Επίπεδες Προβολικές Κυβικές Καμπύλες

1) Ταξινόμηση ομαλών, επίπεδων κυβικών καμπυλών

Ας υποθέσουμε ότι το K είναι ένα αλγεβρικώς κλειστό σώμα χαρακτηριστικής διάφορης τού 2 ή τού 3, και F ένα ομογενές πολυώνυμο βαθμού 3, $F \in K[X_0, X_1, X_2]_3$, ελεύθερο τετραγώνων. Τότε το F καθορίζει μία καμπύλη $\mathbb{V}_+(F) \subseteq \mathbb{P}^2_K$, η οποία θα λέγεται <u>κυβική</u>. Σκοπός αυτής της ενότητας είναι η ταξινόμηση των ομαλών κυβικών καμπυλών μέχρις προβολικής ισοδυναμίας.

Παρατηρούμε ότι μία ομαλή καμπύλη οφείλει να είναι ανάγωγη: πράγματι, σε αντίθετη περίπτωση $\mathbb{I}_+(\mathbb{V}_+(F)) = \langle F \rangle$ δεν είναι πρώτο, ισοδύναμα το F δεν είναι ανάγωγο. Οπότε $F = GH$, G, H μη σταθερά, και $\mathbb{V}_+(F) = \mathbb{V}_+(G) \cup \mathbb{V}_+(H)$. Από το θεώρημα τού Bezout, $\mathbb{V}_+(G) \cap \mathbb{V}_+(H) \neq \emptyset$ κ' έστω p κοινό σημείο τους. Τότε $\forall i \in \{0,1,2\}$ ισχύει:

$$\frac{\partial}{\partial X_i} F = \frac{\partial}{\partial X_i}(GH) = \frac{\partial}{\partial X_i} G H + G \frac{\partial}{\partial X_i} H \quad \text{και επειδή } H(p) = G(p) = 0_K$$

$$\left(\frac{\partial}{\partial X_i} F\right)(p) = H(p)\left(\frac{\partial}{\partial X_i} G\right)(p) + G(p)\left(\frac{\partial}{\partial X_i} H\right)(p) = 0_K + 0_K = 0_K$$

Οπότε από το κριτήριο τού Jacobi το p είναι ιδιάζον σημείο της $\mathbb{V}_+(F)$.

Από εδώ και εμπρός θα υποθέτουμε ότι το F είναι ανάγωγο πολυώνυμο και καταχρηστικά θα συμβολίζουμε την αντίστοιχη καμπύλη με το ίδιο σύμβολο F (και άρα οι καμπύλες F κ' λF είναι ίσες $\forall \lambda \in K$)

Η ταξινόμηση των ομαλών επίπεδων κυβικών καμπυλών βασίζεται στο γεγονός ότι έχουν τουλάχιστον ένα σημείο καμπής που ορίζεται ως ακολούθως:

Ορισμός 1.1. Έστω C μια οποιαδήποτε επίπεδη προβολική καμπύλη (όχι απαραίτητα κυβική) και $p \in C$ ένα ομαλό σημείο της. Λέμε ότι το p είναι σημείο καμπής της C αν υπάρχει L ώστε $I(p, C \cap L) \geq 3 \; (\geq 2)$.
(Η εν λόγω L είναι μοναδική, διότι εφάπτεται της C στο ομαλό σημείο p. Δηλαδή αν $c_i = \left(\frac{\partial}{\partial x_i} F\right)(p)$, τότε $L = \mathbb{V}_+(c_0 x_0 + c_1 x_1 + c_2 x_2)$, αν $d = \deg C \neq 0_K$.)

Θα δείξουμε ότι τα σημεία καμπής μίας ομαλής καμπύλης F καθορίζονται από τα σημεία τομής της λεγόμενης εσσιανής καμπύλης της με την ίδια.

