Εισαγωγή

Εστω E μια ελλειπτική καμπύλη ορισμένη στο σώμα $\mathbb{Q}$. Πρώτος ο Poincare όριοε στα 1901 πράξη πρόσθεσης των ρητών σημείων της ελλειπτικής καμπύλης E και απέδειξε ότι τα σημεία αυτά, με την πράξη αυτή, αποτελούν αβελιανή ομάδα. Ο Mordell απέδειξε ότι η ομάδα αυτή είναι πεπερασμένα παραγόμενη. Αμέσως μετά ο A. Weil απέδειξε ότι το ίδιο ισχύει και για την ομάδα των K-ρητών σημείων ελλειπτικής καμπύλης ορισμένης στο K, $E(K)$, όπου K αλγεβρικό σώμα αριθμών.

Τα κύρια προβλήματα που αφορούν την μελέτη των ελλειπτικών καμπύλων είναι τα εξής: Αν E/K δοομένη ελλειπτική καμπύλη, τότε ποιά είναι η ομάδα των σημείων πεπερασμένης τάξης της $E(K)$, $E_{tor}(K)$ και πόσο είναι ο rank της $E(K)$; Οταν μας δοθεί η E/K είναι σχετικά εύκολο να βρεθεί η ομάδα $E_{tor}(K)$ της E. Απείρως δυσκολότερο όμως είναι το ερώτημα: Αν K αλγεβρικό σώμα αριθμών, τότε ποιές είναι οι πεπερασμένες ομάδες που εμφανίζονται σαν αμάδες σημείων πεπερασμένης τάξης ελλειπτική καμπύλης E ορισμένης στο σώμα K (ή σε υπόσωμά του);

Μια σχετική εικασία του Manin (1969), ισχυρίζεται ότι υπάρχει σταθερά $B := B(K)$, η οποία εξαρτάται μόνο από το σώμα K και η οποία φράσσει την τάξη όλων των ομάδων $E_{tor}(K)$, όπου E μια ελλειπτική καμπύλη ορισμένη στο σώμα K. Μάλιστα μια ισχυρότερη μορφή της εικασίας του Manin είναι ότι η σταθερά B δεν εξαρτάται από το σώμα, αλλά μόνο από τον βαθμό της επέκτασης $d = (K : \mathbb{Q})$. Ας σημειωθεί εδώ ότι η εικασία του Manin αποδείχτηκε πρόσφατα (1994), από τον L. Merel. Συγκεκριμένα απέδειξε ότι, αν μια ελλειπτική καμπύλη E, ορισμένη επί ενός αλγεβρικού σώματος αριθμών K, βαθμού $d > 1$ υπέρ το $\mathbb{Q}$ έχει σημείο τάξης πρώτου αριθμού p, τότε $p < d^{3d^2}$. Σε μια εργασία που άφησε εποχή στα Μαθηματικά ο B. Mazur απέδειξε ότι αν E είναι μια ελλειπτική καμπύλη ορισμένη στο $\mathbb{Q}$, τότε η ομάδα $E_{tor}(\mathbb{Q})$, είναι μία από τις ακόλουθες:

$$\mathbb{Z}/m\mathbb{Z}, \quad \text{αν} \;\; m \leq 10 \;\; \text{ή} \;\; m = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\nu\mathbb{Z}, \quad \text{αν} \;\; \nu \leq 4.$$

Σημαντικά αποτελέσματα όσον αφορά την εικασία του Manin επέτυχαν και οι Kamienny, Kenku, Mommose.

Σκοπό της εργασίας, είναι η μελέτη των K-ρητών σημείων πεπερασμένης τάξης μιας ελλειπτικής καμπύλης E, όπου K είναι ένα αλγεβρικό σώμα αριθμών, ή μια στοιχειώδης 2-αβελιανή άπειρη επέκταση του $\mathbb{Q}$.

Κορμός της εργασίας, είναι το βιβλίο του Silverman ([Si1]), όσον αφορά την γενική θεωρία, το άρθρο των Fung-Müller-Williams-Zimmer ([Fu]), το οποίο αναφέρεται σε ελλειπτικές καμπύλες με ακέραια απόλυτη αναλλοίωτο ορισμένες σε απλά κυβικά σώματα αριθμών και τέλος το άρθρο των Laska-Lorenz ([La-Lo]), το οποίο αναφέρεται στά F-ρητά σημεία πεπερασμένης τάξης ελλειπτικών καμπύλων ορισμένων στο $\mathbb{Q}$, όπου F η στοιχειώδης 2-αβελιανή επέκταση του $\mathbb{Q}$, $F = \mathbb{Q}(\sqrt{z}|z \in \mathbb{Z})$. Για την κατανόηση της παρούσας εργασίας απαιτούνται γνώσεις Αλγεβρικής Θεωρίας αριθμών Ι και Θεωρίας Εκτιμήσεων.

Στο πρώτο κεφάλαιο κάνουμε μια σύντομη επισκόπιση της θεωρίας των ελλειπτικών καμπύλων και στην συνέχεια δίνουμε πλήρη περιγραφή των πολυωνύμων διαίρεσης, τα οποία μας εξασφαλίζουν μια χρήσιμη και κομψή γραφή των συντεταγμένων των πολλαπλασίων ενός ρητού σημείου μιας ελλειπτική καμπύλης. Στο δεύτερο κεφάλαιο ορίζουμε την έννοια της τυπικής ομάδας και ιδιαίτερα αναφερόμαστε στην τυπική ομάδα μιας ελλειπτικής καμπύλης , της οποίας μελετούμε τις ιδιότητες. Επίσης μελετούμε την τυπική ομάδα μιας ελλειπτικής καμπύλης ορισμένης σε τοπικό σώμα αριθμών. Στο τρίτο κεφάλαιο αναπτύσσουμε την θεωρία αναγωγής ελλειπτικών καμπύλων, με σκοπό την εξαγωγή χρήσιμων συμπερασμάτων για την μελέτη των ιδιοτήτων των σημείων πεπερασμένης τάξης μιας ελλειπτικής καμπύλης. Στο τέταρτο κεφάλαιο, συνδιάζουμε τα αποτελέσματα των τριών προηγουμένων κεφαλαίων στην περίπτωση που η καμπύλη E έχει ακέραια απόλυτη αναλλοίωτο και αποδεικνύουμε το κύριο θεώρημα του κεφαλαίου, το οποίο μας δίνει σχέσεις διαίρεσης της τάξης της torsion ομάδας $E_{tor}(K)$, ανάλογα με τον τύπο αναγωγής που έχουμε. Στην συνέχεια εφαρμόζουμε αυτό το θεώρημα στην περίπτωση όπου το σώμα K είναι απλό κυβικό σώμα αριθμών και προσδιορίζουμε όλες τις δυνατές ελλειπτικές καμπύλες E και όλα τα δυνατά σώματα K, με torsion ομάδα μια από αυτές που μας εξασφαλίζει το θεώρημα. Στο πέμπτο και τελευταίο κεφάλαιο, προσδιορίζουμε όλες τις δυνατές torsion ομάδες $E_{tor}(F)$, μιας ελλειπτικής καμπύλης E ορισμένης στο $\mathbb{Q}$, όπου το σώμα F είναι η στοιχειώδης 2-αβελιανή επέκταση του $\mathbb{Q}$, $F = \mathbb{Q}(\sqrt{z}|z \in \mathbb{Z})$. Αποδεικνύουμε ότι η ομάδα $E_{tor}(K)$ είναι πεπερασμένη και έχει 31 δυνατότητες. Το γεγονός ότι η ομάδα $E_{tor}(K)$ είναι πεπερασμένη προκύπτει από ένα πιο γενικό θεώρημα το οποίο απέδειξαν (ανεξάρτητα) οι Serre και Imai και μια πλήρη απόδειξη αυτού μπορεί να δει κανείς στο [Ri].

Τέλος θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή και Δάσκαλό μου Γιάννη Αντωνιάδη, ο οποίος με βοήθησε να ανακαλύψω την ομορφιά των προβλημάτων της Θεωρίας Αριθμών, καθώς και για τις πολύτιμες συμβουλές και υποδείξεις του.

19.10.1995,

.

1 Γενικά περί ελλειπτικών καμπύλων

1.1 Εισαγωγή στις ελλειπτικές καμπύλες

Εστω $E : \mathrm{Y}^2 + \alpha_1\mathrm{XY} + \alpha_3\mathrm{Y} = \mathrm{X}^3 + \alpha_2\mathrm{X}^2 + \alpha_4\mathrm{X} + \alpha_6,$ όπου $\alpha_i \in \mathrm{K}$, μια ελλειπτική καμπύλη στην γενική μορφή του Weierstrass, ορισμένη στο σώμα K. Με Δ θα συμβολίζουμε την διακρίνουσά της και με j την απόλυτο αναλλοίωτο αυτής.

Αν η χαρακτηριστική του K είναι διαφορετική του 2, τότε μπορούμε να απλοποιήσουμε την παραπάνω εξίσωση, κάνοντας τον εξής μετασχηματισμό:

$$Y \mapsto \frac{1}{2}(Y - a_1X - a_3), \quad \text{και} \quad X \mapsto X.$$

Η εξίσωση της καμπύλης γίνεται

$$E : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6,$$

όπου τα $b_i \in \mathrm{K}$ δίνονται από τις εξής σχέσεις:

- $b_2 = a_1^2 + 4a_2,$
- $b_4 = 2a_4 + a_1a_3,$
- $b_6 = a_3^2 + 4a_6.$

Αν τώρα κάνουμε τους μετασχηματισμούς :

- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$
- $c_4 = b_2^2 - 24b_4,$
- $c_6 = b_2^3 + 36b_2b_4 - 216b_6,$

τότε προκύπτει ότι :

- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$
- $j = c_4^3/\Delta.$

Εύκολα βλέπει κανείς ότι:

- $4b_8 = b_2b_6 - b_4^2$ και $1728\Delta = c_4^3 - c_6^2$

Αν επιπλέον η χαρακτηριστική του K, $\mathrm{char}(K) \neq 2, 3$ τότε αντικαθιστώντας

$$\text{το } X \text{ μέ } \quad \frac{X - 3b_2}{36}, \text{ καί το } Y \text{ με } \quad \frac{Y}{216}$$

εξαφανίζουμε τον όρο X^2 καί παίρνουμε την απλούστερη εξίσωση:

$$E : Y^2 = X^3 - 27c_4X - 54c_6.$$

Συνεπώς είδαμε ότι άν το σώμα Κ είναι χαρακτηριστικής διαφορετικής του 2 και του 3, τότε η ελλειπτική καμπύλη E γράφεται στην λεγόμενη μικρή μορφή του Weierstrass

$$E : Y^2 = X^3 + AX + B \quad \text{όπου } \mathrm{A}, \mathrm{B} \in K.$$

Επίσης δύο ελλειπτικές καμπύλες E καί $\hat{E}$ ορισμένες στο σώμα Κ,

$$E : \mathrm{Y}^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad \text{και},$$

$$\hat{E} : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

θα λέγονται αμφίρρητα ισόμορφες, όταν υπάρχουν $r, s, t, u \in K$ και $u \in K^*$, τέτοια ώστε :

$$\mathrm{X} = u^2x + r, \quad \mathrm{Y} = u^3y + su^2x + t,$$

Επίσης τα a_i και a_i', $i \in \{1, 2, 3, 4, 6\}$ συνδέονται από τις ακόλουθες σχέσεις:

$$\begin{aligned}
ua_1' &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1
\end{aligned}$$

Τέλος τα b_i, b_i', c_i, c_i' και οι διακρίνουσες Δ, Δ' των αντίστοιχων καμπύλων συνδέονται από τις σχέσεις:

$$u^2b_2' = b_2 + 12r$$

$$
\begin{aligned}
u^4 b_4' &= b_4 + r b_2 + 6r^2 \\
u^6 b_6' &= b_6 + 2r b_4 + r^2 b_2 + 4r^3 \\
u^8 b_8' &= b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \\
u^4 c_4' &= c_4 \\
u^6 c_6' &= c_6 \\
u^{12} \Delta' &= \Delta
\end{aligned}
$$

Για μία ελλειπτική καμπύλη E ορίζουμε ως αναλλοίωτο του Hasse την σταθερά :

$$\delta_E \equiv -c_4/c_6 \pmod{K^{*^2}}, \quad \text{όταν} \quad c_4, c_6 \neq 0.$$

Αποδεικνύεται δε ότι ισχύει ([Κον], θεώρημα 2.8, σελ. 22) :

Πρόταση 1.1 j E $\bar{K}$ (K). j δ_E, K.

Σημειώνουμε ότι ένα απλό παράδειγμα αμφίρρητου μετασχηματισμού, είναι ο μετασχηματισμός από την γενική μορφή στην μικρή μορφή του Weierstrass που είδαμε πιο πριν .

Το σύνολο $E(\mathrm{K}) := \{P = [x, y, z] \in \mathcal{P}_2(K)/y^2 z = x^3 + Axz^2 + Bz^3\}$, μαζί με το επ' άπειρο σημείο $O = [0, 1, 0]$ αποτελούν αβελιανή προσθετική ομάδα, με ουδέτερο στοιχείο το O. Αν K είναι ένα αλγεβρικό σώμα αριθμών, τότε λόγω του θεωρήματος των Mordell-Weil, η ομάδα αυτή είναι πεπερασμένα παραγόμενη

$$E(K) \cong E_{tor}(K) \bigoplus \mathbb{Z}^{r_K}$$

με ομάδα σημείων πεπερασμένης τάξης $E_{tor}(K)$ καί rank $r_K \in \mathbb{N}_0$ ([Αν 2]) .

1.2 Συνάρτηση του Weierstrass και πολυώνυμα διαίρεσης

Θεωρούμε ένα δικτυωτό L στο μιγαδικό επίπεδο $\mathbb{C}$, δηλαδή μιά ελεύθερη αβελιανή ομάδα διάστασης 2 υπέρ το $\mathbb{Z}$ και έστω ω_1, ω_2 μια βάση του. Μια ελλειπτική συνάρτηση f (ως προς το δυκτιωτό L) είναι εξ ορισμού μια μερόμορφη συνάρτηση του $\mathbb{C}$ με την επιπλέον ιδιότητα της L-περιοδικότητας, δηλαδή $f(z) = f(z + w)$, $\forall w \in L$.

Αμεση συνέπεια του ορισμού είναι ότι όταν μια ελλειπτική συνάρτηση είναι ολόμορφη (δεν έχει πόλους), είναι απαραίτητα σταθερά διότι ως συνεχής συνάρτηση στον μιγαδικό τόρο $\mathbb{C}/L$

που είναι συμπαγής, θα είναι φραγμένη συνάρτηση και άρα, λόγω περιοδικότητας σταθερή (Θεώρημα Liouville).

Ορίζουμε επίσης ως θεμελιώδες παραλληλόγραμμο του δικτυωτού L, το σύνολο όλων των σημείων $a + t_1\omega_1 + t_2\omega_2$, όπου το a ανήκει στο $\mathbb{C}$ και $0 \leq t_i < 1$

Χωρίς αποδείξεις αναφέρουμε τα παρακάτω θεωρήματα :

Θεώρημα 1.2 P L f (L) P. T f P 0 .

Πόρισμα 1.3 f ( ) $\mathbb{C}/L$.

Θεώρημα 1.4 , 1.2, P f . a_i f P f m_i a_i, $\sum m_i = 0$.

Θεώρημα 1.5 1.4, :

$$\sum m_i a_i \equiv 0 mod L.$$

Ο ενδιαφερόμενος αναγνώστης μπορεί να βρει τις αποδείξεις των παραπάνω προτάσεων στο [La], σελ. $3-5$.

Χαρακτηριστικό παράδειγμα ελλειπτικής συνάρτησης αποτελεί η $\wp$ -συνάρτηση του Weierstrass

$$\wp(z) = \frac{1}{z^2} + \sum \frac{1}{(z-w)^2} - \frac{1}{w^2},$$

όπου το άθροισμα διατρέχει όλες τις μη-μηδενικές περιόδους του δικτυωτού $L = [\omega_1, \omega_2]$. Χωρίς αποδείξεις επίσης αναφέρουμε τις παρακάτω ιδιότητες της $\wp$-συνάρτησης του Weierstrass ([La], σελ $6-10$). Η συνάρτηση $\wp$ συγκλίνει ομοιόμορφα στα συμπαγή σύνολα που δεν περιέχουν σημεία του δικτυωτού L. Επίσης η $\wp$ είναι άρτια συνάρτηση, ενώ η παράγωγός της είναι περιττή. Εχει δε στο $z = 0$, ανάπτυγμα της μορφής:

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + G_6 z^4 + \cdots$$

και η παράγωγός της:

$$\wp'(z) = \frac{-2}{z^3} + 6G_4 z + 20G_6 z^3 + \cdots,$$

όπου τα G_i , δίνονται από τις σχέσεις $G_i(L) = G_i = \sum_{w \neq 0} \frac{1}{w^i}$. Ορίζουμε:

$$g_2 := 60G_4, \quad g_3 := 140G_6$$

Η $\wp$-συνάρτηση του Weierstrass ικανοποιεί την ακόλουθη διαφορική εξίσωση:

$$\wp'(z)^2 = 4\wp^3(z) - g_2\wp(z) - g_3.$$

Συνεπώς γίνεται πλέον φανερό ότι τα σημεία $(\wp(z), \wp'(z))$, είναι σημεία της επίπεδης κυβικής καμπύλης

$$y^2 = 4x^3 - g_2x - g_3$$

όπου το πολυώνυμο του δεξιού μέλους έχει διακρίνουσα

$$\Delta(\omega_1, \omega_2) = \Delta = g_2^3 - 27g_3^2 \neq 0.$$

Αρα η παραπάνω καμπύλη είναι μια ελλειπτική καμπύλη και η $\wp$-συνάρτηση του Weierstrass την παραμετρίζει μέσω του (αναλυτικού) ισομορφισμού :

$$\mathbb{C}/L - \{\mathrm{O}\} \longrightarrow E(\mathbb{C}) - \{O\}$$

$$z \mapsto (1, \wp(z), \wp'(z)).$$

Στην συνέχεια θα ορίσουμε τα πολυώνυμα διαίρεσης και θα μελετήσουμε τις ιδιότητές τους.

Αν A είναι αβελιανή προσθετική ομάδα και n ένας φυσικός αριθμός με A_n θα συμβολίζουμε την υποομάδα των στοιχείων $u \in \mathrm{A}$ τέτοια ώστε $nu = 0$.

Κατ' αρχήν θα αποδείξουμε ότι για κάθε φυσικό αριθμό $n \geq 1$ υπάρχει ελλειπτική συνάρτηση f_n, τέτοια ώστε :

$$(f_n(z))^2 = n^2 \prod(\wp(z) - \wp(u)),$$

όπου το γινόμενο διατρέχει όλα τα $u \in (\mathbb{C}/L)_n$, $u \neq 0$.

Πράγματι :

Για n περιττό όλοι οι παράγοντες θα έχουν πολλαπλότητα 2, διότι οι δύο τιμές $\pm u$ δεν είναι ισοδύναμες modulo L και δίνουν, προφανώς, την ίδια τιμή, $\wp(u) = \wp(-u)$.

Για n άρτιο όλοι οι παράγοντες του γινομένου έχουν πολλαπλότητα 2, εκτός αυτών για τους οποίους ισχύει $2u \equiv 0 \pmod L$. Προφανώς, αυτοί αντιστοιχούν στις τιμές $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{\omega_3}{2}$ ($\omega_3 = \omega_1 + \omega_2$) και έχουν πολλαπλότητα 1. Σε αυτά τα σημεία η συνάρτηση $\wp - \wp(u)$ έχει διπλή ρίζα και ισχύει ότι ([La], σελ. 10)

$$(\wp')^2 = 4\prod(\wp - \wp(u)),$$

όπου το γινόμενο διατρέχει τα σημεία u τάξης 2, $u \neq 0$. Αρα το γινόμενο, $\prod(\wp(z) - \wp(u))$, όπου $u \in (\mathbb{C}/L)_n$, είναι τέλειο τετράγωνο.

Επομένως η συνάρτηση ορισμού του $f_n(z)^2$, είναι τέλειο τετράγωνο. Μπορούμε λοιπόν να διαλέξουμε το πρόσημο της $f_n(z)$, έτσι ώστε:

Για n περιττό $f_n = P_n(\wp)$, όπου P_n πολυώνυμο βαθμού $\frac{n^2-1}{2}$ και

$$f_n = n\wp^{\frac{n^2-1}{2}} + \cdots .$$

Για n άρτιο $f_n = \frac{1}{2}\wp' P_n(\wp)$, όπου το P_n είναι πολυώνυμο βαθμού $\frac{n^2-4}{2}$ και

$$f_n = \frac{n}{2}\wp'\wp^{\frac{n^2-4}{2}} + \cdots$$

Συνεπώς σε κάθε περίπτωση έχουμε ανάπτυγμα στο σημείο $z = 0$ της μορφής

$$f_n(z) = \frac{(-1)^{n+1}n}{z^{n^2-1}} + \cdots .$$

Διότι, στο ανάπτυγμα στο $z = 0$ της $\wp$-συνάρτησης του Weierstrass ο πρώτος όρος είναι ο $\frac{1}{z^2}$, ενώ της $\wp'$ είναι $\frac{-2}{z^3}$. Επομένως ο πρώτος του αναπτύγματος στο $z = 0$ της f_n , είναι:

$$n(\frac{1}{z^2})^{\frac{n^2-1}{2}} = \frac{n}{z^{n^2-1}} \quad \text{για } n \text{ περιττό},$$

$$(\frac{n}{2})(\frac{-2}{z^3})(\frac{1}{z^2})^{\frac{n^2-4}{2}} = \frac{-n}{z^{n^2-1}}, \quad \text{για } n \text{ άρτιο},$$

δηλαδή το ζητούμενο.

Στην συνεχεια ορίζουμε για κάθε φυσικό αριθμό $n \geq 1$ την εξής ακολουθία συναρτήσεων:

$$\wp_n(z) = \wp(nz)$$

Θεώρημα 1.6

$$\wp_n = \wp - \frac{f_{n+1}f_{n-1}}{f_n^2}.$$

Απόδειξη : Θα αποδείξουμε ότι η συνάρτηση $\wp(nz) - \wp(z)$ (εκτός των σημείων του δικτυωτού L), έχει:

1. πόλους ακριβώς στις ρίζες της $(f_n)^2$, όλες με την ίδια πολλαπλότητα, 2.

2. ρίζες στα σημεία z τέτοια ώστε $nz \equiv \pm z mod L$

Πράγματι:

Κατ'αρχήν σε κάθε δικτυωτό $L = [\omega_1, \omega_2]$ του $\mathbb{C}$ ορίζουμε, εκτός από την $\wp$-συνάρτηση του Weierstrass και την σ-συνάρτηση του Weierstrass ως εξής:

$$\sigma(z) = z \cdot \prod_{\omega \in L, \omega \neq 0} (1 - \frac{z}{\omega}) \exp(z/\omega + \frac{1}{2}(z/\omega)^2).$$

Για την σ-συνάρτηση του Weierstrass, είναι γνωστό ότι έχει ρίζες πολλαπλότητας 1 στα σημεία του δικτυωτού L ([La], σελ. 19).

Οι σ και $\wp$-συναρτήσεις του Weierstrass συνδέονται από την ακόλουθη σχέση ([La], θεώρημα 6.2, σελ. 23):

$$\wp(z) - \wp(a) = -\frac{\sigma(z+a)\sigma(z-a)}{(\sigma(z))^2(\sigma(a))^2}, \quad a \in \mathbb{C} - L \quad (*).$$

Η συνάρτηση $\wp(z) - \wp(nz)$ έχει πόλους (εκτός των σημείων του δικτυωτού) στα σημεία για τα οποία ισχύει $nz \equiv 0 \pmod{L}$, δηλαδή ακριβώς σε αυτά τα u όπου η f_n^2 έχει ρίζες τάξης 2.

Είναι προφανές ότι τα σημεία για τα οποία ισχύει $nz \equiv \pm z \pmod{L}$ είναι ρίζες της συναρτησης $\wp(z) - \wp(nz)$. Επιπλέον όλες αυτές οι ρίζες έχουν πολλαπλότητα 1. Για να το δούμε αυτό ας θέσουμε:

$$\varphi(z) := \wp(nz) - \wp(z),$$

οπότε:

$$\varphi'(z) = n\wp'(nz) - \wp'(z).$$

Συνεπώς εάν $nz \equiv \pm z mod L$, τότε :

$$\varphi'(z) = n\wp'(\pm z) - \wp'(z) = \pm n\wp'(z) - \wp'(z) = (\pm n - 1)\wp'(z) \neq 0,$$

διότι $n \neq 1$. Αρα η συνάρτηση:

$$\frac{f_n^2(\wp_n - \wp)}{f_{n+1} f_{n-1}},$$

είναι ελλειπτική και δεν έχει ρίζες ή πόλους εκτός από τα σημεία του δικτυωτού L. Επομένως η παραπάνω συνάρτηση είναι σταθερή . Εχει δε στο 0 ανάπτυγμα του οποίου ο πρώτος όρος είναι:

$$\frac{n^2(\frac{1}{n^2} - 1)}{(n+1)(n-1)} = -1.$$

Αρα πράγματι:

$$\wp_n = \wp - \frac{f_{n+1}f_{n-1}}{f_n^2}. \quad \square$$

Με την βοήθεια του θεωρήματος 1.6 θα υπολογίσουμε στην συνέχεια την έκφραση των f_n σαν πολυώνυμα της $\wp$-συνάρτησης του Weierstrass για μικρές τιμές του n. Για τον σκοπό μας αυτό θα χρησιμοποιήσουμε την εξής σχέση ([La], σελ. 13):

$$\wp_2 = -2\wp + \frac{1}{4}(\frac{\wp''}{\wp'})^2.$$

Ομως παραγωγίζοντας την διαφορική εξίσωση της συνάρτησης του Weierstrass, έχουμε:

$$\wp'' = 6\wp^2 - \frac{1}{2}g_2.$$

Συνδιάζοντας αυτές τις δύο σχέσεις, έχουμε:

$$\wp_2 = \wp - \frac{3\wp^4 - \frac{3}{2}\wp^2 - 3g_3\wp - \frac{1}{16}g_2^2}{(\wp')^2}.$$

Από τους τύπους των f_n προκύπτει αμέσως ότι:

$$f_1 = 1 \quad \text{και} \quad f_2 = \wp'$$

Από το θεώρημα 1.6 έχουμε $\wp_2 - \wp_1 = -\frac{f_3}{(\wp')^2}$. Αρα:

$$f_3 = 3\wp^4 - \frac{3}{2}g_2\wp^2 - 3g_3\wp - \frac{1}{16}g_2^2.$$

Ανάλογα, με την βοήθεια του θεωρήματος 1.6 και του " θεωρήματος πρόσθεσης " της $\wp$-συνάρτησης του Weierstrass ([La], σελ. $10-13$), μπορεί κανείς να αποδείξει ότι:

$$f_4 = \frac{1}{2}\wp'(4\wp^6 - 5g_2\wp^4 - 20g_3\wp^3 - \frac{5}{4}g_2^2\wp^2 - g_2g_3\wp - 2g_3^2 + \frac{1}{16}g_2^3).$$

Ισχύει το ακόλουθο θεώρημα :

Θεώρημα 1.7 *$m > n$. :*

$$f_{m+1}f_{m-1}f_n^2 - f_{n+1}f_{m-1}f_m^2 = f_{m+n}f_{m-n}.$$

Απόδειξη : Λόγω του θεωρήματος 1.6 έχουμε :

$$\wp - \wp_n = \frac{f_{n+1}f_{n-1}}{f_n^2} \qquad \text{και} \qquad \wp - \wp_m = \frac{f_{m+1}f_{m-1}}{f_m^2}. \qquad \text{Αρα:}$$

$$\wp_n - \wp_m = \frac{f_{m+1}f_{m-1}f_n^2 - f_{n+1}f_{n-1}f_m^2}{f_m^2 f_n^2}.$$

Επομένως αρκεί να αποδείξουμε ότι:

$$\wp_n - \wp_m = \frac{f_{m+n}f_{m-n}}{f_n^2 f_m^2}.$$

Παρατηρούμε ότι η συνάρτηση $\wp_m - \wp_n$, έχει ρίζες στα σημεία u τέτοια ώστε:

$$mu \equiv \pm nu \not\equiv 0 \pmod{L}$$

και μάλιστα με πολλαπλότητα 1 (λόγω της σχέσης $(*)$). Ομως οι συναρτήσεις f_n, f_m, δεν έχουν ρίζες σε αυτά τα u διότι τα σημεία nu, mu δεν είναι ισοδύναμα με 0 modulo L. Επομένως τα σημεία u τέτοια ώστε $mu \equiv \pm nu \not\equiv 0 \pmod{L}$ είναι ρίζες της συνάρτησης:

$$f_{n+1}f_{n-1}f_m^2 - f_{m+1}f_{m-1}f_n^2.$$

Από την άλλη πλευρά όμως η συνάρτηση $f_{m+n}f_{m-n}$ έχει ακριβώς αυτά τα u ως ρίζες, ενώ η συνάρτηση $f_{n+1}f_{n-1}f_m^2 - f_{m+1}f_{m-1}f_n^2$ έχει πόλους μόνο στα σημεία του δικτυωτού L. Συνεπώς η συνάρτηση :

$$\frac{f_{m+n}f_{m-n}}{f_{n+1}f_{n-1}f_m^2 - f_{m+1}f_{m-1}f_n^2}$$

είναι σταθερή. Εχει δε στο $z = 0$ ανάπτυγμα του οποίου ο πρώτος όρος είναι

$$\frac{(m+n)(m-n)}{(n+1)(n-1)m^2 - (m+1)(m-1)n^2} = -1.$$

Αρα πράγματι:

$$f_{m+1}f_{m-1}f_n^2 - f_{n-1}f_{n+1}f_n^2 = f_{m+n}f_{m-n}. \qquad \square$$

Σαν ειδική περιπτωση, κάνουμε τους μετασχηματισμούς:

$$(m \mapsto n+1, \;\; n \mapsto n) \quad \text{και} \quad (m \mapsto n+1, \;\; n \mapsto n-1),$$

και παίρνουμε το ακόλουθο:

Θεώρημα 1.8 $\qquad n \geq 1, \qquad :$

$$f_{2n+1} = f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1},$$

$$\wp' f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2).$$

Θέτουμε:

$$X := \wp, \quad Y := \frac{1}{2}\wp', \quad a =: -\frac{1}{4}g_2, \quad b =: -\frac{1}{4}g_3$$

οπότε παίρνουμε ελλειπτική καμπύλη στην μικρή μορφή του Weierstrass :

$$\mathrm{Y}^2 = \mathrm{X}^3 + \mathrm{a}\mathrm{X} + b.$$

Από την παραπάνω αντικατάσταση προκύπτει αμέσως ότι οι συναρτήσεις f_n είναι πολυώνυμα των μεταβλητών X, Y. Οι τύποι της σελίδος 8, γράφονται:

$$f_1 = 1, \quad f_2 = 2Y, \quad f_3 = 3X^4 + 6aX^2 + 12bX - a^2,$$

$$f_4 = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3).$$

Βλέπουμε λοιπόν από τα παραπάνω ότι για $n = 1, 2, 3, 4$ μπορούμε να γράψουμε:

$$f_n = P_n(X), \text{ για } n \text{ περιττό και}$$

$$f_n = 2YP_n(X), \text{ για } n \text{ άρτιο}$$

όπου τα P_n είναι πολυώνυμα με συντελεστές από τον δακτύλιο $\mathbb{Z}[a, b, X]$. Αυτό ισχύει για κάθε φυσικό αριθμό n. Για να το δούμε θα πρέπει κατ' αρχήν, με την βοήθεια του θεωρήματος 1.8, να αποδείξουμε τους παρακάτω αναδρομικούς τύπους:

$$P_{2n+1} = f_{2n+1} = P_{n+2}P_n^3 - P_{n+1}^3P_{n-1}16Y^4 \text{ , για n περιττό}$$

$$P_{2n+1} = f_{2n+1} = -16Y^4P_{n+2}P_n^3 - P_{n+1}^3P_{n-1}, \quad \text{για } n \text{ άρτιο,}$$

$$P_{2n} = P_n(P_{n+2}P_{n-1}^2 - P_{n-2}P_{n+1}^2)$$

και στην συνέχεια να χρησιμοποιήσουμε μαθηματική επαγωγή. Θα αποδείξουμε τον πρώτο από τους τρείς τύπους. Ομοια αποδεικνύονται και οι άλλοι δύο.

Αν ο n είναι περιττός , τότε ο $n+2$ είναι επίσης περιττός ενώ οι $n+1$ και $n-1$ είναι άρτιοι. Αρα:

$$P_{2n+1} = f_{2n+1} = f_{n+2}f_n^3 - f_{n+1}^3f_{n-1} = P_{2n+2}P_n^3 - (2YP_{n+2})^3 2YP_{n-1},$$

δηλαδή το ζητούμενο.

Ας γράψουμε $\psi_n(X,Y) := f_n$, για κάθε φυσικό αριθμό n και ας ορίσουμε, επιπλέον, $\psi_0 := 0$ και $\psi_{-n} := -\psi_n$ ($n \in \mathbb{N}$). Με την βοήθεια των παραπάνω αναδρομικών τύπων, μπορούμε να υπολογίσουμε τον σταθερό όρο του πολυωνύμου $\psi_{2n+1}(X)$. Συγκεκριμένα θα αποδείξουμε ότι ισχύει:

$$\psi_{2n+1}(0) = (-1)^n a^{n^2+n} \text{ , αν b=0.}$$

Πράγματι :

$$\psi_{2n+1} = f_{2n+1} = P_{2n+1}, \text{ αφού 2n+1 περιττός.}$$

Συνεπώς :

$$\psi_{2n+1}(0) = P_{2n+1}(0).$$

Αντικαθιστώντας όμως $X = 0$ και $b = 0$, η εξίσωση του Weierstrass $Y^2 = X^3 + aX + b$ μας δίνει ότι και $Y = 0$.

Αρα από τους παραπάνω αναδρομικούς τύπους έχουμε:

$$\psi_{2n+1}(0) = P_{n+2}(0)P_n^3(0) \text{ , για n περιττό ,}$$

$$\psi_{2n+1}(0) = -P_{n+1}^3(0)P_{n-1}(0) \text{ , για n άρτιο .}$$

Εστω ότι ο φυσικός αριθμός n είναι περιττός, $n = 2\lambda + 1$, $\lambda \in \mathbb{N}$. Συνεχίζουμε τώρα την απόδειξη επαγωγικά ως πρός λ. Εστω $\lambda = 0$, δηλαδή $n = 1$. Τότε:

$$\psi_3(0) = P_3(0)P_1^3(0) = f_3(0)f_1^3(0).$$

Ομως $f_1 = 1$, $f_3 = 3X^4 + 6aX^2 + 12bX - a^2$. Δηλαδή:

$$\psi_3(0) = -a^2 = (-1)^1 a^{1^2+1}, \quad \text{ισχύει.}$$

Εστω τώρα ότι ισχύει το ζητούμενο για όλους τους φυσικούς τους μικρότερους του λ. Αφού ο n είναι περιττός έπεται ότι:

$$\psi_{2n+1}(0) = P_{n+2}(0)P_n^3(0).$$

Επίσης προφανώς ισχύει:

$$P_{n+2}(0) = f_{n+2}(0) = \psi_{n+2}(0).$$

Ομοια $P_n(0) = \psi_n(0)$. Προφανώς $n+2 = 2(\lambda+1)+1$. Επομένως μπορούμε να εφαρμόσουμε την επαγωγική υπόθεση για τα $\psi_n = \psi_{2\lambda+1}$, $\psi_{n+2} = \psi_{2(\lambda+1)+1}$. Εχουμε

$$\psi_{2n+1}(0) = \psi_{2(2\lambda+1)+1}(0) = \psi_{n+2}(0)\psi_n^3(0) = (-1)^\lambda a^{3\lambda^2+3\lambda}(-1)^{\lambda+1}a^{(\lambda+1)^2+(\lambda+1)}$$

$$\Rightarrow \psi_{2n+1}(0) = (-1)^{2\lambda+1}a^{3\lambda^2+3\lambda+(\lambda+1)^2+\lambda+1}$$

$$\Rightarrow \psi_{2n+1}(0) = (-1)^n a^{4\lambda^2+6\lambda+2} = (-1)^n a^{n^2+n}.$$

Αρα για n περιττό ισχύει το ζητούμενο . Ομοια δουλεύουμε για n άρτιο.

Το παρακάτω θεώρημα συνοψίζει την δουλειά που έχουμε κάνει μέχρι τώρα στα πολυώνυμα διαίρεσης:

Θεώρημα 1.9 $P = (x, y)$,

$$E : Y^2 = X^3 + aX + b. \qquad :$$

$$\begin{aligned} \phi_n(x) &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\ 4y\omega_n &= \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2. \end{aligned}$$

:

1. $nP = (\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3})$.

2. ϕ_n , ψ_n n $\frac{\psi_n}{2y}$ n $\mathbb{Z}[a, b, x]$. :

$$\phi_n(x) = x^{n^2} + \cdots, \qquad 1.$$

$$\psi_n^2(x) = n^2x^{n^2-1} + \cdots, \qquad n^2.$$

3. $y^{-1}\omega_n$ n , ω_n n $\mathbb{Z}[a, b, x]$, 1.

