ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
Τμήμα Μαθηματικών

Αριστείδης Κοντογεώργης

Ομάδες Αυτομορφισμών Αλγεβρικών Καμπύλων

Διδακτορική Διατριβή

Ηράκλειο 1998

Εισαγωγή

Έστω C μία αλγεβρική προβολική καμπύλη γένους $g \geq 2$, ορισμένη πάνω από το αλγεβρικά κλειστό σώμα k, χαρακτηριστικής $p \geq 0$. Είναι γνωστό ότι η ομάδα των αυτομορφισμών G της C είναι πεπερασμένη. Σε αυτή την εργασία μελετούμε την δομή των ομάδων αυτομορφισμών μερικών συγκεκριμένων οικογενειών καμπύλων. Επιτρέπουμε οι οικογένειες καμπύλων που μελετάμε να έχουνε και ιδιόμορφες καμπύλες. Στην περίπτωση αυτή, δηλαδή στην περίπτωση που μία καμπύλη είναι ιδιόμορφη, θα εννοούμε τους αυτομορφισμούς ενός προβολικού, πλήρους, μη ιδιόμορφου μοντέλου της ή ισοδύναμα τους αυτομορφισμούς των αντίστοιχων σωμάτων συναρτήσεων. Κρίναμε λοιπόν βολικό να παρουσιάσουμε την θεωρία τους, σε όρους των σωμάτων συναρτήσεων και των αντίστοιχων θέσεων τους.

Αναλυτικά η διάρθρωση των κεφαλαίων έχει ως εξής:

Στο πρώτο κεφάλαιο μελετούμε το παρακάτω πρόβλημα: Θεωρούμε μία αβελιανή επέκταση F του σώματος συναρτήσεων F_0, με αβελιανή ομάδα Galois A. Ποιά είναι η σχέση της ομάδας αυτομορφισμών του F_0 με την ομάδα αυτομορφισμών του F; Η μέθοδος που ακολουθούμε, προκειμένου να απαντήσουμε στο παραπάνω ερώτημα είναι η εξής: Δίνουμε αναγκαίες συνθήκες, ώστε η ομάδα A να είναι κανονική υποομάδα της ομάδας αυτομορφισμών G_F του σώματος F. Έτσι το πρόβλημα υπολογισμού της δομής της ομάδας G_F ανάγεται σε ένα πρόβλημα επέκτασης μιας υποομάδας H της ομάδας αυτομορφισμών G_{F_0} του σώματος F_0 με αβελιανό πυρήνα A. Όπως είναι γνωστό τα προβλήματα επεκτάσεων ομάδων ανάγονται στον υπολογισμό των συνομολογιακών κλάσεων της ομάδας $H^2(H,A)$ που αντιστοιχούν σε δεδομένη επέκταση. Επιπλέον δίνουμε κριτήρια ώστε η δομή της ομάδας G_F να εξαρτάται από τον τύπο διακλάδωσης της επέκτασης σωμάτων F/F_0.

Στο δεύτερο κεφάλαιο, εφαρμόζουμε τα παραπάνω εργαλεία στα σώματα συναρτήσεων των καμπύλων με επίπεδα μοντέλα της μορφής $y^n = f(x)$ και καθορίζουμε τις δυνατές δομές των ομάδων αυτομορφισμών, κάνοντας χρήση των θεωρημάτων ταξινόμισης των πεπερασμένων υποομάδων της ομάδας αυτομορφισμών του ρητού σώματος συναρτήσεων.

Στο επόμενο κεφάλαιο, υπολογίζουμε τις ομάδες αυτομορφισμών των σωμάτων συναρτήσεων $F_{n,m}$ των καμπύλων $x^n+y^m-1=0$ όπου $n \neq m$, και η χαρακτηριστική δεν διαιρεί τα n,m. Η μέθοδος που ακολουθούμε είναι λίγο διαφορετική από τις προηγούμενες μεθόδους. Εξ' αιτίας της μεγάλης συμμετρίας του παραπάνου επίπεδου μοντέλου, μπορούμε να υπολογίσουμε μια βάση ολόμορφων διαφορικών καθώς και την δομή των ημιομάδων του Weierstrass σε συγκεκριμένα σημεία. Με αυτό τον τρόπο αποδεικνύουμε ότι η ομάδα $\mu(m)$ είναι κανονική υποομάδα της ομάδας αυτομορφισμών $F_{n,m}$. Είναι ενδιαφερόν να παρατηρήσουμε ότι όταν $m|n$ και το $n-1$ είναι δύναμη της χαρακτηριστικής τότε η ομάδα αυτομορφισμών έχει τάξη πολύ μεγαλύτερη από το φράγμα του Hurwitz στην χαρακτηριστική 0. Η περίπτωση $n=m$ ήταν γνωστή από την εργασία του Leopoldt από τις αρχές της δεκαετίας του 70.

Στο τέταρτο κεφάλαιο, επεκτείνουμε ένα αποτέλεσμα του J.P. Serre που υπολόγισε τις ομάδες αυτομορφισμών των modular καμπύλων $X(p)$ για p πρώτο και υπολογίζουμε τις ομάδες αυτομορφισμών των καμπύλων $X(N)$, για κάθε φυσικό N. Όπως προέκειψε, μετά από επικοινωνία με τον J.P. Serre ο παραπάνω υπολογισμός της ομάδας αυτομορφισμών των καμπύλων $X(N)$, ήταν γνωστός στους ειδικούς της περιοχής.

Στο τελευταίο κεφάλαιο, υπολογίζουμε τις ομάδες αυτομορφισμών των υπερεπιφανειών Fermat. Αποδεικνύουμε αρχικά ότι κάθε αυτομορφισμός των υπερεπιφανειών Fermat είναι περιορισμός ενός αυτομορφισμού του περιβάλλοντος προβολικού χώρου και στην συνέχεια υπολογίζουμε τους αυτομορφισμούς που διατηρούν την εξίσωση Fermat αναλλοίωτη. Και το αποτέλεσμα αυτό, ήτανε γνωστό από το 1987 από τον T. Shioda. Η μέθοδος του Shioda μου έγινε γνωστή από τον T. Katsura και αφού η διδακτορική μου διατριβή είχε ποιά ολοκληρωθεί.

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή κ. Γιάννη Αντωνιάδη για την βοήθεια που μου πρόσφερε σε όλη την διάρκεια των μεταπτυχιακών σπουδών μου. Επίσης θα ήθελα να ευχαριστήσω τον καθηγητή P. Roquette για το ενδιαφέρον που έδειξε για την εργασία μου καθώς και τα σχόλια και τις υποδείξεις του. Ευχαριστώ επίσης το Ίδρυμα

Κρατικών Υποτριφιών του οποίου υπήρξα υπότροφος.

Ευχαριστώ ιδιαίτερα τους γονείς μου Γιάννη και Μαρία καθώς και τους φίλους και συνεργάτες μου στο πενεπιστήμιο Κρήτης Μαρίνα, Δημήτρη, Θανάση, Γιώργο.

Ηράκλειο 18 Δεκεμβρίου 1988

Περιεχόμενα

Κεφάλαιο 1

Αβελιανές επεκτάσεις

Έστω F_0 ένα αλγεβρικό σώμα συναρτήσεων, με βαθμό υπερβατικότητας μονάδα, ορισμένο υπέρ ενός αλγεβρικά κλειστού σώματος k, χαρακτηριστικής $p \geq 0$. Θεωρούμε μία πεπερασμένη αβελιανή επέκταση F του F_0 γένους $g_F \geq 2$, με ομάδα Galois $Gal(F/F_0) = A$. Είναι γνωστό ότι η ομάδα αυτομορφισμών, έστω G, του F είναι πεπερασμένη. ([11] σελ. 368). Σκοπός μας είναι να συσχετίσουμε την ομάδα αυτομορφισμών G του F με την ομάδα αυτομορφισμών του F_0. Μπορούμε να γράψουμε την μικρή ακριβή ακολουθία

$$1 \longrightarrow A \longrightarrow N_G(A) \longrightarrow H \longrightarrow 1, \tag{1.1}$$

όπου $N_G(A)$ συμβολίζει τον κανονικοποιητή του A στην G και H, είναι μια πεπερασμένη υποομάδα της ομάδας αυτομορφισμών του F_0.

Κάτω από κατάλληλες συνθήκες έχουμε ότι $A \lhd G$ συνεπώς $N_G(A) = G$. Το γεγονός αυτό μας επιτρέπει να μελετήσουμε την ομάδα των αυτομορφισμών του F σαν ένα πρόβλημα επεκτάσεων πεπερασμένων υποομάδων της ομάδας αυτομορφισμών του F_0, οι οποίες εμφανίζονται σαν πηλίκα G/A. Οι Brandt και Stichtenoth [4] χρησιμοποίησαν παρόμοιες τεχνικές προκειμένου να υπολογίσουν τις ομάδες αυτομορφισμών υπερελλειπτικών καμπύλων, δηλαδή κυκλικών επεκτάσεων βαθμού δύο, ενός ρητού σώματος συναρτήσεων. Επίσεις ο Brandt [3] στην διδακτορική διατριβή του, μελέτησε γενικότερα κυκλικές επεκτάσεις του ρητού σώματος συναρτήσεων βαθμού πρώτου αριθμού.

Ας υποθέσουμε προς το παρόν ότι $A \lhd G$. Γράφουμε την ομάδα A σαν ένα ευθύ άθροισμα $A = A_{reg} \oplus A_p$, όπου A_p είναι το p-κομμάτι της αβελιανής ομάδας A, δηλαδή η μέγιστη αβελιανή p-υποομάδα της ομάδας A, $A_{reg} = A/A_p$, $(|A_{reg}|, p) = 1$. Παρατηρούμε ότι A_p είναι επίσης μια κανονική υποομάδα της G και έτσι λαμβάνουμε την ομάδα αυτομορφισμών G σε δύο βήματα

$$1 \longrightarrow A_p \longrightarrow G_p \longrightarrow H \longrightarrow 1,$$

$$1 \longrightarrow A_{reg} \longrightarrow G \longrightarrow G_p \longrightarrow 1,$$

όπου G_p συμβολίζει την επέκταση της H με A. Αφού το σώμα k είναι αλγεβρικά κλειστό, κάθε αβελιανή επέκταση με ομάδα Galois τάξης πρώτης προς την χαρακτηριστική είναι επέκταση του Kummer και κάθε αβελιανή επέκταση με Galois p-ομάδα, όπου p είναι η χαρακτηριστική, είναι επέκταση του Artin-Schreir .

Συνοψίζοντας, θα πρέπει να απαντήσουμε στα παρακάτω ερωτήματα:

- Κάτω από ποιες προϋποθέσεις μπορούμε να εξασφαλίσουμε ότι $A \lhd G$.
- Πως μπορούμε να περιγράψουμε την δομή της ομάδος G, δεδομένου ότι $A \lhd G$.
- Ποια είναι η υποομάδα H, των αυτομορφισμών του σώματος F_0, που επεκτείνονται σαν αυτομορφισμοί του F, δηλαδή ποιό είναι το πηλίκο G/A.

Θα ξεκινήσουμε από το πρώτο ερώτημα:

1.1 Συνθήκες κανονικότητας

Γράφουμε την αβελιανή ομάδα A σαν ευθύ άθροισμα [1] κυκλικών υποομάδων

$$A = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i}.$$

Παρατηρούμε ότι, $A \lhd G$ αν και μόνο αν

$$A_i := \bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i} \lhd G,$$

αφού συζυγή στοιχεία έχουν την ίδια τάξη.

Θα επεκτείνουμε ένα θεώρημα του Accola [1] το οποίο θα μας δώσει μια ικανή συνθήκη ώστε η ομάδα A_i να είναι κανονική σε ολόκληρη την ομάδα αυτομορφισμών. Έστω A_i ευθύς προσθεταίος στην ανάλυση της A, όπως ορίστηκε παραπάνω. Η ομάδα A_i γράφεται σαν ευθύ άθροισμα κυκλικών ομάδων ισόμορφων με την $\mathbb{Z}_{n_i}$. Έστω T_λ, $\lambda = 1, ..., r_i$ οι γεννήτορες των κυκλικών προσθετέων της A_i. Ενδεχομένως οι παραπάνω γεννήτορες να σταθεροποιούν διαφορετικό πλήθος θέσεων. Για κάθε s φυσικό θα συμβολίζουμε με A_i^s την υποομάδα της A_i που παράγεται από τα T_λ που σταθεροποιούν s το πλήθος θέσεις. Δυό συζυγείς αυτομορφισμοί έχουν το ίδιο πλήθος σταθερών σημείων. Έτσι η ομάδα A_i είναι κανονική υποομάδα της ομάδας G αν και μόνο αν όλες οι υποομάδες A_i^s είναι κανονικές υποομάδες της G.

Στην συνέχεια θα συμβολίζουμε με A μια αβελιανή ομάδα ισόμορφη με $\oplus_{i=1}^{t} \mathbb{Z}_{n_i}$ τέτοια ώστε οι t, το πλήθος γεννήτορες της A, $\{T_1, ..., T_t\}$ να σταθεροποιούν το ίδιο πλήθος s θέσεων του F. Θέτουμε $T = T_1$ και έστω Q μια θέση του F που να σταθεροποιείται από τον T. Κατά την διάρκεια της απόδειξης αυτής θα συμβολίζουμε με n την τάξη του T.

Θεωρούμε το συζυγές $\widetilde{T} := \sigma T \sigma^{-1}$ του T με ένα τυχαίο αυτομορφισμό σ της G. Είναι σαφές ότι $\widetilde{T}$ σταθεροποιεί την θέση $\sigma(Q)$. Έστω $\tilde{F}^A$ το σώμα των σταθερών στοιχείων του F υπό την $\sigma A \sigma^{-1}$.

Λήμμα 1.1.1 *Υπάρχει συνάρτηση $f \in \tilde{F}^A$, με μοναδικό πόλο στο $q := rest|_{\tilde{F}^A}\sigma(Q)$ ο οποίος επιπλέον είναι πόλος τάξης $\kappa \leq \gamma + 1$, όπου γ είναι το γένος του $\tilde{F}^A$*

Απόδειξη: Θεωρούμε τον χώρο συναρτήσεων

$$\mathcal{L}\left((\gamma+1)q\right) = \{f \in \tilde{F}^A : (f) + (\gamma+1)q \geq 0\}.$$

Από το θεώρημα των Riemann-Roch υπολογίζουμε ότι η διάσταση του παραπάνω χώρου είναι μεγαλύτερη ή ίση με δύο, δηλαδή το ζητούμενο. □

Ο divisor της f, σαν συνάρτηση του F είναι

$$div_F(f) = (f)_0 - n\kappa \sum_{\tau \in \sigma A \sigma^{-1}/\widetilde{T}} \tau(\sigma(Q)).$$

Έχουμε λοιπόν ότι $\deg f \leq n^t(\gamma+1)$. Ας θεωρήσουμε τώρα τις συναρτήσεις $h_i := f - T_i \circ f$ και ας υποθέσουμε ότι μία από αυτές, έστω η h_i, δεν είναι σταθερή. Τότε

$$\deg h_i \leq 2\deg f - r_i \leq 2n^t(\gamma+1) - r_i,$$

[1] Οι ομάδες αυτομορφισμών θεωρούνται πολλαπλασιαστικές. Ο παραπάνω προσθετικός συμβολισμός είναι καταχρηστικός αλλά τον προτιμούμε διότι καθιστά περισσότερο σαφή την αναλογία με την γραμμική άλγεβρα

όπου r_i είναι ο αριθμός των πόλων της f, λαμβάνοντας υπόψην την πολλαπλότητα. Πράγματι, για μια θέση P του F

$$v_P(h_i) = v_P(f - T_i \circ f) \geq \min \{v_P(f), v_P(T \circ f)\},$$

άρα αν η θέση P είναι ένας πόλος της h_i τότε η P είναι ένας πόλος της f ή της $T_i \circ f$. Επιπλέον αν P είναι ένας κοινός πόλος των $f, T_i \circ f$ τότε δεν είναι πόλος της h_i.