Ορισμός 1.2 Έστω F μία τυχούσα επίπεδη καμπύλη. Ο πίνακας του Hesse (ή Εσσιανός πίνακας) της F ορίζεται να είναι:

$$B_F := \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{0 \leq i,j \leq 2}$$

Για κάθε $p \in K^3 \setminus \{0_K\}$ ο $B_F(p)$ είναι απλώς ο πίνακας μίας συμμετρικής διγραμμικής μορφής, της διγραμμ. μορφής που αντιστοιχεί στο ομογενές κομμάτι βαθμού 2 του αναπτύγματος Taylor της F στο p (που είναι μία τετραγωνική μορφή).
Ορίζουμε:

$$H_F := \det B_F$$

το πολυώνυμο του Hesse της F. Είναι πράγματι ομογενές πολυώνυμο, και αν $H_F \neq 0_{K[x_0,x_1,x_2]}$ τότε $\deg H_F = 3(d-2)$, όπου $d = \deg F$. (Φυσικά $d < 2 \Rightarrow H_F \equiv 0$, και η ποσότητα $3(d-2)$ έχει πάντα νόημα

Σε περίπτωση που το H_F δεν είναι ταυτοτικά μηδέν και $d \geq 3$, καθορίζεται μία καμπύλη βαθμού $3(d-2)$ η λεγόμενη <u>εσσιανή τής F.</u>

Λήμμα 1.1 Έστω $A \in Gl(3,K)$, L η αντίστοιχη γραμμική απεικόνιση $\mathbb{A}^3_K \longrightarrow \mathbb{A}^3_K$. Τότε για κάθε $F \in K[X_0, X_1, X_2]$, $H_{F^L} = (\det A)^2 (H_F)^L$. Ειδικότερα,

$$\mathbb{V}_+(H_{F^L}) = \mathbb{V}_+((H_F)^L) = \tilde{L}^{-1}(\mathbb{V}_+(H_F)),\ \tilde{L} \text{ ο αντίστοιχος}$$

προβολικός μετασχηματισμός.

Απόδειξη Απλή εφαρμογή τού κανόνα τής αλυσίδας. □

Πρόταση 1.1 Έστω F μία ομαλή επιπεδική καμπύλη βαθμού $d \geq 3$ με αντίστοιχη εσσιανή $H = H_F$. Ας υποθέσουμε ότι $\text{μκδ}(\text{char}(K), d-1) = 1$. Τότε το $F \cap H$ ταυτίζεται με το σύνολο των σημείων καμπής τής F.

Απόδειξη Έστω $p \in F$ τυχόν ομαλό σημείο. Θα δείξουμε ότι, αν συμβολίσουμε την εφαπτομένη στο p ως T_pF,

$I_p(P, F \cap T_pF) \geq 3 \Leftrightarrow p \in H$

Από το προηγούμενο λήμμα, μπορούμε να διαλέξουμε $L \in GL(3,K)$, με αντίστοιχο $\tilde{L} \in PGL(2,K)$ ώστε $L([0:0:1]) = P$, $L(\mathbb{V}_+(X_1)) = T_pF$. Οπότε αρκεί να δείξουμε το ζητούμενο για $P = (0:0:1)$, $T_pF = \mathbb{V}_+(X_1)$.

Αν αποομογενοποιήσουμε ως προς X_2 έχουμε:

$$F_*(X_0, X_1) = X_1(a + bX_0 + cX_1 + g(X_0, X_1)) + eX_0^2 + h(X_0),$$

όπου $a, b, c, e \in K$, $a \neq 0_K$, όλοι οι όροι του $g(X_0, X_1)$ έχουν βαθμό ≥ 2, όλοι οι όροι τού h έχουν βαθμό ≥ 3

($a \neq 0_K$ επειδή σε αντίθετη περίπτωση το (0,0) θα ήταν ιδιάζον σημείο)

Επειδή το F έχει υποτεθεί ανάγωγο, $(F_*)^* = F$ οπότε
$F(x_0, x_1, x_2) = a x_2^{d-1} x_1 + b x_2^{d-2} x_0 x_1 + c x_2^{d-2} x_1^2 + e x_2^{d-2} x_0^2 + Q$,
όπου Q έχει όρους βαθμού ≥ 3 ως προς x_0, x_1

Επομένως έχουμε $H_F([0:0:1]) = \det \begin{pmatrix} 2e & b & 0_k \\ b & 2c & (d-1)a \\ 0_k & (d-1)a & 0_k \end{pmatrix} =$

$= -2ea^2(d-1)^2$.

