$rational point with not all of its coordinates lie in F. Hence, Question 4.1.2 is equivalent to

Question 4.1.3. Is there an algorithm for deciding the truth of formulas of the following form

$$\exists \mathrm{x} = (x_1, \ldots, x_n) \in F(t)^n : f_1(\mathrm{x}) = \cdots = f_m(\mathrm{x}) = 0 \wedge \left(\bigvee_{i=1}^{n} T(x_i) \right)$$

in $F(t)$?

The above sentence is a positive existential formula of $\mathcal{L}_T$ over $F(t)$. It is obvious that if the positive existential theory of $F(t)$ in $\mathcal{L}_T$ is decidable, then the geometric problem of 4.1.2 will have a positive answer, while if the positive existential theory of $F(t)$ in $\mathcal{L}_T$ turn out to be undecidable, then it will not provide us a negative answer, but it is a first step towards it. Although the geometric problem is still open, it is proved for any field F that satisfies a hypothesis in [8]. For a nice presentation of more geomtric problems connected to analogues of HTP, the reader is advised to see [17] section 2 and [18] section 12.

4.2 Positive existential theory of $R[t]$ in L_T

Several years after Denef prooved the undecidability of $R[t]$ in the language $\mathcal{L}_t$, Pheidas and Zahidi in the paper [15] examined the decision problem of $R[t]$ in the language $\mathcal{L}_T$. The methods they used are similar to Denef but the proofs are different and more elementary.

[1] Prime field is a field with no proper subfields. One can show that every field contains a unique prime field.

Again we work over an integral domain R, with $\text{char}(R) = 0$. Let $a \in R[t]$ such that $T(a)$. We consider the Pell equation

$$X^2 - (a^2 - 1)Y^2 = 1. \tag{4.2.1}$$

We define two recursive sequenses X_n, Y_n of $R[t]$ be setting $X_0(a) = 1$, $Y_0(a) = 0$ and for any $n \in \mathbb{N}$

$$X_{n+1}(a) = aX_n(a) + (a^2 - 1)Y_n(a)$$

and

$$Y_{n+1}(a) = X_n(a) + aY_n(a).$$

We can extend this definition to integers simply by setting $X_{-n} = X_n$ and $Y_{-n} = -Y_n$, where n denotes any positive integer. Since $(X_1, Y_1) = (a, 1)$ is a (non-trivial) solution of (4.2.1), observe that the pairs (X_n, Y_n) are also solutions of (4.2.1) for $n \in \mathbb{Z}$ [2].

Lemma 4.2.1. *If $T(a)$ holds, then $a^2 - 1$ is not a square in $R[t]$.*

Proof. Suppose that $a^2 - 1 = d^2$, for some $d \in R[t]$, then $(a + d)(a - d) = 1$ meaning that $a + d, a - d$ are both divisors of 1. Hence $a + d, a - d$ lay in R, so $2a \in R$ and therefore $a \in R$, which is a contradiction since a is not a constant. □

Let u be an algebraic element over $K(t)$,where $K = \text{Q}(R)$, such that $u^2 = a^2 - 1$.

Lemma 4.2.2. *The pairs (X_n, Y_n) satisfy*

- $X_n + uY_n = (X_1 + uY_1)^n$
- $X_{n+m} = X_n X_m + u^2 Y_n Y_m$
- $Y_{n+m} = Y_n X_m + X_n Y_m$

for any $n, m \in \mathbb{Z}$.

Proof. The equations can be shown easily by induction. □

Remark 4.2.3. It is now clear, by the first equation, that (X_n, Y_n) are the same polynomials that appear in [4] by setting $a = t$.

Lemma 4.2.4. *Let $a \in R[t]$, for which $T(a)$. Then the solutions of 4.2.1 are given by $(\pm X_n(a), Y_n(a))$ for $n \in \mathbb{Z}$.*

Proof. We have already seen that $(\pm X_n(a), Y_n(a))$ satisfy 4.2.1 for $n \in \mathbb{Z}$.

Conversely, assume that (X, Y) is a solution of 4.2.1, such that deg $(X) = m$. We will show that $(X, Y) = (\pm X_s, Y_s)$, for some integer s, by doing induction to the degree of X. We observe that $X \neq 0$, otherwise we would have that $(a^2 - 1)Y^2 = 1$, therefore $a^2 - 1$ is a divisor of 1, hence $a^2 - 1 \in R$, which is a contradiction since a is not a constant. Therefore, $m \geq 0$. If $m = 0$, then $X \in R$, thus $(a^2 - 1)Y^2 \in R$ and since $T(a)$ holds we obtain that Y must be equal to zero and therefore $X^2 = 1$. So, for $m = 0$, we obtain the solution $(\pm X_0, Y_0)$.