Υπενθυμίζουμε ότι με s συμβολίζουμε το πλήθος των θέσεων του F που σταθεροποιούντε από το T_i. Στην περίπτωση που

$$2n^t(\gamma + 1) < s$$

τότε

$$\deg h_i \leq 2n^t(\gamma + 1) - r_i < s - r_i \leq \deg h_i,$$

αφού κάθε σταθερή θέση του T_i η οποία δεν είναι πόλος της f είναι ρίζα της h_i, άτοπο. Συνεπώς οι συναρτήσεις h_i είναι όλες σταθερές και ίσες με μηδέν.

Αποδείξαμε ότι η f μένει αναλλοίωτη υπό την δράση της A, δηλαδή $k(f) \subseteq \tilde{F}^A$. Αν το σώμα $\tilde{F}^A \cong F^A$ είναι ρητό, τότε η συνάρτηση f του $\tilde{F}^A$ έχει πόλο τάξης 1 στο q, δηλαδή $\tilde{F}^A = k(f)$. Ο γεννήτορας του συζυγούς σώματος F^A είναι $\sigma f \sigma^{-1} = f$, δηλαδή $\tilde{F}^A = F^A$ και συνεπώς $A \lhd G$.

Παρατηρούμε ότι η A αφήνει αναλλοίωτο το σύνολο των διαφορετικών θέσεων του F οι οποίες βρίσκονται υπεράνω της q. Το σύνολο των διαφορετικών θέσεων του F οι οποίες βρίσκονται υπεράνω της q αποτελείται από τους πόλους της f. Το πλήθος τους είναι n^{t-1}, συνεπώς αφού η ομάδα A με n^t το πλήθος στοιχεία, αφήνει αναλλοίωτο ένα σύνολο με n^{t-1} στοιχεία, υπάρχει ένα στοιχείο $T' \in A$, τέτοιο ώστε το T' και το $\tilde{T}$ να έχουν το ίδιο σύνολο σταθερών θέσεων.

Έστω $G(Q)$ η ομάδα ανάλυσης στην θέση Q. Στην περίπτωση που $(p, |G(Q)|) = 1$, (και γ τυχαίο) έχουμε ότι $T' = T^i$ αφού γεννούν κυκλικές υποομάδες της κυκλικής ομάδας ανάλυσης κάθε θέσης που σταθεροποιούν.

Αποδείξαμε δηλαδή την

Πρόταση 1.1.2 *Έστω F/F_0 αβελιανή επέκταση με ομάδα Galois*

$$Gal(F/F_0) = A = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i}.$$

Θέτουμε $A_i = \oplus_{j=1}^{r_i} \mathbb{Z}_{n_i}$ και έστω $A_i^{s_j}$ η υποομάδα της A_i που γεννάται από τα στοιχεία που σταθεροποιούν s_j θέσεις. Θα συμβολίζουμε με $\gamma(A_i^{s_j})$ το γένος των σωμάτων συναρτήσεων $F^{A_i^{s_j}}$.

Αν για κάθε $i, s_j \neq 0$ έχουμε ότι

$$2\,|A_i^{s_j}|(\gamma(A_i^{s_j}) + 1) < s_j,$$

και οι τάξεις των ομάδων ανάλυσης των θέσεων που σταθεροποιούνται από τα $A_i^{s_j}$ είναι p-ελεύθερες, ή $\gamma(A_i^{s_j}) = 0$ τότε $A \lhd G$.

Θα χρησιμοποιήσουμε κυρίως το παρακάτω

Πόρισμα 1.1.3 *Έστω F/F_0 κυκλική επέκταση με ομάδα Galois*

$$Gal(F/F_0) \cong C_n$$

όπου F_0 ρητό σώμα συναρτήσεων. Έστω s το πλήθος των θέσεων που σταθεροποιεί ο γεννήτορας της κυκλικής ομάδας C_n. Στην περίπτωση που $2n < s$ έχουμε ότι $C_n \lhd Aut(F)$.

Παρατήρηση: Αν το F είναι ένα υπερελλειπτικό σώμα συναρτήσεων, τότε η υπερελλειπτική involution ορίζει μια κανονική υποομάδα τάξης δύο της ομάδας των αυτομορφισμών.

1.2 Επεκτάσεις ομάδων

Το πρόβλημα της επέκτασης της πεπερασμένης ομάδας H με αβελιανό πυρήνα A, είναι η εύρεση όλων των ομάδων G που δέχονται την A σαν κανονική υποομάδα και επιπλέον $G/A \cong H$. Τα παραπάνω εκφράζονται με την μικρή ακριβή ακολουθία

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\pi} H \longrightarrow 1$$

Η αβελιανή ομάδα ($\mathbb{Z}$-module) A αποκτά την δομή H-module μέσω της δράσης δια συζυγίας. Ακριβέστερα, αφού ο ομομορφισμός π είναι επί, μπορούμε να διαλέξουμε μία section ρ της H στην G, δηλαδή για κάθε $h \in H$ να διαλέξουμε ένα στοιχείο $\rho(h) \in \pi^{-1}(h)$. Στην συνέχεια ορίζουμε δράση της H στην A:

$$a^h := \rho(h) a \rho(h^{-1}), \text{ για κάθε } a \in A, \text{ και } h \in H.$$

Παρατηρούμε ότι ο ορισμός της δράσης είναι ανεξάρτητος της section. Η δράση μπορεί να θεαθεί ως μια παράσταση β του H πάνω στους αυτομορφισμούς της A:

$$\beta : H \longrightarrow Aut(A).$$

Η αβελιανή ομάδα A γράφεται σαν ευθύ άθροισμα κυκλικών υποομάδων:

$$A = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i},$$

συνεπώς $Aut(A) = \oplus_{i=1}^{s} GL_{r_i}(\mathbb{Z}_{n_i})$, όπου με $GL_{r_i}(\mathbb{Z}_{n_i})$ συμβολίζουμε τους αντιστρέψιμους $r_i \times r_i$ πίνακες με στοιχεία από τον δακτύλιο $\mathbb{Z}_{n_i}$. Η αναπαράσταση β λοιπόν, μπορεί να αναλυθεί σε ένα ευθύ άθροισμα $\beta = \oplus_{i=1}^{s} \beta_i$ όπου $\beta_i \in GL_{r_i}(\mathbb{Z}_{n_i})$ είναι αντιστρέψιμοι $r_i \times r_i$ πίνακες με συντελεστές στον δακτύλιο $\mathbb{Z}_{n_i}$. Θα συμβολίζουμε με $\{\beta_i(\sigma)\}_{k,l}$ $1 \leq k, l \leq r_i$, τον πίνακα που αντιστοιχεί στην $\beta_i(\sigma)$.

Στην ειδική περίπτωση $r_i = 1$, έχουμε ότι $GL_1(\mathbb{Z}_{n_i}) \cong \mathbb{Z}_{n_i}^*$.

Θα ονομάζουμε δυο επεκτάσεις G_1 και G_2 ισοδύναμες (ο αναγνώστης μπορεί να ελέγξει ότι πρόκειται πραγματικά για μία σχέση ισοδυναμίας) αν υπάρχει ομομορφισμός ϕ που να κάνει το παρακάτω διάγραμμα

$$\begin{tikzcd} & & G \arrow[d, "\phi"] \arrow[dr] & & \\ 1 \arrow[r] & A \arrow[ur] \arrow[dr] & {} & H \arrow[r] & 1 \\ & & G' \arrow[ur] & & \end{tikzcd}$$

αντιμεταθετικό. Είναι γνωστό ότι οι ισοδύναμες, κατά την παραπάνω έννοια, επεκτάσεις ταξινομούνται από τις κλάσεις συνομολογίας $H^2(H, A)$.

Αξίζει να παρατηρήσουμε ότι είναι δυνατόν σε δυο μη ισοδύναμες επεκτάσεις οι «μεσαίες» ομάδες να είναι ισόμορφες. Για παράδειγμα όλες οι επεκτάσεις της κυκλικής ομάδας C_p με C_p, όπου p πρώτος αριθμός, είναι ομάδες τάξης p^2, συνεπώς αβελιανές. Δηλαδή υπάρχουν μόνο δύο δυνατότητες για την «μεσαία» ομάδα, οι C_{2p} και $C_p \times C_p$. Από την άλλη υπολογίζεται ότι $H^2(C_p, C_p) \cong C_p$. Φυσικά, λόγω του 5-λήμματος ο ομομορφισμός ϕ είναι ισομορφισμός, από όπου έχουμε το παρακάτω φράγμα:

$$i(H, A) \leq \left| H^2(H, A) \right|$$

όπου $i(H, A)$ συμβολίζει το πλήθος των μη ισόμορφων «μεσαίων» ομάδων που πέρνουμε επεκτείνοντας την ομάδα H με A.

1.3 Επεκτάσεις του Kummer

Υπενθυμίζουμε μερικά βασικά στοιχεία από τις επεκτάσεις του Kummer.

Έστω F/F_0 αβελιανή επέκταση αλγεβρικών σωμάτων συναρτήσεων, με αβελιανή ομάδα Galois A. Έστω m ο εκθέτης της A, δηλαδή το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της A. Θα ονομάζουμε την επέκταση F/F_0 m-επέκταση του Kummer , όταν το σώμα F_0 έχει m το πλήθος διαφορετικές m-ρίζες της μονάδας. Η υπόθεση αυτή έχει ως επακόλουθο, το ότι $(|A|, p) = 1$. Θα συμβολίζουμε με $\hat{A}$ την ομάδα των χαρακτήρων της A, δηλαδή $\hat{A} = Hom(A, \mathbb{C}))$. Αφού η ομάδα A είναι αβελιανή έχουμε ότι $A \cong \hat{A}$.

Η παρακάτω πρόταση χαρακτηρίζει τις επεκτάσεις του Kummer.

Πρόταση 1.3.1 *Έστω F/F_0 επέκταση του Kummer της οποίας η ομάδα Galois έχει εκθέτη $m' \mid m$. Θα συμβολίζουμε με $M(F^*)$ την υποομάδα του F^*, των στοιχείων των οποίων οι m δυνάμεις ανήκουν στο F_0^* και με $N(F_0^*) < F_0$ την υποομάδα του F_0 των m δυνάμεων του $M(F^*)$. Έχουμε την ακριβή ακολουθία*

$$1 \longrightarrow F_0^* \longrightarrow M(F^*) \xrightarrow{\lambda} \hat{A} \longrightarrow 1,$$

όπου η συνάρτηση λ στέλνει το στοιχείο ρ στον χαρακτήρα χ_ρ, ορισμένο από

$$\chi_\rho(s) := \frac{s(\rho)}{\rho}, \quad s \in A.$$

Ισχύει ότι $M(F^*)/F_0^* \cong A$. Επίσης $F = F_0(M(F^*))$ και το σώμα F είναι πεπερασμένα παραγώμενο

$$F = F_0(y_1, ..., y_r),$$

από τα $y_i \in M(F^*)$, αν και μόνο αν τα cosets y_iF_0 γεννούν την ομάδα $M(F^*)/F^*$.

Επιπλέον η συνάρτηση

$$\mu : \left\{ \begin{array}{ccc} M(F^*) & \longrightarrow & N(F^*)/F^{*m} \\ y & \longmapsto & y^m F^{*m} \end{array} \right.$$

είναι επιμορφισμός με πυρήνα $\ker \mu = F_0^*$. Συνεπώς

$$\frac{M(F^*)}{F_0^*} \cong \frac{N(F^*)}{F_0^{*m}} \cong A.$$

Τέλος αν τα στοιχεία $u_1, ..., u_r$ είναι τέτοια ώστε τα cosets $u_iF_0^{*m}$ γεννούν την ομάδα $N(F^*)/F_0^{*m}$, τότε $F = F_0(\sqrt[m]{u_1}, ..., \sqrt[m]{u_r})$.

Απόδειξη: Jacobson [15] κεφ. 8.9 II τόμος.

Ας υποθέσουμε ότι η F είναι μια επέκταση του Kummer του F_0 με αβελιανή ομάδα Galois $A := Gal(F/F_0)$, της οποίας ο εκθέτης είναι m. Υποθέτουμε επίσης ότι η ομάδα A είναι κανονική υποομάδα της πλήρους ομάδας αυτομορφισμών G του F, με άλλα λόγια η παρακάτω ακολουθία

$$1 \longrightarrow A \longrightarrow G \longrightarrow H \longrightarrow 1, \tag{1.2}$$

είναι ακριβής. H είναι μια υποομάδα της ομάδος αυτομορφισμών του σώματος συναρτήσεων F_0. Γράφουμε την αβελιανή ομάδα A σαν ένα ευθύ άθροισμα κυκλικών υποομάδων

$$A = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i}.$$

Το σώμα F γράφεται

$$F = F_0(y_1, ..., y_t)$$

όπου $y_i \in M(F^*)$, αν και μόνο αν τα cosets $y_iF_0^*$ γεννούν την $M(F^*)/F_0^*$, ή ισοδύναμα αν

$$F = F_0(\sqrt[m]{u_1}, \sqrt[m]{u_2}, ..., \sqrt[m]{u_t}),$$

όπου $\sqrt[m]{u_i}$ είναι μια m-οστή ρίζα του u_i, αν και μόνο αν τα $u_1, ..., u_t$ είναι στοιχεία του $N(F^*)$ τέτοια ώστε τα cosets $u_iF_0^{*m}$ να γεννούν $N(F^*)/F_0^{*m}$.