Επειδή $\gcd(\mathrm{char}(k), d-1) = 1$ κ' $a \neq 0_k$ έχουμε
$H_F([0:0:1]) = 0_k \iff e = 0_k$

Αν επικεντρωθούμε στο συσχετικό σύνολο $U_2 \cong \mathbb{A}_k^2$,
έχουμε $\mathcal{O}_{\mathbb{A}_k^2,0} / \langle e x_0^2 + h(x_0), x_1 \rangle \mathcal{O}_{\mathbb{A}_k^2,0} \cong \mathcal{O}_{\mathbb{A}_k^1,0} / \langle e x_0^2 + h(x_0) \rangle \mathcal{O}_{\mathbb{A}_k^1,0}$
όπου ο ισομορφισμός επάγεται από την εκτίμηση $x_1 = 0$
Επειδή η τάξη του h είναι ≥ 3, έχουμε ότι
$\delta = \dim_k (\mathcal{O}_{\mathbb{A}_k^1,0} / \langle e x_0^2 + h(x_0) \rangle \mathcal{O}_{\mathbb{A}_k^1,0}) \geq 2$ και $\delta \geq 3 \iff e = 0$

Οπότε $I(P, F \cap T_P F) \geq 3 \iff e = 0 \iff P \in H$. $\square$

Πόρισμα 1.1 Κάθε ομαλή κυβική καμπύλη (γενικότερα, καμπύλη βαθμού d με $\gcd(\mathrm{char}(k), d-1) = 1$) έχει τουλάχιστον ένα σημείο καμπής

Απόδειξη Από το Θεώρημα του Bezout μία κυβική καμπύλη τέμνει την εσσιανή της και αρκεί να εφαρμόσουμε την προηγούμενη πρόταση. $\square$

Παρατήρηση: Μπορεί να δειχθεί ότι στην πραγματικότητα υπάρχουν ακριβώς εννέα σημεία καμπής

Χρησιμοποιώντας το προηγούμενο αποτέλεσμα θα δείξ
με ότι κάθε ομαλή κυβική είναι προβολικώς ισοδύναμη με κάποια από τις λεγόμενες κυβικές καμπύλες του Weierstras που ως συσχετικές ποικιλότητες έχουν εξίσωση $y^2=X^3-g_2X-g_3$ (άλλες φορές χρησιμοποιείται και η μορφή $y^2=4X^3-g_2X-g_3$)

Πρόταση 1.2 Έστω C_{g_2,g_3} η κυβική καμπύλη που ορίζετ από το πολυώνυμο $X_2^2X_0-X_1^3-g_2X_1X_0^2-g_3X_0^3$

α) Η C_{g_2,g_3} είναι ομαλή α.αν $4g_2^3+27g_3^2\neq 0$. Επίσης, η C_{g_2,g_3} έχει σημείο καμπής στο $[0:0:1]$

β) Έστω F ανάγωγη ομαλή κυβική καμπύλη. Τότε $\exists\, g_2,g_3$ με $4g_2^3+27g_3^2\neq 0$ τ.ω. η F να είναι προβολικώς ισοδύναμ με την C_{g_2,g_3}

Απόδειξη α) Το μοναδικό κοινό σημείο της C_{g_2,g_3} με την ευθεία $X_0=0$ είναι το $[0:0:1]$, που από το κριτήριο του Jacobi είναι ομαλό. Έστω τυχόν σημείο της καμπύλης της μορφής $[1:x:y]$, $x,y\in k$. Τότε $y^2=x^3-g_2x-g_3$ και το σημείο είναι ιδιάζον (χρησιμοποιώντας και πάλι το ίδιο κριτήριο) αν και μόνο αν $y=0$ και $3x^2+a=0$. Δηλαδή αν και μόνο αν $f(x)=0$ και $f'(x)=0$, όπου $f(t)=t^3-g_2t-g_3$, ισοδύναμα το f έχει διπλή ρίζα στο x, ισοδύναμα $disc(f)=-(4g_2^3+27g_3^2)$
$\Leftrightarrow 4g_2^3+27g_3^2=0$ (επειδή x τυχόν).

Το ότι η C_{g_2,g_3} έχει σημείο καμπής στο $[0:0:1]$ θα προκύψει από τα παρακάτω.

β) Εφαρμόζοντας κατάλληλο προβολικό μετασχηματισμό στην F, μπορούμε να υποθέσουμε ότι το σημείο καμπής, του οποίου την ύπαρξη γνωρίζουμε, βρίσκεται στο σημείο $[0:0:1]=P$ και ότι η εφαπτομένη της F σε αυτό το σημείο είναι η $X_0=0$

• Αν $F = P_0 X_2^3 + P_1 X_2^2 + P_2 X_2 + P_3$, με $P_i \in k[X_0, X_1]$ $\deg P_i = i$,
τότε $F(0,0,1) = 0 \Rightarrow P_0(0,0) + P_1(0,0) + P_2(0,0) + P_3(0,0) = 0 \Rightarrow$
ο σταθερός όρος του $P_0 + P_1 + P_2 + P_3$ είναι $0 \Rightarrow P_0 = 0$