Απόδειξη :

1. Λόγω του γνωστού ισομορφισμού ο οποίος παραμετρίζει την ελλειπτική καμπύλη E έχουμε $P = (x, y) = (\wp(z), \wp'(z))$, για κάποιο $z \in \mathbb{C}/L$. Για λόγους απλότητας εγκαταλείπουμε στα παρακάτω την παράμετρο z. Η πρώτη συνιστώσα του σημείου nP είναι:

$$x(nP) = \wp_n = \wp - \frac{f_{n+1}f_{n-1}}{f_n^2} \Rightarrow x(nP) = x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}.$$

Θα υπολογίσουμε και την δεύτερη συνιστώσα, $y(nP)$ του σημείου nP. Εξ ορισμού έχουμε:

$$\omega_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y}$$

Αρα σε συνδιασμό με τον τύπο για το f_{2n} (θεώρημα 1.8) ισχύει:

$$\frac{\omega_n}{\psi_n^3} = \frac{\psi_{2n}}{2\psi_n^4}.$$

Στην συνέχεια θα αποδείξουμε ότι:

$$\wp'(u) = -\frac{\sigma(2u)}{\sigma^4(u)}.$$

Πράγματι, λόγω της σχέσεως $(*)$ της σελίδος 7, ισχύει η σχέση:

$$\frac{\wp(z) - \wp(u)}{z-u} = -\frac{\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2\sigma(u)^2}}{z-u},$$

για κάθε $z \in \mathbb{C}, u \in \mathbb{C} - L$. Επομένως:

$$\wp'(u) = -\lim_{z\to u} \frac{\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2\sigma(u)^2}}{z-u} = (\lim_{z\to u} \frac{\sigma(z-u)}{z-u}) \cdot (\lim_{z\to u} \frac{\sigma(z+u)}{\sigma(z)^2\sigma(u)^2}),$$

εάν βεβαίως υπάρχουν τα όρια. Θα αποδείξουμε ότι πράγματι υπάρχουν. Εχουμε:

$$\lim_{z\to u} \frac{\sigma(z+u)}{\sigma(z)^2\sigma(u)^2} = \frac{\sigma(2u)}{\sigma(u)^4}.$$

Επίσης $\lim_{z\to u} \frac{\sigma(z-u)}{z-u} = 1$, διότι από τον ορισμό της σ-συνάρτησης του Weierstrass, έχουμε:

$$\frac{\sigma(z-u)}{z-u} = \prod_{\omega\in L, \omega\neq 0} (1 - \frac{z-u}{\omega}) \exp(\frac{z-u}{\omega} + \frac{1}{2}(\frac{z-u}{\omega})^2),$$

το οποίο συγκλίνει στο 1, όταν το z τείνει στο u. Αρα ισχύει το ζητούμενο.

Αποδεικνύεται ότι ([Fo], πρόταση 2.3, σελ. 15) :

$$\psi_n(u) = (-1)^{n+1} \frac{\sigma(nu)}{\sigma(u)^{n^2}}.$$

Αρα :

$$\wp'(nu) = -\frac{\sigma(2nu)}{\sigma^4(nu)} = -\frac{\frac{\sigma(2nu)}{\sigma^{(2n)^2}(u)}}{(\frac{\sigma(nu)}{\sigma^{n^2}(u)})^4} = \frac{\psi_{2n}(u)}{\psi_n^4(u)}.$$

Συνεπώς έχουμε :

$$y(nP) = \wp'(nu) = \frac{\psi_{2n}(u)}{\psi_n^4(u)} = \frac{\omega_n}{\psi_n^3}.$$

2. Το $\psi_n = f_n = P_n(\wp)$ για n περιττό είναι πολυώνυμο του $\mathbb{Z}[x,a,b]$, βαθμού $\frac{n^2-1}{2}$ και με συντελεστή του μεγιστοβαθμίου όρου n^2. Τώρα για το φ_n παρατηρούμε ότι αν ο n είναι περιττός τότε οι $n+1$, $n-1$ είναι άρτιοι, και άρα:

$$\psi_{n+1} = \frac{n+1}{2}\wp' P_{n+1}(\wp),$$

όπου το $P_{n+1}(\wp)$ πολυώνυμο βαθμού $\frac{(n+1)^2-4}{2}$ και όμοια :

$$\psi_{n-1} = \frac{n-1}{2}\wp' P_{n-1}(\wp),$$

όπου το P_{n-1} , είναι βαθμού $\frac{(n-1)^2-4}{2}$. Επομένως:

$$\psi_{n+1}\psi_{n-1} = (n^2-1)(\frac{\wp'}{2})^2 P_{n+1}(\wp)P_{n-1}(\wp).$$

Ομως ισχύει ότι:

$$\frac{\wp'}{2} = y^2 = x^3 + ax + b,$$

δηλαδή το $\frac{\wp'}{2}$ είναι πολυώνυμο βαθμού 3 ως προς x και το γινόμενο $P_{n+1}(\wp)P_{n-1}(\wp)$, είναι βαθμού, $\frac{(n+1)^2-4}{2} + \frac{(n-1)^2-4}{2} = n^2-3$. Συνεπώς το γινόμενο $\psi_{n+1}\psi_{n-1}$ είναι πολυώνυμο βαθμού $n^2-3+3 = n^2$ ως προς x. Αρα το φ_n είναι πολυώνυμο βαθμού n^2 και ανήκει προφανώς στον δακτύλιο $\mathbb{Z}[x,a,b]$. Οσον αφορά τώρα τον συντελεστή του μεγιστοβαθμίου όρου του φ_n παρατηρούμε τα εξής : Τα πολυώνυμα ψ_n^2, και $\psi_{n+1}\psi_{n-1}$, έχουν συντελεστές μεγιστοβαθμίου όρου n^2 και n^2-1 αντίστοιχα. Επομένως το πολυώνυμο:

$$\varphi_n(x) = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

έχει συντελεστή μεγιστοβαθμίου όρου $n^2-(n^2-1) = 1$. Κατά εντελώς όμοιο τρόπο δουλεύουμε και για τα $\psi_n/2y$, $y^{-1}\omega_n$, ω_n. □

Τέλος το επόμενο θεώρημα μας δίνει τις ακόλουθες ιδιότητες διαίρεσης του Cassels :

Θεώρημα 1.10 *1.* 2^s 2 n. 2^{2s} $\psi_n^2(x,a,b)$.

2. $n = 2^s$, :

$$2^{-2s}\psi_n^2 = x^{n^2-1} + h(x),$$

$h(x)$ $\mathbb{Z}[x,a,b]$ n^2-1, x.

3. $n = p^s$, p ,

$$g_{p^s}(x) = \frac{\psi^2_{p^s}}{\psi^2_{p^{s-1}}},$$

$\mathbb{Z}[x, a, b]$, p^2 .

Απόδειξη :

1. Εστω ότι ο n είναι περιττός , δηλαδή $s = 0$. Τότε, όπως είδαμε πιο μπροστά, η τιμή της σταθεράς στο $\psi_n(0)$, για $b = 0$, μας δίνει ± 1. Δηλαδή το πολυώνυμο $\psi_n(x, a, b)$ έχει ένα όρο με συντελεστή ± 1 και συνεπώς έχουμε το ζητούμενο.

   Εξετάζουμε τώρα τι γίνεται για n άρτιο. Θέτουμε $n := 2k$, $k \in \mathbb{N}$.

   Επειδή $\psi_2 = 2y$, συνεπάγεται ότι η πρόταση ισχύει για $k = 1$, $n = 2$.

   Συνεχίζουμε επαγωγικά. Εστω ότι ισχύει το ζητούμενο για όλους τους άρτιους μικρότερους του $n = 2k$. Θα αποδείξουμε ότι ο 2^{2s} είναι η μεγαλύτερη δύναμη που διαιρεί το ψ^2_{2k}. Καταρχάς για κάθε k φυσικό, ισχύει $\psi_{2k} = 2\psi_k\omega_k$, διότι

   $$\wp'\psi_{2k} = \psi_k(\psi_{k+2}\psi^2_{k-1} - \psi_{k-2}\psi^2_{k+1}), \text{ λόγω του θεωρήματος 1.8}$$

   $$\text{Επομένως } \psi_{2k} = \frac{1}{\wp'}\psi_\kappa 4y\omega_k = \frac{1}{2y}\psi_k 4y\omega_k, \text{ λόγω του θεωρήματος 1.9}$$

   Δηλαδή:

   $$\psi_{2k} = 2\psi_k\omega_k.$$

   Επομένως:

   $$\psi^2_{2k} = 4\psi^2_k\omega^2_k$$

   Για k περιττό, ο μέγιστος κοινός διαιρέτης των συντελεστών του ψ^2_k, είναι 1. Επιπλέον, λόγω του θεωρήματος 1.9

   $$\omega^2_k = (y^{-1}\omega_k)^2 \cdot y^2 = (y^{-1}\omega_k)^2 \cdot (x^3 + ax + b) \in \mathbb{Z}[x, a, b].$$

   και ο μέγιστος κοινός διαιρέτης των συντελεστών του πολυωνύμου ω^2_k είναι 1. Αρα η μεγαλύτερη δύναμη του 2 που διαιρεί τον μέγιστο κοινό διαιρέτη των συντελεστών του ψ^2_{2k}, για k περιττό είναι $2^2 = 4$, όπως ακριβώς ζητούσαμε.

   Για k άρτιο, ο μέγιστος κοινός διαιρέτης των συντελεστών του πολυωνύμου ω^2_k, είναι 1, λόγω του 3 του θεωρήματος 1.9. Επιπλέον από την υπόθεση της μαθηματικής επαγωγής προκύπτει ότι εάν ο 2^s είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον $n = 2k$, δηλαδή ο 2^{s-1} είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον k, τότε ο $2^{2(s-1)}$ είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον μέγιστο κοινό διαιρέτη των συντελεστών του ψ_k^2. Επομένως ο $2^2 \cdot 2^{2(s-1)}$, είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον μέγιστο κοινό διαιρέτη των συντελεστών του ψ_{2k}^2. Αρα ισχύει το ζητούμενο για κάθε φυσικό αριθμό k, δηλαδή για όλους τους άρτιους $n = 2k, \quad k \in \mathbb{N}$.

2. Αυτό είναι απλή εφαρμογή του θεωρήματος 1.9 για $n = 2^s$.

3. Τέλος έστω $n = p^s$, όπου ο p είναι περιττός πρώτος. Τότε, εξ ορισμού έχουμε:

$$\psi_{p^s}^2(x) = p^{2s} \prod(\wp(z) - \wp(u)), \qquad (x = \wp(z))$$

όπου το γινόμενο διατρέχει όλα τα u που ανήκουν στο $(\mathbb{C}/L)_{p^s}$. Επίσης:

$$\psi_{p^{s-1}}^2(x) = p^{2s-2} \prod(\wp(z) - \wp(u)),$$

οπου το γινόμενο διατρέχει όλα τα u που ανήκουν στο $(\mathbb{C}/L)_{p^{s-1}}$. Αρα διαιρώντας το $\psi_{p^s}^2(x)$, με το $\psi_{p^s-1}^2(x)$, έχουμε

$$g_{p^s}(x) = p^2 \prod(\wp(z) - \wp(u)),$$

όπου το $u \in (\mathbb{C}/L)_{p^s} - (\mathbb{C}/L)_{p^{s-1}}$ και το γινόμενο είναι το πολυώνυμο του $\wp$, $P_n(\wp)$ με συντελεστές από το $\mathbb{Z}$.

Αρα πράγματι το $g_{p^s}(x)$ είναι πολυώνυμο του $\mathbb{Z}[x, a, b]$, με συντελεστή μεγιστοβαθμίου όρου p^2.

Επίσης οι συντελεστές του $g_{p^s}(x)$ είναι πρώτοι μεταξύ τους, διότι ο μέγιστος κοινός διαιρέτης των συντελεστών των πολυωνύμων $\psi_{p^s}(x)$, $\psi_{p^{s-1}}(x)$ είναι 1 (λόγω του 1 του παρόντος θεωρήματος) και επομένως από το Λήμμα του Gauss το ίδιο θα ισχύει και για το πηλίκον τους που είναι το $g_{p^s}(x)$. $\square$

2 Τυπικές ομάδες

Στο κεφάλαιο αυτό R θα συμβολίζει έναν μη-τετριμμένο αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο $1 \in R$.

2.1 Ορισμοί - Ιδιότητες

Ορισμός 2.1 *(,)* $\mathcal{F}$, R, $F(X,Y) \in R[[X,Y]]$, *:*

1. $F(X,Y) = X + Y + G(X,Y)$, $G(X,Y) \in R[[X,Y]]$ *(* X Y *)* 2.
2. $F(X, F(Y,Z)) = F(F(X,Y),Z)$.
3. $F(X,Y) = F(Y,X)$.
4. $i(T) \in R[[T]]$, $F(T, i(T)) = 0$.
5. $F(X,0) = X$, $F(0,Y) = Y$

F $\mathcal{F}$.

Παρατηρήσεις :

1. Κατ' αρχήν ισχύει: $F(0,0) = 0$ (λόγω της ιδιότητας 1 του ορισμού). Συνεπώς οι δυναμοσειρές $F(X,F(Y,Z))$, και $F(F(X,Y),Z)$, της ιδιότητας 2 του ορισμού, είναι καλά ορισμένες τυπικές δυναμοσειρές του δακτυλίου $R[[X,Y,Z]]$.
2. Εστω $\mathcal{M} := XR[[X,Y]]$. Αν $f, g \in \mathcal{M}$, ορίζουμε $(f \circ g)(X) := f(g(X))$. Τότε το ιδεώδες $\mathcal{M}$, γίνεται πολλαπλασιαστική ημιομάδα με πράξη την "$\circ$", και η δυναμοσειρά X είναι το μοναδιαίο στοιχείο της ημιομάδας, δηλαδή $X \circ f = f \circ X = f$. Επομένως εαν $f \circ g = g \circ f = X$, όπου $f, g \in \mathcal{M}$, τότε γράφουμε $f = g^{-1}$ και $g = f^{-1}$.

Λήμμα 2.2 $a \in R^*$ $f(T) \in R[[T]]$, $f(T) = aT + \cdots$, $g(T) \in R[[T]]$ $f(g(T)) = T$. $g(f(T)) = T$.

Απόδειξη : Θα κατασκευάσουμε ακολουθία πολυωνύμων $g_n(T) \in R[T]$, τέτοια ώστε:

$$f(g_n(T)) \equiv T mod T^{n+1}, \text{ και } g_{n+1} \equiv g_n(T) mod T^{n+1}.$$

Θα δείξουμε ότι το όριο $\lim_{n\to\infty} g_n(T)$, υπάρχει και εαν θέσουμε $g(T) := \lim_{n\to\infty} g_n(T)$, προφανώς ισχύει ότι $f(g(T)) = T$. Κάνουμε επαγωγή επί του n. Για $n = 1$, ορίζουμε $g_1(T) := a^{-1}T$. Το $g_1(T)$ επαληθεύει την σχέση $f(g_1(T)) \equiv T mod T^2$. Εστω ότι ισχύει ισχύει η υπόθεση της μαθηματικής επαγωγής, δηλαδή ότι έχουμε κατασκευάσει το στοιχείο $g_{n-1}(T)$. Εξετάζουμε αν υπάρχει $\lambda \in R$, τέτοιο ώστε η $g_n(T) = g_{n-1}(T) + \lambda T^n$, να ικανοποιεί την ζητούμενη ιδιότητα:

$$f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) \equiv f(g_{n-1}(T)) + a\lambda T^n mod T^{n+1} \equiv T + bT^n + a\lambda T^n mod T^{n+1}$$

για κάποιο $b \in R$, λόγω της υπόθεσης της μαθηματικής επαγωγής. Αρκεί λοιπόν να πάρουμε $\lambda := -\frac{b}{a}$, το οποίο είναι στοιχείο του R, διότι $a \in R^*$. Ετσι εξασφαλίζουμε την ύπαρξη δυναμοσειράς $g(T) \in R[[T]]$, τέτοιας ώστε $f(g(T)) = T$. Επιπλέον εφαρμόζοντας το g στο $f(g(T)) = \mathrm{T}$, έχουμε $g(f(g(T))) = g(T)$, το οποίο είναι ταυτότητα στον δακτύλιο $R[[g(T)]]$. Συνεπώς $g(f(T)) = T$.

Τέλος αν υποθέσουμε ότι υπάρχει $h(T) \in R[[T]]$, τέτοιο ώστε $f(h(T)) = T$, τότε:

$$g(T) = g(f(h(T))) = (g \circ f)(h(T)) = h(T),$$

που μας αποδεικνύει την μοναδικότητα του $g(T)$. $\square$

Στην συνέχεια κάνοντας χρήση του λήμματος 2.2 μπορούμε να αποδείξουμε ότι, οι ιδιότητες 1 και 2 του ορισμού, δίνουν τις ιδιότητες 4 και 5. Αποδεικνύουμε την ιδιότητα 4.

Πρόταση 2.3 $F(X,Y) \in R[[X,Y]]$ 1 2 2.1. $i(X) \in R[[X]]$, $F(X,i(X)) = F(i(X),X) = 0$.

<u>Απόδειξη :</u> Θεωρούμε την συναμοσειρά $G(X,Y) := X - F(X,Y)$, που προφανώς δεν έχει σταθερό όρο. Αν θεωρήσουμε την $G(X,Y)$, ως δυναμοσειρά μόνο του Y, με συντελεστές από τον δακτύλιο $R[[X]]$, τότε η δυναμοσειρά $g_X(Y) := G(X,Y) \in (R[[X]])[[Y]]$, είναι της μορφής $g_X(\mathrm{Y}) = aY + \cdots$, όπου $a = -1 \in R[[X]]^*$. Συνεπώς μπορούμε να εφαρμόσουμε το λήμμα 2.2 . Υπάρχει λοιπόν δυναμοσειρά $i_X(Y) \in (R[[X]])[[Y]]$ τέτοια ώστε $g_X(i_X(Y)) = Y$. Ορίζουμε $i(X,Y) := i_X(Y) \in R[[X,Y]]$. Τότε:

$$g_X(i_X(Y)) = G(X, i(X,Y)) = X - F(X, i(X,Y)) \Longrightarrow Y = X - F(X, i(X,Y)).$$

Επομένως στον δακτύλιο $R[[T]]$, όπου T := X = Y έχουμε $0 = F(T, i(T,T))$. Θέτουμε $i(T) := i(T,T)$ και συνεπώς έχουμε αποδείξει την ύπαρξη δυναμοσειράς $i(T) \in R[[T]]$, τέτοιας ώστε $F(T, i(T)) = 0$. Εντελώς όμοια αποδεικνύεται ότι $F(i(T), T) = 0$.

Αποδεικνύουμε τέλος υπάρχει μοναδική δυναμοσειρά $i(T) \in R[[T]]$ τέτοια ώστε $F(T, i(T)) = F(i(T), T) = 0$. Αν υποθέσουμε ότι υπάρχει και δεύτερη δυναμοσειρά $j(T) \in R[[T]]$, τέτοια ώστε $F(j(T), T) = F(T, j(T)) = 0$, τότε:

$$i(T) = F(F(T, j(T)), i(T)) = F(j(T), F(T, i(T))) = j(T).\square$$

<u>Παραδείγματα :</u>

1. Η τυπική προσθετική ομάδα, που συμβολίζεται με $\hat{G}_a$. Δίνεται από τον τυπικό νόμο ομάδας $F(X,Y) = X + Y$.

2. Η τυπική πολλαπλασιαστική ομάδα ,που συμβολίζεται με $\hat{G}_m$. Δίνεται από τον τυπικό νόμο ομάδας $F(X,Y) = X + Y + XY$.

Ορισμός 2.4 $(\mathcal{F}, F)$ $(\mathcal{G}, G)$, R. $\mathcal{F}$ $\mathcal{G}$, $f(T) \in T \cdot R[[T]]$, $f(F(X,Y)) = G(f(X), f(Y))$. $(\mathcal{F}, F)$, $(\mathcal{G}, G)$ $\exists g : \mathcal{G} \to \mathcal{F}$, , $f(g(T)) = g(f(T)) = T$.

Ορισμός 2.5 $(\mathcal{F}, F)$, . :

$$[m] : \mathcal{F} \longrightarrow \mathcal{F}, \qquad m \in \mathbb{Z}, \ :$$

$$[0](T) = 0, \ \ [m+1](T) = F([m](T), T), \ \ [m-1](T) = F([m](T), i(T)).$$

Εύκολα επαληθεύεται (επαγωγικά) ότι είναι ομομορφισμός και λέγεται απεικόνιση πολλαπλασιασμού με m.

Πρόταση 2.6 $\mathcal{F}$ R $m \in \mathbb{Z}$. :

1. $[m](T) = mT + \ (\ )$.

2. $m \in R^*$, m, .

<u>Απόδειξη :</u>

1. Κατ' αρχήν θεωρούμε την περίπτωση όπου $m \geq 0$ και αποδεικνύουμε το ζητούμενο επαγωγικά ως προς m. Πράγματι, για $m = 0$ έχουμε $[0](\mathrm{T}) = 0$. Εστω ότι ισχύει το ζητούμενο για τον φυσικό αριθμό m. Επομένως:

$$[m+1](T) = F([m](T), T) = [m](T) + T + (\text{όροι μεγαλύτερου βαθμού})$$

$$= mT + T + \text{όροι μεγαλύτερου βαθμού } = (m+1)T + (\text{όροι μεγαλύτερου βαθμού}).$$

Δηλαδή ισχύει για κάθε $m \geq 0$. Αν τώρα $m < 0$, τότε χρησιμοποιούμε την ταυτότητα:

$$0 = F(T, i(T)) = T + i(T) + (\text{όροι μεγαλύτερου βαθμού}),$$

από την οποία έπεται ότι $i(T) = -T + (\text{όροι μεγαλύτερου βαθμού})$, και εφαρμόζουμε επαγωγή για το $-m$.

2. Αν $m \in R^*$, τότε το γεγονός ότι ο $[m]$ είναι ισομορφισμός είναι άμεση συνέπεια του 1 και του λήμματος 2.2. □

2.2 Η τυπική ομάδα μιας ελλειπτικής καμπύλης

Εστω μία ελλειπτική καμπύλη E, με εξίσωση Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in R.$$

Κάνουμε τον εξής μετασχηματισμό:

$$z := -\frac{x}{y}, \quad w := -\frac{1}{y}.$$

Δηλαδή $x = z/w$ και $y = -1/w$. Ο μετασχηματισμός αυτός μας μεταφέρει το επ' άπειρο σημείο της καμπύλης E, στην αρχή των αξόνων $(0, 0)$. Η εξίσωση της E σε συντεταγμένες (z, w), είναι:

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 := f(z, w)$$

$$\Longrightarrow w = z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3 = z^3+(a_1z+a_2z^2)[z^3+(a_1z+a_2z^2)w+\cdots]$$

$$= z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6 + \cdots = z^3(1 + A_1z + A_2z^2 + \cdots),$$

όπου $A_n \in \mathbb{Z}[a_1, \cdots, a_6]$. Εκφράσαμε δηλαδή το w ως δυναμοσειρά του z. Θα αποδείξουμε ότι αυτή η δυναμοσειρά συγκλίνει καθώς επίσης ότι $w(z) = f(z, w(z))$.

Ορίζουμε επαγωγικά την εξής ακολουθία πολυωνύμων:

$$f_1(z, w) := f(z, w), \quad f_{m+1}(z, w) := f_m(z, f(z, w)).$$

Τότε παίρνουμε σαν $w(z) := \lim_{m\to\infty} f_m(z, 0)$, και επομένως αρκεί να αποδείξουμε ότι αυτό το όριο έχει νόημα στον δακτύλιο $\mathbb{Z}[a_1, a_2, \cdots, a_6][[z]]$.

Πρόταση 2.7 *1.* *:*

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbb{Z}[a_1, a_2, \cdots, a_6][[z]]$$

2. $w(z)$, $w(z) = f(z, w(z))$.

Για την απόδειξη της παραπάνω πρότασης, χρειαζόμαστε το Λήμμα του Hensel (σε μία πιο γενική μορφή)

Λήμμα 2.8 R I, $F(w) \in R[w]$. $a \in R$, ($n \geq 1$), $F(a) \in I^n$ $F'(a) \in R^*$. $\alpha \in R$, $\alpha \equiv F'(a) mod I$, *:*

$$w_0 = a, w_{m+1} = w_m - \frac{F(w_m)}{\alpha}$$

$b \in R$, *:*

$$F(b) = 0 \qquad b \equiv a mod I^n.$$

R b.

Απόδειξη : [Αν 1] (Στην πραγματικότητα πρόκειται για μια από τις μορφές του αλγόριθμου του Newton). □

Προχωρούμε τώρα στην απόδειξη της πρότασης 2.7:

Απόδειξη της πρότασης 2.7 : Εφαρμόζουμε το λήμμα 2.8 για $R := \mathbb{Z}[a_1, a_2, \cdots, a_6][[z]]$, $I := (z)$, $a := 0$, $\alpha := -1$ και $F(w) =: f(z, w) - w$. Πράγματι :

$$F(0) = f(z, 0) - 0 = f(z, 0) \in I^3$$

$$F'(0) = f'(z, w)|_{w=0} - 1 = -1 + a_2 z + \cdots,$$

που προφανώς είναι μονάδα του R. Επίσης:

$$w_0 = a = 0, w_{m+1} = w_m - \frac{F(w_m)}{\alpha} = w_m + F(w_m)$$

$$\Longrightarrow F(w_0) = F(a) = F(0) = f(z, 0),$$

$$F(w_m) = f(z, w_m) - w_m \Longrightarrow F(w_m) + w_m = f(z, w_m) = f(z, f_m(z, 0)) = w_{m+1} \square$$

Εκφράζουμε τα x, y ως δυναμοσειρές του z :

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \cdots,$$

$$y(z) = \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + \cdots,$$

όπου οι συντελεστές των αναπτυγμάτων Laurent των $x(z), y(z)$ έχουν συντελεστές από τον δακτύλιο $\mathbb{Z}[a_1, a_2, \cdots, a_6]$.

Το ζευγάρι $(x(z), y(z),)$ μας δίνει μία " τυπική " λύση της εξίσωσης του Weierstrass, η οποία ανήκει στο σώμα πηλίκων του δακτυλίου των τυπικών δυναμοσειρών. Θα μπορούσαμε να προσπαθήσουμε να " παράγουμε " σημεία της ελλειπτικής καμπύλης E/K, παίρνοντας ένα στοιχείο $z \in K$ και κοιτάζοντας το ζευγάρι $(x(z), y(z))$. Επειδή όμως οι $x(z)$, $y(z)$ είναι άπειρες σειρές δεν έχουν πάντα νόημα. Οταν όμως το σώμα K είναι πλήρες τοπικό σώμα, ως πρός μία διακριτή εκτίμηση υ, με δακτύλιο ακεραίων R, μέγιστο ιδεώδες $\mathcal{M}$ και οι συντελεστές της εξίσωσης του Weierstrass της E, a_i, είναι στοιχεία του δακτυλίου R, τότε οι δυναμοσειρές $x(z), y(z)$ αποκτούν νόημα και συγκλίνουν δίνοντας σημείο $(x(z), y(z))$ της ελλειπτικής καμπύλης E. Ετσι λοιπόν κατασκευάζεται κατά φυσιολογικό τρόπο η εμφύτευση:

$$\mathcal{M} \overset{\varphi}{\hookrightarrow} E(K).$$

Η εικόνα της απεικόνισης φ, είναι όλα τα σημεία $(x, y) \in E(K)$, τέτοια ώστε $xy^{-1} \in \mathcal{M}$.

Εστω z_1, z_2 ανεξάρτητες μεταβλητές και $w_i := w(z_i)$, για $i = 1, 2$. Τότε στο (w, z)-επίπεδο η ευθεία που συνδέει τα ("τυπικά ") σημεία (w_1, z_1), (w_2, z_2) έχει κλίση:

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, a_2, \cdots, a_6][[z_1, z_2]].$$

Σημειώνουμε μάλιστα ότι το λ δεν έχει ούτε σταθερό, ούτε πρωτοβάθμιο όρο. Επίσης ορίζουμε:

$$\nu := \nu(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, a_2, \cdots, a_6][[z_1, z_2]].$$

Τότε η ευθεία που περνά από τα σημεία (w_1, z_1), (w_2, z_2) έχει εξίσωση $w = \lambda z + \nu$. Αντικαθιστώντας στην εξίσωση του Weierstrass, παίρνουμε ένα κυβικό πολυώνυμο ως πρός z, που έχει ως ρίζες του τα z_1, z_2. Εστω z_3, η τρίτη του ρίζα. Τότε το z_3 μπορεί να εκφραστεί ως δυναμοσειρά των z_1, z_2 :

$$z_3 = z_3(z_1, z_2) = -z_1 - z_2 + \frac{a_1\lambda + a_3\lambda^2 - a_2\nu - 2a_4\lambda\nu - 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3},$$

το οποίο ανήκει στον δακτύλιο των τυπικών δυναμοσειρών $\mathbb{Z}[a_1, a_2, \cdots, a_6][[z_1, z_2]]$. Επιπλέον λόγω του νόμου ομάδος της ελλειπτικής καμπύλης E, τα σημεία (w_i, z_i), $i = 1, 2, 3$ αθροίζονται στο επ' άπειρο σημείο της καμπύλης O. Στο (x, y)-επίπεδο το αντίθετο του σημείου (x, y), είναι το σημείο $(x, -y - a_1x - a_3)$. Συνεπώς το αντίθετο του σημείου (z, w), θα έχει z-συντεταγμένη ($z = -x/y$):

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, a_2, \cdots, a_6][[z]].$$

Αυτή η σχέση μας δίνει τον τυπικό νόμο ομάδας:

$$F(z_1, z_2) = i(z_3(z_1, z_2)) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - \cdots \in \mathbb{Z}[a_1, a_2, \cdots, a_6][[z_1, z_2]],$$

και επαληθεύει τις ιδιότητες ορισμού της τυπικής ομάδας.

2.3 Ομάδες επισυναπτόμενες σε τυπικές ομάδες

Μία τυπική ομάδα, είναι απλά ένας νόμος ομάδας. Αν όμως ο δακτύλιος R είναι τοπικός και πλήρης δακτύλιος, και εαν οι μεταβλητές παίρνουν τιμές από το μοναδικό μέγιστο ιδεώδες του R, τότε η δυναμοσειρά ορισμού της τυπικής ομάδας, συγκλίνει. Στα επόμενα θα είναι:

R πλήρης τοπικός δακτύλιος,

$\mathcal{M}$ το μέγιστο ιδεώδες του R,

$\tilde{K}$ το σώμα πηλίκων $R/\mathcal{M}$,

$\mathcal{F}$ μία τυπική ομάδα ορισμένη στον R, με τυπικό νόμο ομάδας $F(X, Y)$.

Ορισμός 2.9 $\mathcal{F}/R$, $\mathcal{M}$, :

$$x \oplus_{\mathcal{F}} y = F(x, y), \quad x, y \in \mathcal{M}$$

:

$$\ominus_{\mathcal{F}} x = i(x), \quad x, y \in \mathcal{M}.$$

$\mathcal{F}(\mathcal{M})$.

Καθ' όμοιο τρόπο, αν $m \geq 1$, ορίζουμε την υποομάδα της $\mathcal{F}(\mathcal{M})$, $\mathcal{F}(\mathcal{M}^n)$, της οποίας το σύνολο ορισμού είναι το $\mathcal{M}^n$.

Παρατήρηση : Το γεγονός ότι ο R είναι πλήρης τοπικός δακτύλιος συνεπάγεται ότι οι δυναμοσειρές $F(x, y)$ και $i(x)$, συγκλίνουν όταν $x, y \in \mathcal{M}$. Επομένως τα αξιώματα ορισμού της τυπικής ομάδος δίνουν δομή ομάδος στην $\mathcal{F}(\mathcal{M})$, και δομή υποομάδος στην $\mathcal{F}(\mathcal{M}^n)$.

Παραδείγματα :

1. Η προσθετική ομάδα $\hat{G}_a(\mathcal{M})$, είναι το σύνολο $(\mathcal{M}, +)$ εφοδιασμένο με την συνηθισμένη πράξη πρόσθεσης στο $\mathcal{M}$. Επομένως η παρακάτω ακολουθία προσθετικών ομάδων είναι ακριβής:

$$0 \longrightarrow \hat{G}_a(\mathcal{M}) \longrightarrow R \longrightarrow \tilde{K} \longrightarrow 0$$

2. Η πολλαπλασιαστική ομάδα $\hat{G}_m(\mathcal{M})$, είναι η ομάδα των 1-μονάδων ($1 + \mathcal{M}$), με την συνηθισμένη πράξη πολλαπλασιασμού. Ομοια λοιπόν έχουμε την παρακάτω μικρή ακριβή ακολουθία πολλαπλασιαστικών ομάδων:

$$0 \longrightarrow \hat{G}_m(\mathcal{M}) \longrightarrow R^* \longrightarrow \tilde{K}^* \longrightarrow 0$$

3. Εστω $\hat{E}$, η τυπική ομάδα της ελλειπτικής καμπύλης E/K, όπου K είναι το σώμα πηλίκων του δακτυλίου R. Οπως γνωρίζουμε οι δυναμοσειρές $x(z), y(z)$, ορίζουν την απεικόνιση:

$$\mathcal{M} \longrightarrow E(K)$$

$$z \mapsto (x(z), y(z))$$

η οποία επάγει ομομορφισμό της ομάδων της $\hat{E}(\mathcal{M})$ στην $E(K)$. Αποδεικνύεται μάλιστα ότι η παρακάτω ακαλουθία είναι ακριβής:

$$0 \longrightarrow \hat{E}(\mathcal{M}) \longrightarrow E(K) \longrightarrow \tilde{E}(\tilde{K}) \longrightarrow 0$$

αν η καμπύλη $\tilde{E}$, όπου εξ ορισμού είναι η E modulo $\mathcal{M}$, είναι μη-ιδιόμορφη. Στην γλώσσα της θεωρίας αναγωγής στην οποία θα αναφερθούμε εκτενώς στο επόμενο κεφάλαιο, το γεγονός αυτό σημαίνει ότι η $\hat{E}(\mathcal{M})$ είναι ο πυρήνας της απεικόνισης αναγωγής.

Πρόταση 2.10 *1.* $n \geq 1$, *:*

$$\mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1}) \longrightarrow \mathcal{M}^n/\mathcal{M}^{n+1}$$

, .

2. p $\tilde{K}$*.* $\mathcal{F}(\mathcal{M})$ p*.*

Απόδειξη :

1. Αφού τα αντίστοιχα σύνολα είναι ίσα, αρκεί να αποδείξουμε ότι η παραπάνω απεικόνιση είναι μορφισμός ομάδων. Ας πάρουμε στοιχεία $x, y \in \mathcal{M}^n$. Τότε:

   $$x \oplus_{\mathcal{F}} y = F(x,y) = x + y + \cdots \equiv x + y \ \ mod \mathcal{M}^{n+1},$$

   που αποδεικνύει το ζητούμενο.

2. Ας πάρουμε στοιχείο $x \in \mathcal{F}(\mathcal{M})$, τάξης $m \in \mathbb{N}$. Αν πολλαπλασιάσουμε το x με κατάλληλη δύναμη του p, είναι φανερό ότι αρκεί να αποδείξουμε ότι δεν υπάρχουν μη-μηδενικά σημεία πεπερασμένης τάξης, με τάξη πρώτη προς τον p. Κατ' αρχήν ο δακτύλιος R είναι δακτύλιος της Noether. Θα αποδείξουμε επαγωγικά ότι $x \in \mathcal{F}(\mathcal{M}^n)$, για κάθε φυσικό αριθμό n και επομένως, λογω του θεωρήματος του Krull ([B-I-V], σελ. 65) έπεται ότι $x = 0$. Εξ υποθέσεως $x \in \mathcal{F}(\mathcal{M})$. Αρα η ισχύει το ζητούμενο για $n = 1$. Εστω ότι $x \in \mathcal{F}(\mathcal{M}^n)$. Η εικόνα του x, $\bar{x} \in \mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1})$, έχει τάξη που διαιρείται από τον m. Από την άλλη πλευρά όμως η ομάδα $\mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1})$ έχει σημεία που η τάξη τους διαιρείται μόνο με p, διότι είναι ισόμορφη με την ομάδα $\mathcal{M}^n/\mathcal{M}^{n+1}$. Επομένως $\bar{x} = 0$, δηλαδή $x \in \mathcal{F}(\mathcal{M}^{n+1})$. Αρα $x \in \mathcal{F}(\mathcal{M}^n)$ για κάθε φυσικό αριθμό n.

   $\square$

3 Ελλειπτικές καμπύλες ορισμένες σε τοπικά σώματα

Σε αυτό το κεφάλαιο θα μελετήσουμε την ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης E ορισμένης σε τοπικό σώμα αριθμών με κύριο σκοπό την εξαγωγή συμπερασμάτων για τις ιδιότητες των σημείων πεπερασμένης τάξης της E. Στα παρακάτω θα κρατήσουμε τον ακόλουθο συμβολισμό:

K_υ : τοπικό σώμα αριθμών πλήρες ως προς μια διακριτή εκτίμηση υ,

R : ο δακτύλιος των ακεραίων του K_υ, $R = \{x \in K_\upsilon / \upsilon(x) \geq 0\}$,

R^* : η ομάδα των μονάδων του R, $R^* = \{x \in K_\upsilon / \upsilon(x) = 0\}$,

P_υ : το μέγιστο ιδεώδες του R, $P_\upsilon = \{x \in K_\upsilon / \upsilon(x) > 0\}$,

π : ο γεννήτορας του P_υ, $P_\upsilon = \pi R$,

$\tilde{K}_\upsilon$: το σώμα υπολοίπων του R, $\tilde{K}_\upsilon = R/P_\upsilon$.