[2] We will later show that (X_n, Y_n) are the same sequences as those appearing in Section 3.1

For the induction hypothesis, assume that the lemma holds for the solutions (Z, W) of 4.2.1 such that $\deg(Z) < m$. Set

$$Z_1 = aX + (a^2-1)Y,\ W_1 = X + aY \text{ and} \tag{4.2.2}$$
$$Z_2 = aX - (a^2-1)Y,\ W_2 = X - aY. \tag{4.2.3}$$

Now we have that

$$\begin{aligned} Z_1Z_2 &= a^2X^2 - (a^2-1)^2Y^2 \\ &= a^2X^2 + (a^2-1)(1-X^2) \\ &= X^2 + a^2 - 1 \end{aligned}$$

so $\deg(Z_1Z_2) = \deg(X^2 + a^2 - 1)$. We have that (4.2.1) is equivalent to $X^2 - 1 = (a^2-1)Y^2$, hence $\deg(X^2-1) = \deg(a^2-1) + \deg(Y^2)$, thus we obtain that $\deg(X) = \deg(a) + \deg(Y)$. So, $\deg(X) \geq \deg(a)$. Consequently, $\deg(Z_1Z_2) \leq \deg(X^2)$. Therefore, either $\deg(Z_1) = \deg(Z_2) = \deg(X)$ or $\deg(Z_i) < \deg(X)$ for $i = 1$ or 2. In the first case we have that $\deg(Z_1 + Z_2) \leq \deg(X) \Leftrightarrow \deg(2aX) \leq \deg(X)$, which is a contradiction since a and X do not lay in R. Therefore, $\deg(Z_1) < \deg(X)$ or $\deg(Z_2) < \deg(X)$. Assume that $\deg(Z_1) < \deg(X)$ (the other case is similar). We observe that (Z_1, W_1) satisfy 4.2.1 so by induction hypothesis $(Z_1, W_1) = (\pm X_k, Y_k)$ for some $k \in \mathbb{Z}$. The equations in 4.2.3 are equivalent to

$$X = aZ_1 - (a^2-1)W_1$$

and

$$Y = -Z_1 + aW_1.$$

So, if $(Z_1, W_1) = (X_k, Y_k)$ then $(X, Y) = (X_{k-1}, Y_{k-1})$, while if $(Z_1, W_1) = (-X_k, Y_k)$ then $(X, Y) = (-X_{k+1}, Y_{k+1})$. Eitherwise $(X, Y) = (\pm X_s, Y_s)$, for an integer s, which gives us the desired result. □

Lemma 4.2.5. *For any natural number n, the degrees of X_n, Y_n in a are $n, n-1$ respectively.*

Proof. Assume $n \in \mathbb{N}$. Then lemma 4.2.2 implies

$$\begin{aligned} X_n(a) &= \sum_{i \text{ even}}^{n} \binom{n}{i} a^{n-i}(a^2-1)^{i/2} \\ &= \left(\sum_{i \text{ even}}^{n} \binom{n}{i} \right) a^n + \text{terms of lower degree in } a \\ &= 2^{n-1}a^n + \text{terms of lower degree in } a. \end{aligned}$$

Therefore, the degree of X_n in a is n. In a similar way, one can prove that the degree of Y_n in a is $n-1$. □

Lemma 4.2.6. *For any $n, m \in \mathbb{Z}$, n divides m in $\mathbb{Z}$ if and only if Y_n divides Y_m in $R[t]$.*

Proof. Suppose $n, m \geq 0$ (the other case is similar) and $m = kn$ for some $k \in \mathbb{N}$. Then lemma 4.2.2 implies

$$X_{kn} + uY_{kn} = (X_n + uY_n)^k .$$

Hence,

$$Y_{kn} = \sum_{i \text{ odd}}^{k} \binom{k}{i} X_n^{k-i} Y_n^i (a^2-1)^{\frac{i-1}{2}} .$$

Thus $Y_n \,|\, Y_{kn}$.
Conversely, suppose that Y_n divides Y_m in $R[t]$. If $n = 0$, then $m = 0$, thus suppose that $n > 0$. Hence $m = nq + r$, for some $q, r \in \mathbb{N}$ with $0 \leq r < n$. By lemma 4.2.2 Y_m can be written in the form

$$Y_m = Y_{nq}X_r + X_{nq}Y_r.$$

Since $Y_n \,|\, Y_m$ and $Y_n \,|\, Y_{nq}$ we obtain

$$\begin{aligned}
&Y_n \,|\, X_{nq}Y_r \Rightarrow \\
&Y_n \,|\, X_{nq}^2 Y_r \Rightarrow \\
&Y_n \,|\, (1 + (a^2-1)Y_{nq})Y_r \Rightarrow \\
&Y_n \,|\, Y_r + (a^2-1)Y_{nq}Y_r \Rightarrow \\
&Y_n \,|\, Y_r.
\end{aligned}$$

Suppose that $r \neq 0$, then $Y_r \neq 0$. Hence, $\deg(Y_n) \leq \deg(Y_r)$. By lemma 4.2.5 we obtain that $n \leq r$ which contradicts with $r < n$. Thus, $r = 0$ and $n \,|\, m$. □

The case char(R)=p, p>2. Assume that R has positive characteristic $p > 2$.