• Επίσης, επειδή $I(P, F \cap X_0) \geq 3$ και $\deg F = 3$, $\deg X_0 = 1$, από το θεώρημα του Bezout προκύπτει ότι $I(P, F \cap X_0) = 3$
Επειδή $P \in U_2 = \{[X_0 : X_1 : X_2] \mid X_2 \neq 0_k\}$, έχουμε ότι
$$\dim_k \left(\mathcal{O}_{\mathbb{A}^2_{k,P}} / \langle F(X_0, X_1, 1), X_0 \rangle \mathcal{O}_{\mathbb{A}^2_{k,P}} \right) = 3$$

(Χρησιμοποιώντας τον ισομορφισμό $U_2 \cong \mathbb{A}^2_k$ και συντεταγμένες X_0, X_1 στο $\mathbb{A}^2_k$)

Όμως αν θεωρήσουμε την εκτίμηση $k[X_0, X_1] \to k[X_1]$, $X_0 \to 0$, πυρήνα $\langle X_0 \rangle$ και χρησιμοποιήσουμε
έχουμε ότι $\left(\mathcal{O}_{\mathbb{A}^2_{k,0}} / \langle F(X_0, X_1, 1), X_0 \rangle \mathcal{O}_{\mathbb{A}^2_{k,p}} \right) \cong \mathcal{O}_{\mathbb{A}^1_{k,0}} / \langle F(0, X_1, 1) \rangle \mathcal{O}_{\mathbb{A}^1_{k,0}}$

όπου θεωρούμε το $k[X_1]$ ως δακτύλιο συντεταγμένων του $\mathbb{A}^1_k$. Η διάσταση του τελευταίου δακτυλίου εύκολα δείχνεται ότι είναι ίση με την πολλαπλότητα της ρίζας στο 0, δηλ. με την μέγιστη δύναμη του X_1 που διαιρεί το $F(0, X_1, 1)$, άρα και το $F(0, X_1, X_2)$. Οπότε $X_1^3 \mid F(0, X_1, X_2)$. Επειδή $\deg F(0, X_1, X_2) = 3$, προκύπτει ότι οι συντελεστές των $X_1^2 X_2$, $X_1 X_2^2$ στο $F(0, X_1, X_2)$, άρα και στο F είναι μηδέν.

Επομένως, $F = a X_1^3 + b X_1^2 X_0 + c X_1 X_2 X_0 + d X_2^2 X_0 + e X_0^2 X_1 + f X_0^2 X_2 + g X_0^3$, όπου $a, b, c, d, e, f, g \in k$.

Αν $a = 0$, τότε $X_0 \mid F$ που είναι άτοπο, αφού F ανάγωγο. Άρα $a \neq 0$.
Επιπλέον, $\frac{\partial F}{\partial X_0}(p) = d$, $\frac{\partial F}{\partial X_1}(p) = \frac{\partial F}{\partial X_2}(p) = 0$. Επειδή το p είναι ομαλό σημείο του F, $d \neq 0$.

Αφού $\mathrm{char}K \neq 2$, $2 \neq 0_K$, άρα μπορούμε να εφαρμόσουμε τον αυτομορφισμό $w(X_0, X_1, X_2) = (X_0, X_1, X_2 - (c/2d)X_1 - (f/2d)X_0)$ στο F και να πάρουμε

$$F^w = a_1 X_1^3 + b_1 X_1^2 X_0 + c_1 X_2^2 X_0 + d_1 X_0^2 X_1 + e_1 X_0^3, \text{ με}$$

$a_1 = a \neq 0$, $c_1 = d \neq 0$.

Επίσης, $3 \neq 0_K$ και κατόπιν τούτου εφαρμόζουμε τον $\sigma(X_0, X_1, X_2) = (X_0, X_1 - (b_1/3a_1)X_0, X_2)$ και έχουμε

$$F^{w\sigma} = (F^w)^\sigma = a_2 X_1^3 + b_2 X_0 X_2^2 + c_2 X_0^2 X_1 + d_2 X_0^3 \text{ με}$$

$a_2 = a_1 \neq 0$, $b_2 = c_1 = d \neq 0$. Τέλος, αν $u, v \in \mathbb{C}$ με $u^3 = 1/a_2$, $v^2 = -1/b_2$ η εφαρμογή του αυτομορφισμού $\tau(X_0, X_1, X_2) = (X_0, uX_1, vX_2)$ επί του $G = F^{w\sigma}$ μας δίνει

$$G^\tau = X_2^2 X_0 - X_1^3 - g_2 X_1 X_0^2 - g_3 X_0^3, \text{ για κάποια } g_2, g_3 \in K$$

