Επεκτάσεις του Δέκατου Προβλήματος του Hilbert:Οι προσπάθειες για τους ρητούς

Ορέστης Ράπτης

Μεταπτυχιακό Πρόγραμμα
στη Λογική και Θεωρία Αλγορίθμων και
Υπολογισμού

$\mu\prod\lambda\forall$

Σεπτέμβριος 2002

1 Πρόλογος

Η διπλωματική αυτή εργασία αποτελεί μία προσπάθεια παρουσίασης των βημάτων που έχουν γίνει για την επίλυση της σημαντικότερης ίσως επέκτασης του Δέκατου Προβλήματος του Hilbert, εκείνης που αφορά την επιλυσιμότητα τυχούσης διοφαντικής εξίσωσης στους ρητούς.

Συγκεκριμένα το μεγαλύτερο τμήμα της βασίζεται στα όσα έχει κάνει ο Θανάσης Φειδάς προς την κατεύθυνση της αρνητικής λύσης αυτού αλλά και παραπλήσιων προβλημάτων. Επίσης παρουσιάζεται η αντίθετη κατεύθυνση, η οποία σχετίζεται με την ισχύ μιας εικασίας του Mazur, και γίνεται μία σύντομη επισκόπηση άλλων επεκτάσεων του Δέκατου Προβλήματος του Hilbert.

Θα ήθελα να ευχαριστήσω το διευθυντή του Μεταπτυχιακού Προγράμματος καθηγητή κ. Γιάννη Μοσχοβάκη και τα άλλα δύο μέλη της τριμελούς επιτροπής για τη διπλωματική μου εργασία καθηγητές κ.κ. Κ.Δημητρακόπουλο και Μ.Μυτιληναίο.

2 Εισαγωγή

Το 1900 ο David Hilbert,προετοιμάζοντας την ομιλία του στο Δεύτερο Παγκόσμιο Συνέδριο Μαθηματικών που θα γινόταν στο Παρίσι, συνέταξε έναν κατάλογο 23 ανοικτών προβλημάτων που πίστευε ότι θα έδειχναν τις σημαντικότερες ερευνητικές κατευθύνσεις για το μέλλον της επιστήμης του.Ένα από τα προβλήματα που δεν παρουσίασε στο συνέδριο αν και συμπεριέλαβε στον κατάλογό του ήταν και το υπ'αριθμόν δέκα.Το πρόβλημα,που έγινε γνωστό ως ¨Δέκατο Πρόβλημα του Hilbert¨(στο εξής ΔΠΧ) ήταν διατυπωμένο ως εξής:

¨10.ΑΠΟΦΑΝΣΗ ΠΕΡΙ ΤΗΣ ΕΠΙΛΥΣΙΜΟΤΗΤΑΣ ΜΙΑΣ ΔΙΟΦΑΝΤΙΚΗΣ ΕΞΙΣΩΣΗΣ. Δοθείσης μιας διοφαντικής εξίσωσης με οποιοδήποτε αριθμό μεταβλητών και ακέραιους συντελεστές:να βρεθεί μέθοδος με την οποία να μπορεί κανείς σε πεπερασμένο αριθμό βημάτων να αποφανθεί για το αν η εξίσωση έχει λύση στους ακέραιους¨

Από τη διατύπωση συμπεραίνει κανείς ότι κατά πάσα πιθανότητα οHilbertδεν είχε σκεφτεί ότι θα μπορούσε να μην υπάρχει μια τέτοια μέθοδος.[1]

Ο λόγος είναι ότι μέχρι τότε πολλές τέτοιες μέθοδοι για διάφορα προβλήματα είχαν εφευρεθεί από μαθηματικούς(από τον Ευκλείδη μέχρι το Sturm)και κάθε φορά η μαθηματική κοινότητα τις αναγνώριζε ως τέτοιες πέραν πάσης αμφιβολίας.Έτσι,η έννοια της ¨μεθόδου¨ δεν είχε γίνει ακόμα μαθηματικό αντικείμενο.Χρειάστηκαν περίπου 35 χρόνια από εκείνη την ομιλία του Hilbert και η δουλειά,μεταξύ άλλων, των Kurt Gödel, Alonzo Church, Emil Post, Alan Turing, Stephen Cole Kleene, ώστε οι μέθοδοι αυτές,που επικράτησε να λέγονται ¨αλγόριθμοι¨να μελετηθούν και πρώτα απ'όλα να υπάρξει ένας σαφής και κοινά αποδεκτός ορισμός για το ποιές συναρτήσεις (από τους φυσικούς στους φυσικούς)είναι υπολογίσιμες από αλγορίθμους και,επομένως,ποιές όχι.Χρειάστηκαν άλλα 35 χρόνια και η δουλειά μεταξύ άλλων των Martin Davis, Julia Robinson, Hilary Putnam,για να ολοκληρωθεί από τον Yuri Matiyasevich το 1970 η απόδειξη του ότι δεν υπάρχει αλγόριθμος που να πληροί τις απαιτήσεις του Hilbert.Για να εξηγήσουμε λίγο καλύτερα την ακριβή απάντηση στο ΔΠΧ θα χρειαστούμε κάποιους ορισμούς.

Ορισμός 1 *Παραμετρική οικογένεια διοφαντικών εξισώσεων είναι μια εξίσωση της μορφής* $P(a_1, a_2, ..., a_n, x_1, x_2, ...x_m) = 0$,*όπου* P *ένα πολυώνυμο με ακέραιους συντελεστές οι μεταβλητές του οποίου χωρίζονται σε παραμέτρους(οι* $a_1, a_2, ..., a_n$*) και αγνώστους(οι* $x_1, x_2, ...x_m$*).*

Έτσι,για κάθε επιλογή τιμών για τις παραμέτρους$a_1, a_2, ..., a_n$ παίρνουμε μια διαφορετική εξίσωση με m μεταβλητές που μπορεί να έχει ή να μην έχει λύση.

Ορισμός 2 *Ένα σύνολο* Δ n*-άδων ονομάζεται διοφαντικό όταν υπάρχει μια παραμετρική οικογένεια διοφαντικών εξισώσεων* $P(a_1, ..., a_n, x_1, ...x_m) = 0$ *ώστε*

[1] Εκείνη την εποχή είχαν ήδη κάνει την εμφάνισή τους οι ιδέες τουCantor(για τις οποίες ο Hilbert είχε δείξει τόσο ενδιαφέρον ώστε ως πρώτο στη λίστα του πρόβλημα να θέσει το Πρόβλημα του Συνεχούς)και ήταν γνωστό ότι υπήρχαν σύνολα με υπεραριθμήσιμα το πλήθος στοιχεία·έτσι,εφόσον οι ¨μέθοδοι¨,ότι κι αν ήταν αυτές,θα έπρεπε να είναι πεπερασμένες ακολουθίες συμβόλων,άρα αριθμήσιμές το πλήθος,τρόπον τινά ήδη ήταν εν δυνάμει γνωστό πως υπήρχαν αντικείμενα μη περιγράψιμα με κάποια ¨μέθοδο¨.Δεν μπορεί λοιπόν να αποκλειστεί η εκδοχή ο Hilbert να είχε σκεφτεί κάτι τέτοιο,να είχε δηλαδη σκεφτεί πως πιθανόν να μην υπήρχε η ζητούμενη μέθοδος,και να μην το πίστευε.

$$\langle a_1, ..., a_n \rangle \in \Delta \iff \exists x_1, ..., x_m P(a_1, ..., a_n, x_1, ..., x_m) = 0 \tag{1}$$

Κάποιες βασικές ιδιότητες των διοφαντικών συνόλων έπονται σχεδόν κατέυθείαν από τον ορισμό τους.Π.χ. η ένωση καθώς και η τομή δύο διοφαντικών συνόλων Δ_1, Δ_2 είναι διοφαντικό σύνολο αφού αν

$\langle a_1, ..., a_n \rangle \in \Delta_1 \iff \exists x_1, ..., x_m P_1(a_1, ..., a_n, x_1, ...x_m) = 0$ και
$\langle a_1, ..., a_n \rangle \in \Delta_2 \iff \exists y_1, ..., y_m P_2(a_1, ..., a_n, x_1, ...y_m) = 0$ τότε
$\langle a_1, ..., a_n \rangle \in \Delta_1 \bigcup \Delta_2 \iff$
$\exists x_1, ..., x_m, y_1, ..., y_m P_1(a_1, ..., a_n, x_1, ...x_m) P_2(a_1, ..., a_n, y_1, ...y_m) = 0$ και
$\langle a_1, ..., a_n \rangle \in \Delta_1 \bigcap \Delta_2 \iff$
$\exists x_1, ..., x_m, y_1, ..., y_m P_1(a_1, ..., a_n, x_1, ...x_m)^2 + P_2(a_1, ..., a_n, y_1, ...y_m)^2 = 0$

Μια τεχνικής φύσεως παρατήρηση που θα είναι χρήσιμη λίγο αργότερα: Για καθαρά τεχνικούς λόγους είναι απλούστερο να μελετάμε το πρόβλημα του αν υπάρχει αλγόριθμος που να αποφασίζει αν μία τυχούσα διοφαντική εξίσωση έχει λύση στους φυσικούς και αυτό θα κάνουμε στο εξής.Για να βεβαιωθούμε όμως ότι τα δύο εκ πρώτης όψεως διαφορετικά προβλήματα είναι κατ' ουσίαν το ίδιο αρκεί να βρούμε αλγορίθμους με τους οποίους να ανάγεται το πρώτο πρόβλημα στο δεύτερο και αντιστρόφως:

Επειδή, με βάση το Θεώρημα του Lagrange ,κάθε φυσικός αριθμός γράφεται ως άθροισμα τεσσάρων τετραγώνων, το πρόβλημα της ύπαρξης ή μη φυσικών ως ριζών μπορεί να αναχθεί στο αντίστοιχο για ακέραιες ρίζες.Π.χ. η εξίσωση

$$x^3 + y^3 = z^3 \tag{2}$$

έχει ρίζες στους φυσικούς αν και μόνο αν η εξίσωση $({x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2)^3 + ({y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2)^3 = ({z_1}^2 + {z_2}^2 + {z_3}^2 + {z_4}^2)^3$ έχει ρίζες στους ακεραίους.Για την αντίστροφη αναγωγή δεν έχουμε παρά να παρατηρήσουμε ότι η διοφαντική εξίσωση $P(x_1, ..., x_n) = 0$ έχει λύση στους ακεραίους εάν και μόνον εάν η εξίσωση $P(b_1 - c_1, ...b_n - c_n) = 0$ έχει ρίζες στους φυσικούς.

Επιπλέον,είναι εύκολο να δει κανείς ότι π.χ. η εξίσωση $P(x_1, ..., x_n) = 0$ έχει μία λύση στους φυσικούς για την οποία $x_1 \geq 5$ εάν και μόνον εάν η εξίσωση $P(x_1 + 5, ..., x_n) = 0$ έχει λύση στους φυσικούς.

Υπενθυμίζουμε ότι ένα σύνολο λέγεται αναδρομικό όταν υπάρχει αλγόριθμος που αποφασίζει αν τυχόν στοιχείο ανήκει σε αυτό ή όχι,ενώ αναδρομικά απαριθμήσιμο (α.α.) όταν υπάρχει αλγόριθμος που υπολογίζει με οποιαδήποτε σειρά,όλα τα στοιχεία του.Ένα από τα βασικότερα αποτελέσματα της Θεωρίας αναδρομής ειναι το ότι υπάρχει α.α. σύνολο που δεν είναι αναδρομικό.Είναι προφανές το ότι κάθε διοφαντικό συνολο ειναι α.α.:χρειάζεται απλώς,αν π.χ ένα διοφαντικό σύνολο Δ περιγράφεται από την (1) να διατάξουμε όλες τις $n + m$-άδες πιθανών τιμών τών μεταβλητών σε μια καλή διάταξη μήκους ω και να τις δοκιμάζουμε όλες με τη σειρά.Όταν κάποια δώσει τιμή 0 στο πολυώνυμο,βεβαιωνόμαστε ότι η αντιστοιχη πρώτη n-άδα ανήκει στο Δ.Το 1953 ο Martin Davis διατύπωσε την εικασία ότι ισχύει και το αντίστροφο,δηλαδή ότι κάθε α.α. σύνολο είναι διοφαντικό.Αν αυτή η εικασία ίσχυε, τότε,με βαση τα παραπάνω, η απάντηση στο ΔΠΧ θα ήταν πως δεν υπάρχει ο ζητούμενος αλγόριθμος.Πράγματι,η απάντηση στο ΔΠΧ ολοκληρώθηκε με την απόδειξη της εικασίας αυτής. Πρέπει να σημειώσουμε επίσης ότι η απόδειξη των Martin Davis, Julia Robinson,Hilary Putnam καιYuri Matiyasevich είναι κατασκευαστική, υπό την έννοια ότι ξεκινώντας από μία αριθμητική παράσταση ενός α.α. συνόλου,δηλαδή έναν ανοικτό τύπο στη γλώσσα της αριθμητικής του οποίου προηγούνται μόνον υπαρξιακοί και φραγμένοι καθολικοί ποσοδείκτες,μπορούμε να βρούμε την αντίστοιχη παραμετρική οικογένεια εξισώσεων που δείχνει ότι το σύνολο αυτό είναι διοφαντικό.

Τι θα συνέβαινε όμως αν ο Hilbert δίκιο,αν δήλαδή υπήρχε αλγόριθμος που να λύνει το ΔΠΧ;

Πολλές συγκεκριμένες οικογένειες διοφαντικών εξισώσεων έχουν μελετηθεί και ξέρουμε αν έχουν ή οχι ακέραιες ρίζες.Οι τεχνικές όμως είναι κάθε φορά διαφορετικές και ενίοτε πολύ δύσκολες.Αν υπήρχε ο αλγόριθμος του ΔΠΧ θα είχαμε μια ενιαία μέθοδο αντιμετώπισης του ερωτήματος αυτού για όλες τις διοφαντικές εξισώσεις.Δεν είναι όμως μόνο αυτό.Πολλά σημαντικά προβλήματα μπορούν να αναχθούν στην επιλυσιμότητα κάποιας διοφαντικής εξίσωσης,καποια με προφανείς τρόπους και άλλα με κάπως δυσκολότερους.

Μερικά παραδείγματα:

1 Ως γνωστόν η (2) είναι μια υποπερίπτωση του Τελευταίου Θεωρήματος του Fermat.Υπάρχει όμως και τρόπος να αναχθεί ολόκληρο το Θεώρημα(Εικασία μέχρι πριν από λίγα χρόνια) στην επιλυσιμότητα μίας διοφαντικής εξίσωσης.Πράγματι,ένα από τα βασικά βήματα της απάντησης στο ΔΠΧ ήταν η αναγωγή της επιλυσιμότητας οποιασδήποτε εκθετικής διοφαντικής εξίσωσης (που μπορεί να έχει δηλαδή και εκθέτες ως αγνώστους) στην επιλυσιμότητα μιας (συνήθους)διοφαντικής εξίσωσης.Υπάρχει δηλαδή ένα πολυώνυμο $A(a, b, g, x_1, ...x_n)$ ώστε

$$a = b^g \iff \exists x_1, ...x_n A(a, b, g, x_1, ..., x_n) = 0 \qquad (3)$$

Έτσι,με βάση και τις ιδιότητες των διοφαντικών συνόλων που έχουμε ήδη αναφέρει ,μπορούμε να κατασκευάσουμε ένα πολυώνυμο που έχει ακέραιες ρίζες εάν και μόνον εάν το Τελευταίο Θεώρημα του Fermat είναι λάθος.(χρησιμοποιώντας και την παραπάνω τεχνική για την ¨ενσωμάτωση¨ στην εξίσωση των κατάλληλων ανισώσεων).

2 Γνωρίζοντας πια ότι οι κλάσεις των α.α. και των διοφαντικών συνόλων ταυτίζονται,παρατηρούμε ότι π.χ.το σύνολο των αρτίων αριθμών ≥ 2 που δεν είναι άθροισμα δύο πρώτων είναι α.α.,οπότε και διοφαντικό, και άρα μπορούμε να κατασκευάσουμε μία συγκεκριμένη παραμετρική διοφαντική εξίσωση $K(a, x_1, ..., x_n) = 0$ που για κάθε a έχει λύση εάν και μόνον εάν το a είναι αντιπαράδειγμα για την εικασία του Goldbach.Έτσι τελικά η εικασία του Goldbach είναι ισοδύναμη με το ότι η εξίσωση $K(x_0, x_1, ..., x_n) = 0$ δεν έχει καμία $n + 1$-άδα ως λύση.

3 Μπορεί επίσης να κατασκευαστεί μια διοφαντική εξίσωση που έχει ρίζες εάν και μόνον εάν δεν ισχύει η Υπόθεση του Riemann(ανοικτό πρόβλημα ως σήμερα) ενώ ανάλογη ήταν η κατάσταση για τη γνωστή ως Εικασία των Τεσσάρων Χρωμάτων,η οποία αποδείχθηκε το 1976 από τους K.Appel και W.Haken.

4 Τα παραπάνω παραδείγματα είναι χωρίς αμφιβολία σημαντικά,δεν είναι όμως ¨φυσικά¨,δεν είναι δηλαδή προβλήματα παραπλήσια με το ΔΠΧ που ανάγονται σ' αυτό με τρόπο που συνδέεται άμεσα με την ίδια τη φύση τους.

Παραπλήσια με το ΔΠΧ προβλήματα και άρα απολύτως φυσιολογικά εξεταζόμενα μαζί του είναι αυτά που ζητούν την εύρεση αλγορίθμου που, δοθέντος ενός πολυωνύμου με συντελεστές από κάποιο δακτύλιο R_1, να αποφασίζει αν το πολυώνυμο έχει ρίζες σε κάποιον άλλο δακτύλιο R_2.Για πολλές και σημαντικές περιπτώσεις το πρόβλημα αυτό ανάγεται στο ΔΠΧ·φαίνεται ότι ο Hilbert διαισθανόταν(ή ίσως το είχε μελετήσει)ότι το ΔΠΧ όπως τέλικα το διατύπωσε στον κατάλογό του ήταν το πιο ¨δύσκολο¨ από αυτά τα παραπλήσια προβλήματα. Από αυτά τα τελευταία ίσως το πιο σημαντικό είναι τρόπον τινά το αυθεντικό:ο ίδιος ο Διόφαντος δηλαδή,μελετώντας τις φερώνυμες εξισώσεις έψαχνε ρητές λύσεις και όχι αναγκαστικά ακέραιες. Η αναγωγή του προβλήματος αυτού στο ΔΠΧ γίνεται ως εξής: Έστω ότι θέλουμε να βρούμε αν η διοφαντική εξίσωση

$$P(x_1, ..., x_n) = 0 \tag{4}$$

έχει ρητές λύσεις.Είναι προφανές ότι αυτό συμβαίνει εάν και μόνον εάν η εξίσωση

$$P(\frac{y_1 - t_1}{z+1}, ..., \frac{y_n - t_n}{z+1}) = 0 \tag{5}$$

έχει λύσεις στους φυσικούς, δηλαδή εάν και μόνον εάν η διοφαντική εξίσωση

$$(z+1)^d P(\frac{y_1 - t_1}{z+1}, ..., \frac{y_n - t_n}{z+1}) = 0 \tag{6}$$

(όπου d ο βαθμός του P) έχει ρίζες στους φυσικούς. Άλλα παραδείγματα σ' αυτό το πνεύμα είναι τα προβλήματα του αν υπάρχει αλγόριθμος που να αποφασίζει αν μια τυχούσα διοφαντική εξίσωση έχει ρίζες στο δακτύλιο των ακεραίων του Gauss ,δηλ.στους αριθμούς της μορφής $g + hi$,όπου $g, h \in \mathbb{Z}$ και i η φανταστική μονάδα, [2] σε διάφορα αριθμητικά σώματα,σε διάφορους δακτυλίους πολυωνύμων,αλλά και σε σώματα π.χ. ρητών συναρτήσεων με συντελεστές από κάποιο δακτύλιο κ.τ.λ. Στα παράκατω θα κάνουμε μια

[2]Η αναγωγή και αυτού του προβλήματος στο ΔΠΧ γίνεται με τον σχεδόν προφανή τρόπο:Έστω ότι θέλουμε να βρούμε αν η διοφαντική εξίσωση $P(x_1, \ldots, x_l)$ έχει ρίζες στο δακτύλιο του Gauss.Είναι προφανές ότι αυτό συμβαίνει εάν και μόνον εάν η εξίσωση

$$P(g_1 + h_1 i, \ldots, g_l + h_l i) \tag{7}$$

έχει ρίζες στους ακεραίους.Στην (7) μπορούμε να χωρίσουμε τους πραγματικούς από τους μιγαδικούς συντελεστές:

$$P(g_1 + h_1 i, \ldots, g_l + h_l i) = P_1(g_1, \ldots, g_l, h_1, \ldots, h_l) + iP_2(g_1, \ldots, g_l, h_1, \ldots, h_l) \tag{8}$$

Έτσι,η $P(x_1, \ldots, x_l) = 0$ έχει ρίζες στους ακέραιους του $Gauss$ εάν και μόνον εάν η εξίσωση

$$P_1(g_1, \ldots, g_l, h_1, \ldots, h_l)^2 + P_2(g_1, \ldots, g_l, h_1, \ldots, h_l)^2 = 0$$

έχει ρίζα στους ακέραιους.Το 1975 ο J.Denef πέτυχε και την αντίστροφη αναγωγή,αποδεικνύοντας έτσι ότι δεν υπάρχει αλγόριθμος που να αποφασίζει αν μια τυχούσα διοφαντική εξίσωση έχει ρίζα στο δακτύλιο των ακέραιων του Gauss.

σύντομη και οπωσδήποτε ελλιπή επισκόπηση των αποτελεσμάτων που σχετίζονται με τα προβλήματα που ίσως ο Hilbert ϑέλησε να ϑέσει εμμέσως και που τελικά η Ιστορία των Μαθηματικών,με ελαφρά ειρωνεία,άφησε αναπάντητα απαντώντας ακριβώς στο Δέκατο Πρόβλημά του.Πλήρη απόδειξη ϑα δώσουμε μόνο για ένα από αυτά ενώ ϑα σταθούμε ιδιαίτερα στις προσπάϑειες που γίνονται να λυθεί το αντίστοιχο του ΔΠΧ για τους ρητούς.

3 Γενική επισκόπηση και μία αποδείξη

3.1 Διάφορες επεκτάσεις του ΔΠΧ·λυμένα και άλυτα προβλήματα

Κατ' αρχήν θα επαναδιατυπώσουμε μερικούς ορισμούς,γενικεύοντάς τους,για να μπορέσουμε να διατυπώσουμε με ενοποιημένο τρόπο τα διάφορα αποτελέσματα που θα αναφέρουμε αμέσως μετά.

Ορισμός 3 *Έστω R ένας μεταθετικός δακτύλιος με μονάδα και L μια γλώσσα για τη θεωρία δακτυλίων,δηλαδή μια γλώσσα που περιέχει τουλάχιστον τα συναρτησιακά σύμβολα +,·,και τις σταθερές 0(για το ουδέτερο στοιχείο ως προς την πρόσθεση),1(για το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό). Έστω R^L ο υποδακτύλιος του R που παράγεται από τα στοιχεία για τα οποία υπάρχουν σύμβολα σταθερών στην L.Διοφαντικό πολυώνυμο (στην L επί του R) είναι ένα πολυώνυμο με συντελεστές από το R^L (και οποιουνδήποτε αριθμό μεταβλητών). Αντιστοίχως,αν το P είναι ένα διοφαντικό πολυώνυμο στην L ,η $P = 0$ καλείται διαφαντική εξίσωση και η $P \neq 0$ διοφαντική ανίσωση στην L.*

Στα επόμενα,εκτός αν κάνουμε συγκεκριμένη αντίθετη αναφορά, θα εννοούμε ότι $L = \{+, \cdot, 0, 1\}$.

