An analogue of Hilbert's Tenth Problem for the ring of exponential sums

Dimitra Chompitaki

Supervisor:
Thanases Pheidas

Master's Thesis

University of Crete
Department of Mathematics and Applied Mathematics

Herakleion
September, 2016

The committee of this Thesis consists of:
Mihalis Kolountzakis, Professor of Department of Mathematics and Applied Mathematics, University of Crete
Thanases Pheidas (Supervisor), Professor of Department of Mathematics and Applied Mathematics, University of Crete
Xavier Vidaux, Professor of Department of Mathematics, University of Concepción (Chile)

Firstly, I would like to express my gratitude to my supervisor Thanases Pheidas for all his help, guidance and continuous support during the development of this work. Prof. Pheidas' instructions on research and write a paper were very valuable and educational for me. Additionally, I would like to say a big THANKS for trusting me and giving me the opportunity to work with him on the ring of Exponential Sums. I am also grateful to Prof. Xavier Vidaux and Prof. Mihalis Kolountzakis for spending time reading this thesis and providing useful suggestions.

Contents

Εκτενής Περίληψη

Το κεντρικό θέμα της διπλωματικής είναι το αν ο δακτύλιος των εκθετικών αθροισμάτων έχει αποφασίσιμη θετική υπαρξιακή θεωρία. Αυτό είναι ένα πρόβλημα ανάλογο του 10^{ou} προβλήματος του Hilbert για το δακτύλιο των εκθετικών αθροισμάτων μίας μεταβλητής υπεράνω του σώματος των μιγαδικών αριθμών (παρακάτω θα δοθούν ακριβείς ορισμοί). Το πρόβλημα αυτό μπορεί να θεωρηθεί ως ένα πρώτο βήμα για να δοθεί μία απάντηση στην ακόλουθη ερώτηση:

Έστω $\mathcal{H}$ ο δακτύλιος των αναλυτικών συναρτήσεων πάνω στους μιγαδικούς της ανεξάρτητης μεταβλητής z και L_z η γλώσσα της αριθμητικής προσαυξημένη κατά ένα σταθερό – σύμβολο για τη z : $L_z = \{+, \cdot, 0, 1, z\}$

Ερώτηση: Είναι η θετική υπαρξιακή θεωρία του $\mathcal{H}$ στην L_z αποφασίσιμη;

Αυτό το πρόβλημα έχει ουσιαστική σημασία και είναι ακόμα ανοιχτό. Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να διαβάσει τη σχετική βιβλιογραφία που αναφέρεται στο Introduction.

Μέρος της διπλωματικής είναι επίσης η σύντομη παρουσίαση άλλων τριών προβλημάτων αποφασισιμότητας των οποίων τεχνικές και αποτελέσματα χρησιμοποιήθηκαν στην απόδειξη του ανάλογου του 10^{ou} Προβλήματος του $Hilbert$ για το δακτύλιο των εκθετικών αθροισμάτων.

Εισαγωγικά

Το 10^o Πρόβλημα του Hilbert

Το 10^o Πρόβλημα του Hilbert (θα το συμβολίζουμε HTP) ρωτάει αν υπάρχει ένας αλγόριθμος που να απαντάει πάντα σωστά στην ερώτηση αν μία πολυωνυμική εξίσωση πολλών μεταβλητών με ακέραιους συντελεστές έχει ή δεν έχει ακέραιες λύσεις. Το πρόβλημα ανακοινώθηκε από τον ίδιο τον Hilbert το 1900. Ο Yuri Matjiasevich έδωσε αρνητική απάντηση στο πρόβλημα το 1970. Ο Matjiasevich για να καταλήξει στο συμπέρασμα ότι δεν υπάρχει τέτοιος αλγόριθμος βασίστηκε στην ερευνητική δουλειά των Martin Davis , Hilary Putmnan και Julia Robinson. Έπειτα ήταν λογικό να αναρωτηθούν αν θα μπορούσε να υπάρξει ένας τέτοιος αλγόριθμος αν θεωρήσουμε έναν άλλον δακτύλιο πέρα από τους ακεραίους. Για παράδειγμα, είναι ήδη γνωστή η απάντηση για τους δακτυλίους των φυσικών, πραγματικών και μιγαδικών αριθμών όπως επίσης και για το σώμα των ρητών συναρτήσεων. Ωστόσο, το ανάλογο του HTP για το σώμα των ρητών αριθμών είναι ανοιχτό και μάλιστα θεωρείται ως το κύριο ανοιχτό πρόβλημα της περιοχής. Στο κεφάλαιο Introduction παρουσιάζουμε κάποια ανάλογα του HTP υπεράνω δακτυλίων των οποίων η δομή τους χρησιμοποιείται συχνά στα μαθηματικά.

Διοφαντικό Πρόβλημα - Θετική Υπαρξιακή Θεωρία - Ορισμοί

Θεωρία μίας δομής: είναι το σύνολο των προτάσεων που είναι αληθείς στη δομή.

(Θετική) υπαρξιακή θεωρία μίας δομής: είναι το σύνολο των (θετικών) υπαρξιακών προτάσεων που είναι αληθείς στη δομή.

Γλώσσα L: είναι μία ακολουθία συμβόλων η οποία εν γένει περιλαμβάνει τα σύμβολα $+$ (για την πρόσθεση) , $\cdot$ (για τον πολλαπλασιασμό) , 0 (για το ουδέτερο στοιχείο της πρόσθεσης στον R) και 1 (για το ουδέτερο στοιχείο του πολλαπλασιασμού στον R). Επίσης, στην L μπορεί να περιλαμβάνονται σύμβολα για ειδικά στοιχεία του δακτυλίου R.

Λέμε ότι το **Διοφαντικό πρόβλημα** για το δακτύλιο R με συντελεστές στον R' είναι μη επιλύσιμο αν υπάρχει ένας αλγόριθμος που να αποφασίζει αν μία πολυωνυμική εξίσωση πολλών μεταβλητών με συντελεστές στον R' έχει λύση στον R.

Η Εξίσωση του Pell

Η διοφαντική εξίσωση

$$x^2 - dy^2 = 1 \tag{0.0.1}$$

όπου d είναι θετικός ακέραιος ελεύθερος τετραγώνου, είναι γνωστή ως η εξίσωση του Pell.
Οι J.Robinson, M.Davis και ο Y.Matjiasevich χρησιμοποίησαν εξισώσεις της παραπάνω μορφής και εισήγαγαν νέους μεθόδους για την επίλυση προβλημάτων της περιοχής. Μία σημαντική και ιδιαίτερα χρήσιμη παρατήρηση για τις λύσεις της εξίσωσης του Pell είναι η ακόλουθη:

Παρατήρηση: Έστω (a_1, b_1) και (a_2, b_2) λύσεις της παραπάνω εξίσωσης. Τότε το ζευγάρι $(a_1, b_1) \oplus (a_2, b_2) = (a_1a_2 + db_1b_2, a_1b_2 + a_2b_1)$ είναι επίσης λύση της εξίσωσης.

Το ανάλογο του HTP για τους πολυωνυμικούς δακτυλίους και τους τετραγωνικούς δακτυλίους

Το ανάλογο HTP για τους πολυωνυμικούς δακτυλίους

Θεώρημα: Έστω R μία ακέραια περιοχή χαρακτηριστικής 0 τότε το διοφαντικό πρόβλημα για τον $R[T]$ με συντελεστές στο $\mathbb{Z}[T]$ είναι μη επιλύσιμο.

Ιδέα της απόδειξης: Ο $Denef$ ορίζει με υπαρξιακό τρόπο τους ακεραίους μέσα στο δακτύλιο $R[T]$. Το καταφέρνει αυτό χρησιμοποιώντας τις λύσεις μίας εξίσωσης που είναι μία μορφή της εξίσωσης του $Pell$ υπεράνω του $R[T]$. Συγκεκριμένα αποδεικνύει το παρακάτω λήμμα

Ορίζει μονοσήμαντα δύο ακολουθίες πολυωνύμων $(x_n), (y_n), n = 0, 1, 2, \ldots,$ στο $\mathbb{Z}[T]$, θέτοντας

$$x_n + Uy_n = (T + U)^n. \tag{0.0.2}$$

όπου U είναι ένα στοιχείο της αλγεβρικής θήκης του $R[T]$ που ικανοποιεί το παρακάτω

$$U^2 = T^2 - 1. \tag{0.0.3}$$

Λήμμα: Οι λύσεις της εξίσωσης $x^2 - (T^2 - 1)y^2 = 1$ υπεράνω του δακτυλίου $R[T]$ δίνονται ακριβώς από

$$x = \pm x_n, \quad y = \pm y_n, \quad n = 0, 1, 2, \ldots$$

όταν βρισκόμαστε σε $char(R) \neq 2$.

και έπειτα για T=1 αντιστοιχεί τις λύσεις y_n με το n όπου $n = 0, 1, 2, \cdots$.

Καταλήγει στο συμπέρασμα ότι αν το Διοφαντικό πρόβλημα για το δακτύλιο $R[T]$ με συντελεστές στο δακτύλιο $\mathbb{Z}[T]$ είναι επιλύσιμο, τότε το Διοφαντικό πρόβλημα για τους ακεραίους θα είναι επιλύσιμο το οποίο αντιφάσκει με την αρνητική απάντηση που έδωσε ο $Matjiasevich$.

Ένα ανάλογο του HTP για τους πολυωνυμικούς δακτυλίους στη γλώσσα L_T

Έστω η γλώσσα $L_T = \{0, 1, +, \cdot, T\}$ και το κατηγόρημα $T[x]$ ερμηνεύεται ως "$x \notin A$".

Θεώρημα: Η θετική υπαρξιακή θεωρία ενός πολυωνυμικού δακτυλίου A, με A μία ακέραια περιοχή, στη γλώσσα L_T, είναι μη αποφασίσιμη .

Οι λύσεις της εξίσωσης του *Pell* χρησιμοποιούνται και από τους *Pheidas* και *Zahidi* για να ορίσουν με έναν θετικό υπαρξιακό τρόπο τους ακεραίους υπεράνω του δακτυλίου $A[t]$ μέσα από τη δομή της L_T. Οπότε, αποδεικνύουν το ακόλουθο λήμμα:

Λήμμα: Υποθέτουμε ότι $a \in A[t]$ για το οποίο T$[a]$ (δηλ. a δεν είναι μία σταθερά). Τότε οι λύσεις της εξίσωσης

$$x^2 - (a^2 - 1)y^2 = 1 \tag{0.0.4}$$

δίνονται ακριβώς από $(x, y) = (\pm x_n[a], y_n[a])$ για $n \in \mathbb{Z}$.

Τελικά καταλήγουν στην παρακάτω αναγωγή που αποδεικνύει το θεώρημα: Αν υπήρχε αλγόριθμος που να αποφασίζει ποια θετική υπαρξιακή πρόταση της L_T είναι αληθής μέσα στον $A[t]$ τότε θα είχαμε έναν αλγόριθμο που να αποφασίζει αν μία Διοφαντική εξίσωση υπεράνω των ακεραίων έχει μία λύση στους ακεραίους ή όχι, το οποίο αντιφάσκει με την αρνητική απάντηση στο HTP που έδωσε ο *Matjiasevich*.

Το ανάλογο του HTP για το δακτύλιο των ακεραίων του Gauss

Θεώρημα: Το ανάλογο του HTP για κάθε τετραγωνικό δακτύλιο είναι μη επιλύσιμο.