Επίσης υποθέτουμε ότι η εκτίμηση υ είναι κανονικοποιημένη, δηλαδή $\upsilon(\pi) = 1$. Κάνουμε μάλιστα την σύμβαση $\upsilon(0) = \infty$. Τέλος υποθέτουμε ότι τα K_υ και $\tilde{K}_\upsilon$ είναι τέλεια σώματα (δηλαδή κάθε αλγεβρική τους επέκταση είναι διαχωρίσιμη).

3.1 Ελάχιστα μοντέλα του Weierstrass

Εστω E ελλειπτική καμπύλη ορισμένη στο σώμα K_υ, και έστω:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

μιά εξίσωση του Weierstrass για την E. Κάνουμε τον μετασχηματισμό:

$$(X, Y) \mapsto (u^{-2}X, u^{-3}Y), \quad (u \in K_\upsilon^*)$$

που μας δίνει εξίσωση του Weierstrass με συντελεστές $u^i a_i$ ($a_i \mapsto u^i a_i$). Συνεπώς διαλέγοντας $u \in K_\upsilon^*$ που να διαιρείται από αρκετά μεγάλη δύναμη του π καταλήγουμε σε εξίσωση του Weierstrass με συντελεστές στον δακτύλιο R. Τότε όμως $\upsilon(\Delta) \geq 0$ και εφ' όσον η υ είναι διακριτή εκτίμηση μπορούμε να αναζητήσουμε μοντέλο ελλειπτικής καμπύλης E με διακρίνουσα $\upsilon(\Delta)$ "όσο το δυνατό μικρή".

Ορισμός 3.1 *E/K_υ . Weierstrass E υ $\upsilon(\Delta)$ $a_1, a_2, a_3, a_4, a_6 \in R$.*

Πώς μπορούμε όμως να ελέγξουμε αν μια δοσμένη εξίσωση του Weierstrass είναι ελάχιστη; Καταρχήν όλα τα a_i πρέπει να ανήκουν στον δακτύλιο R και ειδικότερα $\Delta \in R$. Αν η εξίσωση δεν είναι ελάχιστη, τότε υπάρχει αμφίρητη αλλαγή συντεταγμένων που δίνει διακρίνουσα $\Delta' = u^{-12}\Delta \in R$. Βλέπουμε λοιπόν ότι η διακρίνουσα αλλάζει μόνο κατά βήματα του 12. Συνεπώς αν $a_i \in R$ και $\upsilon(\Delta)$ μικρότερο του 12 τότε η εξίσωση είναι ελάχιστη. Ομοίως αφού $c_4' = u^4 c_4$ και $c_6' = u^6 c_6$, έχουμε ότι εάν $a_i \in R$ και c_4 μικρότερο του 4, c_6 μικρότερο του 6, τότε η εξίσωση είναι ελάχιστη. Μάλιστα εάν η χαρακτηριστική του σώματος K_υ είναι διαφορετική των 2 και 3 τότε ισχύει και το αντίστροφο. Σημειώνουμε επίσης ότι για τυχόν τοπικό σώμα K_υ υπάρχει ένας αλγόριθμος του Tate ([Ta]), που μας προσδιορίζει αν μια εξίσωση του Weierstrass είναι ελάχιστη.

Παράδειγμα : Εστω η ελλειπτική καμπύλη:

$$E : Y^2 + XY = X^3 + 1$$

Υπολογίζουμε: $c_4 = b_2^2 - 24b_4$, $b_2 = a_1^2 + 4a_2 = 1$, $b_4 = 2a_4 + a_1a_3 = 0$ και άρα $c_4 = 1$. Συνεπώς για κάθε θέση υ ισχύει $\upsilon(c_4) = \upsilon(1) = 0$, το οποίο είναι μικρότερο του 4. Αρα η εξίσωση της E είναι ελάχιστη.

Πρόταση 3.2 *1.* E/K_υ *Weierstrass.*

2. *Weierstrass ,* *:*

$$x = u^2x' + r \quad y = u^3y' + u^2sx' + t,$$

$u \in R^*$ $r, s, t \in R$.

Απόδειξη :

1. Είναι προφανές ότι πάντα μπορούμε να βρούμε μία εξίσωση του Weierstrass με $a_i \in R$ και $\upsilon(\Delta)$, όσο το δυνατόν μικρό, διότι η εκτίμηση υ είναι διακριτή.

2. Εστω ότι η δοσμένη εξίσωση είναι σε ελάχιστη μορφή και έστω ότι και η καμπύλη που προκύπτει από την αρχική, μέσω αλλαγής συντεταγμένων, είναι επίσης ελάχιστη. Τότε $\upsilon(\Delta) = \upsilon(\Delta')$. Ομως $\Delta = u^{12}\Delta'$ και επομένως $u \in R^*$. Επίσης λόγω της σχέσης (Κεφ. 1, σελ. 2) που μας εκφράζει το b_6' συναρτήσει του b_6 (αντίστοιχα το b_8' συναρτήσει του

b_8), βλέπουμε ότι το $4r^3$ (αντίστοιχα $3r^4$), ανήκει στον δακτύλιο R. Συνεπώς $r \in R$. Ομοια η σχέση που εκφράζει το a_2', συναρτήσει του a_2 μας δίνει ότι $s \in R$ και τέλος η σχέση που εκφράζει το a_6', συναρτήσει του a_6 μας δίνει ότι $t \in R$. □

3.2 Αναγωγή modulo π

Θεωρούμε την φυσική προβολή:

$$R \longrightarrow R/\pi R$$

$$t \mapsto \tilde{t} = t + \pi R$$

Εχοντας λοιπόν μια ελλειπτική καμπύλη E με συντελεστές από τον δακτύλιο R, μπορούμε να ανάγουμε τους συντελεστές της modulo π. Η καμπύλη που προκύπτει $\tilde{E}$ είναι ορισμένη στο σώμα $\tilde{K}_\upsilon$ και λέγεται η ανηγμένη της αρχικής modulo π. Η ανηγμένη καμπύλη είναι πιθανόν να έχει ιδιομορφίες.

Ορισμός 3.3 *1.* E *(stable)* K_υ $\tilde{E}$ -.

2. E *(semistable)* K_υ $\tilde{E}$ *( ).* *(split multiplicative),* - K_υ .

3. E *(unstable)* K_υ $\tilde{E}$ *( )*

Εστω τώρα $P \in E(K_\upsilon)$. Τότε μπορούμε να βρούμε ομογενείς συντεταγμένες $P = [x_0, y_0, z_0]$, $x_0, y_0, z_0 \in R$, τέτοιες ώστε τουλάχιστο ένα από από τα x_0, y_0, z_0 να ανήκει στο R^*. Συνεπώς το αναγόμενο σημείο $\tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$, ανήκει στην $\tilde{E}(\tilde{K}_\upsilon)$. Ορίζουμε δηλαδή την απεικόνιση αναγωγής:

$$E(K_\upsilon) \longrightarrow \tilde{E}(\tilde{K}_\upsilon)$$

$$P \mapsto \tilde{P}$$

Σημειώνουμε δε ότι η ανηγμένη καμπύλη $\tilde{E}$ μπορεί να είναι ιδιόμορφη. Γνωρίζουμε όμως ότι σε κάθε περίπτωση το σύνολο των μη-ιδιόμορφων σημείων της που το συμβολίζουμε $\tilde{E}_{ns}(\tilde{K}_\upsilon)$ αποτελεί ομάδα ([Si 1], πρόταση 2.5) Ορίζουμε τα εξής υποσύνολα της $E(K_\upsilon)$:

$$E^{(0)}(K_\upsilon) := \{P \in E(K_\upsilon) / \tilde{P} \in \tilde{E}_{ns}(\tilde{K}_\upsilon)\}$$

$$E^{(1)}(K_\upsilon) := \{P \in E(K_\upsilon) / \tilde{P} = \tilde{O}\}.$$

Από τον ορισμό της η $E^{(0)}(K_\upsilon)$ είναι το σύνολο των σημείων της E με μη-ιδιόμορφη αναγωγή ενώ η $E^{(1)}(K_\upsilon)$ είναι ο πυρήνας της απεικόνισης αναγωγής.

Πρόταση 3.4 :

$$0 \longrightarrow E^{(1)}(K_\upsilon) \longrightarrow E^{(0)}(K_\upsilon) \longrightarrow \tilde{E}_{ns}(\tilde{K}_\upsilon) \longrightarrow 0,$$

modulo π.

Απόδειξη : Ο νόμος ομάδος, τόσο στην $E(K_\upsilon)$, όσο και στην $\tilde{E}_{ns}(\tilde{K}_\upsilon)$, ορίζεται, παίρνοντας την τομή της καμπύλης με ευθείες του προβολικού επιπέδου, P^2. Επειδή η απεικόνιση αναγωγής $P^2(K_\upsilon) \to P^2(\tilde{K}_\upsilon)$ απεικονίζει ευθείες σε ευθείες, συνεπάγεται ότι η $E^{(0)}(K_\upsilon)$ είναι ομάδα και η απεικόνιση $E^{(0)}(K_\upsilon) \to \tilde{E}_{ns}(\tilde{K}_\upsilon)$, είναι ομομορφισμός ομάδων. Επιπλέον η $E^{(1)}(K_\upsilon)$, είναι ομάδα, διότι είναι ο πυρήνας της απεικόνισης αναγωγής. Προφανώς $E^{(1)}(K_\upsilon) \subseteq E^{(0)}(K_\upsilon)$ (διότι το $\tilde{O}$ δεν είναι ιδιόμορφο σημείο της $\tilde{E}$). Επομένως έχουμε ακρίβεια στην πρώτη θέση. Επίσης η ακρίβεια στην δεύτερη θέση προκύπτει από το γεγονός ότι η $E^{(1)}(K_\upsilon)$ είναι ο πυρήνας της απεικόνισης αναγωγής. Μένει λοιπόν να αποδείξουμε την ακρίβεια στην τελευταία θέση, δηλαδή ότι η απεικόνιση αναγωγής $E^{(0)}(K_\upsilon) \longrightarrow \tilde{E}_{ns}(\tilde{K}_\upsilon)$ είναι επί, γεγονός που θα προκύψει από το λήμμα του Hensel και από την πληρότητα του σώματος K_υ.

Εστω $f(x,y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ και $\tilde{f}(x,y)$ το αντίστοιχο πολυώνυμο ανηγμένο modulo π. Δοθέντος σημείου $\tilde{P} = (\alpha, \beta) \in \tilde{E}_{ns}(\tilde{K}_\upsilon)$, έχουμε ότι $\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$, είτε $\frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0$. Υποθέτουμε, χωρίς περιορισμό της γενικότητας, ότι ισχύει $\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$. Διαλέγουμε $y_0 \in R$ τέτοιο ώστε $\tilde{y}_0 = \beta$ και εξετάζουμε την εξίσωση $f(x, y_0)$. Κάνοντας αναγωγή modulo π παρατηρούμε ότι η ανηγμένη εξίσωση έχει το α ως απλή ρίζα, διότι η μερική παράγωγος της $\tilde{f}$ ως προς x στο σημείο $(\alpha, \tilde{y}_0)$ δεν είναι 0. Αρα από το λήμμα του Hensel $\exists x_0 \in R$ τέτοιο ώστε $\tilde{x}_0 = \alpha$ και $f(x_0, y_0) = 0$. Αρα το σημείο $P = (x_0, y_0) \in E^{(0)}(K_\upsilon)$ ανάγεται στο $\tilde{P}$. □

3.3 π - αδικά φίλτρα

Εστω $E : Y^2 = X^3 + AX + B$ ελλειπτική καμπύλη, με συντελεστές από το σώμα K_υ. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $A, B \in R$. Σκοπός αυτής της παραγράφου είναι η μελέτη του πυρήνα της απεικόνισης αναγωγής.

Ο πυρήνας της απεικόνισης αναγωγής είναι το σύνολο των σημείων της E που απεικονίζονται στο $\tilde{O}$, δηλαδή είναι το σημείο O μαζί με τα σημεία $(x, y) \in E(K_\upsilon)$ τέτοια ώστε $x, y \notin R$. Πράγματι αν ένα από τα x, y ανήκει στον R τότε και τα δύο θα ανήκουν στον R. Συνεπώς γράφοντας το $P = (x, y)$ σε ομογενείς συντεταγμένες $P = [x, y, 1]$ όπου $x, y \in R$ και ανάγοντας το σημείο P modulo π παίρνουμε $\tilde{P} = [\tilde{x}, \tilde{y}, 1] \neq \tilde{O}$, δηλαδή καταλήγουμε σε άτοπο.

Αν $x, y \notin R$ (δηλαδή το σημείο $P = (x, y)$ ανήκει στον πυρήνα της απεικόνισης αναγωγής), τότε η ultrametric ανισότητα δίνει $\|y\|^2 = \|x\|^3$ (όπου η $\|\cdot\|$ είναι η μετρική που προκύπτει από την εκτίμηση υ). Επομένως $\|x\| = c^{2n}$, $\|y\| = c^{3n}$, όπου $c \geq 1$, και n φυσικός αριθμός. Αυτόν τον φυσικό αριθμό n τον ονομάζουμε επίπεδο αναγωγής του σημείου $P = (x, y)$.

Η ακόλουθη πρόταση συνδέει την θεωρία αναγωγής, με την θεωρία των τυπικών ομάδων ελλειπτικών καμπύλων:

Πρόταση 3.5 *E/K_υ Weierstrass. $\hat{E}/R$ E $w(z) \in R[[z]]$ (. 2, . 22). :*

$$\hat{E}(\pi R) \longrightarrow E^{(1)}(K_\upsilon)$$
$$z \mapsto (\frac{z}{w(z)}, -\frac{1}{w(z)})$$

($z = 0$ ’ O).

Απόδειξη : Από την θεωρία των τυπικών ομάδων ελλειπτικών καμπύλων (Κεφάλαιο 2) γνωρίζουμε ότι το σημείο $(z/w(z), -1/w(z))$, ικανοποιεί την εξίσωση της καμπύλης E. Επίσης η δυναμοσειρά $w(z) = z^3(1 + \cdots)$, συγκλίνει $\forall z \in \pi R$. Επομένως το σημείο $(z/w(z), -1/w(z))$ ανήκει στην ομάδα $E(K_\upsilon)$ όταν $z \in \pi R$, και εφόσον $\upsilon(-1/w(z)) = -3\upsilon(z)$, το εν λόγω σημείο ανήκει στην ομάδα $E^{(1)}(K_\upsilon)$. Αρα η απεικόνιση:

$$\hat{E}(\pi R) \longrightarrow E^{(1)}(K_\upsilon)$$
$$z \mapsto (\frac{z}{w(z)}, -\frac{1}{w(z)}),$$

είναι καλώς ορισμένη. Επιπλέον αφού ο τυπικός νόμος ομάδας στην $\hat{E}$ προκύπτει από τον νόμο ομάδας της καμπύλης E, είναι προφανές ότι η παραπάνω απεικόνιση είναι ομομορφισμός. Είναι δε και μονομορφισμός, διότι $w(z) = 0$, μόνο όταν $z = 0$. Απομένει λοιπόν να αποδείξουμε ότι είναι επί.

Εστω σημείο $(x,y) \in E^{(1)}(K_\upsilon)$. Συνεπώς το (x,y) ανάγεται modulo π στο απ' άπειρο σημείο της καμπύλης $\tilde{E}$ και άρα $\upsilon(x) < 0$, $\upsilon(y) < 0$ και $3\upsilon(x) = 2\upsilon(y) = -6n$, όπου n το επίπεδο του σημείου (x,y). Επομένως $x/y \in \pi R$, δηλαδή η απεικόνιση:

$$E^{(1)}(K_\upsilon) \longrightarrow \hat{E}(\pi R)$$

$$(x,y) \mapsto -\frac{x}{y}$$

είναι καλώς ορισμένη. Μάλιστα είναι μονομορφισμός (με το ίδιο ακριβώς σκεπτικό όπως και προηγουμένως). Δηλαδή οι απεικονίσεις:

$$\hat{E}(\pi R) \longrightarrow E^{(1)}(K_\upsilon) \longrightarrow \hat{E}(\pi R)$$

είναι μονομορφισμοί, και η σύνθεσή τους είναι η ταυτότητα. Αρα είναι ισομορφισμοί. □

Εστω τώρα $N \geq 1$. Θεωρούμε τον μετασχηματισμό:

$$X_N = \pi^{2N}X, Y_N = \pi^{3N}Y.$$

Η εξίσωση της καμπύλης μετασχηματίζεται ως εξής:

$$E_N : Y_N^2 = X_N^3 + \pi^{4N}AX_N + \pi^{6N}B.$$

Κάνουμε αναγωγή modulo π και καταλήγουμε στην ιδιόμορφη καμπύλη:

$$\tilde{E}_N : Y_N^2 = X_N^3.$$

Παρατηρούμε ότι αν ένα σημείο $P = (x,y) \in E(K_\upsilon)$ απεικονίζεται στο ιδιόμορφο σημείο $(\tilde{0},\tilde{0})$ ανν το επίπεδό του είναι μικρότερο του N. Πράγματι το σημείο (x,y) απεικονίζεται στο $(\tilde{0},\tilde{0})$ ανν $\pi | x_N, y_N$, δηλαδή ανν $x_N = u\pi^{2k}, y_N = u'\pi^{3k}$, όπου $u,u' \in R^*$ και $k \geq 1$ φυσικός αριθμός. Ισοδύναμα τότε, $x\pi^{2N} = u\pi^{2k}, y\pi^{3N} = u'\pi^{3k}$ και αυτό συμβαίνει τότε και μόνο τότε όταν $x = u\pi^{2(k-N)}, y = u'\pi^{3(k-N)}$. Ομως $x,y \notin R$ και άρα το k είναι αυστηρά μικρότερο του N.

Επίσης αν το σημείο $P = (x,y)$ ανήκει στον πυρήνα της απεικόνισης αναγωγής τότε το επίπεδό του είναι μεγαλύτερο του N (η απόδειξη γίνεται κατά όμοιο τρόπο).

Τέλος αποδεικνύεται ότι η ομάδα των μη ιδιόμορφων σημείων της καμπύλης $\tilde{E}_N$ είναι η προσθετική ομάδα του σώματος $\tilde{K_\upsilon} \cong \frac{R}{\pi R}$ ([Si 1], πρόταση 2.5)

Θεώρημα 3.6 $E^{(N)}$ E N, $E^{(N)}$:

$$E \supset E^{(0)} \supset E^{(1)} \supset \cdots \supset E^{(N)} \supset \cdots$$

$E^{(N)}/E^{(N+1)}$ $N \geq 1$ p.

<u>Απόδειξη :</u> Κατ' αρχήν οι εγκλεισμοί είναι προφανείς. Αποδεικνύουμε τώρα ότι οι $E^{(N)}$ είναι ομάδες.

Κάνουμε τον μετασχηματισμό $t = \frac{x}{y}$, $s = \frac{1}{y}$ που μας μεταφέρει το επ' άπειρο σημείο O στην αρχή των αξόνων $(0,0)$.

Στις νέες συντεταγμένες τα σύνολα $E^{(N)}$ μπορούν να χαρακτηριστούν ως το σύνολα των ζευγών (s,t) τέτοια ώστε $\pi^N|t$, $\pi^{3N}|s$, διότι αν $x = u\pi^{-2N}$, $y = u'\pi^{-3N}$, όπου $u, u' \in R^*$, τότε $t = \frac{u}{u'}\pi^N$ και $s = \frac{1}{u'}\pi^{3N}$.

Η εξίσωση της καμπύλης E σε συντεταγμένες (s,t), είναι:

$$s = t^3 + As^2t + Bs^3.$$

Αν $P_1 = (t_1, s_1)$, $P_2 = (t_2, s_2)$ είναι σημεία της νέας καμπύλης, τότε:

$$s_2 - s_1 = (t_2^3 - t_1^3) + A(s_2^2 t_2 - s_1^2 t_1) + B(s_2^3 - s_1^3).$$

Αν λοιπόν $t_1 \neq t_2$, τότε η κλίση της ευθείας $s = at + \beta$, $\quad a = \frac{s_2 - s_1}{t_2 - t_1}$, που διέρχεται από τα σημεία P_1, P_2, είναι

$$a = (t_1^2 + t_1t_2 + t_2^2) + As_2^2 + At_1(s_2 + s_1)a + Ba(s_2^2 + s_1s_2 + s_1^2)$$

$$\Longrightarrow a = \frac{t_2^2 + t_1t_2 + t_1^2 + As_2^2}{1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1s_2 + s_1^2)}$$

και άρα $\pi^{2N}|a$.

Αν $P_3 = (t_3, s_3)$ είναι το τρίτο σημείο τομής της ευθείας $s = at + \beta$, με την καμπύλη E, τότε τα t_1, t_2, t_3 είναι οι λύσεις της εξίσωσης:

$$at + \beta = t^3 + A(at+\beta)^2 t + B(at+\beta)^3 \Longrightarrow 0 = t^3(1 + Ba^3 + Aa^2) + t^2(2Aa\beta + 3Ba^2\beta) + \cdots$$

$$\Longrightarrow t_1 + t_2 + t_3 = -\frac{2Aa\beta + 3Ba^2\beta}{1 + Ba^3 + Aa^2}.$$

Ο παρονομαστής του κλάσματος ανήκει προφανώς στον R^* (διότι $a, A, B \in R$). Επίσης αφού $\beta = s_1 - at_1$ συνεπάγεται ότι $\pi^{3N}|\beta$ συνεπώς $\pi^{5N}|t_1 + t_2 + t_3$.

Αν λοιπόν $\pi^N | t_1, t_2$, τότε $\pi^N | t_3$, που αυτό σημαίνει ότι $P_3 = (t_3, s_3) \in E^{(N)}$. Αρα οι $E^{(N)}$ είναι πράγματι ομάδες (προφανώς αβελιανές).

Θέλουμε τέλος να αποδείξουμε ότι οι ομάδες $E^{(N)}/E^{(N+1)}$ είναι γινόμενο κυκλικών ομάδων τάξης p. Περιορίζουμε καταρχήν την μελέτη μας σε p-αδικά σώματα. Θα αποδείξουμε ότι σε αυτά τα σώματα ισχύει ότι η τάξη της $E^{(N)}/E^{(N+1)}$ είναι p. Θεωρούμε τις εξής απεικονίσεις:

$$E^{(0)} \longrightarrow E^{(N)} \longrightarrow E^{(N)}/E^{(N+1)}$$

$$(x, y) \mapsto (p^{2N}x, p^{3N}y) \mapsto (p^{2N}x, p^{3N}y) + E^{(N+1)}$$

που είναι και οι δύο επί. Συνεπώς η απεικόνιση $E^{(0)} \longrightarrow E^{(N)}/E^{(N+1)}$ είναι επί και έχει προφανώς πυρήνα την ομάδα $E^{(1)}$. Επομένως:

$$E^{(N)}/E^{(N+1)} \cong E^{(0)}/E^{(1)} \cong \tilde{E}_{ns}$$

όπου η τελευταία ισομορφία ισχύει λόγω της πρότασης 3.4 .

Επιπλέον αφού η αναγωγή είναι προσθετικού τύπου, έχουμε ότι ([Si 1], σελ. 61):

$$\tilde{E}_{ns} \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^+ \cong (\mathbb{Z}/p\mathbb{Z})^+$$

Αρα η τάξη της ομάδος $\tilde{E}_{ns}$ είναι p.

Εξετάζουμε τώρα τι γίνεται σε πεπερασμένες επεκτάσεις του $\mathbb{Q}_p$, K_υ. Εχουμε:

$$E^{(N)}/E^{(N+1)} \cong \tilde{E}_{ns} \cong (\tilde{K}_\upsilon)^+.$$

Ομως $(\tilde{K}_\upsilon : \mathbb{Z}/p\mathbb{Z}) = f$ (ο βαθμός αδρανείας του ιδεώδους πR). Συνεπώς το σώμα $\tilde{K}_\upsilon$ είναι ισόμορφο με f " αντίγραφα " του πεπερασμένου σώματος $\mathbb{Z}/p\mathbb{Z}$. Αρα πράγματι η $E^{(N)}/E^{(N+1)}$ είναι γινόμενο κυκλικών ομάδων τάξης p. □

Πρόταση 3.7 *p $m \in \mathbb{N}$, , m p. :*

1. *$E^{(1)}(K_\upsilon)$ m.*

2. *- $E(K_\upsilon)$ m, $E(K_\upsilon)[m]$, $1-1$.*

<u>Απόδειξη :</u>

1. Εστω $P = (x, y) \in E(K_\upsilon)$ σημείο τάξης m. Τότε $x, y \in R$ διότι αν $x, y \notin R$, τότε το σημείο $P = (x, y)$, θα ανήκε σε κάποιο από τα επίπεδα αναγωγής. Συνεπώς μπορούμε να υποθέσουμε ότι $P \in E^{(N)}$, αλλά $P \notin E^{(N+1)}$. Αυτό σημαίνει ότι το P είναι μη-μηδενικό στοιχείο της ομάδος $E^{(N)}/E^{(N+1)}$ και άρα έχει τάξη p. Αυτό όμως είναι άτοπο διότι $(m, p) = 1$. Αρα το σημείο P έχει ακέραιες συντεταγμένες $x, y \in R$. Ομως η ομάδα $E^{(1)}$ περιέχει σημεία που οι συντεταγμένες τους δεν είναι ακέραιες. Αρα πράγματι η $E^{(1)}$ δεν περιέχει σημεία τάξης m.

   Επίσης μία άλλη απόδειξη μπορεί να δοθεί χρησιμοποιώντας την θεωρία των τυπικών ομάδων. Εχουμε την μικρή ακριβή ακολουθία:

$$0 \longrightarrow E^{(1)}(K_\upsilon) \longrightarrow E^{(0)}(K_\upsilon) \longrightarrow \tilde{E}(\tilde{K}_\upsilon) \longrightarrow 0.$$

   Ομως $\hat{E}(\pi R) \cong E^{(1)}(K_\upsilon)$, (από την πρόταση 3.5) όπου $\hat{E}$ είναι η τυπική ομάδα που αντιστοιχεί στην ελλειπτική καμπύλη E. Επιπλέον η $\hat{E}(\pi R)$ δεν έχει μη-τετριμμένα σημεία τάξης m, (λόγω της πρότασης 2.10) και άρα ισχύει το ζητούμενο.

2. Εχουμε πάντα την μικρή ακριβή αλολουθία:

$$0 \longrightarrow E^{(1)}(K_\upsilon) \longrightarrow E^{(0)}(K_\upsilon) \longrightarrow \tilde{E}_{ns}(\tilde{K}_\upsilon) \longrightarrow 0$$

   Οταν όμως η ανηγμένη καμπύλη είναι μη ιδιόμορφη τότε $E^{(0)}(K_\upsilon) = E(K_\upsilon)$ και $\tilde{E}_{ns}(\tilde{K}_\upsilon) = \tilde{E}(\tilde{K}_\upsilon)$. Συνεπώς ισχύει:

$$\tilde{E}(\tilde{K}_\upsilon) \cong E(K_\upsilon)/E^{(1)}(K_\upsilon).$$

   Αφού όμως η ομάδα $E^{(1)}(K_\upsilon)$ δεν περιέχει σημεία τάξης πρώτης προς τον p έχουμε το ζητούμενο. □

Κατά την αποδεικτική διαδικασία της προηγούμενης πρότασης είδαμε ότι αν ένα σημείο $P = (x, y)$ μιας ελλειπτικής καμπύλης E/K_υ έχει τάξη m με $(m, p) = 1$, τότε $x, y \in R$. Στα παρακάτω θα προσπαθήσουμε να απαντήσουμε στο εξής ερώτημα: Τι συμβαίνει στην περίπτωση όπου $(m, p) \neq 1$;

Πρόταση 3.8 *:*

$$E^{(N)}/E^{(5N)} \longrightarrow \pi^N R/\pi^{5N} R$$

$$P \mapsto t(P)$$

.

Απόδειξη : Κάνοντας τον μετασχηματισμό $t := \frac{x}{y}$, $s := \frac{1}{y}$, γνωρίζουμε ότι αν το σημείο $P = (x, y) \in E^{(N)}$ τότε $\pi^N | t$, $\pi^{3N} | s$. Αν μάλιστα $P_1 = (t_1, s_1), P_2 = (t_2, s_2), P_3 = (t_3, s_3)$ είναι σημεία της προκύπτουσας καμπύλης στο (t, s)-επίπεδο, που να βρίοκονται στην ίδια ευθεία, τότε: $t_1 + t_2 + t_3 \equiv 0 mod \pi^{5N} R$.

Θεωρούμε τώρα τις απεικονίσεις:

$$E^{(N)} \longrightarrow \pi^N R \longrightarrow \pi^N R / \pi^{5N} R$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y} \mapsto t(P) + \pi^{5N} R.$$

Παρατηρούμε ότι η απεικόκόνιση $E^{(N)} \longrightarrow \pi^N R / \pi^{5N} R$, έχει πυρήνα την ομάδα $E^{(5N)}$. Αποδείξαμε δηλαδή ότι η απεικόνιση $E^{(N)} / E^{(5N)} \longrightarrow \pi^N R / \pi^{5N} R$ είναι $1 - 1$.

Επίσης όπως γνωρίζουμε από την θεωρία των τυπικών ομάδων ελλειπτικών καμπύλων δοθέντος $t \in \pi R$, κατασκευάζονται δυναμοσειρές $x(t)$, $y(t)$, οι οποίες (δεδομένου ότι το σώμα K_υ είναι πλήρες ως προς την διακριτή εκτίμηση υ) συγκλίνουν και συνεπώς δίνουν σημείο $P = (x(t), y(t))$ στην ελλειπτική καμπύλη E. Συνεπώς η απεικόνιση $P \mapsto t(P)$ είναι επί. Αρα έχουμε την ζητούμενη ισομορφία. □

Πόρισμα 3.9 π p. $E^{(N)}$, $N \geq 1$, m, p.

Απόδειξη : Εστω $P = (x, y) \in E^{(N)} - E^{(N+1)}$, τάξης m, όπου $(m, p) = 1$. Τότε από την απόδειξη του θεωρήματος 3.8, έχουμε $t(2P) \equiv 2t(P) \pmod{\pi^{5N} R}$. Επομένως $t(mP) \equiv mt(P) \equiv 0 \pmod{\pi^{5N} R}$. Συνεπώς $mt(P) \in \pi^{5N} R$. Ομως το ιδεώδες $\pi^{5N} R$, είναι πρωτεύων ιδεώδες (δες [A-M], σελ. $50 - 58$), διότι $rad(\pi^{5N} R) = \pi R$ (με $rad(A)$ συμβολίζουμε το ριζικό ενός ιδεώδους A) και αφού $m \notin \pi R$, συνεπάγεται ότι $t(P) \in \pi^{5N} R$. Αρα $P \in E^{(5N)}$, που είναι άτοπο. □

Πόρισμα 3.10 m , m . $P = (x, y)$ $ord(P) = m$, $x \in R$.

Απόδειξη : Εστω ότι $x \notin R$. Τότε $P \in E^{(N)}$ για κάποιον φυσικό αριθμό $N \geq 1$. Εστω δε $m = l^n n_0$ για κάποιους φυσικούς αριθμούς l, n, n_0 τέτοιους ώστε ο l να μην διαιρεί τον n_0

και ο π να μην διαιρεί τον l στον R. Τότε το σημείο $n_0 P \neq O$ και η τάξη του είναι l^n. Ομως οι l^n και π είναι πρώτοι μεταξύ τους. Ατοπο, λόγω του πορίσματος 3.9. Αρα πράγματι $x \in R$.
$\square$

Πόρισμα 3.11 $P, Q \in E(K_\upsilon)$ m $mP = Q$. $x(P)$ $x(Q)$.

Απόδειξη : Εστω $P \in E^{(N)} - E^{(N+1)}$ δηλαδή ο π^{2N} είναι η μεγαλύτερη δύναμη του π που διαιρεί τον παρονομαστή του $x(P)$. Τότε το σημείο $Q = mP$ ανήκει στην $E^{(N)}$ (αφού όπως αποδείξαμε είναι ομάδα). Συνεπώς το Q είναι επιπέδου τουλάχιστο N και άρα η δύναμη του π που βρίσκεται στον παρονομαστή του $x(Q)$ είναι μεγαλύτερη ή ίση από τον $2N$. Αρα πράγματι ο παρονομαστής του $x(P)$ διαιρεί τον παρονομαστή του $x(Q)$. $\square$

Το ακόλουθο θεώρημα μας δίνει ένα φράγμα, του επιπέδου των σημείων πεπερασμένης τάξης.

Θεώρημα 3.12 $P \in E(K_\upsilon)$, m. π p, e ($p = \pi^e u$, $u \in R^*$). $P \in E^{(N)}$, $N \geq 1$, $N \leq \frac{e}{4}$.

Απόδειξη : Κατ' αρχήν θα αποδείξουμε ότι κατ' ανάγκη m είναι δύναμη πρώτου. Διότι αν ο m δεν είναι δύναμη πρώτου αριθμού p, τότε αφού $mP = O$ συνεπάγεται (πόρισμα 3.9) ότι $x(P) \in R$. Ατοπο, διότι $P \in E^{(N)}$, $N \geq 1$. Αρα $m = p^k$, για κάποιον φυσικό αριθμό $k \geq 1$.

Εστω $Q := p^{m-1}P$, δηλαδή $pQ = O$. Εχουμε:

$$P \in E^{(N)} \Longrightarrow Q \in E^{(N)} \Longrightarrow \pi^N | t(Q).$$

Αν r είναι η μεγαλύτερη δύναμη του π που διαιρεί τον $t(Q)$, τότε

$$O = t(pQ) \equiv p \cdot t(Q) mod \pi^{5r} R \Longrightarrow \pi^e \cdot u \cdot t(Q) \equiv O mod \pi^{5r} R.$$

Ομως $t(Q) = \pi^r u'$, για κάποιο $u' \in R^*$. Αρα:

$$\pi^{e+r} \equiv O mod \pi^{5r} R \Longrightarrow \pi^{5r} | \pi^{e+r} \Longrightarrow 5r \leq e + r \Longrightarrow r \leq \frac{e}{4}.$$

$\square$

Θεώρημα 3.13 π p e. $P = (x, y) \in E(K_\upsilon)$, p^s, :

1. $p = 2$, $x, y \in R$.

2. $p \neq 2$, $P \in E^{(N)}$, $N \leq \frac{e}{\varphi(p^s)}$, e $p-1$, p $E^{(1)}$.

<u>Απόδειξη :</u>

1. Αν $p = 2$, ισχύει ότι το $x(P)$ είναι ρίζα του πολυωνύμου $2^{-2s}\psi_{2^s}^2$, που είναι μονικό πολυώνυμο του $R[x] := \mathbb{Z}[a, b, x]$ (θεώρημα 1.10). Ομως ο R είναι ακέραια κλειστός (ως διακριτός δακτύλιος εκτίμησης). Αρα $x \in R$.

2. Εστω τώρα $p \neq 2$. Για κάποιον φυσικό αριθμό n, $1 \leq n \leq p^s$ και $(n, p) = 1$, γράφουμε $nP := (x_n, y_n)$. Εχουμε $\varphi(p^s)$ τέτοια πολλαπλάσια του σημείου P, με ακριβή τάξη p^s. Επίσης όπως γνωρίζουμε οι συντεταγμένες x_n είναι ρίζες των πολυωνύμων:

$$g(X) = \frac{\psi_{p^s}(X)}{\psi_{p^{s-1}}^2(X)} \qquad (\text{ Θεώρημα } 1.10),$$

τα οποία έχουν συντελεστή μεγιστοβαθμίου όρου p^2 και ακέραιους συντελεστές (πρώτους μεταξύ τους). Είναι προφανές δε ότι:

$$g(X) = p^2(X - x_n)\prod(X - x(Q))$$

όπου το γινόμενο διατρέχει όλα τα Q που έχουν τάξη ακριβώς p^s και $Q \neq nP$. Επιπλέον ισχύει ότι ότι ο παρονομαστής του x_1 διαιρεί τον παρονομαστή του x_n, (πόρισμα 3.11), συνεπώς $\|x_n\| \leq \|x_1\|$. Ομως $(n, p) = 1$, άρα και $(n, p^s) = 1$, συνεπώς υπάρχουν ακέραιοι m_1, m_2, τέτοιοι ώστε:

$$nm_1 + p^s m_2 = 1 \Longrightarrow m_1 nP + m_2 p^s P = P \Longrightarrow m_1(nP) = P.$$

Εφαρμόζοντας ξανά το πόρισμα 3.11 για το σημείο nP, έχουμε ότι $\|x_1\| \leq \|x_n\|$. Αρα ισχύει η ισότητα $\|x_1\| = \|x_n\|$. Παρατηρούμε ότι ο σταθερός όρος του $g(X)$ είναι στοιχείο του R ($g(X) \in R[X]$). Συνεπώς η απόλυτη τιμή του σταθερού όρου του $g(X)$, είναι:

$$\|p^2\|\|x_1\|^{\varphi(p^s)} \leq 1 \Longrightarrow \|x_1\|^{\varphi(p^s)} \leq \|p\|^{-2} = p^2 \Longrightarrow \|x_1\| \leq p^{\frac{2}{\varphi(p^s)}} \quad (*).$$

Ομως $\|p\| = \|\pi\|^e$. Επίσης $\|x_1\| \geq \|\pi^{-2N}\| = p^{2N/e}$ $(**)$. Συνδιάζοντας τις δύο ανισοτικές σχέσεις $(*)$ και $(**)$ εχουμε:

$$\frac{2N}{e} \leq \frac{2}{\varphi(p^s)} \Longrightarrow N \leq \frac{e}{\varphi(p^s)}.\square$$

Παρατήρηση : Εστω $n = p^s$, όπου p περιττός πρώτος. Εστω δε $P \in E^{(N)}$, $N \leq \frac{e}{\varphi(p^s)}$. Ομως $e = \upsilon(p)$, $\varphi(p^s) = p^s - p^{s-1}$, και άρα έχουμε ότι $N \leq \frac{\upsilon(p)}{p^s - p^{s-1}}$. Από την άλλη πλευρά όμως, αφού το P έχει επίπεδο N, ισχύει $\pi^{2N}x(P), \pi^{3N}y(P) \in R$. Αρα:

$$N = [\frac{\upsilon(p)}{p^s - p^{s-1}}].$$

3.4 Η τάξη της ομάδος $E(K_\upsilon)/\mathrm{E}^{(0)}(K_\upsilon)$

Σκοπός αυτής της παραγράφου είναι η απόδειξη του εξής θεωρήματος:

Θεώρημα 3.14 *(Kodaira , Neron)* E/K_υ . E , $E(K_\upsilon)/\mathrm{E}^{(0)}(K_\upsilon)$ $-\upsilon(j)$. $E(K_\upsilon)/E^{(0)}(K_\upsilon)$ 4.