Θα συμβολίζουμε με $\tilde{y}_i$ το διάνυσμα $(y_{1,i}, ..., y_{r_i,i})$ $1 \leq i \leq s$, των αντιπροσώπων από cosets τέτοια ώστε τα $y_{1,i}F^*, ..., y_{r_i,i}F^*$ να γενούν την $\bigoplus_{j=1}^{r_i} \mathbb{Z}_{n_i} < A$ και $\tilde{u}_i$ το διάνυσμα $(u_{1,i}, ..., u_{r_i,i})$ $1 \leq i \leq s$, τέτοιο ώστε

$$\tilde{y}_i^m = \tilde{u}_i \text{ δηλαδή } y_{j,i}^m = u_{j,i} \; 1 \leq j \leq r_i, 1 \leq i \leq s.$$

Για ένα διάνυσμα $a = (a_i)_{i=1,...,\lambda}$ από εδώ και στο εξής θα συμβολίζουμε με a^m το διάνυσμα $(a_i^m)_{i=1,...,\lambda}$. Τέλος με $\bar{y} = (\tilde{y}_1, ..., \tilde{y}_s)$ (αντίστ. $\bar{u} = (\tilde{u}_1, ..., \tilde{u}_s)$) συμβολίζουμε το διάνυσμα που αποτελείται από όλα τα $\tilde{y}_i$ (αντις. $\tilde{u}_i$), $i = 1, ..., s$. Ο ισομορφισμός του Kummer $A \cong M(F^*)/F_0^*$ μας επιτρέπει να γράψουμε την δράση της G επί της A σε όρους των γεννητόρων $\tilde{y}_i$, κατά τον ακόλουθο τρόπο:

$$\sigma(\tilde{y}_1, ..., \tilde{y}_s) \bmod F_0^* = (\tilde{y}_1^{\beta_1(\sigma)}, ..., \tilde{y}_s^{\beta_s(\sigma)}) \bmod F_0^*,$$

όπου $\tilde{y}_i^{\beta_i(\sigma)} = (\prod_{\nu=1}^{r_i} y_{\nu,i}^{\beta_i(\sigma)_{1,\nu}}, ..., \prod_{\nu=1}^{r_i} y_{\nu,i}^{\beta_i(\sigma)_{1,r_i}}) \bmod F_0^*$ και $\beta_i(\sigma) \in GL_{r_i}(\mathbb{Z}_{n_i})$.

Συνεπώς υπάρχει ένα διάνυσμα $\bar{B}(\sigma) = (\tilde{B}_1(\sigma), ..., \tilde{B}_s(\sigma))$ στο $F_0^{*(r_1+\ldots+r_s)}$, τέτοιο ώστε

$$\sigma(\bar{y}) = \bar{y}^{\beta(\sigma)}\bar{B}(\sigma).$$

Τα στοιχεία $\bar{B}(\sigma)$ μπορούν να προσδιοριστούν από την εξίσωση $\bar{y}^m = \bar{u}$. Πράγματι,

$$\begin{aligned} \sigma(\tilde{y}_i)^m &= \left(\prod_{\nu=1}^{r_i} y_{\nu,i}^{\beta_i(\sigma)_{1,\nu}}, ..., \prod_{\nu=1}^{r_i} y_{\nu,i}^{\beta_i(\sigma)_{1,r_i}}\right)^m \bmod F_0^* = \\ &= \left(\prod_{\nu=1}^{r_i} u_{\nu,i}^{\beta_i(\sigma)_{1,\nu}}, ..., \prod_{\nu=1}^{r_i} u_{\nu,i}^{\beta_i(\sigma)_{1,r_i}}\right) \bmod F_0^{*m}. \end{aligned} \tag{1.3}$$

Συνεπώς,

$$\sigma(\tilde{u}_i) = \sigma(\tilde{y}_i)^n = \left(\prod_{\nu=1}^{r_i} u_{\nu,i}^{\beta_i(\sigma)_{1,\nu}} B_{i,1}(\sigma), ..., \prod_{\nu=1}^{r_i} u_{\nu,i}^{\beta_i(\sigma)_{1,r_i}} B_{i,r_i}(s)\right) = \tilde{u}_i^{\beta_i(\sigma)}\tilde{B}_i(\sigma)^m. \tag{1.4}$$

Η παραπάνω εξίσωση μας δίνει μια ικανή και αναγκαία συνθήκη για να μπορούμε να επεκτείνουμε αυτομορφισμούς του σώματος F_0 σε αυτομορφισμούς του F. Συγκεκριμένα ισχύει η παρακάτω πρόταση:

Πρόταση 1.3.2 *Ο αυτομορφισμός σ_0 του F_0, επεκτείνεται σε αυτομορφισμό της Kummer επέκτασης F αν και μόνο αν οι εξισώσεις:*

$$\sigma_0(\tilde{u}_i) = \tilde{u}_i^{\beta_i(\sigma)} \cdot \tilde{x_i}^m, \; i = 0, ..., s,$$

έχουν λύσεις $\tilde{x_i}$ στο F_0^*.

1.3.1 Διακλαδώσεις σε επεκτάσεις του Kummer

Σε κυκλικές επεκτάσεις του Kummer ισχύει η παρακάτω πρόταση ([26], σελ. 111)

Πρόταση 1.3.3 *Έστω F_0/k αλγεβρικό σώμα συναρτήσεων, ορισμένο υπέρ το αλγεβρικά κλειστό σώμα σταθερών k. Έστω n φυσικός αριθμός. Υποθέτουμε ότι $u \in F_0$ είναι στοιχείο που να ικανοποιεί $u \neq w^d$ για κάθε $w \in F_0$ και για κάθε $d \mid n$, $d > 1$. Στην κυκλική επέκταση του Kummer*

$$F_0' = F_0(y), y^n = u$$

ο δείκτης διακλάδωσης e_P και το πλήθος των θέσεων r_P του F_0' που επεκτείνουν μια θέση P του F_0, υπολογίζονται ως εξής:

$$r_P = (n, v_P(u)), \quad e_P = \frac{n}{r_P}, \tag{1.5}$$

όπου v_P είναι η διακριτή εκτίμηση του F_0 που αντιστοιχεί στη θέση P.

Στην συνέχεια F θα είναι μία αβελιανή επέκταση του F_0, με ομάδα Galois A. Έστω Q μια θέση του F η οποία διακλαδίζεται στην επέκταση F/F_0 και έστω P ο περιορισμός της στο σώμα F_0. Θα συμβολίζουμε με $A(Q) < A$, την υποομάδα ανάλυσης που αντιστοιχεί στην θέση Q. Η ομάδα $A(Q)$ είναι ισόμορφη με την ομάδα αδρανείας $A_0(Q)$, αφού το σώμα των σταθερών k, είναι αλγεβρικά κλειστό. Παρατηρούμε ότι η $A(Q)$ περιέχεται μόνο σε ένα ευθύ κυκλικό προσθεταίο της A. Έστω yF^* ένας γεννήτορας αυτού του κυκλικού προσθεταίου, και $y_1F^*, .., y_nF^*$ οι γεννήτορες των άλλων κυκλικών προσθεταίων της ομάδας A, κάτω από την ταύτιση του Kummer , όπως αυτή δίνεται στην (1.3.1). Στην επέκταση $F_0(y_1, ..., y_n)/F_0$ η θέση P δεν διακλαδίζεται, άρα διακλαδίζεται μόνο στην επέκταση $F_0(y)/F_0$ και αναλύεται πλήρως στην επέκταση $F/F_0(y)$. Το σύνολο των θέσεων που διακλαδίζονται στην επέκταση F/F_0 λοιπόν, μπορεί να υπολογιστεί κάνοντας χρήση της θεωρίας των κυκλικών επεκτάσεων του Kummer (πρόταση 1.3.3). Η παραπάνω παρατήρηση αποδεικνύει την ακόλουθη

Πρόταση 1.3.4 *Έστω $u_1, ..., u_t$ στοιχεία του $N(F^*)$, τέτοια ώστε τα cosets $u_iF_0^{*m}$ να γενούν την $N(F^*)/F_0^{*m}$. Για κάθε u_i και κάθε θέση P του F_0 θέτουμε $r_i(P) := (n_i, v_P(\sqrt[m/n_i]{u_i}))$, όπου n_i είναι η τάξη του $u_iF_0^{*m}$ στην $N(F^*)/F_0^{*m}$. Αν Q είναι μια θέση του F υπέρ το P έχουμε ότι*

$$e(Q/P) = n_i/r_i(P),$$

και υπάρχουν $\frac{|A|}{e(Q/P)}$ θέσεις του F, υπέρ το P.

1.4 Υπολογισμός της δομής ομάδος

Όπως είδαμε στην παράγραφο (1.3) η δομή του A σαν H-module περιγράφεται πλήρως από την αντιστοιχία Kummer .

Η ίδια θεωρία μας δίνει την δυνατότητα να περιγράψουμε τον συνομολογιακό κύκλο $\alpha \in H^2(H, A)$ σε όρους των γεννοποιόντων ριζικών.

Από την πρόταση (1.3.2) έχουμε ότι οι συντεταγμένες του $\bar{B}(\sigma)$ είναι n-οστές ρίζες του $\sigma(\bar{u})/\bar{u}^{\beta(\sigma)}$. Διαφορετικές επιλογές n-οστών ριζών καταλήγουν σε διαφορετικές επεκτάσεις του αυτομορφισμού σ σε αυτομορφισμό του F. Στην γλώσσα των επεκτάσεων ομάδων, η επιλογή των n-οστων ριζών οδηγεί σε μία section

$$\rho : H \longrightarrow G.$$

Ο αυτομορφισμός $\rho(\sigma)$ ορίζεται ως εξής:

$$\rho(\sigma) = \begin{cases} y & \longmapsto & y^{\beta(\sigma)}B_\sigma \\ u & \longmapsto & \sigma(u)\ \forall u \in F_0 \end{cases}.$$

Από την θεωρία των επεκτάσεων ομάδων, ο 2-συνκύκλος που ορίζει την συνομολογιακή κλάση $\alpha \in H^2(H, A)$ που αντιστοιχεί στην επέκταση (1.2) δίνεται από

$$[\cdot,\cdot] : \begin{cases} G_0 \times G_0 & \longrightarrow & A \\ \sigma, \tau & \longmapsto & B_\sigma^{\beta(\tau)}\sigma(B_\tau)B_{\sigma\tau}^{-1} \end{cases}. \tag{1.6}$$

1.4.1 Δομή ομάδος και τύπος διακλάδωσης

Σε αυτή την παράγραφο, θα προσπαθήσουμε να εξετάσουμε την επιρροή του τύπου διακλάδωσης στην δομή της ομάδας αυτομορφισμών. Είναι γνωστό από τις εργασίες των Brand και Stichtenoth [4], [3] ότι αν $A = C_q$ είναι κυκλική ομάδα τάξης πρώτου αριθμού, τότε η δομή της επέκτασης G καθορίζεται αποκλειστικά από την σχετική διακλάδωση στις επεκτάσεις F/F_0 και F_0/F^G. Θα αναζητήσουμε συνθήκες για να ισχύει αυτό στην γενική περίπτωση.

Υπενθυμίζουμε ότι η αβελιανή ομάδα A έχει τάξη που δεν διαιρείται από την χαρακτηριστική p.

Θα ξεκινήσουμε την μελέτη μας από την «τοπική» περίπτωση: Θεωρούμε την θέση P του F_0, και έστω $H(P)$ η υποομάδα της H που κρατά σταθερή την θέση P. Είναι γνωστό ότι ([20] σελ. 68)

$$H(P) \cong \mathcal{E}_p(t) \rtimes C_m,$$

όπου η ομάδα $\mathcal{E}_p(t)$ είναι στοιχειώδης αβελιανή p-ομάδα, τάξης p^t, και η C_m, είναι κυκλική ομάδα τάξης m. Αν α είναι η συνομολογιακή κλάση που αντιστοιχεί στην επέκταση (1.2) η συνομολογιακή κλάση που αντιστοιχεί στην υποεπέκταση

$$1 \longrightarrow A \longrightarrow \pi^{-1}(H(P)) \longrightarrow H(P) \longrightarrow 1, \tag{1.7}$$

ισούται με $res_{H\to H(P)}(\alpha)$. Δεδομένης της μικρής ακριβούς ακολουθίας

$$1 \longrightarrow \mathcal{E}_p(t) \longrightarrow \mathcal{E}_p(t) \rtimes C_m \longrightarrow C_m \longrightarrow 1,$$

και του ότι $H^1(\mathcal{E}_p(t), A) = 0$ (υπενθυμίζουμε ότι $(p, |A|) = 1$), η restriction-inflation ακολουθία δίνει

$$1 \longrightarrow H^2\left(\frac{\mathcal{E}_p(t) \rtimes C_m}{\mathcal{E}_p(t)}, A^{\mathcal{E}_p(t)}\right) \longrightarrow H^2(\mathcal{E}_p(t) \rtimes C_m, A) \longrightarrow H^2(\mathcal{E}_p(t), A) \longrightarrow 1.$$

Άρα, αφού $H^2(\mathcal{E}_p(t), A) = 0$ (υπενθυμίζουμε ότι $(p, |A|) = 1$), έχουμε ότι

$$H^2(\mathcal{E}_p(t) \rtimes C_m, A) \cong H^2(C_m, A^{\mathcal{E}_p(t)}),$$

οπότε προκειμένου να υπολογίσουμε την δομή ομάδος $\pi^{-1}(H(P))$, αρκεί να υπολογίσουμε την δομή ομάδος $G' := \pi_1^{-1}(C_m)$ στην επέκταση:

$$1 \longrightarrow A^{\mathcal{E}_p(t)} \longrightarrow G' \xrightarrow{\pi_1} C_m \longrightarrow 1.$$

Χωρίς περιορισμό της γενικότητας λοιπόν θα υποθέτουμε ότι $H(P)$ είναι κυκλική.

Έστω Q μια θέση του F υπεράνω της θέσεως P. Θα αποδείξουμε το παρακάτω

Λήμμα 1.4.1 *Στην περίπτωση που η θέση Q αναλύεται πλήρως στην επέκταση F/F_0, δηλαδή αν $A(Q) = 1$, τότε η μικρά ακριβής ακολουθία*

$$1 \longrightarrow A \longrightarrow \pi^{-1}(H(P)) \longrightarrow H(P) \longrightarrow 1,$$

διασπάται και, ισοδύναμα, η αντίστοιχη συνομολογιακή κλάση

$$res_{H\to H(P)}\alpha$$

είναι τετριμμένη.

Απόδειξη: Θεωρούμε τον πυρήνα $ker\beta$ της παράστασης

$$\beta : H(P) \longrightarrow Aut(A).$$

Σύμφωνα με την παραπάνω παρατήρηση μπορούμε να υποθέσουμε ότι $H(P) \cong C_m$. Η ομάδα $ker\beta$ είναι πεπερασμένη υποομάδα της κυκλικής ομάδας $H(P) \cong C_m$. Έστω $S \in \pi^{-1}(H(P))$, τέτοιο ώστε η εικόνα του $\pi(S)$ να είναι γεννήτορας της κυκλικής ομάδας C_m. Μπορούμε να διαλέξουμε για γεννήτορα του $ker\beta < H(P)$, το στοιχείο $\pi(S)^r$ με $r \mid m$. Εξ ορισμού το $\pi(S)^r$ δρα στο τυχαίο $a \in A$ ως εξής:

$$a^{\pi(S)^r} = S^r a S^{-r}.$$

Από την άλλη αφού $S^r \in ker\beta$ έχουμε ότι

$$S^r a S^{-r} = a,$$

και συνεπώς η ομάδα $\pi^{-1}(ker\beta)$ που παράγεται από τα στοιχεία της A και από το S^r είναι αβελιανή.

Έστω $T_1, T_2 ..., T_\kappa$ οι γεννήτορες της αβελιανής ομάδας A και έστω n_i η τάξη του T_i. Θα συμβολίζουμε με G_i την αβελιανή ομάδα που παράγεται από τα T_i, S^r.

Ισχυριζόμαστε ότι κάθε p-Sylow υποομάδα της G_i είναι ισόμορφη με την $C_{p^{v_1}} \times C_{p^{v_2}}$, όπου v_1, v_2 είναι οι εκθέτες του p στην ανάλυση του n_i και m/r σε πρώτους παράγοντες.