Εμάς μας ενδιαφέρει ωστόσο, η επιλυσιμότητα των διοφαντικών εξισώσεων υπεράνω του δακτυλίου του *Gauss* ο οποίος συμβολίζεται με $\mathbb{Z}[i]$. Τα στοιχεία του $\mathbb{Z}[i]$ είναι της μορφής $a + ib$ όπου $a, b \in \mathbb{Z}$.

Για να αναχθεί το HTP στο ανάλογο του για το $\mathbb{Z}[i]$ ο *Denef* χρησιμοποιεί αποτελέσματα από το [5] ,δείχνει ότι η σχέση $x \in \mathbb{N}$ είναι διοφαντική υπεράνω

του $\mathbb{Z}[i]$ και έπειτα αποδεικνύει ότι το σύνολο των ακεραίων είναι ορίσιμο υπεράνω του $\mathbb{Z}[i]$ κατασκευάζοντας ένα σύστημα διοφαντικών εξισώσεων όπως φαίνεται στο παρακάτω λήμμα το οποίο για να το αποδείξει κάνει χρήση ξανά των λύσεων της εξίσωσης του $Pell$.

Λήμμα: Υπάρχει ένα πεπερασμένο σύστημα Σ διοφαντικών εξισώσεων με αγνώστους $t, x, \ldots, s \in \mathbb{Z}[i]$ τέτοιο ώστε οι ακόλουθες δύο συνθήκες να ικανοποιούνται:

(1) Αν Σ έχει μία λύση $\langle t, x, \ldots, s\rangle$ στο $\mathbb{Z}[i]$, τότε $t \in \mathbb{Z}$.

(2) Αν $k \in \mathbb{N}$ και $k \neq 0$, τότε Σ έχει μία λύση $\langle t, x, \ldots, s\rangle$ ιν $\mathbb{Z}[i]$ με $t = k^2$.

Ένα ανάλογο του HTP για το δακτύλιο των εκθετικών αθροισμάτων

Ορισμός: Ο δακτύλιος των **εκθετικών πολυωνύμων**, συμβ. $\mathbb{C}[z]^E$ είναι ο μικρότερος δακτύλιος που περιέχει το $\mathbb{C}[z]$ και το e^z και είναι κλειστός κάτω από τις αριθμητικές πράξεις και τη σύνθεση.

Ορισμός: Ο δακτύλιος των **εκθετικών αθροισμάτων** με τις συνήθεις πράξεις, συμβ. $EXP(\mathbb{C})$ είναι ένας υποδακτύλιος του $\mathbb{C}[z]^E$ και τα στοιχεία του είναι της μορφής

$$a = \alpha_0 + \alpha_1 e^{\mu_1 z} + \cdots + \alpha_N e^{\mu_N z} \tag{0.0.5}$$

όπου $\alpha_0, \alpha_1, \ldots, \alpha_N \in \mathbb{C} \setminus \{0\}$ και $\mu_i \in \mathbb{C} \setminus \{0\}\cdot$ και είναι ανά δύο διακριτά.

Ορισμός: Το πολυώνυμο $Laurent$ με συντελεστές σε ένα σώμα F είναι μία έκφραση της μορφής

$$p = \sum_k p_k z^k, \quad p_k \in F$$

όπου z είναι μία τυπική μεταβλητή, k είναι ακέραιος και πεπερασμένοι συντελεστές p_k είναι διάφοροι του μηδενός.

Θεωρούμε τώρα τη γλώσσα

$$L = \{+, \cdot, 0, 1, e^z\} \tag{0.0.6}$$

Ερώτηση: Είναι η θετική πρωτοτάξια θεωρία του $EXP(\mathbb{C})$, ως μία δομή της γλώσσας L, αποφασίσιμη ή μη αποφασίσιμη;

Σε ένα πρόσφατο μη δημοσιευμένο *paper* οι $P.DAquino$, $Th.Pheidas$ και $G.Terzo$ έχουν δώσει αρνητική απάντηση σε αυτή την ερώτηση. Εδώ θα παρουσιάσουμε μία διαφορετική απόδειξη μερικώς βασισμένη στη δική τους, χρησιμοποιώντας όμως ως βασικό εργαλείο τις λύσεις της εξίσωσης του $Pell$ αντί για τις ελλειπτικές καμπύλες τις οποίες χρησιμοποιούν στην άλλη απόδειξη. Η ιδέα της χρήσης της εξίσωσης του $Pell$ είναι του $A.Macintyre$. Η στρατηγική της απόδειξης που ακολουθήσαμε είναι ιδέα του Θ.Φειδά και μετά μαζί δείξαμε ότι αυτά που σκέφτηκε ισχύουν. Τα αποτελέσματα μας θεωρούνται ως ένα ανάλογο του HTP και ένα μεγάλο βήμα για να αποδειχθεί η ίδια ερώτηση για

τα εκθετικά πολυώνυμα. Αποδεικνύουμε βασικά δύο θεωρήματα των οποίων δίνουμε και μία περίληψη των αποδείξεων τους.

Θεώρημα: Οι λύσεις της εξίσωσης

$$(e^{2z}-1)y^2 = x^2 - 1 \tag{0.0.7}$$

όπου τα x και y ανήκουν στο $EXP(\mathbb{C})$ δίνονται από

$$(x,y) = \kappa \odot (\pm e^z, 1) \oplus \lambda \odot (\pm e^{-z}, \mathrm{i}e^{-z}) \tag{0.0.8}$$

όπου

$$\kappa \odot (e^z,1) = (e^z,1) \oplus \cdots \oplus (e^z,1)$$

($(e^z,1)$ προστίθεται στον εαυτό του υπό τον νόμο $\oplus$ κ φορές.)
και για κάθε λύση (a_1,b_1), (a_2,b_2) της εξίσωσης ο νόμος $\oplus$ ορίζεται από $(a_1,b_1)\oplus(a_2,b_2) = (a_1a_2 + (e^{2z}-1)b_1b_2, a_1b_2 + a_2b_1)$.

Σημαντικά σημεία της απόδειξης:

Ένα ανάλογο της εξίσωσης του $Pell$ υπεράνω του $EXP(\mathbb{C})$

Θεωρούμε την εξίσωση

$$(e^{2z}-1)y^2 = x^2 - 1 \tag{0.0.9}$$

όπου $x, y \in EXP(\mathbb{C})$. Για να χαρακτηρίσουμε όλες τις λύσεις της παραπάνω εξίσωσης θα χρησιμοποιήσουμε ιδέες από [38]και [28]. Αρχικά θα δώσουμε κάποιες πληροφορίες σχετικές με την αλγεβρική δομή του $EXP(\mathbb{C})$.
Σταθεροποιοούμε μία λύση (x,y) της εξίσωσης (0.0.9) και παρατηρούμε από τον ορισμό του $EXP(\mathbb{C})$ ότι τα $\hat{x}$ και $\hat{y}$ ανήκουν σε ένα δακτύλιο της μορφής $R = \mathbb{C}[e^{\mu_1 z}, e^{-\mu_1 z}, \ldots, e^{\mu_k z}, e^{-\mu_k z}]$, όπου k είναι ένας φυσικός αριθμός και κάθε $\mu_i \in \mathbb{C}$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι ισχύει

$$\mu_1 = 1 \ ,$$

για το δακτύλιο R.
Έστω $\{1, \rho_2, \cdots, \rho_\ell\}$, όπου $\rho_i \in \mathbb{C}$, να είναι μία βάση του διανυσματικού χώρου

που γεννιέται από μ_i υπεράνω του σώματος $\mathbb{Q}$. Τότε είναι προφανές ότι κάθε μ_i είναι ένας γραμμικός συνδυασμός υπεράνω του $\mathbb{Q}$ των $\{1, \rho_2, \cdots, \rho_\ell\}$.
Άρα, για κάθε μ_i υπάρχουν ακέραιοι n_{ij} και ένας θετικός ακέραιος N_i τέτοιος ώστε $\mu_i = \frac{1}{N_i}\sum_{j=1}^{\ell} n_{ij}\rho_j$. Διαλέγοντας το N να είναι το ελάχιστο κοινό πολλαπλάσιο των N_i έχουμε ότι για κάθε $i = 1, \dots k$ ότι $\mu_i = \frac{1}{N}\sum_{j=1}^{\ell} n'_{ij}\rho_j$ για κάποιους ακέραιους $nÆ_{ij}$. Τότε παρατηρούμε ότι για κάθε i, $e^{\mu_i z}, e^{-\mu_i z} \in \mathbb{C}[e^z, e^{-z} \dots, e^{\mu_k z}, e^{-\mu_k z}]$, άρα $\mathbb{C}[e^z, e^{-z} \dots, e^{\mu_k z}, e^{-\mu_k z}] \subseteq \mathbb{C}[e^{\frac{1}{N}z}, e^{-\frac{1}{N}z}, \dots, e^{\frac{1}{N}\rho_\ell z} e^{-\frac{1}{N}\rho_\ell z}]$.
Άρα,

$$x, y \in R = \mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, \dots, e^{\frac{1}{N}\rho_\ell \cdot z}, e^{-\frac{1}{N}\rho_\ell \cdot z}]$$

.

Τώρα ισχυριζόμαστε ότι τα $\{e^{\frac{1}{N}\cdot z}, \dots, e^{\frac{1}{N}\rho_\ell \cdot z}\}$ είναι αλγεβρικώς ανεξάρτητα υπεράνω του $\mathbb{C}$. Αυτό ακολουθεί από το ότι $\{\frac{1}{N}, \dots, \frac{1}{N}\rho_\ell\}$ είναι γραμμικά ανεξαρτητα υπεράνω του $\mathbb{Q}$ και από το ακόλουθο λήμμα από [38]:
Λήμμα: Έστω ότι $\{\nu_1, \dots, \nu_\ell\}$ είναι ένα σύνολο μιγαδικών αριθμών, οι οποίοι είναι γραμμικώς ανεξάρτητοι υπεράνω του $\mathbb{Q}$. Τότε το σύνολο των συναρτήσεων $\{e^{\nu_1 \cdot z}, \dots, e^{\nu_\ell \cdot z}\}$ είναι αλγεβρικώς ανεξάρτητα στο $\mathbb{C}$.

Άρα, το σύνολο των συναρτήσεων είναι $\{e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, \dots, e^{\frac{1}{N}\rho_\ell \cdot z}, e^{-\frac{1}{N}\rho_\ell \cdot z}\}$ είναι αλγεβρικώς ανεξάρτητο υπεράνω του $\mathbb{C}$. Θέτουμε

$$\begin{aligned} Z &= e^{\frac{1}{N}z} \\ t_2 &= e^{\frac{1}{N}\rho_2 \cdot z} \\ &\dots \\ t_\ell &= e^{\frac{1}{N}\rho_\ell \cdot z} \end{aligned} \quad . \quad (0.0.10)$$

Τότε $x, y \in \mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, t_2, t_2^{-1}, \dots t_\ell, t_\ell^{-1}]$ και τα στοιχεία $t_2, \dots t_\ell$ μπορούν να θεωρηθούν ως μεταβλητές του $\mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}]$.

Άρα η αρχική εξίσωση γίνεται

$$(Z^{2N} - 1)y^2 = x^2 - 1 \quad (0.0.11)$$

υπεράνω του δακτυλίου

$$\mathbb{C}[Z, Z^{-1}, t_2, t_2^{-1}, \dots, t_\ell, t_\ell^{-1}] \ .$$

Σε επόμενο στάδιο βλέπουμε ότι κάθε λύση παραπάνω εξίσωσεις θα βρίσκεται στο $\mathbb{C}[Z^N, Z^{-N}]$.

Πρώτα όμως αποδεικνύουμε ότι x, y είναι μέσα στον $\mathbb{C}[Z, Z^{-1}]$.

