1 Η ομάδα στις κυβικές καμπύλες

Θεωρούμε μια λεία (χωρίς ιδιομορφίες) κυβική καμπύλη $V(F)$. Μια λεία καμπύλη $V(F) \subset P^2_{\mathbb{C}}$ είναι πάντα ανάγωγη (Αποδ: αν δεν ήταν ανάγωγη τότε $F = F_1F_2$ και άρα $V(F) = V(F_1)\bigcup V(F_2)$ με $deg(F_1) \geq 1$ και $deg(F_2) \geq 1$. Κάθε ένα από τα $deg(F_1) * deg(F_2)$ κοινά σημεία είναι τουλάχιστον διπλό σημείο του $V(F)$, επειδή είναι σημείο του $V(F_1)$ και του $V(F_2)$, άρα είναι ιδιόμορφο. Άτοπο). Η καμπύλη είναι τρίτου βαθμού και άρα κάθε ευθεία που διέρχεται από δύο σημεία της καμπύλης τέμνει την καμπύλη σε ένα ακόμη σημείο. Η εφαπτομένη σε ένα σημείο της διέρχεται από ένα ακόμη σημείο της καμπύλης, εκτός αν είναι σημείο καμπής, τότε η εφαπτομένη τέμνει την καμπύλη μόνο στο σημείο καμπής, όμως με πολλαπλότητα τομής 3.
Θα ορίσουμε μια διμελή πράξη στη λεία κυβική καμπύλη, με τον κανόνα χορδής-εφαπτομένης, που κάνει την καμπύλη ομάδα.
Έστω O ένα σημείο καμπής της λείας κυβικής καμπύλης $V(F)$. Η λεία κυβική καμπύλη έχει εννέα τέτοια σημεία . Αν A, B είναι δύο σημεία της $V(F)$ συμβολίζουμε με $P = AB$ το τρίτο σημείο τομής της ευθείας που διέρχεται από τα A, B και της καμπύλης $V(F)$. Στην περίπτωση που το $A = B$ συμβολίζουμε με AA το τρίτο σημείο τομής της εφαπτομένης στο Α στην $V(F)$ με την $V(F)$. Ορίζουμε $A + B$ να είναι το τρίτο σημείο τομής της ευθείας που διέρχεται από το O και το AB με την $V(F)$.

Θεώρημα 1 Η πράξη αυτή κάνει την καμπύλη $V(F)$ αβελιανή ομάδα με ουδέτερο στοιχείο το O.

Σχέδιο απόδειξης Από τον ορισμό φαίνεται ότι $A + B$ είναι ίσο με το $B + A$, επειδή η ευθεία που ορίζεται από τα A, B είναι η ίδια με την ευθεία που ορίζεται από τα B, A. Άρα η πράξη είναι μεταθετική.

Στη συνέχεια θα αποδείξουμε ότι το O είναι το ουδέτερο στοιχείο της ομάδας. Θα βρούμε το $A + O$. Η ευθεία που διέρχεται από τα A, O τέμνει την καμπύλη στο σημείο AO. Φέρνουμε την ευθεία που διέρχεται από το AO και το O. Αυτή είναι η ίδια με την προηγούμενη, άρα το τρίτο σημείο τομής, είναι το O. Ώστε $A + O = O$ για κάθε A, δηλαδή το O είναι **ουδέτερο στοιχείο ως προς την πρόσθεση**.
Θα βρούμε το $A + AO$. Η ευθεία που διέρχεται από τα A, AO τέμνει την καμπύλη στο σημείο O. Φέρνουμε την ευθεία που διέρχεται από το O και το O, δηλαδή την εφαπτομένη στην καμπύλη. Αλλά το σημείο O είναι σημείο καμπής, άρα το τρίτο σημείο τομής είναι το ίδιο το O. Ώστε $A + AO = O$, που σημαίνει ότι το **αντίθετο** του A είναι το AO, δηλαδή το τρίτο σημείο που η ευθεία που διέρχεται από τα A, O τέμνει την κυβική.

Η μόνη ιδιότητα της ομάδας που δεν είναι προφανής είναι η προσεταιριστική.

Ορισμός 2 Ελλειπτική καμπύλη C λέγεται μια λεία κυβική καμπύλη μαζί με ένα σημείο καμπής O και την ομάδα που ορίζεται πάνω στην C με τον κανόνα χορδής-εφαπτόμενης και με ουδέτερο στοιχείο το O.