Πράγματι, έστω p ένας πρώτος διαιρέτης του $(n_i, m/r)$. Έστω G_i^p μια p-Sylow υποομάδα του G_i, και A^i η ομάδα που παράγεται από τα T_j, $j = 1, ..., k$, $j \neq i$ Σχηματίζουμε τον παρακάτω πύργο σωμάτων

$$\begin{array}{ccccl}
 & F^{A^i} & & & \\
 & | & & & \\
\multirow{5}{*}{$G_i^p \left\{ \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \right.$} & L := F^{\langle A^i, T_i^{n_i/p^{v_1}} \rangle} & & Q_1, ..., Q_{p^{v_1}} & \\
 & | & & \backslash / & \text{αναλύεται πλήρως} \\
 & F_0 & & P_1 & \\
 & | & & | & \text{διακλαδίζεται πλήρως} \\
 & F_0^{C_{p^{v_2}}} & & p_1 & \\
 & | & & & \\
 & F^{G_i} & & &
\end{array}$$

Όπου p_1 είναι ο περιορισμός της θέσης P_1 στο $F_0^{C_{p^{v_2}}}$, και $Q_1, ..., Q_{p^{v_1}}$ οι επεκτάσεις της θέσης P_1 του F_0 στο $F^{\langle A^i, T_i^{n_i/p^{v_1}} \rangle} =: L$. Η ομάδα $Gal(L/F_0) \cong C_{p^{v_1}}$. Αν C είναι μια κυκλική υποομάδα του G_i^p που περιέχει την $Gal(L/F_0)$

$$Gal(L/F_0) \leq C \leq G_i^p$$

τότε $C = Gal(L/F_0)$. Διαφορετικά, θα υπήρχε ένα ενδιάμεσο σώμα

$$L^C < L_T(Q_1) < L$$

που θα αντιστοιχούσε στην ομάδα ανάλυσης $C(Q_1)$ τέτοιο ώστε η Q_1 να αναλύεται στην επέκταση $L_T(Q_1)/L^C$ και να διακλαδίζεται στην $L/L_T(Q_1)$. Το παραπάνω όμως είναι αδύνατον, αφού οι υποομάδες μιας κυκλικής p-ομάδος C είναι πλήρως διατεταγμένες ως προς τον εγκλεισμό. Η παρατήρηση αυτή μαζί με το θεώρημα ταξινόμισης αβελιανών ομάδων μας δίνουν ότι $G_i^p \cong C_{p^{v_1}} \times C_{p^{v_2}}$. Κάνοντας χρήση του θεωρήματος ταξινόμησης αβελιανών ομάδων άλλη μια φορά, παίρνουμε $G_i = C_n \times \ker\beta$ άρα

$$\pi^{-1}(\ker\beta) = A \times \ker\beta.$$

Συνεπώς

$$A \cap \langle S^r \rangle = \{1\}. \tag{1.8}$$

Επιστρέφουμε στην μελέτη της $\pi^{-1}(C_m)$. Η ομάδα $\pi^{-1}(C_m)$ μπορεί να γραφεί με την βοήθεια γεννητόρων και σχέσεων:

$$\pi^{-1}(C_m) = \langle T_i^{n_i} = 1, ST_iS^{-1} = T_1^{\beta_{i1}(S)} \cdots T_\kappa^{\beta_{i\kappa}(S)}, S^x = 1 \rangle. \tag{1.9}$$

Απομένει να υπολογίσουμε την τάξη x του S. Γνωρίζουμε ότι το $\pi(S)$ έχει τάξη m, άρα $S^m \in A$. Από την άλλη όμως $S^m = (S^r)^{m/r} \in A$ συνεπώς $(S^m) \in A \cap \langle S^r \rangle$ οπότε κατ' ανάγκη $S^m = 1$ από την (1.8). Από την γραφή της π^{-1} σε γεννήτορες και σχέσεις, πιστοποιούμε ότι η ομάδα π^{-1} είναι ένα ημιευθύ γινόμενο.□

Έστω P θέση του F_0, και $H(P)$ η ομάδα ανάλυσης της. Υπάρχουν εν γένει s το πλήθος διαφορετικές θέσεις $Q_1, ..., Q_s$ που επεκτείνουν την P στο F. Η ομάδα A είναι αβελιανή άρα όλες οι ομάδες ανάλυσης των θέσεων $Q_1, ..., Q_s$ είναι ίσες. Έστω λοιπόν

$$A(Q) < A$$

η ομάδα ανάλυσης μιας από αυτές. Αφού η θέση P διακλαδίζεται πλήρως στην επέκταση $F_0/F_0^{H(P)}$ έχουμε ότι οι θέσεις $Q_1, ..., Q_s$ και μόνον αυτές επεκτείνουν την θέση $p := P \cap F_0^{H(P)}$ στο F.

Η ομάδα $Gal(F/F_0^{H(P)})$ που επεκτείνει την $H(P)$ με A, δρα δια συζυγίας και μεταβατικά επί των ομάδων ανάλυσης $A(Q_i)$. Δηλαδή για κάθε $\sigma \in Gal(F/F_0^{H(P)})$ το $\sigma A(Q) \sigma^{-1} = A(Q)$. Συνεπώς η $A(Q)$ δέχεται την δομή ενός $H(P)$-module .

Λήμμα 1.4.2 *Αν το $H(P)$-module A γράφεται σαν ευθύ άθροισμα $A = A(Q) \oplus A/A(Q)$, τότε η δομή της ομάδας $\pi^{-1}(H(P))$ καθορίζεται από την διακλάδωση της θέσης P στην επέκταση F/F_0.*

Απόδειξη: Η διάσπαση $A = A(Q) \oplus A/A(Q)$ μας επιτρέπει την διάσπαση των ομάδων συνομολογίας και ιδιαίτερα της συνομολογιακής κλάσης που αντιστοιχεί στην επέκταση ομάδων 1.7

$$H^2(H(P), A) = H^2(H(P), A(Q)) \oplus H^2(H(P), A/A(Q)).$$

Συνεπώς, η συνομολογιακή κλάση

$$\alpha \in H^2(H(P), A)$$

που αντιστοιχεί στην επέκταση 1.7 διασπάται σε άθροισμα $\alpha = \alpha_1 + \alpha_2$, με $\alpha_1 \in H^2(H(P), A(Q))$ και $\alpha_2 \in H^2(H(P), A/A(Q))$.

Εφαρμόζοντας το λήμμα 1.4.1 στην αβελιανή επέκταση $F^{A(Q)}/F_0$, έχουμε ότι $\alpha_2 = 0$. □

Παρατήρηση: Η διάσπαση $A = A(Q) \oplus A/A(Q)$ είναι ισοδύναμη με το ότι οι κυκλικές ομάδες ανάλυσης $A(Q)$ είναι μέγιστες κυκλικές υποομάδες στην A, δηλαδή δεν υπάρχει κυκλική υποομάδα της A, που να περιέχει γνήσια την $A(Q)$.

Παρατήρηση: Το πρόβλημα εύρεσης της συνομολογιακής κλάσης $\alpha \in H^2(H(P), A)$ μπορεί να λάβει και μια δεύτερη μορφή «τοπικότητας». Θεωρούμε τις θέσεις p, P, Q των $F_0^{H(P)}, F_0$ και F αντίστοιχα που αποτελούν η κάθε μία περιορισμό της άλλης. Θα συμβολίζουμε με $Com_p(F_0^{H(P)}), Com_P(F_0), Com_Q(F)$ αντίστοιχα, τις πληρώσεις (σώματα Laurent αναπτυγμάτων) των σωμάτων $F_0^{H(P)}, F_0, F$ ως προς τις θέσεις p, P, Q αντίστοιχα.

$$
\begin{tikzcd}[arrows=dash]
Q \arrow[d] & F \arrow[r] \arrow[d] & Com_Q(F) \arrow[d] \\
P \arrow[d] & F_0 \arrow[r] \arrow[d] & Com_P(F_0) \arrow[d] \\
p & F_0^{H_p} \arrow[r] & Com_p(F_0^{H_p})
\end{tikzcd}
$$

Δηλαδή έχουμε ανάγει το πρόβλημα της επέκτασης στον υπολογισμό της ομάδας Galois στα τοπικά σώματα. Φυσικά και πάλι μπορούμε να έχουμε μια ακριβή γραφή για τον συνκύκλο, η οποία προκύπτει από την εξίσωση (1.6) θεωρώντας κάθε όρο στην τοπικοποίηση

$$
[\cdot,\cdot] : \left\{ \begin{array}{ccc} H(P)\times H(P) & \longrightarrow & A(P) \\ \sigma,\tau & \longmapsto & \hat{B}_\sigma^{\beta(\tau)}\sigma(\hat{B}_\tau)\hat{B}_{\sigma\tau}^{-1} \end{array} \right. , \tag{1.10}
$$

όπου για ένα στοιχείο $f \in F$ με $\hat{f}$ θα συμβολίζουμε το ανάπτυγμα Laurent του.

Ο τύπος διακλάδωσης καθορίζει την συνομολογιακή κλάση $res_{G\to G(P)}\alpha$ τοπικά. Προκειμένου να απαντήσουμε στο καθολικό ερώτημα, συγκεντρώνουμε τις απαντήσεις από όλα τα τοπικά προβλήματα μαζί: Θεωρούμε τον ομομορφισμό

$$
\begin{array}{ccc} H^2(H,A) & \stackrel{\Phi}{\longrightarrow} & \prod_P H^2(H(P),A) \\ \alpha & \longmapsto & \prod_P res_{H\to H(P)}\alpha \end{array} \tag{1.11}
$$

Για να καθορίζεται η ολική συνομολογιακή κλάση α από τον «τύπο διακλάδωσης» αρκεί ο Φ να είναι «ένα προς ένα» ή ισοδύναμα

$$
\ker\Phi = \bigcap_P \ker res_{H\to H(P)}\alpha = \{1\}
$$

Θα δώσουμε μία ικανή συνθήκη που να εξασφαλίζει ότι η συνάρτηση Φ, όπως αυτή ορίζεται στην (1.11), να είναι μονομορφισμός.

Είναι γνωστό ότι αν η S είναι μια υποομάδα της πεπερασμένης ομάδας H τότε η σύνθεση $cor_{S,H}\circ res_{H,S}$ είναι πολλαπλασιασμός με $[H:S]$ ([32], πόρισμα 2-4-9) . Δηλαδή για $S = H(P)$ έχουμε το παρακάτω μεταθετικό διάγραμμα

$$
\begin{tikzcd}
H^2(H,A) \arrow[rr, "{[H:H(P)]}"] \arrow[dr, "res"'] & & H^2(H,A) \\
& H^2(H(P),A) \arrow[ur, "cor"'] &
\end{tikzcd} .
$$

Ο δείκτης $|H : H(P)|$ ταυτίζεται με τον αριθμό r_p των θέσεων του σώματος F_0 που επεκτείνουν μια θέση p του F_0^H. Ισχύει λοιπόν το παρακάτω

Λήμμα 1.4.3 *Αν r_p συμβολίζει τον αριθμό των θέσεων του σώματος F_0, υπεράνω μιας θέσης p του F_0^H και επιπλέον ο μέγιστος κοινός διαιρέτης όλων των r_p είναι μονάδα, όταν το p διατρέχει τις θέσεις του F_0^H, τότε ο μορφισμός Φ είναι μονομορφισμός.*

Δυστυχώς, ο $\ker\Phi$ δεν είναι σε όλες τις περιπτώσεις μονάδα, και συνεπώς η δομή ομάδας της επέκτασης δεν καθορίζεται από τον τύπο διακλάδωσης. Αν για παράδειγμα, το F_0 είναι ένα σώμα συναρτήσεων γένους αυστηρά μεγαλύτερου του μηδενός, τότε μπορεί να υπάρχουν αυτομορφισμοί του F_0, οι οποίοι να μην σταθεροποιούν καμμία θέση του F_0, συνεπώς οι επεκτάσεις τους σε αυτομορφισμούς μιας αβελιανής επέκτασης F του F_0, δεν γίνεται να επηρεάζονται από τον τύπο διακλάδωσης. Από τον τύπο των Riemann-Hurwitz προκύπτει ότι αν η ομάδα H δρα χωρίς σταθερά σημεία επί του σώματος F, τότε

$$2g_F - 2 = |H| \cdot (2g_{F^H} - 2),$$

δηλαδή η τάξη της ομάδας H διαιρεί την χαρακτηριστική του Euler.

Παράδειγμα: Έστω F_0 ένα ελλειπτικό σώμα συναρτήσεων, ορισμένο επί ενός αλγεβρικά κλειστού σώματος k. Η ομάδα αυτομορφισμών του F_0 είναι άπειρη, αφού κάθε θέση $P \in E := \mathbb{P}(F_0)$ επάγει ένα αυτομορφισμό

$$P : \left\{ \begin{array}{ccc} F_0 & \longrightarrow & F_0 \\ Q & \longmapsto & Q + P \end{array} \right. .$$

Δηλαδή το σύνολο των θέσεων E του F_0, αποτελεί υποομάδα της $Aut(F_0)$. Η ομάδα των αυτομορφισμών $G(0)$ που κρατά σταθερό το ουδέτερο στοιχείο της ελλειπτικής καμπύλης E, είναι ισόμορφη με ([25], σελ. 103)

$$G(0) \cong \left\{ \begin{array}{cll} \mathbb{Z}_2 & \text{αν} & j(E) \neq 0, 1728 \\ \mathbb{Z}_4 & \text{αν} & j(E) = 1728,\ p \neq 2, 3 \\ \mathbb{Z}_6 & \text{αν} & j(E) = 0,\ p \neq 2, 3 \\ \mathbb{Z}_3 \rtimes \mathbb{Z}_4 & \text{αν} & j(E) = 0, 1728,\ p = 3 \\ (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3 & \text{αν} & j(E) = 0, 1728,\ p = 2. \end{array} \right.$$

Ολόκληρη δε η ομάδα αυτομορφισμών είναι ισόμορφη με

$$Aut(F_0) \cong E \rtimes G(0).$$

Θεωρούμε H μια πεπερασμένη υποομάδα της ομάδας αυτομορφισμών ενός ελλειπτικού σώματος συναρτήσεων F_0, η οποία να επεκτείνεται σε αυτομορφισμούς μιας αβελιανής επέκτασης F/F_0. Υποθέτουμε επιπλέον, ότι το γένος του F είναι μεγαλύτερο του 2. Από την δομή της $Aut(F_0)$, έχουμε ότι

$$H \cong H_{tor} \rtimes H(0),$$

όπου H_{tor} είναι υποομάδα πεπερασμένης τάξης της E και $H(0) \lhd G(0)$. Οι αυτομορφισμοί που επεκτείνουν την H_{tor} σχηματίζουν μια υποομάδα των αυτομορφισμών του F με τάξη $|A| \cdot |H_{tor}|$ η οποία δρα ελεύθερα επί του F. Συνεπώς το $|A| \cdot |H_{tor}|$ θα πρέπει να διαιρεί το $2g_F - 2$. Στην ειδική περίπτωση που $H_{tor} = \{1\}$, έχουμε ότι η συνάρτηση Φ είναι μονομορφισμός.

