Σκέψεις για τα Μαθηματικά,
100 χρόνια από την ίδρυση
της Ελληνικής Μαθηματικής Εταιρείας

Αριθμητική Γεωμετρία, ιστορία, επιτεύγματα και μέλλον

Γιάννης Αντωνιάδης & Αριστείδης Κοντογεώργης

1. Εισαγωγή Η Θεωρία των Αριθμών έχει χαρακτηριστεί από τον Gauss ως η Βασίλισσα των επιστημών. Πολλές φορές όμως η διδασκαλία της δίνει την αίσθηση ότι αποτελείται από μια σειρά ευφυών τεχνασμάτων μακριά από τον κύριο κορμό των Μαθηματικών. Ένας από τους στόχους της εργασίας αυτής είναι να δείξουμε ότι ο παραπάνω ισχυρισμός απέχει πολύ από την πραγματικότητα. Η Θεωρία Αριθμών σχετίζεται με κάθε είδους Μαθηματική Θεωρία και τεχνική από τομείς που αρχικά φαντάζουν ξένοι όπως η Γεωμετρία, η Τοπολογία, η Αριθμητική Ανάλυση ή η Μαθηματική Φυσική. Δεν αρκεί ο χώρος για να περιγράψουμε κάθε δυνατή σχέση της Θεωρίας Αριθμών με τα Μαθηματικά, οπότε θα περιοριστούμε στους τομείς που γνωρίζουμε καλύτερα, την *Αριθμητική Γεωμετρία* και την *Θεωρία Κλάσεων Σωμάτων* αλλά και τις προσπάθειες βασισμένες στις δύο παραπάνω θεωρίες για την απόδειξη του τελευταίου Θεωρήματος του Fermat.

2. Αλγεβρική οπτική της Γεωμετρίας Από τον καιρό του Ευκλείδη και του περίτεχνου συστήματός του, η θέαση της έννοιας της Γεωμετρίας έχει αλλάξει δραματικά. Έγινε σαφές ότι ένα γεωμετρικό αντικείμενο μπορεί να περιγραφεί ικανοποιητικά από τον δακτύλιο συναρτήσεων που ορίζονται πάνω του. Θα μπορούσαμε να πούμε ότι η συνειδητοποίηση της παραπάνω αρχής ήρθε από πολλούς τομείς των Μαθηματικών όπως η θεωρία των επιφανειών Riemann, η Αλγεβρική Γεωμετρία και η Συναρτησιακή Ανάλυση. Ας προσπαθήσουμε να εξηγήσουμε τους παραπάνω συσχετισμούς.

2.1. Επιφάνειες Riemann Ο Riemann θέλησε να μελετήσει την έννοια μιγαδικών συναρτήσεων οι οποίες ορίζονται για παράδειγμα ως n-στες ρίζες πολυωνύμων $f(x) \in \mathbb{C}[x]$, όπως η $\sqrt[n]{f(x)}$. Η θεώρηση αυτή οδήγησε στα σώματα μερομόρφων συναρτήσεων, τα οποία μπορούν να προσεγγιστούν ως αλγεβρικές επεκτάσεις του σώματος ρητών συναρτήσεων $\mathbb{C}(x)$ και οδηγούν σε αλγεβρικές καμπύλες, οι οποίες ορίζονται μέσω μιας εξίσωσης $y^n = f(x)$. Η ιδέα της επιφάνειας Riemann η οποία προκύπτει από n το πλήθος αντίγραφα του μιγαδικού επιπέδου, τα οποία κολλάνε μεταξύ τους στις ρίζες του πολυωνύμου $f(x)$, είχε γεννηθεί. Επιπρόσθετα έγινε σαφές ότι όλη η γεωμετρία της αλγεβρικής καμπύλης αντανακλάται στις αλγεβρικές ιδιότητες του σώματος μερομόρφων συναρτήσεών της $\mathcal{M}(X)$. Δεν πρέπει να παραβλέψουμε την σημασία της ανάλυσης μίας συνάρτησης $f \in \mathcal{M}(X)$ ως δυναμοσειράς $f(z) = \sum_{i=0}^{\infty} a_i z^i$, μέσω ενός χάρτη $z : X \to \mathbb{C}$. Η ανάλυση αυτή όπως θα δούμε υπήρξε κινητήρια δύναμη της p-αδικής ανάλυσης. Για περισσότερες λεπτομέρειες με έμφαση στην σχέση με την θεωρία Galois και την Αλγεβρική Τοπολογία παραπέμπουμε στο [13].

2.2 Αλγεβρική Γεωμετρία Η Αλγεβρική Γεωμετρία αποτελεί έναν ευρύτατο κλάδο των Μαθηματικών ο οποίος διαπερνά και σχετίζεται με σχεδόν κάθε Μαθηματική θεωρία. Η πηγή της βασίζεται στο πρόβλημα της περιγραφής του χώρου λύσεων ενός συστήματος πολυωνυμικών εξισώσεων

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

Ασφαλώς ένα τέτοιο σύστημα είναι πολύ δύσκολο να λυθεί επακριβώς. Γρήγορα όμως έγινε αντιληπτό ότι οι λύσεις δεν εξαρτώνται τόσο από τα πολυώνυμα, αλλά από το ιδεώδες I που αυτά παράγουν μέσα στον δακτύλιο των πολυωνύμων $R = \mathbb{C}[x_1, \ldots, x_n]$. Επίσης ισοδύναμα ορίζεται και ο δακτύλιος πηλίκο

R/I. Στην περίπτωση που το ιδεώδες I είναι ριζικό ιδεώδες, δηλαδή $f^m \in I$ αν και μόνο αν $f \in I$, τότε ο δακτύλιος R/I είναι με φυσιολογικό τρόπο ο δακτύλιος των πολυωνυμικών συναρτήσεων πάνω στο σύνολο μηδενισμού $V(I)$ των πολυωνύμων $f_1, \ldots, f_m$. Πράγματι δύο πολυωνυμικές συναρτήσεις ϕ_1, ϕ_2 από τον περιβάλλοντα χώρο $\mathbb{C}^n$ στο $\mathbb{C}$ περιορίζονται στην ίδια συνάρτηση στο $V(I)$ αν η διαφορά τους είναι η μηδενική συνάρτηση στο $V(I)$ και μπορεί να αποδειχθεί ότι κάποια δύναμη της ανήκει στο I. Ακόμα και στην περίπτωση που το I δεν είναι ριζικό, ο δακτύλιος R/I αντανακλά απειροστές ιδιότητες του V/I. Τα σύνολα μηδενισμού $V(I)$ ιδεωδών ονομάζονται ομοπαραλληλικές αλγεβρικές πολλαπλότητες, ενώ οι αντίστοιχοι δακτύλιοι R ονομάζονται δακτύλιοι κανονικών συναρτήσεων.

Οι ομοπαραλληλικές πολλαπλότητες δεν είναι συμπαγείς και χρειάζονται την κατάλληλη έννοια συμπληρώματος στο άπειρο. Αυτό επιτυγχάνεται με την έννοια των προβολικών αλγεβρικών συνόλων, τα οποία είναι υποσύνολα του προβολικού χώρου $\mathbb{P}^r$ και ορίζονται ως τόποι μηδενισμού ιδεωδών που παράγονται από ομογενή πολυώνυμα. Αρχικά η Αλγεβρική Γεωμετρία περιορίστηκε σε αλγεβρικές πολλαπλότητες οι οποίες ορίζονται πάνω από το σώμα $\mathbb{C}$. Ο André Weil ήταν από τους πρώτους που κατανόησαν την ανάγκη της ανάπτυξης της Αλγεβρικής Γεωμετρίας πάνω από μη αλγεβρικά κλειστά σώματα αλλά και πάνω από σώματα πεπερασμένης χαρακτηριστικής, για τις ανάγκες της επίλυσης Διοφαντικών εξισώσεων και όχι μόνο.