Lemma 4.2.7. *For any natural number s, $X_{np^s} = (X_n)^{p^s}$.*

Proof. From lemma 4.2.2 follows

$$\begin{aligned}
X_{np^s} + uY_{np^s} &= (X_1 + uY_1)^{np^s} \\
&= (X_n + uY_n)^{p^s} \\
&= (X_n)^{p^s} + u(Y_n)^{p^s}(a^2-1)^{\frac{p^s-1}{2}},
\end{aligned}$$

which completes the proof. □

Lemma 4.2.8. *$n = \pm p^s$ for some natural number s if and only if $X_n(a+1) = X_n(a) + 1$.*

Proof. Suppose that $n = \pm p^s$. From lemma 4.2.7 follows

$$X_{p^s}(a+1) = (X_1(a+1))^{p^s} = (a+1)^{p^s} = (X_1(a)+1)^{p^s} = X_{p^s}(a) + 1.$$

Conversely, suppose that $X_n(a+1) = X_n(a) + 1$ and $n > 0$. Notice that n cannot be zero, otherwise we have $1 = 2$, which is impossible. Hence we can write $n = qp^s$, with $q, s \in \mathbb{N}_0$ and $q \not\equiv 0 (\text{mod } p)$. From lemma 4.2.7 follows

$$(X_q(a+1))^{p^s} = (X_q(a))^{p^s} + 1 = X_{qp^s}(a) + 1.$$

Thus, $X_q(a+1) = X_q(a) + 1$. From lemma 4.2.2 we have

$$X_q(a) = c_1 a^q + c_2 a^{q-1} + S,$$

where $c_1, c_2 \in R$, $c_1 \neq 0$ and S contains terms of lower degree in a. In addition,

$$\begin{aligned} X_q(a+1) &= c_1(a+1)^q + c_2(a+1)^{q-1} + \dots \\ &= c_1 \left(a^q + \binom{q}{q-1} a^{q-1} + \dots \right) + c_2(a^{q-1} + \dots) + \dots \\ &= c_1 a^q + (c_2 + qc_1)a^{q-1} + \dots \end{aligned}$$

Therefore, if $q \geq 2$, then $c_2 = c_2 + c_1 q$, which contradicts with $c_1 \neq 0$ and $q \not\equiv 0 (\text{mod } p)$. Hence, $q = 1$ and $n = p^s$, while if $n < 0$ we conclude $n = -p^s$. □

Lemma 4.2.9. *Assume that R has characteristic $p > 2$. Then for any $n \neq 0$*

$$\begin{gathered} n|^p m \leftrightarrow \\ \exists Z_1, Z_2, W_1, W_2 \in R[t] : Z_1^2 - (X_n(a)^2 - 1)W_1^2 = 1 \wedge Z_2^2 - ((X_n(a)+1)^2 - 1)W_2^2 = 1 \wedge \\ Z_1 = X_m(a) \wedge Z_2 = Z_1 + 1. \end{gathered}$$

Proof. Suppose that $n|^p m$. Then $m = \pm np^s$, for some natural number s. Assume that $m = np^s$ (the case $m = -np^s$ can be treated similarly). Choose $Z_1 = X_{p^s}(X_n(a))$ and $Z_2 = X_{p^s}(X_n(a) + 1)$. Then, by lemmas 4.2.7, 4.2.8 yields

$$\begin{aligned} Z_1 &= X_{p^s}(X_n(a)) \\ &= (X_n(a))^{p^s} \\ &= X_{np^s}(a) \\ &= X_m(a) \end{aligned}$$

and

$$\begin{aligned} Z_2 &= X_{p^s}(X_n(a) + 1) \\ &= X_{p^s}(X_n(a)) + 1 \\ &= X_m(a) + 1 \\ &= Z_1 + 1. \end{aligned}$$

Furthermore, we have that Z_1 and Z_2 satisfy (4.2.1) by lemma 4.2.4.
Conversely, suppose the right-hand-side of the equivalence is satisfied. Then, $Z_1 = X_k(X_n(a))$ and $Z_2 = X_l(X_n(a) + 1)$, for some natural numbers k, l. Since $Z_2 = Z_1 + 1$, $X_k(X_n(a))$ and $X_l(X_n(a) + 1)$ have the same degree in a. Consequently, by lemma 4.2.5 $k = l$ and by lemma 4.2.8 we have $k = \pm p^s$, for some natural number s. Hence, by lemma 4.2.7

$$\begin{aligned} X_m(a) &= Z_1 \\ &= \pm X_k(X_n(a)) \\ &= \pm (X_n(a))^{p^s} \\ &= \pm X_{np^s}. \end{aligned}$$