Κατ' αρχήν όταν η καμπύλη E/K_υ έχει καλή αναγωγή, ισχύει ότι $E(K_\upsilon) = E^{(0)}(K_\upsilon)$ και συνεπώς δεν έχουμε να αποδείξουμε τίποτα.

Ξεκινούμε από την περίπτωση όπου η καμπύλη E έχει αναγωγή προσθετικού τύπου. Θα περιοριστούμε σε περιπτώσεις όπου η χαρακτηριστική του σώματος $\tilde{K}_\upsilon$ είναι διαφορετική των 2 και 3 (για τις περιπτώσεις χαρακτηριστικής 2 ή 3 παραπέμπουμε στο [Pa]) . Ας συμβολίσουμε την τάξη της ομάδος $E(K_\upsilon)/E^{(0)}(K_\upsilon)$ με m.

Εστω $E : Y^2 = X^3 + aX + b$, ελάχιστο μοντέλο του Weierstrass. Συνεπώς αφού η χαρακτηριστική του σώματος $\tilde{K}_\upsilon$ δεν είναι 2 ή 3, ισχύει ότι $\upsilon(\Delta)$ μικρότερο του 12, καθώς επίσης ότι $\upsilon(a)$ μικρότερο του 4, $\upsilon(b)$ μικρότερο του 6 (σελ. 29).

Πρόταση 3.15 $E/K_\upsilon : Y^2 = X^3 + aX + b$ *Weierstrass* E. E *modulo* π, *:*

1. $\upsilon(a) \geq 1$ $\upsilon(b) = 1$, $m = 1$.
2. $\upsilon(a) = 1$ $\upsilon(b) \geq 2$, $m = 2$.
3. $\upsilon(a) \geq 2$ $\upsilon(b) = 2$, $m = 3$.
4. $\upsilon(a) = 2$ $\upsilon(b) \geq 3$, $m = 4$.
5. $\upsilon(a) = 2$ $\upsilon(j) < 0$, $m = 4$.
6. $\upsilon(a) \geq 3$ $\upsilon(b) = 4$, $m = 3$.

7. $\upsilon(a) = 3 \;\; \upsilon(b) \geq 5, \;\; m = 2.$

8. $\upsilon(a) \geq 4 \;\; \upsilon(b) = 5, \;\; m = 1.$

Απόδειξη :

1. Εστω $\upsilon(a) \geq 1$ και $\upsilon(b) = 1$. Αν υπάρχει σημείο $P = (x, y) \in E(K_\upsilon) - E^{(0)}(K_\upsilon)$ τότε απεικονίζεται μέσω της απεικόνισης αναγωγής στο ιδιόμορφο σημείο $(\tilde{0}, \tilde{0})$ της καμπύλης $\tilde{E}$. Συνεπώς $\pi | x, y$. Κάνουμε τον μετασχηματισμό:

$$x = \pi x', \quad y = \pi y'.$$

Η προκύπτουσα καμπύλη είναι η:

$$E' : \pi^2 (y')^2 = \pi^3 (x')^3 + a\pi x' + b.$$

Ομως $\upsilon(b) = 1$. Αρα ο b γράφεται στην μορφή $b = \pi u, \;\; u \in R^*$. Επίσης έχουμε ότι $\upsilon(a) \geq 1$, συνεπώς ο a γράφεται στην μορφή $a = \pi^k u'$, $u' \in R^*, \;\; k \geq 1$. Αντικαθιστώντας στην εξίσωση της E', έχουμε:

$$E' : \pi^2 (y')^2 = \pi^3 (x')^3 + u' \pi^{k+1} x' + \pi u, \qquad \text{δηλαδή}$$

$$E' : \pi (y')^2 = \pi^2 (x')^3 + u' \pi^k x' + u.$$

Συνεπώς, $\pi | u$. Ατοπο. Αρα $E(K_\upsilon) = E^{(0)}(K_\upsilon)$, δηλαδή $m = 1$

2. Εστω $\upsilon(a) = 1$ και $\upsilon(b) \geq 2$. Τότε $a = \pi u$ και $b = \pi^k u'$, $u, u' \in R^*$ και $k \geq 2$. Η καμπύλη E έχει εξίσωση:

$$E : y^2 = x^3 + \pi u x + \pi^k u'.$$

Εστω δύο σημεία $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(K_\upsilon) - E^{(0)}(K_\upsilon)$. Τότε τα σημεία P, Q απεικονίζονται μέσω της απεικόνισης αναγωγής στο ιδιόμορφο σημείο $(\tilde{0}, \tilde{0})$, δηλαδή $\pi | x_i, y_i$, $i = 1, 2$. Αποδεικνύουμε ότι ισχύει η $P + Q \in E^{(0)}(K_\upsilon)$.

Εστω ότι δεν ισχύει. Τότε έχουμε ότι $\pi | x(P+Q)$. Αν $P \neq Q$, ισχύει:

$$x(P+Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

Το κλάσμα $\frac{y_2-y_1}{x_2-x_1}$ δεν ανήκει στο ιδεώδες πR, διότι αν ανήκε, θα γραφόταν στην μορφή $\pi^l \bar{u}$, όπου $l \geq 1$ και $\bar{u} \in R^*$. Τότε θα είχαμε:

$$y_2 - y_1 = \pi^l \bar{u}(x_2 - x_1) \Longrightarrow y_2^2 - y_1^2 = \pi^l \bar{u}(x_2 - x_1)(y_2 + y_1)$$

$$\Longrightarrow (x_2 - x_1)(x_1^2 + x_1 x_2 + x_2^2) + \pi u(x_2 - x_1) = \pi^l \bar{u}(x_2 - x_1)(y_2 + y_1)$$

$$\Longrightarrow x_1^2 + x_1 x_2 + x_2^2 + \pi u = \pi^l \bar{u}(y_2 + y_1).$$

Παρατηρούμε ότι η μεγαλύτερη δύναμη του π που διαιρεί το πρώτο μέλος της ισότητας είναι ο ίδιος ο π, ενώ το δεύτερο μέλος της ισότητας διαιρείται τουλάχιστο από τον π^2, άτοπο. Συνεπώς το κλάσμα $\frac{y_2-y_1}{x_2-x_1}$ δεν ανήκει στο ιδεώδες πR. Δηλαδή είναι μονάδα του δακτυλίου R. Αρα ο $x(P+Q) \in R^*$, διότι $x_1, x_2 \in \pi R$, άτοπο. Αρα πράγματι $P + Q \in E^{(0)}(K_\upsilon)$ (η περίπτωση $P = Q$, γίνεται εντελώς όμοια). Ομως τότε θα έχουμε μόνο δύο πλευρικές ομάδες της $E^{(0)}(K_\upsilon)$ στην $E(K_\upsilon)$, δηλαδή $m = 2$

3. Εστω $\upsilon(a) \geq 2$ και $\upsilon(b) = 2$. Τότε $a = \pi^k u$, $b = \pi^2 u'$, όπου $u, u' \in R^*$ και $k \geq 2$. Η εξίσωση της ελλειπτικής καμπύλης E, είναι:

$$E : y^2 = x^3 + \pi^k ux + \pi^2 u'.$$

Εστω $P = (x, y) \in E(K_\upsilon) - E^{(0)}(K_\upsilon)$. Αρα $\pi | x, y$. Παρατηρούμε τώρα ότι ο π^2 δεν διαιρεί τον y (διότι εάν τον διαιρούσε τότε θα έπρεπε $\pi | u'$, άτοπο). Επομένως κάθε σημείο $P \in E(K_\upsilon) - E^{(0)}(K_\upsilon)$, γράφεται στην μορφή $P = (x, \pi w), \ \ x \in \pi R, w \in R^*$. Ας πάρουμε ένα άλλο σημείο $Q \in E(K_\upsilon) - E^{(0)}(K_\upsilon), \ \ Q = (x', \pi w')$, όπου $x' \in \pi R, \ \ w' \in R^*$. Η x-συντεταγμένη του σημείου $P + Q$, είναι:

$$x(P+Q) = (\frac{\pi(w' - w)}{x' - x})^2 - x - x'.$$

Εχουμε:

$$\Rightarrow \frac{\pi(w' - w)}{x' - x} = \frac{x'^2 + x^2 + xx' + \pi^{k+1} u}{\pi(w' + w)}$$

Παρατηρούμε ότι το $P + Q \in E^{(0)}(K_\upsilon)$ ανν ο π δεν διαιρεί το $x(P+Q)$ δηλαδή ανν ο π δεν διαρεί το $\frac{\pi(w'-w)}{x'-x}$. Επομένως, $\pi^2 | \pi(w' - w) \Leftrightarrow w' \equiv w \pmod{\pi}$. Κάνουμε τον μετασχηματισμό:

$$x := \pi h \quad y := \pi w.$$

Η νέα εξίσωση της καμπύλης E, είναι η:

$$E : \pi^2 w^2 = \pi^3 h^3 + \pi^{k+1} uh + \pi^2 u' \quad \text{και ισοδύναμα :}$$

$$E : w^2 = \pi h^3 + \pi^{k-1} uh + u'.$$

Αναγάγουμε την E modulo π και παίρνουμε την εξίσωση:

$$w^2 \equiv u' \pmod{\pi}.$$

Η παραπάνω εξίσωση μας οδηγεί σε δύο λύσεις modulo π, $w \equiv \pm s \pmod{\pi}$. Ομως $s \not\equiv -s \pmod{\pi}$, διότι εάν ήταν τότε $\pi|2s \Rightarrow \pi|s$, δηλαδη το π θα διαιρεί το w, άτοπο. Αρα έχουμε τουλάχιστο δύο πλευρικές ομάδες της $E^{(0)}(K_\upsilon)$ στην $\mathrm{E}(\mathrm{K}_\upsilon)$, την πλευρική ομάδα των σημείων που η y-συντεταγμένη τους ανήκει στο $s\pi + \pi^2 R$ και την πλευρική ομάδα των σημείων που η y-συντεταγμένη τους ανήκει στο $-s+\pi^2 R$. Αν $w \equiv s \pmod{\pi}$, τότε βρισκόμαστε στην ίδια πλευρική ομάδα και αν $w \equiv -s \pmod{\pi}$, τότε βρισκόμαστε στην άλλη πλευρική ομάδα. Συνολικά έχουμε τρεις πλευρικές ομάδες την ταυτοτική και τις άλλες δύο που αποδείξαμε ότι υπάρχουν. Αρα πράγματι $m = 3$.

Οι περιπτώσεις $4, 5, 6$ αποδεικνύονται κατά όμοιο τρόπο με την περίπτωση 3. Η περίπτωση 7, αποδεικνύεται όμοια με την περίπτωση 2 και τέλος η παρίπτωση 8, αποδεικνύεται όμοια με την περίπτωση 1. $\square$

Παρατήρηση : Υπάρχει και άλλη απόδειξη της προηγούμενης πρότασης, η οποία χρησιμοποιεί εργαλεία Αλγεβρικής Γεωμετρίας ([Ta]).

Αμεση συνέπεια της πρότασης 3.15 είναι το:

Πόρισμα 3.16 E/K_υ . E *modulo* π. $E(K_\upsilon)/E^{(0)}(K_\upsilon)$, 4.

Απομένει να εξετάσουμε την περίπτωση όπου η ελλειπτική καμπύλη E/K_υ, έχει διαχωριζομένη πολλαπλασιαστική αναγωγή modulo π. Η περίπτωση αυτή συνδέει άμεσα την θεωρία των ελλειπτικών καμπύλων ορισμένων σε τοπικά σώματα με τις καμπύλες του Tate. Τι είναι όμως μια καμπύλη του Tate;

Ορισμός 3.17 K_υ υ, $q \in \pi R$. *Tate* :

$$E_q : Y^2 - XY = X^3 - h_2 X - h_3,$$

$h_2, h_3, \quad q$:

$$h_2 = 5\ sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n} \qquad h_3 = \frac{1}{12} \sum_{n=1}^{\infty} \frac{(5n^3 + 7n^5) q^n}{1-q^n},$$

p- $\|\cdot\|$ υ.

Για $w \in (\bar{K_\upsilon})^*$, ορίζουμε τις σειρές ως εξής:

$$X_q(w) = \sum_{n \in \mathbb{Z}} \frac{q^n w}{(1-q^n w)^2} - 2 \sum_{n=1}^{\infty} \frac{n q^n}{1-q^n}$$

$$Y_q(w) = \sum_{n \in \mathbb{Z}} \frac{(q^n w)^2}{(1-q^n w)^3} - \sum_{n=1}^{\infty} \frac{n q^n}{1-q^n}$$

Αποδεικνύεται το εξής θεώρημα ([Kov], σελ.84):

Θεώρημα 3.18 *(Tate)* $X_q(w)$, $Y_q(w)$ $(\bar{K_\upsilon})^*$:

$$\varphi : (\bar{K_\upsilon})^* \longrightarrow E_q(\bar{K_\upsilon})$$

$$w \mapsto (X_q(w), Y_q(w)), \quad w \notin q^{\mathbb{Z}}$$

$$w \mapsto O, \quad w \in q^{\mathbb{Z}}$$

φ $q^{\mathbb{Z}}$.

Επίσης ισχύει η εξής πρόταση ([Kov], θεωρ. 4.5) :

Πρόταση 3.19 $j \in K_\upsilon^*$ $\upsilon(j)$, *Tate* j.

Πόρισμα 3.20 E/K_υ, *modulo* π. *Tate* E_q, E, $\bar{K_\upsilon}$.

Στην συνέχεια αποδεικνύουμε την εξής πρόταση:

Πρόταση 3.21 E/K_υ *Tate* E_q, E, K_υ.

Απόδειξη : Εστω ότι η ελλειπτική καμπύλη E/K_υ δίνεται από την ελάχιστη εξίσωση του Weierstrass:

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

Αν υποθέσουμε ότι η καμπύλη E έχει διαχωριζόμενη πολλαπλασιαστική αναγωγή modulo π, τότε χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι το ιδιόμορφο σημείο modulo π είναι το σημείο $(\tilde{0}, \tilde{0})$, που αυτό σημαίνει ότι:

$$a_3 \equiv a_4 \equiv a_6 \equiv 0 \pmod{\pi}$$

Αρα :

$$b_4 = a_1 a_3 + 2a_4 \equiv 0 \pmod{\pi},$$

$$b_6 = a_3^2 + 4a_6 \equiv 0 \pmod{\pi},$$

$$c_4 = b_2^2 - 24b_4 \equiv b_2^2 \pmod{\pi}.$$

Επειδή η E έχει πολλαπλασιαστική αναγωγή έπεται ότι $c_4 \not\equiv 0 (mod \pi)$ ([Si1],σελ. 180). Επομένως $b_2 \not\equiv 0 \pmod{\pi}$. Υπολογίζουμε την αναλλοίωτο του Hasse της ελλειπτικής καμπύλης E :

$$\delta_E = -\frac{c_4}{c_6} = \frac{b_2^2 - 24b_4}{b_2^3 + 36b_2b_4 - 216b_6} = \frac{1}{b_2}\left(\frac{1 - 24\frac{b_4}{b_2^2}}{1 + 36\frac{b_4}{b_2^2} + 216\frac{b_6}{b_2^3}}\right)$$

Εχουμε $\|\frac{b_4}{b_2^2}\| = \|b_4\|$, που είναι μικρότερο του 1, διότι $b_4 \equiv 0 mod \pi$. Επίσης :

$$\|\frac{b_4}{b_2^2} + 6\frac{b_6}{b_2^3}\| \leq \max\{\|\frac{b_4}{b_2^2}\|, \|\frac{b_6}{b_2^3}\|\},$$

το οποίο είναι μικρότερο του 1, διότι $b_4 \equiv b_6 \equiv 0 \pmod{\pi}$ και $\|b_2\| = 1$. Γνωρίζουμε όμως ότι αν το $\|x\|$ είναι μικρότερο του 1 τότε το $1 + 4x$, είναι τέλειο τετράγωνο στο K_υ ([Kον], λήμμα 4.6). Συνεπώς:

$$\delta_E \equiv \frac{1}{b_2} \equiv b_2 mod (K_\upsilon^*)^2.$$

Κάνουμε αναγωγή της E modulo π :

$$\tilde{E} : Y^2 + \tilde{a}_1 XY - \tilde{a}_2 X^2 = X^3$$

Αφού όμως η αναγωγή της ελλειπτικής καμπύλης E είναι διαχωριζομένη, υπάρχουν $\tilde{\alpha}, \tilde{\beta}$, $\tilde{\alpha} \neq \tilde{\beta}$, με $\tilde{\alpha}, \tilde{\beta} \in \tilde{K}_\upsilon$, τέτοια ώστε :

$$\tilde{E} : (Y - \tilde{\alpha}X)(Y - \tilde{\beta}X) = X^3.$$

Λόγω όμως του λήμματος του Hensel, υπάρχουν α, β, από το σώμα K_υ τα οποία ανάγονται modulo π στα $\tilde{\alpha}$, $\tilde{\beta}$. Συνεπώς :

$$b_2 = a_1^2 + 4a_2 = (\alpha + \beta)^2 + 4(-\alpha\beta) = (\alpha - \beta)^2 \in (K_\upsilon^*)^2.$$

Δηλαδή $\delta_E \equiv 1 \pmod{(K_\upsilon^*)^2}$. Από το [Kον], πόρισμα 4.7 έχουμε ότι $\delta_{E_q} \equiv 1 \pmod{(K_\upsilon^*)^2}$. Επομένως $\delta_{E_q} \equiv \delta_E \equiv 1 \pmod{(K_\upsilon^*)^2}$, δηλαδή οι E, E_q, είναι ισόμορφες πάνω από το K_υ.

Η άλλη κατεύθυνση είναι προφανής. □

Εστω ελλειπτική καμπύλη E/K_υ, με διαχωριζομένη πολλαπλασιαστική αναγωγή. Τότε, όπως αποδείξαμε, υπάρχει καμπύλη του Tate E_q, τέτοια ώστε:

$$E(K_\upsilon) \cong E_q(K_\upsilon) \cong K_\upsilon^*/q^{\mathbb{Z}}.$$

Κάνουμε την γνωστή διαδικασία με τα π-αδικά φίλτρα στην E_q :

$$E_q(K_\upsilon) \supset E_q^{(0)}(K_\upsilon) \supset E_q^{(1)}(K_\upsilon)$$

Ισχύει ότι (πρόταση 3.4):

$$E_q^{(0)}(K_\upsilon)/E_q^{(1)}(K_\upsilon) \cong (\tilde{E}_q)_{ns}(\tilde{K}_\upsilon)$$

Επίσης θεωρούμε το εξής "φιλτράρισμα " :

$$K_\upsilon^*/q^{\mathbb{Z}} \supset R^* \supset R_1^*$$

όπου $R_1^* := \{a \in R^*/a \equiv 1 mod \pi\}$. Προφανώς ισχύει ότι $R^*/R_1^* \cong \tilde{K_\upsilon}^*$. Επιπλέον ισχύει ότι $\varphi(R_1^*) \subset E_q^{(1)}(K_\upsilon)$. Πράγματι, έστω $w \in R_1^*$. Εχουμε :

$$X_q(w) = \sum_{n \in \mathbb{Z}} \frac{q^n w}{(1-q^n w)^2} - 2s_1(q) = \sum_{n=1}^{\infty} \frac{q^n w}{(1-q^n w)^2} + \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty} \frac{q^n w}{(q^n - w)^2} - 2s_1(q),$$

όπου $s_1(q) = \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}$. Ο πρώτος, ο τρίτος και ο τέταρτος όρος του αθροίσματος διαιρούνται με τον π. Εστω ϑ το άθροισμά τους. Τότε:

$$X_q(w) = \vartheta + \frac{w}{(1-w)^2} = \frac{\vartheta(1-w)^2 + w}{(1-w)^2}.$$

Ο αριθμητής του $X_q(w)$ είναι μονάδα του R, ενώ ο παρονομαστής του διαιρειται από τον π^2. Ομοια δουλεύοντας με το $Y_q(w)$, συμπεραίνουμε ότι ο π^3, διαιρεί τον $Y_q(w)$. Αρα πράγματι $\varphi(R_1^*) \subset E_q^{(1)}(K_\upsilon)$. Στην συνέχεια θα αποδείξουμε ότι τελικά ισχύει η ισότητα.

Χρησιμοποιώντας την γλώσσα των τυπικών ομάδων (παράδειγμα σελ. 25), έχουμε:

$$R_1^* \cong \hat{G}_m(\pi R)$$

$$u \mapsto 1 - u$$

Επίσης λόγω της πρότασης 3.5, ισχύει ότι:

$$E_q^{(1)}(K_\upsilon) \cong \hat{E}_q(\pi R)$$

$$P = (x, y) \mapsto -\frac{x}{y},$$

όπου με $\hat{E}$, συμβολίζουμε την τυπική ομάδα της E, και με $\hat{G}_m$, συμβολίζουμε την τυπική πολλαπλασιαστική ομάδα. Λόγω των παραπάνω ισομορφισμών, έχουμε:

$$\hat{G}_m(\pi R) \longrightarrow R_1^* \longrightarrow E_q^{(1)}(K_\upsilon) \longrightarrow \hat{E}_q(\pi R)$$

$$t \mapsto -\frac{X_q(1-t)}{Y_q(1-t)}$$

Αντικαθιστούμε το $1-t$, με w στις σειρές $X_q(w)$, $Y_q(w)$, οι οποίες ως σειρές Laurent του t, έχουν ανάπτυγμα της μορφής:

$$X_q(1-t) = t^{-2}(1 + \sum_{m=1}^{\infty} a_m t^m)$$

$$Y_q(1+t) = -t^{-3}(1 + \sum_{m=1}^{\infty} b_m t^m)$$

με συντελεστές $a_m, b_m \in R$. Το πηλίκον $\frac{X_q(1-t)}{Y_q(1-t)}$ είναι μια δυναμοσειρά της μορφής $-t(1 + \sum_{m=1}^{\infty} \gamma_m t^m)$. Αρκεί λοιπόν να αποδείξουμε ότι η απεικόνιση: $\psi : t \mapsto -t(1 + \sum_{m=1}^{\infty} \gamma_m t^m)$, είναι επί. Αυτό όμως είναι άμεση συνέπεια του λήμματος 2.4, που μας εξασφαλίζει την ύπαρξη δυναμοσειράς $\lambda(T) \in R[[T]]$, με την ιδιότητα $\psi(\lambda(T)) = T$, δηλαδή η απεικόνιση ψ είναι επί, διότι για κάθε $w \in \pi R$ έχουμε $\psi(\lambda(w)) = w$. Αρα ισχύει τελικά η ισότητα $\varphi(R_1^*) = E_q^{(1)}(K_\upsilon)$.

Δουλέυοντας καθ' όμοιο τρόπο, όπως με την ομάδα R_1^*, έχουμε οτι $\varphi(R^*) \subset E_q^{(0)}(K_\upsilon)$. Λόγω του ότι $\varphi(R_1^*) = E_q^{(1)}(K_\upsilon)$, έχουμε την εξής εμφύτευση στις ομάδες πηλίκα:

$$\tilde{K}_\upsilon^* \cong R^*/R_1^* \hookrightarrow E_q^{(0)}(K_\upsilon)/E_q^{(1)}(K_\upsilon) \cong (\tilde{E}_q)_{ns}(\tilde{K}_\upsilon)$$

$$u \mapsto (\frac{u}{(1-u)^2}, \frac{u^2}{(1-u)^3})$$

Η απεικόνιση $\tilde{K}_\upsilon^* \longrightarrow \tilde{E}_q(\tilde{K}_\upsilon)$ είναι επί, λόγω του θεωρήματος 3.18 (Tate) και έχει αντίστροφο την $(x, y) \mapsto \frac{y^2}{x^3}$. Αρα $R^*/R_1^* \cong E_q^{(0)}(K_\upsilon)/E_q^{(1)}(K_\upsilon)$. Θεωρούμε το εξής αντιμεταθετικό διάγραμμα:

$$1 \longrightarrow R_1^* \longrightarrow R^* \longrightarrow \tilde{K}_\upsilon^* \longrightarrow 1$$

$$0 \to E_q^{(1)}(K_\upsilon) \to E_q^{(0)}(K_\upsilon) \to \tilde{E}_{ns}(\tilde{K}_\upsilon) \to 0$$

από το οποίο γίνεται πλέον φανερό ότι η απεικόνιση $\varphi : R^* \to E_q^{(0)}(K_\upsilon)$, είναι ισομορφισμός ομάδων. Συνεπώς:

$$\mathrm{K}_\upsilon^*/R^* q^{\mathbb{Z}} \cong E_q(K_\upsilon)/E_q^{(0)}(K_\upsilon)$$

Τέλος η απεικόνιση:

$$K_\upsilon^*/R^* q^{\mathbb{Z}} \longrightarrow \mathbb{Z}/\upsilon(q)\mathbb{Z}$$

$$u \mapsto \upsilon(u)$$

είναι ισομορφισμός ομάδων. Επομένως η τάξη της ομάδος $E_q(K_\upsilon)/\mathrm{E}_q^{(0)}(K_\upsilon)$, είναι $\upsilon(q) = -\upsilon(j)$, όπου η απόλυτη αναλλοίωτος j δίνεται ως δυναμοσειρά του q, $j = \frac{1}{q} + 744 + \cdots$. Αρα η τάξη της ομάδος $E(K_\upsilon)/E^{(0)}(K_\upsilon)$, όταν έχουμε διαχωριζομένη πολλαπλασιαστική αναγωγή, είναι πράγματι $-\upsilon(j)$. Αποδείξαμε λοιπόν πλήρως το θεώρημα των Kondaira-Neron.

4 Σημεία πεπερασμένης τάξης ελλειπτικών καμπύλων

4.1 Γενική θεωρία

Εστω E ελλειπτική καμπύλη οριομένη σε ένα αλγεβρικό σώμα αριθμών K. Εστω δε υ μία διακριτή εκτίμηση του σώματος K. Παίρνουμε την πλήρωση του K, K_υ ως προς την εκτίμηση υ και, χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι η E είναι υ-ελάχιστη στο σώμα K_υ. Κατά τα γνωστά μας, με R θα συμβολίζουμε τον δακτύλιο των ακεραίων του K_υ, με πR το μοναδικό μέγιστο ιδεώδες του R (όπου π είναι ο γεννήτορας του μέγιστου ιδεώδους) και τέλος με $\tilde{K}_\upsilon$ το σώμα υπολοίπων του K. Επιπλέον με $e := e_\upsilon$ και $f := f_\upsilon$ θα συμβολίζουμε τον δείκτη διακλάδωσης και τον βαθμό αδρανείας αντίστοιχα του ιδεώδους πR. Επομένως η τάξη του σώματος $\tilde{K}_\upsilon$ είναι p^{f_υ}, όπου p είναι ο αντίστοιχος πρώτος αριθμός του $\mathbb{Q}$, πάνω από τον οποίο βρίσκεται ο πR. Θέτουμε $q = p^{f_\upsilon}$. Προφανώς ισχύουν οι εξής εγκλεισμοί:

$$K \subseteq K_\upsilon \Longrightarrow E(K) \subseteq E(K_\upsilon)$$

Οπως γνωρίζουμε η ελλειπτική καμπύλη E έχει ([Si1], πρόταση 5.1, σελ. 180):

- Καλή αναγωγή modulo π όταν: $\upsilon(\Delta) = 0$. Τότε ισχύει $\upsilon(j) \geq 0$.
- Πολλαπλασιαστική αναγωγή modulo π όταν: $\upsilon(\Delta) > 0$ και $\upsilon(c_4) = 0$. Τότε $\upsilon(j) < 0$.
- Προσθετική αναγωγή modulo π όταν: $\upsilon(\Delta) > 0$ και $\upsilon(c_4) > 0$. Τότε η $\upsilon(j)$, μπορεί να έχει οποιοδήποτε πρόσημο.

Επομένως εάν περιοριστούμε σε ελλειπτικές καμπύλες E που έχουν απόλυτη αναλλοίωτο j τέτοια ώστε $\upsilon(j) \geq 0$ (δηλαδή $j \in R$), τότε η E έχει καλή ή προσθετική αναγωγή modulo π.

Το θεώρημα που ακολουθεί είναι πολύ βασικό στην μελέτη των σημείων πεπερασμένης τάξης.

Θεώρημα 4.1 $E_{tor}(K)$, :

1. E modulo π, :

$$\#E_{tor}(K) \ \mid \ \#\tilde{E}(\tilde{K}_{\mathfrak{v}}) \cdot p^{2t} \leq (1 + q_{\mathfrak{v}} + 2\sqrt{q_{\mathfrak{v}}})p^{2t}$$

2. E modulo π, :

$$\#E_{tor}(K) \ \mid \ \#E(K_{\mathfrak{v}})/E^{(0)}(K_{\mathfrak{v}}) \cdot p^{2+2t} \leq 4p^{2+2t}$$

:

(a) $p = 2$, $\#E_{tor}(K) \ \mid \ 2^{4+2t} \cdot 3$

(b) $p = 3$, $\#E_{tor}(K) \ \mid \ 2^2 \cdot 3^{3+2t}$

(c) $p = 5$, $\#E_{tor}(K) \ \mid \ 2^2 \cdot 3 \cdot 5^{2+2t}$

$$t := \begin{cases} 0 & \varphi(p^\nu) > e \\ \max\{\nu \in \mathbb{N}/\varphi(p^\nu) \leq e\} & , \end{cases}$$

φ Euler.

3. E modulo π, :

$$\#E_{tor}(K) \ \mid \ \mathfrak{v}(\Delta) \cdot (p^{2f_{\mathfrak{v}}} - 1) \cdot p^{2t}$$

Απόδειξη : Ισχύουν τα εξής :

$$E(K) \subset E(K_{\mathfrak{v}}) \Rightarrow E_{tor}(K) \subset E_{tor}(K_{\mathfrak{v}}) \Rightarrow \#E_{tor}(K) \ \mid \ \#E_{tor}(K_{\mathfrak{v}})$$

$$\text{Προφανώς έχουμε,} \quad \frac{E_{tor}(K_{\mathfrak{v}})}{E^{(1)}_{tor}(K_{\mathfrak{v}})} \subset \frac{E(K_{\mathfrak{v}})}{E^{(1)}(K_{\mathfrak{v}})},$$

όπου $E^{(1)}_{tor}(K_{\mathfrak{v}}) := E^{(1)}(K_{\mathfrak{v}}) \cap E_{tor}(K_{\mathfrak{v}})$ και, όπως έχουμε αποδείξει στο προηγούμενο κεφάλαιο (δες θεώρημα 3.6, σελ. 34), είναι πεπερασμένη p-ομάδα. Εχουμε λοιπόν την ακόλουθη ιδιότητα διαίρεσης:

$$\#E_{tor}(K_{\mathfrak{v}}) \ \mid \ \#\frac{E(K_{\mathfrak{v}})}{E^{(1)}(K_{\mathfrak{v}})} \cdot \#E^{(1)}_{tor}(K_{\mathfrak{v}})$$

Θεωρούμε σημείο $P = (x, y) \in E^{(1)}_{tor}(K_{\mathfrak{v}})$. Εστω n ο μέγιστος φυσικός τέτοιος ώστε $P \in E^{(n)}(K_{\mathfrak{v}})$, δηλαδή $\mathfrak{v}(x) = -2n$. Επιπλέον το σημείο $P \in E^{(n)}(K_{\mathfrak{v}})$, έχει τάξη p^ν, για κάποιον $\nu \in \mathbb{N}$. Επομένως σύμφωνα με το θεώρημα 3.13 έχουμε, $n \leq e/\varphi(p^\nu)$. Αν ίσχυε ότι $\varphi(p^\nu) > e$, τότε $n < 1$, που είναι άτοπο. Συνεπώς έχουμε $\varphi(p^\nu) \leq e$, δηλαδή $\nu \leq t$ (εξ ορισμού του t). Επειδή δε η p^ν-torsion υποομάδα έχει βαθμό (rank) 2, ισχύει:

$$\# E^{(1)}_{tor}(K_\upsilon) \ \mid \ p^{2t}$$

$$\text{Αρα,} \quad \# E_{tor}(K) \ \mid \ \# \frac{E(K_\upsilon)}{E^{(1)}(K_\upsilon)} \cdot p^{2t}$$

Ξεχωρίζουμε τις εξής περιπτώσεις:

1. Εστω ότι έχουμε καλή αναγωγή modulo π. Τότε $E(K_\upsilon) = E^{(0)}(K_\upsilon)$. Συνεπώς:

$$\# \frac{E(K_\upsilon)}{E^{(1)}(K_\upsilon)} = \# \frac{E^{(0)}(K_\upsilon)}{E^{(1)}(K_\upsilon)} = \# \tilde{E}(\tilde{K}_\upsilon) \leq 1 + q_\upsilon + 2\sqrt{q_\upsilon}$$

   λόγω της υπόθεσης του Riemann ([Si1], σελ. 131).