Κεφάλαιο 2

Καμπύλες της μορφής $y^n = f(x)$

Έστω αλγεβρικά κλειστό σώμα k. Σε αυτό το κεφάλαιο θα θεωρήσουμε κυκλικές επεκτάσεις του ρητού σώματος συναρτήσεων $k(x)$. Θεωρούμε το σώμα συναρτήσεων F της καμπύλης $y^n = f(x)$, όπου το $f(x) \in k[x]$ δεν είναι δ-δύναμη για κάθε $\delta \mid n$. Το F είναι μια κυκλική Kummer επέκταση του ρητού σώματος συναρτήσεων $k(x)$. Αφού το σώμα σταθερών k είναι αλγεβρικά κλειστό, στην επέκταση $F/k(x)$ δεν εμφανίζεται αδράνεια. Η διακλάδωση και η ανάλυση των θέσεων υπολογίζεται ως εξής:

Έστω P μία θέση του $k(x)$ και έστω υ_P η διακριτή εκτίμηση που της αντιστοιχεί. Το πλήθος r_P των θέσεων του F που βρίσκονται υπεράνω της P είναι

$$r_P = (n, \upsilon_P(f(x))) \tag{2.1}$$

ενώ ο αντίστοιχος βαθμός διακλάδωσης είναι $e_P = n/r_P$.

Αναλύουμε το $f(x)$ σε γινόμενο αναγώγων παραγόντων στο $k[x]$.

$$f(x) = \prod_{i=1}^{s} (x - \rho_i)^{d_i}.$$

Έχουμε ότι

$$\upsilon_P(f) = \begin{cases} d_i & \text{αν} \quad P = P_{x=\rho_i} \\ -d := \sum_{i=1}^{s} d_i & \text{αν} \quad P = P_\infty \\ 0 & \qquad\ \text{διαφορετικά} \end{cases} \tag{2.2}$$

Από τις (2.1) και (2.2) έχουμε ότι

$$e_P = \begin{cases} n/(n, d_i) & \text{αν} \quad P = P_{x=\rho_i} \\ n/(n, d) & \text{αν} \quad P = P_\infty \\ 1 & \qquad\ \text{διαφορετικά} \end{cases} \tag{2.3}$$

Έστω $A_1, ..., A_n$ οι θέσεις του F που επεκτείνουν το $P_{x=0}$, και $Q_{\rho_i, j}/j = 1, ..., (n, d_i)$ οι θέσεις που επεκτείνουν την $P_{x=\rho_i}$ και Γ_i $i = 1, ..., (n, d)$ οι θέσεις που επεκτείνουν το P_∞. Από τα παραπάνω μπορούμε να υπολογίσουμε τους divisors των συναρτήσεων x, y.

$$(x) = \sum_{i=1}^{n} A_i - \frac{n}{(n,d)} \sum_{i=1}^{(n,d)} \Gamma_i \tag{2.4}$$

$$(y) = \sum_{i=1}^{s} \frac{d_i}{(n, d_i)} \sum_{j=1}^{(n,d_i)} Q_{\rho_i, j} - \sum_{j=1}^{(d,n)} \frac{d}{(n,d)} \Gamma_j. \tag{2.5}$$

Πράγματι, για τους συντελεστές του divisor (y), αρκεί να παρατηρήσουμε ότι

$$n \cdot v_Q(y) = v_Q(f(x)) = e(Q/P) \cdot v_P(f(x)).$$

Η διαφορίζουσα της διαχωρίσιμης επέκτασης $F/k(x)$ υπολογίζεται

$$D(F/k(x)) = \sum_{i=1}^{s} \left(\frac{n}{(n,d_i)} - 1\right) \sum_{j=1}^{(n,d_i)} Q_{\rho_i,j} + \sum_{i=1}^{(n,d)} \left(\frac{n}{(n,d)} - 1\right) \Gamma_i \tag{2.6}$$

Από τον τύπο $(dx) = D(F/k(x)) - 2(x)_\infty$ ([13], σελ. 455) και την (2.6) έχουμε

$$(dx) = \sum_{i=1}^{s} \left(\frac{n}{(n,d_i)} - 1\right) \sum_{j=1}^{(n,d_i)} Q_{\rho_i,j} + \sum_{i=1}^{(n,d)} \left(\frac{n}{(n,d)} - 1 - \frac{2n}{(n,d)}\right) \Gamma_i. \tag{2.7}$$

Από την παραπάνω εξίσωση μπορούμε να υπολογίσουμε το γένος του F. Πράγματι $\deg dx = 2g_F - 2$, άρα

$$g_F = 1 + \frac{1}{2}\left(ns - \sum_{i=1}^{s}(n,d_i) - n - (n,d)\right). \tag{2.8}$$

Θέτουμε $\omega := dx/y^{n-1}$, και παρατηρούμε ότι για να είναι ένα διαφορικό της μορφής

$$x^\kappa y^\lambda \omega,$$

ολόμορφο πρέπει και αρκεί

$$nd - d - n - (n,d) - \lambda d - \kappa n \geq 0, \tag{2.9}$$

$$\lambda d_i + n - nd_i + d_i - (n,d_i) \geq 0, \ \ \kappa \geq 0 \tag{2.10}$$

Στην γενική περίπτωση τα ολόμορφα διαφορικά είναι πολύ περισσότερα από αυτά της μορφής $x^\kappa y^\lambda \omega$. Στην ειδική όμως περίπτωση $d_i = 1$, δηλαδή όταν κανένα πεπερασμένο σημείο της αφινικής καμπύλης $y^n = f(x)$ δεν είναι ιδιόμορφο, τότε οι συνθήκες 2.10 ανάγονται στις $\kappa \geq 0, \lambda \geq 0$, και ο $Towse$ [28] απέδειξε ότι το σύνολο

$$I := \left\{(\kappa,\lambda) \in \mathbb{N}^2 : nd - d - n - (n,d) - \lambda d - \kappa n \geq 0\right\}$$

έχει πληθάριθμο ακριβώς g_F. Άρα το σύνολο

$$x^\kappa y^\lambda \omega, (\kappa,\lambda) \in I, \tag{2.11}$$

αποτελεί μία βάση ολόμορφων διαφορικών.

Θα περιοριστούμε σε επεκτάσεις για τις οποίες ισχύει η συνθήκη $(n,d_i) = 1$ για όλα τα $i = 1,...,s$, ή ισοδύναμα σε κυκλικές Kummer επεκτάσεις, στις οποίες οι θέσεις που διακλαδίζονται, διακλαδίζονται πλήρως.

Χωρίς περιορισμό της γενικότητας μπορούμε να περιοριστούμε σε συναρτήσεις

$$f(x) = \prod_{i=1}^{s}(x - \rho_i)^{d_i}, d_i \in \mathbb{Z}$$

τέτοιες ώστε $0 < d_i < n$ και $d := \sum_{i=1}^{s} d_i \equiv 0 \bmod n$, δηλαδή το επάπειρο σημείο της καμπύλης δεν διακλαδίζεται.

Από την εξίσωση (2.8) και λαμβάνοντας υπόψην ότι $(n,d_i) = 1$, $(n,d) = n$ λαμβάνουμε τον παρακάτω τύπο γένους:

$$g = \frac{(n-1)(s-2)}{2}.$$

Αποδείξαμε στο πόρισμα 1.1.3 ότι υπό την προϋπόθεση $2n < s$, η ομάδα $Gal(F/F_0) \lhd G$. Η συνθήκη $2n < s$ είναι ισοδύναμη με την $(n-1)^2 < g_F$.

Στην ειδική περίπτωση $k = \mathbb{C}$ και $n = p$ είναι πρώτος, οι Victor Gonzalez και Rubi Rodriguez [7] έδωσαν μία καλύτερη συνθήκη: Χρησιμοποίησαν το γνωστό αποτέλεσμα ότι μία καμπύλη C είναι ένα $p-$κυκλικό κάλυμμα της προβολικής ευθείας αν και μόνο αν έχει ένα g_p^1 ελεύθερο βάσης γραμμικό σύστημα και το ότι η ομάδα αυτομορφισμων μεταθέτει όλα τα γραμμικά συστήματα της μορφής g_p^1. Συνεπώς αν το γραμμικό σύστημα g_p^1, είναι μοναδικό, τότε η κυκλική ομάδα Galois $Gal(C/\mathbb{P}^1)$, είναι κανονική στην G. Μία ικανή συνθήκη ώστε ένα γραμμικό σύστημα g_p^1 να είναι μοναδικό είναι:

$$2 \leq p \leq \frac{g}{2} + 1, \tag{2.12}$$

όπως απέδειξαν οι Arbarello-Cornalba στο [2], άρα, αν ισχύει η (2.12), τότε $C_p \lhd G$.

2.1 Συνθήκες επεκτασιμότητας

Θα αντιμετωπίσουμε σ' αυτή την παράγραφο το αντίστροφο πρόβλημα. G_0 είναι μία τυχαία πεπερασμένη υποομάδα της ομάδας αυτομορφισμών του ρητού σώματος συναρτήσεων F_0. Είναι δυνατόν να επεκτείνουμε κάθε αυτομορφισμό του G_0, σε ένα αυτομορφισμό του F;

Η παράσταση δράσης στην περίπτωση μας, όπου η επέκταση του Kummer παράγεται από ένα γεννοποιόν ριζικό μόνο, ανάγεται σε ένα ομομορφισμό

$$\beta : \left\{ \begin{array}{ccc} H & \longrightarrow & Aut(C_n) \cong \mathbb{Z}_n^* \\ \sigma & \longmapsto & \beta(\sigma) \bmod n \end{array} \right. , \tag{2.13}$$

Η παρακάτω πρόταση δίνει μία ικανή και αναγκαία συνθήκη.

Πρόταση 2.1.1 *Έστω $D = div(f(x))_0$ ο ριζικός divisor του πολυωνύμου $f(x)$ του σώματος F_0. Υποθέτουμε ότι $\deg(D) = d \equiv 0 \bmod n$ Έστω σ_0 ένας αυτομορφισμός του F_0.*

(α) *Τα παρακάτω είναι ισοδύναμα:*

- *Για κάθε αυτομορφισμό σ_0 της G_0 ισχύει*

$$\sigma_0(D) \equiv \beta(\sigma_0) D \bmod n$$

- *Υπάρχει ένας αυτομορφισμός σ του σώματος συναρτήσεων F τέτοιος ώστε $\sigma|_{F_0} = \sigma_0$.*

(β) *Τα παρακάτω είναι ισοδύναμα:*

- *Υπάρχει ένας αυτομορφισμός σ του σώματος συναρτήσεων F τέτοιος ώστε $\sigma|_{F_0} = \sigma_0$ και $\sigma T = T\sigma$ όπου T είναι γεννήτορας της κυκλικής ομάδας $Gal(F/F_0)$.*
- *$\sigma(D) = D$.*

όπου γράφοντας $D \equiv D' \bmod n$, για δυο divisors με τον ίδιο φορέα, εννοούμε ότι $u_P(D) \equiv u_P(D')$ για κάθε $P|D, D'$.

Απόδειξη:

(α) Η γενική συνθήκη επεκτασιμότητας που δώσαμε στην πρόταση 1.3.2 μας δίνει ότι ότι ο αυτομορφισμός σ_0 του F_0 επεκτείνεται σε σε αυτομορφισμό της Kummer επέκτασης $F = F_0(y), y^n = f(x)$ αν και μόνο αν η συνάρτηση

$$\frac{\sigma_0(f(x))}{f(x)^{\beta(\sigma_0)}},$$

είναι n-οστή δύναμη ρητής συνάρτησης στο σώμα $k(x)$. Δηλαδή κάθε συντελεστής του κυρίου divisor της παραπάνω συνάρτησης είναι πολλαπλάσιο του n. Έχουμε λοιπόν για $u = f(x)$

$$div_{F_0}\left(\frac{\sigma_0(u)}{u^{\beta(\sigma_0)}}\right) = \sigma_0(div_{F_0}(u)) - \beta(\sigma_0)div_{F_0}(u)$$
$$= \sigma_0(div_0(u)) - \sigma_0(div_\infty(u)) - \beta(\sigma_0)div_0(u) + \beta(\sigma_0)div_\infty(u).$$

Όμως έχουμε προυποθέσει ότι $div_\infty(u) = deg(f(x))$ είναι πολλαπλάσιο του n, συνεπώς και το

$$\sigma_0(div_0(u)) - \beta(\sigma_0)div_0(u)$$

είναι πολλαπλάσιο του n.

(β) Αφού η επέκταση σ στο F του σ_0 μετατίθεται με τον γεννήτορα T έχουμε ότι $\beta(\sigma_0) = 1$, και συνεπώς ισχύει:

$$\sigma_0(D) \equiv D \bmod n.$$

Το αποτέλεσμα προκύπτει τελικά από το ότι $0 < d_i < n$. □

Υπενθυμίζουμε ότι $D = div(f(x))_0$. Το $\mathrm{supp}(D)$ ισούται με το σύνολο των θέσεων του F_0 που διακλαδίζονται στην επέκταση F/F_0. Αφού $C_n \lhd G$, κάθε αυτομορφισμός σ της G, μεταθέτει τις θέσεις του $\mathrm{supp}(D)$. Οι σταθερές θέσεις του $\mathrm{supp}(D)$ υπό την δράση του G_0 διακλαδίζονται στην επέκταση $F_0/F_0^{G_0}$.

Ορισμός 2.1.2 *Έστω G_0 μία πεπερασμένη ομάδα αυτομορφισμών του ρητού σώματος συναρτήσεων F_0 και έστω $A := \{P_1, ..., P_f\}$ το σύνολο των θέσεων του F_0 που διακλαδίζονται στην $F_0/F_0^{G_0}$. Έστω επίσης $A_R \subset A$ ένα G_0- αναλλοίωτο υποσύνολο του A και $\beta : G_0 \longrightarrow \mathbb{Z}_n^*$ ένας ομομορφισμός ομάδων. Με*

$$\mathcal{D}_n(G_0, A_R \subset A, \beta) \subset Div(F_0),$$

θα συμβολίζουμε το υποσύνολο των divisors D του F_0 τέτοιο ώστε:

- Η ομάδα G_0 αφήνει το $\mathrm{supp}(D)$ αναλλοίωτο,
- $A \cap \mathrm{supp}(D) = A_R$,
- $(v_P(D), n) = 1$ για όλες τις θέσεις $P \in \mathrm{supp}(D)$.
- $\sigma(D) \equiv \beta(\sigma)D \bmod n$ για όλα τα $\sigma \in G_0$.

Παρατήρηση: Έστω $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$. Οι σταθερές θέσεις του $\mathrm{supp}(D)$ υπό την δράση της ομάδας G_0 διακλαδίζονται στην επέκταση $F_0/F_0^{G_0}$. Αν $\sigma \in G_0$ σταθεροποιεί μία θέση $P \in \mathrm{supp}(D)$ τότε $\beta(\sigma) \equiv 1 \bmod n$. Πράγματι , $\sigma(D) \equiv \beta(\sigma)D \bmod n$ και $v_P(D) \equiv \beta(\sigma)v_P(D) \bmod n$ άρα $\beta(\sigma) \equiv 1 \bmod n$ αφού $v_P(D) \in \mathbb{Z}_n^*$.