Thus, $m = \pm np^s$ and $n|^p m$. □

Let $Z \sim 0$ denote that $a - 1 \,|\, Z$ in $R[t]$, for any $Z \in R[t]$. Then we have that

$$Z \sim 0 \leftrightarrow \exists V \in R[t] : Z = V(a-1).$$

Therefore the relation $\sim$ is defined by a positive existential formula in the language $\mathcal{L}_T$. Moreover, the lemma 3.1.7, for $t = a$ such that $T(a)$, gives us

$$Y_n \equiv n \,(\operatorname{mod} a - 1). \tag{4.2.4}$$

Now we are in position to prove the following

Theorem 4.2.10. *The positive existential theory of a polynomial ring $R[t]$, in the language $\mathcal{L}_T$, is undecidable.*

Proof. 1) *Case char$(R) = 0$.* In order to prove this we need to show that for any polynomial P with coefficients in $\mathbb{Z}$ we have that "$P = 0$ has a solution over $\mathbb{Z}$ if and only if $\tilde{P} = 0$ has a solution over $R[t]$" for some polynomial $\tilde{P}$ with coefficients in $\mathbb{Z}[t]$. Let $P(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$. If $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ is a solution of the equation $P = 0$ then by lemma 3.1.7 we have

$$P(Y_{z_1}, \ldots, Y_{z_n}) \equiv P(z_1, \ldots, z_n)(\operatorname{mod} a-1) \equiv 0 \,(\operatorname{mod} a-1).$$

Therefore $P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$. Conversely, assume that $P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$ for some $z_1, \ldots, z_n \in \mathbb{Z}$, then we have

$$\begin{gathered} P(Y_{z_1}, \ldots, Y_{z_n}) \equiv 0 \,(\operatorname{mod} a-1) \Leftrightarrow \\ P(z_1, \ldots, z_n) \equiv 0 \,(\operatorname{mod} a-1). \end{gathered}$$

Since $P(z_1, \ldots, z_n)$ is a constant and a is not, we have that $P(z_1, \ldots, z_n) = 0$. Thus we showed that

$$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Y_{z_1}, \ldots, Y_{z_n} \in R[t] : P(Y_{z_1}, \ldots, Y_{z_n}) \sim 0$$

and the relation $\sim$ is defined by a positive existential formula of $\mathcal{L}_T$ with parameter a. So if there was an algorithm that could decide the truth of positive existential sentences of $\mathcal{L}_T$ in $R[t]$ there would be an algorithm that could decide whether a diophantine equation over $\mathbb{Z}$ has a solution in $\mathbb{Z}$ or not, which is a contradiction according to [11].

2) *Case char$(R) = p > 2$.* The integers can be represented by the solutions of (4.2.1), i.e. the pair (X_n, Y_n) represents the integer n. Addition of integers $m + n$ corresponds to (X_{n+m}, Y_{n+m}) as given by the formulas in lemma 4.2.2. The relations $n \mid m$ and $|^p$ are definable by a positive existential sentence of $\mathcal{L}_T$ over $R[t]$, by lemmas 4.2.6 and 4.2.9 respectively. Hence, if there was an algorithm that could decide the truth of positive existential sentences over $R[t]$ in the language $\mathcal{L}_T$, we could convert it to an algorithm that could decide the truth of positive existential sentences of $\mathbb{Z}$ in the language which contains the addition, divisibility and localized divisibility, which is a contradiction according to corollary 2.0.9. Hence the theorem follows.

□

4.3 Positive existential theory of Laurent polynomial ring in L_T

Since we have already discussed the decision problem of the polynomial ring in the language $\mathcal{L}_T$, it is natural to ask what happens when we invert a non-constant element of the polynomial ring. In particular, we will try to prove that the existential theory of the Laurent polynomial ring $F[t,t^{-1}]$ in the language $\mathcal{L}_T$ is undecidable, where F denotes a field of zero characteristic. The methods we used for the proof are the same as Pheidas's and Zahidi's (see [15]).

Notation 4.3.1. Let $P = \sum_{i=r}^{r'} \alpha_i t^i$ an element of $F[t,t^{-1}]$, with $r, r' \in \mathbb{Z}$ and $r \leq r'$. We define the **positive degree** of P

$$\deg_+(P) = \begin{cases} r', & \text{if } r' \geq 0 \\ -\infty, & \text{if } r' < 0 \end{cases}$$

and the **negative degree** of P

$$\deg_-(P) = \begin{cases} r, & \text{if } r \leq 0 \\ +\infty, & \text{if } r > 0. \end{cases}$$

Remark 4.3.2. Let $P \in F[t,t^{-1}]$. From the definitions, we can easily deduce that $\deg_+(P) \geq 0$ or $\deg_+(P) = -\infty$ and $\deg_-(P) \leq 0$ or $\deg_+(P) = +\infty$.