Ας δούμε ένα παράδειγμα της φιλοσοφίας του Weil. Θεωρούμε μία αλγεβρική προβολική πολλαπλότητα που ορίζεται στο σώμα $\bar{\mathbb{F}}_p$ και ας θεωρήσουμε το πλήθος των λύσεων N_r πάνω από κάθε σώμα $\mathbb{F}_{p^r}$. Σχηματίζουμε την γεννήτρια συνάρτηση:

$$Z(X,t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) \in \mathbb{Q}[[t]].$$

Για παράδειγμα αν $X = \mathbb{P}^1$ τότε υπολογίζουμε ότι $N_r = \#\mathbb{P}^1(\mathbb{F}_{p^r}) = p^r + 1$ και υπολογίζουμε ότι

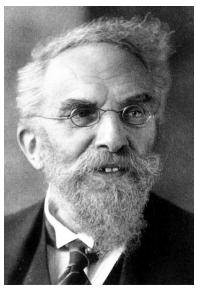
$$Z(\mathbb{P}^1, t) = \exp\left(\sum_{r=1}^{\infty} (q^r + 1)\frac{t^r}{r}\right) = \frac{1}{(1-t)(1-qt)}.$$

Ο Weil διατύπωσε μία σειρά από εικασίες

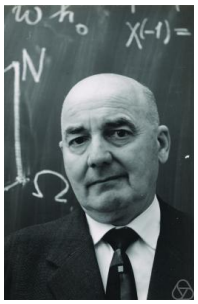
(1) Η $Z(X,t)$ είναι ρητή συνάρτηση του t και γράφεται ως $Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$
(2) $Z(X, 1/q^n t) = \pm q^{nE/2} t^E Z(X,t)$, όπου $E = \Delta \cdot \Delta, \Delta \subset X \times X$.
(3) $P_0(t) = 1 - t$, $P_{2n} = 1 - q^n t$ και για κάθε $1 \leq i \leq 2n-1$, $P_i(t) \in \mathbb{Z}[t]$, $P_i(t) = \prod_j (1 - a_{ij}t)$ με $|a_{ij}| = q^{1/2}$.

Θεωρούμε το $x \in \bar{\mathbb{F}}_p$. Είναι γνωστό ότι $x \in \mathbb{F}_{p^r} \Leftrightarrow x^{p^r} = x$. Τα σταθερά σημεία του μορφισμού Frobenius $x \mapsto x^{p^r}$ του συνόλου V είναι οι λύσεις που ζητάμε. Ο Weil παρατήρησε όταν αν είχε μία κατάλληλη θεωρία ομολογίας για αλγεβρικές πολλαπλότητες τότε θα μπορούσε να μετρήσει το πλήθος N_r με βάση τον τύπο σταθερών σημείων του Lefschetz και να αποδείξει τις παραπάνω εικασίες. Μία τέτοια θεωρία αναπτύχθηκε από τον A. Grothendieck και θα την περιγράψουμε συνοπτικά στην συνέχεια.

2.3. p-αδική Ανάλυση Είναι σαφές ότι οι δακτύλιοι $\mathbb{Z}$ και $k[x]$, όπου το k είναι ένα σώμα, μοιράζονται πολλά κοινά χαρακτηριστικά. Είναι και οι δύο περιοχές κυριών ιδεωδών,



είναι εφοδιασμένοι με έναν αλγόριθμο διαίρεσης κτλ. Ο Kurt Hensel θέλησε να προχωρήσει την αναλογία ακόμα περισσότερο ορίζοντας την έννοια της δυναμοσειράς γύρω από ένα πρώτο ιδεώδες $p \lhd \mathbb{Z}$. Ας ξεκινήσουμε παρατηρώντας ότι στην περίπτωση $k = \mathbb{C}$ τα μέγιστα ιδεώδη του δακτυλίου $\mathbb{C}[x]$ είναι ακριβώς τα κύρια ιδεώδη $\langle x - a \rangle$, όπου το a διατρέχει τους μιγαδικούς αριθμούς. Η δε σειρά Taylor ενός πολυωνύμου $f(x) \in \mathbb{C}[x]$ δεν είναι τίποτε άλλο παρά μια σειρά διαιρέσεων πολυωνύμων. Πράγματι, στο $f(x) = a_0 + a_1(x - a) + \cdots a_n(x - a)^n$ ο σταθερός συντελεστής είναι το υπόλοιπο της διαίρεσης του $f(x)$ με $x - a$, στην συνέχεια το a_1 είναι το υπόλοιπο της διαίρεσης του πολυωνύμου $(f(x) - a_0)/(x - a)$ με $x - a$ κτλ. Είναι σαφές ότι σε μια περιοχή του σημείου a ένα πολυώνυμο είναι κοντά στο 0 αν διαιρείται με όσο το δυνατόν μεγαλύτερη δύναμη του $x - a$. Δεδομένης μιας ποσότητας $0 < c < 1$ μπορούμε να ορίσουμε μία νόρμα για $f \in \mathbb{C}[x]$ ορίζοντας $\|f\| = c^{\nu}(f)$ όπου $\nu(f)$ η μεγαλύτερη δύναμη ώστε $(x - a)^{\nu(f)} \mid f(x)$. Θεωρούμε ότι $\nu(0) = \infty$, άρα $\|0\| = 0$. Τα παραπάνω ορίζουν μία μετρική χωρίς όμως ο χώρος των πολυωνύμων να είναι πλήρης μετρικός χώρος. Μετά από μία διαδικασία πλήρωσης (ακολουθίες Cauchy modulo μηδενικές ακολουθίες) καταλήγουμε στον χώρο των τυπικών δυναμοσειρών $\mathbb{C}[[x]]$, ο οποίος περιλαμβάνει τα αναπτύγματα Taylor.



Η ιδέα του Hensel ήταν να εφαρμόσει την παρακάτω θεωρία στον δακτύλιο $\mathbb{Z}$. Ένα $n \in \mathbb{Z}$ μπορεί να γραφεί ως $n = p^{\nu(n)}u$, με $p \nmid u$. Διαλέγουμε και πάλι μια σταθερά $0 < c < 1$ και θέτουμε $\|n\| = c^{\nu(n)}$. Αυτή η κατασκευή οδηγεί σε μία μετρική στο $\mathbb{Z}$ η οποία στην συνέχεια με πλήρωση οδηγεί στον δακτύλιο $\mathbb{Z}_p$ των p-αδικών ακέραιων. Αυτός αποτελείται από «τυπικές δυναμοσειρές» της μορφής: $\sum_{\nu=0}^{\infty} a_i p^i$ με $0 \leq a_i < p$. Η παραπάνω θεωρία δεν έτυχε της προσοχής που της άξιζε και ο Hilbert αρχικά είχε εκφραστεί με μη κολακευτικά λόγια. Η αλλαγή ήρθε από τον Helmut Hasse. Όντας φοιτητής στο πανεπιστήμιο του Göttingen έπεσε στα χέρια του ένα βιβλίο του Hensel που εξηγούσε τους p-αδικούς αριθμούς. Καταγοητευμένος πήγε στο πανεπιστήμιο του Marburg για να δουλέψει υπό την επίβλεψη του Hensel. Και η δύναμη των p-αδικών αριθμών δεν άργησε να φανεί. Ο Hasse απέδειξε την αρχή τοπικού-καθολικού (local-global-principle) η οποία αναφέρει ότι μία τετραγωνική μορφή έχει ρίζες στο $\mathbb{Q}$ αν και μόνο αν έχει έχει ρίζες σε όλα τα σώματα $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Τι καλό έχει αυτό; Τα σώματα $\mathbb{Q}_p$ είναι πλήρη και μπορούμε να χρησιμοποιήσουμε μεθόδους της Αριθμητικής Ανάλυσης (σύγκλιση επαναληπτικών σχημάτων) προκείμενου να αποδείξουμε ότι μία Διοφαντική εξίσωση έχει λύση. Επιπλέον τα εργαλεία που ανέπτυξε ο Newton για εύρεση ριζών πολυωνύμων που εκφράζονται ως δυναμοσειρές, μπορούν να χρησιμοποιηθούν αυτούσια και στην περίπτωση των p-αδικών αριθμών. Τα παραπάνω φαντάζουν υπερβολικά τεχνικά όμως διδάσκονται σε κάθε μάθημα στοιχειώδους θεωρίας αριθμών. Πρόκειται για την μέθοδο η οποία δεδομένης μιας λύσης μιας πολυωνυμικής εξίσωσης modulo p μας δίνει διαδοχικά λύσεις της Διοφαντικής εξίσωσης modulo p^n, δείτε [9, προτ. 4.7.2].