Οπότε η F είναι ισοδύναμη με την κυβική C_{g_2, g_3}. Επειδή η F είναι ομαλή, το ίδιο θα είναι και η C_{g_2, g_3} και άρα από το α), $4g_2^3 + 27g_3^2 \neq 0_K$. Επίσης παρατηρούμε ότι αυτοί οι αυτομορφισμοί διατήρησαν το $[0:0:1]$, και άρα είναι σημείο καμπής για την C_{g_2, g_3}.

__Ορισμός 1.3__ Έστω ομαλή κυβική καμπύλη C_{g_2, g_3} με $4g_2^3 + 27g_3^2 \neq 0$. Ορίζουμε την ποσότητα $J(g_2, g_3) = \dfrac{g_2^3}{4g_2^3 + 27g_3^2}$ και την ονομάζουμε __αναλλοίωτο της καμπύλης__ C_{g_2, g_3}. Ενίοτε συμβολίζεται και ως $J(C_{g_2, g_3})$

Έστω C η κλάση προβολικής ισοδυναμίας μίας ομαδικής κυβικής. Σύμφωνα με την πρόταση 1.2 η C περιέχει μία κυβική $F = X_2^2 X_0 - X_1^3 - g_2 X_1 X_0^2 - g_3 X_0^3$, $4g_2^3 + 27 g_3^2 \neq 0$, και για οποιαδήποτε άλλη τέτοια κυβική F' έχουμε $F' \in C \Leftrightarrow J(F) = J(F')$. Έτσι η J είναι πράγματι αναλλοίωτος των κλάσεων προβολικής ισοδυναμίας των ομαδικών κυβικών καμπυλών. Τέλος, δεν είναι δύσκολο να δούμε ότι για κάθε $\lambda \in K$ υπάρχει επιλογή g_2, g_3 ώστε $J(C_{g_2, g_3}) = \lambda$. Οπότε το σύνολο των κλάσεων ισοδυναμίας των ομαδικών κυβικών καμπυλών παραμετρικοποιείται από το K.

2) Η δομή της ομάδας επί κυβικών καμπυλών

Έστω F μία ομαλή κυβική καμπύλη, $Q_1, Q_2 \in F$ δύο σημεία της. Τότε υπάρχει μοναδική ευθεία L και μοναδικό σημείο R τέτοια ώστε $L * C = Q_1 + Q_2 + R$. Πράγματι, αν $Q_1 \neq Q_2$ τότε θεωρούμε την μοναδική ευθεία L που τα περιέχει και τα δύο, ενώ αν $Q_1 = Q_2$ η εφαπτομένη L στο $Q = Q_1 = Q_2$ είναι η μοναδική που περιέχει το Q με $I(Q, L \cap C) \geq 2$ (επειδή F ομαλή)

Σε κάθε περίπτωση $\deg(Q_1 + Q_2) = 2$, και επειδή $\deg(L * C) = 3$ από το Θεώρημα του Bezout, $\deg(L * C - Q_1 - Q_2) = 1$; και άρα $L * C - Q_1 - Q_2 = R$, για κάποιο σημείο $R \in F$ που είναι προφανώς μονοσήμαντα ορισμένο. Μάλιστα $R = Q_1$ ή $Q_2 \Leftrightarrow L$ εφάπτεται της F στο Q_1, Q_2 αντίστοιχα και $R = Q_1 = Q_2 \Leftrightarrow R$ είναι σημείο καμπής για την F.

Ορισμός 2.1 Για κάθε ομαλή κυβική καμπύλη C ορίζεται η διμελής πράξη
$$\dot{+} : C \times C \longrightarrow C, \quad (P, Q) \longmapsto R$$
, όπου το R ορίζεται όπως παραπάνω

Πρόταση 2.1 Η διμελής πράξη που ορίστηκε παραπάνω ικανοποιεί τις εξής ιδιότητες:

i) $P \dot{+} Q = Q \dot{+} P, \ \forall P, Q \in C$

ii) $P \dot{+} (Q \dot{+} P) = (P \dot{+} Q) \dot{+} P = Q$

Απόδειξη Η i) είναι προφανής. Όσο για τη (ii), αν $R = Q \dot{+} P$ τότε για μοναδική L, $L * C = P + Q + R$, $Q = L * C - P - R$, άρα το $Q = P \dot{+} R$ εξ ορισμού. □