Λήμμα: Έστω A να είναι μία ακέραια περιοχή, που περιέχει το $\mathbb{C}[Z, Z^{-1}]$, τέτοιος ώστε $Z^{2N} - 1$ να μην είναι τετράγωνο στο A. Έστω t να είναι μία μεταβλητή και (x, y) να είναι μία λύση της 3.3.7 με $x, y \in A[t, t^{-1}]$. Τότε $x, y \in A$.

Άρα η λύση (x, y) της εξίσωσης 3.3.7 ανήκει στο δακτύλιο $\mathbb{C}[Z, Z^{-1}]$ και η λύση $(\hat{x}, \hat{y})$ της εξίσωσης 3.3.7 ανήκει στο δακτύλιο $\mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}]$.

Οι λύσεις της γενικευμένης εξίσωσης του Pell υπεράνω του $\mathbb{C}[Z, Z^{-1}]$

Λήμμα: Οι λύσεις της εξίσωσης 3.3.7 δίνονται από $(\pm x, y) = (x_\kappa[Z^N], y_\kappa[Z^N]) \oplus (x_\lambda[Z^{-N}], -\mathrm{i}Z^{-N} y_\lambda[Z^{-N}])$, για $\kappa, \lambda \in \mathbb{Z}$.

Ιδέα της απόδειξης:
Έστω (x, y) μία λύση της 3.3.7 , όπου $x, y \in \mathbb{C}[Z, Z^{-1}]$ και $x \notin \mathbb{C}$.

Γνωρίζουμε από τα προηγούμενα ότι οι λύσεις της 3.3.7 φτιάχνουν μία ομάδα με την πράξη $\oplus$ που δίνεται από $(a_1, b_1) \oplus (a_2, b_2) = (a, b)$, όπου

$$a = a_1 a_2 + (Z^{2N} - 1) b_1 b_2 \text{ και } b = a_1 b_2 + b_1 a_2 \ . \tag{0.0.12}$$

Ορίζουμε,

$$(\tilde{x}, \tilde{y}) = (x, y) \oplus (x_1[Z^N], y_1[Z^N]) \tag{0.0.13}$$

ανδ

$$(\underline{x}, \underline{y}) = (x, y) \ominus (x_1[Z^N], y_1[Z^N]) \tag{0.0.14}$$

όπου $\ominus$ είναι το αρνητικό σύμβολο το οποίο σχετίζεται με το νόμο του $\oplus$.

Ο τρόπος που αποδεικνύουμε το λήμμα είναι:

Υποθέτουμε ότι $deg_+(x) \geq N$. Αποδεικνύουμε ότι ένα από τα $\deg_+(\tilde{x})$ και $\deg_+(\underline{x})$ είναι μικρότερο από $\deg_+(x)$. Επαναλαμβάνοντας την ίδια διαδικασία

παίρνουμε ότι υπάρχει ένα $\kappa \in \mathbb{Z}$ τέτοιο ώστε, θέτοντας $(\dot{x}, \dot{y}) = (x, y) \ominus (\kappa \odot (Z^N, 1))$, έχουμε ότι $\deg_+(\dot{x}) < N$. Έπειτα αποδεικνύουμε ότι οι μόνες λύσεις $(\dot{x}, \dot{y})$ με $\deg_+(\dot{x}) < N$ είναι υπεράνω του $\mathbb{C}[Z^{-1}]$. (Σε αυτή την περίπτωση το Λήμμα ακολουθεί απο [23]).

Με επαγωγή στο θετικό βαθμό του x αποδεικνύουμε το λήμμα.

Θεώρημα: Ο δακτύλιος $\mathbb{Z}[i]$ είναι θετικά υπαρξιακά ορισμένος υπεράνω του $EXP(\mathbb{C})$, ως L-δομή. Άρα η θετική υπαρξιακή θεωρία αυτής της δομής είναι μη αποφασίσιμη.

Ορίζουμε $V \sim U$ να σημαίνει ότι τα πολυώνυμα V και U στο $\mathbb{C}[Z, Z^{-1}]$ παίρνουν την ίδια τιμή για $Z = 1$. Αποδεικνύουμε τα παρακάτω λήμματα τα οποία χρειάζονται για την απόδειξη του θεωρήματος.

Λήμμα Έχουμε ότι $y_{\kappa,\lambda} \sim \kappa - i\lambda$, για $n, \kappa, \lambda = 0, 1, 2, \ldots$

Παρατήρηση: Η σχέση $W \sim 0$ είναι διοφαντική υπεράνω $\mathbb{C}[Z, Z^{-1}]$ με συντελεστές στο $\mathbb{Z}[Z, Z^{-1}]$:

$$W \sim 0 \text{ αν και μόνον εάν } \exists x \in \mathbb{C}[Z, Z^{-1}] : W = (Z - 1)x \ .$$

Ορίζουμε την πρωτοτάξια σχέση $Imt(y)$ στο $\mathbb{C}[Z, Z^{-1}]$ ως εξής :

$$Imt(y) \leftrightarrow y \in \mathbb{C}[Z, Z^{-1}] \bigwedge \exists x \in \mathbb{C}[Z, Z^{-1}] : x^2 - (Z^{2N} - 1)y^2 = 1 \ .$$

Λήμμα: Ισχύει ότι :

ι Η σχέση $Imt(y)$ είναι διοφαντική υπεράνω $\mathbb{C}[Z, Z^{-1}]$ με συντελεστές στο $\mathbb{Z}[Z, Z^{-1}]$.

ιι Αν το y ικανοποιεί τη $Imt(y)$, τότε υπάρχουν ακέραιοι κ, λ τέτοιοι ώστε $y \sim \kappa - i\lambda$.

ιιι Για κάθε ακέραιο κ, λ υπάρχει ένα πολυώνυμο $Laurent$ y που ικανοποιεί τη $Imt(y)$ και τη $y \sim \kappa - i\lambda$.

Απόδειξη του Θεωρήματος

Από το προηγούμενο λήμμα έχουμε ότι ισχύει:

$$\exists z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \Leftrightarrow \exists Z_1, \ldots, Z_n \in \mathbb{C}[Z, Z^{-1}] :$$

$$(Imt(Z_1) \wedge \cdots \wedge Imt(Z_n) \wedge P(Z_1, \ldots, Z_n) \sim 0).$$

Η τελευταία σχέση γράφεται ισοδύναμα

$$\bigwedge_{i=1}^{n} \mathrm{Imt}(Z_i) \bigwedge P(Z_1, \ldots, Z_n) \sim 0$$

και προσομοιώνουμε κάθε $Imt(Z_i)$ με το

$$\exists X_i \in \mathbb{C}[Z, Z^{-1}] : X_i^2 - (Z^{2N} - 1)Z_i^2 = 1$$

Αφού οι Imt και $\sim$ είναι διοφαντικές υπεράνω $\mathbb{C}[Z, Z^{-1}]$ με συντελεστές στο $\mathbb{Z}[Z, Z^{-1}]$ εύκολα μπορούμε να βρούμε ένα πολυώνυμο P^* που να ικανοποιεί τα παρακάτω: Υπάρχει αλγόριθμος που να βρίσκει για κάθε πολυώνυμο $P(z_1, \ldots, z_n)$ υπεράνω $\mathbb{Z}[i]$, ένα πολυώνυμο $P^*(Z_1, \ldots, Z_m)$ υπεράνω $\mathbb{Z}[Z, Z^{-1}]$ τέτοιο ώστε

$$\exists z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \text{ αν και μόνο αν } \exists Z_1, \ldots, Z_m \in \mathbb{C}[Z, Z^{-1}] : P^*(Z_1, \ldots, Z_m) = 0 \tag{0.0.15}$$

Άρα αν το διοφαντικό πρόβλημα για το $\mathbb{C}[Z, Z^{-1}]$ με συντελεστές στο $\mathbb{Z}[Z, Z^{-1}]$ ήταν επιλύσιμο, τότε το διοφαντικό προβλημα για το $\mathbb{Z}[i]$ θα ήταν επιλύσιμο, το οποίο αντιφάσκει με την αρνητική απάντηση του ανάλογου του HTP για το $\mathbb{Z}[i]$ που έδωσε ο [7].

Abstract

At a glance: We prove that the positive existential theory of the ring of exponential sums is undecidable.

Define the set of *exponential sums*, EXP($\mathbb{C}$), to be the the set of expressions

$$a = \alpha_0 + \alpha_1 e^{\mu_1 z} + \cdots + \alpha_N e^{\mu_N z}$$

where $\alpha_i, \mu_j \in \mathbb{C}$. We ask whether the positive existential first order theory of EXP($\mathbb{C}$), as a structure of the language

$$\mathbf{L} = \{+, \cdot, 0, 1, e^z\}$$

is decidable or undecidable. Our result may be considered as an analogue of Hilbert's Tenth Problem for this structure and as a step to answering the similar problem for the ring of exponential polynomials, which is still open. We prove:

Theorem 1 *The ring of gaussian integers $\mathbb{Z}[i]$ is positive existentially definable over EXP($\mathbb{C}$), as an L-structure. Hence the positive existential theory of this structure is undecidable.*

In order to prove Theorem 1 we adapt techniques of [8] and we show Theorem 2:

We consider the equation

$$(e^{2z}-1)y^2 = x^2 - 1 \tag{0.0.16}$$

where $x, y \in \mathrm{EXP}(\mathbb{C})$.

Let (a_1, b_1) and (a_2, b_2) be solutions of (0.0.16). We define the law $\oplus$ by

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1a_2 + (e^{2z}-1)b_1b_2, a_1b_2 + a_2b_1)$$

The pair $(a, b) = (a_1, b_1) \oplus (a_2, b_2)$ is also a solution of (0.0.16).
We denote by $\kappa \odot (a, b) = (a, b) \oplus \cdots \oplus (a, b)$. ($(a, b)$ added to itself by $\oplus$ κ times.)

Theorem 2 *The solutions of the equation (0.0.16) are given by*

$$(x, y) = \kappa \odot (\pm e^z, 1) \oplus \lambda \odot (\pm e^{-z}, \mathrm{i}e^{-z}).$$

The proof uses techniques of [38], [28] and [23].

Important points of the proof

We would like to characterise all the solutions of Equation (0.0.16) over $\mathrm{EXP}(\mathbb{C})$. Observe that, by the definition of $\mathrm{EXP}(\mathbb{C})$, x and y lay in some ring of the form $R = \mathbb{C}[e^{\mu_1 z}, e^{-\mu_1 z}, \ldots, e^{\mu_k z}, e^{-\mu_k z}]$, where k is a natural number and each $\mu_i \in \mathbb{C}$.

In [28] it is shown that one can choose the μ_i in such a way that $\mu_1 = \frac{1}{N}$, for some natural number N, and the set $\{1, \mu_2, \cdots, \mu_k\}$ is linearly independent over the field $\mathbb{Q}$. By results of [38] it follows that the set $\{e^{\mu_1 z}, \ldots, e^{\mu_k z}\}$ is algebraically independent over $\mathbb{C}$. So the question about solutions of (0.0.16) becomes

Given a natural number N, find the solutions of

$$(Z^{2N}-1)y^2 = x^2 - 1 \tag{0.0.17}$$

over the ring

$$\mathbb{C}[Z, Z^{-1}, t_2, t_2^{-1}, \ldots, t_\ell, t_\ell^{-1}],$$

where $Z = e^{\frac{1}{N}}$ and the elements $t_2, \ldots t_\ell$ are variables over may be considered as variables over $\mathbb{C}[Z, Z^{-1}]$. At a first stage we show that any solution of (0.0.17) does not depend on the varables t_j, i.e. is over $\mathbb{C}[Z, Z^{-1}]$. Then, extending techniques of [23] we show that any solution is over the ring $\mathbb{C}[Z^N, Z^{-N}]$. Finally we give the characterization of solutions as in Theorem 2. Subsequently the set of integers is positive existentially definable, by techniques of [8] and [7].