Example 4.3.3.

1) Let $P = t^3 + t$. Then the positive degree of P is $\deg_+(P) = 3$ and the negative degree of P is $\deg_-(P) = +\infty$.

2) Let $P = t^{-1} + t^{-6}$. Then the positive degree of P is $\deg_+(P) = -\infty$ and the negative degree of P is $\deg_-(P) = -6$. Note that the degree of P is $\deg(P) = -1$, that is the highest power of t.

Let $P, Q \in F[t,t^{-1}]$, then we have the following properties:

i) If $\deg_+(P) \geq 0$ and $\deg_+(Q) \geq 0$ ($\deg_-(P) \leq 0$ and $\deg_-(Q) \leq 0$) then $\deg_+(PQ) = \deg_+(P) + \deg_+(Q)$ (respectively $\deg_-(PQ) = \deg_-(P) + \deg_-(Q)$).

ii) $\deg_+(P+Q) \leq \max\{\deg_+(P), \deg_+(Q)\}$ ($\deg_-(P+Q) \geq \min\{\deg_-(P), \deg_-(Q)\}$) and the equality holds when $\deg_+(P) \neq \deg_+(Q)$ (respectively $\deg_-(P) \neq \deg_-(Q)$).

Remark 4.3.4. Assume $a \in F[t,t^{-1}]$, such that $T(a)$ holds. We observe that $a^2 - 1$ can be a perfect square in $F[t,t^{-1}]$. Indeed, let $d \in F[t,t^{-1}]$, so that $a^2 - 1 = d^2$. Then $(a+d)(a-d) = 1$, hence $a+d, a-d$ are units of $F[t,t^{-1}]$. So there exist $c \in F^*$, $m \in \mathbb{Z}$ such that

$$a + d = ct^m$$
$$a - d = \frac{1}{c}t^{-m}.$$

Therefore, if a is of the form $\frac{1}{2}\left(ct^m + \frac{1}{c}t^{-m}\right)$ for some $c \in F^*$, $m \in \mathbb{Z}$, then $a^2 - 1$ is a perfect square in $F[t,t^{-1}]$.

To fix this problem, we work with the Pell equation

$$X^2 - (a^4 - 1)Y^2 = 1. \tag{4.3.1}$$

Our new recursive sequences are obtained by setting $X_0(a) = 1$, $Y_0(a) = 0$ and inductively for $n \in \mathbb{N}$

$$X_{n+1}(a) = a^2 X_n(a) + (a^4 - 1)Y_n(a)$$

and

$$Y_{n+1}(a) = X_n(a) + a^2 Y_n(a).$$

We extend the definition to the integers by setting $X_{-n} = X_n$ and $Y_{-n} = -Y_n$, where n is a natural number. So we have the following

Lemma 4.3.5. *Let $a \in F[t, t^{-1}]$, such that $T(a)$ holds. Then $a^4 - 1$ is not a square in $F[t, t^{-1}]$.*

Proof. Suppose that $a^4 - 1 = d^2$, for some $d \in F[t, t^{-1}]$. Then $(a^2 + d)(a^2 - d) = 1$, so we obtain that there exist $c \in F^*$, $m \in \mathbb{Z}$ such that

$$\begin{aligned} a^2 + d &= ct^m \\ a^2 - d &= \frac{1}{c}t^{-m}. \end{aligned}$$

Therefore

$$a^2 = \frac{1}{2}(ct^m + \frac{1}{c}t^{-m}). \tag{4.3.2}$$

We will show that $c_1 t^m + c_2 t^{-m}$ cannot be a perfect square in $F[t, t^{-1}]$, with $c_1, c_2 \in F^*$. Since $a \notin F$, we have $m \neq 0$. Let $r = \deg(a)$ and $r' = \deg_{\text{min}}(a)$. Assume, without the loss of generality, that $m \geq 0$ and $-m \leq 0$. Then, by (4.3.2) we obtain that $m = 2r$ and $-m = 2r'$, thus $r' = -r$ and $r \neq 0$. So $a = \alpha_{-r}t^{-r} + \alpha_{-r+1}t^{-r+1} + \cdots + \alpha_{r-1}t^{r-1} + \alpha_r t^r$, with $\alpha_i \in F$ for $i = -r, -r+1, \ldots, r$. Obviously, $\alpha_{-r} \neq 0$ and $\alpha_r \neq 0$. Then

$$a^2 = \alpha_{-r}^2 t^{-2r} + (\sum_{\substack{i,j \in \{-r,\ldots,r\} \\ i+j=-2r+1}} \alpha_i\alpha_j)t^{-2r+1} + \cdots + \sum_{\substack{i,j \in \{-r,\ldots,r\} \\ i+j=0}} \alpha_i\alpha_j + \cdots + (\sum_{\substack{i,j \in \{-r,\ldots,r\} \\ i+j=2r-1}} \alpha_i\alpha_j)t^{2r-1} + \alpha_r^2 t^{2r}.$$