2.4. Συναρτησιακή Ανάλυση Ανεξάρτητα από τα παραπάνω στη συναρτησιακή ανάλυση έχουμε επίσης ένα δυϊσμό γεωμετρικών και αλγεβρικών εννοιών. Ισχύει το περίφημο Θεώρημα των Gelfand-Naimark το οποίο ταυτίζει τις κατηγορίες των τοπικά συμπαγών χώρων με τις αντιμεταθετικές C^*-άλγεβρες ή τις κατηγορίες των συμπαγών χώρων με τις αντιμεταθετικές C^*-άλγεβρες με μονάδα. Υπενθυμίζουμε ότι μία C^*-άλγεβρα είναι μία άλγεβρα με νόρμα ώστε $\|ab\| \leq \|a\| \cdot \|b\|$ η οποία είναι πλήρης ως προς την νόρμα και είναι εφοδιασμένη με μία ενέλιξη (involution) $a \mapsto a^*$ ώστε $\|a^*a\| = \|a\|^2$. Πράγματι μπορούμε σε ένα τοπολογικό χώρο X να αντιστοιχίσουμε την C^*-άλγεβρα των συνεχών συναρτήσεων $X \to \mathbb{C}$ και αντιστρόφως από μία C^*-άλγεβρα μπορούμε να ανακτήσουμε τον τοπολογικό χώρο ως το σύνολο των μεγίστων ιδεωδών της άλγεβρας. Η αναλογία πηγαίνει βαθύτερα: Σύμφωνα με το θεώρημα του Swan (αντ. Serre) η κατηγορία των διανυσματικών δεσμών πάνω από ένα συμπαγή χώρο Hausdorff (αντ. πάνω από μία ομοπαραλληλική αλγεβρική πολλαπλότητα) είναι ισοδύναμη με την κατηγορία των πεπερασμένα παραγόμενων προτύπων πάνω από την άλγεβρα των συνεχών συναρτήσεων (αντ. κανονικών συναρτήσεων) στο X.

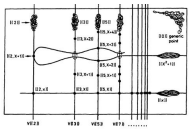
2.5 Μια επανάσταση: Η θεωρία των σχημάτων Με βάση τα παραπάνω έγινε σαφές ότι γεωμετρικές ιδιότητες αντανακλώνται μέσα σε δακτυλίους καταλλήλων συναρτήσεων. Επίσης από τα αποτελέσματα των Hensel-Hasse έγινε σαφές ότι κομμάτια της θεωρίας μιγαδικών συναρτήσεων μπορούν να ορισθούν κατάλληλα για τον δακτύλιο $\mathbb{Z}$. Ήταν η σειρά του Alexander Grothendieck να μπει στο παιχνίδι. Αρχικά ο Grothendieck δούλεψε πάνω στην Συναρτησιακή Ανάλυση, υπό την επίβλεψη των Laurent Schwartz και Jean Dieudonné. Ο τομέας όμως που έλαμψε ήταν η Αλγεβρική Γεωμετρία, η οποία πραγματικά χωρίζεται στην προ και μετά Grothendieck εποχή. Δεδομένου ενός αντιμεταθετικού δακτυλίου R υπάρχει γεωμετρικό αντικείμενο X για το οποίο ο R να είναι ο δακτύλιος συναρτήσεων του X; Ο Grothendieck όρισε ως $X = \mathrm{Spec}(R)$, το σύνολο των πρώτων ιδεωδών του R και εφοδίασε το X με τοπολογία κατά αναλογία με το θεώρημα των Gelfand-Naimark. Για παράδειγμα στο $\mathbb{Z}$ ένας ακέραιος n ορίζει μία συνάρτηση στο σύνολο των πρώτων ιδεωδών ως εξής: $n(p) = n \mod p$.

Αν και στο παράδειγμα του $\mathbb{Z}$ τα πρώτα (μη μηδενικά) ιδεώδη είναι ίδια με τα μέγιστα η κατάσταση ανατρέπεται σε γενικότερους αντιμεταθετικούς δακτυλίους, όπου μπορεί κανείς να βρει πρώτα ιδεώδη που δεν είναι μέγιστα. Η ιδέα του Grothendieck να θεωρήσει ως «γεωμετρικό αντικείμενο» ενός αντιμεταθετικού δακτυλίου το σύνολο των πρώτων αντί του συνόλου των μεγίστων ιδεωδών, επέτρεψε το να μπορούμε να θεωρούμε τις αλγεβρικές υποπολλαπλότητες ως σημεία και αυτό έδωσε μια νέα οπτική στην Αλγεβρική Γεωμετρία.

Οι τεχνικές του Grothendieck προχώρησαν ακόμα περισσότερο την ιδέα του Weil να αναπτύξουμε την Αλγεβρική Γεωμετρία υπέρ οποιουδήποτε σώματος. Στην μετά Grothendieck εποχή οι αλγεβρικές πολλαπλότητες μπορούν να οριστούν και υπέρ αντιμεταθετικών δακτυλίων. Με αυτό τον τρόπο οι λύσεις Διοφαντικών εξισώσεων μπορούν να θεαθούν ως γεωμετρικά αντικείμενα. Γενικότερα το να θεωρήσει κανείς αλγεβρικά σύνολα υπέρ ενός δακτυλίου αντί ενός σώματος προσέφερε την έννοια της οικογένειας ή της διαταραχής (deformation). Έτσι για παράδειγμα μία αθώα Διοφαντική εξίσωση όπως η $y^2 = x^3 - 1$ η οποία αντιστοιχεί στον δακτύλιο $\mathbb{Z}[x, y]/\langle y^2 - x^3 - 1\rangle$, έχει «οριζόντιες λύσεις» ζευγάρια $(x, y) \in \mathbb{Z}^2$, οι οποίες όμως δίνουν και κάθετες τομές modulo κάθε πρώτο ιδεώδες του $\mathbb{Z}$, ισοδύναμο με το να θεωρήσουμε τις λύσεις modulo p. Εδώ η γεωμετρία γίνεται εμφανής γιατί οι λύσεις mod p δεν μπορεί να

διαφέρουν πολύ αφού αποτελούν αλγεβρικά ισοδύναμες τομές, μία έννοια που αντιστοιχεί στον cobordism της συνήθους Διαφορικής Γεωμετρίας.

2.6 Εφαρμογές στην Θεωρία Αριθμών Οι εφαρμογές της γεωμετρικής αυτής αναλογίας είναι πάμπολες για να περιγραφούν ικανοποιητικά σε τόσο λίγο χώρο, αλλά ας εξηγήσουμε την συνεισφορά της γεωμετρικής θέασης στην επίλυση των εικασιών του Weil. Γενικά τα αλγεβρικά σύνολα ορισμένα πάνω από ένα γενικό σώμα μπορούν να εφοδιαστούν με την τοπολογία του Zariski. Αυτή είναι μια τοπολογία στην οποία τα κλειστά είναι τα αλγεβρικά υποσύνολα. Έχει όμως ένα μειονέκτημα: τα ανοιχτά σύνολα της είναι πολύ μεγάλα. Έτσι για παράδειγμα σε ένα ανάγωγο ομοπαραλληλικό αλγεβρικό σύνολο (δηλαδή ο δακτύλιος συναρτήσεων είναι ακέραια περιοχή) κάθε ανοιχτό είναι πυκνό. Αυτό εξανεμίζει τις ελπίδες μας να ισχύει το θεώρημα τοπικής αντιστροφής αφού δεν υπάρχουν μικρές περιοχές σημείων και τα fibre bundles δεν μπορούν να είναι τοπικά τετριμμένα. Η ιδέα του Grothendieck ήταν να ορίσει ως περιοχές ενός σημείου P όλες τις συναρτήσεις $X \xrightarrow{f} Y \ni P$ οι οποίες δεν μηδενίζουν το διαφορικό της f στο P, δηλαδή να επιβάλλει το θεώρημα τοπικής αντιστροφής! Με αυτό τον τρόπο έφτιαξε ένα σύστημα περιοχών, που αν και δεν αποτελούν τοπολογία με την συνήθη έννοια, επιτρέπουν να ορίσουμε συνομολογία κατά Čech. Αυτή αποδείχτηκε ότι είναι η κατάλληλη έννοια αλγεβρικής τοπολογίας που αναζητούσε ο Weil. Ο P. Deligne κατάφερε κάνοντας χρήση της παραπάνω θεωρίας (συνομολογία étale) να αποδείξει τις εικασίες του Weil και να κερδίσει το βραβείο Fields το 1978. Η συνομολογία étale έρχεται εφοδιασμένη με την κατάλληλη ομοτοπική θεωρία αλλά και θεωρία καλυπτικών απεικονίσεων. Θα δούμε ότι η προσέγγιση αυτή είναι βασική για την θεωρία Galois και την θεωρία των αναπαραστάσεων Galois.