The results of Theorem 2 may be stated as

The set of solutions of

$$(T^2 - 1)y^2 = x^2 - 1$$

over the tower of rings

$$\cup_N \mathbb{C}[T^{\frac{1}{N!}}, T^{-\frac{1}{N!}}]$$

stabilizes at the level of $\mathbb{C}[T, T^{-1}]$.

Chapter 1

Introduction

The focus of this Thesis is on answering an analogue of Hilbert's Tenth Problem for the ring of Exponential Sums of one variable over the field of complex numbers (which we denote by $EXP(\mathbb{C})$). Specifically, we show that this analogue is unsolvable. One may view this problem as an effort towards answering the following question. We consider the ring of functions $\mathcal{H}$ of the independent variable z, analytic on $\mathbb{C}$. Let L_z be the language of arithmetic, augmented by a constant-symbol for z: $L_z = \{+, \cdot; 0, 1, z\}$. We ask:

Question 1 *Is the positive existential theory of $\mathcal{H}$ in L_z decidable?*

History-Previous results: The Question is still open. For details on known relative facts see [24]. R. Robinson in [30] proved that the L_z-theory of $\mathcal{H}$ is undecidable. Rubel in [31] asked the Question and the more general one: Given a polynomila equation of many variables over $\mathbb{C}[z]$, decide whether it has a solution which is a tuple of analytic functions of z, with a prescribed radius of convergence (say around $z = 0$). The Question is also mentioned in the surveys [29] and [32].

More is known for the ring $\mathcal{H}_p$ of functions analytic on the p-adic plane $\mathbb{C}_p$ (undecidable diophantine theory, [17]) and for its quotient field $\mathbb{M}_p$ (undecidable diophantine theory in the language that extends L_z by a predicate for the property of a meromorphic function to have no pole at $z = 0$, [41]).

To show that the positive existential theory of ring of Exponential Sums is undecidable which is presented in Chapter 3, we used results from [8], [23] and [7]. For this reason in Chapter 2 we give the main Theorems and Lemmas of these papers.

In Chapter 1 we also present some information regarding Hilbert's Tenth Problem and some analogues of Hilbert's Tenth Problem for some structures of common use.

1.1 Hilbert's Tenth Problem

Hilbert's Tenth Problem: *Give a procedure which, in a finite number of steps, can determine whether a polynomial equation (in several variables) with integer coefficients has or does not have integer solutions.*
In modern mathematics Hilbert's Tenth Problem asks for an algorithm to determine the solvability in integers of Diophantine equations over $\mathbb{Z}$,i.e. of polynomials with integer coefficients (1900).

Yuri Matiyasevich gave a negative answer to Hilbert's Tenth Problem in 1970. He based his work on M.Davis', H.Putman's and J.Robinson's research work. More concretely, in 1953 Martin Davis had shown that every listable set (recursively enumerable) has an arithmetical representation with a single bounded universal quantifier. After some years Martin Davis, Hilary Putnam and Julia Robinson considered the broader class of so called exponential Diophantine equations and obtained a purely existential exponential Diophantine representations for all listable sets (Exponential Diophantine Equation are allowed to have expressions of the form x^y, for variables x and y, ranging over the natural numbers). However in the beginning of the 1950's Julia Robinson had found a sufficient condition for transforming an arbitrary exponential Diophantine equation into an equivalent Diophantine equation. The final step, performed by Yuri Matiyasevich in 1970, consisted in fulfilling this condition of Julia Robinson by providing a Diophantine representation of the set of ordered pairs (u, v) such that $v = F_{2u}$ where F_n is the nth Fibonacci number.

After this results, it was natural to ask whether such an algorithm exists if one considers a ring other than the ring of integers. For example, the Real Numbers, the Complex numbers and a field of rational functions. Hilbert's Tenth Problem for the field of rational numbers is a (or the) major open problem of this area. However Jochen Koenigsmann have showed that $\mathbb{Z}$ is

definable in $\mathbb{Q}$ by a universal first-order formula in the language of rings.

We now present a list of decidability properties of some ring structures of common use.

L_T is the language $\{+, \cdot; =; 0, 1\}$ which, for rings of functions is augmented by the predicate T which is interpreted as 'x is not a constant function'. For rings of functions of the variable z the language L_z is as above.
$\mathbb{Z}$ is the ring of rational integers, $\mathcal{O}_K$ is the ring of integers of the number field K, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{R}$ the field of real numbers, $\mathbb{C}$ the field of complex numbers, $\mathbb{F}_q$ is the finite field with q elements, $B[z]$ the ring of polynomials in the variable z with coefficients in the ring B, $B(z)$ the corresponding field of rational functions in z, $\mathcal{H}(\mathcal{D})$ the ring of analytic functions of the variable z as that ranges in an open superset of the subset D in the complex plane, $\mathcal{M}(\mathcal{D})$ is the corresponding field of meromorphic functions, U is the open unit disk. $EXP(\mathbb{C})$ is the ring of exponential sums.

The first column shows whether the positive existential theory of the ring in the language L_T is decidable or not ('Y' means decidable, 'N' means undecidable, 'conj. N' means 'conjectured to be undecidable', '?' denotes an open problem), the second column corresponds to the similar properties in the language L_z and the third column to that of the full theory in the language L_T for the rings $\mathbb{Z}$, $\mathcal{O}_K$ and $\mathbb{Q}$ and the language L_z for the remaining rings.

Note that it is known that the theories of many rings $\mathcal{O}_K$ are undecidable (e.g. for abelian K) and it has been conjectured that all of them are, but the question for arbitrary K remains open.

	ex. th. (in L_T)	ex. th. in L_z	full th.
$\mathbb{Z}$	N		N
$\mathcal{O}_K$	conj. N		N
$\mathbb{Q}$	?		N
$\mathbb{F}_q[z], \mathbb{R}[z], \mathbb{C}[z]$	N	N	N
$\mathbb{F}_q(z)$	?	N	N
$\mathbb{R}(z)$	?	N	N
$\mathbb{C}(z)$	?	?	?
$\mathcal{H}(\{a\})$	Y	Y	Y
$\mathcal{H}(\mathcal{U})$	Y	?	N
$\mathcal{H}(\mathbb{C})$	?	?	N
$\mathcal{M}(\mathcal{U})$	Y	?	?
$\mathcal{M}(\mathbb{C})$	?	?	?
$\mathbb{R}[[z]]$	Y	Y	Y
$\mathbb{F}_p[[z]]$	Y	Y	?
$EXP(\mathbb{C})$	?	N	N

For a fast introduction to applications of Model Theory to Algebra the reader may consult [3] and [40]. The solution of HTP can be found in [18] and is explained very nicely to the non-expert in [5]. Surveys of questions similar to the present paper's are [22], [24], [29] and [33]. Surveys of elimination ('decidability') techniques and results can be found in [36] (and many later more specialized articles, from the Algebraist's point of view). For our terminology in Algebra we follow [16].

1.2 Positive Existential Theory, a definition

The definitions are from [26].

Structure: consists of a set along with a collection of finitary operations and relations that are defined on it.

Language: each structure comes with a language i.e. a set of symbols for the relations, functions and distinguished elements of the structure.

The first order sentences: of the language of the structure are the sentences built using the symbols of the language, with the variables ranging over the universe of the structure, quantifiers and logical connectives, by the usual rules.

Existential Formula $\alpha(\bar{x})$: is a formula of the form

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

where $m \geq 0$ and $\phi(\bar{x}, \bar{y})$ is quantifier-free (without quantifiers).

Positive existential formula $\alpha(\bar{x})$: An existential formula, as above, with the formula $\phi(\bar{x}, \bar{y})$ has no negations.

(Positive) Existential sentence : a (positive) existential formula which is a sentence (without free variables).

The (full) theory: of the structure is the set of sentences which are true in the structure.

The (positive) existential theory of a structure: is the set of (positive) existential sentences that are true in the structure.

We say that the theory (resp. existential theory, positive-existential theory) is **decidable** if there is an algorithm that determines whether any given sentence (resp. existential sentence, positive-existential sentence) is true or false in the structure. Otherwise the theory is **undecidable**.

1.3 Diophantine Problem

The definitions are from [8] and [22].

Let R be a commutative ring with unity and R' be a subring of R. Let $D(x_1, \ldots, x_n)$ be a relation in R.

Language L (more detail definition): is a sequence of symbols which generally include the symbols + (for addition), $\cdot$ (for multiplication), 0 (for the additive identity of R) and 1 (for the multiplicative identity of R). L can also include symbols for special elements of R. Also, in some cases can exist a structure of a ring R without the full strength of multiplication or addition. In this case, the language L contains symbols for other operations or relations.

Diophantine polynomial in L over R: is a polynomial in several variables whose coefficients can be built from the elements which have symbols to represent them in the language, using addition and multiplication (that is, the coefficients of Diophantine polynomials are elements of the ring which is generated by the elements with symbols in the language).

Diophantine equation: is of the form $P(x_1, ..., x_j, y_1, ..., y_k) = 0$ where $P(\bar{x}, \bar{y})$ is a diophantine polynomial. (Diophantine inequation is $P(\bar{x}, \bar{y}) \neq 0$.)

Diophantine Relation: The $D(x_1, \ldots, x_n)$ is diophantine over R if there exists a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ over R such that for all $x_1, \ldots, x_n$ in R

$$D(x_1, \ldots, x_n) \text{ is diophantine over } R \leftrightarrow$$

$$D(x_1, \ldots, x_n) \leftrightarrow \exists y_1, \ldots, y_m \in R : P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

We have the same definition for subsets of R by regarding them as 1-ary relations:
If P can be chosen such that its coefficients lay in R', then we have that $D(x_1, \ldots, x_n)$ is diophantine over R with coefficients in R'.

We say that the **diophantine problem** for R with coefficients in R' is unsolvable (solvable) if there exists no (an) algorithm to decide whether or not a polynomial equation in several variables with coefficients in R' has a solution in R.

Observation: If R is an integral domain and if D_1 and D_2 are diophantine over R[T] with coefficients in $R'[T]$, then also $D_1 \cup D_2$ and

often $D_1 \cap D_2$ (if T is not a square in R[T]) are diophantine over R[T] with coefficients in $R'[T]$.
Indeed,

$$(P_1 = 0 \cup P_2 = 0) \leftrightarrow (P_1 P_2 = 0) \quad \text{and} \quad (P_1 = 0 \cap P_2 = 0) \leftrightarrow (P_1^2 + T P_2^2 = 0).$$

Note: In a similar fashion: Let R be an integral domain and L be the language of rings extended by constant symbols. Consider R as an L-structure. Assume that D is in L such that the interpretation of D is not a square in R. Then any system of diophantine equations in R[D] is (effectively) equivalent to one diophantine equation. Moreover, the Diophantine problem for R[D] in language L is unsolvable if and only if the positive existential theory of R[D] as a structure of L is undecidable.

1.4 Pell's Equation

(Based on [22] and [27])

An especially notorious Diophantine equation,is the equation

$$x^2 - dy^2 = 1 \tag{1.4.1}$$

where d is a positive integer other than a perfect square.

The equation is referred to as *Pell's Equation*. Julia Robinson, Martin Davis and Yuri Matiyasevich used such an equation of the above form in solving some problems of the area.