Η θεωρία των Ελλειπτικών καμπυλών έχει τις ρίζες την στην δουλειά του Διόφαντου (Έλληνα μαθηματικού που έζησε πιθανόν γύρω στο 250 μ.Χ στην Αλεξάνδρεια και ασχολήθηκε με Άλγεβρα και Θεωρία Αριθμών) και των *Abel* και *Jacobi*. Η θεωρία

των Ελλειπτικών καμπυλών έχει εντυπωσιακές εφαρμογές στην Θεωρία των Αριθμών, όπως φαίνεται και από το σημαντικό ρόλο που έπαιξε στην απόδειξη του Θεωρήματος του *Fermat* από τον *Wiles* το 1994 (βλ. *Wiles*, *Modular elliptic curves and Fermat's Last Theorem*, *Annals of Mathematics* 141 (1995) 443-551). Επίσης έχει εφαρμογές στην Κρυπτογραφία με τον αλγόριθμο Ελλειπτικών καμπυλών του *Lenstra* (βλ. *F.W.Lenstra*, *Factoring integers with elliptic curves* , *Annals of Mathematics* 126 (1987) 649-673). Στη συνέχεια θα δούμε απλές γεωμετρικές εφαρμογές. Η χρήση της Θεωρίας Ομάδων δίνει γεωμετρικά συμπεράσματα με απλές αποδείξεις, όπου οι αντίστοιχες γεωμετρικές αποδείξεις, αν υπάρχουν, είναι πολύπλοκες.

Θεώρημα 3 Τα $3n$ σημεία (όχι απαραίτητα διαφορετικά) $P_1, P_2, ...P_{3n}$ της λείας κυβικής καμπύλης C είναι τα σημεία τομής (με αντίστοιχες πολλαπλότητες τομής, αν κάποιο εμφανίζεται περισσότερο από μια φορά) της C με μια καμπύλη βαθμού n αν και μόνο αν

$$P_1 + P_2 + ... + P_{3n} = O.$$

Ειδικότερα, τρία σημεία είναι συνευθειακά αν και μόνο αν

$$P_1 + P_2 + P_3 = O.$$

Αν L είναι η εφαπτόμενη στην κυβική σε ένα σημείο της D που τέμνει την κυβική και στο σημείο E, τότε έχουμε $2D + E = O$. Ενώ για τα σημεία καμπής έχουμε $3F = O$.

Έστω O το ουδέτερο στοιχείο της ομάδας. Το O είναι σημείο καμπής άρα μπορούμε να φέρουμε από το O τρείς εφαπτομένες προς την κυβική. Έστω O_1, O_2, O_3 τα σημεία επαφής. Τότε από τις τρείς εφαπτομένες ευθείες έχουμε τις παρακάτω εξισώσεις $2O_1 + 0 = 0, 2O_2 + O = O, 2O_3 + O = O$. Δηλαδή $2O_1 = O, 2O_2 = O, 2O_3 = O$. Άρα τα τρία σημεία έχουν τάξη 2 (στην πραγματικότητα συμπεραίνουμε ότι έχουν τάξη διαιρέτη του 2. Δεν μπορούν όμως να έχουν τάξη 1, αφού το μόνο στοιχείο που έχει τάξη 1 είναι το ουδέτερο (δηλ. το O). Δεν υπάρχει άλλο σημείο τάξης 2. Αν υπήρχε, έστω το X, τότε θα είχαμε $2Q = O$, δηλαδή $2Q + O = O$. Άρα η εφαπτομένη στο X διέρχεται από το O. Αυτό όμως ισχύει μόνο για τα τρία σημεία O_1, O_2, O_3.

Θεώρημα 4 Τα τρία σημεία O_1, O_2, O_3 είναι συνευθειακά.

Απόδειξη Έστω L η ευθεία που διέρχεται από τα O_1, O_2. Η L διέρχεται και από ένα τρίτο σημείο της κυβικής, έστω το Y. Τότε έχουμε για την ευθεία L: $O_1+O_2+Y = O$ και άρα και $2O_1 + 2O_2 + 2Y = O$. Όμως $2O_1 = O, 2O_2 = O$ άρα και $2Y = O$. Δηλαδή το Y έχει τάξη διαιρέτη του 2, άρα $Y \in O, O_1, O_2, O_3$. Εξετάζουμε όλες τις περιπτώσεις: Αν $Y = O$ τότε $O_1 + O_2 + O = O$, όμως $2O_1 + O = O$ άρα $O_1 = O_2$, άτοπο. Αν $Y = O_1$ τότε η εξίσωση $O_1 + O_2 + Y = O$ γίνεται $O_1 + O_2 + O_1 = O$, δηλαδή $2O_1 + O_2 = O$ και άρα $O_2 = O$, άτοπο. Αν $Y = O_2$ τότε η εξίσωση $O_1 + O_2 + Y = O$ γίνεται $O_1 + O_2 + O_2 = O$, δηλαδή $O_1 + 2O_2 = O$ και άρα $O_1 = O$, άτοπο. Συνεπώς

τελικά $Y = O_3$. Άρα τα τρία σημεία O_1, O_2, O_3 είναι συνευθειακά.