Ορισμός 4 *Αν η F είναι διάζευξη πεπερασμένων το πλήθος συστημάτων διοφαντικών εξισώσεων και ανισώσεων,ο τύπος $\exists \vec{x} F$ ονομάζεται υπαρξιακός τύπος και το σύνολο που ορίζεται μέσω αυτού υπαρξιακό.Αν στην F υπάρχουν μόνο εξισώσεις ο τύπος και το αντίστοιχο σύνολο καλούνται θετικά υπαρξιακά ενώ αν η F αποτελείται από μία μόνο εξίσωση,ο τύπος και το αντίστοιχο σύνολο καλούνται διοφαντικά.*

Υπένθυμίζουμε ότι θεωρία του δακτυλίου R για τη γλώσσα L ονομάζεται το σύνολο των προτάσεων της γλώσσας L που αληθεύουν στον R (με τη συνήθη ερμηνεία των διαφόρων συμβόλων). Αναλόγως ορίζουμε την υπαρξιακή και την θετικά υπαρξιακή θεωρία του R για την L ως το σύνολο των υπαρξιακών ή θετικά υπαρξιακών προτάσεων της L που αληθεύουν στον R.Θα αποδείξουμε τώρα κάποιες βασικές ιδιότητες των αντικειμένων που μόλις ορίσαμε.

Λήμμα 1 *Έστω R ένας δακτύλιος και L μια γλώσσα όπως στον ορισμό 3*

1 *Η τομή καθώς και η ένωση πεπερασμένων το πλήθος υπαρξιακών συνόλων είναι υπαρξιακό σύνολο.*

2 *Αν ο R είναι ακεραία περιοχή της οποίας το σώμα πηλίκων δεν είναι αλγεβρικά κλειστό,κάθε θετικά υπαρξιακό σύνολο είναι διοφαντικό.*

3 *Αν το R είναι σώμα,κάθε υπαρξιακό σύνολο είναι θετικά υπαρξιακό .*

4 *Αν το σύνολο $R \backslash \{0\}$ είναι θετικά υπαρξιακό και η θετικά υπαρξιακή θεωρία του R αποφασίσιμη,τότε η υπαρξιακή θεωρία του B,όπου B το σώμα πηλίκων του R,είναι επίσης αποφασίσιμη.*

Απόδειξη

1 Έστω ότι τα υπαρξιακά σύνολα E_1, E_2 ορίζονται από τους τύπους $\exists \vec{x} F_1$ και $\exists \vec{x'} F_2$ αντιστοίχως,όπως στον ορισμό 4,όπου ο F_1 είναι διάζευξη των συστημάτων $r_1, ...r_n$ και ο F_2 των $p_1, ...p_m$. Τότε το $E_1 \bigcap E_2$ ορίζεται από τον τύπο $\exists \vec{x} \exists \vec{x'} ((r_1 \wedge p_1) \vee (r_1 \wedge p_2) \vee \ldots (r_n \wedge p_m)$ και το $E_1 \bigcup E_2$ από τον τύπο $\exists \vec{x} \exists \vec{x'} F_0 \vee F_0$.

2 Αρκεί από δύο τυχούσες πολυωνυμικές εξισώσεις

$$f_1(x_1, \ldots, x_m) = 0 \tag{9}$$

και

$$f_2(x_1, \ldots, x_m) = 0 \tag{10}$$

να μπορούμε να βρούμε μία τρίτη

$$g(x_1, \ldots, x_m) \tag{11}$$

ώστε η (11) να έχει λύση στον R εάν και μόνον εάν και η (9) και η (10)έχουν. Πράγματι, αν μπορούμε να το κάνουμε αυτό τότε αν το θετικά υπαρξιακό σύνολο E_1 ορίζεται από τον τύπο $\exists \vec{x} F_1$ όπως στον ορισμό 4,όπου ο F_1 είναι διάζευξη των συστημάτων $r_1, ...r_l$,καθένα από τα $r_1, \ldots, r_l$ μπορεί να αναχθεί σε μία πολυωνυμική εξίσωση.Τα αντίστοιχα πολυώνυμα στη συνέχεια μπορούν να πολλαπλασιαστούν, και, ακριβώς επειδή ο R είναι ακεραία περιοχή η τελική πολυωνυμική εξίσωση θα έχει ρίζες εάν και μόνον εάν ένα από τα $r_1, ...r_l$ έχει.

Έστω λοιπόν B το σώμα πηλίκων του R και $H(x) = \sum_{i=0}^{n} h_i x^i \in R[x]$ ένα πολυώνυμο χωρίς ρίζες στο B.Παρατηρούμε ότι το πολυώνυμο $H' = x^n H(x^{-1}) = \sum_{i=0}^{n} h_i x^{n-i}$, επειδή ακριβώς το B είναι σώμα, επίσης δεν μπορεί να έχει ρίζες στο B .Κατασκευάζουμε τώρα την εξίσωση

$$g(x_1, \ldots, x_m) = \sum_{i=0}^{n} h_i f_1(x_1, ...x_m)^i f_2(x_0, ..., x_m)^{n-i} = 0. \tag{12}$$

Αν για κάποια m-άδα $a_1, ..., a_m \in R$ έχουμε $f_1(x_1, ...x_m) = f_2(x_1, ...x_m) = 0$, τότε προφανώς $g(x_1, ...x_m) = 0$.Αντιστρόφως,αν για κάποια m-άδα $a_1, ..., a_m \in R$, $g(x_1, ...x_m) = 0$ αλλά $f_1(x_1, ..., x_m) \neq 0$ τότε διαιρώντας με ${f_1}^n$ παίρνουμε

$$\sum_{i=0}^{n} h_i (\frac{f_2}{f_1})^{n-i} = H'(\frac{f_2}{f_1}) = 0, \tag{13}$$

που είναι άτοπο επειδή το H' δεν έχει ρίζες στο B.Τέλος,αν για κάποια m-άδα $a_1, ..., a_m \in R$, $g(x_1, ...x_m) = 0$ αλλά $f_2(x_1, ..., x_m) \neq 0$,ακολουθώντας την ίδια διαδικασία καταλήγουμε στο $H\left(\frac{f_1}{f_2}\right) = 0$,που είναι επίσης άτοπο.

3 Δεν έχουμε παρά να παρατηρήσουμε ότι σε έναν υπαρξιακό τύπο της μορφής,π.χ. $\exists \vec{x} P(x_1, ..., x_n) \neq 0$ (του οποίου οι ελεύθερες μεταβλητές εμφανίζονται στους συντελεστές του πολυωνύμου)μπορούμε να προσθέσουμε μια δεσμευμένη μεταβλητή παίρνοντας έναν καινούριο τύπο που ορίζει το ίδιο σύνολο ως εξής:$\exists \vec{x} \exists y \; [yP(x_1, ..., x_n) - 1 = 0]$

4 Παρατηρούμε ότι,με βάση την απόδειξη της προηγούμενης παρατήρησης, αρκεί να δείξουμε το ζητούμενο για την θετικά υπαρξιακή θεωρία του B.Αν λοιπόν το F είναι διάζευξη συστήματος L-διοφαντικών εξισώσεων με ελεύθερες μεταβλητές τις $x_1, ..., x_n$,τότε

$$(\exists x_1, ...x_n \in B)F \iff (\exists x_1, ..., x_n, y_1, ...y_n \in R)[(y_1 \neq 0 \wedge ...y_n \neq 0) \wedge F']$$

όπου το F' προέρχεται από το F με καταλληλο πολλαπλασιασμό των εξισώσεων (π.χ. η $2{x_1}^2x_2 + {x_3}^4 + 5 = 2$ θα γινόταν ${y_1}^2y_2{y_3}^4(2{x_1}^2x_2 + {x_3}^4 + 5) = 2{y_1}^2y_2{y_3}^4$.Η δεύτερη αυτή πρόταση είναι θετικά υπαρξιακή λόγω της υπόθεσης.Έτσι αρκεί να εφαρμόσουμε σ' αυτήν τον αλγόριθμο που υποθέσαμε ότι υπάρχει.

Η επέκταση του ΔΠΧ που θα έλεγε κανείς ότι συγγενεύει περισσότερο με το αρχικό πρόβλημα είναι εκείνη που αφορά την αναζήτηση λύσεων όχι στον δακτύλιο των ακεραίων αλλά σε δακτυλίους αλγεβρικών ακεραίων κάποιου αριθμητικού σώματος (δηλ. πεπερασμένης επέκτασης του $\mathbb{Q}$).Προς αυτήν την κατεύθυνση,το 1959 η Julia Robinson έδειξε ότι ο δακτύλιος των αλγεβρικών ακεραίων (ριζών μονικών πολυωνύμων με ακέραιους συντελεστές) οποιουδήποτε αριθμητικού σώματος έχει μη αποφασίσιμη θεωρία.Η μέθοδος της βασιζόταν στην απόδειξη του ότι το $\mathbb{Z}$ είναι ορίσιμο σε οποιονδήποτε τέτοιο δακτύλιο,όχι όμως υπαρξιακά·έτσι,το αντίστοιχο του ΔΠΧ για τυχόντα δακτύλιο αυτής της μορφής έμεινε και μένει ανοικτό στη γενική περίπτωση.Παρ' όλ' αυτά για αρκετές σημαντικές περιπτώσεις η απάντηση είναι γνωστή,και σε όλες είναι η μη αποφασισιμότητα της αντίστοιχης θεωρίας.Συγκεκριμένα,το πρόβλημα έχει λυθεί για πλήρως πραγματικά [3] αριθμητικά σώματα(δηλ.εκείνα στα οποία το -1 δεν είναι άθροισμα τετραγώνων),για αβελιανά αριθμητικά σώματα(των οποίων,δηλαδή η ομάδα Galois είναι αβελιανή),καθώς και αριθμητικά σώματα που έχουν ακριβώς δύο μη πραγματικές εμφυτεύσεις.Εικάζεται ότι η υπαρξιακή θεωρία του δακτυλίου των αλγεβρικών ακεραίων οποιουδήποτε αριθμητικού σώματος είναι μη αποφασίσιμη,αλλά δεν έχει βρεθεί ακόμα μέθοδος που να ενοποιεί τις αποδείξεις των παραπάνω αποτελεσμάτων.Παρεπιπτόντως, είναι ενδιαφέρον το εξής αποτέλεσμα, αντίθετου από τα προηγούμενα είδους, για το δακτύλιο όλων των αλγεβρικών ακεραίων:όχι μόνο η διοφαντική του θεωρία (Rumely,1986) αλλά όλη η πρωτοβάθμια θεωρία του είναι αποφασίσιμη (van den Dries,1988).Το ίδιο ισχύει και για την πρωτοβάθμια θεωρία των πραγματικών αλγεβρικών αριθμών(Prestel και Schmid,1991).

Άλλη περίπτωση που έχει προσελκύσει τους μελετητές είναι οι πολυωνυμικοί δακτύλιοι R[t] όπου R μεταθετική ακέραια περιοχή.Το πρόβλημα αποκτά ενδιαφέρον από τη στιγμή που στη γλώσσα για την οποία διατυπώνεται έχει προστεθεί τουλάχιστον άλλο ένα σύμβολο πέραν των 0,1,+,·.

Πράγματι,αν περιοριστούμε στη γλώσσα $L = \{+, \cdot, 0, 1\}$ τότε το ΔΠΧ για τον R[t] ανάγεται στο ΔΠΧ για τον R αφού αν η τυχούσα διοφαντική εξίσωση

$$P(x_1, ..., x_n) = 0 \tag{14}$$

με συντελεστές στον R_L έχει ρίζες στον R τότε προφανώς έχει ρίζες στον R[t] ενώ αν έχει ρίζες στον R[t] κάποια n-άδα πολυωνύμων $p_1(x), ..., p_n(x)$ τότε θέτοντας $p_i(1) = r_i$ για κάθε $1 \leq i \leq n$ παίρνουμε $P(r_1, ..., r_n) = 0$.

[3]μεταφράζω,ίσως αδόκιμα,τον όρο "totally" ή "formally" real number fields

Η πιο φυσιολογική επέκταση της γλώσσας $L = \{+, \cdot, 0, 1\}$ είναι η $L' = L \cup \{t\}$ όπου η σταθερά t ερμηνεύεται ακριβώς ως το υπερβατικό επί του R στοιχείο.Για αυτή την επεκτεταμένη γλώσσα ο Denef απέδειξε κατ' αρχήν ότι δεν υπάρχει αλγόριθμος-λύση του ΔΠΧ για τον δακτύλιο R[t] όταν ο R είναι ακέραια περιοχή χαρακτηριστικής 0 (το 1978) και στη συνέχεια οποιασδήποτε χαρακτηριστικής (το 1984).

Πιο ενδιαφέρουσα,αφού έχει αρκετές ομοιότητες και με το ΔΠΧ για το $\mathbb{Q}$,είναι η περίπτωση του σώματος των ρητών συναρτήσεων Σ(t) επί ενός σώματος Σ,την οποία μελετάμε επίσης για τη γλώσσα $L' = L \cup \{t\}$.Έχει αποδειχθεί ότι η πρωτοβάθμια θεωρία του σώματος Σ(t),όπου το Σ είναι σώμα χαρακτηριστικής > 0 δεν είναι αποφασίσιμη αν το Σ είναι πεπερασμένο($Er\check{s}ov$,1965 για σώματα χαρακτηριστικής > 2 και Penzin,1973 για σώματα χαρακτηριστικής 2) ή αν το Σ είναι τέλειο[4] (Cherlin,1984).Όπως όμως και σε άλλες περιπτώσεις, οι αποδείξεις δεν εξειδικεύτηκαν εύκολα ώστε να φτάσουμε στην απόδειξη της μη αποφασισιμότητας των αντίστοιχων υπαρξιακών θεωριών.Παρ'όλαυτά,έχει δειχθεί ότι δεν υπάρχει αλγόριθμος-λύση του ΔΠΧ σε καμία από τις παρακάτω περιπτώσεις:

ι) Όταν το Σ είναι πραγματικό σώμα[5]π.χ. όταν Σ=$\mathbb{R}$.

ιι) Όταν το Σ είναι πεπερασμένο(Φειδάς,1991 για πεπερασμένα σώματα χαρακτηριστικής > 2 και Videla,1994 για πεπερασμένα σώματα χαρακτηριστικής 2)

ιιι) Στην περίπτωση του $\mathbb{C}(t_1, t_2)$ (για γλώσσα επαυξημένη με δύο σύμβολα σταθερών)

Σημαντικό ανοικτό πρόβλημα αυτού του είδους είναι το ΔΠΧ(ή,ακόμα, η αποφασισιμότητα όλης της πρωτοβάθμιας θεωρίας) του $\mathbb{C}(t)$.

Άλλη ενδιαφέρουσα κατηγορία προβλημάτων αυτής της μορφής,για την οποία προς το παρόν υπάρχουν λίγα αποτελέσματα, είναι το ΔΠΧ για δακτυλίους μιγαδικών συναρτήσεων,αναλυτικών σε κάποια ανοικτή περιοχή ενός συνεκτικού υποσυνόλου του μιγαδικού επιπέδου.

[4]Ένα σώμα Σ καλείται τέλειο αν κάθε πολυώνυμο $p(x) \in \Sigma[x]$ είναι γινόμενο αναγώγων πολυωνύμων όλες οι ρίζες των οποίων είναι απλές

[5]Ένα σώμα Σ ονομάζεται πραγματικό όταν 1)είναι διατάξιμο,δηλ. υπάρχει υποσύνολό του Θ⊆Σ (το σύνολο των θετικών στοιχείων του) κλειστό ως προς πρόσθεση και πολλαπλασιασμό τέτοιο ώστε το Σ να είναι η ξένη ένωση των Θ,0,-Θ. (Με βάση ένα θεώρημα των Artin και Schreier ένα σώμα Σ είναι διατάξιμο εάν και μόνον εάν είναι πλήρως πραγματικό,βλ.σ.7)

2)Κάθε θετικό στοιχείο του Σ έχει μια τετραγωνική ρίζα στο Σ

3)κάθε πολυώνυμο μιας μεταβλητής, περιττού βαθμού,με συντελεστές στο Σ έχει ρίζα στο Σ.

Ισχύει το εξής:το σώμα Σ είναι πραγματικό εάν και μόνον εάν είναι πλήρως πραγματικό και καμία γνήσια, αλγεβρική επέκτασή του δεν είναι πλήρως πραγματική.

3.2 Το ΔΠΧ για σώματα ρητών συναρτήσεων επί πεπερασμένου σώματος χαρακτηριστικής > 2

Στο υποκεφάλαιο αυτό θα παρουσιάσουμε την απόδειξη του Φειδά για το εξής:

Θεώρημα 1 *Δεν υπάρχει αλγόριθμος που να αποφασίζει για την ισχύ τυχούσας υπαρξιακής πρότασης στη γλώσσα* $L_t = +, \cdot, 0, 1, t$ *στο σώμα των ρητών συναρτήσεων επί οποιουδήποτε πεπερασμένου σώματος χαρακτηριστικής* > 2.

Ο λόγος που διαλέγουμε να παρουσιάσουμε αυτό το αποτέλεσμα είναι το γεγονός ότι τα σώματα αυτά έχουν αρκετές κοινές ιδιότητες με το σώμα των ρητών και έτσι η αρνητική λύση του ΔΠΧ για αυτά αποτελεί μια πρώτη,πολύ ασαφή ακόμη, ένδειξη ότι αρνητική θα είναι η λύση και για την περίπτωση των ρητών. Παρά την ομοιότητα πάντως,χρειάζεται να είμαστε πολύ επιφυλακτικοί,αφού όπως θα δούμε ευθύς αμέσως, το βασικό εργαλείο που χρησιμοποιείται στην παρακάτω απόδειξη είναι η ύπαρξη ενός υπερβατικού στοιχείου επί μιας πεπερασμένης επέκτασης του πρώτου[6] σώματος που περιέχεται στο σώμα που μελετάμε. Έτσι,δεν φαίνεται πώς μια γενίκευση των τεχνικών που χρησιμοποιούνται παρακάτω θα επέτρεπε να φτάσουμε σε λύση του ΔΠΧ για τους ρητούς.Πράγματι,όπως θα δούμε στο επόμενο κεφάλαιο,τα εργαλεία που χρησιμοποιούνται στην περίπτωση αυτή είναι πολύ διαφορετικά. Όπως σε όλες τις σχετικές αποδείξεις,η ¨καρδιά¨ της όλης διαδικασίας είναι η ¨κωδικοποίηση¨ της θεωρίας του δακτυλίου των ακεραίων στη γλώσσα $L = \{0, 1, +, \cdot\}$.Συγκεκριμένα,θέλουμε να βρούμε έναν αλγόριθμο που για κάθε θετικά υπαρξιακή πρόταση ϕ στη γλώσσα L να δίνει μια υπαρξιακή πρόταση ϕ' στη γλώσσα L_t ούτως ώστε η ϕ' να αληθεύει στη δομή την οποία κάθε φορά μελετάμε(εδώ ένα σώμα ρητών συναρτήσεων επί κάποιου πεπερασμένου σώματος χαρακτηριστικής > 2) εάν και μόνον εάν η ϕ αληθεύει στους ακέραιους.Είναι εύκολο να δει κανείς ότι αν μία τέτοια αναγωγή είναι εφικτή ,τότε η αποφασισιμότητα της υπαρξιακής θεωρίας της δομής αυτής συνεπάγεται ότι και η θετικά υπαρξιακή θεωρία του δακτυλίου των ακεραίων είναι αποφασίσιμη,κάτι που είναι άτοπο,λόγω της απάντησης στο κλασσικό ΔΠΧ.

Η αναγωγή που περιγράψαμε θα γίνει σε δύο στάδια,εκ των οποίων το ένα θα δεχτούμε ότι γίνεται χωρίς απόδειξη.Συγκεκριμένα, έστω η γλώσσα $L' = \{0, 1, +, \geq, |_p\}$ όπου η διμελής σχέση $\geq$ ερμηνεύεται φυσιολογικά ως ¨μεγαλύτερο ή ίσο¨ ενώ η διμελής σχέση $|_p$ ερμηνεύεται ως εξής:$s_1|_p s_2 \longleftrightarrow \exists s_3[s_2 = p^{s_3}s_1]$.Θα παραλείψουμε την απόδειξη του ότι υπάρχει αλγόριθμος μέσω του οποίου η θετικά ύπαρξιακή θεωρία του δακτυλίου των ακεραίων στη γλώσσα L ανάγεται στην διοφαντική θεωρία της L' για το δακτύλιο των ακεραίων,όπου έχουμε τροποποιήσει ελαφρώς τον ορισμό της διοφαντικής θεωρίας επιτρέποντας στους διοφαντικούς τύπους συζεύξεις πολυωνύμων(για την ακρίβεια αθροισμάτων,αφού δεν έχουμε το συναρτησιακό σύμβολο για τον πολλαπλασιασμό) με ατομικούς τύπους.Η απόδειξη αυτή έχει επίσης γίνει από το Φειδά το 1987.Αντίθετα,θα δώσουμε πλήρη την απόδειξη για το ότι η διοφαντική θεωρία του δακτυλίου των ακεραίων στη γλώσσα L' ανάγεται στη διοφαντική θεωρία του σώματος που μας ενδιαφέρει στη γλώσσα L.

[6]Θυμίζουμε ότι πρώτα σώματα ονομάζονται αυτά που δεν περιέχουν γνήσια υποσώματα,ή αλλιώς,αυτά που είναι ισόμορφα είτε με τους ρητούς είτε με το $\mathbb{Z}_p$ για κάποιο πρώτο p.

Έστω λοιπόν Σ ένα πεπερασμένο σώμα με p^k στοιχεία,όπου p πρώτος,η χαρακτηριστική του Σ. Έστω r πρώτο πολυώνυμο του $\Sigma(t)$,δηλ. μονικό πολυώνυμο ανάγωγο επί του $\Sigma[t]$ και τυχόν $g \in \Sigma(t), g \neq 0$.Τότε το g γράφεται κατά μοναδικό τρόπο ως $g = r^n h$,όπου $h \in \Sigma(t), n \in \mathbb{Z}$ και το r δεν διαιρεί ούτε τον αριθμητή ούτε τον παρονομαστή του h.Ο αριθμός n ονομάζεται τάξη του g στο r και συμβολίζεται με $ord_r g$. Η βασική ιδέα είναι να αναχθούν οι ακέραιοι στις τάξεις των στοιχείων του $\Sigma(t)$ στο t.Διατυπώνουμε πρώτα τα λήμματα που θα χρειαστούμε για την απόδειξη. Έστω Σ πεπερασμένο σώμα χαρακτηριστικής $p > 2$,με $e = p^k$ στοιχεία.