2.7. Θεμελιώδης ομάδα Σε τοπολογικούς χώρους (υπό προϋποθέσεις) ορίζεται η θεμελιώδης ομάδα $\pi_1(X, x_0)$ ως η ομάδα των κλάσεων ομοτοπίας κλειστών μονοπατιών με αφετηρία το σημείο x_0 και πράξη μεταξύ δύο μονοπατιών το μονοπάτι που ορίζεται από την διαδοχή τους. Η θεωρία των καλυπτικών χώρων ταξινομεί τα λεγόμενα καλύμματα με βάση τις υποομάδες της θεμελιώδους ομάδας και είναι φτιαγμένη κατ΄εικόνα και ομοίωση με την θεωρία Galois των επεκτάσεων σωμάτων. Η αναλογία της θεωρίας γίνεται σαφέστερη στην περίπτωση των επιφανειών Riemann. Οι απεικονίσεις μεταξύ επιφανειών Riemann μπορούν να περιγραφούν πλήρως (μετά από αφαίρεση κάποιων σημείων, των «σημείων διακλάδωσης») μέσω τοπολογικών καλύμματων, ενώ η θεωρία Galois που περιγράφει τα τοπολογικά καλύμματα είναι ακριβώς η θεωρία Galois των επεκτάσεων των μερομόρφων συναρτήσεων.

Για τον Grothendieck η παραπάνω σχέση ήταν αρκετή για να περιγράψει την θεμελιώδη ομάδα étale. Το τοπολογικό κάλυμμα αντικαθίσταται από το étale κάλυμμα (το οποίο χονδρικά σημαίνει μη ιδιόμορφο διαφορικό) και η θεμελιώδης ομάδα ορίζεται με βάση όλες τις δυνατές ομάδες πεπερασμένων étale καλυμμάτων. Υπάρχει μια κατασκευή στην οποία ένα τέτοιο σύστημα ομάδων συνδέεται σε μια μεγάλη ομάδα: το αντίστροφο όριο. Στην περίπτωση που κοιτάμε μια αλγεβρική πολλαπλότητα η οποία επιδέχεται étale αλλά και συνηθισμένη θεμελιώδη ομάδα, όπως για παράδειγμα μια επιφάνεια Riemann, τότε οι δύο ομάδες συνδέονται με την έννοια της προπεπερασμένης πλήρωσης:

$$\pi_1^{\text{ét}}(X, x_0) = \widehat{\pi_1(X, x_0)} = \varprojlim_{N \lhd \pi_1(X, x_0)} \pi_1(X, x_0)/N.$$

Παράλληλα, στην θεωρία απείρων αλγεβρικών επεκτάσεων Galois, όπως για παράδειγμα στην επέκταση $\bar{\mathbb{Q}}/\mathbb{Q}$, υπάρχει μία παρόμοια κατασκευή. Μια άπειρη ομάδα Galois $\mathrm{Gal}(K/k)$ γίνεται μία τοπολογική ομάδα, όπου μια βάση ανοιχτών συνόλων αποτελούν οι υποομάδες $\mathrm{Gal}(K/N)$, ώστε N/k πεπερασμένη επέκταση Galois. Η προσθήκη της τοπολογίας στην δομή της ομάδας Galois είναι απαραίτητη αφού το θεμελιώδες θεώρημα της θεωρίας Galois ισχύει μόνο για τις κλειστές υποομάδες. Η λεγόμενη απόλυτη ομάδα Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ περιέχει πληροφορία για κάθε επέκταση Galois του σώματος των ρητών αριθμών. Μπορεί να περιγραφεί ως το αντίστροφο όριο του συστήματος όλων των ομάδων Galois κάθε πεπερασμένης επέκτασης Galois $N/\mathbb{Q}$ και την κατασκευή αυτή την συμβολίζουμε ως $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = \lim_{\leftarrow} \mathrm{Gal}(N/\mathbb{Q})$. Αν και θεμελιώδους σημασίας, η παραπάνω ομάδα παραμένει μυστηριώδης. Για παράδειγμα εκτός από τον ταυτοτικό ισομορφισμό και την μιγαδική συζυγία, δεν είμαστε σε θέση να γράψουμε με ακριβή τρόπο κανένα άλλο στοιχείο αυτής της ομάδας. Επίσης δεν γνωρίζουμε ποιες είναι οι ομάδες $\mathrm{Gal}(N/\mathbb{Q})$ οι οποίες υπεισέρχονται στο παραπάνω όριο. Αποτελεί δε ένα ανοιχτό ονομαστό πρόβλημα το λεγόμενο *αντίστροφο πρόβλημα της Θεωρίας Galois* η εξής εικασία: κάθε πεπερασμένη ομάδα, εμφανίζεται ως ομάδα Galois κάποιας επέκτασης $N/\mathbb{Q}$. Εισαγωγικά κείμενα στα Ελληνικά για την μελέτη της απόλυτης ομάδας Galois είναι τα [16], [11] ενώ πολύ ενδιαφέρον είναι και το [1]. Επιστρέφοντας στην θεωρία της étale θεμελιώδους ομάδας υπάρχει η εξής αξιοσημείωτη ισότητα:

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = \pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Q})).$$

Ο J. Milne [5] επιχειρηματολογεί, προκειμένου να τονίσει την σημασία των παραπάνω κατασκευών, για το ποιο είναι «το περισσότερο ενδιαφέρον αντικείμενο» στα Μαθηματικά και καταλήγει στην μελέτη της παρακάτω μικρής ακριβούς ακολουθίας:

$$1 \to \pi_1^{\text{ét}}(X_{\bar{\mathbb{Q}}}, \bar{x}) \to \pi_1^{\text{ét}}(X, x) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1,$$

όπου $X = \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$. Η κατανόηση της παραπάνω επέκτασης σχετίζεται με σειρά εξωτικών Μαθηματικών θεωριών, όπως τα mixed Tate motives, τις K-ομάδες σωμάτων αριθμών και τις ειδικές τιμές ζήτα συναρτήσεων, όπως περιγράφει ο P. Deligne στο [2].

3. Galois Αναπαραστάσεις Πως θα καταλάβουμε την ομάδα $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$; Είναι γενική Μαθηματική αρχή, να προσπαθούμε να αναδιατυπώσουμε ένα πρόβλημα με ένα διαφορετικό τρόπο ο οποίος να είναι περισσότερο προσιτός, περισσότερο κοντά σε ένα πρόβλημα το οποίο γνωρίζουμε να χειριζόμαστε σωστά. Αυτή η μέθοδος στην θεωρία των ομάδων ονομάζεται *Θεωρία Αναπαραστάσεων*. Γενικά αναζητούμε ομορφισμούς από την ομάδα που μελετούμε στην ομάδα που γνωρίζουμε καλύτερα από κάθε άλλη, η οποία είναι η ομάδα των $n \times n$ αντιστρέψιμων πινάκων.