Therefore, by equalizing the coefficients in (4.3.2) we obtain that

$$\begin{gathered} 2\alpha_{-r}\alpha_{-r+1} = 0 \overset{\alpha_{-r}\neq 0}{\Longrightarrow} \alpha_{-r+1} = 0 \\ 2\alpha_{-r}\alpha_{-r+2} + \alpha_{-r+1}^2 = 0 \Rightarrow \alpha_{-r+2} = 0 \\ \vdots \\ \alpha_{-r}\alpha_0 + \alpha_{-r+1}\alpha_1 + \cdots + \alpha_0\alpha_{-r} = 0 \Rightarrow 2\alpha_0\alpha_{-r} = 0 \Rightarrow \alpha_0 = 0 \\ \alpha_{-r+1}\alpha_0 + \alpha_{-r}\alpha_1 + \cdots + \alpha_0\alpha_{r+1} = 0 \Rightarrow \alpha_1 = 0 \\ \vdots \\ \alpha_{-r}\alpha_r + \alpha_{-r+1}\alpha_{r-1} + \cdots + \alpha_r\alpha_{-r} = 0 \Rightarrow 2\alpha_{-r}\alpha_r = 0 \end{gathered}$$

which is a contradiction, since $\alpha_{-r}, \alpha_r \neq 0$. □

Let u be an algebraic element over an extension of $F(t)$, such that $u^2 = a^4 - 1$.

Lemma 4.3.6. *The pairs* (X_n, Y_n) *satisfy* $X_n + uY_n = (X_1 + uY_1)^n$.

Proof. We will do induction to n. For $n = 1$, the lemma holds. Assume that the lemma holds for $n = k$. Then

$$\begin{aligned} X_{k+1} + uY_{k+1} &= a^2 X_k + u^2 Y_k + uX_k + ua^2 Y_k \\ &= a^2(X_k + uY_k) + u(X_k + uY_k) \\ &= (X_k + uY_k)(a^2 + u) \\ &= (X_1 + uY_1)^k (X_1 + uY_1) \\ &= (X_1 + uY_1)^{k+1}. \end{aligned}$$

□

Let supppose for a moment that the following lemma holds.

Lemma 4.3.7. *Let* $a \in F[t, t^{-1}]$*, such that* $T(a)$ *holds. Then the solutions of* (4.3.1) *are given by* $(X, Y) = (\pm X_n, Y_n)$*,* $n \in \mathbb{Z}$*.*

Let $Z \sim 0$ denote the relation $a^2 - 1 \,|\, Z$ in $F[t, t^{-1}]$. Then we have that

$$Z \sim 0 \leftrightarrow \exists V \in F[t, t^{-1}] : Z = V(a^2 - 1).$$

Thus, the relation $Z \sim 0$ is defined by a positive existential formula in the language $\mathcal{L}_T$. By lemma 3.1.7, for $t = a^2$ such that $T(a)$, we obtain

$$Y_n \equiv n (\text{mod } a^2 - 1).$$

Theorem 4.3.8. *The positive existential theory of* $F[t, t^{-1}]$*, in the language* $\mathcal{L}_T$*, is undecidable.*

Proof. Let $P(t_1, \dots, t_n)$ a polynomial with coefficients lay in $\mathbb{Z}$ and $(z_1, \dots, z_n) \in \mathbb{Z}^n$ a root of P. Then, by the previous observation, we have

$$P(Y_{z_1}, \dots, Y_{z_n}) \equiv P(z_1, \dots, z_n) (\text{mod } a^2 - 1) \equiv 0 (\text{mod } a^2 - 1).$$

Therefore, $P(Y_{z_1}, \dots, Y_{z_n}) \sim 0$.

Now, assume that $P(Y_{z_1}, \dots, Y_{z_n}) \sim 0$, for some integers $z_1, \dots, z_n$. By the definition of $\sim$, we have that $P(Y_{z_1}, \dots, Y_{z_n}) \equiv 0 (\text{mod } a^2 - 1)$, so by previous observation we obtain

$$\begin{gathered} P(Y_{z_1}, \dots, Y_{z_n}) \equiv 0 (\text{mod } a^2 - 1) \Leftrightarrow \\ P(z_1, \dots, z_n) \equiv 0 (\text{mod } a^2 - 1). \end{gathered}$$