Θεώρημα 5 Τα τρία σημεία O_1, O_2, O_3 τάξης 2 μαζί με το O αποτελούν μια ομάδα τάξης 4 ισόμορφη με την ομάδα του $Klein$, $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Θεώρημα 6 Τα εννέα σημεία καμπής, μιας λείας κυβικής καμπύλης, είναι ανά τρία συνευθειακά.

Απόδειξη Έστω K_1, K_2 σημεία καμπής και $V(L)$ η ευθεία που διέρχεται από τα K_1, K_2. Έστω X το τρίτο σημείο τομής. Από τις ιδιότητες της ομάδας έχουμε $3K_1 = O$, $3K_2 = O$ και $K_1 + K_2 + X = O$. Από τις εξισώσεις συμπεραίνουμε ότι $3X = O$, δηλαδή ότι το σημείο X είναι σημείο καμπής (Απόδειξη: Θεωρούμε την εφαπτομένη στο σημείο X. Έστω ότι αυτή τέμνει την καμπύλη σε ένα σημείο Y, τότε έχουμε $2X + Y = O$. Και επειδή είναι $3X = O$, συμπεραίνουμε ότι $Y = X$. Άρα το X είναι σημείο καμπής).

Παρατήρηση 7 Επειδή ανά τρία τα 9 σημεία καμπής είναι συνευθειακά, ισχύουν τα εξής: Έχουμε 12 συνολικά ευθείες που διέρχονται από τα σημεία καμπής. Από κάθε σημείο διέρχονται 4 από αυτές. Και σε καθε ευθεία βρίσκονται 3 σημεία καμπής.

Θεώρημα 8 Τα εννέα σημεία καμπής, μιας λείας κυβικής καμπύλης, αποτελούν μια ομάδα τάξης 9 ισόμορφη με την ομάδα $\mathbb{Z}_3 \times \mathbb{Z}_3$.

ΑΣΚΗΣΕΙΣ

- 1. Η κανονική εξίσωση του $Weierstrass$ μιας κυβικής καμπύλης είναι της μορφής

$$Y^2 = X^3 + aX^2 + bX + c.$$

  Δείξτε ότι η παραπάνω κυβική καμπύλη έχει ένα σημείο καμπής στο άπειρο. Στη θεωρία των ελλειπτικών καμπυλών συνήθως αυτό το σημείο καμπής επιλέγεται για ουδέτερο σημείο της ομάδας, όταν για αριθμοθεωρητικούς σκοπούς χρησιμοποιείται η ομάδα στις κυβικές.

- 2. Αποδείξτε ότι τα σημεία $(0, 1, 0), (0, 0, 1)$ της καμπύλης $V(Y^2Z + Z^2Y - X^3)$ είναι σημεία καμπής. Βρείτε τουλάχιστον ένα ακόμη σημείο καμπής.

- 3. Δίνεται μια λεία κυβική και μια κωνική που τέμνει την κυβική σε ένα μόνο σημείο. Τι ξέρετε για το σημείο αυτό· Πόσα σημεία και ποιά της κυβικής καμπύλης μπορεί να έχουν την ιδιότητα αυτή;

- 4. Αποδείξτε, χωρίς χρήση του θεωρήματος 3, ότι έξι διαφορετικά σημεία A, B, C, D, E, F μιας λείας κυβικής $V(F)$ ανήκουν στην ίδια κωνική αν και μόνο αν

$$A + B + C + D + E + F = 0,$$

  στην ομάδα που ορίζεται με τον κανόνα χορδής-εφαπτομένης στην κυβική.

- 5. Το 1621 ο *Bachet* προσπαθώντας να βρει ρητές λύσεις της Διοφαντικής εξίσωσης

$$Y^2 - X^3 = c$$

παρατήρησε ότι αν (x, y) είναι ρητή λύση τότε και η

$$(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3})$$

είναι ρητή λύση της ίδιας εξίσωσης. Σήμερα γνωρίζουμε ότι αν ισχύει $xy \neq 0$ και $c \neq 1$, $c \neq -432$ τότε επαναλαμβάνοντας την παραπάνω διαδικασία οδηγούμαστε σε άπειρες διαφορετικές ρητές λύσεις. Για παράδειγμα η εξίσωση

$$Y^2 - X^3 = -2$$

έχει προφανή ρητή λύση την $(3, 5)$. Χρησιμοποιώντας τον τύπο του *Bachet* μπορούμε να πάρουμε άπειρες ρητές λύσεις της ίδιας εξίσωσης, όπως

$$(\frac{129}{100}, \frac{383}{1000}), (\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}), ...$$

Αποδείξτε τον τύπο του *Bachet* δείχνοντας ότι η εφαπτομένη στην καμπύλη $V(Y^2 - X^3 - c)$ στο σημείο της (x, y) διέρχεται από το σημείο της καμπύλης

$$(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}).$$