Solutions with y =0 will be called trivial, all the rest non-trivial.

Over $\mathbb{Z}$ it can be proved that such an equation has always non-trivial solutions.

Important Observation: Let (a_1, b_1) and (a_2, b_2) be solutions of 1.4.1. Then the pair $(a_1, b_1) \oplus (a_2, b_2) = (a_1 a_2 + d b_1 b_2, a_1 b_2 + a_2 b_1)$ is also a solution of 1.4.1.

The set of points of Equation 1.4.1 forms an abelian group with the negative element of $\ominus(a, b)$ is $(a, -b)$ and the identity element of the group is (1,0). The group operation is given by algebraic functions of the coordinates of the involved points. Such group is called an Algebraic group.

Chapter 2

Analogues of Hilbert's Tenth Problem for Polynomial Rings and Quadratic Rings

2.1 The analogue of Hilbert's Tenth Problem for Polynomial Rings

[1]In August of 1977 Denef published his proof that the Diophantine problem for a ring of polynomials over an integral domain of characteristic zero is unsolvable.

The main theorem is:

Theorem 3 *Let R be an integral domain of characteristic zero; then the Diophantine problem for R[T] with coefficients in $\mathbb{Z}[T]$ is unsolvable. (R[T] denotes the ring of polynomials over R, in one variable T.)*

It is obvious 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.

Let R be a commutative ring with unity.

[1]for the full proof see [8]

Denef managed to find an existential definition of $\mathbb{Z}$ in R[T] using the solutions of an analogue of Pell's Equation. Particularly, he constructs a model of $\mathbb{Z}$ in R[T] by 'interpreting' the rational integers as certain polynomials in R[T]: to the integer n associate an polynomial y_n (see below).

2.1.1 The solutions of an analogue of Pell's equation

Denef considers the following analogue of Pell's equation

$$x^2 - (T^2 - 1)y^2 = 1 \tag{2.1.1}$$

over R[T].

Then, he defines two sequences $(x_n), (y_n), n = 0, 1, 2, \ldots$ of polynomials in $\mathbb{Z}[T]$, by setting

$$x_n + Uy_n = (T + U)^n. \tag{2.1.2}$$

where U is an element in the algebraic closure of R[T] satisfying

$$U^2 = T^2 - 1. \tag{2.1.3}$$

Observation: The relation (2.1.2) defines x_n and y_n uniquely seperating rational and irrational parts.

Denef proves the following Lemma for $char(R) \neq 2$.

Lemma 4 *The solutions of* (2.1.1) *over R[T] are given precisely by*

$$x = \pm x_n, \quad y = \pm y_n, \quad n = 0, 1, 2, \ldots$$

2.1.2 The final result

One defines the Diophantine relation $V \sim W$ means that the polynomials V and W in R[T] take the same value at T=1.

Then one observes the following relation of the polynomial y_n with the integer n : corresponds the solutions y_n with the naturals numbers as follows:

Lemma 5 *For $n = 0, 1, 2, \ldots$ we have $y_n \sim n$.*

Proof From (2.1.2) and (2.1.3) it follows

$$y_n = \sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i} (T^2 - 1)^{(i-1)/2} T^{n-i}. \tag{2.1.4}$$

and for T=1 we obtain that $y_n = n$. ∎

Then, one defines the 1-ary relation Imt(y) in $R[T]$ by

$$Imt(y) \leftrightarrow y \in R[T] \bigwedge \exists x \in R[T] : x^2 - (T^2 - 1)y^2 = 1$$

.

Lemma 6 *(i)The relation Imt(y) is diophantine over R[T] with coefficients in $\mathbb{Z}[T]$.*
(ii) If y satisfies Imt(y), then there exists an integer m such than $y \sim m$.
(iii) For every integer m there exists a polynomial y satisfying Imt(y) and $y \sim m$.

Proof They are followed immediately from Lemma 3 and Lemma 4. ∎

The proof of Theorem 1

Proof There exists an algorithm to find for any polynomial $P(z_1, \ldots, z_n)$ over $\mathbb{Z}$, a polynomial $P^*(Z_1, \ldots, Z_m)$ over $\mathbb{Z}[T]$ such that

$$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Z_1, \ldots, Z_m \in R[T] : P^*(Z_1, \ldots, Z_m) = 0 \tag{2.1.5}$$

One can construct a system of polynomial equations over R[T] with coefficients in $\mathbb{Z}[T]$ by taking the original equation together with and for each i = 1, . . . , n the relation $Imt(Z_i) \sim 0$. The new system of equations has a solution over R[T] if and only if $P(z_1, ..., z_n)$ has a solution in $\mathbb{Z}$. Also, the system of equations over R[T] with coefficients in $\mathbb{Z}[T]$ is equivalent to a single polynomial equation with coefficients in $\mathbb{Z}[T]$. Thus, one easily obtain a polynomial P^* satisfying (2.1.5).

Hence if the diophantine problem for R[T] with coefficients in $\mathbb{Z}[T]$ were solvable, then the diophantine problem for $\mathbb{Z}$ would be solvable which would contradict the negative answer to Hilbert's Tenth Problem given in [Matijasevich]. ■

2.2 The udecidability of a ring of polynomials over an integral domain of characteristic zero in the language L_T

[2]Pheidas and Zahidi in 1999 worked over a polynomial ring $A[t]$ (with A an integral domain) in the language

$$L_T = \{0, 1, +, \cdot, T\}$$

where the predicate $T[x]$ is interpreted as "$x \notin A$" (i.e. T is a symbol for the property "is not a constant").

They proved that the positive existential theory of a polynomial ring A with A an integral domain, in the language L_T, is undecidable.

Note that from above Denef's results, it is known that if A[t] is a polynomial ring over an integral domain A then its positive existential theory in the language

$$L = \{0, 1, t, +, \cdot\}$$

is undecidable.

Theorem 7 *The positive existential theory of a polynomial ring A, with A an integral domain, in language L_T, is undecidable.*

Let $a \in A[t]$, with a not a constant, that is $T[a]$. Pheidas and Zahidi worked with the solutions of the following analogue of Pell's equation

$$x^2 - (a^2 - 1)y^2 = 1 \tag{2.2.1}$$

Observations: $(a, 1)$ is a non constant solution of 2.2.1.
Consider $x_0 = 1$ and $y_0 = 0$ and working inductively setting $x_1 = a$ and $y_1 = 1$, implies that the pairs (x_n, y_n) for any positive integer n defined by

$$x_{n+1} = x_n a + (a^2 - 1)y_n$$

and

$$y_{n+1} = x_n + a y_n$$

[2]for the full proof see [23]

are solutions of 2.2.1.
Holds that $x_{-n} = x_n$ and $y_{-n} = -y_n$.

Therefore, the above equation has obviously the solutions

$$x = \pm x_n[a], \quad y = \pm y_n[a], \quad n = 0, 1, 2, \ldots$$

over $A[t]$ and the question is if there are more solutions than the knowns. The answer to the question is no as we can see from the following Lemma:

Lemma 8 *Assume that $a \in A[t]$ for which T[a] (i.e. a is non constant). Then the solution of 2.2.1 are given by $(x, y) = (\pm x_n[a], y_n[a])$ for $n = 0, 1, 2, \cdots$.*

Notes of the proof:

The proof is an induction on the degree of the polynomial x ('Method of descent'). Assume that (x, y) is a solution of 2.2.1 and $deg(x) = m$ the degree of the polynomial x. Assume that the lemma holds for the solutions (z,w) of 2.2.1 with $deg(z) < m$. Then they prove that (x, y) is of the form (x_k, y_k) for some integer k, which proves the lemma. The idea of the proof may be found in chapter 3 in the proof of Lemma 17.

From this (Lemma 6) one can give a diophantine definition of $\mathbb{Z}$ in a manner similar to that did Denef.

2.3 The analogue of Hilbert's Tenth Problem for Gaussian Ring

[3]In August of 1975 Denef proved that:

Theorem 9 *The analogue of Hilbert's Tenth problem for any quadratic ring is unsolvable.*

In this section, we will present the main Lemma of Denef for an imaginary quadratic ring, known as Gaussian Ring and denoted by $\mathbb{Z}[i]$. The elements of $\mathbb{Z}[i]$ are of the form $a+ib$ where a, b are in $\mathbb{Z}$ and called Gaussian integers.

The undecidability of the positive existential theory of the ring of Gaussian integers is reduced to the undecidability of the positive existential theory of the ring of rational integers.

So, it is sufficient to establish that the set of rational integers is Diophantine in the ring of Gaussian integers.

For this purpose, Denef uses results of [5] and he only has to show that the relation $x \in N$ is Diophantine over $Z[i]$ as follows:
Let d' be a square free rational integer

$$x, y \in \mathbb{Z}[i] \Longrightarrow (x = 0 \wedge y = 0 \Leftrightarrow x^2 - d'y^2 = 0)$$

. Denef combines the previous fact with
Lagrange's Theorem (: Every natural number is the sum of four squares of natural numbers.) and finally it is sufficient to prove the following Main Lemma:

Lemma 10 *There exists a (finite) system Σ of Diophantine equations in the unknowns $t, x, \ldots, s \in \mathbb{Z}[i]$ such that the following two conditions are satisfied:*

(1) If Σ has a solution $\langle t, x, \ldots, s\rangle$ in $\mathbb{Z}[i]$, then $t \in \mathbb{Z}$.

(2) If $k \in \mathbb{N}$ and $k \neq 0$, then Σ has a solution $\langle t, x, \ldots, s\rangle$ in $\mathbb{Z}[i]$ with $t = k^2$.

Denef constructs such a system of diophantine equations for any imaginary quadratic ring which is obviously suitable for $\mathbb{Z}[i]$.

[3]for the full proof see [7] and [19]

Chapter 3

An analogue of Hilbert's Tenth Problem for Exponential Sums

In this chapter we prove that the positive existential theory of the ring of exponential sums, in a rather natural language is undecidable. These results are new. Thanases Pheidas conjectured the strategy of proof and then we showed that it works.

3.1 Exponential Polynomials

In general, exponential polynomials are functions on fields, rings or abelian groups that take the form of polynomials in a variable and an exponential function. We define

Definition 11 *The ring of* ***exponential polynomials****, denoted by* $\mathbb{C}[z]^E$*, is the smallest ring that contains* $\mathbb{C}[z]$ *and* e^z *and is closed under the arithmetical operations and composition.*

The ring of exponential sums is a subring of the ring of exponential polynomials.

3.1.1 Exponential Sums

Define the set of **exponential sums**, denoted by $EXP(\mathbb{C})$, to be the the set of expressions

$$a = \alpha_0 + \alpha_1 e^{\mu_1 z} + \cdots + \alpha_N e^{\mu_N z} \tag{3.1.1}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_N \in \mathbb{C} \setminus \{0\}$ and $\mu_i \in \mathbb{C} \setminus \{0\}$; and μ_i are pairwise distinct.

Definition 12 *The ring of exponential sums, denoted by $EXP(\mathbb{C})$, is the ring of elements of exponential sums.*

3.2 Laurent Polynomials

We will use the Laurent polynomials so we list some basic relevant facts.

A Laurent polynomial in the variable z over a field $\mathbf{F}$ is an element of $\mathbf{F}[z, z^{-1}]$.
Obviously, a Laurent polynomial with coefficients in a field $\mathbf{F}$ is an expression of a unique form of

$$p = \sum_k p_k z^k, \quad p_k \in \mathbf{F}$$

where z is a formal variable, the summation index k is an integer (not necessarily positive) and only finitely many coefficients p_k are non-zero.