Ένα στοιχείο $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ είναι εξ ορισμού ένας αυτομορφισμός $\sigma : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$ ο οποίος επιπρόσθετα περιορίζεται σε ένα αυτομορφισμό $N \to N$ για κάθε πεπερασμένη επέκταση Galois $N/\mathbb{Q}$. Η πρώτη ιδέα είναι να αφήσουμε τον σ να δράσει πάνω σε κάθε κυκλοτομικό σώμα $\mathbb{Q}(\zeta_n)$. Ως αυτομορφισμός θα δώσει $\sigma(\zeta_n) = \zeta_n^{a(n)}$, όπου το $a(n) \in \mathbb{N}$, $(a(n), n) = 1$. Με λίγα λόγια, η πληροφορία που θα πάρουμε για την μορφή του σ από την κατασκευή αυτή βρίσκεται αποθηκευμένη στους εκθέτες $a(n)$ οι οποίοι όλοι μαζί μπορούν να αποτυπωθούν σε ένα στοιχείο του $\hat{a} \in \hat{\mathbb{Z}}^* = \mathrm{GL}_1(\hat{\mathbb{Z}})$, όπου $\hat{\mathbb{Z}}$ είναι η προπεπερασμένη πλήρωση του $\mathbb{Z}$. Η δε συνάρτηση $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_1(\hat{\mathbb{Z}})$ είναι μια αναπαράσταση της απόλυτης ομάδας Galois η οποία ονομάζεται *ο κυκλοτομικός χαρακτήρας*. Δυστυχώς ένα σημαντικό ποσό πληροφορίας στην εικόνα του κυκλοτομικού χαρακτήρα χάνεται.

Πράγματι η εικόνα είναι μια αβελιανή ομάδα, οπότε ο μεταθέτης της απόλυτης ομάδας Galois απεικονίζεται στην μονάδα.

3.1 Θεωρία Κλάσεων σωμάτων Το Θεώρημα των Kronecker-Weber αναφέρει ότι οι αβελιανές επεκτάσεις του $\mathbb{Q}$ παράγονται από τιμές της εκθετικής συνάρτησης $\exp : \tau \to e^{2\pi i\tau}$ για $\tau \in \mathbb{Q}$. Αν θεωρήσουμε ως $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ την μέγιστη αβελιανή επέκταση του $\mathbb{Q}$, τότε το Θεώρημα των Kronecker-Weber έχει ως συνέπεια ότι $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \widehat{\mathbb{Z}}^*$.

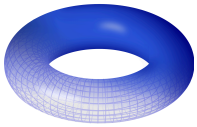
Η μελέτη των αβελιανών επεκτάσεων ενός δεδομένου σώματος K είναι το αντικείμενο της *θεωρίας κλάσεων σωμάτων*. Γενικά K είναι ένα σώμα αριθμών, ή ένα σώμα συναρτήσεων μίας μεταβλητής (καθολικά σώματα) ή ένα τοπικό σώμα. Η θεωρία κλάσεων σωμάτων έχει πολλές διαφορετικές διατυπώσεις σε πολλές διαφορετικές γλώσσες. Γενικά, τα βασικά θεωρήματα αυτής δίνουν μία αντίισοδυναμία $\psi : \mathbf{Ab}_K \to \mathbf{Sub}_X$ ανάμεσα στην κατηγορία των αβελιανών επεκτάσεων του K και την κατηγορία $\mathbf{Sub}_X$ των ανοιχτών υποομάδων μιας τοπικά συμπαγούς αβελιανής ομάδας $X = X(K)$, η οποία ορίζεται αποκλειστικά σε όρους του σώματος K. Η ομάδα $X(K)$ στην περίπτωση των καθολικών σωμάτων είναι η idèle class group ή η πολλαπλασιαστική ομάδα K^* στην περίπτωση που το K είναι τοπικό σώμα. Ο ορισμός της αντί-ισοδυναμίας απεικονίζει μια αλγεβρική επέκταση L/K στην εικόνα της $N_{L/K}X(L) \subset X(K)$. Το θεώρημα ύπαρξης εξασφαλίζει ότι κάθε ανοιχτή υποομάδα $H \subset X(K)$ είναι της μορφής $N_{L/K}X(L)$ για κάποια L/K αβελιανή επέκταση, το λεγόμενο σώμα κλάσεων της H. Το πρόβλημα της ακριβούς περιγραφής του $L = \psi^{-1}(H)$ αποτελεί το λεγόμενο *12ο πρόβλημα του Hilbert*. Το πρόβλημα αυτό παραμένει ανοιχτό, ενώ είναι γνωστές μερικές ειδικές περιπτώσεις, όπως όταν το $K = \mathbb{Q}$ (η ακριβής περιγραφή εδώ δίνεται μέσω του θεωρήματος Kronecker-Weber), η περίπτωση των μιγαδικών τετραγωνικών σωμάτων αριθμών αλλά και μερικές περιπτώσεις από σώματα συναρτήσεων όπου η ακριβής περιγραφή δίνεται με την βοήθεια των τάξεως-1 προτύπων Drinfeld.

3.2. Μη αβελιανές επεκτάσεις Αν θέλουμε να μελετήσουμε μη αβελιανές επεκτάσεις χρειαζόμαστε να κάνουμε κάτι καλύτερο και την απάντηση θα μας την δώσει και πάλι η γεωμετρική διαίσθηση. Παρατηρούμε ότι τα κυκλοτομικά σώματα αριθμών $\mathbb{Q}(\zeta_n)$ στην πραγματικότητα παράγονται από τις συντεταγμένες n-οστών ριζών της μονάδας, δηλαδή παράγονται από τα σημεία πεπερασμένης τάξης της άπειρης ομάδας S^1 του μοναδιαίου κύκλου.

3.3. Ελλειπτικές Καμπύλες Οι ελλειπτικές καμπύλες είναι καμπύλες οι οποίες οφείλουν το όνομα τους στο πρόβλημα της εύρεσης μήκους τόξου πάνω σε ελλείψεις. Το πρόβλημα αυτό ανάγεται σε υπολογισμό ολοκληρωμάτων της μορφής

$$\int \frac{1}{\sqrt{x^3 + ax + b}} dx.$$

Ο υπολογισμός των παραπάνω ολοκληρωμάτων ήταν ένα από τα κύρια προβλήματα της Ανάλυσης τον προπερασμένο αιώνα και πρώτης τάξης Μαθηματικοί όπως οι Euler, Weierstrass, Abel, Jacobi ασχολήθηκαν μαζί τους. Το παραπάνω ολοκλήρωμα οδηγεί στην μελέτη δύο (μιγαδικών) συναρτήσεων x, y οι οποίες ικανοποιούν μια εξίσωση της μορφής $y^2 = x^3 + ax + b$ ή ισοδύναμα την μελέτη των μιγαδικών αριθμών $(x, y) \in \mathbb{C}^2$ που ικανοποιούν την παραπάνω εξίσωση. Ο χώρος λύσεων του παραπάνω κυβικού πολυωνύμου αποτελεί μια επιφάνεια Riemann.



Γενικότερα θεωρούμε το ομογενοποιημένο πολυώνυμο $y^2z = x^3 + axz^2 + bz^3$ με $a, b \in k$ ώστε το το $x^3 + ax + b$ να έχει απλές ρίζες και θεωρούμε το σύνολο των λύσεων ως υποσύνολο του προβολικού επιπέδου $\mathbb{P}^2_k$. Στο σύνολο λύσεων μπορεί να οριστεί μια δομή αβελιανής ομάδας ως εξής: Σταθεροποιούμε το σημείο στο άπειρο με προβολικές συντεταγμένες $O = [0 : 1 : 0]$ το οποίο θα αποτελεί το ουδέτερο στοιχείο της πράξης. Δεδομένων δύο σημείων P, Q φέρνουμε την ευθεία που τα συνδέει η οποία τέμνει την αλγεβρική καμπύλη στο σημείο PQ. Στην συνέχεια ενώνουμε το σημείο O με το PQ και το τρίτο σημείο επαφής θα είναι το αποτέλεσμα της άθροισης $P+Q$. Η παραπάνω πράξη φαίνεται αρκετά αφύσικη, στην πραγματικότητα όμως αντανακλά το γεγονός ότι στην περίπτωση $k = \mathbb{C}$ το σύνολο λύσεων του προβολικού αλγεβρικού συνόλου αποτελεί τοπολογικά ένα τόρο ο οποίος αντιστοιχεί στην ομάδα πηλίκο $\mathbb{C}/\Lambda$, όπου το Λ είναι μια διακριτή υποομάδα του $\mathbb{Z}$, ισόμορφη ως ομάδα με το $\mathbb{Z}^2$. Τα παραπάνω ήταν γνωστά στους Weierstrass, Jacobi, Abel οι οποίοι μιλούσαν για την «διπλή περιοδικότητα των ελλειπτικών συναρτήσεων». Οι ελλειπτικές συναρτήσεις φυσικά δεν είναι τίποτα άλλο από το σώμα των μερόμορφων συναρτήσεων της ελλειπτικής καμπύλης την οποία την θεωρούμε ως επιφάνεια Riemann.