2. Αν έχουμε προσθετική αναγωγή modulo π, τότε:

$$\frac{E(K_\upsilon)}{E^{(0)}(K_\upsilon)} \cong \frac{E(K_\upsilon)/E^{(1)}(K_\upsilon)}{E^{(0)}(K_\upsilon)/E^{(1)}(K_\upsilon)}$$

$$\text{άρα,} \quad \# \frac{E(K_\upsilon)}{E^{(1)}(K_\upsilon)} = \# \frac{E(K_\upsilon)}{E^{(0)}(K_\upsilon)} \cdot \# \frac{E^{(0)}(K_\upsilon)}{E^{(1)}(K_\upsilon)}$$

   Επίσης η $E(K_\upsilon)/E^{(0)}(K_\upsilon)$ έχει τάξη μικρότερη ή ίση του 4 (θεώρημα 3.14, σελ. 41). Επιπλέον:

$$\# \frac{E^{(0)}(K_\upsilon)}{E^{(1)}(K_\upsilon)} = \# \tilde{E}_{ns}(\tilde{K}_\upsilon) = \# \tilde{K}_\upsilon^+ = q_\upsilon = p^{f_\upsilon}$$

$$\text{Συνεπώς έχουμε,} \quad \# \frac{E(K_\upsilon)}{E^{(1)}(K_\upsilon)} \ \mid \ 2^2 \cdot 3 \cdot p^{f_\upsilon}$$

   Μάλιστα το f, μπορεί να αντικατασταθεί με 2, διότι η $\tilde{K_\upsilon}^+$, είναι στοιχειώδης αβελιανή p-ομάδα και όπως γνωρίζουμε το p-torsion κομμάτι της $E(K_\upsilon)$ είναι της μορφής $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

$$\text{Επομένως,} \quad \# \frac{E(K_\upsilon)}{E^{(1)}(K_\upsilon)} \ \mid \ 2^2 \cdot 3 \cdot p^2$$

$$\text{Αρα έχουμε,} \quad \# E_{tor}(K) \ \mid \ \# \frac{E(K_\upsilon)}{E^{(0)}(K_\upsilon)} \cdot p^{2+2t} \leq 4 \cdot p^{2+2t}.$$

   Τέλος για $p = 2$:

$$\# E_{tor}(K) \ \mid \ \# \frac{E(K_\upsilon)}{E^{(0)}(K_\upsilon)} \cdot p^{2+2t} \ \mid \ 3 \cdot 4 \cdot 2^{2+2t} = 3 \cdot 2^{4+2t}.$$

Για $p = 3$:

$$\#E_{tor}(K) \ | \ 4 \cdot 3 \cdot 3^{2+2t} = 4 \cdot 3^{3+2t}$$

Και για $p = 5$:

$$\#E_{tor}(K) \ | \ 4 \cdot 3 \cdot 5^{2+2t}$$

3. Εστω ότι η ελλειπτική καμπύλη E έχει αναγωγή πολλαπλασιαστικού τύπου modulo π. Τότε γνωρίζουμε ότι υπάρχει καμπύλη του Tate E_q, η οποία είναι ισόμορφη με την E, σε τετραγωνική επέκταση του K_υ, έστω L. Επίσης ισχύει ότι η τάξη της ομάδος $E_q(L)/E_q^{(0)}(L)$, είναι $|\upsilon(j)|$. Ομως $E(K_\upsilon) \subset E(L) \cong E_q(L)$. Συνεπώς έχουμε την εξης εμφύτευση στις ομάδες πηλίκα:

$$\frac{E(K_\upsilon)}{E^{(0)}(K_\upsilon)} \hookrightarrow \frac{E(L)}{E^{(0)}(L)}.$$

Αρα η τάξη της ομάδος $E(K_\upsilon)/E^{(0)}(K_\upsilon))$, διαιρεί τον $|\upsilon(j)|$. Επίσης:

$$\#\frac{E^{(0)}(K_\upsilon)}{E^{(1)}(K_\upsilon)} = \#\tilde{E}_{ns}(\tilde{K}_\upsilon).$$

Αν είχαμε διαχωριζομένη πολλαπλασιαστική αναγωγή (δηλαδή οι κλίσεις των εφαπτομένων στον κόμβο ανήκαν στο σώμα $\tilde{K}_\upsilon$) τότε θα ίσχυε ότι $\tilde{E}_{ns}(\tilde{K}_\upsilon) \cong \tilde{K}_\upsilon^*$. Συνεπώς όταν η E έχει αναγωγή πολλαπλασιαστικού τύπου, διαχωριζομένη ή μη, πάντοτε ισχύει:

$$\tilde{E_{ns}}(\tilde{K}_\upsilon) \subset \tilde{K}_\upsilon(\sqrt{t})^* \cong (\bigoplus_{i=1}^{2f_\upsilon} \mathbb{Z}/p\mathbb{Z})^*,$$

όπου η $\tilde{K}_\upsilon(\sqrt{t})$ είναι τετραγωνική επέκταση του σώματος $\tilde{K}_\upsilon$. Ομως η τάξη της ομάδας $(\oplus_{i=1}^{2f}\mathbb{Z}/p\mathbb{Z})^*$ είναι $p^{2f_\upsilon} - 1$. Επομένως η τάξη της ομάδος $\tilde{E}_{ns}(\tilde{K}_\upsilon)$, διαιρεί τον αριθμό $p^{2f_\upsilon} - 1$.

$$\text{Αρα,} \quad \#E_{tor}(K) \ | \ |\upsilon(j)| \cdot (p^{2f_\upsilon} - 1) \cdot p^{2t}. \ \square$$

4.2 $\mathcal{S}$-μονάδες και ιδιάζουσες $\mathcal{S}$-μονάδες

Εστω Σ_K, το σύνολο όλων των θέσεων του K, και $\mathcal{C}$ ένα πεπερασμένο υποσύνολο του Σ_K που να περιέχει τις άπειρες θέσεις του K. Ορίζουμε $\mathcal{S} := \Sigma_K - \mathcal{C}$ και συμβολίζουμε με $O(\mathcal{S})$ τον δακτύλιο των $\mathcal{S}$-ακεραίων του σώματος K (δηλαδή τον δακτύλιο που περιέχει στοιχεία $a \in K$ τέτοια ώστε $\upsilon(a) \geq 0$, για κάθε $\upsilon \in \mathcal{S}$) και με $U(\mathcal{S})$, την ομάδα των $\mathcal{S}$-μονάδων του δακτυλίου $O(\mathcal{S})$. Θεμελιώδους σημασίας είναι το θεώρημα των Dirichlet-Hasse-Chevalley ([Wei]):

Θεώρημα 4.2 $\mathcal{S}$- K . :

$$U(\mathcal{S}) \cong W \bigoplus \mathbb{Z}^{s-1}$$

W K $s := \#\mathcal{C}$.

Ορισμός 4.3 ϵ K, $\mathcal{S}$-, $\gamma \in K^*$, $\epsilon, \epsilon - \gamma \in U(\mathcal{S})$. ϵ $\mathcal{S}$-, $\mathcal{S}$- $\gamma = 1$.

Αποδεικνύεται το εξής θεώρημα (δες αποδεικτική διαδικασία του θεωρήματος 4.1, [Si1], σελ. 253) :

Θεώρημα 4.4 K . :

$$\alpha \mathrm{X}^3 + \beta Y^3 = \gamma, \quad \alpha, \beta, \gamma \in K^*$$

$(x, y) \in U(\mathcal{S})^2$.

Σαν συνέπεια έχουμε το ακόλουθο:

Θεώρημα 4.5 $\mathcal{S}$-, $\gamma \in K^*$, , .

<u>Απόδειξη :</u> Κατ' αρχήν γράφουμε:

$$\gamma = \epsilon + [-(\epsilon - \gamma)]$$

Δηλαδή οδηγούμαστε σε εξίσωση της μορφής $\epsilon + \epsilon' = \gamma$ (1), όπου $\epsilon, \epsilon' \in U(\mathcal{S})$. Αρκεί λοιπόν να αποδείξουμε ότι η εξίσωση (1) έχει πεπερασμένου πλήθους λύσεις $\epsilon, \epsilon' \in U(\mathcal{S})$.

Από το θεώρημα των Dirichlet-Hasse-Chevalley, έχουμε ότι υπάρχουν $s-1$ ελεύθεροι γεννήτορες $\eta_1, \eta_2, \cdots, \eta_{s-1}$ και ρίζες της μονάδος ζ, ζ', τέτοια ώστε:

$$\epsilon = \zeta \eta_1^{\rho_1} \cdots \eta_{s-1}^{\rho_{s-1}}$$

$$\epsilon' = \zeta' \eta_1^{r_1} \cdots \eta_{s-1}^{r_{s-1}}, \qquad (\rho_i, r_j \in \mathbb{Z}).$$

Εστω $\rho_i = \mu_i + 3\kappa_i$ και $r_j = \nu_j + 3\lambda_j$, όπου $0 \leq \mu_i,\, \nu_j \leq 2$, $i, j = 1, \cdots, s-1$. Θέτουμε:

$$\alpha := \zeta \eta_1^{\mu_1} \cdots \eta_{s-1}^{\mu_{s-1}}, \qquad \beta := \zeta' \eta_1^{\nu_1} \cdots \eta_{s-1}^{\nu_{s-1}}$$

$$x := \eta_1^{\kappa_1} \cdots \eta_{s-1}^{\kappa_{s-1}}, \qquad y := \eta_1^{\lambda_1} \cdots \eta_{s-1}^{\lambda_{s-1}}$$

Για $i, j \in \{1, \cdots, s-1\}$, αφήνουμε τα μ_i, ν_j να πάρουν όλες τις δυνατές τιμές στις δύο πρώτες εξισώσεις. Τότε η εξίσωση (1), μπορεί να αντικατασταθεί από $3^{2(s-1)}$ εξιοώσεις της μορφής:

$$\alpha X^3 + \beta Y^3 = \gamma \qquad (2).$$

Αν το πλήθος των ριζών της μονάδος του σώματος K είναι w τότε αφήνοντας τα ζ, ζ', να διατρέχουν το σύνολο των ριζών της μονάδος, παίρνουμε συνολικά $w^2 3^{2(s-1)}$, εξιοώσεις του τύπου της (2). Σύμφωνα όμως με το θεώρημα 4.4 οι εξισώσεις αυτής της μορφής έχουν πεπερασμένες το πλήθος λύσεις στο σύνολο των $\mathcal{S}$-μονάδων. $\square$

4.3 Παραμετρίσεις

Εστω E ελλειπτική καμπύλη ορισμένη σε ένα αλγεβρικό σώμα αριθμών K, με εξίσωση:

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

Απαιτούμε τα εξής:

1. $P = (0, 0) \in E_{tor}(K)$.

2. Η τάξη του σημείου P δεν είναι 2 ή 3.

3. Η ευθεία $Y = 0$, εφάπτεται της E στο σημείο P.

Κάνοντας στοιχειώδεις λογαριασμούς έχουμε αντίστοιχα:

1. $a_6 = 0$

2. $a_2 \neq 0$, $a_3 \neq 0$

3. $a_3 \neq 0$, $a_4 = 0$

Επομένως μπορούμε να κάνουμε τον εξής μετασχηματισμό:

$$X \mapsto (\frac{a_2}{a_3})^2 X, \quad Y \mapsto (\frac{a_2}{a_3})^3 Y$$

Επίσης θέτουμε:

$$1 - c := \frac{a_1 a_2}{a_3}, \quad -b := \frac{a_2^3}{a_3^2} (\neq 0)$$

Η νέα εξίσωση της E, είναι:

$$E(b,c) : Y^2 + (1-c)XY - bY = X^3 - bX^2 \quad (b, c \in K),$$

η οποία ονομάζεται $E(b,c)$-μορφή του Kubert. Για λόγους συντομίας θέτουμε $\theta := 1 - c$. Η διακρίνουσα και η απόλυτη αναλλοίωτος της $E(b,c)$, είναι:

$$\Delta(b,c) = b^3(\theta^4 - \theta^3 - 8\theta^2 b + 36\theta b + 16b^2 - 27b), \quad j(b,c) = \frac{[(\theta^2 - 4b)^2 + 24\theta b]^3}{\Delta(b,c)}$$

Οι παραπάνω παραμετρίσεις ισχύουν όταν η ελλειπτική καμπύλη E, πληροί τις προυποθέσεις 1., 2., 3.

Εαν το σημείο $P = (0,0)$, είναι τάξης 3, ισχύει ότι $a_3 \neq 0$, διότι εάν $a_3 = 0$ τότε $P = -P \Rightarrow 2P = 0$, που είναι άτοπο διότι το σημείο P έχει τάξη 3. Κάνοντας μάλιστα τον μετασχηματισμό:

$$Y \mapsto Y + (\frac{a_2}{a_3})X, \quad X \mapsto X,$$

η εξίσωση της ελλειπτικής καμπύλης E, είναι της μορφής:

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2$$

Ομως $3P = O \Leftrightarrow 2P = -P \Leftrightarrow x(P) = x(2P)$ και αφού $P = (0,0)$, έπεται ότι $0 = -\frac{b_8}{b_6}$, δηλαδή $b_8 = 0$ και ισοδύναμα $a_2 a_3^2 = 0 \Leftrightarrow a_2 = 0$. Αρα μία ελλειπτική καμπύλη E, η οποία έχει σημείο τάξης 3, δέχεται την ακόλουθη παραμέτριση:

$$E : Y^2 + a_1 XY + a_3 Y = X^3, \quad a_3 \neq 0.$$

Εστω τώρα Σ_K, το σύνολο όλων των θέσεων του σώματος K και $\mathcal{C}$ ένα πεπερασμένο υποσύνολο του Σ_K που περιέχει και τις άπειρες θέσεις του σώματος K. Θέτουμε $\mathcal{S} := \Sigma_K - \mathcal{C}$. Ισχύει το εξής πολύ βασικό θεώρημα :

Θεώρημα 4.6 E K, $\mathcal{S}$- j. E, $P=(0,0)$, :

1. $E_{tor}(K) \supseteq \mathbb{Z}/2\mathbb{Z}$, E :

$$E: Y^2 = X(X^2 + a_2X + a_4), \quad a_2, a_4 \in K, \quad a_4 \neq 0$$

twist E :

$$E_d: Y^2 = X(X^2 + a_2dX + a_4d^2), \quad d \in K^*$$

$d := a_2^{-1}$. $c := \frac{a_2^2}{a_4}$, $b := c-4$ $e := 16b$, $j = \frac{(e+16)^3}{e}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow 0 \leq \mathfrak{v}(e) \leq 12\mathfrak{v}(2), \forall \mathfrak{v} \in \mathcal{S}$$

2. $E_{tor}(K) \supseteq \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$, E :

$$E: Y^2 = X(X+r)(X+s), \quad r,s \in K, \quad r \neq s, \quad r,s \neq 0$$

E , :

$$E': Y^2 = aX(X-1)(X-\mu), \quad a \in K^*, \quad \mu \in K^* - \{1\}$$

$e := 2^4 \cdot \mu$, $j = \frac{(2^8 - 2^4 \cdot e + e^2)^3}{e^2(2^4 - e)}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) \quad 0 \leq \mathfrak{v}(e) \leq 8\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) \quad 0 \leq \mathfrak{v}(e-16) \leq 8\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

3. $E_{tor}(K) \supseteq \mathbb{Z}/4\mathbb{Z}$, E :

$$E: Y^2 + XY - bY = X^3 - bX^2, \quad b \in K^*$$

$e := b^{-1}$, $j = \frac{[e(e+16)+16]^3}{e(e+16)}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) \quad 0 \leq \mathfrak{v}(e) \leq 8\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) \quad 0 \leq \mathfrak{v}(e+16) \leq 8\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

4. $E_{tor}(K) \supseteq \mathbb{Z}/8\mathbb{Z}$, E :

$$E: Y^2 + (1-c)XY - bY = X^3 - bX^2, \quad b \in K^*, \quad c \in K$$

$c=(2d-1)(d-1)d^{-1},\quad b=cd.\quad e:=d^{-1},\quad :$

$$j=\frac{(e^8-16e^7+96e^6-288e^5+480e^4-488e^3+224e^2-64e+16)^3}{e^2(2-e)^4(1-e)^8(e^2-8e+8)}$$

:

$$j\in O(\mathcal{S})\Longrightarrow\begin{cases}(1)\quad 0\le \mathfrak{v}(e)\le \frac{5}{2}\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\\ (2)\quad 0\le\mathfrak{v}(2-e)\le 2\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\\ (3)\quad (1-e)\in U(\mathcal{S}) & \\ (4)\quad 0\le\mathfrak{v}(e^2-8e+8)\le 5\mathfrak{v}(2) & \mathfrak{v}|2,\ \mathfrak{v}\in\mathcal{S}\end{cases}$$

5. $E_{tor}(K)\supseteq\mathbb{Z}/2\mathbb{Z}\bigoplus\mathbb{Z}/4\mathbb{Z},\quad E\quad :$

$$E:Y^2(X^2+2(a^2+1)X+(a^2-1)^2),\qquad a\in K^*-\{\pm1\}$$

$e:=4a,\quad j=\frac{(256e^2+(e^2-16)^2)^3}{e^2(e^2-16)^4}.\quad :$

$$j\in O(\mathcal{S})\Longleftrightarrow\begin{cases}(1)\quad 0\le\mathfrak{v}(e)\le 4\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\\ (2)\quad 0\le\mathfrak{v}(e^2-16)\le 8\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\end{cases}$$

6. $E_{tor}(K)\supseteq\mathbb{Z}/4\mathbb{Z}\bigoplus\mathbb{Z}/4\mathbb{Z},\quad E\quad :$

$$E:Y^2=X(X^2+(2(a^2+1)X+(a^2-1)^2),\qquad a\in K^*-\{\pm1\}$$

$\sqrt{-1},\quad \sqrt{a}\in K.\quad e:=4a,\quad j=\frac{(256e^2+(e^2-16)^2)^3}{e^2(e^2-16)^4}.\ :$

$$j\in O(\mathcal{S})\Longleftrightarrow\begin{cases}(1)\quad 0\le\mathfrak{v}(e)\le 4\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\\ (2)\quad 0\le\mathfrak{v}(e^2-16)\le 8\mathfrak{v}(2) & \forall\mathfrak{v}\in\mathcal{S}\end{cases}$$

7. $E_{tor}(K)\supseteq\mathbb{Z}/2\mathbb{Z}\bigoplus\mathbb{Z}/8\mathbb{Z},\quad E\quad :$

$$E:Y^2+(1-c)XY-bY=X^3-bX^2,\qquad b\in K^*,\qquad c\in K$$

:

$$c=(2d-1)(d-1)d^{-1},\quad b=cd,\quad d=a(8a+2)(8a^2-1)^{-1}$$

$d(d-1)(2d-1)(8d^2-8d+1)\neq 0.$

$$j=\frac{\{[(1-c)^2-4b]^2+24b(1-c)\}^3}{b^3\{[(1-c)^2-4b]^2+8(1-c)^3-27b-9(1-c)[(1-c)^2-4b]\}}$$

:

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) & -2\mathfrak{v}(2) \le \mathfrak{v}(a) \le 0 & \forall \mathfrak{v} \in \mathcal{S} \\ (2) & \mathfrak{v}(8a+2) = \mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (3) & -\mathfrak{v}(2) \le \mathfrak{v}(2a+1) \le 2 & \forall \mathfrak{v} \in \mathcal{S} \\ (4) & -\mathfrak{v}(2) \le \mathfrak{v}(8a^2-1) \le \frac{7}{2}\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

8. $E_{tor}(K) \supseteq \mathbb{Z}/3\mathbb{Z}$, E :

$$E : Y^2 + cXY + c^2Y = X^3, \quad c \in K^*$$

$e := c - 27$, $j = \frac{(e+27)(e+3)^3}{e}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow 0 \le \mathfrak{v}(e) \le 6\mathfrak{v}(3), \quad \forall \mathfrak{v} \in \mathcal{S}$$

9. $E_{tor}(K) \supseteq \mathbb{Z}/9\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - bY = X^3 - bY, \quad b \in K^*, \ c \in K$$

$c = f(d-1)$, $f \in K$, $d = f(f-1)+1$, $b = cd$, :

$$j = \frac{\{[(1-c)^2 - 4b]^2 + 24b(1-c)\}^3}{b^3\{[(1-c)^2-4b]^2 + 8(1-c)^3 - 27b - 9(1-c)[(1-c)^2-4b]\}}$$

:

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) & f \in U(\mathcal{S}) \\ (2) & f-1 \in U(\mathcal{S}) \end{cases} ,$$

10. $E_{tor}(K) \supseteq \mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}/3\mathbb{Z}$, E :

$$E : Y^2 = X^3 + AX + B, \quad a, b \in K$$

$-A = 3a(a^3+8)$, $-B = 2(a^6 - 20a^3 - 8)$ $\sqrt{-3} \in K$. $e := 3a$, :

$$j = \left(\frac{e[(e-3)(e^2+3e+9)+3^5]}{(e-3)(e^2+3e+9)}\right)^3$$

:

$$j \in O(\mathcal{S}) \Longrightarrow \begin{cases} (1) & e \in O(\mathcal{S}) \\ (2) & \mathfrak{v}(e^3-27) \le 6\mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \\ (3) & \mathfrak{v}(e-3) \le 3\mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

11. $E_{tor}(K) \supseteq \mathbb{Z}/6\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - c(c+1)Y = X^3 - c(c+1)X^2, \quad c \in K^* - \{\pm 1\}$$

$e := c^{-1}$, $j = \frac{((1+e)^3(9+e)-16e)^3}{e^2(1+e)^3(9+e)}$. :

$$j \in O(\mathcal{S} \Longleftrightarrow \begin{cases} (1) & 0 \le \mathfrak{v}(e) \le 2\mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) & 0 \le \mathfrak{v}(1+e) \le 3\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (3) & \mathfrak{v}(9+e) = 0 & \mathfrak{v} \quad 6 \;\; \mathfrak{v} \in \mathcal{S} \\ (4) & \mathfrak{v}(9+e) = \mathfrak{v}(1+e) & \mathfrak{v}|2, \quad \mathfrak{v} \in \mathcal{S} \\ (5) & \mathfrak{v}(9+e) = \theta(e) & \mathfrak{v}|3, \quad \mathfrak{v} \in \mathcal{S} \end{cases}$$

12. $E_{tor}(K) \supseteq \mathbb{Z}/12\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - bY = X^3 - bY, \quad b \in K^*, \;\; c \in K$$

$d = m + t$, $f = m(1-t)^{-1}$, $c = f(d-1)$, $b = cd$, $m = (3t - t^2 - 1)(t-1)^{-1}$.
$e := t^{-1}$, :

$$j = \frac{\{[(1-c)^2 - 4b]^2 + 24b(1-c)\}^3}{b^3\{[(1-c)^2 - 4b]^2 + 8(1-c)^3 - 27b - 9(1-c)[(1-c)^2 - 4b]\}}$$

:

$$j \in O(\mathcal{S}) \Longrightarrow \begin{cases} (1) & 0 \le \mathfrak{v}(e) \le \mathfrak{v}(2) + \frac{1}{2}\mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) & e - 1 \in U(\mathcal{S}) & \\ (3) & \mathfrak{v}(e-2) = 0 & \mathfrak{v} \quad 2 \;\; \mathfrak{v} \in \mathcal{S} \\ (4) & \mathfrak{v}(e-2) = \mathfrak{v}(e) & \mathfrak{v}|2, \; \mathfrak{v} \in \mathcal{S} \end{cases}$$

13. $E_{tor}(K) \supseteq \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/6\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - bY = X^3 - bX^2, \quad b \in K^*, c \in K^* - \{1\}$$

$b = c(1+c)$, $c = (10-2a)(a^2-9)^{-1}$. E :

$$j = \frac{\{[(1-c)^2 - 4b]^2 + 24b(1-c)\}^3}{b^3\{[(1-c)^2 - 4b]^2 + 8(1-c)^3 - 27b - 9(1-c)[(1-c)^2 - 4b]\}}$$

$c = -2\frac{a-5}{(a+3)(a-3)}$ $b = -2\frac{(a-5)(a-1)^2}{(a+3)^2(a-3)^2}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) \quad \mathfrak{v}(2) \leq \mathfrak{v}(a+3) \leq 3\mathfrak{v}(2) + \mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) \quad \mathfrak{v}(2) \leq \mathfrak{v}(a-3) \leq \mathfrak{v}(2) + \mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \\ (3) \quad \mathfrak{v}(2) \leq \mathfrak{v}(\alpha-1) \leq 3\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (4) \quad \mathfrak{v}(2) \leq \mathfrak{v}(a-5) \leq 3\mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (5) \quad \mathfrak{v}(2) \leq \mathfrak{v}(a-9) \leq 3\mathfrak{v}(2) + \mathfrak{v}(3) & \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

14. $E_{tor}(K) \supseteq \mathbb{Z}/5\mathbb{Z}$, E :

$$E : Y^2 + (1-b)XY - bY = X^3 - bX^2, \quad b \in K^*$$

$j = \frac{((b^2-11b-1)^2+5b(2((b^2-11b-1)+b)^3}{b^5(b^2-11b-1)}$. :

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) \quad b \in U(\mathcal{S}) \\ (2) \quad \mathfrak{v}(b^2 - 11b - 1) \leq 3\mathfrak{v}(5) \quad \forall \mathfrak{v} \in \mathcal{S} \end{cases}$$

15. $E_{tor}(K) \supseteq \mathbb{Z}/10\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - bY = X^3 - bX^2, \quad b \in K^*, \ c \in K$$

$b = cd$, $c = f(d-1)$, $d = f^2(f-(f-1)^2)^{-1}$, $f \in K^*$. $e := f^{-1}$. E, :

$$j = \frac{\{[(1-c)^2 - 4b]^2 + 24b(1-c)\}^3}{b^3\{[(1-c)^2-4b]^2 + 8(1-c)^3 - 27b - 9(1-c)[(1-c)^2-4b]\}}$$

$c, d-1, b,$ (e):

$$c = \frac{(e-1)(e-2)}{e(e-(1-e)^2)}, \quad d - 1 = \frac{(e-1)(e-2)}{e-(1-e)^2}, \quad b = \frac{(e-1)(e-2)}{e(e-(1-e)^2)^2}$$

:

$$j \in O(\mathcal{S}) \Longrightarrow \begin{cases} (1) \quad 0 \leq \mathfrak{v}(e) \leq \mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (2) \quad 0 \leq \mathfrak{v}(e-2) \leq \mathfrak{v}(2) & \forall \mathfrak{v} \in \mathcal{S} \\ (3) \quad (1-e) \in U(\mathcal{S}) \end{cases}$$

16. $E_{tor}(K) \supseteq \mathbb{Z}/7\mathbb{Z}$, E :

$$E : Y^2 + (1-c)XY - bY = X^3 - bY, \quad b \in K^*, c \in K$$

$b = d^2(d-1)$, $c = d(d-1)$, $d \in K^* - \{1\}$. E, :

$$j = \frac{(d^8 - 12d^7 + 42d^6 - 56d^5 + 35d^4 - 14d^2 + 4d + 1)^3}{d^7(d-1)^7(d^3 - 8d^2 + 5d + 1)}$$

:

$$j \in O(\mathcal{S}) \Longrightarrow \begin{cases} (1) \quad d \in U(\mathcal{S}) \\ (2) \quad d - 1 \in U(\mathcal{S}) \end{cases}$$

17. $E_{tor}(K) \supseteq \mathbb{Z}/11\mathbb{Z}$, E :

$$E : X^2 + (1-c)XY - bY = X^3 - bX^2, \quad b \in K^*, c \in K$$

:

$$b = cr, \quad r = r_1 + 1, \quad r_1 = 1/r_2, \quad r_2 = 1/V, \quad U = \frac{1}{4}U_2$$

$$c = s(r-1), \quad s = s_1 + 1, \quad s_1 = 1/s_2, \quad s_2 = U/V, \quad V = \frac{1}{8}V_2 - \frac{1}{2}$$

E, :

$$j = \frac{\{[(1-c)^2 - 4b]^2 + 24b(1-c)\}^3}{b^3\{[(1-c)^2 - 4b]^2 + 8(1-c)^3 - 27b - 9(1-c)[(1-c)^2 - 4b]\}}$$

$b, c,$ V_2, U_2 :

$$c = \frac{1}{16U_2}(V_2 - 4 + 2U_2)(V_2 - 4), \quad b = \frac{1}{8}c(V_2 + 4).$$

:

$$j \in O(\mathcal{S}) \Longrightarrow \begin{cases} (1) \quad 0 \le \upsilon(U_2) \le 2\upsilon(2) & \forall \upsilon \in \mathcal{S} \\ (2) \quad 0 \le \upsilon(U_2 - 4) \le 2\upsilon(2) & \forall \upsilon \in \mathcal{S} \\ (3) \quad \upsilon(V_2 - 4) = \frac{3}{2}\upsilon(U_2) & \forall \upsilon \in \mathcal{S} \\ (4) \quad \upsilon(V_2 + 4) = \frac{3}{2}\upsilon(U_2) & \forall \upsilon \in \mathcal{S} \\ (5) \quad \upsilon(V_2 - 4 + 2U_2) = \frac{3}{2}\upsilon(U_2) & \forall \upsilon \in \mathcal{S} \end{cases}$$

Απόδειξη : Θα αποδείξουμε μόνο την περίπτωση 3. Ολες οι άλλες αποδεικνύονται με όμοιο τρόπο. Σημειώνουμε ότι περιπτώσεις $1-3$, $5, 6$, $8-12$, 14 και 16 αποδεικνύονται στο [Mu], και οι υπόλοιπες στο [Str].

Εστω E/K ελλειπτική καμπύλη, η οποία περιέχει το σημείο $P = (0,0)$. Εστω δε ότι το σημείο P είναι τάξης 4. Συνεπώς η καμπύλη E δέχεται παραμέτριση της μορφής $E(b,c)$.

Εχουμε ότι $4P = 0$, δηλαδή $2P = -2P \Leftrightarrow (b, bc) = (b, 0)$. Ομως $b \neq 0$, επομένως $c = 0$. Αρα η E έχει εξίσωση της μορφής :

$$\mathrm{E} : Y^2 + XY - bY = X^3 - bX^2, \qquad b \in K^*$$

Αν θέσουμε $e := b^{-1}$, τότε εύκολα υπολογίζουμε ότι :

$$j = \frac{(e(e+16)+16)^3}{e(e+16)}$$

Εστω τώρα ότι $j \in O(\mathcal{S})$. Θα αποδείξουμε ότι τότε ισχύουν:

$$0 \leq \upsilon(e) \leq 8\upsilon(2) \tag{1}$$

$$0 \leq \upsilon(e+16) \leq 8\upsilon(2) \tag{2}$$

για κάθε θέση υ του $\mathcal{S}$. Εστω ότι δεν ισχύει ότι $0 \leq \upsilon(e)$ για όλες τις εκτιμήσεις υ του σώματος K, δηλαδή υπάρχει εκτίμηση υ του σώματος K τέτοια ώστε $\upsilon(e) < 0$. Παίρνουμε την πλήρωση του σώματος K, K_υ ως προς την διακριτή εκτίμηση υ. Εστω π ο γεννήτορας του μοναδικού μέγιστου ιδεώδους του δακτυλίου R. Τότε ο e γράφεται στην μορφή $e = \pi^{-k}u$, όπου ο k είναι φυσικός αριθμός $k \geq 1$ και ο u μονάδα του δακτυλίου των ακεραίων του σώματος K_υ. Αντικαθιστούμε τον e στην εξίσωση που μας δίνει την απόλυτη αναλλοίωτο και έχουμε:

$$j = \frac{(\pi^{-k}u(\pi^{-k}u+16)+16)^3}{\pi^{-k}u(\pi^{-k}u+16)} = \frac{(u(u+16\pi^k)+16\pi^{2k})^3}{\pi^{4k}u(u+16\pi^k)}$$

Ο αριθμητής του j είναι μονάδα του δακτυλίου των ακεραίων του σώματος K_υ και ο παρονομαστής ανήκει στο μέγιστο ιδεώδες που γεννάται από τον π, δηλαδή η απόλυτη αναλλοίωτος j δεν είναι ακεραία, $\upsilon(j) < 0$. Ατοπο, διότι $j \in O(\mathcal{S})$. Αρα πράγματι $0 \leq \upsilon(e)$.

Επίσης $0 \leq \upsilon(e+16)$, διότι $\upsilon(e+16) \geq \min\{\upsilon(e), \upsilon(16)\} \geq 0$.

Αποδεικνύουμε τώρα ότι αν $j \in O(\mathcal{S})$, τότε $\upsilon(e) \leq 8\upsilon(2)$. Εστω ότι δεν ισχύει, δηλαδή υπάρχει εκτίμηση υ τέτοια ώστε $\upsilon(e) > 8\upsilon(2)$. Επομένως $\upsilon(\frac{e}{2^8}) > 0$. Κάνουμε πλήρωση του K ως προς την εκτίμηση υ και έστω π ο γεννήτορας του μέγιστου ιδεώδους του δακτυλίου R. Τότε $\pi | \frac{e}{2^8}$. Εχουμε :

$$j = \frac{(e(e+16)+16)^3}{e(e+16)} = \frac{(1 + e(\frac{e}{2^8} \cdot 2^4 + 1))^3}{\frac{e}{2^8}(\frac{e}{2^8} \cdot 2^4 + 1)}$$

Ο αριθμητής του j είναι φανερά μονάδα του δακτυλίου των ακεραίων του σώματος K_υ, ενώ ο παρονομαστής ανήκει στο μέγιστο ιδεώδες που παράγεται από τον π. Αρα $\upsilon(j) < 0$, άτοπο. Εντελώς όμοια αποδεικνύεται ότι $\upsilon(e+16) \leq 8\upsilon(2)$.

Απομένει λοιπόν να αποδείξουμε το αντίστροφο. Εστω ότι υπάρχει εκτίμηση υ του σώματος K τέτοια ώστε $\upsilon(j) < 0$. Τότε αναγκαστικά η καμπύλη E θα έχει κακή αναγωγή (modulo π). Αυτό σημαίνει ότι $a_3 = -b \equiv 0 \pmod{\pi}$ ([Hus], παρατήρηση 7.1, σελ. 78), δηλαδή $\pi | b \Rightarrow \upsilon(b) > 0$. Ομως $e = b^{-1}$, και επομένως $\upsilon(e) < 0$, ατοπο. Αρα ισχύει η ζητούμενη ισοδυναμία. □

Σαν αποτέλεσμα των θεωρημάτων 4.5, 4.6, έχουμε το ακόλουθο:

Θεώρημα 4.7 K, $\mathcal{S}$- j $E_{tor}(K)$, :

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}/3\mathbb{Z}$$

$$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/11\mathbb{Z}$$

$\mathcal{S}$- $j \in K$, E/K $E_{tor}(K)$ *Klein* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Απόδειξη : Θα παρουσιάσουμε μόνο την περίπτωση όπου $E_{tor} \supseteq \mathbb{Z}/5\mathbb{Z}$. Ολες οι άλλες αποδεικνύονται με όμοιο τρόπο ([Str]). Αφού $E_{tor}(K) \supseteq \mathbb{Z}/5\mathbb{Z}$, η καμπύλη E έχει την εξής παραμέτριση (θεώρημα 4.16, περίπτωση 14):

$$E : Y^2 + (1-b)XY - bY = X^3 - bX^2, \quad b \in K^*$$

Θέτουμε $e := b$. Τότε ισχύει ότι:

$$j \in O(\mathcal{S}) \Longleftrightarrow \begin{cases} (1) & e \in U(\mathcal{S}) \\ (2) & 0 \leq \upsilon(e^2 - 11e - 1) \leq 3\upsilon(5) \quad \forall \upsilon \in \mathcal{S} \end{cases}$$

Αρκεί λοιπόν να αποδείξουμε ότι υπάρχουν μόνο πεπερασμένου πλήθους $e \in K^*$ που να ικανοποιούν τις σχέσεις (1) και (2). Θεωρούμε το σώμα $K' := K(\sqrt{5})$. Εστω $\mathcal{C}'$ ένα πεπερασμένο σύνολο θέσεων του K', που περιέχει τις επεκτάσεις των θέσεων του K οι οποίες ανήκουν στο $\mathcal{C}$ καθώς και τις θέσεις του K' που διαιρούν τον 5. Εστω δε $\mathcal{S}' := \Sigma_{K'} - \mathcal{C}'$. Στο σώμα K', έχουμε :

$$e^2 - 11e - 1 = [e - (\frac{11}{2} - \frac{5}{2}\sqrt{5})][e - (\frac{11}{2} + \frac{5}{2}\sqrt{5})].$$

Ομως λόγω της σχέσεως (1), ισχύει ότι $e \in U(\mathcal{S}')$. Επίσης $e - \frac{11}{2} \pm \frac{5}{2}\sqrt{5} \in U(\mathcal{S}')$, λόγω της σχέσεως (2) (διότι το $\mathcal{S}'$ δεν περιέχει θέσεις του K' που διαιρούν τον 5 και άρα $\upsilon(e^2 - 11e - 1) = 0$). Αρα το e είναι ιδιάζουσα $\mathcal{S}'$-μονάδα, ως προς $\frac{11}{2} \pm \frac{5}{2}\sqrt{5} \in (K')^*$. Επομένως σύμφωνα με το θεώρημα 4.5 έπεται ότι υπάρχουν μόνο πεπερασμένα το πλήθος e, που να ικανοποιούν τις σχέσεις (1) και (2). Αρα ισχύει το ζητούμενο. □

4.4 Ελλειπτικές καμπύλες ορισμένες σε " απλά " κυβικά σώματα αριθμών

Ορισμός 4.8 $\mathbb{Q}$ $K := \mathbb{Q}(\sqrt[3]{ab^2})$, a, b , .

Τα απλά κυβικά σώματα $\mathbb{Q}(\sqrt[3]{ab^2})$ και $\mathbb{Q}(\sqrt[3]{a^2b})$, προφανώς ταυτίζονται, συνεπώς χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι $a > b$. Επίσης το σύνολο $\{1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\}$, είναι μία $\mathbb{Q}$-βάση της επέκτασης $K/\mathbb{Q}$. Συνεπώς κάθε στοιχείο $x \in K$, γράφεται κατά μοναδικό τρόπο στην μορφή:

$$x = x_1 + x_2\sqrt[3]{ab^2} + x_3\sqrt[3]{a^2b}, \quad x_1, x_2, x_3 \in \mathbb{Q}.$$

Επίσης η norm ενός στοιχείου x στην επέκταση $K/\mathbb{Q}$, είναι:

$$N(x) := N_{K/\mathbb{Q}}(x) = x_1^3 + x_2^3ab^2 + x_3^3a^2b - 3x_1x_2x_3ab.$$

Ορισμός 4.9 $K = \mathbb{Q}(\sqrt[3]{ab^2})$, :

1. *Dedekind I*, $a \not\equiv \pm b \pmod 9$

2. *Dedekind II*, $a \equiv \pm b \pmod 9$

Σκοπός μας είναι ο πλήρης προσδιορισμός όλων των ελλειπτικών καμπύλων E με ακέραια απόλυτη αναλλοίωτο j και μη-τετριμμένη υποομάδα πεπερασμένης τάξης $E_{tor}(K)$, σε απλά κυβικά σώματα αριθμών. Προς αυτήν την κατεύθυνση θα μας χρειαστεί η γνώση της αριθμητικής των απλών κυβικών σωμάτων αριθμών. Ισχύει το εξής θεώρημα ([Na]):

Θεώρημα 4.10 $K = \mathbb{Q}(\sqrt[3]{ab^2})$. :

1. K *Dedekind I*, K :

$$\{1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\}$$

$x \in O_K$, :

$$x = x_1 + x_2\sqrt[3]{ab^2} + x_3\sqrt[3]{a^2b}, \quad x_1, x_2, x_3 \in \mathbb{Z}$$

K, $\Delta_K = -3(3ab)^2$.

2. K *Dedekind II*, K :

$$\{\gamma, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\},$$

γ $\gamma = \frac{1}{3}(1 + a\sqrt[3]{ab^2} + b\sqrt[3]{a^2b})$. $x \in O_K$, :

$$x = \frac{1}{3}(x_1 + x_2\sqrt[3]{ab^2} + x_3\sqrt[3]{a^2b})$$

$x_1, x_2, x_3 \in \mathbb{Z}$ $x_1 \equiv ax_2 \equiv bx_3 \pmod 3$. K, $\Delta_K = -3(ab)^2$.