Λήμμα 2.1.3 *Αν $\beta(\sigma) \equiv 1 \bmod n$ για όλα τα P τέτοια ώστε $\sigma(P) = P$ και για όλα τα $\sigma \in G_0$, τότε το σύνολο $\mathcal{D}_n(G_0, A_R \subset A, \beta)$ δεν είναι κενό.*

Απόδειξη: Θα κατασκευάσουμε καταρχήν το σύνολο $\mathrm{supp}(D)$. Έστω μία θέση Q_1 του F_0 και έστω η τροχιά $O(Q_1, G_0)$ του Q_1 υπό την δράση του G_0. Διαλέγουμε μία θέση Q_2 εκτός του $O(Q_1, G_0)$ και θεωρούμε την τροχιά $O(Q_2, G_0)$.

Με αυτό τον τρόπο μπορούμε να κατασκευάσουμε ένα σύνολο τροχιών $O(Q_i, G_0)$ τέτοιες ώστε

$$O(Q_i, G_0) \cap O(Q_j, G_0) = \emptyset \text{ για } i \neq j$$

και $A_R \subset \bigcup_{i=1}^{s} O(Q_i, G_0)$. Θεωρούμε ένα divisor D ο οποίος να έχει σαν φορέα του D

$$\mathrm{supp}(D) := \bigcup_{i=1}^{s} O(Q_i, G_0).$$

Για κάθε $P \in O(Q_i, G_0)$ θέτουμε $v_P(D) := \lambda(Q_i) \cdot \beta(\sigma)$, όπου σ είναι το στοιχείο της G_0 τέτοιο ώστε $\sigma(Q_i) = P$, και $\lambda(Q_i)$ είναι οποιοσδήποτε ακέραιος πρώτος με τον n. Αργότερα θα διαλέξουμε κατάλληλα $\lambda(Q_i)$ έτσι ώστε να εξασφαλίσουμε $\deg(D) \equiv 0 \bmod n$. Ο divisor D είναι καλά ορισμένος αφού αν $\sigma, \sigma' \in G_0$ τέτοια ώστε $\sigma(Q_i) = \sigma'(Q_i) = P$ τότε $\sigma' \cdot \sigma^{-1}(Q_i) = Q_i$ συνεπώς $\beta(\sigma') \equiv \beta(\sigma) \bmod n$.□

Ορισμός 2.1.4 *Έστω G_0 μια πεπερασμένη ομάδα αυτομορφισμών του ρητού σώματος συναρτήσεων F_0 και έστω $A = \{P_1, ..., P_f\}$, $A_R \subset A$ όπως και στον ορισμό 2.1.2. Θα λέμε ότι ο τύπος διακλάδωσης $(G_0, A_R \subset A, \beta)$ υλοποιείται, αν υπάρχει κυκλική επέκταση F του F_0 ορισμένη όπως στην σελίδα 15, τέτοια ώστε $C_n = Gal(F/F_0)$ να είναι μία κανονική υποομάδα ολόκληρης της ομάδας αυτομορφισμών G, $G/C_n \cong G_0$ και το σύνολο A_R να αποτελείται από τις θέσεις του A που διακλαδίζονται στην επέκταση F/F_0.*

Αν ο divisor $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ μπορεί να κατασκευαστεί έτσι ώστε

$$\deg D \equiv 0 \bmod n$$

και η άπειρη θέση $P_\infty \notin \mathrm{supp}\, D$, τότε ο τύπος διακλάδωσης $(G_0, A_R \subset A, \beta)$ υλοποιείται. Πράγματι, θέτουμε $F = F_0(y)$, όπου

$$y^n = \prod_{P \in \mathrm{supp}(D)} (x - x(P))^{v_P(D)},$$

και $x(P) \in k$ συμβολίζει το πεπερασμένο σημείο του $\mathbb{P}^1(k)$, που αντιστοιχεί στην θέση P. Ο ισχυρισμός προκύπτει από την πρόταση 2.1.1. Ας σημειωθεί ότι προκειμένου να εξασφαλίσουμε ότι $G_0 \lhd G$ αρκεί να πάρουμε

$$\#\,\mathrm{supp}(D) > [n/2] + 1.$$

Στην περίπτωση που $\deg D \equiv 0 \bmod n$ και $P_\infty \in \mathrm{supp}\, D$, μπορούμε να βρούμε ένα μετασχηματισμό Möbius $a \in PGL(2,k)$ τέτοιο ώστε $P_\infty \notin Q(\mathrm{supp}\, D)$, έτσι ώστε ο τύπος διακλάδωσης $(QG_0Q^{-1}, Q(A_R) \subset Q(A), \beta)$ να είναι υλοποιήσιμος.

Θα υπολογίσουμε τον βαθμό του $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$. Έστω σ_0 ένας τυχαίος αυτομορφισμός του G_0 τάξης m. Το σύνολο $\mathrm{supp}(D)$ διαχωρίζεται σε τροχιές υπό την δράση του σ_0 :

$$\mathrm{supp}(D) = \bigcup_{i=1}^{k_{\sigma_0}} O(P_i, \langle\sigma_0\rangle).$$

Έστω $P \in \mathrm{supp}(D)$, και μία P θέση που να μην σταθεροποιείται από τον σ_0. Η τροχιά του P υπό την δράση του $\langle\sigma_0\rangle$ είναι

$$O(P, \langle\sigma_0\rangle) = \{P, \sigma_0(P), ..., \sigma_0^{m-1}(P)\}$$

(παρατηρούμε ότι αν P δεν σταθεροποιείται από τον μετασχηματισμό Möbius σ_0 τότε δεν σταθεροποιείται από καμία δύναμη του σ_0.) Η παραπάνω τροχιά αντιστοιχεί στον divisor

$$\sum_{i=0}^{m-1} \lambda\beta(\sigma_0^i)\sigma_0^i(P) \quad :$$

του οποίου ο βαθμός υπολογίζεται modulo p^a

$$\sum_{i=0}^{m-1} \lambda\beta(\sigma_0^i) = \begin{cases} \lambda\frac{\beta(\sigma_0)^m-1}{\beta(\sigma_0)-1} \equiv 0 \bmod p^a & \text{αν} \quad \beta(\sigma_0) \not\equiv 1 \bmod p^a \\ \lambda m \bmod p^a & \text{αν} \quad \beta(\sigma_0) \equiv 1 \bmod p^a \end{cases}, \tag{2.14}$$

για κάθε $p^a \mid n$ τέτοιο ώστε $p^{a+1} \nmid n$.

Παρατήρηση 2.1.5 *Παρατηρούμε ότι αν $P \in \operatorname{supp}(D)$, όπου*

$$D \in \mathcal{D}_n(G_0, A_R \subset A, \beta),$$

είναι divisor βαθμού $\deg(D) \equiv 0 \bmod n$, και P είναι μία σταθερή θέση του $\sigma \in G_0$, τότε $\beta(\sigma) \equiv 1 \bmod n$. Αν σ έχει δυο σταθερές θέσεις P_1, P_2 και $P_1 \in \operatorname{supp}(D), P_2 \notin \operatorname{supp}(D)$ τότε κατ ανάγκην έχουμε $(n,m)=1$, όπου m είναι η τάξη του σ. Πράγματι, ο βαθμός του D είναι

$$\deg(D) = v_{P_1}(D) + \sum \lambda_i m \equiv 0 \bmod n.$$

Θα πρέπει λοιπόν $(n,m)|v_{P_1}(D)$, άτοπο, εκτός αν $(n,m)=1$.

Λήμμα 2.1.6 *Αν υπάρχει $\sigma \in G_0$ τέτοιο ώστε $\beta(\sigma) \not\equiv 1 \bmod p^a$, για κάθε πρώτο p, όπου $p^a \mid n, p^{a+1} \nmid n$, τότε κάθε divisor $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ έχει βαθμό $0 \bmod n$.*

Απόδειξη: Ο σ δρα επί του $\operatorname{supp}(D)$ χωρίς σταθερά σημεία, αφού

$$\beta(\sigma) \not\equiv 1 \bmod n.$$

Το αποτέλεσμα προκύπτει από την εξίσωση 2.14.□

Λήμμα 2.1.7 *Στην περίπτωση που $A_R = \emptyset$, δηλαδή καμία από τις θέσεις που διακλαδίζονται στην επέκταση $F_0/F_0^{G_0}$ δεν διακλαδίζεται στην επέκταση F/F_0 τότε μπορούμε να κατασκευάσουμε ένα divisor $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ βαθμού $0 \bmod n$.*

Απόδειξη: Παρατηρούμε ότι η ομάδα G_0 δρα χωρίς σταθερά σημεία στο $\operatorname{supp}(D)$, αφού $A_R = \emptyset$. Άρα μπορούμε να πάρουμε άρτιο αριθμό από τροχιές $O(Q_i, G_0)$ $i = 1, ..., r$ και να θέσουμε $\lambda(Q_i) \equiv -\lambda(Q_{r-i}) \bmod n$. Η κατασκευή αυτή μας δίνει ότι $\deg D \equiv 0 \bmod n$. □

2.2 Δομή ομάδος

2.2.1 Πεπερασμένες υποομάδες της $PGL(2,k)$

Οι πεπερασμένες ομάδες αυτομορφισμών ενός ρητού σώματος συναρτήσεων δίνονται από το παρακάτω

Θεώρημα 2.2.1 *[30] Έστω $F_0 = k(x)$ ένα ρητό σώμα συναρτήσεων με σώμα σταθερών k αλγεβρικά κλειστό, χαρακτηριστικής $p \geq 0$. Έστω G_0 μία μη-τετριμένη πεπερασμένη ομάδα αυτομορφισμών του F_0 και $F_1 := F_0^{G_0}$ το σώμα των σταθερών στοιχείων της G_0. Έστω r το πλήθος των θέσεων του F_1 που διακλαδίζονται στην επέκταση F_0/F_1 και $e_1, ..., e_r$ οι αντίστιχοι δείκτες διακλάδωσης. Η ομάδα G_0 είναι μία από τις παρακάτω ομάδες και η επέκταση F_0/F_1 έχει ένα από τους παρακάτω τύπους διακλάδωσης*

1. *Κυκλική ομάδα C_m τάξης m πρώτης προς την χαρακτηριστική p με τύπο διακλάδωσης $r = 2$, $e_1 = e_2 = |G_0|$*

2. *Στοιχειώδης αβελιανή p-ομάδα με τύπο διακλάδωσης $r = 1$, $e = |G_0|$*

3. *Διεδρική ομάδα D_m τάξης $2m$ όπου $p = 2$, $(p, m) = 1$, με τύπο διακλάδωσης $r = 2$, $e_1 = 2$, $e_2 = n$ ή $p \neq 2$, $(p, m) = 1$, με τύπο διακλάδωσης $r = 3$, $e_1 = e_2 = 2$, $e_3 = m$.*

4. *Η εναλλάσουσα ομάδα A_4 στην περίπτωση χαρακτηριστικής $p \neq 2, 3$ με τύπο διακλάδωσης $r = 3$, $e_1 = 2$, $e_2 = e_3 = 3$.*

5. *Η συμμετρική ομάδα S_4 στην περίπτωση χαρακτηριστικής $p \neq 2, 3$ με τύπο διακλάδωσης $r = 3$, $e_1 = 2, e_2 = 3, e_3 = 4$.*

6. *Η εναλλάσουσα ομάδα A_5 όπου $p = 3$, με τύπο διακλάδωσης $r = 2, e_1 = 6, e_2 = 5$, ή $p \neq 2, 3, 5$ με τύπο διακλάδωσης $r = 3$, $e_1 = 2, e_2 = 3, e_3 = 5$.*

7. *Ημιευθύ γινόμενο στοιχειώδους αβελιανής $p-$ομάδας τάξης q με κυκλική ομάδα τάξης m όπου $m|q-1$ και τύπο διακλάδωσης $r = 2$, $e_1 = |G_0|, e_2 = m$.*

8. *$PSL(2, q)$ στην περίπτωση χαρακτηριστικής $p \neq 2, q = p^m$ και τύπο διακλάδωσης $r = 2$, $e_1 = \frac{q(q-1)}{2}, e_2 = \frac{q+1}{2}$.*

9. *$PGL(2, q)$ στην περίπτωση χαρακτηριστικής $q = p^m$ και τύπο διακλάδωσης $r = 2, e_1 = q(q-1), e_2 = q+1$.*

2.2.2 Συνομολογιακοί υπολογισμοί

Αν η ομάδα C_n είναι ένα τετριμμένο G_0 module δηλαδή η συνάρτηση β όπως ορίστηκε στην (2.13) είναι τετριμμένη, τότε είναι σχετικά εύκολο να υπολογίσουμε την ομάδα συνομολογίας κάνοντας χρήση του «παγκοσμίου θεωρήματος συντελεστών»: [3]

$$H^2(G_0, C_n) \cong Hom\left(H_2(G_0, \mathbb{Z}), C_n\right) \oplus Ext\left(H_1(G_0, \mathbb{Z}), C_n\right), \tag{2.15}$$

όπου ο δακτύλιος $\mathbb{Z}$ θεωρείται εδώ σαν τετριμμένο G_0-module . Η ομολογική ομάδα $H_2(G, \mathbb{Z})$ είναι ο πολλαπλασιαστής του Schur ο οποίος είναι γνωστός για όλες τις πεπερασμένες υποομάδες $PGL(2, k)$ [3] που εμφανίζονται στο θεώρημα 2.2.1. Η ομάδα ομολογίας $H_1(G_0, \mathbb{Z})$ είναι η αβελιανοποίηση $\frac{G_0}{[G_0, G_0]}$ της G_0. Κάνοντας χρήση των παραπάνω αποτελεσμάτων μπορούμε να υπολογίσουμε τον παρακάτω πίνακα συνομολογίας

Ομάδα G_0	$H^2(G_0, C_n)$
C_m	$\mathbb{Z}_{(n,m)}$
D_m	0 αν $(n,2) = 1$ $\mathbb{Z}_2$ αν $(n,2) = 2, (m,2) = 1$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ αν $(n,2) = (m,2) = 2$
A_4	$\mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,3)}$
A_5	$\mathbb{Z}_{(2,n)}$
S_4	$\mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$
$PSL(2,q)$	1 αν $p = 2, p^f \neq 4$ $\mathbb{Z}_{(2,n)}$ αν $p > 2, p^f \neq 9, p^f = 4$, όπου $q = p^f$ $\mathbb{Z}_{(6,n)}$ αν $p^f = 9$
$PGL(2,q)$	$\mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$

Θα αναφέρουμε επίσης την παρακάτω πρόταση, την οποία και θα χρησιμοποιήσουμε αργότερα

Πρόταση 2.2.2 *[32, σελ. 93] Υπάρχει μονομορφισμός*

$$\begin{array}{rcl} H^2(G,A) = \bigoplus_{p|s} H^2(G,A)_p & \xrightarrow{\Phi} & \bigoplus_{p|s} H^2(G_p,A) \\ a = \sum_{p|s} a_p & \longmapsto & \sum_{p|s} res_{(G\to G_p)} a_p \end{array},$$

όπου η G_p διατρέχει τις p-Sylow υποομάδες της G, ενώ η $H^2(G,A)_p$ θα συμβολίζει το p-κομμάτι της πεπερασμένης αβελιανής ομάδας $H^2(G,A)$, $s = |G|$.