Λήμμα 2 *Το τυχόν $g \in \Sigma(t)$ είναι p^n-οστή δύναμη του t για κάποιο $n \in \mathbb{N}$ εάν και μόνον εάν υπάρχουν $a, b \in \Sigma(t)$ ώστε $g - t = a^p - a$ και $g^{-1} - t^{-1} = b^p - b$.*

Λήμμα 3 *Για τυχόν $g \in \Sigma(t)$ το $a = \frac{g^p+t}{g^p-t}$ έχει μόνο απλές ρίζες και μόνο απλούς πόλους.*

Λήμμα 4 *Έστω $g_1, g_2 \in \Sigma(t)$ με $g_1 g_2 \neq 0$ και $a = \frac{{g_1}^p+t}{{g_1}^p-t}, b = \frac{g_2+t^{p^j}}{g_2-t^{p^j}}$ για κάποιο $j \geq 0$.Τότε $g_2 = {g_1}^{p^{j+1}}$ εάν και μόνον εάν υπάρχουν $d_1, d_2, d_3, d_4, d_5 \in \Sigma(t)$ ώστε*

$$b^2 - a^2 = {d_1}^p - d_1 \tag{15}$$
$$b^{-2} - a^{-2} = {d_2}^p - d_2 \tag{16}$$
$$b^2 t^{p^j} - a^2 t = {d_3}^p - d_3 \tag{17}$$
$$b^{-2} t^{-p^j} - a^{-2} t^{-1} = {d_4}^p - d_4 \tag{18}$$
$$b - a = {d_5}^p - d_5 \tag{19}$$

Λήμμα 5 *Έστω $g \in \Sigma(t)$.Τότε $ord_t g \geq 0$ εάν και μόνον εάν υπάρχει $j \in \mathbb{N}, j \neq 0$ ώστε $\exists a_0, ..., a_{e-1} \in \Sigma(t)[\frac{(1-t^{p^j-1})tg^p}{1+tg^p} = {a_0}^e - a_0 + t{a_1}^e + t^2{a_2}^e + ... + t^{e-1}{a_{e-1}}^e]$.*

Από το Λήμμα 2 το σύνολο των p^n-οστών δύνάμεων του t για όλα τα $n \in \mathbb{N}$,(άρα και για τα $n \in \mathbb{N}$, με $n \neq 0$) είναι διοφαντικό.Έτσι,από το Λήμμα 5 το σύνολο των $g \in \Sigma(t)$ για τα οποία $ord_t g \geq 0$ είναι διοφαντικό,αφού η συνθήκη " υπάρχει $j \in \mathbb{N}, j \neq 0$ ώστε $f = t^{p^j-1}$" είναι διοφαντική και το $\Sigma(t)$ δεν είναι αλγεβρικά κλειστό,οπότε τα θετικά υπαρξιακά υποσύνολά του είναι διοφαντικά.Από το Λήμμα 4 τώρα,η διμελής σχέση P με $P(g_1, g_2) \longleftrightarrow \exists j \in \mathbb{N}[g_2 = g_1^{p^j}]$ είναι επίσης διοφαντική.Παρατηρούμε τώρα ότι $\exists j \in \mathbb{N}(ord_t g_2 = p^j ord_t g_1) \longleftrightarrow \exists m \in \Sigma(t) \exists j \in \mathbb{N}[m = {g_1}^{p^j} \wedge ord_t m = ord_t g_2] \longleftrightarrow \exists m \in \Sigma(t) \exists j \in \mathbb{N}[m = {g_1}^{p^j} \wedge ord_t(\frac{g_2}{m}) \geq 0 \wedge ord_t(\frac{m}{g_2}) \geq 0]$. Άρα η συνθήκη $\exists j \in \mathbb{N}(ord_t g_2 = p^j ord_t g_1)$ είναι διοφαντική. Αρκεί λοιπόν να αντιστοιχήσουμε τον τυχόντα ακέραιο c με το σύνολο των στοιχείων του $\Sigma(t)$ με τάξη c.Η πρόσθεση στο $\mathbb{Z}$ αντιστοιχεί ακριβώς με τον πολλαπλασιασμό στο $\Sigma(t)$ υπό την έννοια ότι $ord_t(g_1 g_2) = ord_t g_1 + ord_t g_2$, η σχέση $\geq$ αντιστοιχεί στη διοφαντική σχέση $ord_t(\frac{g_1}{g_2}) \geq 0$ και η σχέση $|_p$ στην $\exists j \in \mathbb{N}(ord_t g_2 = p^j ord_t g_1)$.Είναι τώρα προφανές ότι αν υπάρχει αλγόριθμος που να αποφασίζει αν η τυχούσα δοφαντική πρόταση στο $\Sigma(t)$ αληθεύει,τότε υπάρχει αντίστοιχος και για τον δακτύλιο $\mathbb{Z}$ στη γλώσσα L',κάτι που είναι άτοπο.(Βλέπε και παρακάτω, τον ορισμό των διοφαντικών μοντέλων:Εδώ ουσιαστικά έχουμε πάρει ως διοφαντικό μοντέλο του $\mathbb{Z}$ το σύνολο των κλάσεων ισοδυναμίας του $\Sigma(t)$ ως προς τη σχέση της ισότητας των τάξεων στο t.)

Θα αποδείξουμε τώρα τα 4 Λήμματα.

Απόδειξη του Λήμματος 2 Έστω ότι υπάρχει $n \in \mathbb{N}$ ώστε $g = t^{p^n}$.Αν $n = 0$ η συνθήκη ισχύει για $a = b = 0$.Αν $n \neq 0$ τότε αρκεί να πάρουμε $a = t^{p^{n-1}} + t^{p^{n-2}} + \cdots + t, b = t^{-p^{n-1}} + t^{-p^{n-2}} + \cdots + t^{-1}$,αφού μπορεί εύκολα κανείς να δείξει,λαμβάνοντας υπ'οψιν απλές ιδιότητες των πράξεων μεταξύ πολυωνύμων και την ιδιότητα της χαρακτηριστικής,ότι

$$t^{p^n} - t = (t^{p^{n-1}} + t^{p^{n-2}} + \cdots + t)^p - (t^{p^{n-1}} + t^{p^{n-2}} + \cdots + t)$$

και

$$t^{-p^n} - t^{-1} = (t^{-p^{n-1}} + t^{-p^{n-2}} + \cdots + t^{-1})^p - (t^{-p^{n-1}} + t^{-p^{n-2}} + \cdots + t^{-1}).$$

Για το αντίστροφο:έστω ότι υπάρχουν $a, b \in \Sigma(t)$ ώστε

$$g - t = a^p - a \tag{20}$$
$$g^{-1} - t^{-1} = b^p - b. \tag{21}$$

Έστω επίσης $\bar{\Sigma}$ η αλγεβρική κλειστότητα του Σ.Θα αποδείξουμε κάτι ελαφρώς ισχυρότερο,ότι δηλαδή αν υπάρχουν $a, b \in \bar{\Sigma}(t)$ ώστε $g - t = a^p - a$ και$g^{-1} - t^{-1} = b^p - b$,τότε το g είναι p^n-οστή δύναμη του t για κάποιο $n \in \mathbb{N}$. Διακρίνουμε δύο περιπτώσεις:

α)Υπάρχει κάποιο $d \in \bar{\Sigma}(t)$ ώστε $g = d^p$.Τότε $d - t = (a-d)^p - (a-d)$ και $d^{-1} - t^{-1} = (b - d^{-1})^p - (b - d^{-1})$.Αν το d είναι επίσης p-οστή δύναμη,μπορούμε να εφαρμόσουμε την ίδια μέθοδο κτλ.,ενώ αν μπορούμε να δείξουμε ότι για κάποιο $n \in \mathbb{N}$ $d = t^{p^n}$,τότε $g = t^{p^{n+1}}$.Έτσι αρκεί να εξετάσουμε την αντίθετη περίπτωση:

β)Δεν υπάρχει κάποιο $d \in \bar{\Sigma}(t)$ ώστε $g = d^p$.Θα μετρήσουμε τώρα την πολλαπλότητα των ριζών του g. Έστω ότι $a = \frac{a_1}{a_2}$. Τότε $a^p - a = \frac{{a_1}^p - a_1 a_2^{p-1}}{a_2^p}$,δηλ.κάθε πόλος του $a^p - a = g - t$,άρα και του g έχει πολλαπλότητα ένα πολλαπλάσιο του p.Από την εξίσωση (21) συνεπάγεται ότι κάθε ρίζα του g εκτός από το 0(που είναι πόλος του t^{-1}) έχει πολλαπλότητα κάποιο πολλαπλάσιο του p.Τελικά το g δεν μπορεί παρά να είναι της μορφής

$$g = d^p t^i \tag{22}$$

για κάποιο $d \in \bar{\Sigma}(t)$ και κάποιο $i \in \mathbb{N}$. Έστω τώρα ότι $b = \frac{b_1}{b_2}$,με τα $b_1, b_2 \in \bar{\Sigma}[t]$ πρώτα μεταξύ τους.Από την (21) έχουμε ότι $g^{-1} = \frac{t({b_1}^p - b_1 {b_2}^{p-1}) - {b_2}^p}{t b_2^p}$.Αν το t δεν διαιρεί το b_2,τότε δεν μπορεί και να διαιρεί τον αριθμητή του κλάσματος $\frac{t({b_1}^p - b_1 {b_2}^{p-1}) - {b_2}^p}{t b_2^p}$,άρα το t είναι ρίζα πολλαπλότητας 1 του g.Αν το t είναι ρίζα πολλαπλότητας q του b_2,τότε είναι ρίζα πολλαπλότητας ακριβώς 1 του αριθμητή του κλάσματος αυτού(επειδή δεν μπορεί να διαιρεί το b_1) και άρα είναι ρίζα πολλαπλότητας qp του g.Άρα το i στην (22) είναι ή 1 ή πολλαπλάσιο του p.Η τελευταία περίπτωση αποκλείεται,αφού το g δεν είναι p-οστή δύναμη..Έτσι τελικά $g = d^p t$ για κάποιο $d \in \bar{\Sigma}(t)$.Μένει να δείξουμε ότι $d = 1$.Ισχύουν:

$$(d-1)^p = d^p - 1 \Longrightarrow g - t = t((d-1)^p) \Longrightarrow t((d-1)^p) = a^p - a. \tag{23}$$

Έστω τώρα $d - 1 = \frac{u_1}{u_2}, a = \frac{v_1}{v_2}$ με $u_1, u_2, v_1, v_2 \in \bar{\Sigma}[t]$ ώστε τα u_1, u_2 να είναι πρώτα μεταξύ τους,τα v_1, v_2 επίσης και τα u_2, v_2 να είναι μονικά πολυώνυμα.Άν το

t διαιρεί το u_2 και $g \neq t$ οδηγούμαστε σε άτοπο,αφού αυτό σημαίνει ότι το 0 είναι πόλος του $g-t$,άρα και του g,οπότε επειδή $g-t=a^p-a \Longrightarrow g=a^p-a+t \Longrightarrow d^pt=\frac{a_1{}^p-a_1a_2^{p-1}+ta_2{}^p}{a_2{}^p}$ το 0 είναι πόλος του g με πολλαπλότητα πολλαπλάσιο του p,κάτι που είναι άτοπο,ακριβώς από την (22).Έστω λοιπόν ότι το t δεν διαιρεί το u_2.Από την (23) παίρνουμε

$$\frac{tu_1{}^p}{u_2{}^p}=\frac{(v_1{}^p-v_1v_2{}^{p-1})}{v_2{}^p} \tag{24}$$

Είναι εύκολο τώρα να δούμε ότι και στις δύο πλευρές της (24) αριθμητές και παρανομαστές είναι πρώτοι μεταξύ τους και οι παρανομαστές είναι μονικά πολυώνυμα.(Αν π.χ κάποιο ανάγωγο πολυώνυμο στο $\bar{\Sigma}[t]$ διαιρεί το $(v_1{}^p-v_1v_2{}^{p-1})$ και το $v_2{}^p$ τότε διαιρεί το v_2 και το v_1,άτοπο, ή το v_2 και $v_1{}^{p-1}-v_2{}^{p-1}$,δηλαδή το v_2 και το v_1,άτοπο.)Ισχύει δηλαδή $u_2=v_2$ και

$$tu_1{}^p=v_1{}^p-v_1v_2{}^{p-1}. \tag{25}$$

Από την τελευταία αυτή εξίσωση μπορούμε να συμπεράνουμε ότι το $v_2{}^{p-1}$ διαιρεί το $tu_1{}^p-v_1{}^p$ και επειδή $p-1 \geq 2$(εδώ χρησιμοποιείται ουσιαστικά το ότι η χαρακτηριστική είναι $\neq 2$) μπορούμε επίσης να συμπεράνουμε ότι το v_2 διαιρεί την τυπική παράγωγο ως προς t του $tu_1{}^p-v_1{}^p$.Υπολογίζοντας την παράγωγο αυτή παρατηρούμε ότι ισούται με $u_1{}^p$,αφού οι p-οστές δυνάμεις παραγωγιζόμενες δίνουν πολλαπλάσια του p,δηλαδή 0.Έχουμε τώρα ότι το $v_2=u_2$ διαιρεί το $u_1{}^p$ και ότι τα u_1,u_2 είναι πρώτα μεταξύ τους.Μπορούμε να συμπεράνουμε ότι το u_2 είναι σταθερό και αφού είναι και μονικό,$u_2=1$.

Από την (25) παίρνουμε $tu_1{}^p=v_1{}^p-v_1$. Εξετάζοντας τώρα την παραπάνω εξίσωση βλέπουμε ότι αν $u_1 \neq 0$ το πολυώνυμο $tu_1{}^p$ έχει βαθμό $\equiv 1(mod\, p)$ ενώ το $v_1{}^p-v_1$ έχει βαθμό $\equiv 0(mod\, p)$.Άρα πρέπει $u_1=0$,δηλ. $d=1$,που είναι το ζητούμενο.

Απόδειξη του Λήμματος 3

Γράφουμε το g ως πηλίκο πρώτων μεταξύ τους $g_1,g_2 \in \bar{\Sigma}[t]$: $g=\frac{g_1}{g_2}$.Έστω τώρα r μια διπλή ρίζα του a.Τότε το $(t-r)^2$ διαιρεί τον αριθμητή του $a=\frac{g_1{}^p+tg_2{}^p}{g_1{}^p-tg_2{}^p}$,οπότε το $(t-r)$ διαιρεί την τυπική παράγωγο του $g_1{}^p+tg_2{}^p$,δηλ.το $g_2{}^p$,οπότε και το g_2.Τελικά το $(t-r)$ πρέπει να διαιρεί το $g_1{}^p$,οπότε και το g_1.Αλλά τα g_1,g_2 είναι πρώτα μεταξύ τους,οπότε οδηγούμαστε σε άτοπο.Ουσιαστικά το ίδιο επιχείρημα δείχνει ότι το a δεν μπορεί να έχει ούτε διπλούς πόλους.

Απόδειξη του Λήμματος 4

Κατάρχήν, αν $g_2=g_1{}^{p^{j+1}}$,τότε

$a^{p^j}=\frac{(g_1{}^p+t)^{p^j}}{(g_2{}^p-t)^{p^j}}=\frac{g_1{}^{p^{j+1}}+t^{p^j}}{g_1{}^{p^{j+1}}-t^{p^j}}=\frac{g_2+t^{p^j}}{g^p-t^{p^j}}=b$. Είναι εύκολο να δούμε ότι ισχύει και το αντίστροφο,δηλ.αν $a^{p^j}=b$ τότε $g_2=g_1{}^{p^{j+1}}$, οπότε μπορούμε για τις ανάγκες της απόδειξης να χειριζόμαστε τη συνθήκη $a^{p^j}=b$. Έστω τώρα ότι $a^{p^j}=b$.Τότε $b^2=(a^2)^{p^j},b^2t^{p^j}=(a^2t)^{p^j}$.Μπορούμε λοιπόν να επικαλεστούμε τα επιχειρήματα της απόδειξης του Λήμματος 2,αφού έχουμε στοιχεία που είναι p^j-οστές δυνάμεις άλλων,και να δείξουμε ότι υπάρχουν $d_1,d_2,d_3,d_4,d_5 \in \Sigma(t)$ που ικανοποιούν τις σχέσεις (15) έως (19).

Για το αντίστροφο:

Έστω $\bar{\Sigma}(t)$ η αλγεβρική κλειστότητα του Σ.Όπως και για το Λήμμα 2,θα αποδείξουμε κάτι ελαφρώς ισχυρότερο,ότι δηλαδή αν υπάρχουν $d_1, d_2, d_3, d_4, d_5 \in \bar{\Sigma}(t)$ που ικανοποιούν τις σχέσεις (15) έως (19),τότε $g_2 = {g_1}^{p^{j+1}}$. Έστω κατάρχήν ότι $j = 0$.Από την (17) και την (15) παίρνουμε

$$t(d_1^p - d_1) = d_3^p - d_3. \tag{26}$$

Έστω ότι $d_1 = t^e \frac{k}{l}$ και $d_3 = t^f \frac{m}{n}, k, l, m, n \in \bar{\Sigma}[t],\ e, f \in \mathbb{Z}$, το t δεν διαιρεί κανένα από τα k, l, m, n,τα k, l όπως και τα m, n είναι πρώτα μεταξύ τους και τα l, n είναι μονικά.Από την (26) έπεται ότι $\frac{t(t^{pe}k^p - t^e k l^{p-1})}{l^p} = \frac{t^{pf}m^p - t^f m n^{p-1}}{n^p}$.Είναι εύκολο να δει κανείς ότι στα παραπάνω κλάσματα αριθμητές και παρονομαστές είναι πρώτοι μεταξύ τους,ενώ οι παρονοματές είναι μονικά πολυώνυμα.Πρέπει λοιπόν να ισχύει $l = n$ και

$$t(t^{pe}k^p - t^e k l^{p-1}) = t^{pf}m^p - t^f m l^{p-1}. \tag{27}$$

Εξετάζουμε τώρα τις δύο πλευρές της (27) όσον αφορά την τάξη τους στο t για να βρούμε τα πρόσημα των e και f. Είναι εύκολο να υπολογίσουμε ότι αν $e < 0$, τότε $ord_t[t(t^{pe}k^p - t^e k l^{p-1})] = pe + 1 < 0$,οπότε αν $f \geq 0, ord_t[t^{pf}m^p - t^f m l^{p-1}] \geq 0$, άτοπο και αν $f < 0, ord_t[t^{pf}m^p - t^f m l^{p-1}] = pf$, δηλ.$pe + 1 = pf$, επίσης άτοπο. Άρα αναγκαστικά $e > 0$, δηλ. $ord_t[t(t^{pe}k^p - t^e k l^{p-1})] \geq 0$ και $f \geq 0$.

Μετά την παραπάνω παρατήρηση έχουμε φτάσει τώρα σε μια εξίσωση στο $\bar{\Sigma}[t]$:$l^{p-1}(t^f m - t^{e+1}k) = t^{pf}m^p - t^{pe+1}k^p$. Έτσι το l^{p-1} διαιρεί το $t^{pf}m^p - t^{pe+1}k^p$,και επειδή $p - 1 \geq 2$ μπορούμε να συμπεράνουμε ότι το l διαιρεί την τυπική παράγωγο του $t^{pf}m^p - t^{pe+1}k^p$, η οποία(ο υπολογισμός είναι παρόμοιος με εκείνον στην απόδειξη του Λήμματος 2) ισούται με $t^{pe}k^p$.Επειδή το (ανάγωγο) t δεν διαιρεί το l,το l πρέπει να διαιρεί το k^p·αλλά τα k, l είναι πρώτα μεταξύ τους,οπότε το l πρέπει να είναι κάποιο σταθερό πολυώνυμο,και αφού είναι μονικό,$l = 1$.

Η (27) γίνεται τώρα

$$t(t^{pe}k^p - t^e k) = t^{pf}m^p - t^f m. \tag{28}$$

Αν τα πολυώνυμα στα δύο μέλη της (28) είναι $\neq 0$ τότε ο βαθμός του $t(t^{pe}k^p - t^e k)$ είναι $\equiv 1 (mod\, p)$ ενώ του $t^{pf}m^p - t^f m \equiv 0 (mod\, p)$,κάτι που είναι άτοπο.Άρα $t(t^{pe}k^p - t^e k) = t^{pf}m^p - t^f m = 0$,δηλ.$k = m = 0$, άρα και $a^2 = b^2$,που συνεπάγεται ότι $a = -b$ ή $a = b$.

Έστω,προς απαγωγή σε άτοπο,ότι $a = -b$.Από την (19) παίρνουμε $2a = -(d_5^p - d_5)$.Επειδή τώρα από το Λήμμα 3 και την υπόθεση ξέρουμε ότι το $2a$ έχει μόνο απλούς πόλους ενώ με εύκολες πράξεις φαίνεται ότι το $-(d_5^p - d_5)$ έχει μόνο πόλους των οποίων η πολλάπλότητα είναι πολλαπλάσιο του p,συμπεραίνουμε ότι και τα δύο δεν έχουν κανένα πόλο,που σημαίνει ότι $a \in \bar{\Sigma}[t]$.Γράφουμε τώρα το g_1 ως πηλίκο $g_1 = \frac{h_1}{h_2}, h_1, h_2 \in \bar{\Sigma}[t]$ όπου τα h_1, h_2 είναι πρώτα μεταξύ τους και το h_2 μονικό.Έχουμε τώρα: $a = \frac{{h_1}^p + t{h_2}^p}{{h_1}^p - t{h_2}^p}$.Έστω ένας κοινός διαρέτης των ${h_1}^p + t{h_2}^p, {h_1}^p - t{h_2}^p$.Αυτός πρέπει να διαιρεί τα αθροίσματα και τις διαφορές τους,δηλ.τα $2{h_1}^p, 2t{h_2}^p (\neq 0$ επειδή η χαρακτηριστική δεν είναι 2,κάτι που χρησιμοποιείται άλλη μία φορά)και άρα μπορεί να είναι μόνο το t,αλλιώς τα ${h_1}^p + t{h_2}^p, {h_1}^p - t{h_2}^p$ είναι πρώτα μεταξύ τους.Αν το t τα διαιρεί,τότε το

$\frac{h_1{}^p - th_2{}^p}{t}$ είναι παρονομαστής σε μια γραφή του a στην οποία αριθμητής και παρονομαστής είναι πρώτοι μεταξύ τους.Όμως,επειδή το t διαιρεί το h_1 ο βαθμός του $\frac{h_1{}^p - th_2{}^p}{t}$ είναι τουλάχιστον $p-1$,δηλ. δεν είναι 0,οπότε $a \notin \bar{\Sigma}[t]$, άτοπο.Αν πάλι τα $h_1{}^p + th_2{}^p, h_1{}^p - th_2{}^p$ είναι πρώτα μεταξύ τους,τότε,επειδή $a \in \bar{\Sigma}[t]$, πρέπει $h_1{}^p - th_2{}^p = \sigma$ για κάποιο $\sigma \in \bar{\Sigma}$. Όμως επειδή το $\bar{\Sigma}$ είναι αλγεβρικά κλειστό,δηλ.υπάρχει σάυτό μια p-οστή ρίζα του σ,έστω σ', ισχύει $th_2{}^p = h_1{}^p - \sigma'^p = (h_1 - \sigma')^p$. Αφού το $th_2{}^p$ είναι p-οστή δύναμη,πρέπει $h_2 = 0$,άτοπο.

Τελικά $a = b$ και από την αρχική παρατήρηση που κάναμε έπεται ότι $g_1{}^p = g_2$.