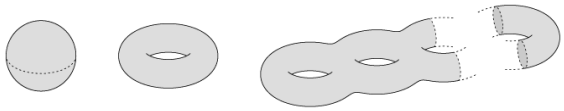
Αν έχουμε τώρα μια ελλειπτική καμπύλη η οποία ορίζεται υπέρ του $\mathbb{Q}$ για παράδειγμα $a, b \in \mathbb{Q}$ τότε τα σημεία τάξης n της ομάδας του τόρου $\mathbb{C}/\Lambda \cong S^1 \times S^1$ είναι η ομάδα $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ και η ομάδα $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ δρα επί αυτών. Αν θεωρήσουμε ως $n = \ell^k$, δηλαδή δυνάμεις του πρώτου ℓ, τότε όπως και στην περίπτωση των κυκλοτομικών σωμάτων λαμβάνουμε μια αναπαράσταση:

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell), \text{ όπου } \mathbb{Z}_\ell \text{ είναι οι ακέραιοι } \ell\text{-αδικοί.}$$

Το πλεονέκτημα σε αυτή την κατασκευή είναι ότι η εικόνα δεν είναι πλέον αβελιανή ομάδα συνεπώς ένα κομμάτι του μεταθέτη της απόλυτης ομάδας Galois επιβιώνει στην εικόνα. Η παραπάνω κατασκευή μπορεί να γενικευτεί από δράσεις της απόλυτης ομάδας Galois σε ομάδες σημείων πεπερασμένης τάξης σε Ιακωβιανές πολλαπλότητες αλγεβρικών καμπυλών μεγαλύτερου γένους, οι οποίες είναι μιγαδικές αναλυτικές πολλαπλότητες ισόμορφες με $\mathbb{C}^g/\Lambda$, $g \in \mathbb{N}, g \geq 1$. Θα δούμε ότι η θεωρία των αναπαραστάσεων Galois έπαιξε σημαντικό ρόλο στην απόδειξη του Τελευταίου Θεωρήματος του Fermat.

4. Διοφαντικές Εξισώσεις Ας θεωρήσουμε μία Διοφαντική εξίσωση της μορφής $f(x, y) = 0$ της οποίας αναζητούμε ρητές ρίζες. Για παράδειγμα $f(x, y) = x^n + y^n - 1$. Η αλγεβρική εξίσωση $f(x, y) = 0$ αν θεωρηθεί προβολικά (μετά από ομογενοποίηση) πάνω από το σώμα των μιγαδικών αριθμών δίνει μια συμπαγή επιφάνεια Riemann η οποία τοπολογικά μπορεί να αναπαρασταθεί ως ένας τόρος με g το πλήθος τρύπες, όπως στο παρακάτω σχήμα. Η εικασία του Mordell αναφέρει ότι αν $g > 1$ τότε η Διοφαντική εξίσωση έχει πεπερασμένες το πλήθος λύσεις. Η Εικασία αυτή αποδείχτηκε το 1984 από τον G. Faltings. Στην περίπτωση δε των καμπύλων Fermat μπορεί κανείς να αποδείξει ότι $g = (n-1)(n-2)/2$. Άρα αν $n \geq 4$ έχουμε ότι η εξίσωση Fermat έχει πεπερασμένο πλήθος λύσεων. Γενικότερα οι λύσεις μιας Διοφαντικής εξίσωσης $f(x, y) = 0$ καθορίζονται από την τοπολογική συμπεριφορά της αντίστοιχης επιφάνειας Riemann ως εξής:

Γένος	Λύσεις
$g = 0$	Καμμία λύση ή άπειρες λύσεις που δίνονται από ρητή παραμετρικοποίηση
$g = 1$	Οι λύσεις έχουν δομή πεπερασμένα παραγόμενης αβελιανής ομάδας
$g \geq 2$	Πεπερασμένες λύσεις (Εικασία Mordell- Θεώρημα Faltings



Η περίπτωση του γένους 0 είναι καλά κατανοητή. Μάλιστα στην περίπτωση που μπορούμε να βρούμε μια λύση υπάρχει η μέθοδος της ρητής παραμέτρισης η οποία μας επιτρέπει να βρούμε όλες τις λύσεις. Ενδεικτικά αναφέρουμε ότι το πρόβλημα υπολογισμού των Πυθαγορείων τριάδων μπορεί να αντιμετωπιστεί με τέτοια εργαλεία [9, προτ. 2.3.8]. Η περίπτωση του γένους 1 στην περίπτωση που έχουμε μια λύση οδηγεί στην θεωρία των ελλειπτικών καμπύλων. Πρόκειται για μια πολύ πλούσια και ερευνητικά ενεργή περιοχή της Θεωρίας Αριθμών. Είναι γνωστό ότι οι λύσεις σχηματίζουν μια πεπερασμένα παραγόμενη αβελιανή ομάδα η οποία είναι ισόμορφη με την $\mathbb{Z}^r + E_{\text{tor}}$. Συνεπώς αν έχουμε μία λύση P μπορούμε να λογαριάσουμε πολλές λύσεις υπολογίζοντας τα πολλαπλάσια nP. Ένα ιδιαίτερα ενδιαφέρον πρόβλημα είναι η Εικασία των Birch και Swinnerton-Dyer (η οποία αποτελεί και ένα από τα 7 προβλήματα του Ινστιτούτου Clay που η λύση τους δίνει 10^6 δολάρια) και αναφέρει ότι η τάξη r του ελεύθερου κομματιού της ελλειπτικής καμπύλης είναι η τάξη της ρίζας της L-σειράς της ελλειπτικής καμπύλης στο $s = 1$. Τι γίνεται στην περίπτωση που $g \geq 2$; Αν μπορούσε κάποιος να δώσει ένα άνω φράγμα στο Θεώρημα του Faltings, θα μπορούσαμε να δοκιμάσουμε όλες τις μικρότερες υποψήφιες λύσεις. Μάλιστα ο Faltings είχε θέσει αυτό το πρόβλημα στον μαθητή του S. Mochizuki, ο οποίος κατέληξε στην εξωτική p-αδική θεωρία Teichmüller. Ας περιγράψουμε μία άλλη προσέγγιση, την μέθοδο των Chabauty-Coleman, η οποία θα μας δώσει την δυνατότητα να μιλήσουμε για μια σχέση της Θεωρίας Αριθμών με τις θεωρίες βαθμίδας (gauge theories) από την Φυσική.

Τα σημεία μιας καμπύλης X γένους $g \geq 2$ δεν μπορούν να δεχτούν δομή ομάδας. Υπάρχει όμως ένα υποκατάστατο, η Ιακωβιανή πολλαπλότητα $J(X)$ η οποία αποτελεί μια μιγαδική αναλυτική πολλαπλότητα μιγαδικής διάστασης g, η οποία έχει δομή αβελιανής ομάδας. Μάλιστα αν μπορούμε να βρούμε ένα ρητό σημείο O στην X τότε ορίζεται μια εμφύτευση $X(\mathbb{Q}) \hookrightarrow J(X)(\mathbb{Q})$. Σε αυτή την περίπτωση μια στρατηγική για να βρούμε το σύνολο λύσεων-σημείων της $X(\mathbb{Q})$ θα ήταν να βρούμε τις λύσεις του $J(X)(\mathbb{Q})$, αξιοποιώντας την δομή ομάδας του τελευταίου συνόλου, και στην συνέχεια να προσδιορίσουμε ποια από τα τελευταία σημεία ανήκουν στο $X(\mathbb{Q})$. Αξίζει να αναφέρουμε εδώ ότι όπως και στις ελλειπτικές καμπύλες η ομάδα $J(X)(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα και μάλιστα υπάρχουν αλγόριθμοι που υπολογίζουν την δομή της.