Later we will use the following fact:

Lemma 13 *If $\boldsymbol{F}$ is an integral domain, the **units** (i.e. divisors of 1) of the Laurent polynomial ring $\boldsymbol{F}[z, z^{-1}]$ have the form λz^k, where λ is a unit of $\boldsymbol{F}$ and k is an integer.*

Proof We observe that any non zero element of $\mathbf{F}[z, z^{-1}]$ can be written as $p(z)z^k$ where $p(z) \in \mathbf{F}[z]$ and $p(0) \neq 0$ and $k \in \mathbb{Z}$. It is obvious that for any z^k there exists z^{-k} in $\mathbf{F}[z, z^{-1}]$ such that $z^{-k}z^k = 1$. Thus, if $p(z)z^k$ is invertible, then $p(z)$ will be invertible. The inverse of $p(z)$ would be of the form $q(z)z^n$ where $q(z) \in \mathbf{F}[z]$ and $q(0) \neq 0$ and $n \in \mathbb{Z}$. So it is hold that

$$p(z)q(z)z^n = 1 \tag{3.2.1}$$

but for $z = 0$ the 3.2.1 is impossible except for $n = 0$. Therefore, $p(z)q(z) = 1$ in $\mathbf{F}[z]$ so we obtain that p(z) and q(z) belong to $\mathbf{F}$ and are both units of $\mathbf{F}$ so $p(z) = \lambda$ for $\lambda \in \mathbf{F}$. On the other hand, every element of the form λz^k where $\lambda \in F$ and $\lambda \neq 0$ is invertible in $\mathbf{F}[z, z^{-1}]$. ■

3.3 Undecidability of the existential theory of the ring of exponential sums

We consider the following language

$$L = \{+, \cdot, 0, 1, e^z\} \tag{3.3.1}$$

L contains symbols for the ring operations on $EXP(\mathbb{C})$ and constant-symbols for its elements 0, 1 and e^z. The only relation symbol of L is the usual one for equality (=). We consider $EXP(\mathbb{C})$ as a model of L, with the interpretation of the symbols.

We ask

Question 2 *Is the positive existential first order theory of $EXP(\mathbb{C})$, as a structure of the language L, decidable or undecidable?*

In other words, we ask whether there is an algorithm, which, given a finite set of polynomial equations, in many variables and with coefficients in $\mathbb{Z}[e^z]$, the algorithm replies (always correctly) to the question whether the equations have or do not have a common solution over $EXP(\mathbb{C})$.

In a recent unpublished paper P. D Aquino, Th. Pheidas and G. Terzo have had partial results in the direction of proving a negative answer (actually, a considerably more general statement) but they do it only pending on a number theoretic hypothesis. We provide a new proof, based partially on theirs, but using different tools ('Pell Equations' instead of Elliptic Curves). Our approach has been suggested by A. Macintyre. Our result may be considered as an analogue of Hilbert's Tenth Problem for this structure and as a step to answering the similar problem for the ring of exponential polynomials, which is still open. We prove:

Theorem 14 *The ring of gaussian integers $\mathbb{Z}[i]$ is positive existentially definable over $EXP(\mathbb{C})$, as an L-structure. Hence the positive existential theory of this structure is undecidable.*

In order to prove Theorem 14 we adapt techniques of [7] and we show the following Theorem

We consider the equation

$$(e^{2z}-1)y^2 = x^2 - 1 \tag{3.3.2}$$

where $x, y \in EXP(\mathbb{C})$.

Let (a_1, b_1) and (a_2, b_2) be solutions of 3.3.2. We define the law $\oplus$ by

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1a_2 + (e^{2z}-1)b_1b_2, a_1b_2 + a_2b_1) \tag{3.3.3}$$

The pair $(a, b) = (a_1, b_1) \oplus (a_2, b_2)$ is also a solution of 3.3.2.

It is easy to see that the law $\oplus$ makes the set of solutions of 3.3.2 into a commutative group. This follows from the observation that $\oplus$ corresponds to multiplication in $EXP[\mathbb{C}][\sqrt{e^{2z}-1}]$ as follows: (with notation as above)

$$(a_1 + \sqrt{e^{2z}-1}b_1) \cdot (a_2 + \sqrt{e^{2z}-1}b_2) = a + \sqrt{e^{2z}-1}b \ .$$

The 'negative' of the point (a, b) denoted $\ominus(a, b)$ is $(a, -b)$ and the identity element of the group is $(1, 0)$.
We denote by $\kappa \odot (a, b) = (a, b) \oplus \cdots \oplus (a, b)$. ($(a, b)$ added to itself by $\oplus$ κ times.)

Theorem 15 *The solutions of the equation*

$$(e^{2z}-1)y^2 = x^2 - 1 \tag{3.3.4}$$

where the unknowns x and y range over $EXP(\mathbb{C})$ are given by

$$(x, y) = \kappa \odot (\pm e^z, 1) \oplus \lambda \odot (\pm e^{-z}, \mathrm{i}e^{-z}). \tag{3.3.5}$$

The proof uses techniques of [38], [28] and [23].

3.3.1 An analogue of Pell's equation over $EXP(\mathbb{C})$

We would like to characterise all the solutions of Equation 3.3.2 over $EXP(\mathbb{C})$.

The algebraic structure of $EXP(\mathbb{C})$

We need some information about the algebraic structure of $EXP(\mathbb{C})$.
From now on we fix a solution (x, y) of Equation 3.3.2. Observe that, by the definition of $EXP(\mathbb{C})$, x and y lay in some ring of the form $R = \mathbb{C}[e^{\mu_1 z}, e^{-\mu_1 z}, \ldots, e^{\mu_k z}, e^{-\mu_k z}]$, where k is a natural number and each $\mu_i \in \mathbb{C}$. Fix such a ring. Without loss of generality we adopt the convention that

$$\mu_1 = 1.$$

(for reasons that will become clear later).

Let $\{1, \rho_2, \cdots, \rho_\ell\}$, where $\rho_i \in \mathbb{C}$, be a basis of the vector space which is generated by the μ_i over the field $\mathbb{Q}$. Then it is obvious that each μ_i is a linear combination over $\mathbb{Q}$ of $\{1, \rho_2, \cdots, \rho_\ell\}$.
Hence, for each μ_i there are integers n_{ij} and a positive integer N_i such that $\mu_i = \frac{1}{N_i}\sum_{j=1}^{\ell} n_{ij}\rho_j$. Taking N to be the least common multiple of the N_i we have that for each $i = 1, \ldots k$ we have $\mu_i = \frac{1}{N}\sum_{j=1}^{\ell} n'_{ij}\rho_j$ for some integers n'_{ij}. Then we observe that, for each i, $e^{\mu_i z}, e^{-\mu_i z} \in \mathbb{C}[e^z, e^{-z} \ldots, e^{\mu_k z}, e^{-\mu_k z}]$, hence $\mathbb{C}[e^z, e^{-z} \ldots, e^{\mu_k z}, e^{-\mu_k z}] \subseteq \mathbb{C}[e^{\frac{1}{N}z}, e^{-\frac{1}{N}z}, \ldots, e^{\frac{1}{N}\rho_\ell z}, e^{-\frac{1}{N}\rho_\ell z}]$.
Therefore,

$$x, y \in R = \mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, \ldots, e^{\frac{1}{N}\rho_\ell \cdot z}, e^{-\frac{1}{N}\rho_\ell \cdot z}]$$

.

Now we claim that the set $\{e^{\frac{1}{N}\cdot z}, \ldots, e^{\frac{1}{N}\rho_\ell \cdot z}\}$ is algebraically independent over $\mathbb{C}$. This follows from the fact that the set $\{\frac{1}{N}, \ldots, \frac{1}{N}\rho_\ell\}$ is linearly independent over $\mathbb{Q}$ and the following Lemma from [38]:

Lemma 16 *Assume that $\{\nu_1, \ldots, \nu_\ell\}$ is a set of complex numbers, which is linearly independent over $\mathbb{Q}$. Then the set of functions $\{e^{\nu_1 \cdot z}, \ldots, e^{\nu_\ell \cdot z}\}$ is algebraically independent over $\mathbb{C}$.*

Thus, the set of functions $\{e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, \ldots, e^{\frac{1}{N}\rho_\ell \cdot z}, e^{-\frac{1}{N}\rho_\ell \cdot z}\}$ is algebraically

independent over $\mathbb{C}$. Set

$$\begin{aligned} Z &= e^{\frac{1}{N}z} \\ t_2 &= e^{\frac{1}{N}\rho_2 \cdot z} \\ &\cdots \\ t_\ell &= e^{\frac{1}{N}\rho_\ell \cdot z} \end{aligned} \quad . \tag{3.3.6}$$

Then $x, y \in \mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}, t_2, t_2^{-1}, \ldots t_\ell, t_\ell^{-1}]$ and the elements $t_2, \ldots t_\ell$ may be considered as variables over the ring $\mathbb{C}[e^{\frac{1}{N}\cdot z}, e^{-\frac{1}{N}\cdot z}]$. (Recall that the meaning of the phrase $t_2, \cdots, t_\ell$ are variables over an integral domain A means by definition that $t_2, \cdots, t_\ell$ are algebraically independent over the quotient field of A.)

Therefore, Equation 3.3.2 becomes

$$(Z^{2N} - 1)y^2 = x^2 - 1 \tag{3.3.7}$$

over the ring

$$\mathbb{C}[Z, Z^{-1}, t_2, t_2^{-1}, \ldots, t_\ell, t_\ell^{-1}] \ .$$

At a later stage we will see that any such solution has to be over $\mathbb{C}[Z^N, Z^{-N}]$. (that is, the variables $t_2, \cdots, t_\ell$ do not occur in x, y and each of x, y is a function over $\mathbb{C}$ only of Z^N).

First we prove that x, y are in $\mathbb{C}[Z, Z^{-1}]$.

Lemma 17 *Let A be an integral domain, containing $\mathbb{C}[Z, Z^{-1}]$, such that $Z^{2N} - 1$ is not a square in A. Let t be a variable and let (x, y) be a solution of 3.3.2 with $x, y \in A[t, t^{-1}]$. Then $x, y \in A$.*

Proof By factoring $x^2 - (Z^{2N} - 1)y^2 = 1$ over the ring $R[t, t^{-1}]$, where $R = A[\sqrt{Z^{2N} - 1}]$ we obtain that

$$(x - \sqrt{Z^{2N} - 1}y)(x + \sqrt{Z^{2N} - 1}y) = 1$$

so $(x - \sqrt{Z^{2N} - 1}y)$ and $(x + \sqrt{Z^{2N} - 1}y)$ are both divisors of 1 in $R[t, t^{-1}]$. So they are units of $R[t, t^{-1}]$ and by 13 they are of the form

$$x + \sqrt{Z^{2N} - 1}y = \lambda t^{\kappa} \tag{3.3.8}$$
$$x - \sqrt{Z^{2N} - 1}y = \lambda^{-1} t^{-\kappa} \tag{3.3.9}$$

where λ is a unit in $A[\sqrt{Z^{2N} - 1}]$ and $\kappa \in \mathbb{Z}$.

We add the 3.3.8 and 3.3.9 equations and solving for x we obtain that

$$x = \frac{\lambda t^{\kappa} + \lambda^{-1} t^{-\kappa}}{2} \tag{3.3.10}$$

Assume that $\kappa \neq 0$. We will prove this leads to a contradiction.
By hypothesis $x \in A[t, t^{-1}]$. Considering x as an element of $A[\sqrt{Z^{2N} - 1}][t, t^{-1}]$, it is written uniquely as a sum of terms of the form at^n, for pairwise distinct n and with $a \in A[\sqrt{Z^{2N} - 1}] \setminus \{0\}$. Since $\kappa \neq -\kappa$ we obtain that $\lambda, \lambda^{-1} \in A$.