Θα κάνουμε επαγωγή στο j. Έστω ότι το Λήμμα ισχύει για το $j-1 \geq 0$.

Αν το g_2 είναι p-οστή δύναμη κάποιου $c \in \bar{\Sigma}(t)$ τότε και το b είναι p-οστή δύναμη,και συγκεκριμένα του $d = \frac{c+t^{p^{j-1}}}{c-t^{p^{j-1}}}$. Συμπεραίνουμε ότι:

1. $(d_1 - d^2)^p - (d_1 - d^2) = d_1{}^p - d^{p2} - d_1 + d^2 =$(από την15)$d^2 - a^2$
2. $(d_2 - d^{-2})^p - (d_2 - d^{-2}) =$(όπως παραπάνω,από την 16)$d^{-2} - a^{-2}$
3. $(d_3 - d^2 t^{p^{j-1}})^p - (d_3 - d^2 t^{p^{j-1}}) =$ (όπως παραπάνω,από την 17)$d^2 t^{p^{j-1}} - a^2 t$
4. $(d_4 - d^{-2} t^{-p^{j-1}})^p - (d_4 - d^{-2} t^{-p^{j-1}})$(όπως παραπάνω,από την 18) $= d^{-2} t^{-p^{j-1}} - a^2 t^{-1}$
5. $(d_5 - d)^p - (d_5 - d) =$(όπως παραπάνω,από την 19)$d - a$

Από την επαγωγική υπόθεση,έπεται ότι $d = a^{p^{j-1}}$,άρα $b = a^{p^j}$,δηλ. και $g_2 = g_1{}^{p^{j+1}}$.

Μένει να δείξουμε ότι αν υποθέσουμε ότι $j \geq 0$ και ότι το g_2 δεν είναι p-οστή δύναμη,οδηγούμαστε σε άτοπο.Έστω ότι το b είναι p-οστή δύναμη,π.χ. $b = w^p$.Έχουμε τότε $\frac{g_2 + t^{p^j}}{g_2 - t^{p^j}} = b$.Αν $b = 1$ τότε $0 = 2t^{p^j}$,άτοπο επειδή $p \neq 2$.Αν $b = w^p \neq 1$, τότε $g_2 = \frac{-t^{p^j}(1+w^p)}{1-w^p} = \frac{(-t)^{p^j}(1+w)^p}{(1-w)^p}$,δηλ. το g_2 είναι p-οστή δύναμη,άτοπο,οπότε το b δεν είναι p-οστή δύναμη.Το επόμενο βήμα είναι να δειξουμε ότι όλοι οι πόλοι και οι ρίζες του b εκτός πιθανόν από το 0 έχουν πολλαπλότητα κάποιο πολλαπλάσιο του p.Έστω,προς άτοπο, s κάποιο πρώτο στοιχείο του $\bar{\Sigma}[t], s \neq t$ με $ord_s b < 0$ και $ord_s b \not\equiv 0 (mod\, p)$.Τότε,επειδή $p \neq 2$, $ord_s b^2 \not\equiv 0 (mod\, p)$. Παίρνουμε τώρα περιπτώσεις βασίζόμενοι στην (15).Από το Λήμμα 3 γνωρίζουμε ότι $ord_s a^2 = 0$,2 ή-2.Είναι εύκολο να δείξουμε ότι αν $ord_s d_1 < 0$, τότε η τάξη του $d_1{}^p - d_1$ στο s είναι αρνητικός αριθμός,πολλαπλάσιο του p,και σε κάθε περίπτωση ισούται με την τάξη στο s του $d_1{}^p - d_1 + a^2$, οπότε οδηγούμαστε σε άτοπο.Άρα η τάξη στο s του $d_1{}^p - d_1$ είναι θετικός αριθμός,οπότε $ord_s a^2 = ord_s b^2$ και τελικά $ord_s a = ord_s b = -1$ και $ord_s(d_1^p - d_1) \geq 0$. Με τα ίδια επιχειρήματα μπορούμε να συμπεράνουμε από την (17) ότι $ord_s(d_3^p - d_3) \geq 0$.Συνδυάζοντας τα παραπάνω συμπεράσματα με τις (15) και (17) παίρνουμε:$ord_s[b^2(t^{p^j})] = ord_s[d_3^p - d^3 - t(d_1^p - d_1)] \geq 0$.Επειδή λοιπόν $ord_s[b^2(t^{p^j})] =\geq 0$ και $ord_s b = -1$,πρέπει να ισχύει $ord_s[t^{p^j} - t] \geq 2$.Αφού λοιπόν το s^2 διαιρεί το $t^{p^j} - t$ στο $\bar{\Sigma}[t]$,το s διαιρεί την τυπική παράγωγο του $t^{p^j} - t$,η οποία,αφού $j \neq 0$,είναι -1,άτοπο.Με εντελώς όμοιο τρόπο,βασιζόμενοι στις (16) και (18) καταλήγουμε σε άτοπο αν υποθέσουμε ότι υπάρχει s πρώτο στοιχείο του $\bar{\Sigma}[t], s \neq t$ με $ord_s b > 0$ και $ord_s b \not\equiv 0 (mod\, p)$.

Δείξαμε ότι

$$b = z^p t^e \tag{29}$$

για κάποιο $z \in \bar{\Sigma}(t)$ και $e \in \mathbb{Z}$, όπου το t δεν διαιρεί το z. Είναι προφανές ότι $ord_t a = 0$.Αν $e < 0$,από την (15) ενώ αν $e > 0$ από την (16),με υπολογισμούς όπως παραπάνω,συμπεραίνουμε ότι το p διαιρεί το j.Σε κάθε περίπτωση από την (29) το b είναι p-οστή δύναμη,άτοπο.

Απόδειξη του Λήμματος 5

Έστω κατάρχήν ότι $\exists a_0, ...a_{r-1} \in \Sigma(t)[\frac{(1-t^{p^j-1})tg^p}{1+tg^p} = {a_0}^e - a_0 + t{a_1}^e + t^2{a_2}^e + ... + t^{e-1}{a_{e-1}}^e]$ Είναι γνωστό ότι μπορούμε να γράψουμε το

$${a_0}^e - a_0 + t{a_1}^e + t^2{a_2}^e + ... + t^{e-1}{a_{e-1}}^e \tag{30}$$

με μοναδικό τρόπο ως $\sum_{s=-\infty}^{+\infty} c_s t^s$ για $c_s \in \Sigma$, $s \in \mathbb{Z}$ (σειρά Laurent) .

Θα υπολογίσουμε το c_0,δηλ. το σταθερό όρο.Με τρόπο παρόμοιο μ' αυτούς που είδαμε παραπάνω,για κάθε $a \in \Sigma(t)$)(το βλέπουμε τώρα ως σειρά Laurent),επειδή το e είναι πολλαπλάσιο του p, το a^e είναι άθροισμα μονωνύμων της μορφής $l_s t^{es}$.Έτσι,όταν $1 \leq i \leq e-1$ το μονώνυμο βαθμού $-i$ στο a^e έχει συντελεστή 0,δηλ.ο σταθερός όρος του $t^i a^e$ είναι 0.Επίσης,επειδή η πολλαπλασιαστική ομάδα κάθε πεπερασμένου σώματος είναι κυκλική,και άρα για κάθε $\sigma \in \Sigma, \sigma^e = \sigma$ ο σταθερός όρος του ${a_0}^e$ είναι ίσος με τον σταθερό όρο του a_0.Τελικά $c_0 = 0$.Επίσης μπορούμε να δούμε το $\frac{(1-t^{p^j-1})tg^p}{1+tg^p}$ ως σειρά Laurentτης οποίας ο σταθερός όρος πρέεπει να είναι ίσος με 0.Αν $ord_t g = u < 0$, είναι εύκολο να υπολογίσουμε ότι $ord_t[\frac{(1-t^{p^j i-1})tg^p}{1+tg^p}] = 0$, που σημαίνει ότι ο σταθερός όρος του $\frac{(1-t^{p^j-1})tg^p}{1+tg^p}$ δεν είναι 0.Άρα πρέπει $ord_t g \geq 0$,που ήταν και το ζητούμενο.

Για το αντίστροφο:Έστω ότι $ord_t g \geq 0$.Παρατηρούμε κατάρχήν ότι $\frac{1-tg^p}{1+tg^p} = \frac{g^{-p}-t}{g^{-p}+t}$,οπότε από το Λήμμα 3 το $\frac{1-tg^p}{1+tg^p}$ έχει μόνο απλούς πόλους,άρα και το $1 - \frac{1-tg^p}{1+tg^p} = \frac{2tg^p}{1+tg^p}$, δηλ. και το $\frac{tg^p}{1+tg^p}$ έχει μόνο απλούς πόλους.Έιναι τώρα εύκολο να δει κανείς ότι $ord_t[\frac{tg^p}{1+tg^p}] > 0$ και άρα,αν γράψουμε $\frac{tg^p}{1+tg^p} = \frac{u_1}{u_2}$ όπου $u_1, u_2 \in \Sigma[t]$ και τα u_1, u_2 είναι πρώτα μεταξύ τους,το u_2 είναι ένα πολυώνυμο που έχει μόνο απλές ρίζες και δεν διαιρείται από το t.

Ισχυριζόμαστε τώρα ότι υπάρχει κάποιο $j \in \mathbb{N}, j \neq 0$ ώστε το u_2 να διαιρεί το t^{p^j-1} στο $\Sigma[t]$.Η απόδειξη του ισχυρισμού αυτού στηρίζεται στις ιδιότητες του δακτυλίου-πηλίκο $\Sigma[t]/< u_2 >$,όπου $< u_2 >$ το ιδεώδες που παράγεται από το u_2.Ο δακτύλιος αυτός είναι πεπερασμένος[7]και άρα υπάρχουν φυσικοί αριθμοί $n_1 > n_2$ ώστε τα t^{n_1}, t^{n_2} να ανήκουν στο ίδιο στοιχείο του·με άλλα λόγια υπάρχουν $n_1 > n_2$ ώστε το u_2 να διαιρεί τη διαφορά $t^{n_1} - t^{n_2}$ στο $\Sigma[t]$.Επειδή το u_2 δεν διαιρεί το t,το u_2 διαιρεί το $t^{n_1-n_2} - 1$ στο $\Sigma[t]$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι το $n_1 - n_2$ δεν είναι πολλαπλάσιο του p.[8]Επειδή τώρα το p είναι πρώτος,είναι αντιστρέψιμο στοιχείο του δακτυλίου $\mathbb{Z}/(n_1 - n_2)$.Έτσι υπάρχει $j \in \mathbb{N}, j \neq 0$ ώστε $p^j \equiv 1(mod\, n_1 - n_2)$ δηλ.ώστε το $n_1 - n_2$ να διαιρεί το $p^j - 1$.Εύκολα βλέπουμε τώρα ότι και το $t^{n_1-n_2} - 1$ διαιρεί το $t^{p^j-1} - 1$.Τελικά το

[7]Η απόδειξη στηρίζεται στις στοιχειώδεις ιδιότητες του Σ και είναι μάλλον απλή,αλλά θα την παραλείψουμε.

[8]Αν $n_1 - n_2 = wp$ τότε το u_2 διαιρεί το $t^{wp} - 1 = (t^w - 1)^p$.Αφού το u_2 δεν έχει διπλές ρίζες έπεται ότι διαιρεί και το $t^w - 1$.

u_2 διαιρεί το $t^{p^j-1} - 1$ και μπορούμε να συμπεράνουμε ότι το $\frac{(1-t^{p^j-1})tg^p}{1+tg^p}$ είναι ένα πολυώνυμο στο $\Sigma[t]$ που διαιρείται από το t.

Αρκεί να αποδείξουμε ότι οποιοδήποτε πολυώνυμο στο $\Sigma[t]$, αν διαιρείται από το t, γράφεται στη μορφή $a_0{}^e - a_0 + ta_1{}^e + t^2a_2{}^e + ... + t^{e-1}a_{e-1}{}^e$ για κάποια $a_0, ...a_{e_1} \in \Sigma[t]$.Με επαγώγή στο βαθμό του πολυωνύμου.Αν ο βαθμός του είναι 0 ή το πολυώνυμο είναι το μηδενικό τότε το ζητούμενο είναι προφανές. Το $\Sigma[t]$ είναι ελεύθερο πρότυπο διάστασης e επί του $\Sigma[t^e]$, με βάση το σύνολο $\{1, t, \dots, t^{e-1}\}$.Άρα το $\frac{(1-t^{p^j-1})tg^p}{1+tg^p}$ γράφεται $\frac{(1-t^{p^j-1})tg^p}{1+tg^p} = q_0 + \dots + q_{e-1}t^{e-1}$ για κάποια $q_0, \dots, q_{e-1} \in \Sigma[t^e]$Όμως,επειδή,όπως παρατηρήσαμε παραπάνω,για κάθε $\sigma \in \Sigma, \sigma^e = \sigma$ κάθε στοιχείο του $\Sigma[t^e]$ είναι e-οστή δύναμη κάποιου στοιχείου του $\Sigma[t]$.Έτσι τελικά έχουμε

$$\frac{(1-t^{p^j-1})tg^p}{1+tg^p} = l_0{}^e + l_1{}^e t + \dots + l_{e-1}^e t^{e-1} \tag{31}$$

για κάποια $l_0, \dots, l_{e-1} \in \Sigma[t]$.Αν $l_0 = 0$, τελειώσαμε.Αν όχι,τότε παρατηρούμε ότι,επειδή το t διαιρεί το l_0,το τελευταίο έχει βαθμό τουλάχιστον 1 και ο μεγιστοβάθμιος όρος του l_0^e έχει βαθμό κάποιο πολλαπλάσιο του e.Επειδή παρατηρούμε και ότι κανένα άλλο μονώνυμο που εμφανίζεται στο $l_1{}^e t + \dots + l_{e-1}^e t^{e-1}$ δεν μπορεί να έχει βαθμό πολλαπλάσιο του e, καταλήγουμε στο συμπέρασμα ότι το $\frac{(1-t^{p^j-1})tg^p}{1+tg^p}$ έχει βαθμό γνησίως μεγαλύτερο του βαθμού του l_0.Έτσι για το l_0 ισχύει η επαγωγική υπόθεση,δηλ.το l_0 γράφεται:

$$l_0 = z_0{}^e - z_0 + tz_1{}^e + t^2z_2{}^e + ... + t^{e-1}z_{e-1}{}^e, \tag{32}$$

και τελικά συνδυάζοντας τις (31) και (32) παίρνουμε το ζητούμενο,αφού

$$\frac{(1-t^{p^j-1})tg^p}{1+tg^p} =$$

$$(l_0 + z_0)^e - (l_0 + z_0) + t(l_1 + z_1)^e + t^2(l_2 + z_2)^e + ... + t^{e-1}(l_{e-1} + z_{e-1})^e.$$

4 Το αντίστοιχο του ΔΠΧ για τους ρητούς

4.1 Δύο αντίθετες κατευθύνσεις

Παρόλο που το αντίστοιχο του ΔΠΧ για διάφορους δακτυλίους και σώματα έχει λυθεί,το σημαντικότερο τέτοιου τύπου ερώτημα μένει ανοικτό:υπάρχει αλγόριθμος που να αποφασίζει αν τυχούσα υπαρξιακή πρόταση αληθεύει στο $\mathbb{Q}$; Σε όσες περιπτώσεις (γνωστές τουλάχιστον σε μας) δακτυλίων έχουν δοθεί ολοκληρωμένες λύσεις στις οποίες αποδεικνύεται η ανυπαρξία τέτοιου αλγορίθμου,η ραχοκοκκαλιά της απόδειξης είναι κάποιο τέχνασμα που επιτρέπει τον διοφαντικό ορισμό ενός αντιγράφου των ακεραίων μέσα στον εκάστοτε μελετούμενο δακτύλιο και η επίκληση στη συνέχεια του αποτελέσματος για το ΔΠΧ.Τα τεχνάσματα αυτά όμως είναι κάθε φορά διαφορετικά,και ακόμα και στην περίπτωση που εφαρμόζονται σε κάποιο σώμα ή σε κάποιο διαιρετικό δακτύλιο,[9] δομές που θα έλεγε κανείς ότι μοιάζουν με τους ρητούς,δεν γενικεύονται,τουλάχιστον όχι εύκολα. Το 1949 η Julia Robinson απέδειξε ότι (ολόκληρη) η θεωρία του $\mathbb{Q}$ δεν είναι αποφασίσιμη,βρίσκοντας έναν ορισμό του $\mathbb{Z}$ μέσα στο $\mathbb{Q}$.Ο ορισμός όμως αυτός, που βασιζόταν στην εφαρμογή κάποιων αποτελεσμάτων των Hasse και Minkowski από τη Θεωρία Αριθμών,δεν ήταν διοφαντικός,χρησιμοποιούσε δηλαδή καθολικούς ποσοδείκτες με ουσιαστικό τρόπο,οι οποίοι δεν στάθηκε δυνατό να εξαλειφθούν.Έτσι το ΔΠΧΡ,όπως θα συμβολίζουμε το πρόβλημα χάριν συντομίας, παραμένει ανοικτό.Τελευταία έχουν γίνει προσπάθειες από τον Θανάση Φειδά να δοθεί ένας διοφαντικός ορισμός του $\mathbb{Z}$ μέσα στο $\mathbb{Q}$ ή μάλλον,για να είμαστε ακριβέστεροι,ενός κατάλληλου "αντιγράφου" του $\mathbb{Z}$,οι οποίες χρησιμοποιούν τη Θεωρία των Ελλειπτικών Καμπύλων.Οι προσπάθειες αυτές αν ευοδώνονταν θα έλυναν,όπως θα δούμε,και το ΔΠΧΡ.Μένουν όμως ημιτελείς και επιπλέον το επιθυμητό αποτέλεσμά τους αντιφάσκει με μια εικασία που διατύπωσε ο Barry Mazur που αφορά την τοπολογία των αλγεβρικών πολλαπλοτήτων επί του $\mathbb{Q}$ και η οποία συνεπάγεται ότι δεν μπορεί να υπάρχει διοφαντικός ορισμός του $\mathbb{Z}$ μέσα στο $\mathbb{Q}$.Τις δύο αυτές αντίθετες κατευθύνσεις για τη λύση του ΔΠΧΡ θα εξετάσουμε στα επόμενα.

4.2 Η εικασία του Mazur

Στις αρχές της δεκαετίας του 1990 ο Barry Mazur διατύπωσε κάποιες εικασίες για αλγεβρικές πολλαπλότητες επί του $\mathbb{Q}$.Κάποιες από αυτές χρειάστηκε να τροποποιηθούν ελαφρά εξαιτίας κάποιων αντιπαραδειγμάτων που βρέθηκαν,αυτή όμως που μας ενδιαφέρει εδώ ακόμα δεν έχει χρειαστεί να τροποποιηθεί αλλά ούτε και έχει αποδειχθεί:

Εικασία 1 *Έστω V μια αλγεβρική πολλαπλότητα*[10] *επί του $\mathbb{Q}$.Η τοπολογική κλειστότητα της $V(\mathbb{Q})$ στην $V(\mathbb{R})$ (με τον περιορισμό της συνήθους τοπολογίας από την κατάλληλη δύναμη του $\mathbb{R}$) έχει πεπερασμένο πλήθος συνεκτικών συνιστωσών.*

Η εικασία είναι γνωστό ότι ισχύει για κάποιες συγκεκριμένες πολλαπλότητες,π.χ.τις καμπύλες,αλλά θα παραλείψουμε την απόδειξη. Ο Mazur παρατήρησε ότι αν η

[9] Ένας δακτύλιος R λέγεται διαιρετικός όταν για κάθε $r \in R$ και κάθε $n \in \mathbb{N}$ υπάρχει κάποιο $r' \in R$ ώστε $nr' = r$

[10] (Αλγεβρική) πολλαπλότητα V επί ενός σώματος K ή $V(K)$ ονομάζεται το σύνολο κοινών λύσεων ενός συνόλου πολυωνυμικών εξισώσεων V στις οποίες οι άγνωστοι παίρνουν τιμές στο K

εικασία 1 ισχύει τότε το $\mathbb{Z}$ δεν είναι διοφαντικό στο $\mathbb{Q}$:Αν το $\mathbb{Z}$ ήταν διοφαντικό,θα ήταν η προβολή του $V(\mathbb{Q})$ για κάποια εξίσωση V.Όμως η προβολή αυτή είναι συνεχής και προφανώς η $V(\mathbb{Q})$ είναι πυκνή στην κλειστότητά της,οπότε έχουμε μια συνεχή συνάρτηση από ένα τοπολογικό χώρο που, αν ισχύει η εικασία,έχει πεπερασμένες το πλήθος συνεκτικές συνιστώσες στο $\mathbb{Z}$ που έχει άπειρες το πλήθος συνεκτικές συνιστώσες,κάτι που είναι άτοπο. Μήπως παρ' ολ' αυτά θα μπορούσαμε να βρούμε κάποιο διοφαντικό "αντίγραφο" του $\mathbb{Z}$;Η απάντηση είναι αρνητική,όπως θα δείξουμε αφού δώσουμε τον κατάλληλο ορισμό.

Ορισμός 5 *Ο δακτύλιος R_1 επιδέχεται ενός διοφαντικού μοντέλου D στον δακτύλιο R_2 εάν υπάρχει κάποιο $n \in \mathbb{N}$ και μία 1-1 συνάρτηση $f : R_1 \rightarrowtail {R_2}^n$ ούτως ώστε αν $G_+ \subseteq R_1^3$ και $G_. \subseteq R_1^3$ είναι τα γραφήματα της πρόσθεσης και του πολλαπλασιασμού αντίστοιχα και $f_3 : {R_1}^3 \longrightarrow {R_2}^{3n}$ η συνάρτηση που ορίζεται φυσιολογικά από την f (δηλ. $f_3(a_1, a_2, a_3) = (f(a_1), f(a_2), f(a_3))$) ,$f(R_1) = D$ και οι εικόνες $f(R_1) = D, f(0), f(1)$ καθώς και οι $f_3(G_+)$, $f_3(G_.)$ να είναι διοφαντικά σύνολα.*

Λήμμα 6 *Αν ο δακτύλιος $\mathbb{Z}$ των ακεραίων επιδέχεται διοφαντικού μοντέλου στον δακτύλιο $\mathbb{Q}$ των ρητών τότε δεν υπάρχει αλγόριδμος που να αποτελεί λύση για το ΔΠΧΡ.*

Απόδειξη

Έστω ότι υπήρχε ένας τέτοιος αλγόριθμος,ένα διοφαντικό μοντέλο D και συναρτήσεις f, f_3 όπως στον ορισμό 5.Αρκεί να •δείξουμε πώς η επιλυσιμότητα τυχόντος πολυωνύμου στους ακεραίους μπορεί να αναχθεί στην επιλυσιμότητα κάποιου πολυωνύμου στο δακτύλιο στον οποίο υπάρχει αυτό το διοφαντικό μοντέλο. Αντί πλήρους αποδείξεως (που γίνεται ουσιαστικά με επαγωγή στην πολυπλοκότητα του πολυωνύμου που θέλουμε να δούμε αν έχει ρίζες στο $\mathbb{Z}$) θα δώσουμε ένα παράδειγμα:

$$\exists x_1, x_2 \in \mathbb{Z}(x_1^2 + x_2^3 - 2 = 0) \Longleftrightarrow$$

$$\exists s_1, s_2, s_3, s_4, s_5, s_6, s_7 \in D[\langle s_1, s_2, s_3\rangle \in f_3(G_+) \;\&\; \langle s_4, s_4, s_1\rangle \in f_3(G_.) \;\&$$

$$\langle s_5, s_5, s_6\rangle \in f_3(G_.) \;\&\; \langle s_5, s_6, s_2\rangle \in f_3(G_.) \;\&\; s_7 \in d(1) \;\&\; \langle s_7, s_7, s_3\rangle \in d_3(G_+)]$$

όπου όλες οι συνθήκες που χρησιμοποιήσαμε είναι διοφαντικές αφού το D είναι διοφαντικό μοντέλο του $\mathbb{Z}$. Εντελως όμοια μπορεί κανείς για άλλον δακτύλιο να αποδείξει ανάλογο αποτέλεσμα,αν είναι γνωστό ότι η υπαρξιακή θεωρία του δεν είναι αποφασίσιμη.