Μια ιδέα για την μελέτη του $X(\mathbb{Q})$ είναι η εξής: Ας εμφυτεύσουμε τα $X(\mathbb{Q}) \subset X(\mathbb{R})$ στο $J(X)(\mathbb{Q}) \subset J(X)(\mathbb{R})$. Το σύνολο $J(X)(\mathbb{R})$, ως πραγματική ομάδα Lie, είναι αναλυτικά ισόμορφο με $(\mathbb{R}^g)/\mathbb{Z}^g \times F$, όπου F είναι μια πεπερασμένη ομάδα. Ας θεωρήσουμε την κλειστότητα $\overline{J(X)(\mathbb{Q})}$ στην $J(X)(\mathbb{R})$. Θέλουμε να υπολογίσουμε τα σημεία του $J(X)(\mathbb{Q})$ τα οποία ανήκουν στην υποπολλαπλότητα $X(\mathbb{R})$. Αν για παράδειγμα είχαμε ότι $X(\mathbb{R}) \cap \overline{J(X)(\mathbb{Q})}$

ήταν πεπερασμένο σύνολο τότε θα είχαμε ένα τρόπο να ελέγξουμε το $X(\mathbb{Q})$. Δυστυχώς στην περίπτωση που το $J(\mathbb{Q})$ δεν είναι πεπερασμένη ομάδα, τότε υπάρχει η εικασία του B. Mazur που λέει ότι το $\overline{J(X)(\mathbb{Q})}$ είναι ανοιχτό, το οποίο δίνει ότι η παραπάνω τομή είναι άπειρη. Η μέθοδος των Chabauty-Coleman συνίσταται στην αντικατάσταση του σώματος $\mathbb{R}$ στην παραπάνω ιδέα από το πλήρες σώμα $\mathbb{Q}_p$. Στην περίπτωση αυτή το $\overline{J(X)(\mathbb{Q})}$ στην p-αδική ομάδα Lie $J(X)(\mathbb{Q}_p)$ έχει συχνά διάσταση (ως p-αδική πολ/τα) μικρότερη του g και στην περίπτωση αυτή μπορεί να αποδειχθεί ότι η τομή $X(\mathbb{Q}_p) \cap \overline{J(X)(\mathbb{Q})}$ είναι πεπερασμένη όπως θέλαμε. Μάλιστα ο R. Coleman κατάφερε (μέθοδος p-αδικής ολοκλήρωσης) να δώσει ένα καλό φράγμα του πλήθους $\#X(\mathbb{Q})$ σε σχέση με το πλήθος των σημείων της αναγωγής $X(\mathbb{F}_p)$ modulo p.

4.1 Το τελευταίο θεώρημα του Fermat Ανάμεσα σε όλες τις διοφαντικές εξισώσεις που αντιστοιχούν σε επιφάνειες γένους ≥ 2 η εξίσωση του Fermat

$$x^n + y^n + z^n = 0 \text{ με γένος } g_n = \frac{(n-1)(n-2)}{2}$$

έχει ιδιαίτερη σημασία, τόσο από ιστορικής πλευράς όσο και γιατί ήταν ένα βασικό κίνητρο για την δημιουργία της Αλγεβρικής Θεωρίας Αριθμών και της Αντιμεταθετικής Άλγεβρας. Ας παρατηρήσουμε ότι για $n = 2$ η παραπάνω επιφάνεια έχει γένος 0. Οι δε λύσεις της είναι οι πυθαγόρειες τριάδες και μπορούν να υπολογιστούν με την μέθοδο της ρητής παραμετρικοποίησης [9, 2.3.3]. Η περίπτωση $n = 3$ υπάγεται στις ελλειπτικές καμπύλες και ο ίδιος ο Fermat έδωσε μια ξεχωριστή απόδειξη ότι η εξίσωση δεν έχει μη τετριμμένες λύσεις. Για $n \geq 4$ οδηγούμαστε σε καμπύλες γένους $g \geq 2$ για τις οποίες το θεώρημα Faltings-Mordell εξασφαλίζει το πεπερασμένο των λύσεων.

Στην θεωρία αριθμών υπάρχει το θεώρημα μονοσήμαντης ανάλυσης ακέραιων αριθμών ως γινόμενο πρώτων ενώ για αθροίσματα δεν υπάρχει κανένα θεώρημα μοναδικότητας γραφής. Μία ιδέα για να λυθεί το πρόβλημα του Fermat ήταν να γίνει το άθροισμα γινόμενο ως εξής:

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1}y), \text{ με } \zeta_n = e^{2\pi i/n}.$$

Αυτή η παραγοντοποίηση μας αναγκάζει να δουλέψουμε στον δακτύλιο $\mathbb{Z}[\zeta_n]$ στον οποίο δεν ισχύει, εν γένει, η μοναδική ανάλυση σε γινόμενο πρώτων. Χρειάστηκε μια στρατιά μαθηματικών η οποία ανέπτυξε τον κλάδο της Αλγεβρικής Θεωρίας Αριθμών για να βάλει τα θεμέλια αυστηρότητας για την απόδειξη της εικασίας του Fermat και μάλιστα για μια ειδική περίπτωση, αυτή των ομαλών πρώτων. Πράγματι, μπορούμε με μία ομάδα, την ομάδα κλάσεων C_n να μετρήσουμε πόσο απέχει ο δακτύλιος $\mathbb{Z}[\zeta_n]$ από το να είναι δακτύλιος παραγοντοποίησης. Για όλους τους πρώτους που δεν διαιρούν την τάξη της ομάδας κλάσεων C_n, μπορούμε να αποδείξουμε την εικασία Fermat για $n = p$. Για μία όσο το δυνατόν απλούστερη συζήτηση των παραπάνω παραπέμπουμε στο [7]. Αξίζει να αναφέρουμε ότι μελέτη της ομάδας κλάσεων των κυκλοτομικών σωμάτων αριθμών οδηγεί σε μια συναρπαστική θεωρία, την Θεωρία του Iwasawa.

4.2. Εικασία Taniyama-Shimura Ας θεωρήσουμε μια ελλειπτική καμπύλη $E : y^2 = x^3 + ax + b$ με διακρίνουσα $\neq 0$. Όπως είδαμε μπορούμε να οδηγηθούμε στην ζήτα συνάρτηση

$$\zeta_p(E,T) = \exp\left(\sum_{\nu=1}^{\infty} \frac{\#E(\mathbb{F}_{p^\nu})}{\nu} T^\nu\right)$$

η οποία καταγράφει το πλήθος των σημείων πάνω από τα πεπερασμένα σώματα με p^ν στοιχεία. Συγκεντρώνουμε όλη την πληροφορία των ζ_p στην καθολική ζ-συνάρτηση της ελλειπτικής καμπύλης η οποία ορίζεται ως:

$$\zeta_p(E,s) = \prod_p \zeta_p(E,p^{-1}) = \zeta(s-1)\cdot\left(\sum_{n=1}^{\infty} a_n n^{-s}\right)^{-1}$$

Η εικασία Shimura-Taniyama αναφέρει ότι η $f_E(z) = \sum a_n e^{2\pi i n z}$ είναι μια ειδική μιγαδική συνάρτηση που ονομάζεται *modular form* βάρους 2. Αυτές οι συναρτήσεις σχετίζονται με τα ολόμορφα διαφορικά πάνω σε επιφάνειες Riemann αριθμητικού ενδιαφέροντος και ικανοποιούν συγκεκριμένες μιγαδικές συμμετρίες. Η εικασία αυτή αποδείχτηκε από τον A. Wiles [8] για μια ειδική κατηγορία ελλειπτικών καμπυλών, αυτές της ημιευσταθούς αναγωγής, ενώ ο περιορισμός αυτός αφαιρέθηκε μετά από την δουλειά των C. Breuil, B. Conrad, F. Diamond και R. Taylor.