Αποδεικνύουμε το εξής:

Θεώρημα 4.11 $K = \mathbb{Q}(\sqrt[3]{ab^2})$, . p $\mathbb{Q}$, K :

1. p $3ab$, :

$$p \cdot O_K = \begin{cases} (1) \quad P_1P_2 & p \equiv -1 \pmod 3 \\ (2) \quad P_1P_2P_3 & p \equiv 1 \pmod 3\ ,\ ab^2 \quad \textit{modulo } p \\ (3) \quad P & p \equiv 1 \pmod 3\ ,\ ab^2 \quad \textit{modulo } p \end{cases}$$

(1) $N(P_1) = p$, $N(P_2) = p^2$, (2), $N(P_1) = N(P_2) = N(P_3) = p$, (3) $N(P) = p^3$.

2. $p \mid ab$, $p \cdot O_K = P^3$, $N(P) = p$.

3. $p = 3$ $ab \not\equiv 0 mod 3$, :

$$3 \cdot O_K = \begin{cases} (1) \quad P^3 & K \quad \textit{Dedekind I} \\ (2) \quad P_1^2P_2 & K \quad \textit{Dedekind II} \end{cases}$$

$N(P) = 3$ $N(P_1) = N(P_2) = 3$.

Απόδειξη :

1. Αν $p \equiv -1 \pmod 3$, τότε ο 3 δεν διαιρεί τον $p-1$, επομένως $d := (3, p-1) = 1$. Ομως η ισοδυναμία $x^3 - ab^2 \equiv 0 \pmod p$, έχει λύση ανν $(ab^2)^{\frac{p-1}{d}} \equiv 1 \pmod p$ ([Ir-Ro], πρόταση 7.1.2, σελ. 80), το οποίο ισχύει διότι $d = 1$. Επιπλέον η ισοδυναμία $x^3 - ab^2 \equiv 0 \pmod p$, έχει μία μόνο λύση, διότι $d = 1$. Συνεπώς το πολυώνυμο $x^3 - ab^2$, αναλύεται modulo p σε έναν πρωτοβάθμιο και σε έναν δευτεροβάθμιο όρο. Αρα ο πρώτος αριθμός p αναλύεται στο σώμα K σε δύο πρώτα ιδεώδη P_1, P_2, τέτοια ώστε $N(P_1) = p$ και $N(P_2) = p^2$.

   Εστω τώρα $p \equiv 1 \pmod 3$. Τότε προφανώς ο πρώτος αριθμός p αναλύεται σε δύο πρώτα ιδεώδη στον δακτύλιο $\mathbb{Z}[\omega]$, ($\omega = e^{\frac{2\pi i}{3}}$) έστω Q, Q'. Επομένως η ισοδυναμία $x^3 - ab^2 \equiv 0 mod p$ είναι επιλύσιμη ανν είναι επιλύσιμη modulo Q, δηλαδή ανν το κυβικό σύμβολο $(\frac{ab^2}{Q})_3$ ισούται με 1 ([Ir-Ro], πρόταση 9.3.3, σελ. 112). Ισοδύναμα αυτό ισχύει εάν και μόνο εάν $(ab^2)^{\frac{p-1}{3}} \equiv 1 mod Q$. Συνεπώς αν το ab^2 είναι κυβικό υπόλοιπο modulo p, τότε έχουμε τρεις ακριβώς λύσεις της ισοδυναμίας, διότι $d = 3$, ενώ αν το ab^2 δεν είναι κυβικό υπόλοιπο modulo p τότε η ισοδυναμία δεν είναι επιλύσιμη. Αρα όταν ο ab^2 είναι κυβικό υπόλοιπο modulo p τότε ο πρώτος αριθμός p αναλύεται σε τρία πρώτα ιδεώδη του σώματος K, ενώ όταν ο ab^2 δεν είναι κυβικό υπόλοιπο modulo p, τότε ο p αδρανεί στο σώμα K (με βαθμό αδρανείας 3).

2. Αν ο πρώτος αριθμός p διαιρεί τον ab τότε και στην περίπτωση τύπου Dedekind I και στην περίπτωση τύπου Dedekind II, ο p διαιρεί την διακρίνουσα του σώματος K. Συνεπώς διακλαδίζεται στο σώμα K. Επιπλέον $x^3 - ab^2 \equiv x^3 \pmod p$, αφού $p | ab$. Συνεπάγεται ότι ο πρώτος αριθμός p διακλαδίζεται πλήρως ([Av3]). Αρα ισχύει το ζητούμενο.

3. Αν $p = 3$ και $ab \not\equiv 0 mod 3$, τότε ο $p = 3$ διακλαδίζεται διότι διαιρεί την διακρίνουσα του σώματος και στις δύο περιπτώσεις τύπου Dedekind I και II. Στην περίπτωση τύπου Dedekind I ο 3 δεν περιέχεται στον οδηγό του σώματος K, ενώ στην περίπτωση τύπου Dedekind II περιέχεται στον οδηγό του K. Αρα στην περίπτωση Dedekind I πράγματι $3 \cdot O_K = P^3$, όπου το P είναι πρώτο ιδεώδες του σώματος K. Στην περίπτωση Dedekind II παίρνουμε το στοιχείο $\theta_0 := \frac{1}{3}(1 + ab^2 + a^2b^3) \in K$, και με απλούς λογαριασμούς

βλέπουμε ότι το ανάγωγο πολυώνυμο του θ_0 υπέρ το $\mathbb{Q}$ είναι το:

$$f(X) := X^3 - X^2 + \frac{1}{9}(1-ab)X - \frac{1}{27}(1 - 3ab + a^2b + ab^2)$$

και ο δείκτης του θ_0 δεν είναι 0 modulo 3. Μάλιστα αναγάγοντας το $f(X)$ modulo 3, εύκολα διαπιστώνουμε ότι αναλύεται σε έναν πρωτοβάθμιο όρο και σε ένα τέλειο τετράγωνο. Αρα πράγματι ο πρώτος αριθμός p, έχει την ζητούμενη ανάλυση $p \cdot O_K = P_1^2 P_2$, όπου $N(P_1) = N(P_2) = 3$. $\square$

Ξαναγυρνούμε τώρα στις ελλειπτικές καμπύλες. Ισχύει το εξής θεώρημα :

Θεώρημα 4.12 E $K = \mathbb{Q}(\sqrt[3]{ab^2})$, j, :

$$\upsilon(j) \geq 0, \quad \upsilon \quad K, \quad \upsilon|2 \quad \upsilon|3 \ . \quad (1)$$

$E_{tor}(K)$, :

$$\{O\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$$

$$\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$$

Απόδειξη : Εστω υ θέση του σώματος K. Εστω δε ότι $\upsilon|2$ και π ο uniformizer που αντιστοιχεί στην θέση υ (αν κάνουμε την πλήρωση του σώματος K ως προς την θέση υ, K_υ). Λόγω του θεωρήματος 4.11 πάντα υπάρχει μία τέτοια θέση, τέτοια ώστε $N(\pi) = 2$. Ομοια για κάθε θέση υ που επεκτείνει την θέση που αντιστοιχεί στον πρώτο αριθμό 3, παίρνουμε έναν άλλο uniformizer π', τέτοιον ώστε $N(\pi') = 3$. Επομένως το θεώρημα του Hasse (υπόθεση του Riemann) μας δίνει ότι:

$$\#\tilde{E}(\tilde{K_\upsilon}) < 6 \quad (*)$$

αν η καμπύλη E έχει καλή αναγωγή modulo π για $\pi|2$. Επίσης :

$$\#\tilde{E}(\tilde{K_\upsilon}) < 8 \quad (**)$$

αν η E άχει καλή αναγωγή modulo π για $\pi|3$. Επιπλέον η υπόθεση (1) του παρόντος θεωρήματος μας περιορίζει σε ελλειπτικές καμπύλες που έχουν καλή ή προσθετική αναγωγή modulo π. Ξεχωρίζουμε τις εξής περιπτώσεις:

1. Εστω ότι η ελλειπτική καμπύλη E περιέχει σημείο με τάξη πρώτο αριθμό $p \geq 5$. Τότε η καμπύλη E έχει, λόγω του θεωρήματος 4.1, καλή αναγωγή όταν ο π διαιρεί τον 2 ή τον 3. Μάλιστα λόγω της σχέσεως $(*)$, έχουμε ότι $p = 5$. Διαλέγοντας λοιπόν $\pi|2$ τέτοιον ώστε $N(\pi) = 2$, τότε από το θεώρημα 4.1, έχουμε ότι $\#E_{tor}(K)|5 \cdot 2^4$ (a). Επίσης διαλέγοντας $\pi|3$ τέτοιον ώστε $N(\pi) = 3$), από το ίδιο θεώρημα και από την σχέση $(**)$ έχουμε ότι $\#E_{tor}(K)|5 \cdot 3^2$ (b). Οι σχέσεις (a) και (b), οδηγούν στην ισότητα $\#E_{tor}(K) = 5$.

2. Εστω τώρα ότι η ελλειπτική καμπύλη E δεν περιέχει σημείο τάξης πρώτο αριθμό $p \geq 5$. Τότε το θεώρημα 4.1, μας δίνει ότι:

$$\#E_{tor}(K)| \begin{cases} 2^8 \cdot 3 & \text{αν η } E \text{ έχει προσθετική αναγωγή στον } \pi|2 \;\; (i) \\ 2^2 \cdot 3^5 & \text{αν η } E \text{ έχει προσθετική αναγωγή στον } \pi|3 \;\; (ii) \end{cases}$$

Συνδιάζοντας τις σχέσεις $(*)$, $(**)$, (i) και (ii) , έχουμε την ακόλουθη σχέση διαίρεσης $\#E_{tor}(K)|2^2 \cdot 3$. Κάνοντας λοιπόν όλους του δυνατούς συνδιασμούς έχουμε το ζητούμενο. $\square$

Στα παρακάτω θα διερευνήσουμε ποιές από τις ομάδες πεπερασμένης τάξης που μας εξασφάλισε το θεώρημα $4,11$ εμφανίζονται πράγματι ως υποομάδες πεπερασμένης τάξης μιας ελλειπτικής καμπύλης E/K, όπου K ένα απλό κυβικό σώμα αριθμών. Επιπλέον θα προσδιορίσουμε όλα τα δυνατά σώματα K και τις ελλειπτικές καμπύλες E, με δοσμένη υποομάδα πεπερασμένης τάξης $E_{tor}(K)$.

Εστω $\mathcal{C}$ το σύνολο όλων των απείρων θέσεων του σώματος K και $\mathcal{S} := \Sigma_K - \mathcal{C}$. Εστω δε E ελλειπτική καμπύλη με $\mathcal{S}$-ακέραια απόλυτη αναλλοίωτο j, ορισμένη σε ένα απλό κυβικό σώμα αριθμών $K = \mathbb{Q}(\sqrt[3]{ab^2})$.

Κατ' αρχήν οι συνθήκες ακεραιότητος για την απόλυτη αναλλοίωτο j που προκύπτουν από το θεώρημα 4.6 , μετασχηματίζονται σε norm-εξισώσεις. Πράγματι, έστω p ένας πρώτος αριθμός. Τότε ο p έχει μοναδική ανάλυση σε γινόμενο πρώτων ιδεωδών του σώματος K. Εστω λοιπόν $pO_K = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$, $N(P_i) = p^{f_i}$ η norm του ιδεώδους P_i και f_i, ο βαθμός αδρανείας του P_i. Ισχύει ότι $\sum e_i f_i = n = [K : \mathbb{Q}]$. Ας συμβολίσουμε με υ_{P_i} την μη-αρχιμήδεια εκτίμηση που αντιστοιχεί στο πρώτο ιδεώδες P_i, και με υ_p αυτήν που αντιστοιχεί στον πρώτο αριθμό p. Ειναι προφανές ότι ισχύει $\forall e \in \mathbb{Q} - \{0\}, \;\; \upsilon_{P_i}(e) = e_i\upsilon_p(e)$ (i). Επίσης αν $e \in K - \{0\}$, τότε το κύριο ιδεώδες που παράγεται από τον e, έχει μοναδική ανάλυση σε γινόμενο πρώτων ιδεωδών του σώματος K. Εστω:

$$eO_K = Q_1^{s_1} \cdots Q_k^{s_k}$$

$$\Longrightarrow N_{K/\mathbb{Q}}(e) = N_{K/\mathbb{Q}}(Q_1)^{s_1} \cdots N_{K/\mathbb{Q}}(Q_k)^{s_k}$$
$$\Longrightarrow N_{K/\mathbb{Q}}(e) = p^{\sum s_i f_i}$$

Συνεπώς $\upsilon_p(N_{K/\mathbb{Q}}(e)) = \sum f_i \upsilon_{Q_i}(e)$ (ii). Ας κάνουμε ένα παράδειγμα για να δούμε ότι οι σχέσεις (i) και (ii), οδηγούν σε norm- εξισώσεις. Ας πάρουμε την περίπτωση 1. του θεωρήματος 4.6. Εχουμε:

$$j \in O(\mathcal{S}) \Longleftrightarrow 0 \leq \upsilon_P(e) \leq 12\upsilon_P(2)$$

$$\Longleftrightarrow 0 \leq \upsilon_p(N_{K/\mathbb{Q}}(e)) = \sum f_i \upsilon_{Q_i}(e) \leq \sum f_i 12\upsilon_{Q_i}(2)$$

Ομως $\sum f_i 12\upsilon_{Q_i}(2) = 12\sum f_i e_i \upsilon_p(2)$, λόγω της σχέσης (i), και το τελευταίο ισούται με $12n\upsilon_p(2)$, όπου $\upsilon_p(2) = 0$ ή 1, ανάλογα με το αν $p \neq 2$ ή $p = 2$. Συνεπώς έχουμε

$$N_{K/\mathbb{Q}}(a) = \pm 2^m, \text{όπου } 0 \leq m \leq 12n.$$

Εφαρμόζοντας λοιπόν αυτήν την διαδικασία ανά περίπτωση καταλήγουμε σε norm-εξισώσεις, οι οποίες θα πρέπει να επιλυθούν σε μία απλή κυβική επέκταση του $\mathbb{Q}$. Εχουμε:

1. Εστω ότι ισχύει $E_{tor}(K) \cong \mathbb{Z}/12\mathbb{Z}$.

   Λόγω του θεωρήματος 4.12 έχουμε ότι δεν υπάρχει ελλειπτική καμπύλη E ορισμένη σε απλό κυβικό σώμα αριθμών με ακέραια απόλυτη αναλλοίωτο και υποομάδα πεπερασμένης τάξης $\#E_{tor}(K) > 12$.

   (a) Αν το σώμα K είναι τύπου Dedekind I, τότε από το θεώρημα 4.6 περίπτωση 12, έχουμε ότι η παράμετρος $e \in O_K$. Επομένως, λόγω του θεωρήματος 4.10, ισχύει ότι το e γράφεται κατά μοναδικό τρόπο στην μορφή $e = x_1 + x_2\sqrt[3]{ab^2} + x_3\sqrt[3]{a^2b}$, όπου $x_1, x_2, x_3 \in \mathbb{Z}$ και $a \not\equiv b \pmod 9$. Οδηγούμαστε λοιπόν στις εξής norm-εξισώσεις:

$$N(e) = x_1^3 + x_2^3ab^2 + x_3a^2b - 3x_1x_2x_3ab = \pm 2^n \cdot 3^m \quad (3)$$

$$N(e-1) = N(e) - 3x_1^2 + 3x_1 - 1 + 3x_2x_3ab = \pm 1 \quad (4)$$

$$N(e-2) = N(e) - 6x_1^2 + 12x_1 - 8 + 6x_2x_3ab = \pm 2^n \quad (5)$$

όπου $n \in \{0,1,2,3\}$ και $m \in \{0,1\}$. Πολλαπλασιάζουμε την εξίσωση (4) με 2 και την αφαιρούμε από την εξίσωση (5) και στην συνέχεια λύνουμε ως προς x_1:

$$x_1 = \frac{1}{6}(N(e-2) + N(e) - 2N(e-1) + 6) \qquad (*)$$

Επίσης λύνουμε την εξίσωση (2) ως προς x_2x_3ab :

$$x_2x_3ab = \frac{1}{3}(N(e-1) - N(e) + 3x_1^2 - 3x_1 + 1) \qquad (**)$$

Στην συνέχεια, για δοσμένες τιμές των $N(e)$, $N(e-1)$, $N(e-2)$, υπολογίζουμε το x_1 από την σχέση $(*)$ και απαιτούμε ο x_1 να είναι ακέραιος. Αντικαθιστούμε τον x_1 στην σχέση $(**)$ και αναλύουμε τον $x_2x_3ab \in \mathbb{Z}$ κατά όλους τους δυνατούς τρόπους σε παράγοντες x_2, x_3, a, b, και εξετάζουμε αν ικανοποιούνται οι εξισώσεις $(3)-(5)$. Μέσω αυτού του αλγορίθμου παίρνουμε μόνο δύο λύσεις που ικανοποιούν τις εξισώσεις $(3)-(5)$, για $n = m = 1$ ([Fu]) :

$$e_1 = 2 - \sqrt[3]{2}, \qquad e_2 = -\sqrt[3]{2} - \sqrt[3]{4}$$

Ομως οι αντίστοιχες ελλειπτικές καμπύλες έχουν την ίδια μη-ακέραια απόλυτη αναλλοίωτο:

$$j = \frac{2^6 \cdot 3^2}{5^3}(7765956 + 6163452\sqrt[3]{2} + 4892209\sqrt[3]{4}) \notin O_K$$

Συνεπώς δεν υπάρχει ελλειπτική καμπύλη οριομένη σε απλό κυβικό σώμα αριθμών τύπου Dedekind I, με ακέραια απόλυτη αναλλοίωτο και υποομάδα πεπερασμένης τάξης $E_{tor}(K) \cong \mathbb{Z}/12\mathbb{Z}$.

(b) Αν το σώμα K είναι τύπου Dedekind II, τότε η παράμετρος e γράφεται κατά μοναδικό τρόπο στην μορφή $e = \frac{1}{3}(x_1 + x_2\sqrt[3]{ab^2} + x_3\sqrt[3]{a^2b})$, όπου $x_1, x_2, x_3 \in \mathbb{Z}$, $x_1 \equiv ax_2 \equiv bx_3 \pmod 3$ και $a \equiv \pm b \pmod 9$. Οδηγούμαστε λοιπόν στις εξής norm-εξισώσεις:

$$N(e) = \frac{1}{27}(x_1^3 + x_2^3ab^2 + x_3^3a^2b - 3x_1x_2x_3ab) = \pm 2^n \cdot 3^m \qquad (6)$$

$$N(e-1) = N(e) + \frac{1}{3}(-x_1^2 + 3x_1 - 3 + x_2x_3ab) = \pm 1 \qquad (7)$$

$$N(e-2) = N(e) + \frac{1}{3}(-2x_1^2 + 12x_1 - 24 + 2x_2x_3ab) = \pm 2^n \qquad (8)$$

όπου $n \in \{0,1,2,3\}$ και $m \in \{0,1\}$. Εφαρμόζοντας τον ίδιο αλγόριθμο όπως στην περίπτωση τύπου Dedekind I, καταλήγουμε στο ίδιο συμπέρασμα. Αποδείξαμε λοιπόν την εξής πρόταση:

Πρόταση 4.13 E j K, $E_{tor}(K) \cong \mathbb{Z}/12\mathbb{Z}$.

2. Εστω ότι ισχύει $E_{tor}(K) \cong \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/6\mathbb{Z}$. Από το θεώρημα 4.6, περίπτωση 13, οδηγούμαστε στις ακόλουθες norm-εξισώσεις:

$$N(e) = \pm 2^n, \quad N(e+4) = \pm 2^l \cdot 3^m, \quad N(e-2) = \pm 2^3 \cdot 3^m$$

$$N(e-4) = \pm 2^l, \qquad N(e-8) = \pm 2^n \cdot 3^m$$

όπου $n, l \in \{3, \cdots, 9\}$ και $m \in \{0,1,2,3\}$. Εφαρμόζοντας τον αλγόριθμο που είδαμε στην περίπτωση 1., καταλήγουμε στο εξής συμπέρασμα:

Πρόταση 4.14 E j K $E_{tor}(K) \cong \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/6\mathbb{Z}$.

3. Εστω $E_{tor}(K) \cong \mathbb{Z}/6\mathbb{Z}$. Από το θεώρημα 4.6 και τις προτάσεις 4.13 και 4.14 , έχουμε ότι δεν υπάρχει ελλειπτική καμπύλη E ορισμένη σε απλό κυβικό σώμα αριθμών K, με ακέραια απόλυτη αναλλοίωτο j και υποομάδα πεπερασμένης τάξης $E_{tor}(K) \supset \mathbb{Z}/6\ \mathbb{Z}$. Από το θεώρημα 4.6, περίπτωση 11, έχουμε τις εξής norm-εξιοώσεις:

$$N(e) = \pm 3^n \tag{9}$$

$$N(e+1) = \pm 2^m \tag{10}$$

$$N(e+9) = \pm N(e) \cdot N(e+1) \tag{11}$$

όπου $n \in \{0,1,\cdots,6\}$ και $m \in \{0,1,\cdots,9\}$. Ο αλγόριθμος που χρησιμοποιήσαμε στην περίπτωση 1, μας δίνει 6 καμπύλες, από τις οποίες 2 είναι ορισμένες στο $\mathbb{Q}$ και οι υπόλοιπες 4 είναι ορισμένες στο σώμα $\mathbb{Q}(\sqrt[3]{2})$ ([Fu]).

4. Εστω $E_{tor}(K) \cong \mathbb{Z}/4\mathbb{Z}$. Λόγω του θεωρήματος 4.6 και της πρότασης 4.12, έχουμε ότι δεν υπάρχει ελλειπτική καμπύλη E με ακέραια απόλυτη αναλλοίωτο j ορισμένη σε απλό κυβικό σώμα αριθμών K και υποομάδα πεπερασμένης της $E_{tor}(K) \supset \mathbb{Z}/4\mathbb{Z}$.

(a) Εστω ότι το σώμα K είναι τύπου Dedekind II. Τότε από το θεώρημα 4.6, περίπτωση 3, οδηγούμαστε στις ακόλουθες norm-εξιοώσεις:

$$N(e) = x_1^3 + x_2^3ab^2 + x_3^3a^2b - 3x_1x_2x_3ab = \pm 2^n \qquad (12)$$

$$N(e+16) = N(e) + 48x_1^2 + 768x_1 + 4096 - 48x_2x_3ab = \pm 2^m \qquad (13)$$

όπου $n, m \in \{0, 1, \cdots, 24\}$. Θέτουμε $A = \frac{1}{48}(N(e+16) - N(e) - 4096)$. Τότε οι σχέσεις (12) και (13), δίνουν:

$$x_1 = -8 \pm \sqrt{A + 64 + x_2x_3ab} \quad (*)$$

$$x_2x_3ab = x_1^2 + 16x_1 - A \quad (**)$$

Ομως αφού $x_1, x_2x_3ab \in \mathbb{Z}$, έπεται ότι:

$$N(e+16) - N(e) - 4096 \equiv 0 mod 48$$

Αν $x_2x_3ab < 0$, τότε από την σχέση $(*)$ έχουμε $0 < |x_2x_3ab| \leq A + 64$, και $x_2x_3ab = -(A+64) + z^2$, όπου $z \in \mathbb{Z}$ και $0 \leq z < \sqrt{A+64}$. Συνεπώς για δοσμένη τιμή του A, υπάρχουν πεπερασμένα στο πλήθος z, τέτοια ώστε $0 \leq z < \sqrt{A+64}$. Επομένως για δοσμένη τιμή του z, ισχύουν:

$$x_1 = -8 \pm \sqrt{A + 64 + x_2x_3ab} \quad (\circ)$$

$$x_2x_3ab = -(A+64) + z^2 \quad (\circ\circ).$$

Εφαρμόζουμε τώρα τον αλγόριθμο της περίπτωσης 1., όταν $x_2x_3ab < 0$, έτσι ώστε να ικανοποιούνται οι εξιοώσεις (12), (13) καθώς και οι $(\circ)$, $(\circ\circ)$. Το αποτέλεσμα είναι ότι έχουμε πεπερασμένα στο πλήθος απλά κυβικά σώματα K και πεπερασμένες στο πλήθος παραμέτρους e που να παραμετρίζουν την ελλειπτική καμπύλη E.

Εστω τώρα ότι $x_2x_3ab \geq 0$. Τότε έχουμε ότι:

$$0 \leq (x_2^3ab^2 - x_3^3a^2b)^2 = (x_2^3ab^2 + x_3^3a^2b)^2 - 4(x_2x_3ab)^3$$

$$\Longrightarrow (x_2^3ab^2 + x_3^3a^2b)^2 \geq 4(x_2x_3ab)^3 \overset{(**)}{=} 4(x_1^2 + 16x_1 - A)^3$$

Από την άλλη πλευρά όμως, λόγω των εξιοώσεων (1) και $(**)$, έχουμε:

$$(x_2^3ab^2 + x_3^3a^2b)^2 = (-x_1^3 + 3x_1x_2x_3ab + N(e))^2 = [2(x_1^3 + 48x_1^2 - 3Ax_1 + N(e))]^2$$

$$\Longrightarrow 4(x_1^2+16x_1-A)^3-(2x_1^3+48x_1^2-3Ax_1+N(e))^2 \leq 0$$

$$\Longleftrightarrow 768x_1^4+(16348-4N(e)-96A)x_1^3+(3A^2-96N(e)-3072A)x_1^2$$

$$+(192A^2+6AN(e))x_1+(-4A^3-N^2(e)) \leq 0$$

Προφανώς η τελευταία ανισότητα ικανοποιείται μόνο για πεπερασμένες στο πλήθος τιμές του $x_1 \in \mathbb{Z}$. Για δοσμένη λοιπόν τιμή του x_1, υπολογίζουμε το x_2x_3ab από την σχέση $(**)$. Καταλήγουμε σε πεπερασμένες στο πλήθος ελλειπτικές καμπύλες E, και πεπερασμένα στο πλήθος σώματα K ([Fu]).

(b) : Εστω ότι το σώμα K είναι τύπου Dedekind (II). Σε αυτήν την περίπτωση οδηγούμαστε στις ακόλουθες norm-εξισώσεις :

$$N(e) = \frac{1}{27}(x_1^3+x_2^3ab^2+x_3^3a^2b-3x_1x_2x_3ab) = \pm 2^n \tag{14}$$

$$N(e+16) = N(e)+\frac{1}{3}(16x_1^2+768x_1+12288-16x_2x_3ab) = \pm 2^m \tag{15}$$

όπου $n, m \in \{0, 1, \cdots, 24\}$. Συνεχίζοντας κατά εντελώς όμοιο τρόπο όπως στην περίπτωση τύπου Dedekind I, καταλήγουμε στο συμπέρασμα ότι δεν υπάρχουν ελλειπτικές καμπύλες με ακέραια απόλυτη αναλλοίωτο ορισμένες σε απλό κυβικό σώμα τύπου Dedekind II και υποομάδα πεπερασμένης τάξης $E_{tor}(K) \cong \mathbb{Z}/4\mathbb{Z}$. Συνεπώς η μόνη περίπτωση όπου παίρνουμε δεκτό αποτέλεσμα είναι η περίπτωση σωμάτων τύπου Dedekind I. Μάλιστα όλα τα δυνατά σώματα είναι της μορφής $K = \mathbb{Q}(\sqrt[3]{D})$, όπου το D διατρέχει το σύνολο $\{2, 3, 5, 31\}$ ([Fu]).

5. Εστω $E_{tor}(K) \cong \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$. Στην περίπτωση 4, υπολογίσαμε όλα τα σώματα K και τις παραμέτρους e που ικανοποιούν τις συνθήκες (1) : $0 \leq \upsilon(e)$, και $\upsilon(e+16) \leq 8\upsilon(2)$. Στην προκειμένη περίπτωση θέλουμε να υπολογίσουμε όλα τα σώματα K και τις παραμέτρους e', τέτοιες ώστε (2) : $0 \leq \upsilon(e')$ και $\upsilon(e'-16) \leq 8\upsilon(2)$. Θέτοντας $e' := e+16$, παρατηρούμε ότι υπάρχει $1-1$ αντιστοιχία, μεταξύ των e που ικανοποιούν τις συνθήκες (1) και των e' που ικανοποιούν τις συνθήκες (2). Επομένως έχουμε πεπερασμένες στο πλήθος παραμέτρους e' και πεπερασμένες στο πλήθος απόλυτες αναλλοιώτους j. Δηλαδή πιθανόν να πάρουμε άπειρες το πλήθος ελλειπτικές καμπύλες E, που θα αντιστοιχούν σε πεπρασμένες το πλήθος τιμές της απόλυτης αναλλοιώτου j. ([Fu]).

6. Εστω $E_{tor}(K) \cong \mathbb{Z}/2\mathbb{Z}$ ή $E_{tor}(K) \cong \mathbb{Z}/3\mathbb{Z}$. Οταν $E_{tor}(K) \cong \mathbb{Z}/2\mathbb{Z}$, τότε οδηγούμαστε στην εξής norm-εξίσωση:

$$N(e) = \pm 2^n$$

όπου $n \in \{0, 1, \cdots, 36\}$. Οι λύσεις της παραπάνω εξίσωσης δίνουν άπειρες στο πλήθος ελλειπτικές καμπύλες E και άπειρα απλά κυβικά σώματα K ([Fu]). Αν περιορίσουμε το πρόβλημα στο $K = \mathbb{Q}$ τότε παίρνουμε τις παραμέτρους $e = \pm 2^n$, $n \in \{0, 1, \cdots, 12\}$ και άρα τις απόλυτες αναλλοιώτους $j = 2^{2n}(1 \pm 2^{4-n})^3$. Εντελώς όμοια δουλεύουμε όταν $E_{tor}(K) \cong \mathbb{Z}/3\mathbb{Z}$, και καταλήγουμε στις περιπτώσεις όπου $K = \mathbb{Q}$ στις παραμέτρους $e = \pm 3^n$, $n \in \{0, 1, \cdots, 6\}$.

7. Εστω $E_{tor}(K) \cong \mathbb{Z}/5\mathbb{Z}$. Οι norm-εξισώσεις στις οποίες καταλήγουμε είναι οι εξής:

$$N(e) = \pm 1 \qquad (16)$$

$$N(e^2 - 11e - 1) = \pm 5^n \qquad (17)$$

όπου $n \in \{0, 1, \cdots, 9\}$. Θέτουμε $D := ab^2$, $\delta := \sqrt[3]{ab^2}$, $\bar{\delta} := \sqrt[3]{a^2 b}$ και υποθέτουμε ότι $a > b$. Θα υπολογίσουμε όλες τις δυνατές τιμές του D, ώστε να ισχύουν οι σχέσεις (16) και (17).

Εστω $g(X) := X^2 - 11X - 1 \in \mathbb{Z}[X]$. Αν $e \in U_K$ τότε $\eta := -\frac{1}{e} \in U_K$. Επίσης το στοιχείο $g(\eta) = e^{-2} - 11e^{-1} - 1$, έχει norm $N(g(\eta)) = -N(g(e))$. Συνεπώς αν η e είναι λύση των εξισώσεων (16) και (17), τότε είναι και η η. Αρα χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $|e| > 1$. Θα αποδείξουμε το εξής λήμμα:

Λήμμα 4.15 $|e| > 1950$, e (16) (17).

<u>Απόδειξη :</u> Εστω ότι $|e| > 1950$, $e \in U_K$. Αν e' και $\bar{e}$, είναι τα δυο συζυγή του e, τότε:

$$|N(e)| = |e \cdot e' \cdot \bar{e}| = |e| \cdot |e'|^2 = 1 \Longrightarrow |\frac{1}{e'}| = \sqrt{|e|} > 44$$

Αν ισχύουν οι εξισώσεις (16) και (17) έχουμε ότι ισχύει η σχέση $|N(g(e))/N(e)| = 5^n$ όπου $n \in \{0, 1, \cdots, 9\}$ και επομένως ισχύει ότι:

$$|e - 11 - \frac{1}{e}| \cdot |\frac{1}{e'} + 11 - e'|^2 = 5^n, \quad n \in \{0, \cdots, 9\}. \qquad (18)$$

$$\text{Ομως,} \quad |11 + \frac{1}{e}| \leq 11 + \frac{1}{|e|} < 11 + \frac{1}{1950} \quad \text{και}$$

$$|e - 11 - \frac{1}{e}| \geq ||e| - |11 + \frac{1}{e}|| \Longrightarrow |e - 11 - \frac{1}{e}| > 1950 - 11 - \frac{1}{1950} \quad (*).$$

Επιπλέον ισχύει ότι $|11 - e'| \leq 11 + |e'| < 11 + \frac{1}{44}$, και:

$$|\frac{1}{e'} + 11 - e'| \geq ||\frac{1}{e'}| - |11 - e'||. \quad \text{Αρα:}$$

$$|\frac{1}{e'} + 11 - e'| > 44 - 11 - \frac{1}{44}(**).$$

Συνδιάζοντας τις ανισότητες $(*)$ και $(**)$, έχουμε:

$$|N(g(e))/N(e)| > (1950 - 11 - \frac{1}{1950})(44 - 11 - \frac{1}{44}^{\,2}) > 5^9$$

το οποίο είναι άτοπο λόγω της σχέσεως (18). $\square$

Συμφωνα με το λήμμα 4.15, έχουμε ότι δεν υπάρχει λύση των εξιοώσεων (16) και (17) σε άνα απλό κυβικό σώμα αριθμών που έχει κανονικοποιημένη θεμελιώδη μονάδα $e_0(>1)$, "αρκετά" μεγάλη ($e_0 > 1950$). Από την άλλη μεριά όμως ο Cusick απέδειξε ότι για κάθε απλό κυβικό σώμα αριθμών K με διακρίνουσα $\Delta_K < 0$, ο regulator του K ικανοποιεί την εξής ανισότητα:

$$R(K) = \log e_0 \geq \frac{1}{3}\log(\frac{|\Delta_K|}{27}) \quad (***)$$

Πράγματι, για $e := \frac{1}{e_0}$, έχουμε :

$$\Delta(e) = (e-e')^2(e-\bar{e})^2(e'-\bar{e})^2 = (e')^2\bar{e}^4(1-\frac{e}{e'})^2(1-\frac{e}{\bar{e}}^2)^2(1-\frac{e'}{\bar{e}})^2$$

όπου τα $e, e', \bar{e}$, είναι διατεταγμένα ως εξής $|e| \leq |e'| = |\bar{e}|$. Τότε:

$$\log\Delta(e) \leq \log 4 + 2(\log\bar{e}^2 + \log e'),$$

διότι αν θέσουμε $x := \frac{e}{e'}$, $y := \frac{e'}{\bar{e}}$, παρατηρούμε ότι η συναρτηση

$$f(x,y) := (1-x)(1-y)(1-xy), \quad \text{όπου} \quad |x| \leq 1, |y| \leq 1,$$

έχει μέγιστο το 2 ($f(x,y) \leq 2$). Επίσης ισχύει ότι $e < |e'| = |\bar{e}| = e^{-1/2}$. Συνεπώς:

$$\log\Delta(e) \leq \log 27 + 2(\frac{-3}{2}\log e)$$

$$\Longrightarrow \log\Delta_K \leq \log 27 + 3R(K)$$

Αρα ικανοποιείται η ανισότητα $(***)$.

Οπως γνωρίζουμε η διακρίνουσα ενός απλού κυβικού σώματος αριθμών K, είναι:

$$\Delta_K = -27\frac{(ab)^2}{s^2}, \quad \text{όπου} \quad s = \begin{cases} 1 & \text{όταν } a \not\equiv \pm b \pmod 9 \\ 3 & \text{όταν } a \equiv \pm b \pmod 9 \end{cases}$$

και συνεπώς λόγω της σχέσεως $(***)$ έχουμε το εξής άνω φράγμα:

$$(\frac{ab}{s})^2 \leq e_0^3$$

Επομένως για να ισχύουν οι σχέσεις (16) και (17) στο σώμα $K = \mathbb{Q}(\delta)$ πρέπει να ισχύουν οι ανισότητες:

$$ab \leq s e_0^{3/2} < s(1950)^{3/2} < 86110 \cdot s$$

Θεώρημα 4.16 $R(K)$ *regulator* $K = \mathbb{Q}(\delta)$, :

$$R(K) \geq 2\log(\frac{3\delta - s}{2s})$$

Απόδειξη : Εστω $\eta := e_0^{-1} < 1$. Αφού $\eta \in O_K$ έχουμε:

$$\eta = \frac{r_1 + r_2\delta + r_3\overline{\delta}}{s}$$

όπου $r_1, r_2, r_3 \in \mathbb{Z}$. Αν ω είναι πρωταρχική ρίζα της μονάδος ισχύει:

$$\eta' = \frac{r_1 + r_2\omega\delta + r_3\omega^2\overline{\delta}}{s}$$

$$\bar{\eta} = \frac{r_1 + r - 2\omega^2\delta + r_3\omega\overline{\delta}}{s}$$

Από αυτές τις τρείς εξισώσεις έχουμε:

$$3r_2\delta = s(\eta + \omega^2\eta' + \omega\bar{\eta})$$

$$3r_3\overline{\delta} = s(\eta + \omega\eta' + \omega^2\bar{\eta}$$

Παίρνουμε απόλυτες τιμές:

$$3|r_2|\frac{\delta}{s}, 3|r_3|\frac{\delta'}{s} \leq |\eta| + |\eta'| + |\bar{\eta}| = |\eta| + 2|\eta'| < 1 + 2|\eta'|.$$

Ομως $1 = N(\eta) = \eta \cdot |\eta'|^2 = \frac{|\eta'|^2}{e_0}$, και άρα $|\eta'| = \sqrt{e_0}$. Συνεπώς:

$$|r_2|\delta, \quad |r_3|\delta' < \frac{s(1 + 2\sqrt{e_0})}{3}.$$

Αν τώρα υποθέσουμε ότι $\delta > s(1 + 2\sqrt{e_0})/3$, τότε $r_2 = r_3 = 0$, που αυτό σημαίνει ότι $r_1 = s$ και $\eta = 1$, έχουμε άτοπο. Αρα $\sqrt{e_0} \geq (3\delta - s)/2s$. Επομένως:

$$\frac{1}{2}\log e_0 \geq \log(\frac{3\delta - s}{2s}) \Longrightarrow R(K) \geq 2\log(\frac{3\delta - s}{2s}) \quad \square$$

Από το θεώρημα 4.16 και το λήμμα 4.15, έχουμε ότι αν οι εξισώσεις (16) και (17) έχουν λύση σε κάποιο απλό κυβικό σώμα αριθμών $K = \mathbb{Q}(\delta)$, $\delta = ab^2$, τότε ικανοποιείται η εξής ανισότητα:

$$\frac{3\delta - s}{2s} < \sqrt{1950}$$

Συνεπώς εάν $D = ab^2$, έχουμε το ακόλουθο άνω φράγμα:

$$D < 26391s^3$$

Καταλήξαμε λοιπόν σε πεπρασμένου πλήθους σώματα K και πεπερασμένες στο πλήθος παραμέτρους e_0, με $e_0 < 1950$. Αρα έχουμε μια μόνο ελλειπτική καμπύλη E/K, που παραμετρίζεται από το e_0 (δες [Fu], σελ. 44, πρόταση 6).