Since $P(z_1, \dots, z_n)$ is a constant and $a^2 - 1$ is not, we obtain that $P(z_1, \dots, z_n) = 0$. Thus we have shown the equivalence

$$\exists z_1, \dots, z_n \in \mathbb{Z} : P(z_1, \dots, z_n) = 0 \leftrightarrow \exists Y_{z_1}, \dots, Y_{z_n} \in F[t, t^{-1}] : P(Y_{z_1}, \dots, Y_{z_n}) \sim 0$$

and the relation $\sim$ is defined by a positive existential formula of $F[t, t^{-1}]$ in the language $\mathcal{L}_T$ with parameter a. So if there was an algorithm for deciding the truth of positive existential sentences of $F[t, t^{-1}]$ in the language $\mathcal{L}_T$, then it could be converted into an algorithm for deciding whether a diophantine equation over $\mathbb{Z}$ has an integer solution or not, which contradicts with the negative answer of HTP in [11]. □

An effort to prove lemma 4.3.7.

The method we tried has been introduced in 4.2.4, by Pheidas and Zahidi.

We can easily verify that the pairs $(\pm X_n, Y_n)$, $n \in \mathbb{Z}$ satisfy the equation (4.3.1). Indeed, since $u^2 = a^4 - 1$ we have that the inverse of $a^2 + u$ is $a^2 - u$. Therefore,

$$\begin{aligned} X_n - uY_n &= (X_1 - uY_1)^n \\ &= (a^2 - u)^n \\ &= ((a^2 + u)^{-1})^n \\ &= (a^2 + u)^{-n}. \end{aligned}$$

Thus,

$$\begin{aligned} (\pm X_n)^2 - u^2 Y_n^2 &= (X_n + uY_n)(X_n - uY_n) \\ &= (a^2 + u)^n (a^2 + u)^{-n} \\ &= 1. \end{aligned}$$

So $(\pm X_n, Y_n)$ satisfy (4.3.1).

Conversely, suppose that (X, Y) is a solution of (4.3.1). We will do induction to the degree of Y. Notice that if $Y = 0$ then $X = \pm 1$. Therefore we obtain the solutions $(\pm X_0, Y_0)$, so the lemma holds in this case. Assume that $\deg_+(Y) = \deg_-(Y) = 0$. Then $Y = c$, for some $c \in F^*$. So we have that

$$X^2 - a^4 c^2 = 1 - c^2.$$

Suppose that $c \neq \pm 1$. Then we obtain that

$$\begin{aligned} \frac{1}{1 - c^2}(X^2 - a^4 c^2) = 1 \Rightarrow \\ \frac{1}{1 - c^2}(X + a^2 c)(X - a^2 c) = 1, \end{aligned}$$

so there exist $\tilde{c} \in F^*$ and an integer n such that

$$\begin{aligned} \frac{1}{1 - c^2}(X + a^2 c) &= \tilde{c} t^n \\ (X - a^2 c) &= \frac{1}{\tilde{c}} t^n. \end{aligned}$$

Hence, we obtain

$$a^2 = \frac{(1 - c^2)\tilde{c}}{2c} t^n - \frac{1}{2c\tilde{c}} t^{-n},$$

which is impossibly by the proof of lemma 4.3.5. Consequently, $c = Y = \pm 1$ and therefore $X = \pm a^2$. Hence (X, Y) equals either to $(\pm X_1, Y_1)$ or to $(\pm X_{-1}, Y_{-1})$.

Suppose that the lemma holds for the solutions (Z, W) of (4.3.1) such that

$$\deg_+(W) < \deg_+(Y).$$

Assume that $\deg_+(a) \leq 0$. Since a is not a constant, we have $\deg_-(a) < 0$. We consider the automorphism ϕ of $F[t, t^{-1}]$ that fixes F elementwise and sends t to t^{-1}, so we obtain

$$\begin{aligned} 1 = \phi(1) &= \phi(X^2 - (a^4 - 1)Y^2) \\ &= \phi(X^2) + \phi(Y^2) - \phi(a^4)\phi(Y^2) \\ &= X(t^{-1})^2 + Y(t^{-1})^2 - a(t^{-1})^4 Y(t^{-1})^2. \end{aligned}$$

Therefore, $(X(t^{-1}), Y(t^{-1}))$ is also a solution of (4.3.1) and $\deg_+(a) > 0$. Therefore, without the loss of generality, we can assume that $\deg_+(a) > 0$. Define

$$\begin{aligned} Z_1 = a^2X + (a^4 - 1)Y, W_1 = X + a^2Y \\ Z_2 = a^2X - (a^4 - 1)Y, W_2 = X - a^2Y. \end{aligned}$$

We have $W_1W_2 = X^2 - a^4Y^2 = 1 - Y^2$, thus

$$\deg_+(W_1W_2) = \deg_+(1 - Y^2) \tag{4.3.3}$$

and

$$\deg_-(W_1W_2) = \deg_-(1 - Y^2). \tag{4.3.4}$$

We consider the following cases:

1) *Case* $\deg_+(Y) > 0$. Relation (4.3.3) yields $\deg_+(W_1W_2) = \deg_+(Y^2)$. Assume that $\deg_+(W_1) = \deg_+(W_2) = \deg_+(Y)$. Then $\deg_+(W_1 - W_2) \leq \deg_+(Y)$ and

$$\begin{aligned} \deg_+(W_1 - W_2) &= \deg_+(2a^2Y) \\ &= \deg_+(a^2) + \deg_+(Y). \end{aligned}$$

Consequentely, $\deg_+(a^2) + \deg_+(Y) \leq \deg_+(Y)$, which contradicts to the hypothesis that $\deg_+(a) > 0$. Thus, either $\deg_+(W_1) < \deg_+(Y)$ or $\deg_+(W_2) < \deg_+(Y)$.

2) *Case* $\deg_+(Y) = 0$. Relation (4.3.3) yields $\deg_+(W_1W_2) \leq 0$. Thus, either $\deg_+(W_1) = \deg_+(W_2) = 0$ or one of W_1, W_2 has positive degree equal to $-\infty$. Assume the former case. We have that Y, W_1, W_2 lie in $F[t^{-1}]$. Let $r > 0$. Since $W_1 \in F[t^{-1}]$, we obtain

$$X_r + (a^2Y)_r = 0,$$

where $X_r, (a^2Y)_r$ denote the coefficients of t^r in the polynomials X, a^2Y respectively. In addition, since $W_1 \in F[t^{-1}]$, we obtain

$$X_r - (a^2Y)_r = 0.$$

Hence $2(a^2Y)_r = 0$, so $(a^2Y)_r = 0$. Therefore, $a^2Y \in F[t^{-1}]$ and since $\deg_+(a) > 0$ we obtain that $\deg_+(Y) = -\infty$, which contradicts with our hypothesis. Thus, either $\deg_+(W_1) = -\infty$ or $\deg_+(W_2) = -\infty$. Therefore, since $\deg_+(Y) = 0$, we have that $\deg_+(W_i) < \deg_+(Y)$ for $i = 1$ or 2.

The only case which remains unproven is when $\deg_+(Y) = -\infty$.

Bibliography

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

[2] M. Davis, Y. Matijasevič and J. Robinson, *Hilbert's Tenth Problem. Diophantine Equations: Positive aspects of a negative solution*,Proceedings of Symposia in Pure Mathematics, vol. 28, 323–378, 1976.

[3] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proceedings of the American Mathematical Society, vol. 48, 214–220, 1975.

[4] J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society, vol. 242, 391–399, 1978.

[5] J. Denef, *The diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78 (editors M. Boffa, D. van Dalen, K. McAloon), North-Holland, 131–145, 1979.

[6] J. Denef, *Diophantine sets over algebraic integer rings*, Transactions of the American Mathematical Society, vol. 257, 227–236, 1980.

[7] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Wiley, 3rd Edition, 2003.

[8] K.H. Kim and F.W. Roush, *Undecidability of parametric solutions of polynomial equations*, Proceedings of the American Mathematical Society, vol. 118 (2), 345–348, 1993.

[9] S. Lang, *Algebra*, Springer, Graduate Texts in Mathematics, 2002.

[10] C.L. Liu, *Elements of Discrete Mathematics*, McGraw-Hill, 2nd Edition, 1985.

[11] Y. Matijasevič, *The diophantiness of enumerable sets* , Doklady Akademii Nauka SSSR, vol. 191, 279–282, 1970.

[12] P. Pappas, *A diophantine problem for Laurent polynomial rings*, Proceedings of the American Mathematical Society, vol. 93 (4), 713–718, 1985.

[13] T. Pheidas, *Extensions of Hilbert's Tenth Problem*, Journal of Symbolic Logic, vol. 59 (2), 372–397, 1994.

[14] T. Pheidas, *Diophantine undecidability for addition and divisibility in polynomial rings*, Fundamenta Mathimaticae, vol. 182, 205–220, 2004.

[15] T. Pheidas and K. Zahidi, *Undecidable existential theories of polynomial rings and function fields*, Communications in Algebra, vol. 27 (10), 4993-5010, 1999.

[16] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics, 2007.

[17] T. Pheidas and K. Zahidi, *Decision problems in Algebra and analogues of Hilbert's tenth problem*, . Model theory with Applications to Algebra and Analysis, Cambridge University Press, 207–236, 2008.

[18] B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, https://math.mit.edu/~poonen/papers/aws2003.pdf, 2003.

[19] B. Poonen, *Undecidability in Number Theory*, Notices of the American Mathematical Society, vol. 55 (3), 344–350, 2007.

[20] B. Poonen, *Undecidable problems: A sampler*.

[21] Μ. Μανιού, *Αποφασισιμότητα στην διαφορική άλγεβρα*, μεταπτυχιακή εργασία, e-locus library, 2016.