Θεώρημα 2 *Από την εικασία 1 συνεπάγεται ο δακτύλιος $\mathbb{Z}$ δεν επιδέχεται διοφαντικού μοντέλου στον δακτύλιο $\mathbb{Q}$.*

Απόδειξη

Η απόδειξη ακολουθεί αυτήν των Cornelissen,Zahidi. Έστω ότι υπάρχει ένα τέτοιο μοντέλο $D \subseteq \mathbb{Q}^n$. Τότε υπάρχει μια 1-1 και επί συνάρτηση $d : \mathbb{Z} \longrightarrow D$ και μια διοφαντική εξίσωση $P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0$ ώστε$\forall \langle a_1, \ldots a_n\rangle \in \mathbb{Q}^n$

$$\langle a_1, \ldots a_n\rangle \in D \Longleftrightarrow \exists \langle x_1, \ldots, x_m\rangle \in \mathbb{Q}^m (P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0).$$

Θεωρούμε την αλγεβρική πολλαπλότητα $V(\mathbb{Q}) = \{\langle a_1, ...a_m, x_1, ...x_n\rangle \in \mathbb{Q}^{m+n} : P(a_1, ...a_m, x_1, ...x_n) = 0$ και ορίζουμε τη συνάρτηση προβολής $f : \mathbb{Q}^{m+n} \longrightarrow \mathbb{Q}^m$ όπου $f(a_1, ...a_m, x_1, ...x_n) = (a_1, ...a_m)$,η οποία είναι προφανώς συνεχής και επί.

Αν το D είναι τέτοιο ώστε η κλειστότητά του $\overline{D}$ (στο $\mathbb{R}^n$) να έχει άπειρες το πλήθος συνεκτικές συνιστώσες είναι εύκολο να δει κανείς ότι αν f' είναι η συνεχής επέκταση της f στην κλειστότητα $\overline{V(\mathbb{Q})}$ της $V(\mathbb{Q})$ στην $V(\mathbb{R})$ (δηλ. επίσης η συνάρτηση προβολής) τότε $D \subseteq f'(\overline{V(\mathbb{Q})}) \subseteq \overline{D}$,δηλ.πρέπει η $f'(\overline{V(\mathbb{Q})})$ και άρα η $(\overline{V(\mathbb{Q})})$ να έχει άπειρες το πλήθος συνεκτικές συνιστώσες, κάτι που αντιφάσκει με την εικασία 1.

Αν το D δεν έχει την ιδιότητα αυτή,θα δείξουμε ότι υπάρχει διοφαντικό υποσύνολο του D',που την έχει, και ουσιαστικά θα εφαρμόσουμε την παραπάνω απόδειξη στο D'.Από την εικασία 1 έπεται κατάρχήν ότι η $\overline{V(\mathbb{Q})}$ έχει πεπερασμένες το πλήθος συνεκτικές συνιστώσες. Επειδή τώρα η f' είναι συνεχής,η εικόνα $f'(\overline{V(\mathbb{Q})}$ έχει επίσης πεπερασμένες το πλήθος συνεκτικές συνιστώσες,και επειδή $D \subseteq f'(\overline{V(\mathbb{Q})}$,κάποια από αυτές,έστω η$D_0$ είναι άπειρη.Έτσι υπάρχει μια κατάλληλη προβολή $pr : \mathbb{R}^{m+n} \longrightarrow \mathbb{R}$ ούτως ώστε το $pr(D_0)$ να περιέχει ένα μη τετριμμένο διάστημα με ρητά άκρα,π.χ. $*a, b*$ όπου τα * μπορούν να είναι [,] ή (,). Με κατάλληλο συνεχή και 1-1 μετασχηματισμό t μπορούμε να πετύχουμε $a = 0, b = 1$ Παίρνουμε τώρα τη σύνθεση $t \circ pr \circ f'$ την οποία ονομάζουμε r.Έστω τώρα το εξής υποσύνολο των ακεραίων:

$$A = \{i \in \mathbb{Z} : \exists j \in \mathbb{N}[\frac{1}{2j+3} \leq r(d(n)) \leq \frac{1}{2j+2}]\}$$

Παρατηρούμε ότι η d είναι υπολογίσιμη συνάρτηση αφού,αν ξέρουμε το π.χ. το $d(1)$,επειδή η εικόνα μέσω της d_3,της επαγόμενης από την d συνάρτησης, του γραφήματος της πρόσθεσης είναι διοφαντική(βλ. τον ορισμό 5),μπορούμε να υπολογίσουμε το $d(2)$ στη συνέχεια το $d(3)$ κτλ.Επίσης οι προβολές f' και pr είναι προφανώς υπολογίσιμες και ακόμα επειδή διαλέξαμε τα a, b ρητούς μπορούμε να υποθέσουμε ότι ο μετασχηματισμός t είναι υπολογίσιμη συνάρτηση.Τελικά, αφού η σύνθεση όλων αυτών είναι υπολογίσιμη,από τον ορισμό του A φαίνεται ότι το A είναι αναδρομικά απαριθμήσιμο.Απο αυτό το τελευταίο συμπέρασμα σε συνδυασμό με την απάντηση που δόθηκε τελικά στο ΔΠΧ,έπεται ότι το A είναι διοφαντικό (στο $\mathbb{Z}$).

Έστω τώρα το $D' =_{o\rho} d(A)$. Το D' είναι διοφαντικό στο $\mathbb{Q}$,όπως επιδιώκαμε[11].Μπορούμε λοιπόν,όπως παραπάνω,να κατασκευάσουμε μια συνεχή και επί

[11]Ξαναγράφουμε ουσιαστικά όσα γράψαμε για το Λήμμα 6 χρησιμοποιώντας (αντί πλήρους απόδείξης) σχεδόν το ίδιο παράδειγμα για να διευκολύνουμε τη σύγκριση: Έστω ότι

$$\forall n \in \mathbb{Z}[n \in A \Longleftrightarrow \exists x_1, x_2 \in \mathbb{Z}(x_1^2 + x_2^3 - n - 2 = 0)].$$

Τότε $\forall c \in \mathbb{Q}^n$ ισχύει:

$$c \in D' \Longleftrightarrow \exists s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8 \in D$$

$$[\langle s_1, s_2, c\rangle \in d_3(G_+) \ \& \ \langle s_3, s_3, s_1\rangle \in d_3(G_.) \ \& \ \langle s_2, s_4, s_5\rangle \in d_3(G_+)$$

$$\& \ \langle s_6, s_6, s_4\rangle \in d_3(G_+) \ \& \ s_6 \in d(1) \ \& \ \langle s_7, s_7, s_8\rangle \in d_3(G_.) \ \& \ \langle s_7, s_8, s_5\rangle \in d_3(G_.)]$$

όπου όλες οι συνθήκες που χρησιμοποιήσαμε είναι διοφαντικές αφού το D είναι διοφαντικό μοντέλο του $\mathbb{Z}$.

συνάρτηση g από μια αλγεβρική πολλαπλότητα W επί του $\mathbb{Q}$ στο D'. Από το πώς κατασκευάστηκαν το A και το D' μπορούμε τώρα να συμπεράνουμε ότι για τη συνεχή επέκταση g' της g στην κλειστότητα (με την τοπολογία από την κατάλληλη καρτεσιανή δύναμη του $\mathbb{R}$) $\overline{W}$ της W ισχύει

$$r(g'(\overline{W})) \subseteq \{x \in [0,1] : \exists j \in \mathbb{N}\, [\frac{1}{2j+3} \leq x \leq \frac{1}{2j+2}]\}.$$

Όμως αφού το $r(D)$ είναι πυκνό στο $(0,1)$ για κάθε $j \geq 0$ υπάρχει $n \in A$ ώστε $\frac{1}{2j+3} \leq r(d(n)) \leq \frac{1}{2j+2}$,δηλαδή πρέπει η εικόνα $r(g'(\overline{W})$ να έχει άπειρες το πλήθος συνεκτικές συνιστώσες,κάτι που αντιφάσκει με την εικασία 1.

Πρέπει να σημειώσουμε εδώ ότι η ισχύς της εικασίας του Mazur, δεν συνεπάγεται ότι η υπαρξιακή θεωρία του $\mathbb{Q}$ είναι αποφασίσιμη,τουλάχιστον όχι κατά προφανή τρόπο·συνεπάγεται απλώς τη ματαιότητα κάθε προσπάθειας απόδειξης του αντιθέτου με τις γνωστές μεθόδους.Έτσι κατά κάποιο τρόπο αν αποδειχθεί η εικασία αυτή το ΔΠΧΡ θα μείνει ¨πιο ανοιχτό¨ από ποτέ.

4.3 Προς μια λύση του ΔΠΧΡ:Οι προσπάθειες του Θ.Φειδά

Οι προσπάθειες του Θ.Φειδά κινούνται τρόπον τινά προς την αντίθετη κατεύθυνση,εκείνη της εύρεσης ενός διοφαντικού μοντέλου του $\mathbb{Z}$ μέσα στο $\mathbb{Q}$.Στα επόμενα θα αναφερθούμε σε αυτές τις ημιτελείς ακόμα προσπάθειες:ακολουθώντας τον τρόπο έκθεσης του θέματος από τον ίδιο το Φειδά,θα μελετήσουμε παράλληλα το πρόβλημα για το $\mathbb{Q}$ και για σώματα ρητών συναρτήσεων επί ενός πεπερασμένου σώματος με χαρακτηριστική $\neq 2,3$.Το δεύτερο πρόβλημα,όπως αναφέραμε και παραπάνω,έχει λυθεί από το Φειδά το 1991 για πεπερασμένα σώματα χαρακτηριστικής > 2(απέδειξε ότι η υπαρξιακή θεωρία ενός τέτοιου σώματος είναι μη αποφασίσιμη). Η απόδειξή του όμως χρησιμοποιούσε τεχνικές βασισμένες στην ύπαρξη ενός υπερβατικού επί του πρώτου σώματος στοιχείου καθώς και στη χαρακτηριστική του σώματος των συντελεστών,οπότε η αντιμετώπισή του προβλήματος δεν ήταν ενιαία και δεν φάνηκε να οδηγεί σε λύση του προβλήματος για το $\mathbb{Q}$.Τα σώματα ρητών συναρτήσεων επί πεπερασμένου σώματος είναι δομή αρκετά συγγενής όσον αφορά τις ιδιότητές της με το $\mathbb{Q}$ και από αυτήν την άποψη είναι εύλογη η ελπίδα ότι μια ενιαία αντιμετώπιση του προβλήματος για αυτά τα σώματα θα οδηγήσει σε λύση του προβλήματος και για τους ρητούς.Και οι δύο προσπάθειες έχουν ακόμα κενά,τα οποία θα περιγράψουμε αναλυτικά στα επόμενα.

Η προτεινόμενη μέθοδος είναι η κατασκευή ενός αλγορίθμου που αντιστοιχεί με 1-1 τρόπο σε κάθε ακέραιο ένα σημείο μιας κατάλληλης (ελλειπτικής) καμπύλης με τρόπο ώστε οι εικόνες των γραφημάτων της πρόσθεσης και του πολλαπλασιασμού,καθώς και η εικόνα όλου του $\mathbb{Z}$ να είναι διοφαντικά (στο $\mathbb{Q}$) σύνολα.

Με τους επόμενους ορισμούς ελπίζουμε ότι τα παραπάνω θα αποσαφηνιστούν:

Έστω Σ το σώμα των ρητών ή το σώμα των ρητών συναρτήσεων επί καποιου πεπεραψμένου σώματος χαρακτηριστικής $\neq 2,3$.

Ορισμός 6 *Έστω μια κυβική καμπύλη C,δηλ.ένα πολυώνυμο δύο μεταβλητών, βαθμού 3 με συντελεστές από το Σ. Ένα σημείο Ο επί της κυβικής καμπύλης C ονομάζεται ιδιάζον αν κάθε πρώτου βαθμού εξίσωση δύο μεταβλητών που το έχει* *ως λύση έχει το πολύ δύο κοινές λύσεις με την C.(Ισοδύναμα: αν στο O,οι τυπικές παράγωγοι ως προς και τις δύο μεταβλητές είναι 0.)*

Ορισμός 7 *Ελλειπτική καμπύλη επί ενός σώματος Σ ονομάζουμε μια κυβική καμπύλη, χωρίς ιδιάζοντα σημεία, της μορφής*

$$x^3 + a_1x^2 + a_2x + a_3 = by^2$$

με $a_1, a_2, a_3, b \in \Sigma$ τέτοια ώστε η εξίσωση $x^3 + a_1x^2 + a_2x + a_3 = 0$ να έχει τρεις διακεκριμένες ρίζες(στην αλγεβρική κλειστότητα του Σ).

Για τους σκοπούς μας αρκεί να μελετήσουμε κατάλληλη ελλειπτική εξίσωση C της εξής συγκεκριμένης μορφής:

$$x^3 + ax^2 + x = y^2. \tag{33}$$

με $a \neq +2, -2$. Πράγματι,είναι εύκολο να δει κανείς ότι αν $a \neq +2, -2$, η παραπάνω εξίσωση ορίζει ελλειπτική καμπύλη,αφού το τριώνυμο $x^2 + ax + 1 = 0$ έχει διακρίνουσα διάφορη του μηδενός και επίσης,χρησιμοποιώντας τις τυπικές παραγώγους και την υπόθεση για τη χαρακτηριστική του Σ,μπορούμε με απλές πράξεις να δείξουμε ότι η C δεν έχει ιδιάζοντα σημεία.Στα επόμενα,χάριν συντομίας θα γράφουμε $f[x]$ αντί για $x^3 + ax^2 + x$. Εκείνο που κάνει ενδιαφέρουσα τη μελέτη αυτών των καμπύλων είναι ότι μπορούμε να ορίσουμε στα σημεία της(33) (με συντεταγμένες από το Σ ή/και την αλγεβρική κλειστότητά του) μια πράξη $\oplus$ με την οποία καθίστανται αβελιανή ομάδα,της οποίας ουδέτερο σημείο είναι ένα επιπλέον σημείο P_∞ στο άπειρο.Η ιδέα είναι η εξής:αν τα $P_1(x_1, y_1)$ και $P_2(x_2, y_2)$ είναι δύο σημεία της C τότε

1 αν $y_1 \neq -y_2$, για να βρούμε το σημείο $P_3 = P_1 \oplus P_2$ αρκεί να φέρουμε την ευθεία που περνάει από τα P_1, P_2 (αν τα δύο σημεία ταυτίζονται τότε φέρνουμε την εφαπτομένη) και να βρούμε το τρίτο σημείο τομής της ευθείας αυτής με την C. Αν η ευθεία που έχουμε φέρει δεν εφάπτεται στην καμπύλη τότε το τρίτο αυτό σημείο υπάρχει επειδή η C είναι βαθμού 3·αλλιώς παίρνουμε το σημείο στο οποίο εφάπτονται ευθεία και καμπύλη.Τελικά παίρνουμε ως P_3 το συμμετρικό του σημείου αυτού ως προς τον άξονα των x.

2 Αν $y_1 = -y_2$, $P_3 = P_\infty$.

Δεν θα μπούμε σε λεπτομέρειες για τον υπολογισμό των συνάρτήσεων που με όρισμα τις συντεταγμένες δύο σημείων δίνουν την πρώτη και τη δεύτερη συντεταγμένη του αθροίσματος των δύο σημείων.Το ενδιαφέρον για μας είναι ότι αυτές οι συναρτήσεις είναι ρητές.

Έστω G_C η ομάδα που περιγράψαμε παραπάνω που αποτελείται από τα σημεία με συντεταγμένες από το Σ. Το 1921 ο Mordell απέδειξε ένα πολύ σημαντικό θεώρημα σύμφωνα με το οποίο για Σ=$\mathbb{Q}$ η G_C (όπως και οι ομάδες που σχηματίζονται με ανάλογο τρόπο από άλλες ελλειπτικές καμπύλες επί του $\mathbb{Q}$) είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.Από το γενικό θεώρημα που ισχύει για τις πεπερασμένα παραγόμενες αβελιανές ομάδες συμπεραίνουμε ότι η ομάδα αυτή,που θα συμβολίζουμε με $C(\Sigma)$,είναι ισόμορφη με ευθύ άθροισμα της μορφής $\mathbb{Z}^g + F$,όπου F ομάδα κάθε στοιχείο της οποίας είναι πεπερασμένης τάξης.Το (μοναδικό) g για το οποίο ισχύουν τα παραπάνω ονομάζεται διάσταση της $C(\Sigma)$ ή της καμπύλης C επί του Σ.

Θα συμβολίζουμε με $End(C)$ το σύνολο των ενδομορφισμών της G_C των οποίων οι συντεταγμένες συναρτήσεις είναι ρητές(αλγεβρικών ενδομορφισμών).Είναι εύκολο να δει κανείς ότι το $End(C)$ με τη φυσιολογική επέκταση της πράξης $\oplus$ γίνεται αβελιανή ομάδα ενώ χρησιμοποιώντας και την πράξη που επάγεται από τη σύνθεση συναρτήσεων παίρνουμε μια ενδιαφέρουσα δομή δακτυλίου που θα παίξει σημαντικό ρόλο στα επόμενα.Συγκεκριμένα,ισχύει για το δακτύλιο αυτό ένα σημαντικό θεώρημα,του οποίου θα χρησιμοποιήσουμε μόνο την εξής μορφή,χωρίς απόδειξη:

Θεώρημα 3

1. *Αν η χαρακτηριστική του Σ είναι 0,υπάρχει a ώστε ο δακτύλιος $End(C)$ που κατασκευάσαμε παραπάνω με αφετηρία την καμπύλη $C : x^3 + ax^2 + x = y^2$ να είναι ισόμορφος με το δακτύλιο $\mathbb{Z}$ των ακεραίων.*

2. *Αν η χαρακτηριστική του Σ είναι $\neq 0, 2, 3$, τότε υπάρχει a ώστε ο δακτύλιος $End(C)$ να είναι ισόμορφος με το δακτύλιο των αλγεβρικών ακεραίων κάποιας φανταστικής επέκτασης του $\mathbb{Q}$ διάστασης 2.Υπενθυμίζουμε ότι όπως απέδειξε ο Denef οι δακτύλιοι αυτοί έχουν μη αποφασίσιμες υπαρξιακές θεωρίες,οπότε για τους σκοπούς μας εύρεση διοφαντικού μοντέλου κάποιου εξ' αυτών ή του $\mathbb{Z}$ είναι το ίδιο πράγμα.*

Έτσι από εδώ και στο εξής θα αρκεί να σταθεροποιήσουμε ένα τέτοιο a και να μελετήσουμε την αντίστοιχη καμπύλη,μεταφέροντας όσο το δυνατόν περισσότερα εργαλεία μελέτης από το $\mathbb{Z}$.

Θα χρησιμοποιήσουμε τη "γενική μορφή" ενός σημείου της C: Έστω y ένα υπερβατικό στοιχείο επί του σώματος Σ,και το αντίστοιχο σώμα (ουσιαστικά το σώμα των ρητών συναρτήσεων) που παράγεται από το Σ και το y,$\Sigma(y)$.Έστω επίσης το αλγεβρικό επί του $\Sigma(y)$ στοιχείο r για το οποίο $r^2 = y^3 + ay^2 + y$.Το σημείο (r, y) είναι ακριβώς η "γενική μορφή" που αναφέραμε. Πάνω σε αυτό το σημείο μπορούμε τώρα να εφαρμόσουμε τις διάφορες συναρτήσεις του $End(C)$ (τις οποίες αν χαρΣ=0 μέσω του ισομορφισμού μπορούμε να βλέπουμε ως ακεραίους).Έτσι π.χ. αν $n \in End(C)\backslash\{0\}$ τότε

$$n(r, y) = \underbrace{(r, y) \oplus \cdots \oplus (r, y)}_{n \text{ φορές}} = (h_n(r, y), rg_n(r, y)) \tag{34}$$

όπου οι h_n, g_n είναι ρητές συναρτήσεις δύο μεταβλητών με συντελεστές από το σώμα Σ.Το γιατί γράφουμε rg_n και όχι το απλούστερο φαινομενικά g_n θα φανεί αμέσως παρακάτω.

Θα αναφέρουμε εδώ χωρίς αποδείξεις κάποιες ιδιότητες των (h_n, g_n) που θα χρειαστούν λίγο παρακάτω.

Πρόταση 1 *1)Για το τυχόν $n \in End(C)\backslash\{0\}$ τα h_n, g_n ανήκουν στο $\Sigma(y)$, δεν εμφανίζεται δηλαδή σ' αυτά το r.Επίσης το (h_n, g_n) ικανοποιεί την εξίσωση της ελλειπτικής καμπύλης επί του $\Sigma(y)$ με εξίσωση $f[y]g^2 = f[h]$.*

2)Έστω $m, n \in End(C)$ τέτοια ώστε το mn δεν διαιρείται από την χαρακτηριστική του Σ(ως στοιχείο του $End(C)$) ώστε κάθε πόλος του h_n να είναι και πόλος του

h_m.Τότε η νόρμα του $n, N(n)$ (όπου $N(n) = n\bar{n}$ με $\bar{n}$ το συζυγές στοιχείο του n ως μιγαδικού αριθμού)διαιρεί τη νόρμα του $m, N(m)$ στο $\mathbb{Z}$.

3) Έστω $m \in End(C) \backslash qEnd(C)$,όπου q η χαρακτηριστική του Σ(0 ή ≥ 5).Τότε αν $m \equiv 0 \ (mod 2)$ το h_m έχει τη μορφή $h_m = \frac{1}{f(y)}d^2$ και αν $m \equiv 1 \ (mod 2)$ έχει τη μορφή $h_m = yd^2$,όπου και στις δύο περιπτώσεις οι ρίζες και οι πόλοι του d είναι τάξης 1.

Ανακεφαλαιώνουμε:Είμαστε σχεδόν έτοιμοι να κατασκευάσουμε έναν αλγόριθμο που αντιστοιχεί σε κάθε ακέραιο την εικόνα ενός σημείου μιας ελλειπτικής καμπύλης μέσω του (αλγεβρικού) μορφισμού της ομάδας των σημείων της καμπύλης αυτής που αντιστοιχεί στο συγκεκριμένο ακέραιο.Για τον αλγόριθμο αυτό θα πρέπει να δείξουμε τα εξής τρία πράγματα:

Α Η εικόνα ολόκληρου του $\mathbb{Z}$(ή κάποιου άλλου δακτυλίου του οποίου η διοφαντική θεωρία είναι μη αποφασίσιμη) μέσω του αλγορίθμου είναι σύνολο διοφαντικό στο Σ(δηλ.το $\mathbb{Q}$ ή το σώμα ρητών συναρτήσεων που μας ενδιαφέρει) .