2.2.3 Κυκλικές ομάδες

Ανάμεσα σε όλες ομάδες που μπορεί να εμφανιστούν ως ομάδες αυτομορφισμών ενός ρητού σώματος συναρτήσεων, απλούστερη είναι η κυκλική. Θα αποδείξουμε το παρακάτω

Θεώρημα 2.2.3 *Έστω ότι $G_0 := G/C_n$ είναι ισόμορφη με την κυκλική ομάδα C_m τάξεως m, όπου το m είναι πρώτο προς την χαρακτηριστική του σώματος k. Το σύνολο A των σταθερών θέσεων του $F_0 = k(x)$, υπό την δράση της G_0, αποτελείται από δύο θέσεις $A = \{P_1, P_2\}$. Η ομάδα των αυτομορφισμών G είναι ισόμορφη με:*

a) *C_{nm} αν τουλάχιστον μία από τις θέσεις P_1, P_2, έστω η P_1, διακλαδίζεται πλήρως στην επέκταση F/F_0, δηλαδή όταν $A_R \neq \emptyset$.*

b) *$C_n \rtimes C_m$ αν καμία από τις θέσεις του A δεν διακλαδίζεται στην επέκταση F/F_0, δηλαδή όταν $A_R = \emptyset$.*

Απόδειξη:

a) Στην περίπτωση αυτή, μία τουλάχιστον από τις θέσεις P_1, P_2, έστω η P_1, διακλαδίζεται πλήρως στην επέκταση F/F_0. Αν Q είναι η μοναδική θέση του F η οποία επεκτείνει την P_1, τότε η ομάδα ανάλυσης $G(Q)$ είναι κυκλική [20, σελ. 68] και ίση με G. Η ομάδα G είναι αβελιανή και η συνάρτηση δράσης $\beta : C_m \longrightarrow \mathbb{Z}_n^*$ είναι τετριμμένη.

b) Στην περίπτωση αυτή καμία από τις δύο θέσεις P_1, P_2 δεν διακλαδίζεται στην επέκταση F/F_0. Θα συμβολίζουμε με π, την φυσική προβολή $\pi : G \to G_0$.

Από το λήμμα 1.4.1 έχουμε ότι η μικρά ακριβής ακολουθία

$$1 \longrightarrow C_n \longrightarrow G \longrightarrow C_m \longrightarrow 1$$

διασπάται, δηλαδή $G \cong C_n \rtimes C_m$. Επιπλέον αν S και T είναι γεννήτορες των ομάδων C_m και C_n αντίστοιχα, τότε η μετακυκλική ομάδα G, δέχεται μία παράσταση σε γεννήτορες και σχέσεις:

$$G \cong \langle S, T | S^m = 1, T^n = 1, STS^{-1} = T^{\beta(S)} \rangle$$

(βλέπε και εξίσωση (1.9)). $\square$.

Θα αποδείξουμε ότι οι παραπάνω τύποι διακλάδωσης είναι υλοποιήσιμοι, κατασκευάζοντας ένα divisor εντός του $\mathcal{D}_n(C_m, A_R \subset A, 1)$ τέτοιο ώστε $\deg(D) \equiv 0 \bmod n$. Ας υποθέσουμε πρώτα ότι και οι δύο θέσεις P_1, P_2 διακλαδίζονται στην επέκταση F/F_0. Οι δύο τροχιές $O(P_i, C_m) = \{P_i\}$, $i = 1, 2$ των σταθερών θέσεων P_1, P_2, ανήκουν στο A_R και $A_R = A = \{P_1, P_2\}$. Ο τυχαίος divisor $D \in \mathcal{D}_n(C_m, A_R \subset A, 1)$ είναι της μορφής

$$D = \lambda(P_1)P_1 + \lambda(P_2)P_2 + \sum_{i=1}^{r} \lambda(Q_i) \sum_{P \in O(Q_i, C_m)} P, \text{ για κάποιον } r$$

όπου $Q_i \notin A$ για όλα τα $i = 1, ..., r$. Για να επιλέξουμε divisor βαθμού $0 \bmod n$, θέτουμε $\lambda(P_1) \equiv -\lambda(P_2) \bmod n$, διαλέγουμε τον r άρτιο και $\lambda(Q_i) \equiv -\lambda(Q_{r-i+1}) \bmod n$.

Ας υποθέσουμε τώρα ότι η θέση P_1 διακλαδίζεται και ότι η θέση P_2 αναλύεται στην επέκταση F/F_0, δηλαδή $A_R = \{P_1\}$. Ο τυχαίος divisor στο $\mathcal{D}_n(C_m, A_R \subset A, 1)$ έχει την μορφή

$$D = \lambda(P_1)P_1 + \sum_{i=0}^{r} \lambda(Q_i) \sum_{P \in O(Q_i, C_m)} P.$$

Έχουμε δει ότι η περίπτωση αυτή μπορεί να συμβεί μόνο όταν $(n, m) = 1$, δηλαδή υπάχουν ακεραίοι κ, λ τέτοιοι ώστε $\kappa n + \lambda m = 1$. Διαλέγουμε r άρτιο, και θέτουμε $\lambda(P_1) = 1$, $\lambda(Q_0) = \lambda$ και $\lambda(Q_i) \equiv -\lambda(Q_{r-i+1}) \bmod n$, $i = 1, ..., r$. Αυτό μας δίνει ότι $\deg D \equiv 0 \bmod n$.

Τέλος, η περίπτωση $A_R = \emptyset$ είναι υλοποιήσιμη όπως προκύπτει από το λήμμα 2.1.7.

Πόρισμα 2.2.4 *Έστω G η ομάδα αυτομορφισμών του σώματος συναρτήσεων F, και $G_0 = G/C_n$ η πεπερασμένη πηλικοομάδα αυτομορφισμών του ρητού σώματος συναρτήσεων F_0. Θα συμβολίζουμε με π την φυσική συνάρτηση $G \to G_0$. Έστω επίσης $G_0(P)$ η ομάδα ανάλυσης της θέσης P του F_0. Αν $G_0(P)$ είναι κυκλική τάξης πρώτης προς την χαρακτηριστική p, τότε η ομάδα $G_\pi(P)$ που ορίζεται ως*

$$G_\pi(P) := \{S \in G : \pi(S)P = P\},$$

είναι κυκλική τάξης $n \cdot |G_0(P)|$ στην περίπτωση που η θέση P διακλαδίζεται στην επέκταση F/F_0. Διαφορετικά, δηλαδή όταν η θέση P αναλύεται στην επέκταση F/F_0, η ομάδα $G_\pi(P)$ είναι το ημιευθές γινόμενο της $C_n \rtimes G_0(P)$ με δράση που να δίνεται από την $T^\sigma = T^{\beta(\sigma)}$, όπου σ είναι γεννήτορας της κυκλικής ομάδας $G_0(P)$. Στην πρώτη περίπτωση $\beta(\sigma) \equiv 1 \bmod n$.

Απόδειξη: Παρατηρούμε απλά ότι η $G_\pi(P)$ είναι η ομάδα που αντιστοιχεί στην υποεπέκταση:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_n & \longrightarrow & G_\pi(P) & \longrightarrow & G_0(P) & \longrightarrow & 1 \\
 & & || & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C_n & \longrightarrow & G & \longrightarrow & G_0 & \longrightarrow & 1
\end{array}$$

και ότι $G_\pi(P)$ είναι μία επέκταση της κυκλικής ομάδας $G_0(P)$□.

Στο παραπάνω πόρισμα παρατηρούμε ότι αν η θέση P αναλύεται στην επέκταση F/F_0 ενώ η άλλη επέκταση της κυκλικής ομάδας $G_0(P)$ διακλαδίζεται στην επέκταση F/F_0 τότε $G_\pi(P)$ είναι κυκλική τάξης $n \cdot |G_0(P)|$. Αυτό είναι δυνατόν αφού αναγκαστικά $(n, |G_0(P)|) = 1$ και $C_n \times G_0(P) \cong C_{n \cdot |G_0(P)|}$.

2.2.4 Στοιχειώδεις αβελιανές ομάδες

Θεώρημα 2.2.5 *Έστω ότι η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με μία στοιχειώδης αβελιανή ομάδα $\mathcal{E}_p(t)$ τάξεως p^t, όπου p είναι η χαρακτηριστική του k. Τότε η ομάδα G είναι ισόμορφη με την $C_n \rtimes G_0$. Εάν επιπλέον η μοναδική σταθερή θέση P_1 της G_0 διακλαδίζεται στην επέκταση F/F_0, τότε η ομάδα G είναι ισόμορφη με την $C_n \times G_0$.*

Απόδειξη: Στην επέκταση $F_0/F_0^{G_0}$ μόνο μία θέση P_1 του F_0 διακλαδίζεται. Αφού $(n, |G_0|) = 1$ η πλήρης ομάδα αυτομορφισμών G είναι ένα ημιευθύ γινόμενο, $G = C_n \rtimes G_0$. Η δράση δίνεται από την συνάρτηση β.

Στην περίπτωση που η θέση P_1 διακλαδίζεται πλήρως στην επέκταση F/F_0, έχουμε ότι

$$G = C_n \times G_0.$$

Πράγματι, έστω Q η μοναδική θέση του F που επεκτείνει την P_1. Η ομάδα ανάλυσης $G(Q) = G$ ταυτίζεται με την ομάδα αδρανείας, αφού το σώμα k είναι αλγεβρικά κλειστό. Έτσι $G(Q)$ είναι το ημιευθές γινόμενο μιας κυκλικής ομάδας τάξης πρώτης με το p με μία p-ομάδα $G_1(Q) = G_0$. Δηλαδή το γινόμενο είναι ευθύ και η συνάρτηση β είναι τετριμμένη. □

Ένας divisor στην $\mathcal{D}_n(G_0, A_R \subset \{P_1\}, \beta)$ δίνεται από

$$D = \sum_{P \in A_R} \lambda(P)P + \sum_{i=1}^{s} \lambda(Q_i) \sum_{P \in O(Q_i, G_0)} P,$$

όπου $Q_i \notin A$, $i = 1, \ldots s$. Προκειμένου να αποδείξουμε ότι και οι δύο τύποι διακλάδωσης εμφανίζονται θα πρέπει να διαλέξουμε τον παραπάνω divisor να έχει βαθμό $0 \bmod n$. Στην περίπτωση της πλήρους διακλάδωσης έχουμε $A_R = \{P_1\}$, οπότε παίρνουμε s τροχιές $O(Q_i, G_0)$ με $\lambda(P_1) = \lambda(Q_i) = 1$, τέτοιες ώστε

$$\deg(D) = 1 + sp^a \equiv 0 \bmod n,$$

όπου p^a είναι η τάξη της G_0. Αυτό είναι δυνατόν, αφού $(n, p) = 1$. Στην δεύτερη περίπτωση $A_R = \emptyset$ και το επιθυμητό αποτέλεσμα προκύπτει από το λήμμα 2.1.7.

2.2.5 Ημιευθέα γινόμενα κυκλικών ομάδων με στοιχειώδεις αβελιανές ομάδες

Στην περίπτωση αυτή η ομάδα πηλίκο $G_0 = G/C_n$ είναι ισόμορφη με το ημιευθές γινόμενο μιας στοιχειώδους αβελιανής p-ομάδας τάξης p^t, όπου p είναι η χαρακτηριστική του k, με μία κυκλική ομάδα C_m τάξης m, και $m|p^t - 1$. Στην επέκταση $F_0/F_0^{G_0}$ διακλαδίζονται δύο θέσεις p_1,p_2 του $F_0^{G_0}$, με δείκτες διακλάδωσης $e_1 = |G_0|$ και $e_2 = m$, αντίστοιχα.

Θεώρημα 2.2.6 *Έστω ότι η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με το ημιευθές γινόμενο μίας στοιχειώδους αβελιανής ομάδας $\mathcal{E}_p(t)$ τάξεως p^t, όπου p είναι η χαρακτηριστική του σώματος k, με μία κυκλική ομάδα C_m τάξεως m, $m|p^t - 1$. Η ομάδα αυτομορφισμών G τότε, είναι ισόμορφη με $C_n \rtimes G_0$ αν $A_R = \emptyset$ ή $\mathcal{E}_p(t) \rtimes C_{nm}$ αν $A_R \neq \emptyset$.*

Απόδειξη:
Αν και στην περίπτωση αυτή ενδιαφερόμαστε για στοιχειώδεις αβελιανές ομάδες τάξης δύναμης της χαρακτηριστικής, θα αποδείξουμε ένα πιό γενικό αποτέλεσμα επιτρέποντας στο p να μην είναι δύναμη της χαρακτηριστικής.

Λήμμα 2.2.7 *Θα συμβολίζουμε με $\mathcal{E}_p(t) := \overbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}^{t-\varphi o\rho \acute{\varepsilon} \varsigma}$ μία στοιχειώδη αβελιανή p ομάδα, τάξης p^t, όπου p δεν είναι απαραίτητα η χαρακτηριστική του σώματος k. Θεωρούμε την ομάδα $G_0 = \mathcal{E}_p(t) \rtimes C_m$, με $(m, p) = 1$, που δρα πάνω στο ρητό σώμα συναρτήσεων F_0. Ας υποθέσουμε ότι η υποεπέκταση*

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(\mathcal{E}_p(t)) \longrightarrow \mathcal{E}_p(t) \longrightarrow 1 \tag{2.16}$$

της επέκτασης

$$1 \longrightarrow C_n \longrightarrow G \xrightarrow{\pi} \mathcal{E}_p(t) \rtimes C_m \longrightarrow 1 \tag{2.17}$$

διασπάται, δηλαδή $\pi^{-1}(\mathcal{E}_p(t)) = C_n \rtimes \mathcal{E}_p(t)$. Τότε η ομάδα G είναι ισόμορφη με την $C_n \rtimes (\mathcal{E}_p(t) \rtimes C_m)$ αν και οι δυο σταθερές θέσεις του F_0, υπό την δράση της C_m, αναλύονται στην επέκταση F/F_0 ή είναι ισόμορφη με την $G \cong \mathcal{E}_p(t) \rtimes C_{nm}$ αν μία από τις σταθερές θέσεις του F_0, υπό την δράση της C_m, διακλαδίζεται στην επέκταση F/F_0.

Απόδειξη: Σύμφωνα με την μελέτη των κυκλικών επεκτάσεων, έχουμε δύο δυνατότητες για την ομάδα $\pi^{-1}(C_m)$.

$$\pi^{-1}(C_m) \cong C_n \rtimes C_m \text{ ή } \pi^{-1}(C_m) \cong C_{nm}.$$

Αν $\pi^{-1}(C_m) \cong C_n \rtimes C_m$ τότε κάνοντας χρήση του μονομορφισμού Φ όπως αυτός ορίστηκε στην πρόταση 2.2.2,

$$H^2(\mathcal{E}_p(t) \rtimes C_m, C_n) \xrightarrow{\Phi} \bigoplus_{q||G_0|} H^2(H_q, C_n),$$

όπου η H_q διατρέχει τις q-Sylow υποομάδες της G_0, έχουμε ότι η πλήρης επέκταση (2.17) διασπάται, αφού H_q είναι είτε υποομάδα του $\mathcal{E}_p(t)$ είτε του C_m.