5 Ελλειπτικές καμπύλες ορισμένες σε στοιχειώδεις 2-αβελιανές επεκτάσεις του $\mathbb{Q}$

Εστω ελλειπτική καμπύλη E ορισμένη στο σώμα $\mathbb{Q}$. Σκοπός αυτού του κεφαλαίου είναι η εύρεση όλων των πιθανών ομάδων που εμφανίζονται σαν torsion ομάδες $E_{tor}(F)$, ελλειπτικών καμπύλων E οριομένων στο $\mathbb{Q}$, όπου F είναι στοιχειώδης 2-αβελιανή επέκταση του $\mathbb{Q}$.

5.1 Συνομολογία πεπερασμένων ομάδων

Εστω $\mathcal{G}$, μία πεπερασμένη ομάδα και M μία αβελιανή ομάδα στην οποία δρα η ομάδα $\mathcal{G}$. Συμβολίζουμε την δράση του στοιχείου $s \in \mathcal{G}$ στο στοιχείο $m \in M$ με m^s. Τότε το M είναι ένα (δεξί) $\mathcal{G}$-module, αν:

$$m^1 = m, \quad (m+m')^s = m^s + (m')^s, \quad (m^s)^t = m^{st}$$

Αν M και N είναι $\mathcal{G}$-modules, ένας $\mathcal{G}$-μορφισμός είναι ένας ομομορφισμός $\varphi : M \to N$ αβελιανών ομάδων τέτοιος ώστε $\varphi(m^s) = \varphi(m)^s$, για κάθε $m \in M$ και $s \in \mathcal{G}$.

Για ένα δοσμένο $\mathcal{G}$-module, συχνά μας ενδιαφέρει ο υπολογισμός του μεγαλύτερου υπο-module στο οποίο η $\mathcal{G}$ δρα τετριμμένα.

Ορισμός 5.1 0- $\mathcal{G}$*-module* M, $M^{\mathcal{G}}$ $H^0(\mathcal{G}, M)$, *:*

$$H^0(\mathcal{G}, M) := \{m \in M / m^s = m, \forall s \in \mathcal{G}\}$$

Εστω τώρα η μικρή ακριβής ακολουθία από $\mathcal{G}$-modules:

$$0 \longrightarrow P \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

δηλαδή οι φ και ψ είναι $\mathcal{G}$-module μορφισμοί, όπου ο φ είναι μονομορφισμός, ο ψ είναι επιμορφισμός και η εικόνα του μορφισμού φ, $Im(\varphi)$ ισούται με τον πυρήνα του ψ, $Ker(\psi)$. Παρατηρούμε τότε ότι η ακολουθία των 0-ομάδων συνομολογίας :

$$0 \longrightarrow P^{\mathcal{G}} \longrightarrow M^{\mathcal{G}} \longrightarrow N^{\mathcal{G}}$$

είναι ακριβής, αλλά η απεικόνιση $M^{\mathcal{G}} \to N^{\mathcal{G}}$ δεν είναι εν γένει επί. Με σκοπό να ελέγξουμε πόσο διαφέρει η τελευταία απεικόνιση από το να είναι επί, δίνουμε τον ακόλουθο ορισμό.

Ορισμός 5.2 *M $\mathcal{G}$-module. 1- $\mathcal{G}$ M, :*

$$C^1(\mathcal{G}, M) := \{\xi/\xi : \mathcal{G} \to M\}.$$

1-, :

$$Z^1(\mathcal{G}, M) := \{\xi \in C^1(\mathcal{G}, M)/\xi_{st} = \xi_s^t + \xi_t, \forall s, t \in \mathcal{G}\},$$

$\xi_{st} := \xi(st)$.

1-, :

$$B^1(\mathcal{G}, M) := \{\xi \in C^1(\mathcal{G}, M)/\exists m \in M \ .. \ \xi_s = m^s - m, \forall s \in \mathcal{G}\}$$

1- $\mathcal{G}$-module M :

$$H^1(\mathcal{G}, M) := Z^1(\mathcal{G}, M)/B^1(\mathcal{G}, M)$$

Με άλλα λόγια, η 1-ομάδα συνομολογίας είναι η ομάδα των 1-συνκύκλων $\xi : \mathcal{G} \to M$, modulo την σχέση ισοδυναμίας ότι δύο συνκύκλοι ταυτίζονται εάν η διαφορά τους είναι της μορφής $m^s - m$, για κάποιο $m \in M$.

Παρατηρήσεις:

1. Είναι προφανές ότι εάν η δράση της ομάδος $\mathcal{G}$, στο $\mathcal{G}$-module M είναι τετριμμένη, τότε:

$$H^0(\mathcal{G}, M) = M, \quad \text{και} \quad H^1(\mathcal{G}, M) = Hom(\mathcal{G}, M)$$

2. Ο αναγνώστης που ενδιαφέρεται για κάποιες επιπλέον πληροφορίες για την συνομολογία των πεπερασμένων ομάδων, μπορεί να ανατρέξει στο [Αν4].

5.2 Κλάσεις ισομορφίας ελλειπτικών καμπύλων

Εστω k ένα τέλειο σώμα και $\bar{k}$ η αλγεβρική θήκη του σώματος k. Εστω δε E μία ελλειπτική καμπύλη ορισμένη στο σώμα k και $P = (x, y)$ ένα σημείο της καμπύλης E. Η επέκταση $\bar{k}/k$ είναι μια άπειρη επέκταση του Galois (δες [Κον], παράρτημα, σελ. $99 - 122$). Η ομάδα $Gal(\bar{k}/k)$, δρα κατά φυσιολογικό τρόπο σε κάθε σημείο $P = (x, y)$ της ελλειπτικής καμπύλης E, $P^s = (x^s, y^s)$.

Θεωρούμε τώρα την ομάδα $Aut_{\bar{k}}(E)$, των αυτομορφισμών της ελλειπτικής καμπύλης E πάνω από το σώμα $\bar{k}$, που απεικονίζουν το επ'άπειρο σημείο O στον εαυτό του. Ισχύει το ακόλουθο:

Θεώρημα 5.3 E/k . k ($O \mapsto O$) 24. :

$$|Aut_{\bar{k}}(E)| = \begin{cases} 2 & j(E) \neq 0, 1728 \\ 4 & j(E) = 1728 \quad char(k) \neq 2,3 \\ 6 & j(E) = 0 \quad char(k) \neq 2,3 \\ 12 & j(E) = 0 = 1728 \quad char(k) = 3 \\ 24 & j(E) = 0 = 1728 \quad char(k) = 2 \end{cases}$$

Απόδειξη : Εστω ότι $char(k) \neq 2,3$ (Οι περιπτώσεις χαρακτηριστικής 2 και 3 γίνονται όμοια). Τότε η ελλειπτική καμπύλη E δίνεται από εξίσωση της μορφής:

$$E : Y^2 = X^3 + AX + B.$$

Κάθε αυτομορφισμός της καμπύλης E είναι της μορφής $x = u^2x'$, $y = u^3y'$, όπου $u \in \bar{k}^*$. Επομένως αντικαθιστώντας στην εξίσωση της E, έχουμε ότι $u^{-4}A = A$ και $u^{-6}B = B$. Συνεπώς εαν $AB \neq 0$ (δηλαδή $j(E) \neq 0, 1728$) έπεται ότι $u = \pm 1$. Αν $B = 0$ ($j(E) = 1728$), τότε $u^4 = 1$ και εαν $A = 0$ ($j(E) = 0$) τότε $u^6 = 1$. □

Πόρισμα 5.4 E , k , $char(k) \neq 2,3$. μ_n n- $\bar{k}$, $n = 2$ ($n = 4$, $n = 6$), $j \neq 0, 1728$ ($j = 1728$, $j = 0$), $Gal(\bar{k}/k)$-modules:

$$Aut_{\bar{k}}(E) \cong \mu_n.$$

Απόδειξη : Κατά την αποδεικτική διαδικασία του θεωρήματος 5.3, δείξαμε ότι η απεικόνιση:

$$[\ ] : \mu_n \to Aut_{\bar{k}}(E), \quad [\zeta](x,y) = (\zeta^2 x, \zeta^3 y),$$

είναι ισομορφισμός ομάδων. Ομως η παραπάνω απεικόνιση, αντιμετατίθεται με την δράση της ομάδος του Galois και επομένως είναι ισομορφισμός $Gal(\bar{k}/k)$-modules. □

Εστω τώρα E'/k ελλειπτική καμπύλη twist της E. Επομένως υπάρχει ισομορφισμός $\varphi : E' \to E$, ορισμένος στο σώμα $\bar{k}$. Συμβολίζουμε με $Twist_{\bar{k}}(E)$, το σύνολο των twist της καμπύλης E (modulo ισομορφία υπέρ το σώμα k). Θεωρούμε τώρα την απεικόνιση:

$$\xi : \begin{cases} G(\bar{k}/k) \longrightarrow Aut_{\bar{k}}(E) \\ s \mapsto \xi_s = \varphi^s \varphi^{-1} \end{cases}$$

Θα αποδείξουμε ότι ο ξ, όπως ορίστηκε, είναι 1-συνκύκλος και η συνομολογιακή κλάση του ξ ορίζεται μοναδικά κάτω από ισομορφισμό. Επιπλέον κάθε συνομολογιακή κλάση προέρχεται από κάποια twist της καμπύλης E/k. Κατ' αυτόν τον τρόπο λοιπόν μπορούμε να ταυτίσουμε το σύνολο των twist της καμπύλης E, με την πρώτη ομάδα συνομολογίας $H^1(G(\bar{k}/k), Aut_{\bar{k}}(E))$. Συνοψίζουμε και αποδεικνύουμε τα παραπάνω στο ακόλουθο θεώρημα:

Θεώρημα 5.5 *E () k. twist E'/k E $\bar{k}$- $\varphi : E' \to E$ $\xi_s = \varphi^s\varphi^{-1} \in Aut_{\bar{k}}(E)$, . :*

1. *ξ 1-, s, t $Gal(\bar{k}/k)$ $\xi_{st} = (\xi_s)^t\xi_t$. $\{\xi\}$ ξ_s $H^1(Gal(\bar{k}/k), Aut_{\bar{k}}(E))$.*

2. *:*

$$\mathcal{T} : Twist_{\bar{k}}(E) \longrightarrow H^1(G(\bar{k}/k), Aut_{\bar{k}}(E))$$

   $\mathcal{T}$, $1-1$.

twist E/k (k-) $1-1$ $H^1(Gal(\bar{k}/k), Aut_{\bar{k}}(E))$.

<u>Απόδειξη :</u> Εχουμε $\xi_{st} = \varphi^{st}\varphi^{-1} = (\varphi^s\varphi^{-1})^t(\varphi^t\varphi^{-1}) = \xi_s^t\xi_t$, για κάθε $s, t \in Gal(\bar{k}/k)$. Αρα ο ξ είναι πράγματι 1-συνκύκλος.

Εστω τώρα E''/k μια άλλη twist της καμπύλης E/k που να είναι k-ισόμορφη με την E'/k. Θα αποδείξουμε ότι οι 1-συνκύκλοι $\varphi^s\varphi^{-1}$ και $\psi^s\psi^{-1}$, ανήκουν στην ίδια κλάση συνομολογίας. Εξ υποθέσεως, υπάρχει k-ισομορφισμός $\theta : E'' \to E'$. Ορίζουμε το στοιχείο $\alpha := \varphi\theta\psi^{-1} \in Aut_{\bar{k}}(E)$. Εχουμε:

$$\alpha^s(\psi^s\psi^{-1}) = (\varphi\theta\psi^{-1})^s(\psi^s\psi^{-1}) = \varphi^s\theta^s\psi^{-1} =$$

$$= \varphi^s\theta\psi^{-1} = (\varphi^s\varphi^{-1})(\varphi\theta\psi^{-1}) = (\varphi^s\varphi^{-1})\alpha,$$

το οποίο αποδεικνύει ότι τα στοιχεία $\varphi^s\varphi^{-1}$, $\psi^s\psi^{-1}$, ανήκουν στην ίδια κλάδη συνομολογίας και επομένως η απεικόνιση $\mathcal{T}$ είναι καλώς ορισμένη.

Αποδεικνύουμε τώρα ότι η απεικόνιση $\mathcal{T}$, είναι $1-1$. Εστω E'/k και E''/k, δύο twist της καμπύλης E/k που δίνουν την ίδια κλάση συνομολογίας στην $H^1(Gal(\bar{k}/k), Aut_{\bar{k}}(E))$. Αυτό σημαίνει ότι υπάρχουν $\bar{k}$-ισομορφισμοί $\varphi : E' \to E$, $\psi : E'' \to E'$ και $\bar{k}$-αυτομορφισμός α, τέτοιοι ώστε:

$$\alpha^s(\psi^s\psi^{-1}) = (\varphi^s\varphi^{-1})\alpha, \quad \forall s \in Gal(\bar{k}/k)$$

Ορίζουμε την απεικόνιση $\theta : E'' \to E'$, $\theta = \varphi^{-1}\alpha\psi$. Προφανώς ο θ είναι $\bar{k}$- ισομορφισμός. Επιπλέον, για κάθε $s \in Gal(\bar{k}/k)$, έχουμε:

$$\theta^s = (\varphi^s)^{-1}(\alpha^s\psi^s) = (\varphi^s)^{-1}(\varphi^s\varphi^{-1}\alpha\psi) = \varphi^{-1}\alpha\psi = \theta.$$

Επομένως, η απεικόνιση θ είναι k-ισομορφισμός, δηλαδή οι καμπύλες E' και E'' είναι k-ισόμορφες και συνεπώς δίνουν το ίδιο στοιχείο στο σύνολο $Twist_k(E)$. Αρα η απεικόνιση $\mathcal{T}$ είναι $1-1$.

Εστω τώρα $\xi : Gal(\bar{k}/k) \to Aut_{\bar{k}}(E)$ ένας 1-συνκύκλος. Για να αποδείξουμε ότι η απεικόνιση $\mathcal{T}$ είναι επί, αρκεί να κατασκευάσουμε καμπύλη E'/k και $\bar{k}$-ισομορφισμό $\varphi : E' \to E$, τέτοιον ώστε $\xi_s = \varphi^s\varphi^{-1}$. Προς αυτόν τον σκοπό θεωρούμε το σώμα συναρτήσεων της ελλειπτικής καμπύλης E, $\bar{k}(E)$. Με $\bar{k}(E)_\xi$, συμβολίζουμε το σώμα το οποίο είναι ισόμορφο με το σώμα $\bar{k}(E)$, έστω μέσω του $\bar{k}$-ισομορφισμού $Z : \bar{k}(E) \to \bar{k}(E)_\xi$, όπου όμως η διαφορά ανάμεσα στα δύο σώματα εντοπίζεται στην δράση της ομάδος Galois, $Gal(\bar{k}/k)$. Συγκεκριμένα ορίζουμε $Z(h)^s = Z(h^s\xi_s)$, για κάθε $s \in Gal(\bar{k}/k)$ και $h \in \bar{k}(E)$. Σε αυτό το σημείο δίνουμε κάποιες εξηγήσεις για το πώς δρα η ομάδα Galois $Gal(\bar{k}/k)$ στα στοιχεία του σώματος συναρτήσεων της καμπύλης E, $\bar{k}(E)$. Εστω $h \in \bar{k}(E) = Quot(\bar{k}[x,y]/ < f(x,y) >)$, εαν η E έχει εξίσωση $f(x,y) = 0$. Είναι προφανές ότι η h επάγει καλώς ορισμένη απεικόνιση που την συμβολίζουμε επίσης h από την καμπύλη E στο σώμα $\bar{k}$, $h : E \to \bar{k}$ που απεικονίζει το σημείο $P \in E(\bar{k})$, στην τιμή του $h(P) \in \bar{k}$. Η ομάδα Galois $Gal(\bar{k}/k)$ δρά στο στοιχείο h, δρώντας στους συντελεστές του. Επίσης, αφού η καμπύλη E είναι ορισμένη στο σώμα k, αφήνει το ιδεώδες $< f(x,y) >$ αναλλοίωτο. Επομένως κατ' αυτόν τον τρόπο παίρνουμε μία συγκεκριμένη δράση στο σώμα συναρτήσεων $\bar{k}(E)$. Επίσης ορίζουμε $[h(P)]^s := h^s(P^s)$.

Ορίσαμε λοιπόν την δράση της ομάδος Galois στο σώμα $\bar{k}(E)$ και συνεπώς και την δράση στο σώμα $\bar{k}(E)_\xi$. Εστω $G := Gal(\bar{k}/k)$. Θεωρούμε το σταθερό σώμα του $\bar{k}(E)_\xi$, $F := \bar{k}(E)_\xi^G$. Θα αποδείξουμε το ζητούμενο σε τρία βήματα :

1. $F \cap \bar{k} = k$.

   Εστω $g \in F \cap \bar{k}$. Τότε λόγω ισομορφίας της Z, υπάρχει $h \in \bar{k}(E)$ τέτοιο ώστε $g = Z(h)$, δηλαδή $g = Z(h) \in \bar{k}$. Επειδή όμως η Z είναι ταυτότητα στο $\bar{k}$, έπεται ότι το $h \in \bar{k}$ και επομένως είναι σταθερά. Συνεπώς:

$$Z(h) = Z(h)^s = Z(h^s\xi_s) = Z(h^s),$$

διότι, αφού η h είναι σταθερά, θα είναι σταθερά και η h^s, δηλαδή $h^s\xi_s = h^s$. Επομένως $Z(h) = Z(h^s)$, για κάθε $s \in G$. Επειδή όμως η Z είναι ταυτότητα στο $\bar{k}$, συνεπάγεται ότι $h^s = h$, δηλαδή το ζητούμενο, $h \in k$.

2. $\bar{k} \cdot F = \bar{k}(E)_\xi$.

Για την αποδείξη αυτού του ισχυρισμού, αποδεικνύουμε το εξής λήμμα:

Λήμμα 5.6 *V $\bar{k}$- Galois $G = Gal(\bar{k}/k)$ V, G $\bar{k}$. $V_k := V^G$, :*

$$V = \bar{k} \otimes_k V_k.$$

Απόδειξη : Αρκεί να αποδείξουμε ότι κάθε $v \in V$, είναι $\bar{k}$-γραμμικός συνδιασμός στοιχείων του V_k. Κατ' αρχήν το γεγονός ότι η ομάδα G δρα συνεχώς στον διανυσματικό χώρο V, σημαίνει ότι η υποομάδα της G, $H := \{s \in G / v^s = v\}$ έχει πεπερασμένο δείκτη στην ομάδα G. Η H αντιστοιχεί στην πεπερασμένη επέκταση του Galois L/k. Εστω δε $[L : k] = n$ και $\{a_1, \cdots, a_n\}$, μία βάση της επέκτασης L/k. Αν $Gal(L/k) = \{s_1, \cdots, s_n\}$, τότε για κάθε $i \in \{1, \cdots, n\}$ ορίζουμε τα διανύσματα:

$$w_i := \sum_{j=1}^{n} (a_i v)^{s_j} = \sum_{j=1}^{n} a_i^{s_j} v^{s_j},$$

όπου η τελευταία ισότητα ισχύει διότι η δράση της G στον V είναι συμβατή με την δράση της G στο σώμα $\bar{k}$. Παρατηρούμε ότι τα διανύσματα w_i είναι G-αναλλοίωτα. Επομένως $w_i \in V_k$. Επιπλέον όπως γνωρίζουμε από την θεωρία σωμάτων ο πίνακας $(a_j^{s_i})$, είναι μη-ιδιάζων. Συνεπώς κάθε v^{s_j} γράφεται ως L-γραμμικός συνδιασμός των $w_i \in V_k$ και άρα το ίδιο συμβαίνει και για το στοιχείο $v \in V$. □

Εφαρμόζοντας λοιπόν το λήμμα για $V := \bar{k}(E)_\xi$, $V_k = F$, έχουμε ότι $\bar{k} \otimes_k F = \bar{k}(E)_\xi$. Ομως $\bar{k} \otimes_k F = \bar{k}F$, και άρα ισχύει το 2.

Ενα άμεσο συμπέρασμα που έχουμε από το 2, είναι ότι το σώμα F έχει βαθμό υπερβατικότητος 1 πάνω από το σώμα k. Συνεπώς αφού $F \cap \bar{k} = k$, συνεπάγεται ότι υπάρχει καμπύλη E'/k τέτοια ώστε $F = k(E')$ ([Si1], θεώρημα 2.4, σελ. 25). Επιλέον το 2 μας δίνει ότι:

$$\bar{k}(E') = \bar{k}F = \bar{k}(E)_\xi \cong \bar{k}(E).$$

Αρα οι καμπύλες E και E' είναι ισόμορφες πάνω από το σώμα $\bar{k}$, δηλαδή η E' είναι twist της E. Απομένει λοιπόν να αποδείξουμε ότι μας δίνουν την ίδια κλάση συνομολογίας $\{\xi\}$.

3. Απόδειξη του επί:

   Εστω $\varphi : E' \to E$, ο $\bar{k}$-ισομορφισμός που αντιστοιχεί στον ισομορφισμό των σωμάτων συναρτήσεων $Z : \bar{k}(E) \to \bar{k}(E)_\xi \cong \bar{k}F = \bar{k}(E')$. Δηλαδή $\varphi^* = Z$ (όπου φ^* το pullback της φ, δες [Si1], σελ. 23). Συνεπώς η σχέση $Z(h)^s = Z(h^s\xi_s)$, γράφεται:

   $$Z(h)^s = \varphi^*(h)^s = (h\varphi)^s = h^s\xi_s\varphi \Rightarrow h^s\varphi^s = h^s\xi_s\varphi \Rightarrow \varphi^s = \xi_s\varphi,$$

   που μας δίνει το ζητούμενο. $\square$

5.3 Κάποια τεχνικά λήμματα

Εστω τώρα K μία πεπερασμένη επέκταση του σώματος k. Αν E/k είναι μία ελλειπτική καμπύλη και E'/k twist της καμπύλης E, τότε υπάρχει $\bar{k}$-ισομορφισμός $\varphi : E' \to E$, τέτοιος ώστε για κάθε 1-συνκύκλο $\xi = \xi_s$ της G που παίρνει τιμές στην $Aut_{\bar{k}}(E)$, ισχύει ότι $\varphi^s = \xi_s \circ \varphi$ για κάθε $s \in G = Gal(\bar{k}/k)$. Ιδιαίτερα αυτό ισχύει για κάθε 1-συνκύκλο της G που παίρνει τιμές στην $Aut_K(E)$. Επομένως για κάθε $P \in E'(K)$, έχουμε:

$$(\varphi(P^{s^{-1}}))^s = (\xi_s \circ \varphi)(P)$$

Ισχύει ότι:

$$\varphi(E'(k)) = \{P \in E(K)/P^s = \xi_s(P), \forall s \in G\} \quad (*).$$

Πράγματι, ας πάρουμε $P \in \varphi(E'(k))$. Τότε υπάρχει μοναδικό $Q \in E'(k)$, τέτοιο ώστε $P = \varphi(Q)$. Εχουμε:

$$P^s = \varphi(Q)^s = (\xi_s \circ \varphi)(Q^s) = \xi_s \circ \varphi(Q) = \xi_s(P).$$

Δηλαδή $\varphi(E'(k)) \subseteq \{P \in E(K)/P^s = \xi_s(P), \forall s \in G\}$. Για τον αντίστροφο εγκλεισμό τώρα, ας πάρουμε $P \in E(K)$, τέτοιο ώστε $P^s = \xi_s(P), \forall s \in G$. Τότε λόγω $\bar{k}$-ισομορφίας της απεικόνισης φ έχουμε ότι υπάρχει στοιχείο $Q \in E'(\bar{k})$ τέτοιο ώστε $P = \varphi(Q)$. Επομένως $\varphi(Q)^s = \xi_s\varphi(Q^s)$, και επιπλέον ισχύει ότι $\varphi(Q)^s = P^s = \xi_s(P) = \xi_s \circ \varphi(Q)$. Συνεπώς

$\xi_s \circ \varphi(Q) = \xi_s \circ \varphi(Q^s)$, δηλαδή $\varphi(Q) = \varphi(Q^s)$. Αρα $Q = Q^s$, για κάθε $s \in G$. Επομένως $Q \in E'(k)$, δηλαδή έχουμε και το αντίστροφο εγκλεισμό.

Λήμμα 5.7 $G = Gal(\mathrm{K}/k)$ G n, G $e := e(G)$. E/k, $Aut_{\bar{k}}(E)$ e- E^i *twist* E K- $\varphi_i : E^i \to E$, i $\{1, \cdots, n\}$, - :

$$\bigoplus_{i=1}^{n} E^i(k) \xrightarrow{\oplus \varphi_i} E(K),$$

n.

<u>Απόδειξη :</u> Εστω $\omega \in Aut_{\bar{k}}(E)$, πρωταρχική e-ρίζα της μονάδας και $R := \mathbb{Z}[\omega] \subseteq End_k(E)$. Προφανώς ο R είναι ακεραία περιοχή. Επιπλέον η δράση της ομάδος G στην $E(K)$, επάγει κατά φυσιολογικό τρόπο δράση του δακτυλίου ομάδος $R[G]$ στην ομάδα $E(K)$. Επίσης έχουμε n διαφορετικούς ομομορφισμούς (χαρακτήρες) της ομάδος G :

$$\chi_i : G \to <\omega> \subset R, \quad \text{όπου} \quad i \in \{1, \cdots, n\}.$$

Για κάθε $i \in \{1, \cdots, n\}$ ορίζουμε τα εξής στοιχεία:

$$e_i := \sum_{s \in G} \chi_i(s^{-1}) s \in R[G]$$

Επίσης θεωρούμε το σύνολο:

$$E(K)^i := \{P \in E(K)/P^s = \chi_i(s)P, \ \ \forall s \in G\}$$

Παρατηρούμε ότι $e_i E(K) \subseteq E(K)^i$. Πράγματι, $e_i P = \sum_{s \in G} \chi_i(s^{-1}) P^s$. Συνεπώς αρκεί να αποδείξουμε ότι $(e_i P)^t = \chi_i(t)(e_i P)$, για κάθε $t \in G$. Εχουμε:

$$\chi_i(t)(e_i P) = \chi_i(t) \sum_{s \in G} \chi_i(s^{-1}) P^s = \sum_{s \in G} \chi_i(ts^{-1}) P^s.$$

Θέτουμε $g^{-1} := ts^{-1}$, δηλαδή $s = tg$. Επομένως:

$$\chi_i(t)(e_i P) = \sum_{g \in G} \chi_i(g^{-1}) P^{tg}.$$

Από την άλλη πλευρά όμως $t(e_i P) = \sum_{s \in G} \chi_i(s^{-1}) P^{ts}$. Αρα πράγματι ισχύει ότι $e_i E(K)$ περιέχεται στην ομάδα $E(K)^i$, για κάθε $i \in \{1, \cdots, n\}$.

Επίσης λόγω των σχέσεων ορθογωνιότητας των χαρακτήρων, ισχύει ότι $\sum_{i=1}^{n} e_i = n$. Συνεπώς :

$$\sum_{i=1}^{n} e_i E(K) \subseteq \sum_{i=1}^{n} E(K)^i \Longrightarrow n \cdot E(K) \subseteq \sum_{i=1}^{n} E(K)^i. \tag{19}$$

Η δράση κάθε στοιχείου e_i στα στοιχεία της ομάδος $E(K)^i$, δίνεται με πολλαπλασιασμό με $\sum_{s\in G} \chi_i(s^{-1})\chi_j(s) = n\delta_{ij}$ (λόγω των σχέσεων ορθογωνιότητας των χαρακτήρων). Επομένως για κάθε $i \in \{1, \cdots, n\}$, έχουμε:

$$n \cdot (E(K)^i \bigcap \sum_{j\neq i} E(K)^j) = 0. \tag{20}$$

Επιπλέον παρατηρούμε ότι κάθε χ_i, $i \in \{1, \cdots, n\}$, είναι ένας 1-συνκύκλος της ομάδας G με τιμές στην ομάδα $Aut_K(E)$. Σύμφωνα με το θεώρημα 5.5, στον 1-συνκύκλο χ_i αντιστοιχεί μία ελλειπτική καμπύλη, έστω E^i, η οποία είναι twist της E και συνεπώς υπάρχε $\bar{k}$-ισομορφισμός $\varphi_i : E^i \to E$, τέτοιος ώστε $\varphi_i(E^i(k)) = E(K)^i$ λόγω της σχέσης $(*)$. Δηλαδή μπορούμε εντελώς φυσιολογικά να ορίσουμε την απεικόνιση:

$$\oplus_{i=1}^{n}\varphi_i : \begin{cases} \oplus_{i=1}^{n} E^i(k) \longrightarrow E(K) \\ \sum_{i=1}^{n} a_i \mapsto \sum_{i=1}^{n} \varphi_i(a_i) \end{cases},$$

όπου $a_i \in E^i(k)$ και $\varphi_i(a_i) \in E(K)^i$. Εξετάζουμε τώρα αν ο n μηδενίζει τον πυρήνα και τον συνπυρήνα της απεικόνισης $\oplus_{i=1}^{n}\varphi_i$.

Ο συνπυρήνας της φ μηδενίζεται από τον n, λόγω της σχέσεως (19) και ο πυρήνας λόγω της σχέσης (20). □

<u>Παρατήρηση :</u> Η ομάδα $\varphi_i(E^i(k)) = E(K)^i$, είναι εκ κατασκευής G-αναλλοίωτη. Επιπλέον αν ισχύει ότι $\chi_i(G) \subseteq \{\pm 1\}$, (π.χ $e = 2$) τότε όλες οι υποομάδες της $E(K)^i$ είναι G-αναλλοίωτες. Πράγματι, αν $\mathcal{H}$ είναι μία υποομάδα της $E(K)^i$ και $a \in \mathcal{H}$, τότε $a^s = \pm a \in \mathcal{H}$, δηλαδή η $\mathcal{H}$ είναι G-αναλλοίωτη υποομάδα της $E(K)^i$.

Πόρισμα 5.8 5.7, :

1. $rk[E(K)] = \sum_{i=1}^{n} rk[E^i(k)]$, $rk[E(K)]$ *rank* $E(K)$.

2. p $\mathbb{Q}$. n_p p- n (p n $\mathbb{Q}$). n_p :

$$\oplus_{i=1}^{n} E^i(k)_{(p)} \longrightarrow E(K)_{(p)},$$

$\oplus_{i=1}^{n}\varphi_i$ p- .

Απόδειξη :

1. Ισχύει ότι $\sum_{i=1}^{n} E(K)^i \cong \oplus_{i=1}^{n} E^i(k)/Ker(\oplus_{i=1}^{n}\varphi_i)$. Επίσης ο πυρήνας της απεικόνισης $\oplus_{i=1}^{n}\varphi_i$, μηδενίζεται από τον n. Συνεπώς ο πυρήνας $ker(\oplus_{i=1}^{n}\varphi_i)$, περιέχει μόνο σημεία πεπερασμένης τάξης της ομάδας $\oplus_{i=1}^{n} E^i(k)$ και επομένως δεν επηρεάζει καθόλου τον rank στην ομάδα πηλίκων. Αρα ισχύει ότι $\sum_{i=1}^{n} rk[E(K)^i] = \sum_{i=1}^{n} rk[E^i(k)]$. Επίσης προφανώς ισχύει ότι $\sum_{i=1}^{n} E(K)^i \subseteq E(K)$, επομένως $\sum_{i=1}^{n} rk[E(K)^i] \leq rk[E(K)]$. Ομως $nE(K) \subseteq \sum_{i=1}^{n} E(K)^i$. Αρα:

$$n \cdot rk[E(K)] \leq \sum_{i=1}^{n} rk[E(K)^i] \Rightarrow rk[E(K)] \leq \sum_{i=1}^{n} rk[E(K)^i]$$

$$\Rightarrow rk[E(K)] = \sum_{i=1}^{n} rk[E(K)^i] = \sum_{i=1}^{n} rk[E^i(k)].$$

2. Αν τώρα περιοριστούμε στα p-κομμάτια των ομάδων $\oplus_{i=1}^{n} E^i(k)$ και $E(K)$, τότε ο πυρήνας και ο συν-πυρήνας της απεικόνισης $\oplus_{i=1}^{n}\varphi_i$ είναι τάξης δύναμη του p και συνεπώς μόνο το p-κομμάτι του n, n_p παίζει ρόλο. Αρα ισχύει το ζητούμενο. □

Εξετάζουμε τώρα την ειδική περίπτωση όπου η ομάδα Galois $G = Gal(K/k)$, είναι η λεγόμενη στοιχειώδης 2-αβελιανή ομάδα $G = \mathcal{C}_2^m = \oplus_{i=1}^{m}\mathbb{Z}/2\mathbb{Z}$, όταν η χαρακτηριστική του σώματος k είναι διαφορετική του 2. Τότε υπάρχει k-βάση $\{\theta_1, \theta_2, \cdots, \theta_n\}$ όπου $n = 2^m$, του σώματος K τέτοια ώστε $\theta_i^s = \pm\theta_i$ για κάθε $s \in G$ και για κάθε $i \in \{1, \cdots, n\}$. Ορίζουμε $z_i := \theta_i^2 \in k$. Αφού $e = e(G) = 2$, οι χαρακτήρες $\chi_i : G \to \{\pm 1\}$ που ορίζονται $s \mapsto \theta_i^s\theta_i^{-1}$, είναι όλοι διαφορετικοί μεταξύ τους. Την twist της E με z_i θα την συμβολίζουμε με $E^{(z_i)}$, $i \in \{1, 2, \cdots, n\}$. Τέλος για τους K-ισομορφισμούς f^i, $f^i : E^{(z_i)} \to E$, ισχύει ότι:

$$(f^i(a))^s = \chi_i(s) f^i(a), \forall s \in G, \forall a \in E^{(z_i)}(K).$$

Για κάθε αβελιανή ομάδα V, ορίζουμε το σύνολο $V_{(n)} := \cup_{i\geq 1} V_{n^i}$. Αποδεικνύουμε το εξής λήμμα:

Λήμμα 5.9 k $char(k) \neq 2$ $G = Gal(\bar{k}/k)$ 2- . :

1. $E(K)_{(2)} \neq (0)$, $E(k)_2 \neq 0$.

2. $i \neq 1$, f_i 2- E $E^{(z_i)}$ k, $E^{(z_i)}(k)_2 \cong E(k)_2$. :

$$id \oplus f^i : E(k) \oplus E^{(z_i)}(k) \longrightarrow E(K),$$

$E(k)_2$.

<u>Απόδειξη :</u>

1. Αν $E(K)_{(2)} \neq \{0\}$, τότε η $E(K)_2 \neq \{0\}$ είναι μη-μηδενικό $\mathbb{F}_2[G]$-module. Επειδή όμως η G είναι 2-ομάδα, συνεπάγεται ότι δρα τετριμμένα στα υπο-module της $E(K)_2$. Αρα αυτά τα υπο-module περιέχονται στην $E(k)_2$.