Β Η εικόνα του γραφήματος της πρόσθεσης μέσω της επαγόμενης από τον αλγόριθμο συνάρτησης (με τρεις μεταβλητές) είναι σύνολο διοφαντικό στο Σ.

Γ Η εικόνα του γραφήματος του πολλαπλασιασμού μέσω της επαγόμενης από τον αλγόριθμο συνάρτησης (με τρεις μεταβλητές) είναι σύνολο διοφαντικό στο Σ.

Όπως θα δούμε αμέσως,για την περίπτωση των σωμάτων ρητών συναρτήσεων επί πεπερασμένου σώματος τα Α,Β έχουν δειχθεί ενώ για την περίπτωση του $\mathbb{Q}$ υπάρχουν ακόμα κάποια κενά,που όμως υπάρχει ελπίδα να καλυφθούν με τη χρήση ακριβώς της αναλογίας με την πρώτη περίπτωση.Αντίθετα, το Γ φαίνεται να είναι πολύ πιο δύσκολο και για τις δύο περιπτώσεις και παρά τις κάποιες προόδους που έχουν συντελεσθεί μένουν ακόμα πολλά να γίνουν.

Πρώτα θα μελετήσουμε τα σώματα ρητών συναρτήσεων επί ενός σώματος Σ.Με τρόπο παρόμοιο με αυτόν που είδαμε σε προηγούμενη ενότητα σχολιάζοντας το αντίστοιχο ερώτημα για πολυωνυμικούς δακτυλίους,το πρόβλημα του αν η υπαρξιακή θεωρία ενός τέτοιου σώματος στη γλώσσα του δακτυλίου των πολυωνύμων είναι αποφασίσιμη δεν έχει από μόνο του επιπλέον ενδιαφέρον σε σχέση με το πρόβλημα του αν η υπαρξιακή θεωρία του σώματος των συντελεστών είναι αποφασίσιμη.Έτσι,για να έχουμε ένα ουσιαστικά καινούριο πρόβλημα θα μελετήσουμε την αποφασισιμότητα της υπαρξιακής θεωρίας ενός σώματος ρητών συναρτήσεων $\Sigma(t)$ στην επεκτεταμένη γλώσσα που έχει ένα κατηγορηματικό σύμβολο για τη μεταβλητή t.

Για τεχνικούς λόγους θα αλλάξουμε το όνομα της μεταβλητής.Συγκεκριμένα,αν t είναι η μεταβλητή,τότε υπάρχει κάποιο στοιχείο y στην αλγεβρική κλειστότητα του $\Sigma(t)$ ώστε $y^2 = t$.Είναι εύκολο να δει κανείς ότι το $\Sigma(y)$ είναι ένας διανυσματικός χώρος επί του $\Sigma(t)$ διάστασης 2(μια βάση είναι το $\{1, y\}$).Έτσι κάθε στοιχείο του $\Sigma(y)$ μπορεί να ταυτιστεί με φυσιολογικό τρόπο με ένα ζεύγος (s_1, s_2) στοιχείων του $\Sigma(t)$.Στα ζεύγη αυτά μεταφέρεται με τον ίδιο τρόπο η δομή των δύο πράξεων από το $\Sigma(y)$.Έχουμε λοιπόν όχι μόνο έναν καινούριο τρόπο να βλέπουμε το σώμα $\Sigma(y)$ αλλά και μία δομή η οποία (με επιφανειακό τρόπο) έχει εμπλουτισθεί:Συγκεκριμένα,σε αυτήν την δομή μπορούμε επιπλέον να χρησιμοποιούμε τη σχέση που περιέχει όλα τα ζεύγη της μορφής $(g[y], g[-y])$ για κάθε $g \in \Sigma(y)$.Πιο αυστηρά,έχουμε το εξής:

Πρόταση 2 *Η υπαρξιακή θεωρία ενός σώματος ρητών συναρτήσεων $\Sigma(t)$ στην επεκτεταμένη γλώσσα που έχει ένα κατηγορηματικό σύμβολο για τη μεταβλητή t είναι αποφασίσιμη εαν και μόνον εάν η υπαρξιακή θεωρία του σώματος $\Sigma(y)$ (με τον παραπάνω συμβολισμό) στην επεκτεταμένη γλώσσα που έχει ένα κατηγορηματικό σύμβολο για τη μεταβλητή y και ένα για την προαναφερθείσα σχέση J είναι αποφασίσιμη.*

Απόδειξη

Ουσιαστικά έχουμε την ίδια δομή με την προσθήκη ενός κατηγορηματικού συμβόλου.Έιναι προφανές λοιπόν ότι αν το σύνολο των αληθών υπαρξιακών προτάσεων στο οποίο δεν χρησιμοποιείται το επιπλέον κατηγορηματικό σύμβολο (δηλ. η υπαρξιακή θεωρία του $\Sigma(t)$ στην επεκτεταμένη γλώσσα που έχει ένα κατηγορηματικό σύμβολο για τη μεταβλητή t) δεν είναι αποφασίσιμο,τότε ούτε και το σύνολο όλων των αληθών υπαρξιακών προτάσεων για τη δομή αυτή,(δηλ. η υπαρξιακή θεωρία του σώματος $\Sigma(y)$ στην επεκτεταμένη γλώσσα που έχει ένα κατηγορηματικό σύμβολο για τη μεταβλητή y και ένα για τη σχέση J)είναι αποφασίσιμο.

Έστω τώρα ότι η υπαρξιακή θεωρία του $\Sigma(t)$ για τη γλώσσα που αναφέρεται παραπάνω είναι αποφασίσιμη και έστω τυχών ανοικτός τύπος φ στην γλώσσα για τη δομή $\Sigma(y)$.Έίναι εύκολο να δει κανείς ότι ο φ μπορεί να γραφεί σαν διάζευξη συζεύξεων τύπων της μορφής $p = 0, w \neq 0, T(k), \neg T(l), J(d), \neg J(e)$ όπου τα p, q, d, e είναι πολυώνυμα με συντελεστές στον υποδακτύλιο που παράγεται από τις σταθερές 0,1 και τα σύμβολα $\{+, \cdot\}$.Επειδή ενδιαφερόμαστε για την υπαρξιακή θεωρία και ο υπαρξιακός ποσοδείκτης επιμερίζεται στα διάφορα μέλη της διάζευξης,αρκεί να μελετήσουμε ένα από αυτά,δηλαδή μία σύζευξη της παραπάνω περιγραφείσας μορφής.Ένα παράδειγμα για το πώς μπορεί να γίνει η αναγωγή ίσως είναι διαφωτιστικότερο από την πλήρη απόδειξη.Έστω ότι θέλουμε να βρούμε αν αληθεύει η πρόταση

$$\exists x_1, x_2, x_3, x_4[{x_1}^2 + x^2 + 1 = 0 \wedge x_1 + x_3x_4 + 2 \neq 0 \wedge$$

$$T(x_1) \wedge \neg T(x_2) \wedge J(x_1, x_3) \wedge \neg J(x_3, x_4)]$$

στη δομή $\Sigma(y)$.Έίναι εύκολο να επαληθεύσουμε ότι η αλήθεια της πρότασης αυτής ανάγεται στην αλήθεια της

$$\exists x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 \in \Sigma(t)[(x_1 + yx_2)^2 + (x_3 + yx_4)^2 + 1 = 0$$

$$\wedge (x_1 + yx_2) + (x_5 + yx_6)(x_7 + yx_8) + 2 \neq 0 \wedge T(x_1 + yx_2) \wedge \neg T(x_3 + yx_4)$$

$$\wedge J(x_1 + yx_2, x_5 + yx_6) \wedge \neg J(x_5 + yx_6, x_7 + yx_8)] \iff$$

$$\exists x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9 \in \Sigma(t)[{x_1}^2 + x_9{x_2}^2 + {x_3}^2 + x_9{x_4}^2 + 1 = 0$$

$$\wedge 2x_1x_2 + 2x_3x_4 = 0 \wedge (x_1 + x_5x_7 + x_9x_6x_8 + 2 \neq 0 \vee x_2 + x_6x_7 + x_5x_8 \neq 0) \wedge$$

$$x_1 = 0 \wedge x_2 = 1 \wedge (x_3 \neq 0 \vee x_4 \neq 1) \wedge x_1 = x_5 \wedge$$

$$x_2 = -x_6 \wedge (x_5 \neq x_7 \vee x_6 \neq -x_8) \wedge x_9 = t].$$

Η τελευταια αυτή πρόταση είναι υπαρξιακή αφορά το $\Sigma(t)$ και βρίσκεται στη γλώσσα που χρησιμοποιούμε για τη δομή αυτή.Έτσι,μπορούμε να αποφανθούμε για το αν ισχύει ή όχι.

Έστω τώρα στοιχεία r, q, αλγεβρικά επί του $\Sigma(y)$ που ικανοποιούν τις $r^2 = f[y]$ και $q^2 = f[-y]$.Το σώμα που παράγεται από το Σ και τα τρία στοιχεία y, r, q, θα συμβολίζουμε $A = \Sigma(y, r, q)$. Όπως παραπάνω,στην (34), μπορούμε για κάθε ζεύγος $m, n \in End(C)$ όπου τουλάχιστον ένα εκ των m, n δεν είναι 0 να υπολογίσουμε τις ρητές συναρτήσεις $d_{m,n}, e_{m,n}$ με μεταβλητές τις (y, r, q) ώστε

$$(d_{m,n}, e_{m,n}) = m(y, r) \oplus n(-y, q). \tag{35}$$

Τις συναρτήσεις αυτές μπορούμε να τις δούμε και ως σημεία της ελλειπτικής καμπύλης που έχει την ίδια εξίσωση με την C, θεωρούμενη όμως επί του A αυτή τη φορά. Επειδή τα σώματα $\Sigma(y, r)$ και $\Sigma(y, q)$ είναι διανυσματικοί χώροι διάστασης 2 επί του $\Sigma(y)$,καθεμιά από τις $d_{m,n}, e_{m,n}$ γράφεται με μοναδικό τρόπο ως άθροισμα $l_0 + l_1 r + l_2 q + l_3 rq$, όπου τα l_0, l_1, l_2, l_3 είναι συντελεστές από το $\Sigma(y)$.Έτσι,το να μιλάμε για διοφαντικά,υπαρξιακά κλπ. σύνολα στοιχείων του A δεν έχει ουσιαστική διαφορά από το να μιλάμε για διοφαντικά,υπαρξιακά κλπ. σύνολα τετράδων από το $\Sigma(y)$.Μπορούμε τώρα να διατυπώσουμε το πρώτο σημαντικό συμπέρασμα προς την κατεύθυνση των Α,Β,Γ που αναφέραμε παραπάνω:

Θεώρημα 4 *Τα σύνολα* $\Upsilon_1 = \{(d_{m,0}, e_{m,0}) : m \in End(C)\backslash\{0\}\}, \Upsilon_2 = \{(d_{0,n}, e_{0,n}) : n \in End(C)\backslash\{0\}\}, \Upsilon_3 = \{(d_{m,n}, e_{m,n}) : m, n \in End(C)\backslash\{0\}\}$, $\Upsilon_d = \{(d_{m,m}, e_{m,m}) : m \in End(C)\backslash\{0\}\}$ *είναι υπαρξιακά επί του* $\Sigma(y)$.

Στοιχεία από την απόδειξη

Η πλήρης απόδειξη θα παραλειφθεί·επισημαίνουμε πάντως ότι,όπως η διατύπωση του θεωρήματος για τα Υ_1, Υ_2 θυμίζει το ότι το σύνολο των ακεραίων που είναι γνήσια μεγαλύτεροι του μηδενός είναι διοφαντικό,έτσι και η απόδειξη βασίζεται σε ένα θεώρημα ανάλογο με το θεώρημα του Lagrange.Για το Υ_3 η απόδειξη βασίζεται στα Υ_1, Υ_2 και τον ορισμό της πρόσθεσης ενώ για το Υ_d είναι απαραίτητη η επιπλέον κατηγορηματική σχέση που περιγράψαμε παραπάνω.

Έχουμε τώρα τα απαραίτητα εργαλεία για να περιγράψουμε το πώς μπορεί να γίνει η επιθυμητή αντιστοίχηση των στοιχείων του δακτυλίου $End(C)$. Συγκεκριμένα σε κάθε $m \neq 0 \in End(C)$ αντιστοιχούμε το σημείο της ελλειπτικής καμπύλης C επί του A, $T_m = (d_{m,0}, e_{m,0})$ ή με άλλα λόγια την αντίστοιχη οκτάδα σημείων του $\Sigma(y)$.Από το προηγούμενο θεώρημα έχουμε ότι το σύνολο των οκτάδων αυτών (για τα $m \neq 0 \in End(C)$) είναι υπαρξιακό, δηλ. έχουμε πετύχει το Α από τους στόχους που θέσαμε.Είναι επίσης εύκολο να δούμε ότι επειδή επειδή η πρόσθεση στον δακτύλιο $End(C)$ αντιστοιχεί στην πράξη που έχουμε ορίσει επί των ρητών σημείων της ελλειπτικής καμπύλης ,μπορούμε να βρούμε έναν τύπο χωρίς καθόλου ποσοδείκτες με τον οποίο από δύο τέτοιες οκτάδες να υπολογίζουμε την οκτάδα που αντιστοιχεί στο άθροισμα των στοιχείων από τα οποία έχουν προέλθει.Άρα και το γράφημα της πρόσθεσης,ή για την ακρίβεια το σύνολο $\{(T_{n_1} T_{n_2} T_{n_3}) : n_1 = n_2 + n_3, n_1 n_2 n_3 \neq 0\}$ είναι υπαρξιακό,δηλ. έχουμε πετύχει και τον στόχο Β,πάντα για σώματα ρητών συναρτήσεων επί πεπερασμένου σώματος.Πρέπει να παρατηρήσουμε ίσως εδώ ότι το γεγονός ότι δεν έχουμε αντιστοιχήσει το 0 σε κάποιο σημείο της ελλειπτικής καμπύλης δεν επηρεάζει την ουσία της απόδειξης,αφού μπορούμε να αναγάγουμε την επιλυσιμότητα τυχούσας διφαντικής εξίσωσης στον δακτύλιο $End(C)$ στην επιλυσιμότητα μιας σειράς διοφαντικών εξισώσεων στο $End(C)\backslash\{0\}$ μηδενίζοντας κάθε φορά μία ή περισσότερες μεταβλητές.

Μένει το Γ,η απόδειξη δηλαδή του ότι το γράφημα του πολλαπλασιασμού,το σύνολο $\{(T_{n_1}T_{n_2}T_{n_3}) : n_1 = n_2 \cdot n_3, n_1n_2n_3 \neq 0\}$.Εδώ δεν μπορούμε να εφαρμόσουμε όσα εφαρμόσαμε για την πρόσθεση,αφού ο πολλαπλασιασμός ουσιαστικά αντιστοιχεί σε σύνθεση ενδομορφισμών,και στη γλώσσα που χρησιμοποιούμε δεν υπάρχει σύμβολο για τη σύνθεση,ούτε είναι προφανές το πώς θα το ορίσουμε. Όπως είδαμε και παραπάνω,η απόδειξη δεν είναι ακόμα πλήρης.Η κατεύθυνση που ακολούθησε ο Φειδάς βασιζόμενος σε σημαντικό βαθμό σε ιδέες των K.H.Kim F.W.Roush και η οποία φαίνεται αρκετά υποσχόμενη είναι η δουλειά πάνω στην υπαρξιακή ορισιμότητα της σχέσης της διαιρετότητας,και συγκεκριμένα ενός είδους "διπλής" διαιρετότητας την οποία θα συμβολίζουμε με $|_{KR}$,η οποία συνεπάγεται την υπαρξιακή ορισιμότητα του γραφήματος του πολλαπλασιασμού.Συγκεκριμένα:

Ορισμός 8 *Στο εξής,αν $p \in End(C)\backslash\{0\}$ θα συμβολίζουμε με T_p το σημείο $p(y,r)$ και με U_p το $p(-y,q)$. Έστω λοιπόν (T_g, U_h) και (T_i, U_j) δύο ζεύγη σημείων της ελλειπτικής καμπύλης C, ρητά επί του A.Θα γράφουμε $(T_g, U_h)|_{KR}(T_i, U_j)$ εάν και μόνον εάν υπάρχει κάποιο $k \in End(C)$ ώστε $i = kg$ και $j = kh$.Θα χρησιμοποιούμε το ίδιο σύμβολο για την επαγόμενη σχέση μεταξύ ζευγών στοιχείων του $End(C)$.*

Ισχύει ότι η υποομάδα που αποτελείται από τα σημεία της μορφής $\{T_g \oplus U_h : g, h \in End(C)\}$ είναι ισόμορφη με το ευθύ άθροισμα της (ομάδας) $End(C)$ με τον εαυτό της·έτσι μπορούμε για τους σκοπούς μας να ταυτίζουμε το τυχόν ζεύγος (T_g, U_h) όπου $gh \neq 0$ με το $T_g \oplus U_h = (d_{g,h}, e_{g,h})$ χωρίς πρόβλημα,αφού η αντιστοίχηση είναι ένα προς ένα και ο υπολογισμός για την εύρεση του αθροίσματος αυτού γίνεται με την απλή χρήση ενός τύπου χωρίς ανάγκη ποσοδεικτών.Παρόμοια θα ταυτίζουμε το σημείο $T_g, g \neq 0$ με το $(d_{g,0}, e_{g,0})$ και το $U_h, h \neq 0$ με το $(d_{0,h}, e_{0,h})$.Από το θεώρημα 4 και τα τρία σύνολα που παράγονται από την ταύτιση που περιγράψαμε παραπάνω είναι υπαρξιακά στο $\Sigma(y)$. Μπορούμε τώρα να διατυπώσουμε το εξής:

Θεώρημα 5 *Αν το σύνολο τετράδων (T_g, U_h, T_i, U_j) με $(T_g, U_h)|_{KR}(T_i, U_j)$ και $ghij \neq 0$ είναι υπαρξιακό επί του $\Sigma(y)$, τότε η υπαρξιακή θεωρία του $\Sigma(y)$ είναι μη αποφασίσιμη.*

Απόδειξη

Παρατηρούμε κατ' αρχήν ότι για τα τυχόντα στοιχεία του δακτυλίου $End(C)$ g, i, j ισχύει ότι $(g, 1)|_{KR}(i, j)$ εάν και μόνον εάν $i = gj$. Έστω ότι ισχύει η υπόθεση και ότι με δεδομένα τα T_g, T_j θέλουμε να ορίσουμε με υπαρξιακό τρόπο το T_{gj}.Πρώτο βήμα είναι το να ορίσουμε υπαρξικά το U_j.Αυτό μπορεί να γίνει αν βασιζόμενοι στο θεώρημα 4 γράψουμε έναν υπαρξιακό τύπο που να σημαίνει ότι το U_j είναι το σημείο που ανήκει στο Υ_2, (είναι δηλ. της μορφής $(d_{0,n}, e_{0,n})$ για κάποιο $n \neq 0$) και είναι τέτοιο ώστε το άθροισμα(το οποίο επίσης ορίζεται υπαρξιακά) $T_j \oplus (d_{0,n}, e_{0,n})$ να ανήκει στο Υ_d, δηλ. να είναι της μορφής $(d_{n,n}, e_{n,n})$.Έτσι χρησιμοποιώντας και την υπόθεση μπορούμε να γράψουμε έναν υπαρξιακό τύπο που να σημαίνει ότι $(T_g, U_1)|_{KR}(T_i, U_j)$, κάτι που όπως είδαμε παραπάνω είναι ισοδύναμο με το $i = gj$.Πετύχαμε δηλ. το στόχο Γ,οπότε έχουμε κατασκεύασει στο $\Sigma(y)$ ένα διοφαντικό μοντέλο κάποιου δακτυλίου του οποίου η υπαρξιακή θεωρία δεν είναι αποφασίσιμη,κάτι που σημαίνει όπως έχουμε δείξει στα προηγούμενα ότι ούτε η υπαρξιακή θεωρία του $\Sigma(y)$ είναι αποφασίσιμη.

Οι προσπάθειές μας λοιπόν στο εξής θα επικεντρωθούν στη μελέτη της σχέσης $|_{KR}$.

Κάποια ορολογία που θα χρησιμοποιούμε στα παρακάτω με ελαφρά γενικότερο τρόπο απ'οτι στα προηγούμενα :Για τυχούσα ρητή συνάρτηση r με συντελεστές από κάποιο σώμα (στην περίπτωσή μας στοιχείο του $\Sigma(y)$ ή του A)θα ονομάζουμε ρίζα (αντ.πόλο) της ένα πρώτο ιδεώδες P του δακτυλίου πολυωνύμων με συντελεστές από το ίδιο σώμα στο οποίο η τάξη του r είναι θετική (αντ. αρνητική.)Με τη φράση ¨τάξη ενός στοιχείου r στο πρώτο ιδεώδες P¨ εννοούμε φυσικά την τάξη του σε κάποιο πολυώνυμο που παράγει το ιδεώδες[12].Οι ρίζες και οι πόλοι του r θα ονομάζονται γενικά διαιρέτες του ενώ ειδικοί πρώτοι διαιρέτες θα ονομάζονται αυτοί που περιέχουν το $f[y]f[-y]$.Όταν είναι προφανές από τα συμφραζόμενα το τι εννοούμε θα χρησιμοποιούμε καταχρηστικά τους όρους ¨ρίζα¨ και ¨πόλος¨ και για τα στοιχεία της αλγεβρικής κλειστότητας του σώματος που μελετάμε τα οποία μηδενίζουν το πολυώνυμο που παράγει το αντίστοιχο πρώτο ιδεώδες.

Πρόταση 3 *Έστω $i, j \in End(C)\backslash\{0\}$ τέτοια ώστε το i διαιρεί το j (στο $End(C)$). Τότε κάθε πόλος του h_i είναι πόλος του h_j.*

Απόδειξη

Υπενθυμίζουμε ότι με βάση το 1) της Πρότασης 1 τα h_i, h_j ανήκουν πράγματι στο $\Sigma(y)$.Έστω λοιπόν ότι για κάποιο $k \in End(C), j = ki$.Έστω τώρα ένας πόλος του h_i.Είναι εύκολο να δούμε ότι ο πόλος αυτός πρέπει να είναι η πρώτη συντεταγμένη κάποιου σημείου της καμπύλης που μέσω του ενδομορφισμού i στέλνεται στο σημείο στο ∞, δηλ. στο ουδέτερο στοιχείο της ομάδας των σημείων της ελλειπτικής καμπύλης. Επειδή ο πολλαπλασιασμός όπως είδαμε παραπάνω αντιστοιχεί στη σύνθεση συναρτήσεων,έχουμε ότι $h_j(y) = h_k(h_i(y))$.Είναι εύκολο τώρα να δείξει κανείς ότι επειδή κάθε ενδομορφισμός δεν μπορεί παρά να στέλνει το ουδέτερο στοιχείο στον εαυτό του,ο πόλος του h_i πρέπει να είναι και πόλος του h_j.