Now we subtract the 3.3.9 by 3.3.8 equation and solve for y to obtain

$$y = \frac{\lambda t^{\kappa} - \lambda^{-1} t^{\kappa}}{2\sqrt{Z^{2N} - 1}}$$

By hypothesis $y \in A[t, t^{-1}]$. Working in a way similar to that we worked with x we obtain

$$\frac{\lambda}{\sqrt{Z^{2N} - 1}}, \frac{\lambda}{\sqrt{Z^{2N} - 1}} \in A$$

which, since $\sqrt{Z^{2N} - 1} \notin A$, contradicts the fact that λ is a unit in A. Therefore $\kappa = 0$ and consequently $x, y \in A$. ∎

By the Lemma, through an easy induction on the number of variables t_i, $x, y \in \mathbb{C}[Z, Z^{-1}]$.

Corollary 18 *Let (x, y) be as above then $x, y \in \mathbb{C}[e^{\frac{1}{N} \cdot z}, e^{-\frac{1}{N} \cdot z}]$.*

3.3.2 The solutions of the 'generalised Pell's Equation' 3.3.7 over $\mathbb{C}[Z, Z^{-1}]$

We will find explicity the solutions of Equation 3.3.7.

Consider Equation

$$(T^2-1)y^2 = x^2 - 1 \tag{3.3.11}$$

with $x, y \in \mathbb{C}[T, T^{-1}]$.

We know from Lemma 2 in Subsection 2.1.1 that the solutions of 3.3.11 over $\mathbb{C}[T]$ are given by $(x, y) = (\pm x_n, y_n)$ where, for $n \in \mathbb{N}$

$$(x_n, y_n) = (Tx_{n-1} - (1-T^2)y_{n-1}, Ty_{n-1} + x_{n-1}),\ (x_1, y_1) = (T, 1) \tag{3.3.12}$$

and for $n \in \mathbb{Z}$ $(x_{-n}, y_{-n}) = (x_n, -y_n)$.

Observe that (3.3.11) is written equivalently as

$$(T^{-2}-1)[\mathrm{i}Ty]^2 = x^2 - 1 \tag{3.3.13}$$

hence, by the above, has as solutions over $\mathbb{C}[T^{-1}]$ the pairs $(x, y) = (\pm\bar{x}_n, \bar{y}_n)$, where

$$(\bar{x}_n, \bar{y}_n) = (x_n(T^{-1}), -\mathrm{i}T^{-1}y_n(T^{-1}))\ . \tag{3.3.14}$$

Obviously

$$(\bar{x}_1, \bar{y}_1) = (T^{-1}, -\mathrm{i}T^{-1})\ .$$

Now we are interested in finding the solutions (x, y) over $\mathbb{C}[Z, Z^{-1}]$ of Equation 3.3.7. By setting $T = Z^N$ we see that the solutions of 3.3.11 which we have over $\mathbb{C}[T]$ and over $\mathbb{C}[T^{-1}]$ remain solutions of 3.3.11 over $\mathbb{C}[T, T^{-1}]$ and therefore 3.3.7 has the solutions

$$(\pm x, y) = (\pm x_\kappa(Z^N), y_\kappa(Z^N)) = (Z^N x_{\kappa-1} - (1-Z^{2N})y_{\kappa-1}, Z^N y_{\kappa-1} + x_{\kappa-1}),$$

with $(x_1, y_1) = (Z^N, 1)$. (which are over $\mathbb{C}\left[Z^N\right]$) and the solutions

$$(\pm x, y) = (\bar{x}_\lambda(Z^N), \bar{y}_\lambda(Z^N)) = (x_\lambda[Z^{-N}], -\mathrm{i}Z^{-N}y_\lambda[Z^{-N}]),\ (\bar{x}_1, \bar{y}_1) = (Z^{-N}, -\mathrm{i}Z^{-N})\ .$$

(which are over $\mathbb{C}[Z^{-N}]$). Therefore Equation 3.3.7 has as solutions the following

$$(\pm x, y) = (\pm x_\kappa(Z^N), y_\kappa(Z^N)) \oplus (\bar{x}_\lambda(Z^N), \bar{y}_\lambda(Z^N)) \tag{3.3.15}$$

over $\mathbb{C}[Z, Z^{-1}]$ (where the law $\oplus$ is defined in section .

We will now see that there are no solutions other than the above of Equation (3.3.7) over $\mathbb{C}[Z, Z^{-1}]$, other than those of (3.3.15).

Lemma 19 *The solutions of Equation 3.3.7 over $\mathbb{C}[Z, Z^{-1}]$ are given by $(\pm x, y) = (\pm x_{\kappa,\lambda}, y_{\kappa,\lambda}) = (x_\kappa[Z^N], y_\kappa[Z^N]) \oplus (x_\lambda[Z^{-N}], -\mathrm{i}Z^{-N} y_\lambda[Z^{-N}])$, for $\kappa, \lambda \in \mathbb{Z}$ (the $\pm$ sign is read 'plus or minus').*

Proof Let (x, y) be a solution of 3.3.7, with $x, y \in \mathbb{C}[Z, Z^{-1}]$, with $x \notin \mathbb{C}$.

If $u \in \mathbb{C}[Z, Z^{-1}] \setminus (\mathbb{C}[Z] \cup \mathbb{C}[Z^{-1}])$ then we write it as

$$u = \sum_{k=-r}^{\ell} u_k Z^k, \quad u_k \in \mathbb{C}$$

with r and ℓ non-negative integers and $u_{-r} \cdot u_\ell \neq 0$. We call r the *negative degree* and ℓ the *positive degree* of u. We write (*negative degree of* u)=$\deg_-(u) = r$ and (*positive degree of* u)=$\deg_+(u) = \ell$. If $u \in \mathbb{C}[Z^{-1}]$ and $u_0 = 0$ then we write $deg_+(u) = -\infty$. If $u \in \mathbb{C}[Z]$ and $u_0 = 0$ then we write $deg_-(u) = -\infty$. We adopt the convention that for any real number m we have $-\infty < m$.

Notice that the positive and negative degrees have the following properties:

1. If both $\deg_+(a)$, $\deg_+(b)$ are ≥ 0, then $\deg_+(a \cdot b) = \deg_+(a) + \deg_+(b)$. If both $\deg_-(a)$ and $\deg_-(b)$ are ≥ 0 then $\deg_-(a \cdot b) = \deg_-(a) + \deg_-(b)$.

2. If any of $\deg_+(a)$ and $\deg_+(b)$ is $\neq -\infty$ (respectively, any of $\deg_+(a)$ and $\deg_+(b)$ is $\neq -\infty$) then $\deg_+(a + b) \leq \max\{\deg_+(a), \deg_+(b)\}$ (resp. $\deg_-(a + b) \leq \max\{\deg_-(a), \deg_-(b)\}$. Under the additional hypothesis that $\deg_+(a) \neq \deg_+(b)$ (respectively $\deg_-(a) \neq \deg_-(b)$) then we have that equality holds.

Let the positive degree of x be k, with $k \in \mathbb{N} \cup \{0\} \cup \{-\infty\}$.

We define

$$(\tilde{x}, \tilde{y}) = (x, y) \oplus (x_1[Z^N], y_1[Z^N]) \tag{3.3.16}$$

and

$$(\underline{x},\underline{y}) = (x,y) \ominus (x_1[Z^N], y_1[Z^N]) \tag{3.3.17}$$

The way that we will prove the Lemma is the following:

Assume that $deg_+(x) \geq N$. We will prove that one of $\deg_+(\tilde{x})$ and $\deg_+(\underline{x})$ is less than $\deg_+(x)$. Iterating the procedure we will have established that there is a $\kappa \in \mathbb{Z}$ such that, setting $(\dot{x},\dot{y}) = (x,y) \ominus (\kappa \odot (Z^N, 1))$, we have $\deg_+(\dot{x}) < N$. Next we will prove that the only solutions $(\dot{x},\dot{y})$ with $\deg_+(\dot{x}) < N$ are over $\mathbb{C}[Z^{-1}]$ (in this case the Lemma follows from Lemma 2 in Subsection 2.1.1). Then the Lemma will follow by induction on k.

By the definition of the law $\oplus$ we have

$$\tilde{x} = Z^N x + (Z^{2N} - 1)y \tag{3.3.18}$$
$$\tilde{y} = x + yZ^N \tag{3.3.19}$$
$$\underline{x} = Z^N x - (Z^{2N} - 1)y \tag{3.3.20}$$
$$\underline{y} = -x + yZ^N \ . \tag{3.3.21}$$

We want to estimate the quantities $\deg_+(\tilde{x})$ and $\deg_+(\underline{x})$ and show that,if $\deg_+(x) > 0$ one them is less than $\deg_+(x)$. We have from 3.3.18 and 3.3.20:

$$\tilde{x} \cdot \underline{x} = x^2 Z^{2N} - (Z^{2N} - 1)^2 y^2 = \tag{3.3.22}$$
$$x^2 Z^{2N} - (1 - Z^{2N})(1 - x^2) = x^2 Z^{2N} - (1 - x^2 - Z^{2N} + x^2 Z^{2N}) =$$
$$x^2 + Z^{2N} - 1$$

and

$$\tilde{x} + \underline{x} = 2xZ^N \tag{3.3.23}$$

and

$$\tilde{x} - \underline{x} = 2(Z^{2N} - 1)y \tag{3.3.24}$$

At this point we observe that if $\deg_+(x) \leq 0$ then $x \in \mathbb{C}[Z^{-1}]$ so we know all the solutions of 3.3.7 from Lemma 2 in Subsection 2.1.1 and they are of the required form.

Therefore from now on we assume that $deg_+(x) > 0$.

We notice that if one of $deg_+(\tilde{x})$ or $deg_+(\underline{x})$ is $-\infty$ or 0 then the Lemma follows from Lemma 8subsection.

Therefore, from now on we assume that $\deg_+(\tilde{x}) > 0$ and $deg_+(\underline{x}) > 0$.

We also observe that if $\deg_+(\tilde{x}) = \deg_+(\underline{x})$ then Relation 3.3.22 implies

$$2\deg_+(\tilde{x}) = \deg_+(x^2 + Z^{2N} - 1) \leq 2\max\{\deg_+(x), N\}$$

and Relation 3.3.23 implies

$$\deg_+(\tilde{x}) \geq \deg_+(x) + N$$

which, combined, give

$$\max\{\deg_+(x), N\} \geq \deg_+(\tilde{x}) > \deg_+(x) \text{ and } N$$

which is impossible since $\deg_+(x) > 0$ so $\deg_+(\tilde{x}) \neq \deg_+(\underline{x})$.

Let us now assume that $\deg_+(\underline{x}) > \deg_+(\tilde{x})$. (We leave it to the reader that one obtains the same results if one assumes that $\deg_+(\underline{x}) < \deg_+(\tilde{x})$.)

Assume that $\deg_+(x) > N$. Then, by 3.3.22 we have

$$\deg_+(\tilde{x}) + \deg_+(\underline{x}) = \deg_+(\tilde{x} \cdot \underline{x}) = \deg_+(x^2 + Z^{2N} - 1) = 2\deg_+(x) \ .$$

By 3.3.23,

$$\max\{\deg_+(\tilde{x}), \deg_+(\underline{x})\} \geq \deg_+(x) + \deg_+(Z^N) > \deg_+(x) \ .$$

By the two latter relations we obtain

$$\min\{\deg_+(\tilde{x}), \deg_+(\underline{x})\} < \deg_+(x)$$

.
Therefore, $\deg_+(x) > \deg_+(\tilde{x})$.