Η πορεία προς την απόδειξη του τελευταίου θεωρήματος του Fermat ξεκίνησε από την εργασία του G. Frey, ο οποίος έδωσε ισχυρές λογικοφανείς ενδείξεις, ότι μια τετριμμένη λύση (a,b,c) της εξίσωσης του Fermat $a^p + b^p = c^p$ οδηγεί σε ελλειπτικές καμπύλες $y^2 = x(x+a^p)(x+b^p)$ οι οποίες δεν ικανοποιούν την εικασία Taniyama-Shimura ενώ είναι ημιευσταθούς αναγωγής. Η αυστηρή απόδειξη της ιδέας του Frey δόθηκε από τον K. Ribet και ήταν η αρχή μιας 7ετούς αναζήτησης από τον A. Wiles.

Αξίζει να αναφέρουμε ότι η εικασία Taniyama-Shimura είναι μια ειδική περίπτωση ενός πολύ γενικού προγράμματος γύρω από τα Μαθηματικά, το περίφημο *Πρόγραμμα Langlands* το οποίο χονδρικά αναφέρει ότι όλες οι ζ και L-συναρτήσεις που εμφανίζονται στην Θεωρία Αριθμών προέρχονται από «αυτομορφικές αναπαραστάσεις». Για μια εισαγωγή στα Ελληνικά στο πρόγραμμα Langlands παραπέμπουμε στο [15] ενώ ένα ενδιαφέρον εκλαϊκευτικό κείμενο με ειδικές αναφορές στην Φυσική είναι το [3], εισαγωγικά κείμενα πάνω στα Μαθηματικά του Τελευταίου Θεωρήματος του Fermat είναι το [14] και [17] ενώ ιδιαίτερα ενδιαφέρον είναι το [6].

4.3. Θεωρίες βαθμίδας και Διοφαντικές εξισώσεις Η αρχή του Fermat αναφέρει ότι η τροχιά μιας φωτεινής ακτίνας είναι η λύση ενός προβλήματος βελτιστοποίησης: ανάμεσα σε όλες τις δυνατές τροχιές στις οποίες μπορεί να κινηθεί το φως, επιλέγεται αυτή που απαιτεί τον μικρότερο χρόνο. Αυτή είναι *η αρχή της ελάχιστης δράσης* η οποία στην κατάλληλη μορφή της είναι η βάση των κλασικών θεωριών πεδίου, σωματιδιακής Φυσικής, θεωρίας χορδών και θεωριών βαρύτητας. Υπάρχει άραγε κάποιος άλλος σύνδεσμος ανάμεσα στην θεωρία Αριθμών και στην αρχή ελάχιστης δράσης, πέρα από το μοναδικό μυαλό του Fermat; Θα περιγράψουμε την αρχή της *Αριθμητικής Θεωρίας βαθμίδας* (arithmetic gauge theory) η οποία βασίζεται στις ιδέες του Minhyong Kim [4], ενός μαθηματικού με σημαντική συνεισφορά στις Διοφαντικές εξισώσεις και στην μέθοδο Chabauty που περιγράψαμε νωρίτερα.

Στην Γεωμετρία, τα πεδία gauge είναι principal bundles με συνοχή και ένας από τους τρόπους να μελετηθεί ένα γεωμετρικό αντικείμενο βασίζεται στο ποιες θεωρίες πεδίου μπορεί να υποστηρίξει. Στην αριθμητική περίπτωση μια ομάδα βαθμίδας είναι μια τοπολογική ομάδα U εφοδιασμένη με μια συνεχή δράση της απόλυτης ομάδας Galois G_K. Υπενθυμίζουμε ότι η απόλυτη ομάδα Galois είναι εφοδιασμένη με τοπολογία. Ένα U-gauge field ή principal U-bundle υπέρ του σώματος K είναι ένας τοπολογικός χώρος P

εφοδιασμένος με μια απλά μεταβατική συνεχή δεξιά δράση του U και μια συνεχή αριστερή δράση του G_K οι οποίες είναι συμβατές, δηλαδή $g \cdot p \cdot u = g(p)g(u)$. Αυτού του είδους οι δομές είναι γνωστές στον χώρο της Αριθμητικής Γεωμετρίας και συνομολογίας Galois με τον όρο U-torsor. Μάλιστα ο χώρος των κλάσεων ισομορφισμών από torsors είναι ισόμορφος με την συνομολογία Galois $H^1(G_K, U)$. Ο Kim κατάφερε να δείξει πως στο σύνολο των σημείων $V(\mathbb{Q}_p)$ αντιστοιχούν p-αδικά αριθμητικά πεδία gauge και να δώσει μια αριθμητική έκδοση των εξισώσεων Euler-Lagrange, άμεσα συσχετιζόμενες με τους νόμους αντιστροφής. Με την χρήση της p-αδικής θεωρίας Hodge οι εξισώσεις Euler-Lagrange δίνουν αναλυτικές εξισώσεις για το σημείο $x \in V(\mathbb{Q}_p)$. Αυτές μπορούν να δώσουν έναν αποτελεσματικό τρόπο για να δείξουμε ότι το σύνολο των ρητών σημείων είναι πεπερασμένο και να εκτιμήσουμε το πλήθος των σημείων, σε αντίθεση με την περίφημη απόδειξη του Faltings. Η αναλογία προχωράει πολύ βαθύτερα, αφού ένα φυσικό ανάλογο της δράσης Chern-Simons σε 3-πολλαπλότητες μπορεί να μεταφερθεί στην Αριθμητική. Το γεγονός αυτό προσθέτει μία ακόμα αναλογία στα πλαίσια της Αριθμητικής Τοπολογίας, ενός κλάδου που έχει την βάση του στον Gauss, σύμφωνα με τον οποίο η θεωρία των κόμβων και η θεωρία των πρώτων είναι σε πλήρη αντιστοιχία, [10], [12].

Αναφορές

[1] Avner Ash and Robert Gross. *Fearless symmetry*. Princeton University Press, Princeton, NJ, 2006. Exposing the hidden patterns of numbers, With a foreword by Barry Mazur.

[2] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* **Q** *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.

[3] Edward Frenkel. *Έρωτας και Μαθηματικά*. Αλεξάνδρεια, 2015.

[4] Minhyong Kim. Arithmetic Gauge Theory: A Brief Introduction. 2017.

[5] James S. Milne. Lectures on etale cohomology (v2.21), 2013. Available at www.jmilne.org/math/.

[6] Singh Simon. *Το τελευταίο θεώρημα του Φερμα*. Η γοητεία της γνώσης. Τραυλός.

[7] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.

[8] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[9] Ιωάννης Αντωνιάδης and Αριστείδης Κοντογεώργης. *Θεωρία Αριθμών και εφαρμοφές*. Κάλλιπος, 2015.

[10] Δημοκλής Γκουνταρούλης. Αριθμητική Τοπολογία. Master's thesis, Πανεπιστήμιο Αιγαίου, 2006.

[11] Ανθή Ζερβού. Profinite groups and cohomology. Master's thesis, Πανεπιστήμιο Κρήτης, 2017.

[12] Δημήτρης Κάρδαρης. Αριθμητική Τοπολογία και Φυσική. Master's thesis, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2017.

[13] Σωτήρης Καρανικολόπουλος. Uniformization Αλγεβρικών Καμπυλών. Master's thesis, Πανεπιστήμιο Αιγαίου, 2005.

[14] Αριστείδης Κοντογεώργης. Ημιευσταθείς Ελλειπτικές Καμπύλες και το τελευταίο θεώρημα του Fermat. Master's thesis, Πανεπιστήμιο Κρήτης, 1994.

[15] Γεώργιος Παπάς. Εισαγωγή στο πρόγραμμα Langlands. Master's thesis, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2016.

[16] Μανόλης Τζωρτζάκης. Η θεωρία των dessin d'enfants του Grothendieck. Master's thesis, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2014.

[17] Δημήτρης Χατζάκος. Modular forms και ελλειπτικές καμπύλες. Master's thesis, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2012.

Γιάννης Αντωνιάδης Πανεπιστήμιο Κρήτης, Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών, Πανεπιστημιούπολη Βουτών, 70013 Ηράκλειο Κρήτης, antoniad@math.uoc.gr
Αριστείδης Κοντογεώργης Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Τμήμα Μαθηματικών Πανεπιστημιούπολη, 15784 Αθήνα kontogar@math.uoa.gr