Έχουμε ήδη δει στο 2) της πρότασης 1 ότι ισχύει και ένα μερικό αντίστροφο. Αν λοιπόν υπερπηδηθούν τα εμπόδια του ότι το 2) της πρότασης 1 θέτει τον περιορισμό τα i, j να μην διαιρούνται από τη χαρακτηριστική του Σ και του ότι αναφέρεται σε διαιρετότητα μεταξύ των νορμών των στοιχείων και όχι των ίδιων των στοιχείων,το πρόβλημα του υπαρξιακού ορισμού της διαιρετότητας μεταξύ των σημείων T_i και T_j θα αναχθεί στο πρόβλημα του υπαρξιακού ορίσμού του ότι κάθε πόλος του h_i είναι πόλος και του h_j.Πάντως,αν και η κατεύθυνση αυτή είναι ενδιαφέρουσα και πιθανόν θα οδηγούσε σε άλλα αποτελέσματα,δε θα απαντούσε στο προβλημά μας αφού ακόμα και αν ορίζαμε υπαρξιακά τη σχέση της διαιρετότητας,θα είχαμε ένα διοφαντικό μοντέλο,π.χ. του $\mathbb{Z}$ με τη δομή της πρόσθεσης

[12] βλ.§2.1

και της διαίρεσης.Όμως,όπως έχει δείξει ο Lipshitz το 1978 αυτή η δομή έχει αποφασίσιμη υπαρξιακή θεωρία, αν και ολόκληρη η πρωτοβάθμια θεωρία της δεν είναι αποφασίσιμη.Χρειαζόμαστε λοιπόν γενίκευση των προηγούμενων αποτελεσμάτων,αυτή τη φορά για τη σχέση $|_{KR}$ που ορίσαμε παραπάνω.Πρώτα κάποια προκαταρτικά:

Λήμμα 7 *Αν τα i, j είναι πολλαπλάσια του 2 στο $End(C)\backslash\{0\}$ τότε το $d_{i,j}$ που ορίζεται όπως στην (35) είναι τετράγωνο κάποιου στοιχείου στο A. Το στοιχείο αυτό θα συμβολίζουμε με $l_{i,j}$: είναι τέτοιο ώστε $rl_{i,j}$ ∈Σ(y, rq) και επιπλέον αν $j = 0$ $l_{i,j}$ ∈Σ$(y,)$*

Η απόδειξη βασίζεται στη χρήση του τύπου υπολογισμού του αθροίσματος δύο σημείων της καμπύλης και θα παραλειφθεί.

Χρειαζόμαστε ακόμα να ορίσουμε μια φυσιολογική νόρμα από το $\Sigma(y, rq)$ στο $\Sigma(y)$.Επειδή το $\Sigma(y, rq)$ είναι αλγεβρική επέκταση βαθμού το πολύ 4 επί του $\Sigma(y)$,υπάρχουν το πολύ 4 μονομορφισμοί από το $\Sigma(y, rq)$ στον εαυτό του που διατηρούν σταθερό το $\Sigma(y)$. Ορίζουμε ως νόρμα του τυχόντος e ∈$\Sigma(y, rq)$ το γινόμενο των εικόνων του μέσω των μονομορφισμών αυτών.Θα τη συμβολίζουμε $N'(e)$.

Έχουμε λοιπόν τα (περίπου) αντίστοιχα της πρότασης 3 και του 2) του λήμματος 1,τα οποία προς το παρόν είναι αναπόδεικτοι ισχυρισμοί:

Ισχυρισμός 1 *Έστω $g, h, i, j, k \in End(C)\backslash\{0\}$ πολλαπλάσια του 2 τέτοια ώστε $i = kg$ και $j = kh$.Τότε κάθε διαιρέτης του $N'[rl_{g,h}]$ με περιττή πολλαπλότητα είναι πόλος του $N'[rl_{i,j}]$ με περιττή πολλαπλότητα.*

Το μειονέκτημα του ότι απαιτούμε τα στοιχεία του $End(C)$ που χρησιμοποιούμε να είναι πολλαπλάσια του 2 δεν είναι ουσιαστικό,αφού με κατάλληλους πολλαπλασιασμούς με σταθερούς συντελεστές το γενικό πρόβλημα του αν μια τετράδα στοιχείων ικανοποιεί τη σχέση $|_{KR}$ μπορεί να αναχθεί στο πρόβλημα για πολλαπλάσια του 2.

Ισχυρισμός 2 *Αν για κάποια $g, h, i, j \in End(C)\backslash\{0\}$κάθε πόλος του $N'[rl_{g,h}]$ με περιττή πολλαπλότητα είναι πόλος του $N'[rl_{i,j}]$ τότε υπάρχει $k \in \mathbb{Z}, k \neq 0$ τέτοιο ώστε $N(i) = kN(g)$ και $N(j) = kN(h)$.*

Οι δύο παραπάνω ισχυρισμοί,ακόμα και αν αποδειχθούν ορθοί,προφανώς δεν αρκούν για να ικανοποιήσουν την υπόθεση του θεωρήματος 5 αλλά την ανάγουν στον υπαρξιακό ορισμό κατάλληλης συνθήκης για τις νόρμες κάποιων στοιχείων.Προς αυτήν την κατεύθυνση ο Φειδάς έχει αποδείξει ένα μερικό αποτέλεσμα,το Λήμμα Υπαρξιακής Διαιρετότητας για Σώματα Θετικής Χαρακτηριστικής.Δεν θα μπούμε σε τεχνικές λεπτομέρειες του λήμματος αυτού,αφού παρακάτω θα παρουσιάσουμε το ακριβές αντίστοιχό του για το $\mathbb{Q}$.Σε αδρές γραμμές πάντως η ουσία του λήμματος είναι ότι για σώματα ρητών συναρτήσεων $W = \Sigma_q(y)$ όπου q είναι πρώτος με $q \equiv -1\ mod(4)$, υπάρχει υπαρξιακός τύπος $\varphi(x_1, x_2)$ που εκφράζει ότι κάθε περιττής πολλαπλότητας πόλος p του x_1 τέτοιος ώστε η εξίσωση $x^2 + 1 = 0$ να μην έχει λύσεις στο σώμα-πηλίκο $\frac{W}{\langle p \rangle}$(στο εξής θα γράφουμε $p \in Pr(-1)$) είναι πόλος του x_2.Επικαλούμενοι τώρα και το 3) του λήμματος 1 μπορούμε εύκολα να δείξουμε ότι το $rl_{m,0}$ είναι στοιχείο του W τέτοιο ώστε αν υπάρχει πρώτος $p \in Pr(-1)$ με $ord_p(rl_{m,0})$ περιττό αριθμό,η $\varphi(rl_{m,0}, rl_{mk})$ αληθεύει για κάθε k.

Γνωρίζοντας τώρα ότι το παραπάνω λήμμα ισχύει,μπορούμε να επαναδιατυπώσουμε τροποποιημένο και ενισχυμένο το παρακάτω ζεύγος ισχυρισμών,για σώματα ρητών συναρτήσεων επί πεπερασμένου σώματος όπως παραπάνω :

Ισχυρισμός 3 *Έστω $g, h, i, j, k \in End(C)\backslash\{0\}$ πολλαπλάσια του 2 τέτοια ώστε $i = kg$ και $j = kh$.Τότε τα $N'[rl_{g,h}]$ και $N'[rl_{i,j}]$ ικανοποιούν τις(ασθενείς) συνθήκες(τις οποίες δεν εκθέσαμε αναλυτικά) ώστε $\varphi(N'[rl_{g,h}], N'[rl_{i,j}])$.*

Ισχυρισμός 4 *Έστω $g, h, i, j \in End(C)\backslash\{0\}$ πολλαπλάσια του 2 ώστε κάθε πόλος του $N'[rl_{g,h}]$ με περιττή πολλαπλότητα που ανήκει στο $Pr(-1)$ είναι πόλος του $N'[rl_{i,j}]$.Τότε τότε υπάρχει $k \in \mathbb{Z}, k \neq 0$ τέτοιο ώστε $N(i) = kN(g)$ και $N(j) = kN(h)$.*

Ακόμα και αν οι δύο τελευταίοι ισχυρισμοί ευσταθούν,χρειάζεται να αντιμετωπισθεί το πρόβλημα ότι αφορούν νόρμες στοιχείων και όχι τα στοιχεία αυτά καθεαυτά.Ο Φειδάς εκτιμά ότι αυτό δεν είναι μεγάλο εμπόδιο και ότι είναι δυνατόν να αποδειχθεί το θεώρημα 5 με κατάλληλη ασθενέστερη υπόθεση.Υπενθυμίζουμε ότι όταν και εάν τα παραπάνω βήματα γίνουν, η απόδειξη θα είναι πλήρης μόνο για τα σώματα που ικανοποιούν τις υποθέσεις του Λήμματος Υπαρξιακής Διαιρετότητας.

Περνάμε τώρα στον κυρίως στόχο,την υπαρξιακή θεωρία του $\mathbb{Q}$.Εδώ τα πράγματα είναι πιο δύσκολα, αφού κανένας από τους στόχους Α,Β,Γ δεν έχει επιτευχθεί πλήρως.Θα ακολουθήσουμε στρατηγική ανάλογη με αυτήν που χαράξαμε αμέσως προηγουμένως.Βέβαια,το $\mathbb{Q}$ ως σώμα διαφέρει με ουσιαστικό τρόπο από τα σώματα ρητών συναρτήσεων επί πεπερασμένου σώματος.Οι διαφορές αυτές,το ότι δηλαδή έχει χαρακτηριστική 0 και το ότι το πρώτο σώμα που περιέχει δεν είναι γνήσιο υπόσωμα,διαφοροποιούν,και ενίοτε δυσκολεύουν τις διατυπώσεις των διαφόρων θεωρημάτων αλλά και των προς απόδειξη ισχυρισμών.

Πιο συγκεκριμένα,έχουμε τα εξής:

Ισχυρισμός 5 *Υπάρχει μια ελλειπτική καμπύλη C με εξίσωση*

$$x^3 + ax^2 + x = y^2$$

τέτοια που να υπάρχει κάποιο σημείο (b_1, c_1) της C ώστε:

(1)Το $\Sigma_1 = \mathbb{Q}(b_1)$ να έχει βαθμό ≥ 2 ως επέκταση του $\mathbb{Q}$.

(2)Αν $L_1 = \mathbb{Q}(b_1, c_1)$, η $C(L_1)$ να έχει διάσταση 1 και κάθε σημείο της C με συντελεστές από το L_1 να είναι της μορφής $n(b_1, c_1)$ για κάποιον ακέραιο n.

(3)Να υπάρχει κάποια εμφύτευση ϵ του L_1 στο $\mathbb{C}$, ώστε αν $b_2 = \epsilon(b_1)$, $c_2 = \epsilon(c_1)$, $\Sigma_2 = \epsilon[\Sigma_1]$, $L_2 = \epsilon[L_1]$ και $A = \mathbb{Q}(b_1, b_2, c_1, c_2)$, η διάσταση της $C(A)$ να είναι 2 και κάθε σημείο της C με συντελεστές από το A να είναι της μορφής $n(b_1, c_1) \oplus m(b_2, c_2)$ για κάποιους ακέραιους n, m και $\Sigma_1 \bigcap \Sigma_2 = L_1 \bigcap L_2 = \mathbb{Q}$.

Υπενθυμίζουμε ότι όταν γράφουμε π.χ. $n \in \mathbb{Z}$ εννοούμε τον αντίστοιχο ενδομορφισμό σημείων της καμπύλης,αφού υποθέσαμε ότι το σύνολο των ενδομορφισμών αυτών με πράξεις όπως τις ορίσαμε στην αρχή του κεφαλαίου είναι ισόμορφο με το $\mathbb{Z}$.

Θεώρημα 6 *Αν η C είναι μια καμπύλη που αποτελεί απόδειξη για τον ισχυρισμό 5, τα σύνολα $\Upsilon_1 = \{m(b_1, c_1) : m \in \mathbb{Z}\backslash\{0\}\}, \Upsilon_2 = \{n(b_2, c_2) : n \in \mathbb{Z}\backslash\{0\}\}, \Upsilon_3 = \{n(b_1, c_1) \oplus m(b_2, c_2) : m, n \in \mathbb{Z}, m^2 + n^2 \neq 0, \Upsilon_d = \{n(b_1, c_1) \oplus n((b_2, c_2\} : n \in \mathbb{Z}\backslash\{0\}\}$ είναι υπαρξιακά επί του $\mathbb{Q}$.*

Επισημαίνουμε ότι,όπως και στο θεώρημα 4 επειδή τα σώματα στα οποία αναφέρεται το θεώρημα είναι πεπερασμένες επεκτάσεις του $\mathbb{Q}$,μπορούμε να ταυτίζουμε τα σημεία τους με πεπερασμένες ακολουθίες στοιχείων του$\mathbb{Q}$.Έτσι, όταν αναφερόμαστε στην ορισιμότητα ενός συνόλου,εννοούμε ουσιαστικά την ορισιμότητα κάποιου συνόλου πεπερασμένων ακολουθιών,π.χ δυάδων,τετράδων κλπ. Ορίζουμε πάλι:

Ορισμός 9 *Έστω $m, n \in \mathbb{Z}, m^2 + n^2 \neq 0$.Θα γράφουμε*

$$(d_{n,m}, e_{n,m}) = n(b_1, c_1) \oplus m(b_2, c_2)$$

εννοώντας τις αντίστοιχες ρητές συναρτήσεις,οι οποίες,κατ' αναλογίαν με το λήμμα 1, είναι τελικά μίας μεταβλητής.

Η αντιστοίχηση που σκοπεύουμε να κάνουμε είναι η αντιστοίχηση του τυχόντος φυσικού αριθμού n με το σημείο $d_{n,0}$,για την ακρίβεια εδώ όχι τη ρητή συνάρτηση αλλά το σημείο $n(b_1, c_1)$.Το θεώρημα 6 είναι ακριβές ανάλογο του θεωρήματος 4·η απόδειξή του επίσης θα παραλειφθεί.Κατά συνέπεια,αν αποδειχθεί ο ισχυρισμός 5,θα έχουν επιτευχθεί οι στόχοι Α,Β και για την περίπτωση του $\mathbb{Q}$. Όσον αφορά το Γ,η κατάσταση είναι ακόμα πιο ασαφής απ'οτι στην περίπτωση των ρητών συναρτήσεων επί πεπερασμένων σωμάτων. Όπως και πριν,πρώτο βήμα που αποπειράται κανείς να κάνει για να δείξει την υπαρξιακή ορισιμότητα του γραφήματος του πολλαπλασιασμού είναι να ασχοληθεί με την ορισιμότητα της σχέσης της διαιρετότητας,με απώτερο στόχο την ορισιμότητα κάποιας πιο πολύπλοκης σχέσης,όπως της $|_{KR}$ που είδαμε προηγουμένως. Στην προσπάθεια αυτή θα αποδίδουμε ουσιαστικά διπλό ρόλο στα $x_{n,0}$:θα τα αντιμετωπίζουμε κατά περίπτωση ως ρητές συναρτήσεις ή τα αντίστοιχα σημεία της ελλειπτικής καμπύλης.Μια κατεύθυνση λοιπόν είναι η απόδειξη του ότι αφενός μεν η διαιρετότητα στους ακεραίους είναι ισοδύναμη με κάποια ιδιότητα των αντίστοιχων ρητών συναρτήσεων,αφετέρου δε η ιδιότητα αυτή είναι υπαρξιακά ορίσιμη.Με αυτά κατά νου ο Φειδάς διατυπώνει τους παρακάτω ισχυρισμούς:

Ισχυρισμός 6 *Έστω C ελλειπτική καμπύλη που αποτελεί απόδειξη του ισχυρισμού 5 και m, n ακέραιοι,διάφοροι του μηδενός, ώστε ο m να διαιρεί τον n.Τότε κάθε πόλος του $x_{m,0}$ με πολλαπλότητα k είναι πόλος του $x_{n,0}$ με πολλαπλότητα τουλάχιστον k.*

Ισχυρισμός 7 *Έστω C ελλειπτική καμπύλη που αποτελεί απόδειξη του ισχυρισμού 5.Τότε υπάρχει ακέραιος c,διάφορος του μηδενός ώστε για τους τυχόντες m, n ακέραιους,διάφορους του μηδενός, αν κάθε πόλος του $x_{m,0}$ με πολλαπλότητα k είναι πόλος του $x_{n,0}$ με πολλαπλότητα τουλάχιστον k,το m διαιρεί το cn.*

Μιμούμενοι την τακτική που ακολουθήσαμε για τις ρητές συναρτήσεις επί πεπερασμένου σώματος,θα μπορούσαμε να ορίσουμε κάποια αντίστοιχη με την $|_{KR}$ σχέση,και να προσπαθήσουμε να την αναγάγουμε σε κάποια υπαρξιακά ορίσιμη συνθήκη σχετική με τους πόλους κάποιων ρητών συναρτήσεων.Δυστυχώς η ακριβής επανάληψη της τακτικής αυτής είναι αδιέξοδη,αφού,όπως απέδειξε ο Cornelissen ο αντίστοιχος με τον ισχυρισμό 4 είναι λανθασμένος.Μένει λοιπόν ανοιχτό το πρόβλημα του ποιά ακριβώς είναι η κατάλληλη σχέση της οποίας η υπαρξιακή ορισιμότητα θα οδηγήσει σε μη αποφασίσιμη υπαρξιακή θεωρία και του να βρεθεί κάποια ισοδύναμη ιδιότητα των αντίστοιχων ρητών συναρτήσεων-σημείων κάποιας ελλειπτικής καμπύλης που να είναι υπαρξιακά ορίσιμη.Όσον αφορά αυτό το τελευταίο σκέλος της προσπάθειας,ο Φειδάς έκανε ένα σημαντικό βήμα διατυπώνοντας και αποδεικνύοντας το Λήμμα Υπαρξιακής Διαιρετότητας για το $\mathbb{Q}$.Έιναι εύλογη η προσδοκία ότι το λήμμα αυτό (ή μια λιγότερο ή περισσότερο τροποποιημένη μορφή του) θα αποτελέσει κομβικό σημείο της τελικής λύσης του προβλήματος.Στα παρακάτω θα παρουσιάσουμε την ακριβή διατύπωση και την απόδειξη του λήμματος,βασιζόμενοι σε κάποια θεωρήματα γνωστά από τη Θεωρία Αριθμών.

Κάποια προκαταρτικά:Στα παρακάτω ¨ρίζες¨ και ¨πόλους¨ ενός ρητού αριθμού θα ονομάζουμε τους πρώτους που διαιρούν τον αριθμητή και τον παρονομαστή του αντίστοιχα,όταν αυτός γραφεί ως ανάγωγο κλάσμα ακεραίων.Ανάλογα για την τάξη ενός ρητού σε κάποιον πρώτο.Επίσης με $Pr(-1)$ θα συμβολίζουμε το σύνολο των πρώτων του $\mathbb{Z}$ τέτοιων ώστε η εξίσωση $x^2+1=0$ δεν έχει λύση στο σώμα $\frac{\mathbb{Z}}{\langle p\rangle}$.Τέλος,χρειάζεται να εξηγήσουμε με συντομία τι είναι η πλήρωση ενός σώματος Σ,έννοια που θα χρειαστούμε στην απόδειξη του λήμματος.

Ορισμός 10 *Απόλυτη τιμή στο σώμα Σ ονομάζεται μια συνάρτηση* $|\ |$:$\Sigma \longrightarrow \mathbb{R}$ *με τις ακόλουθες ιδιότητες:*

1)$|x| \geq 0$ *για κάθε* $x \in \Sigma$ *και* $|x| = 0 \longleftrightarrow x = 0$.

2)Για κάθε $x, y \in \Sigma$, *ισχύει* $|xy| = |x| \cdot |y|$.

3)Για κάθε $x, y \in \Sigma$, *ισχύει* $|x+y| \leq |x|+|y|$.*Δεν θα ασχολούμαστε στα επόμενα με την τετριμμένη απόλυτη τιμή ,δηλαδή την* $|x| = 1$ *για κάθε* $x \neq 0$.

Από κάθε απόλυτη τιμή ορίζεται μια μετρική ρ στο Σ θέτοντας $\rho(x, y) = |x-y|$.Χρησιμοποιώντας ένα από τα πλέον βασικά αποτελέσματα της πραγματικής ανάλυσης μπορούμε να πάρουμε τον (ουσιαστικά μοναδικό) πλήρη μετρικό χώρο Σ' στον οποίο το Σ,ως μετρικός χώρος,εμφυτεύεται με τρόπο ώστε η εικόνα του να είναι πυκνό σύνολο.Εκτός από τη δομή του μετρικού χώρου,αυτός ο καινούριος χώρος Σ' κληρονομεί από τον Σ,με πράξεις που ορίζονται φυσιολογικά, και τη δομή του σώματος,και αυτό είναι που μας ενδιαφέρει εδώ.Ο υποδακτύλιος του Σ' που περιέχει τα στοιχεία των οποίων η απόλυτη τιμή $|\ |_p$ είναι ≤ 1 ονομάζεται δακτύλιος εκτίμησης και θα τον συμβολίζουμε με $R(\Sigma')$. Βασικό αποτέλεσμα της σχετικής θεωρίας(Ostrowski,1918) είναι το ότι για το $\mathbb{Q}$ υπάρχουν δύο κατηγορίες πληρώσεων,σωμάτων δηλαδή που κατασκευάζονται με την παραπάνω διαδικασία.Η πρώτη κατηγορία προέρχεται από τη χρήση της συνήθους μετρικής και αποτελείται από το σώμα $\Sigma' = \mathbb{R}$.Η δεύτερη κατηγορία είναι αυτή που προέρχεται από τη χρήση των λεγόμενων $p-$αδικών εκτιμήσεων.

Ορισμός 11 *Έστω p ένας πρώτος αριθμός.Η p-αδική εκτίμηση* $|\ |_p$ *είναι η απόλυτη τιμή που ορίζεται στο* $\mathbb{Q}$ *με τον εξής τρόπο:*

Γράφουμε το τυχόν $x \in \mathbb{Q}\backslash\{0\}$ *στη μορφή* $x = p^r \frac{m}{n}$ *όπου* $r, m, n \in \mathbb{Z}$ *και τα* m, n *δεν διαιρούνται από το p.Θέτουμε τώρα* $|x|_p = \frac{1}{p^r}$.

Θεώρημα 7 *Υπάρχει ένας υπαρξιακός τύπος με δύο ελεύθερες μεταβλητές* $\varphi(x, y)$ *τέτοιος ώστε:*

$i)$ Έστω ότι $x, y \in \mathbb{Q} \backslash \{0\}$, ο $\varphi(x, y)$ αληθεύει και για τον $p \in Pr(-1)$ η τάξη $ord_p(x)$ είναι περιττός αριθμός.Τότε $ord_p(xy^{-2}) \geq 0$.

$ii)$ Έστω ότι για κάποια $x, y \in \mathbb{Q}$ ικανοποιούνται οι παρακάτω τέσσερις συνθήκες:

$\alpha)x > 0, y \neq 0$

$\beta)$Ο x έχει τουλάχιστον μιά ρίζα ή πόλο στο $Pr(-1)$.

$\gamma)$Για κάθε ρίζα ή πόλο p του x με $p \in Pr(-1)$ ώστε η τάξη $ord_p(x)$ να είναι περιττός,ισχύει $ord_p(xy^{-2}) \geq 0$ και

$\delta)$Αν $x = tz^2$ για κάποιον ακέραιο t που δεν διαιρείται από το τετράγωνο κανενός πρώτου και κάποιον ρητό z,τότε $ord_p(zy^{-1}) \geq 1$ ή $t \equiv 1$ ή 2 ή 5 mod 8. Τότε ο $\varphi(x, y)$ αληθεύει.