Assume now that $\deg_+(x) < N$.

From relation 3.3.24 we obtain

$$deg_+(\underline{x}) = 2N + deg_+(y) \tag{3.3.25}$$

From relation 3.3.22 we obtain

$$\deg_+(\underline{x}) + \deg_+(\tilde{x}) = 2N \tag{3.3.26}$$

If $deg_+(y) > 0$ then subtracting the above we have

$$deg_+(\tilde{x}) = -deg_+(y)$$

which is impossible.

If $deg_+(y) = -\infty$ then 3.3.24 implies that $deg_+(\underline{x}) = deg_+(\tilde{x})$ which contradicts our assumption that $deg_+(\underline{x}) > deg_+(\tilde{x})$.

If $deg_+(y) = 0$ then 3.3.25 implies that $deg_+(\underline{x}) = 2N$ and from relation 3.3.26 we obtain that $deg_+(\tilde{x}) = 0$.
Thus, $\deg_+(x) > \deg_+(\tilde{x})$.

Finally assume that $\deg_+(x) = N$. Then, by 3.3.22 we have

$$\deg_+(\tilde{x}) + \deg_+(\underline{x}) = \deg_+(\tilde{x} \cdot \underline{x}) = \deg_+(x^2 + Z^{2N} - 1) \leq 2 \deg_+(x) \ .$$

Therefore, we obtain again that
$\deg_+(x) > \deg_+(\tilde{x})$.

■

As a result, the solutions of Equation (3.3.2) over EXP($\mathbb{C}$) are given by

$$k \odot (\pm e^z, 1) \oplus \lambda \odot (\pm e^{-z}, \mathrm{i}e^{-z}) \tag{3.3.27}$$

where

$$\kappa \odot (e^z, 1) = (x_\kappa[e^z], y_\kappa[e^z])$$

and

$$\lambda \odot (e^z, 1) = (x_\lambda[e^{-z}], -\mathrm{i}e^{-z} \cdot y_\lambda[e^{-z}])$$

which proves Theorem 15.

3.3.3 The proof of Theorem 14

As we said above, by adapting techniques of [7] we will prove our main result, Theorem 14.

Throughout this section we write $V \sim U$ to denote that the Laurent polynomials V and U in $\mathbb{C}[Z, Z^{-1}]$ take the same value at $Z^N = 1$.

Lemma 20 *We have $y_{\kappa,\lambda} \sim \kappa - i\lambda$, for $\kappa, \lambda = 0, \pm 1, \pm 2, \ldots$*

Proof Recall that for for $\kappa = 0, \pm 1, \pm 2, \ldots$ we have

$$x_\kappa|_{Z^N=1} = 1$$

and

$$y_\kappa|_{Z^N=1} = \kappa$$

. Then for $\lambda = 0, \pm 1, \pm 2, \ldots$ we have

$$x_\lambda|_{Z^{-N}=1} = 1$$

and

$$y_\lambda|_{Z^{-N}=1} = -i\lambda$$

. By the definition of the law $\oplus$ we have $y_{\kappa,\lambda}[1] = x_\lambda[1]y_\kappa[1] + x_\kappa[1]y_\lambda[1]$

Thus we obtain

$$y_{\kappa,\lambda|Z^N=1,Z^{-N}=1} = \kappa - i\lambda$$

. ■

Notice now that the relation $W \sim 0$ is diophantine over $\mathbb{C}[Z, Z^{-1}]$ with coefficients in $\mathbb{Z}[Z, Z^{-1}]$:

$$W \sim 0 \text{ if and only if } \exists X \in \mathbb{C}[Z, Z^{-1}] : W = (Z-1)X \ .$$

Let us define the 1-ary relation Imt(Y) in $\mathbb{C}[Z, Z^{-1}]$ by

$$\text{Imt}(Y) \leftrightarrow Y \in \mathbb{C}[Z, Z^{-1}] \bigwedge \exists X \in \mathbb{C}[Z, Z^{-1}] : X^2 - (Z^{2N} - 1)Y^2 = 1 \ .$$

Now from the above two Lemmas we obtain the following:

Lemma 21 *We have :*

i *The relation Imt(y) is diophantine over $\mathbb{C}[Z, Z^{-1}]$ with coefficients in $\mathbb{Z}[Z, Z^{-1}]$.*

ii *If y satisfies Imt(y), then there exist rational integers κ, λ such that $y \sim \kappa - i\lambda$.*

iii *For any rational integers κ, λ there exists a Laurent polynomial y satisfying Imt(y) and $y \sim \kappa - i\lambda$.*

Proof of Theorem 14
Proof

By Lemma 19, we have

$$z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \Leftrightarrow \exists Z_1, \ldots, Z_n \in \mathbb{C}[Z, Z^{-1}] : (Imt(Z_1) \wedge \cdots \wedge Imt(Z_n) \wedge P(Z_1, \ldots \tag{3.3.28}$$

Since $\sim$ and Imt are diophantine (by Lemma 19 i) over $\mathbb{C}[Z, Z^{-1}]$ with coefficients in $\mathbb{Z}[Z, Z^{-1}]$, substituting each of occurrences of any of this relation in 3.3.28 we obtain a polynomial P and each Imt(Z_i) is substituted by

$$\exists X_i \in \mathbb{C}[Z, Z^{-1}] : X_i^2 - (Z^{2N} - 1)Z_i^2 = 1$$

Considering now the note 1.3, we easily obtain a polynomial P^* satisfying the following: There exists an algorithm to find, for any polynomial $P(z_1, \ldots, z_n)$ over $\mathbb{Z}[i]$, a polynomial $P^*(Z_1, \ldots, Z_m)$ over $\mathbb{Z}[Z, Z^{-1}]$ such that

$$\exists z_1, \ldots, z_n \in \mathbb{Z}[i] : P(z_1, \ldots, z_n) = 0 \text{ if and only if } \exists Z_1, \ldots, Z_m \in \mathbb{C}[Z, Z^{-1}] : P^*(Z_1, \ldots, Z_m) = 0 \tag{3.3.29}$$

If there were an algorithm to decide the correctness of sentences as the right -hand side of the last line then the same algorithm would decide the existence of a solution of $P = 0$ in $\mathbb{Z}[i]$, which contradicts the negative answer to the analogue of Hilbert's Tenth Problem given in [7]. ■

Bibliography

[1] A.Baker, *A concise introduction to the Theory of Numbers*,Cambridge University Press (1984)

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[3] G. Cherlin, *Model theoretic Algebra*, Lecture Notes Math. **521** (1976), Springer.

[4] P. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. **22** (1969),131-151.

[5] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973).

[6] F. Delon, *Indécidabilité de la théorie des anneaux de séries formelles à plusieurs variables*, Fund. Math. **CXII** (1981), 215-229.

[7] J.Denef, *Hilbert's Tenth Problem for Quadratic Rings*,Transactions of the American Mathematical Society , **48**(1975), 214-220

[8] J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society, **242**(1978),391-399.

[9] J. Denef, *The diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78, North Holland (1984), 131-145.

[10] J. Denef and L. Lipshitz, *Power series solutions of algebraic differential equations*, Math. Ann. **267** (1980), 1-28.

[11] M. Greenberg, Strictly local solutions of diophantine equations, Pacific J.Math., **51** (1974), 143-153.

[12] K. Kim and F. Roush, *An approach to rational diophantine undecidability*, Proc. Asian Math. Conf., World Scient. Press, Singapore (1992), 242-257.

[13] S. Kochen, *The model theory of local fields*, Lecture Notes in Math. **499** (1975) (Proc. Internat. Summer Inst. and Logic Colloq., Kiel, 1974,), 384–425, Springer.

[14] J. Koenigsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, arXiv:1011.3424 [math.NT], (2010).

[15] J. Koenigsmann, *Undecidability in Number Theory*, arXiv:1309.0441 [math.NT], (2013).

[16] S. Lang, *Algebra*, Springer

[17] L. Lipshitz and T. Pheidas, An analogue of Hilbert's Tenth Problem for p-adic entire functions, The Journal of Symbolic Logic, 60-4 (1995), 1301-1309

[18] Y. Matijasevich, *Enumerable sets are diophantine*, Doklady Akademii Nauka SSSR, **191**(1970), 272-282.

[19] Y. Matjiasevich, *Hilbert's Tenth Problem*, The MIT press (1993).

[20] B. Mazur, *The topology of rational points*, Journal of Experimental Mathematics, **1-1** (1992), 35-45.

[21] B. Mazur, *Questions of decidability and undecidability in number theory*, The Journal of Symbolic Logic, **59-2** (1994), 353-371.

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

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

[24] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics, **270** (2000), 49-106.

[25] T. Pheidas and K. Zahidi, *Analogues of Hilbert's tenth problem*, Model theory with Applications to Algebra and Analysis Vol. 2 (Eds. Zoe Chatzidakis, Dugald Macpherson, Anand Pillay, Alex Wilkie), London Math Soc. Lecture Note Series Nr 250, Cambridge Univ Press, 2008.

[26] T.Pheidas-K.Zahidi, *Decision problems in Algebra and analogues of Hilbert's Tenth Problem*

[27] T.Pheidas, *Methods of proving a negative answer to analogues of Hilbert's Tenth Problem*

[28] T. Pheidas,P. D'Aquino,G. Terzo, *Undecidability of the diophantine theory of exponential sums*, manuscript.

[29] B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, obtainable from http://www-math.mit.edu/ poonen/papers/aws2003.pdf

[30] R. Robinson, *Undecidable rings* , Trans. Amer. Math. Soc. **70** (1951), 137.

[31] L. Rubel, *An essay on diophantine equations for analytic functions*, Expositiones Mathematicae, **14**(1995),81-92.

[32] A. Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions of characteristic zero*, Journal of Number Theory, **40-2** (1992), 218-236.

[33] A. Shlapentokh, *Hilbert's tenth problem over number fields, a survey*, Contemporary Mathematics, **270** (2000), 107-137.

[34] A. Shlapentokh, *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*, Cambridge University Press, (2007).

[35] A. Seidenberg, *A new decision method for elementary algebra*, Annals of Mathematics, Second Series, **60-2** (1954), 365-374.

[36] A. Seidenberg, *Constructions in Algebra*, Transactions AMS, **197** (1974), 273-313.

[37] A. Tarski, *A decision method for elementary algebra and geometry*, RAND Corporation, Santa Monica, Calif. (1948).

[38] L. Van Den Dries, *Exponential rings, exponential polynomials and exponential functions*, Pacific Journal of Mathematics, (1) **113**(1984), 51-66.

[39] L. van den Dries, *A specialization theorem for analytic functions on compact sets*, Proceedings Koninklijke Nederlandse Academie van Weteschappen (A), **85-4** (1988),391-396.

[40] L. van den Dries, *Analytic Ax-Kochen-Ersov theorems*, Proceedings of the International Conference on Algebra, Part **3** (Novosibirsk, 1989), 379–398, Contemp. Math. **131**, Amer. Math. Soc., Providence, RI, 1992.

[41] X. Vidaux, *An analogue of Hilbert's 10th problem for fields of meromorphic functions over non-Archimedean valued fields*, Journal of Number Theory, **101** (2003), 48-73.

[42] A.Weil, *Basic Number Theory*,Springer ,(1995)

[43] V. Weispfenning, *Quantifier elimination and decision procedures for valued fields* in Models and Sets, Lect. Notes Math. **1103**, Springer-Verlag (1984), 419-472.