2. Για κάθε $a \in E^{(z_i)}(k)_2$, $f^i(a) \in E(K)_2$ και εξ ορισμού $(f^i(a))^s = \chi_i(s) f^i(a)$ $\forall s \in G$. Ομως $\chi_i(s) f^i(a) = f^i(a)$, διότι $\chi_i(s) = \pm 1$. Επομένως $f^i(a) \in E(k)_2$ για κάθε $a \in E^{(z_i)}(k)_2$. Ομοια η $(f^i)^{-1}$ απεικονίζει την $E(k)_2$ στην $E^{(z_i)}(k)_2$. Επίσης αν πάρουμε το στοιχείο $(a, a_i) \in E(k) \oplus E^{(z_i)}(k)$, τότε αυτό ανήκει στον πυρήνα της απεικόνισης $id \oplus f^i$, εαν και μόνο εάν $a + f^i(a_i) = 0 = (a + f^i(a_i))^s = a - f^i(a_i)$, όπου το στοιχείο $s \in G$ και είναι τέτοιο ώστε $\chi_i(s) = -1$. Αυτό όμως είναι ισοδύναμο με το γεγονός ότι $2f^i(a_i) = 0$. Τότε όμως (και μόνο τότε) ισχύει ότι και $2a = 0$. Επίσης $a = f^i(a_i)$, δηλαδή $a_i = (f_i)^{-1}(a)$. Αρα:

$$ker(id \oplus f^i) = \{(a, (f^i)^{-1}(a)) / a \in E(k)_2\} \cong E(k)_2,$$

διότι $(f^i)^{-1} : E(k)_2 \xrightarrow{\cong} E^{(z^i)}(k)_2$, όπως αποδείξαμε στο ερώτημα 1. □

Εστω E ελλειπτική καμπύλη οριομένη στο σώμα $\mathbb{Q}$ και έστω $K/\mathbb{Q}$ πεπερασμένη στοιχειώδης 2-αβελιανή επέκταση. Τότε όπως είναι γνωστό μπορούμε πάντα να διαλέξουμε μια $\mathbb{Q}$-βάση του K, $\{\theta_1, \cdots, \theta_n\}$, τέτοια ώστε $\theta_i^2 = z_i \in \mathbb{Z}$. Αν η καμπύλη E έχει εξίσωση του Weierstrass:

$$E : Y^2 = X^3 + AX + B, A, B \in \mathbb{Z},$$

τότε οι twist της E, $E^{(z_i)}$ έχουν εξίσωση:

$$\mathrm{E}^{(z_i)} : Y^2 = X^3 + Az_i^2 X + z_i^3 B$$

και οι ισομορφισμοί $f^i : E^{(z_i)} \to E$, τέτοιοι ώστε $(f^i(e))^s = \chi_i(s) f^i(e)$ για κάθε $s \in G$ και $e \in E^{(z_i)}(\mathbb{Q})$, όπου $e = (x, y)$, δίνονται από την σχέση $f^i(x, y) = (z_i^{-1} x, \theta_i^{-1} z_i^{-1} y)$.

5.4 Αυτομορφισμοί

Σε αυτή την παράγραφο θα ασχοληθούμε με ομάδες αυτομορφισμών που έχουν την ειδική μορφή $Aut(\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z})$, όπου $a, b \in \mathbb{Z}$ λόγω του ότι θα μας χρειαστούν στην συνέχεια. Εστω R ένας αντιμεταθετικός δακτύλιος ο οποίος να έχει ένα μηδενοδύναμο μέγιστο ιδεώδες M, δηλαδή υπάρχει $a \in \mathbb{Z}$ τέτοιο ώστε $M^a = (0)$ ενώ $M^{a-1} \neq (0)$. Εστω δε $I := M^b$ ένα μη-τετριμμένο ιδεώδες του δακτυλίου R όπου $0 < b < a$. Θεωρούμε το R-module $V := R \oplus R/I$. Τότε ο δακτύλιος των ενδομορφισμών του V είναι ισόμορφος με τον γενικευμένο πίνακα-δακτύλιο:

$$End_R(V) \cong \begin{pmatrix} R & Ann_R(I) \\ R/I & R/I \end{pmatrix},$$

διότι αν με $[r]$ συμβολίσουμε τνν κλάση του στοιχείου r στον δακτύλιο R/I τότε ο πίνακας:

$$\begin{pmatrix} r & j \\ [s] & [t] \end{pmatrix} \in \begin{pmatrix} R & Ann_R(I) \\ R/I & R/I \end{pmatrix},$$

δρα στο στοιχείο $\begin{pmatrix} u \\ [v] \end{pmatrix} \in V$, ως εξής:

$$\begin{pmatrix} r & j \\ [s] & [t] \end{pmatrix} \cdot \begin{pmatrix} u \\ [v] \end{pmatrix} = \begin{pmatrix} ru + jv \\ [su + tv] \end{pmatrix}.$$

Επίσης αν συμβολίσουμε με Γ την ομάδα των R-αυτομορφισμών του V, τότε η Γ θα είναι η ομάδα των μονάδων του παραπάνω πίνακα-δακτυλίου. Αν λοιπόν συμβολίζουμε με $U(\cdot)$ τις ομάδες μονάδων, τότε είναι προφανές ότι ισχύει:

$$\Gamma = \begin{pmatrix} U(R) & Ann_R(I) \\ R/I & U(R/I) \end{pmatrix} \qquad (1).$$

Θεωρούμε τώρα την περίπτωση όπου $R := \mathbb{Z}/2^a\mathbb{Z}$ και $I = 2^bR$, όπου $0 < b < a$. Αποδεικνύουμε το ακόλουθο λήμμα:

Λήμμα 5.10 $\Gamma_{a,b} := Aut(\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z})$, a, b $a > b$ $R = \mathbb{Z}/2^a\mathbb{Z}$. *:*

1. $\Gamma_{a,b}$ 2^{a+3b-2}. $b = 1$, $\Gamma_{a,1}$ N U, *:*

$$N := \begin{pmatrix} 1 + 2R & 2^{a-1}R \\ [0] & [1] \end{pmatrix} \cong (1 + 2R, \cdot) \oplus (2^{a-1}R, +)$$

$$U \cong \begin{pmatrix} 1 & 0 \\ R/2R & [1] \end{pmatrix} \cong \mathbb{Z}/2\mathbb{Z},$$

modulo $2R$.

2. O 2- $\Gamma_{a,1}$, $A \subseteq \Gamma_{a,1}$ 8 *(* 4 α = 2 *)*, A 2 $\Gamma_{a,1}$, -

$$D := \begin{pmatrix} 1+2R & 0 \\ [0] & [1] \end{pmatrix}.$$

3. $a = 2$ 3, - A .

<u>Απόδειξη :</u>

1. Αντικαθιστούμε $R = \mathbb{Z}/2^a\mathbb{Z}$ και $I = 2^bR$ στην σχέση (1) :

$$\Gamma_{a,b} = \begin{pmatrix} U(\mathbb{Z}/2^a\mathbb{Z}) & Ann_R(2^bR) \\ \frac{\mathbb{Z}/2^a\mathbb{Z}}{2^bR} & U(\frac{\mathbb{Z}/2^a\mathbb{Z}}{2^bR}) \end{pmatrix}.$$

Εχουμε $\#U(\mathbb{Z}/2^a\mathbb{Z}) = \varphi(2^a) = 2^{a-1}$, όπου φ είναι η συνάρτηση του Euler.

$$\text{Επίσης, } \#\frac{\mathbb{Z}/2^a\mathbb{Z}}{2^b \cdot \mathbb{Z}/2^a\mathbb{Z}} = 2^b \text{ και, } \#U(R/2^bR) = \varphi(2^b) = 2^{b-1}.$$

Τέλος ο μηδενιστής του 2^bR είναι ισόμορφος με την ομάδα πηλίκων $\mathbb{Z}/2^b\mathbb{Z}$, και επομένως $\#Ann_R(2^bR) = 2^b$. Αρα:

$$\#\Gamma_{a,b} = 2^{a-1} \cdot 2^b \cdot 2^{b-1} \cdot 2^b = 2^{a+3b-2}.$$

Εστω $b = 1$. Τότε

$$I = 2R, \quad R/2R \cong \mathbb{Z}/2\mathbb{Z}, \quad U(R/2R) = [1], \quad Ann_R(I) = 2^{a-1}R.$$

Επομένως έχουμε:

$$\Gamma_{a,1} \cong \begin{pmatrix} U(R) & 2^{a-1}R \\ \mathbb{Z}/2\mathbb{Z} & U(\mathbb{Z}/2\mathbb{Z}) \end{pmatrix}$$

Αναγάγουμε τώρα τον $\Gamma_{a,1}$ modulo $2R$ και παίρνουμε τον εξής πίνακα-δακτύλιο:

$$\tilde{\Gamma}_{a,1} \cong \begin{pmatrix} 1 & 0 \\ R/2R & [1] \end{pmatrix} mod 2R$$

Δηλαδή $\tilde{\Gamma}_{a,1} \equiv Umod2R$. Ο πυρήνας της απεικόνισης αναγωγής modulo $2R$ είναι ο πίνακας:

$$N := \begin{pmatrix} 1+2R & 2^{a-1}R \\ [0] & [1] \end{pmatrix}.$$

Αρα έχουμε την μικρή ακριβή ακόλουθία:

$$0 \longrightarrow N \longrightarrow \Gamma_{a,1} \longrightarrow U \longrightarrow 0,$$

που είναι ισοδύναμο με το γεγονός ότι η $\Gamma_{a,1}$, είναι ισόμορφη με το ημιευθύ άθροισμα των N και U. Επίσης είναι προφανές ότι:

$$N = \begin{pmatrix} 1+2R & 2^{a-1}R \\ [0] & [1] \end{pmatrix} \cong (1+2R, \cdot) \oplus (2^{a-1}R, +)$$

και $U \cong \mathbb{Z}/2\mathbb{Z}$, ενώ ο γεννήτορας του U είναι ο

$$u := \begin{pmatrix} 1 & 0 \\ [1] & [0] \end{pmatrix}.$$

2. Παρατηρούμε ότι ο κεντροποιητής (centralizer) του $u \in U$ στον N, είναι ο διαγώνιος πίνακας:

$$D := \begin{pmatrix} 1+2R & 0 \\ [0] & [1] \end{pmatrix}$$

Αν τώρα A είναι στοιχειώδης 2-αβελιανή υποομάδα της $\Gamma_{a,1}$, τότε:

(a) Εάν $A \subseteq N$, τότε η A θα έχει τάξη το πολύ 8 διότι:

$$U(R) \cong 1+2R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}, \quad \text{ενώ} \quad 2^{a-1}R = \mathbb{Z}/2\mathbb{Z}, \quad \text{δηλαδή:}$$

$$N \cong \begin{pmatrix} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ [0] & [1] \end{pmatrix}$$

Συνεπώς η $A \subseteq N$ είναι στοιχειώδης 2-αβελιανή ομάδα μόνο για $a = 2$ ή $a = 3$. Μάλιστα παρατηρούμε ότι για $a = 2$ η τάξη της A είναι το πολύ 4.

(b) Αν τώρα $A \not\subseteq N$ τότε η υποομάδα A θα περιέχει στοιχείο της μορφής $g = nu$, όπου $n \in N$ και $A =< N \cap A, g >$. Επίσης η ομάδα $N \cap A$ κεντροποιεί το στοιχείο g διότι $g \in A$ και η A είναι στοιχειώδης 2-αβελιανή ομάδα. Επομένως η $N \cap A$ κεντροποιεί και το u διότι η N είναι αβελιανή ομάδα ως ευθύ άθροισμα κυκλικών ομάδων. Συνεπάγεται λοιπόν ότι η ομάδα $N \cap A$ περιέχεται στον κεντροποιητή του u στο N δηλαδή περιέχεται στον διαγώνιο ομάδα-πίνακα D που ορίσαμε προηγουμένως. Αρα πράγματι ο A έχει τάξη το πολύ 8 (και 4, για $a = 2$).

Επιπλέον παρατηρούμε, οτι σε κάθε περίπτωση $[A : A \cap D] \leq 2$, διότι $\#\text{A} \leq 8$, $\#D \leq 4$.

3. Τέλος για $a = 2$, ή $a = 3$ κάθε στοιχείο $g \in \Gamma_{a,1}$, τάξης 2 είναι άνω ή κάτω τριγωνικό. Αν ο g είναι ο πίνακας:

$$\begin{pmatrix} 1+i & j \\ [0] & [1] \end{pmatrix},$$

τότε ο g είναι ούτως ή άλλως άνω τριγωνικός. Θα αποδείξουμε ότι εάν ο g δεν είναι ο παραπάνω πίνακας, τότε είναι κάτω τριγωνικός. Πράγματι εάν ένα στοιχείο $g \in \Gamma$ έχει τάξη 2,

$$g = \begin{pmatrix} i+1 & j \\ [1] & [1] \end{pmatrix}, \quad \text{όπου} \quad i \in 2R, \quad j \in 2^{a-1}R, \quad \text{τότε:}$$

$$g^2 \begin{pmatrix} u \\ [v] \end{pmatrix} = \begin{pmatrix} u \\ [v] \end{pmatrix},$$

για κάθε $\begin{pmatrix} u \\ [v] \end{pmatrix}$ και άρα και για $u = 1, v = 0$. Εχουμε :

$$\begin{pmatrix} 1+i & j \\ [1] & [1] \end{pmatrix}^2 \cdot \begin{pmatrix} 1 \\ [0] \end{pmatrix} = \begin{pmatrix} 1+i & j \\ [1] & [1] \end{pmatrix} \cdot \begin{pmatrix} 1+i \\ [1] \end{pmatrix} =$$

$$= \begin{pmatrix} (1+i)^2 + j \\ 2+i \end{pmatrix} = \begin{pmatrix} 1 \\ [0] \end{pmatrix}.$$

Συνεπώς $(1+i)^2 + j = 1$ και $[2+i] = [0]$. Το δεύτερο ισχύει διότι $i \in 2R$. Η σχέση $(1+i)^2 + j = 1$, μας δίνει ότι $i^2 + 2i + j = 0 \Rightarrow i(i+2) + j = 0$. Τώρα, επειδή το $i \in 2R$ γράφεται στην μορφή $i = 2i_1$, όπου $i_1 \in R$ και επομένως $i(i+2) = 4i_1(i_1+1) \in 8R$, διότι είτε $i_1 \in 2R$ είτε $i_1 \in 2R+1$ που και οι δύο περιπτώσεις μας δίνουν ότι $i(i+2) \in 8R$. Συνεπάγεται λοιπόν ότι $j \in 8R$. Ομως

$a \leq 3$ και επομένως $j = 0$. Αρα ο πίνακας g είναι κάτω τριγωνικός, δηλαδή ισχύει το ζητούμενο. $\square$

5.5 Στοιχειώδεις 2-αβελιανές επεκτάσεις του $\mathbb{Q}$

Εστω E μια ελλειπτική καμπύλη ορισμένη στο σώμα $\mathbb{Q}$ και έστω $F \supset \mathbb{Q}$ η μέγιστη 2-αβελιανή επέκταση του $\mathbb{Q}$, δηλαδή $F = \mathbb{Q}(\sqrt{z} \mid z \in \mathbb{Z})$. Σκοπός αυτής της παραγράφου είναι ο προσδιορισμός όλων των δυνατών υποομάδων πεπερασμένης τάξης $E_{tor}(F)$ της ομάδος $E(F)$. Το επόμενο θεώρημα είναι θεμελιώδους σημασίας για τα παρακάτω και το αναφέρουμε χωρίς απόδειξη ([Ke 1], [Ke 2], [Ke 3], [Ke 4], [Ke 5], [Ke 6], [Ke 7], [Maz]):

Θεώρημα 5.11 E $\mathbb{Q}$.

1. **(Mazur)** $E_{tor}(\mathbb{Q})$, 15 :

$$\mathbb{Z}/m\mathbb{Z} \qquad 1 \leq m \leq 10 \quad m = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq n \leq 4.$$

2. **(Kenku)** $E_{tor}(\bar{\mathbb{Q}})$ ($Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-) $\mathbb{Z}/n\mathbb{Z}$, :

$$n \leq 19 \qquad\qquad n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

Πρώτα θα περιγράψουμε όλες τις δυνατότητες για την υποομάδα πεπερασμένης τάξης

$$E(F)_{2'} := \{e \in E(F)/ne = 0, \quad \text{για κάποιον } n \text{ περιττό}\}.$$

Θεώρημα 5.12 $E(F)_{2'}$:

$$\mathbb{Z}/m\mathbb{Z} \quad m \in \{1, 3, 5, 7, 9, 15\}, \qquad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Απόδειξη : Κατ' αρχήν είναι προφανές ότι αρκεί να αποδείξουμε το ζητούμενο για όλες τις πεπερασμένες επεκτάσεις $K/\mathbb{Q}$ τέτοιες ώστε $K \subset F$. Ας σταθεροποιήσουμε μία επέκταση $K/\mathbb{Q}$, με ομάδα Galois $G = \oplus_{i=1}^{m} \mathbb{Z}/2\mathbb{Z}$ όπου m ένας φυσικός αριθμός. Τότε από το πόρισμα 5.8 έχουμε ότι:

$$E(K)_{2'} \cong E^{(z_1)}(\mathbb{Q})_{2'} \oplus \cdots \oplus E^{(z_n)}(\mathbb{Q})_{2'},$$

διότι από το εν λόγω πόρισμα έχουμε ότι για κάθε πρώτο αριθμό p ο πυρήνας και ο συν-πυρήνας της απεικόνισης $E^{(z_i)}(\mathbb{Q})_{(p)} \stackrel{\oplus f^i}{\rightarrow} E(K)_{(p)}$ μηδενίζονται από τον αριθμό n_p που είναι το p-κομμάτι του $n = \#G$. Ομως η G είναι 2-ομάδα και συνεπώς για κάθε πρώτο αριθμό p, $p \neq 2$ έχουμε ότι $n_p = 1$. Επιπλέον τα σημεία πεπερασμένης τάξης που περιέχει η ομάδα $E(F)_{2'}$ είναι μόνο περιττού βαθμού. Επομένως ο πυρήνας και ο συν-πυρήνας (για κάθε i) μηδενίζονται από το 1, δηλαδή είναι ισομορφισμοί. Παίρνοντας λοιπόν το ευθύ άθροισμα ως προς όλα τα i έχουμε το ζητούμενο. Σύμφωνα με την παρατήρηση της δευτέρας παραγράφου (σελ. 89), κάθε ευθύς προσθεταίος της $E(K)_{2'}$, είναι ρητή υποομάδα του $\mathbb{Q}$. Παρατηρούμε μάλιστα ότι κάθε ευθύς προσθεταίος, $E^{(z_i)}(\mathbb{Q})_{2'}$, είναι ισόμορφος με μία από τις ομάδες $\mathbb{Z}/m\mathbb{Z}$ όπου $m \in \{1, 3, 5, 7, 9\}$, διότι αλλιώς θα είχαμε άτοπο από το θεώρημα του Mazur. Σημειώνουμε επίσης ότι κάθε μία από τις ομάδες $\mathbb{Z}/m\mathbb{Z}$, $m \in \{5, 7, 9\}$ μπορεί να εμφανιστεί το πολύ μια μόνο φορά ως ευθύς προσθεταίος στην $E(K)_{2'}$, διότι εάν εμφανιζόταν κάποια από αυτές δύο φορές τότε το K θα περιείχε μία m-ρίζα της μονάδος ([Shi], πρόταση 4.2, σελ. 101) το οποίο είναι άτοπο, διότι η ομάδα Galois G έχει βαθμό 2. Επίσης το πολύ δύο από τις ομάδες $E^{(z_i)}(\mathbb{Q})_{2'}$ θα περιέχουν "αντίγραφο" της ομάδος $\mathbb{Z}/3\mathbb{Z}$. Εξετάζουμε τέλος ποιοί από τους συνδιασμούς των παραπάνω ομάδων μπορούν να εμφανιστούν.

Κατ' αρχήν οι ομάδες $\mathbb{Z}/5\mathbb{Z}$ και $\mathbb{Z}/7\mathbb{Z}$, δεν είναι δυνατόν να εμφανιστούν συγχρόνως ως ευθείς προσθεταίοι στην ομάδα $E(K)_{2'}$ διότι σε αυτήν την περίπτωση η ομάδα $E(K)$ θα περιείχε ρητή υποομάδα ισόμορφη με την $\mathbb{Z}/35\mathbb{Z}$ πράγμα που είναι άτοπο λόγω του θεωρήματος του Kenku. Κατά εντελώς όμοιο τρόπο συμπεραίνουμε ότι οι ομάδες $\mathbb{Z}/5\mathbb{Z}$, και $\mathbb{Z}/9\mathbb{Z}$ καθώς και οι ομάδες $\mathbb{Z}/7\mathbb{Z}$ και $\mathbb{Z}/9\mathbb{Z}$ δεν εμφανίζονται ως ευθείς προσθεταίοι της ομάδος $E(K)_{2'}$. Απομένει δηλαδή να εξετάσουμε τα ζεύγη ομάδων ($\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$) και ($\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$).

Ισχυριζόμαστε ότι οι ομάδες $\mathbb{Z}/9\mathbb{Z}$ και $\mathbb{Z}/3\mathbb{Z}$ δεν μπορούν να εμφανιστούν συγχρόνως ως υποομάδες της $E(K)_{2'}$. Εστω ότι δεν ίσχυε ο ισχυρισμός. Τότε θα υπήρχαν υποομάδες $E^{(z_i)}(\mathbb{Q})_{2'} \cong \mathbb{Z}/9\mathbb{Z}$ και $E^{(z_j)}(\mathbb{Q})_{2'} \cong \mathbb{Z}/3\mathbb{Z}$ της ομάδος $E(K)_{2'}$. Αντικαθιστώντας τώρα την $E^{(z_i)}$ με την E μπορούμε να υποθέσουμε ότι $E(\mathbb{Q})_{2'} \cong \mathbb{Z}/9\mathbb{Z}$ και $E^{(z_i z_j)}(\mathbb{Q})_{2'} \cong \mathbb{Z}/3\mathbb{Z}$. Τότε όμως θα υπήρχε ισογενής της καμπύλης E που θα είχε ρητή κυκλική υποομάδα τάξης 27. Γνωρίζουμε όμως ότι κάθε σημείο της modular καμπύλης $X_0(27)|_{\mathbb{Q}}$ αντιστοιχεί σε ελλειπτική καμπύλη με συντελεστές στο σώμα $\mathbb{Q}$ που περιέχει ρητή κυκλική υποομάδα τάξης

27 ([Si1], σελ. 353). Ομως η modular καμπύλη $X_0(27)$ έχει μόνο ένα ρητό σημείο που δεν είναι ακίδα (cusp) και αυτό το σημείο αντιστοιχεί σε ελλειπτική καμπύλη E που έχει μιγαδικό πολλαπλασιασμό, δακτύλιο ενδομορφισμών τον $\mathbb{Z}(\sqrt{-3})$ και απόλυτη αναλλοίωτο $j = -(12)^3 \cdot (40)^3/9$ ([Ku], λήμμα III2.2, σελ. 213). Ατοπο διότι καμμία ελλειπτική καμπύλη οριομένη στο σώμα $\mathbb{Q}$ δεν έχει τέτοια απόλυτη αναλλοίωτο και σημείο τάξης 9.

Τελος ισχυριζόμαστε ότι οι ομάδες $\mathbb{Z}/3\mathbb{Z}$ και $\mathbb{Z}/7\mathbb{Z}$ δεν μπορούν να εμφανιστούν συγχρόνως ως υποομάδες της $E(K)_{2'}$. Εστω ότι δεν ίσχυε ο ισχυρισμός. Τότε οι δύο αυτές υποομάδες θα γεννούσαν μια ρητή κυκλική υποομάδα της $\bar{E}(\mathbb{Q})$ τάξης 21. Ομως η modular καμπύλη $X_0(21)$ έχει 4 ρητά σημεία που κανένα από αυτά δεν είναι ακίδα (cusp) και καθένα από αυτά τα σημεία αντιστοιχεί σε ελλειπτκή καμπύλη στο $\mathbb{Q}$ με οδηγό (conductor) της μορφής $2^a \cdot 3^b$, όπου a, b φυσικοί αριθμοί ([MF IV], σελ. 80 και 124). Επομένως η καμπύλη E καλή αναγωγή modulo 5. Εστω $E^{(z_1)}(\mathbb{Q})_{2'} \cong \mathbb{Z}/3\mathbb{Z}$ και $E^{(z_2)}(\mathbb{Q})_{2'} \cong \mathbb{Z}/7\mathbb{Z}$. Εστω δε $\tilde{E}$ η ανηγμένη καμπύλη modulo 5. Τότε $N_{25} := \#\tilde{E}(\mathbb{F}_{25}) = 21$. Πράγματι έστω $K_i := \mathbb{Q}(\sqrt{z_i})$, $i = 1, 2$ και έστω $\wp_i$ πρώτο ιδεώδες του σώματος K_i που διαιρεί τον 5. Ορίζουμε $F_{\wp_i} := O_{K_i}/\wp_i$, όπου με O_{K_i} συμβολίζουμε τον δακτύλιο των ακεραίων του σώματος K_i. Κάνουμε αναγωγή modulo $\wp_i$ και παίρνουμε την εξή εμφύτευση (πρόταση 3.7, σελ. 36):

$$E(K_i)_{tor} \hookrightarrow \tilde{E}(F_{\wp_i}) \subseteq \tilde{E}(\mathbb{F}_{25}).$$

Συνεπώς $3|N_{25}$ και $7|N_{25}$. Από την άλλη πλευρά όμως το θεώρημα του Hasse (υπόθεση του Riemann), μας δίνει ότι $N_{25} \leq (5+1)^2 = 36$, και συνεπώς $N_{25} = 21$. Ομως $N_{25} = 26 - a_{25}$, όπου $a_{25} = \pi^2 + \bar{\pi}^2$, για κάποιον π μιγαδικό τέτοιον ώστε $\pi\bar{\pi} = 5$ και $a_5 := \pi + \bar{\pi} \in \mathbb{Z}$. Τότε όμως $21 = 26 - a_{25}$ δηλαδή $a_{25} = 5$. Αρα:

$$a_{25} = (\pi + \bar{\pi})^2 - 2\pi \cdot \bar{\pi} = a_5^2 - 2 \cdot 5 \Rightarrow a_5^2 = 15,$$

που είναι άτοπο διότι $a_5 \in \mathbb{Z}$. Αρα πράγματι οι ομάδες $\mathbb{Z}/3\mathbb{Z}$ και $\mathbb{Z}/7\mathbb{Z}$ δεν εμφανίζονται ως υποομάδες της $E(F)_{2'}$. □

Πρόταση 5.13 $E(F)$:

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Απόδειξη : [La-Lo], σελ. 169 − 170. □

Θεώρημα 5.14 E $\mathbb{Q}$ F 2- $\mathbb{Q}$. $E(F)_{tor}$:

$$\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z} \quad b = 1, 2, 3 \quad r = 0, 1, 2, 3,$$

$$\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad b = 1, 2, 3 \quad r = 0, 1,$$

$$\mathbb{Z}/2^{b}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \quad b = 1, 2, 3,$$

$$\mathbb{Z}/2^{b}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad b = 1, 2, 3.$$

$$, \ \{O\}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z}, \quad \mathbb{Z}/7\mathbb{Z}, \quad \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/15\mathbb{Z}.$$

Απόδειξη : Περιγράφουμε κατ' αρχήν όλες τις δυνατότητες της υποομάδας $E(F)_{(2)}$. Αν ισχύει ότι $E(F)_{(2)} \neq \{0\}$ τότε από λήμμα 5.9 έχουμε ότι $E(\mathbb{Q})_2 \neq \{0\}$ και επομένως το 2-σώμα διαίρεσης της E είναι τεραγωνικό υπέρ το $\mathbb{Q}$, δηλαδή περιέχεται στο σώμα F. Από την άλλη πλευρά το 16-σώμα διαίρεσης της E δεν περιέχεται στο σώμα F (διότι αν ναι τότε το σώμα F θα περιείχε μία πρωταρχική 8η ρίζα της μονάδος που είναι άτοπο, αφού η επέκταση $F/\mathbb{Q}$ είναι στοιχειώδης 2-αβελιανή, δες [Shi], πρόταση 4.2, σελ. 101). Επομένως αν $E(F)_{(2)} \neq \{0\}$, τότε η ομάδα $E(F)_{(2)}$ είναι της μορφής $\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$ με $r \geq 0$ και $b = 1, 2, 3$. Επίσης $r \leq 4$ διότι στην αντίθετη περίπτωση η ομάδα $2^{b}E(F)_{(2)}$ θα περιείχε ρητή κυκλική υποομάδα που η τάξη της θα διαιρούνταν με 32, που είναι άτοπο από το θεώρημα του Kenku. Τέλος εφόσον η ομάδα $\mathbb{Z}/32\mathbb{Z}$ δεν περιέχεται στην $E(F)$, έπεται ότι οι ομάδες $\mathbb{Z}/2^{b+4} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$ για $b = 1, 2, 3$ δεν περιέχονται στην $E(F)$. Δηλαδή δεκτές είναι μόνο οι 13 ομάδες $\{O\}$, $\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$ όπου $b = 1, 2, 3$ και $r = 0, 1, 2, 3$.

Εξετάζουμε τώρα ποιοί είναι οι πιθανοί συνδιασμοί αυτών των ομάδων με τις διάφορες επιλογές που μπορούμε να έχουμε για της ομάδα $E(F)_{2'}$. Κατ' αρχήν εάν $E(F)_{2'} \cong \mathbb{Z}/m\mathbb{Z}$ με $m = 7, 9, 15$ τότε $E(F)_{(2)} = \{0\}$, διότι αν $E(F)_{(2)} \neq \{O\}$, τότε αν $m = 15$ η $E(\bar{\mathbb{Q}})$ θα περιείχε μια ρητή κυκλική υποομάδα τάξης 30, το οποίο είναι άτοπο από το θεώρημα του Kenku. Αν $m = 7, 9$, αφού $E(F)_{(2)} \neq \{O\}$ συνεπάγεται ότι για κάθε twist $E^{(z)}$, της Ε, ισχύει ότι $E^{(z)}(\mathbb{Q})_2 \neq \{O\}$ (λήμμα 5.9, σελ. 90) και συνεπώς θα υπήρχε κυκλική υποομάδα υπέρ το $\mathbb{Q}$ τάξης 14 και 18 αντίστοιχα, άτοπο λόγω του θεωρήματος του Mazur. Επομένως αν $E(F)_{2'} \neq \{0\}$, τότε περιέχει μια ρητή κυκλική υποομάδα τάξης 3 ή 5 και συνεπώς η

$E(F)_{2'}$ δεν μπορεί να περιέχει μια επιπλέον ρητή κυκλική υποομάδα τάξης 8 (θεώρημα 5.11). Επομένως οι πιθανότητες να εμφανιστούν ομάδες της μορφής $E(F)_{(2)} \cong \mathbb{Z}/2^{b+3}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$, απορρίπτονται. Κατά όμοιο τρόπο αν η $E(F)$ έχει σημείο τάξης 5 τότε η E δεν μπορεί να έχει μια ρητή κυκλική υποομάδα τάξης 4 και άρα οι περιπτώσεις $E(F)_{(2)} \cong \mathbb{Z}/2^{b+2}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$ για $b = 1, 2, 3$ απορρίπτονται. Επιπλέον οι τρείς αυτές περιπτώσεις δεν μπορούν εμφανιστούν μαζί με μια ρητή κυκλική υποομάδα τάξης 3 (θεώρημα 5.11). Δηλαδή αποδείξαμε ότι οι 6 περιπτώσεις $E(F)_{(2)} \cong \mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$, για $b = 1, 2, 3$ και $r = 2, 3$, μας δίνουν ότι $E(F)_{2'} = \{0\}$.

Ας υποθέσουμε τώρα ότι $E(F)_{(2)} \cong \mathbb{Z}/2^{b+1}\mathbb{Z} \oplus \mathbb{Z}/2^{b}\mathbb{Z}$, για $b = 1, 2, 3$. Τότε η ομάδα $E(F)_{(2)}$ θα περιείχε ρητή υποομάδα ισόμορφη με την $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ και άρα από το θεώρημα 5.11 έχουμε ότι η ομάδα $E(F)_{2'}$ δεν μπορεί να είναι ισόμορφη με την $\mathbb{Z}/5\mathbb{Z}$ η με την $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Το γεγονός αυτό μας αφήνει πιθανές μόνο τις περιπτώσεις $E(F)_{(2')} \cong \mathbb{Z}/3\mathbb{Z}$ ή $\{0\}$. Αρα έχουμε το ζητούμενο. $\square$

Βιβλιογραφία

[Αν1] Αντωνιάδη Γ. Α., Θεωρία Εκτιμήσεων - Τοπικά Σώματα ,Σημειώσεις, Ηράκλειο 1992.

[Αν2] Αντωνιάδη Γ. Α., Ελλειπτικές Καμπύλες , Σημειώσεις, Ηράκλειο 1985.

[Αν3] Αντωνιάδη Γ. Α., Αλγεβρική Θεωρία Αριθμών Ι, Σημειώσεις, Ηράκλειο 1988.

[Αν4] Αντωνιάδη Γ. Α., Συνομολογία Πεπερασμένων Ομάδων, Σημειώσεις, Ηράκλειο 1993.

[A-M] Atiyah M. F., Macdonald I. G., Introduction to Commutative Algebra, Addison Wesley, 1969.

[B-I-V] Brüske R., Ischebeck F., Vogel F., Kommutative Algebra, Wissenschaftsverlag, 1989.

[Cu] Cusick T. W., Lower Bounds for regulators, in "Number Theory Noordwijkerhout 1983", Lecture Notes in Math., Vol. 1068, Springer-Verlag, 1984.

[Fo] Folz H. G., Ein Beschränktheitssatz für die Torsion von 2-defizienten elliptischen Kurven über algebraischen Zahlkörpern, Dissertation, Universität des Saarlandes, Saarbrücken 1985.

[Fr] Frey G., Some remarks concerning points of finite order on elliptic curves over global fields, Ark. Math. 15 (1977), $1-19$.

[Fu] Fung G. W., Ströher H., Williams H. C., Zimmer H.-G., Torsion Groups of Elliptic Curves with Integral j-Invariant over Pure Cubic Fields, Journal of Number Theory 36 (1990), $12-45$.

[Ha] Hartshorne R., Algebraic Geometry, GTM 52, Springer - Verlag, New York, 1993.

[Hu] Husemöller Dale, Elliptic Curves, GTM 111, Springer-Verlag, New York 1987.

[I-R] Ireland K. - Rosen M., A Classical Introduction to Modern Number Theory. GTM 84, Springer-Verlag, New York 1990

[Ka] Kamienny S., Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math., 109 (1992) 221 – 229.

[Ke1] Kenku M. A., Rational 2^n-torsion points on elliptic curves defined over quadratic fields, J. London Math. Soc. (2) 11 (1975), 93 – 98.

[Ke2] Kenku M. A., Certain torsion points on elliptic curves defined over quadratic fields, J. London Math. Soc. (2) 19 (1975), 233 – 240.

[Ke3] Kenku M. A., The modular curve $X_0(39)$ and rational isogeny, Math. Proc. Cambridge Philos. Soc. 85 (1979), 21 – 23.

[Ke4] Kenku M. A., The modular curve $X_0(169)$ and rational isogeny, J. London Math. Soc. (2), 22 (1980), 239 – 244.

[Ke5] Kenku M. A., The modular curves $X_0(65)$, $X_0(91)$ and rational isogeny, Math. Proc. Camb. Phil. Soc. 87 (1980), 15 – 20.

[Ke6] Kenku M. A., Corrigendum : The modular curve $X_0(169)$ and rational isogeny, J. London Math. Soc. (2) 23 (1981), 428.

[Ke7] Kenku M. A., On the modular curves $X_0(125)$, $X_1(25)$, $X_1(49)$, J. London Math. Soc. (2) 23 (1981), 415 – 427.

[Kον] Κοντογιώργης Α. Ι., Ημιευσταθείς Ελλειπτικές Καμπύλες και το τελευταίο Θεώρημα του Fermat, Μεταπτυχιακή Εργασία, Ηράκλειο 1995.

[Ku] Kubert D. S., Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3) 33, (1976), 193 – 237.

[La] Lang S., Elliptic Curves : Diophantine Analysis, Springer - Verlag, Berlin 1978.

[La-Lo] Laska M., Lorenz M., Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$, Journal für die riene und angewandte Mathematik, Band 355, (1984), 163 – 172.

[Maz] Mazur B., Rational isogenies of prime degree, Invent. Math. 44 (1978), 129 – 162.

[Me] Merel L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres, 1994 (preprint).

[MFV] Modular Functions of One Variable IV, Lecture Notes in Math. Vol. 476, Springer-Verlag, 1975.

[Mu] Müller H., Ströher H., Zimmer H-G., Torsion groups of elliptic curves with integral j-invariant over quadratic fields, Journal für die riene und angewandte Mathematik, 397 (1989), 100 – 161.

[Na] Narkiewicz W., Elementary and Analytic Theory of Algebraic Numbers, PWN-Polish Scientific Publishers, Warszawa 1974.

[Ogg] Ogg A. P., Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. A.M.S. 24 (1975), 221 – 231.

[Pa] Paradopoulos I., Sur la classification de Neron des courbes elliptiques en characteristique residuelle 2 et 3, Journal of Number Theory, 44 (1993), 119 – 152.

[Ri] Ribet K., Torsion Points on Abelian Varieties in Cyclotomic Extensions (Appendix to Katz N. M. and Lang S., Finitness theorems of abelian varieties in cyclotomic extensions), L' Enseignement Math. 27 (1981), 315 – 319.

[Sh] Shimura Goro, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, Princeton 1971.

[Si1] Silverman J.H., The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, New York 1986.

[Si2] Silverman J.H., Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer-Verlag, New York 1994.

[Str] Ströher H., Die Torsiongruppe ellipticher Kurven mit ganzer j-Invariante über rein kubiscen Zahlkörpern, Diploma Thesis, Saarbrücken 1987.

[Ta] Tate J., Algorithm for finding the type on a singular fiber in a elliptic pencil, Modular Functions of One Variable, Lecture Notes on Mathematics, Vol. 476, Springer-Verlag, 1975.

[We] Weiss E., Algebraic Number Theory, Chelsea Publishing Company, New York 1963.