Η παραπάνω ορισθείσα πράξη δεν εφοδιάζει την C με δομή ομάδας. Γι' αυτό ορίζουμε μία καινούργια πράξη $\oplus$ επί της C. Έστω $O \in C$ ένα οποιοδήποτε σημείο της C

<u>Ορισμός 2.2</u> Ορίζουμε $\oplus: C \times C \to C$ ως $p \oplus q = O \dotplus (p \dotplus q) = (p \dotplus q) \dotplus O$

<u>Πρόταση 2.2</u> Το ζεύγος $(C, \oplus)$ αποτελεί αβελιανή ομάδα

<u>Απόδειξη:</u>

(i) $p \oplus q = O \dotplus (p \dotplus q) = O \dotplus (q \dotplus p) = q \oplus p$, $\forall p, q$

(ii) $O \oplus p = O \dotplus (O \dotplus p) = (O \dotplus p) \dotplus O = p$, $\forall p$

(iii) Αναζητάμε p' ώστε $p' \oplus p = O$. $p' \oplus p = O \dotplus (p' \dotplus p)$.
Αν $p' = p \dotplus X$, τότε $p' \oplus p = O \dotplus ((p \dotplus X) \dotplus p) = O \dotplus X$.
Αρκεί λοιπόν $X = O \dotplus O$, οπότε και $p' \oplus p = O \dotplus (O \dotplus O) = O$
Δηλαδή για κάθε p υπάρχει $p' = p \dotplus (O \dotplus O)$ ώστε $p' \oplus p = O$

Για την προσεταιριστικότητα θα χρειαστούμε το ακόλουθο λήμμα:

<u>Λήμμα 2.1</u> Έστω C ανάγωγη κυβική καμπύλη, C', C'' τυχούσες κυβικές καμπύλες. Ας υποθέσουμε ότι $C' * C = \sum_{i=1}^{9} P_i$, όπου τα P_i είναι ομάδα σημείων όχι απαραιτήτως διακεκριμένα, και $C'' * C = \sum_{i=1}^{8} P_i + Q$. Τότε $Q = P_9$

Απόδειξη Έστω $Q \neq P_9$ και L ευθεία που διέρχεται απ' το P_9 αλλά όχι απ' το Q.
$L * C = P_9 + R + S$ για κάποια σημεία $R, S \in C \cap L$ και τότε
$(LC'') * C = P_9 + R + S + \sum_{i=1}^{8} P_i + Q = C' * C + Q + R + S \Rightarrow LC'' * C \succ C' * C$

Από το πόρισμα του Θεωρήματος του Max Noether (πρόταση 4.7) της άλλης παρουσίασης) προκύπτει ότι υπάρχει μία καμπύλη L' (αναγκαστικά ευθεία) ώστε $L' * C = LC'' * C - C' * C = Q + R + S$
Αλλά αφού $L * C = P_9 + R + S$, $L' * C = Q + R + S$, τότε από μοναδικότητα $L = L'$ και $Q = P_9$, άτοπο. Οπότε $Q = P_9$. $\square$

Συνέχεια απόδειξης πρότασης 2.2.

(iv) Έστω $P, Q, R \in C$. Έστω $L_1 * C = P + Q + S'$, $M_1 * C = O + S' + S$, $L_2 * C = S + R + T'$, $M_2 * C = Q + R + U'$, $L_3 * C = O + U' + U$, $M_3 * C = P + U + T''$.

Επειδή $(P \oplus Q) \oplus R = O + T'$ και $P \oplus (Q \oplus R) = O + T''$ αρκεί να δειχθεί ότι $T' = T''$. Έστω $C' = L_1 L_2 L_3$, $C'' = M_1 M_2 M_3$ και εφαρμόζουμε το προηγούμενο λήμμα. $\square$

Παρατηρήσεις

Μπορεί να δειχθεί ότι η δομή της ομάδας $(C, \oplus)$ δεν εξαρτάται από την επιλογή του σημείου O, καθώς και ότι ισόμορφες κυβικές καμπύλες έχουν ισόμορφες ομάδες. Τέλος η $\oplus$ είναι μορφισμός από το $C \times C$ στο C, καθώς και η αντιστροφή. Άρα η $\oplus$ δίνει στην C τη δομή αλγεβρικής ομάδας