Απόδειξη

Ισχυριζόμαστε ότι για τον τύπο

$$\varphi(x, y) \longleftrightarrow \exists a, b, c \in \mathbb{Q}[1 + x(y^{-2} + c^2) = a^2 + b^2] \tag{36}$$

αληθεύουν τα i, ii του θεωρήματος 7.

Πρώτα αποδεικνύουμε το i.Έστω ότι για κάποια $x, y \in \mathbb{Q} \backslash \{0\}$, ο $\varphi(x, y)$ αληθεύει και για τον $p \in Pr(-1)$ η τάξη $ord_p(x)$ είναι περιττός αριθμός,αλλά $ord_p(xy^{-2}) < 0$.Είναι εύκολο να δούμε ότι επειδή ακριβώς οι y^2 και c^2 είναι τετράγωνα,όλοι οι πόλοι και οι ρίζες τους είναι άρτιας τάξης. Ισχύει τώρα γενικά για τυχαίους ρητούς r, s ότι

$$ord_p(r^2 + s^2) = min(ord_p(r^2), ord_p(s^2)) \tag{37}$$

όπως μπορεί εύκολα να δείξει κανείς γράφοντας τα r, s ως ανάγωγα κλάσματα και παίρνοντας περιπτώσεις ανάλογα με τις τάξεις τους.Έτσι συμπεραίνουμε ότι η τάξη $ord_p(xy^{-2} + xc^2)$ είναι περιττός και αρνητικός αριθμός,και άρα και η τάξη του $ord_p(1 + x(y^{-2} + c^2))$. Όμως,ξανά από την (37),η τάξη $ord_p(a^2 + b^2)$ είναι ίση με την τάξη κάποιου τετραγώνου,δηλαδή άρτιος αριθμός.Επειδή τώρα ισχύει και η (36),καταλήγουμε σε άτοπο,οπότε πρέπει $ord_p(xy^{-2}) > 0$, ο.ε.δ.

Για το $ii)$ τώρα :Παρατηρούμε ότι αρκεί,υποθέτοντας ότι ισχύουν τα $\alpha) - \delta)$ να δείξουμε ότι η εξίσωση

$$(1 + xy^{-2})d^2 + xc^2 - a^2 - b^2 \tag{38}$$

έχει μη τετριμμένη λύση στο $\mathbb{Q}$.Πράγματι,αν στη λύση αυτή $d \neq 0$,είναι προφανές ότι ο $\varphi(x, y)$ αληθεύει.Αν $d = 0$,τότε ισχύει $xc^2 = a^2 + b^2$ και επειδή αν $c = 0$, αναγκαστικά $a = b = c = 0$,πρέπει $c \neq 0$.Όμως από το $\beta)$ έπεται ότι και το xc^2, άρα και το $a^2 + b^2$ έχουν τουλάχιστον μία ρίζα ή πόλο περιττής πολλαπλότητας.Αυτό το τελευταίο αντιφάσκει με την (37).

Για να δείξουμε τώρα ότι η (38) έχει μη τετριμμένη λύση θα επικαλεστούμε ένα θεώρημα των Hasse και Minkowski,το οποίο δε θα αποδείξουμε:

Θεώρημα 8 *Μια ομογενής εξίσωση βαθμού 2 έχει μη τετριμμένη λύση σε ένα σώμα Σ εάν και μόνον εάν έχει μη τετριμμένη λύση σε κάθε πλήρωση του Σ.*

Αρκεί λοιπόν να δείξουμε ότι η (38) έχει μη τετριμμένη λύση σε κάθε πλήρωση του $\mathbb{Q}$.Όπως είδαμε παραπάνω,έχουμε να εξετάσουμε δύο ομάδες περιπτώσεων.Η πρώτη και πιο εύκολη είναι το $\mathbb{R}$.Πράγματι,επειδή από το α) έχουμε ότι $x > 0$,ισχύει ότι $1 + xy^{-2} > 0$ και $\sqrt{1 + xy^{-2}} \in \mathbb{R}$.Θέτοντας στην (38) $d = 1, c = 0, a = 0, b = \sqrt{1 + xy^{-2}}$ έχουμε το ζητούμενο.

Η δεύτερη ομάδα περιπτώσεων είναι αυτή που προέρχεται από τις $p-$αδικές πληρώσεις του $\mathbb{Q}$, τις οποίες θα συμβολίζουμε με Σ_p.Θα εξετάσουμε χωριστά την περίπτωση για $p = 2$ ενώ θα παραλείψουμε την απόδειξη για $p \neq 2$.Θα δείξουμε λοιπόν πρώτα ότι η (38) έχει μη τετριμμένη λύση στο Σ_p για κάθε $p \neq 2$.Μας χρειάζονται κάποια ακόμα αποτελέσματα από τη Θεωρία Αριθμών. Συγκεκριμένα, αποδεικνύονται τα εξής:

Λήμμα 8 *Σε κάθε πεπερασμένο σώμα F, και για κάθε $u \in F\backslash\{0\}$, η εξίσωση $u{z_1}^2 + {z_2}^2 + {z_3}^2 = 0$ έχει μη τετριμμένη λύση.*

Λήμμα 9 *(Η μορφή του Λήμματος του Hensel που μας ενδιαφέρει)Έστω $q(z)$ πολυώνυμο με συντελεστές από το $R(\Sigma_p)$ και $a_0 \in R(\Sigma_p)$ ώστε*

$$|q(a_o)|_p < |q'(a_0)^2|_p \tag{39}$$

όπου q' η τυπική παράγωγος του q.Τότε η ακολουθία

$$a_{i+1} = a_i - \frac{q(a_i)}{q'(a_i)} \tag{40}$$

συγκλίνει σε μια ρίζα a του $q(z)$ στο $R(\Sigma_p)$.Επιπλέον

$$|a - a_0|_p \leq \left|\frac{q(a_0)}{q'(a_0)^2}\right|_p < 1. \tag{41}$$

Έστω κατάρχήν ότι $p \notin Pr(-1)$.Τότε αντικαθιστώντας το b με 1 παρατηρούμε ότι η εξίσωση $0 \equiv a^2 + b^2 \ (mod\ p)$ έχει λύσεις με $ab \not\equiv 0 \ (mod\ p)$.Παρατηρούμε τώρα ότι αφού το a είναι ακέραιος,ισχύει $|a|_p \leq 1$, δηλ.$a \in R(\Sigma_p)$.Επίσης το πολυώνυμο $z^2 + 1$ για $z = a$ παίρνει τιμή κάποιο πολλαπλάσιο του p διάφορο του μηδενός δηλ.$|a^2 + 1|_p < 1$, ενώ η τυπική παράγωγός του στο a παίρνει τιμή $2a$, δηλ.κάποιον ακέραιο που,επειδή ακριβώς $p \neq 2$, δεν είναι πολλαπλάσιο του p, οπότε $|(2a)^2|_p = 1$.Έτσι μπορούμε να επικαλεστούμε το λήμμα 9 για να δείξουμε ότι το πολυώνυμο $z^2 + 1$ έχει κάποια ρίζα στο $R(\Sigma_p)$ η οποία προφανώς είναι διάφορη του μηδενός.Έτσι τελικά υπάρχουν $a, b \in \Sigma_p$ με $ab \neq 0$ ώστε $a^2 + b^2 = 0$.Αρκεί τώρα να θέσουμε $c = d = 0$ για να έχουμε τη ζητούμενη λύση της (38).

Έστω τώρα ότι $p \in Pr(-1)$ και ότι η τάξη του x στο $p, ord_p(x)$ είναι περιττή.Τότε από το γ) έχουμε ότι η τάξη $ord_p(xy^{-2})$ είναι ≥ 0 και προφανώς περιττή.Άρα για το πολυώνυμο(με μεταβλητή το z)$z^2 - 1 - xy^{-2}$ μπορούμε να εφαρμόσουμε το λήμμα 9,με τρόπο παρόμοιο με αυτόν που εξηγήσαμε παραπάνω,ξεκινώντας από $z = 1$ και συμπεραίνοντας τελικά ότι το πολυώνυμο $z^2 - 1 - xy^{-2}$ έχει μη τεριμμένη ρίζα στο Σ_p.Αρκεί τώρα να θέσουμε στην(38) όπου a τη ρίζα αυτή,$c = b = 0$ και $d = 1$.

Για την περίπτωση όπου $p \in Pr(-1)$ και η τάξη του x στο $p, ord_p(x)$ είναι άρτια,θέτουμε πρώτα στην (38) $c = 1, d = 0$.Έστω τώρα $x = \frac{x_1}{x_2}p^i$ όπου τα x_1, x_2

είναι πρώτοι μεταξύ τους και δεν διαιρούνται από το p και $x' = \frac{x_1}{x_2}$.Από το λήμμα 8 για το σώμα $\mathbb{Z}_p$ έχουμε ότι η εξίσωση $-x_1x_2{z_1}^2 + {z_2}^2 + {z_3}^2 = 0$ έχει μη τετριμμένη λύση στο $\mathbb{Z}_p$.Αν για αυτή τη λύση $z_1 = 0$ τότε $z_2 = z_3 = 0$, άτοπο ή $p \notin Pr(-1)$,επίσης άτοπο.Άρα και η εξίσωση $-x_1x_2 + {z_2}^2 + {z_3}^2 = 0$ έχει μη τετριμμένη λύση στο $\mathbb{Z}_p$.Εφαρμόζουμε τώρα το λήμμα 9 για το πολυώνυμο(με μεταβλητή το z_2)$-x_1x_2 + {z_2}^2 + {z_3}^2 = 0$ θέτοντας όπου z_3 κάποιον ακέραιο που δίννεται από τη ρίζα του στο $\mathbb{Z}_p$.Σε κάθε περίπτωση έχουμε μία μη τετριμμένη λύση της $-x_1x_2 + {z_2}^2 + {z_3}^2 = 0$ στο Σ_p.Μπορούμε τώρα να πάρουμε $a = \frac{z_2}{x_2}$ και $b = \frac{z_3}{x_2}$.

Μένει η περίπτωση για $p = 2$.Θα παραλείψουμε την απόδειξη για την περίπτωση αυτή,η οποία πάντως στηρίζεται στο ίδιο βασικό εργαλείο,το Λήμμα του Hensel και για την ακρίβεια σε μια παραλλαγή του,καθώς και στη μελέτη κάποιων εξισώσεων mod 8 στην οποία χρησιμοποιείται και το δ) της υπόθεσης.

5 Ένα πρόβλημα ισοδύναμο με το ΔΠΧΡ

Θα τελειώσουμε με κάτι αρκετά διαφορετικό,τη διατύπωση με κομψό τρόπο ενός προβλήματος ισοδύναμου με το ΔΠΧ. Στην εισάγωγή είδαμε πώς μπορεί το ΔΠΧΡ να αναχθεί στο ΔΠΧ.Αφού όμως δεν υπάρχει αλγόριθμος για το ΔΠΧ,μια τέτοια αναγωγή δεν είναι ιδιαίτερα χρήσιμη.Αν όμως καταφέρναμε να αποδείξουμε ότι το ΔΠΧΡ είναι το ίδιο δύσκολο με κάποιο γνήσιο υποπρόβλημα του ΔΠΧ,με το αντίστοιχο ερώτημα δηλαδή για μια μικρότερη κλάση εξίσώσεων,ίσως να είχαμε κάνει ένα πρώτο βήμα προς την λύση του ΔΠΧΡ.Πράγματι,μία πιο δύσκολη,αλλά και πιο σημαντική κατασκευή,που δείχνει ότι το πρόβλημα εύρεσης αλγορίθμου που να αποφασίζει αν τυχόν πολυώνυμο με ακέραιους συντελεστές έχει ρητές ρίζες ανάγεται στο πρόβλημα έυρεσης αλγορίθμου που να αποφασίζει αν τυχόν ομογενές πολυώνυμο(άθροισμα μονωνύμων του ίδιου βαθμού)με ακέραιους συντελεστές έχει μη τετριμμένη ρίζα στους ακεραίους(δηλαδή ρίζα στην οποία τουλάχιστον μία μεταβλητή παίρνει τιμή $\neq 0$ και αντιστρόφως,είναι η παρακάτω:

Για την αντίστροφη κατεύθυνση πρώτα: Έστω

$$P(x_1, ..., x_n) = 0 \tag{42}$$

μια ομογενής διοφαντική εξίσωση.Αν έχει μια μη τετριμμένη ακέραια λύση στην οποία π.χ. $x_i \neq 0$ τότε επειδή όλα τα μονώνυμα είναι του ίδιου βαθμού η εξίσωση

$$P(q_1, ..., q_{i-1}, 1, q_{i+1}, q_n) = 0 \tag{43}$$

έχει μία ρητή λύση,αυτή που δίνεται ως $q_k = \frac{x_k}{x_i}$.Αντίστροφα,από κάθε ρητή λύση $q_1, ..., q_{i-1}, q_{i+1}, q_n$ της (43),μπορούμε να πάρουμε, πολλαπλασιάζοντας με κατάλληλο d μια μη τετριμμένη ακέραια λύση της $P(x_1, ..., x_n) = 0 : x_i = d$, $x_j = dq_j$ για $j = 1, ..., i-1, i+1, ...n$.Τελικά,η (42) έχει μη τετριμμένη ακέραια λύση εάν και μόνον εάν τουλάχιστον μία από τις n εξισώσεις

$$\begin{gathered} P(1, ..., x_n) = 0 \\ \vdots \\ P(x_1, ..., 1) = 0 \end{gathered} \tag{44}$$

έχει ρητή λύση.Έτσι,αν υπήρχε αλγόριθμος που να αποτελεί λύση του ΔΠΧΡ εφαρμόζοντάς τον n φορές στις(45)θα μπορούσαμε να αποφανθούμε για το αν η (42) έχει μη τετριμμένη ακέραια λύση.

Για την ευθεία κατεύθυνση της αναγωγής: Το πρώτο πράγμα που σκέφτεται κανείς είναι να αναγάγει το πρόβλημα της ύπαρξης ρητής λύσης της διοφαντικής εξίσωσης

$$P(q_1, ..., q_n) = 0 \tag{45}$$

σ' εκείνο της ύπαρξης μη τετριμμένης λύσης της ομογενούς εξίσωσης

$$P'(q_1, ..., q_n, u) = u^g P(\frac{q_1}{u}, ..., \frac{q_n}{u}) = 0 \tag{46}$$

όπου g ο βαθμός του πολυωνύμου P.Πράγματι,αν το P έχει ρητή ρίζα,τότε το P' έχει μη τετριμμένη ακέραια ρίζα.Το αντίστροφο όμως δεν ισχύει πάντα,επειδή μπορεί το P' να έχει κάποια μη τετριμμένη λύση για την οποία όμως $u = 0$.Το λεπτό σημείο της απόδειξης είναι ακριβώς αυτό:η κατασκευή μιας ομογενούς διοφαντικής εξίσωσης που να εκφράζει τη συνθήκη

$$q_1{}^2 + \cdots + q_n{}^2 \neq 0 \Longrightarrow u \neq 0 \tag{47}$$

Για κάθε αριθμό k ορίζουμε μια ακολουθία ως εξής:

$$a_k(0) = 0, \qquad a_k(1) = 1, \qquad a_k(n+2) = ka_k(n+1) - a_k(n) \tag{48}$$

Ισχυρισμός 8 *Αν υπάρχει i ώστε*

$$x = a_k(i+1), y = a_k(i) \tag{49}$$

ή

$$y = a_k(i+1), x = a_k(i) \tag{50}$$

τότε το ζεύγος x, y είναι λύση της εξίσωσης

$$x^2 - kxy + y^2 = 1 \tag{51}$$

Θα χρησιμοποιήσουμε τον ισχυρισμό για να αποδείξουμε το ζητούμενο και θα τον αποδείξουμε αμέσως μετά. Για καθε $k \geq 2$ είναι εύκολο να δει κανείς (αποδεκνύεται με επαγωγή) ότι η ακολουθία που ορίζεται από την (48)είναι γνησίως αύξουσα,οπότε από τον ισχυρισμό έπεται ότι η (51) έχει για κάθε φυυσικό c μια λύση x, y με $x \geq c$.Αντίθετα,η εξίσωση

$$x^2 - 4xy + y^2 = 0 \tag{52}$$

έχει μόνο την τετριμμένη (ακέραια) λύση,αφού

$$x^2 - 4xy + y^2 = (x - (2 + \sqrt{3})y)(x - (2 - \sqrt{3})y) \tag{53}$$

Όσον αφορά τις ακέραιες λύσεις της εξίσωσης

$$x^2 - kxy + y^2 = u^4 \tag{54}$$

έχουμε λοιπόν καταλήξει στα εξής:Αν $u = 0$ τότε έχει μόνο την τετριμμένη λύση ενώ αν $u \neq 0$ έχει λύσεις με απεριόριστα μεγάλο x.[13] Χρησιμοποιώντας λοιπόν την (54) διαπιστώνουμε ότι η (47) είναι ισοδύναμη με την

$$x \geq q_1{}^2 + \cdots + q_n{}^2. \tag{55}$$

Χρησιμοποιώντας το Θεώρημα του Lagrange μπορούμε τώρα να γράψουμε:

$$x = q_1{}^2 + \cdots + q_n{}^2 + w_1{}^2 + w_2{}^2 + w_3{}^2 + w_4{}^2 \tag{56}$$

$$y = z_1{}^2 + z_2{}^2 + z_3{}^2 + z_4{}^2 \tag{57}$$

[13] Ο λόγος που χρησιμοποιούμε το u^4 και όχι το u^2 είναι το ότι θέλουμε να πετύχουμε την ομογένεια μιας εξίσωσης που θα κατασκευάσουμε λίγο παρακάτω.

προσθέτοντας τις απαραίτητες μεταβλητές.Αντικαθιστώντας τώρα τις (56)και (57)στην (54)παίρνουμε την ομογενή εξίσωση βαθμού 4

$$
\begin{gathered}
({q_1}^2 + \cdots + {q_n}^2 + {w_1}^2 + {w_2}^2 + {w_3}^2 + {w_4}^2)^2 \\
-4({q_1}^2 + \cdots + {q_n}^2 + {w_1}^2 + {w_2}^2 + {w_3}^2 + {w_4}^2)({z_1}^2 + {z_2}^2 + {z_3}^2 + {z_4}^2) \\
+({z_1}^2 + {z_2}^2 + {z_3}^2 + {z_4}^2)^2 - u^4 = 0
\end{gathered}
$$

την οποία χάριν συντομίας θα συμβολίζουμε

$$\Lambda(q_1, ..., u) = 0. \tag{58}$$

Θα συνδυάσουμε τώρα με κατάλληλο τρόπο τις (58)και (46) για να πάρουμε μια καινούρια ομογενή εξίσωση:

$$\Lambda(q_1, ..., u)^{2g} + P'(q_1, ..., q_n, u)^8 = 0 \tag{59}$$

με βαθμό $8g$.Τελικά,όπως ήταν ο στόχος μας,βρήκαμε την ομογενή διοφαντική εξίσωση (59)που έχει μη τετριμμένη ακέραια λύση εάν και μόνον εάν η (45)έχει ρητή λύση.Μένει κάτι ακόμα:

Απόδειξη του ισχυρισμού 1

Με βάση την ακολουθία που ορίσαμε στην (48) μπορούμε να ορίσουμε μια ακολουθία πινάκων 2×2 ως εξής:

$$A_k(n) = \begin{pmatrix} a_k(n+1) & -a_k(n) \\ a_k(n) & -a_k(n-1) \end{pmatrix} \tag{60}$$

όπου $a_k(-1) = -1$. Μπορούμε εύκολα να δείξουμε με επαγωγή ότι αν

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad J_k = \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix} \tag{61}$$

τότε $A_k(0) = B, A_k(n+1) = A_k(n)J_k$.Έτσι τελικά ισχύει $A_k(n) = {J_k}^n$ και υπολογίζοντας τις διακρίνουσες παίρνουμε: $det(B) = det(J_k) = 1$ και άρα

$$det(A_k(n)) = 1 \tag{62}$$

για κάθε n.Από την (62) παίρνουμε τελικά το ζητούμενο αφού:

$$
\begin{aligned}
1 = a_k(n+1)^2 - a_k(n)a_k(n+2) &= a_k(n+1)^2 - a_k(n)(ka_k(n+1) - a_k(n)) \\
&= a_k(n+1)^2 - ka_k(n+1)a_k(n) + a_k(n)^2.
\end{aligned} \tag{63}
$$

Παρά το αυτόνομο ενδιαφέρον αυτής της αναγωγής,πρέπει να σημειώσουμε ότι,όπως είδαμε και στα προηγούμενα, στις προσπάθειες για τη λύση του ΔΠΧΡ χρησιμοποιούνται πολύ διαφορετικές τεχνικές που δεν έχουν να κάνουν (τουλάχιστον άμεσα) με κάποιον αλγόριθμο που θα έλυνε κάποιο υποπρόβλημα του ΔΠΧ.

6 Βιβλιογραφία

Η διπλωματική αυτή εργασία αποτελεί σε μεγάλο βαθμό παρουσίαση των δημοσιεύσεων του Θανάση Φειδά πάνω στο θέμα,και συγκεκριμένα των:

1)T.Pheidas:*An effort to prove that the existential theory of* $\mathbb{Q}$ *is undecidable*, Contemporary Mathematics,Volume 270,(2000)237-252

2)T.Pheidas:*Hilbert's tenth problem for fields of rational functions over finite fields*,Inventiones Mathamaticae 103(1991)1-8

3)T.Pheidas:*Extensions of Hilbert's Tenth Problem*,Journal of Symbolic Logic,59-2(1994)372-397

4)T.Pheidas and K.Zahidi:*Undecidability of existential theories of rings and fields:a survey*,Contemporary Mathematics,Volume 270(2000)49-105

Επίσης χρήσιμα ήταν τα εξής:

5)Y. Matiyasevich:*Hilbert's Tenth Problem*,MIT Press,1993

6)Y. Matiyasevich:*Hilbert's Tenth Problem:What was Done and What Is To Be Done*,Contemporary Mathematics,Volume 270(2000)1-47

7)G.Cornelissen and K.Zahidi:*Topology Of Diophantine Sets:Remarks on Mazur's Conjectures*,Contemporary Mathematics,Volume 270(2000)253-260

8)J.Denef:*Hilbert's Tenth Problem for quadratic rings*,Proceedings Of the American Mathematical Sciety,48(1975)214-220

9)J.Denef:*The Diophantine Problem For Polynomial Rings and Fields Of Rational Functions*,Transactions Of The American Mathematical Society,242(1978)391-399

10)J.Denef and L.Lipshitz:*Diophantine Sets Over Some Rings Of Algebraic Integers* ,Journal of The London Mathematical Society,(2),18(1978)385-391

11)J.Robinson:*Definability and Decision Problems In Arithmetic*,Journal Of Symbolic Logic,14(1949)98-114

12)Serge Lang:*Algebraic Number Theory*,Springer-Verlag,1986

13)Nathan Jacobson:*Basic Algebra II*,,Hindustan Publishing Corporation,1991

14)Dave Husemöller:*Elliptic Curves*,Springer-Verlag,1987

Στο 3) και στο 4) υπάρχει εκτενέστατη βιβλιογραφία επί σχετικών θεμάτων.

Περιεχόμενα