Αν $\pi^{-1}(C_m) \cong C_{nm}$ τότε θα δείξουμε ότι $G \cong \mathcal{E}_p(t) \rtimes C_{nm}$. Πράγματι, σε αυτή την περίπτωση υπάρχει ένα στοιχείο $R \in G$ τάξης nm, το οποίο γεννά μία υποομάδα της G ισόμορφη προς την κυκλική ομάδα C_{nm}. Αφού η επέκταση (2.16) διασπάται υπάρχει ομομορφισμός

$$j : \mathcal{E}_p(t) \hookrightarrow \pi^{-1}(\mathcal{E}_p(t)) \hookrightarrow G.$$

Επιπλέον $\mathcal{E}_p(t) \cong j(\mathcal{E}_p(t))$ και $j(\mathcal{E}_p(t)) \cap C_{nm} = 1$. Πράγματι αν $x \in j(\mathcal{E}_p(t)) \cap C_{nm}$ τότε $x^m \in j(\mathcal{E}_p(t)) \cap C_n = 1$ άρα $x^m = 1$, και $x = 1$ αφού $(p, m) = 1$. Αυτό αποδυκνείει το επιθυμητό αποτέλεσμα. $\Box$

Επιστρέφουμε στην απόδειξη του θεωρήματος 2.2.6. Ο πρώτος p θα είναι η χαρακτηριστική του k. Έχουμε ότι $(p, n) = 1$, άρα η επέκταση (2.16) διασπάται. Αν, επιπλέον, μία από τις θέσεις που σταθεροποιείται από την C_m, διακλαδίζεται στην F/F_0 τότε $G \cong C_n \rtimes (\mathcal{E}_p(t) \rtimes C_m)$ διαφορετικά $G \cong \mathcal{E}_p(t) \rtimes C_{nm}$. $\Box$.

Προκειμένου να αποδείξουμε την υλοποιήση αυτών των τύπων διακλάδωσης θα πρέπει να επιλέξουμε τον divisor διακλάδωσης

$$D = \sum_{P \in A_R} \lambda(P) P + \sum_{i=1}^{s} \lambda(P_i) \sum_{Q \in O(P_i, G_0)} P,$$

του $\mathcal{D}_n(G_0, A_R \subset A, \beta)$ έτσι ώστε να έχει βαθμό $0 \bmod n$. Θα συμβολίζουμε με Q την μοναδική θέση του F_0 υπεράνω της p_1 και με $Q_1, ..., Q_{p^t}$ τις θέσεις του F_0 υπέρανω της p_2. Παρατηρούμε επίσης ότι

$$O(Q, G_0) = \{Q\}, O(Q_1, G_0) = \{Q_1, ..., Q_{p^t}\}.$$

Διακρίνουμε τις παρακάτω περιπτώσεις για το A_R

- $A_R = \emptyset$. Ο τύπος διακλάδωσης είναι υλοποιήσιμος λόγω του λήμματος 2.1.7.
- $A_R = O(Q, G_0) = \{Q\}$. Στην περίπτωση αυτή ο ομομορφισμός β είναι τετριμμένος. Παρατηρούμε ότι οι σταθερές θέσεις της κυκλικής ομάδας C_m είναι Q, Q' όπου $Q' \in O(Q_1, G_0)$. Άρα, από την παρατήρηση 2.1.5, έχουμε ότι $(n, m) = 1$. Θέτουμε $\lambda(P_i) = 1$, και διαλέγουμε τον αριθμό s των τροχιών τέτοιον ώστε

  $$\deg(D) = 1 + s \cdot |G_0| \equiv 0 \bmod n.$$

  Αυτό είναι δυνατόν αφού $(|G_0|, n) = (n, m) = 1$.
- $A_R = O(Q_1, G_0)$. Έχουμε ότι $C_m < \ker \beta$. Όπως και στην προηγούμενη περίπτωση έχουμε την $(n, m) = 1$ σαν μία αναγκαία συνθήκη για να είναι αυτός ο τύπος διακλάδωσης υλοποιήσιμος. Ο βαθμός του divisor που αντιστοιχεί στην τροχιά $O(P_i, G_0)$ είναι

  $$\sum_{P \in O(Q_i, G_0)} v_P(D) \equiv \begin{cases} 0 \bmod p^a & \text{αν} \quad \beta(\sigma) \not\equiv 1 \bmod p^a \\ \lambda |G_0| \bmod p^a & \text{αν} \quad \beta(\sigma) \equiv 1 \bmod p^a \end{cases}$$

  όπου $p^a \mid n, p^{a+1} \nmid n$. Έστω $n_0 = \prod_{p|n, \beta(\sigma) \equiv 1 \bmod p^a} p^a$. Θα πρέπει να διαλέξουμε το πλήθος των τροχιών s τέτοιο ώστε $\deg(D) \equiv 0 \bmod n_0$. Αυτό είναι δυνατόν θέτοντας

$\lambda(P) = 1$ για όλα τα $P \in \mathrm{supp}(D)$ αφού ο $(n_0, |G_0|)$ διαιρεί το $(n, mp) = (n, m) = 1$ και συνεπώς η εξίσωση

$$\deg(D) = p^t + s \cdot |G_0| \equiv 0 \bmod n_0,$$

έχει μία λύση $\bmod n_0$.

- $A_R = O(Q, G_0) \cup O(Q_1, G_0)$. Στην περίπτωση αυτή ο ομομορφισμός β πρέπει να είναι τετριμμένος. Θέτουμε $\lambda(Q) \equiv -1 \bmod n$, $\lambda(P_i) = \lambda(Q_1) \equiv 1 \bmod n$, και διαλέγουμε το s, τέτοιο ώστε
$$\deg(D) = -1 + p^t + s \cdot |G_0| \equiv 0 \bmod n.$$
Αυτό είναι δυνατόν αφού $(n, |G_0|) \mid m$ και $m \mid p^t - 1$.

2.2.6 Διεδρικές ομάδες

Στην περίπτωση αυτή υποθέτουμε ότι η ομάδα πηλίκο είναι η διεδρική ομάδα D_m η οποία δέχεται μία παράσταση σε γεννήτορες και σχέσεις

$$D_m = \langle a, b / a^m = 1, b^2 = 1, ab = ba^{-1} \rangle.$$

Ο ομομορφισμός δράσης $\beta : D_m \longrightarrow \mathbb{Z}_n^*$ ορίζεται από τις τιμές του στους γεννήτορες a και b.

$$\beta : \begin{cases} a & \longmapsto & \beta(a) \\ b & \longmapsto & \beta(b) \end{cases}$$

Αφού ο β είναι ομομορφισμός ομάδων έχουμε ότι

$$\beta(a)^m \equiv 1 \bmod n, \quad \beta(b)^2 \equiv 1 \bmod n, \quad \beta(a)\beta(b) \equiv \beta(b)\beta(a)^{-1} \bmod n.$$

Ισχυριζόμαστε ότι $ord(\beta(a)) \leq 2$. Πράγματι, αν $ord(\beta(a)) > 2$ τότε $ord(\beta(b)) = 1$, αφού η πολλαπλασιαστική ομάδα $\mathbb{Z}_n^*$ είναι αβελιανή και δεν μπορεί να περιέχει την διεδρική ομάδα $D_{ord(\beta(a))}$. Αλλά τότε $\beta(ab) = \beta(a)\beta(b) = \beta(a)$ άτοπο, αφού η τάξη του $\beta(ab)$ είναι το πολύ 2. Επιπλέον αν $ord(\beta(a)) = 2$ τότε $2|m$ αφού $1 = \beta(a^m) = \beta(a)^m$.

Διακρίνουμε τρεις περιπτώσεις για την $\mathrm{Im}(\beta)$.

$$\mathrm{Im}(\beta) = \{1\} \quad \text{ή} \quad \mathrm{Im}(\beta) \cong \mathbb{Z}_2 \quad \text{ή} \quad \mathrm{Im}(\beta) \cong V_4.$$

Η τρίτη περίπτωση μπορεί να εμφανιστεί μόνο αν $m \equiv 0 \bmod 2$. Θα χρειαστούμε το παρακάτω

Λήμμα 2.2.8 *Έστω $n \in N$ και ℓ ακέραιος τέτοιος ώστε*

$$\ell^2 - 1 \equiv 0 \bmod n.$$

Υπάρχουν ακέραιοι $n^+(\ell), n^-(\ell)$ τέτοιοι ώστε

$$n = n^+(\ell) \cdot n^-(\ell) \qquad \text{όπου} \qquad \left(n^+(\ell), n^-(\ell)\right) = \begin{cases} 2 & \text{αν} \quad n \equiv 0 \bmod 2 \\ 1 & \text{αν} \quad n \equiv 1 \bmod 2 \end{cases}$$

με την επιπλέον ιδιότητα:

$$\ell \equiv 1 \bmod n^+(\ell) \quad \text{και} \quad \ell \equiv -1 \bmod n^-(\ell).$$

Απόδειξη: Ο αριθμός $n^+(\ell)$ ($n^-(\ell)$ αντίστοιχα) είναι ο μέγιστος διαιρέτης του n τέτοιος ώστε $n^+(\ell) | \ell - 1$ ($n^-(\ell) | \ell + 1$, αντίστοιχα). Αν δ είναι ένας διαιρέτης του n τότε $\delta | \ell^2 - 1 = (\ell - 1)(\ell + 1)$ και ο δ διαιρεί και το $\ell - 1$ και το $\ell + 1$ αν και μόνο αν $\delta = 2$ □

Θα εξετάσουμε τις δύο περιπτώσεις του θεωρήματος 2.2.1 για τις δύο διαφορετικές υλοποιήσεις του τύπου διακλάδωσης στην επέκταση $F_0/F_0^{G_0}$, ξεχωριστά.

Περίπτωση A) Η χαρακτηριστική p του σώματος k είναι $p \neq 2$, $(p,m) = 1$. Τρεις θέσεις του $F_1 := F_0^{G_0}$, έστω p_1, p_2, p_3, διακλαδίζονται στην επέκταση $F_0/F_0^{G_0}$ με δείκτες διακλάδωσης $2, 2, m$ αντίστοιχα. Θα συμβολίζουμε με $P_{1,i}, P_{2,i}, P_{3,j}$, όπου $i = 0, ..., m-1, j = 0, 1$ τις θέσεις του F_0 που επεκτείνουν τις p_1, p_2, p_3 αντίστοιχα.

Θεώρημα 2.2.9 *Έστω ότι η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με την διεδρική ομάδα D_m, όπου $p \nmid m$ και $p \neq 2$. Ξεχωρίζουμε τις παρακάτω περιπτώσεις για την δομή της ομάδας G:*

1. *Υποθέτουμε ότι $\{P_{1,i}\}_{0 \le i < m} \cup \{P_{3,j}\}_{j=0,1} \subset A_R$. Σε αυτή την περίπτωση θα πρέπει $(n,m) \mid 2$ ενώ η ομάδα αυτομορφισμών G δέχεται την παρακάτω παράσταση σε γεννήτορες και σχέσεις:*
$$G = \langle R, S | R^2 = S^m, S^{nm} = 1, RSR^{-1} = S^r \rangle,$$
όπου r είναι μία λύση του συστήματος
$$r \equiv 1 \bmod n, \quad r \equiv -1 mod m. \tag{2.18}$$
Αν $(n,m) = 1$ η λύση r είναι μοναδική. Αν $(n,m) = 2$ τότε ξεχωρίζουμε δύο υποπεριπτώσεις:
   - *$n \equiv 2 \bmod 4$. Σε αυτή την περίπτωση η μία λύση του (2.18) προκύπτει όταν $\{P_{2,i}\}_{0 \le i < m} \cap A_R = \emptyset$ και η άλλη όταν $\{P_{2,i}\}_{0 \le i < m} \cap A_R \neq \emptyset$.*
   - *$n \equiv 0 \bmod 4$. Σε αυτή την περίπτωση $\{P_{2,i}\}_{0 \le i < m} \cap A_R = \emptyset$ και υπάρχουν δύο μη ισόμορφες ομάδες που αντιστοιχούν στον ίδιο τύπο διακλάδωσης.*
2. *$A_R = \{P_{3,j}\}_{j=1,2}$. Η ομάδα G είναι ισόμορφη με το ημιευθές γινόμενο $C_{nm} \rtimes C_2$.*
3. *$A_R = \{P_{1,i}\}_{0 \le i < m} \cup \{P_{2,i}\}_{i=1,...,m}$ Σε αυτή την περίπτωση η συνάρτηση β είναι τετριμμένη και η ομάδα G είναι ισόμορφη με την $C_n \times D_m$ αν $(n,2) = 1$ και η G δίνεται απο*
$$G = \langle R, S | R^{2n} = 1, S^m = 1, RSR^{-1} = S^{-1} \rangle,$$
αν $(n,m) = 2$.
4. *$A_R = \emptyset$. Σε αυτή την περίπτωση η G είναι ισόμορφη μ την $C_n \rtimes D_m$, όπου η δράση της D_m στην C_n δίνεται απο την β.*
5. *$A_R = \{P_{1,i}\}_{0 \le i < m}$ Σε αυτή την περίπτωση η G δέχεται την παρακάτω παράσταση*
$$G = \langle R, S | R^{2n} = 1, S^m = 1, (RS)^2 = 1 \rangle.$$

Απόδειξη: Θα ξεκινήσουμε με την ακόλουθη

Παρατήρηση 2.2.10 *Ας υποθέσουμε ότι το $b \in D_m$ σταθεροποιεί την θέση $P_{1,0}$. Οι άλλες θέσεις $P_{1,i}$ μπορούν να αριθμηθούν έτσι ώστε $P_{1,i} = a^i P_{1,0}$. Οι ομάδες ανάλυσης $D_m(P_{1,i})$ κάθε θέσης $P_{1,i}$ είναι της μορφής*
$$D_m(P_{1,i}) = D_m(a^i P_{1,0}) = a^i D_m(P_{1,0}) a^{-i} = \langle a^{2i} b \rangle.$$
Κάθε αυτομορφισμός $ba^k \in D_m$ έχει δύο σταθερές θέσεις. Κάθε θέση της μορφής $P_{1,i}$ σταθεροποιείται από τον $ba^k \neq 1$, αν και μόνο αν $ba^k \in \langle a^{2i} b \rangle$ και αφού $ord(a^{2i}b) = 2$ αυτό είναι ισοδύναμο με την
$$a^{2i} b = ba^k = a^{-k} b \Leftrightarrow 2i \equiv -k \bmod m. \tag{2.19}$$

Αν $(m,2)=2$ τότε η εξίσωση (2.19) έχει δύο λύσεις αν ο k είναι άρτιος, και καμία λύση αν ο k είναι περιττός. Τα παραπάνω αποδεικνύουν ότι οι δύο σταθερές θέσεις του αυτομορφισμού ba^k περιορίζονται στην ίδια θέση p_1 (αν ο $k \equiv 0 \bmod 2$) ή p_2 (αν $k \equiv 1 \bmod 2$). Στην περίπτωση $(m,2)=1$ η εξίσωση (2.19) έχει μοναδική λύση, έτσι μία από της δύο σταθερές θέσεις του ba^k περιορίζεται στην p_1 και η άλλη στην p_2.

Παρατήρηση 2.2.11 *Αφού οι επεκτάσεις F/F_0 και $F_0/F_0^{D_m}$ είναι και οι δυο Galois, οι θέσεις P_i του F_0 πάνω από μία κοινή θέση $p \in F_0^{G_0}$ στην επέκταση F/F_0 ή διακλαδίζονται όλες πλήρως ή αναλύονται όλες πλήρως,*

Ας υποθέσουμε ότι μία από τις θέσεις $P_{3,j}$, έστω η $P_{3,1}$ διακλαδίζεται στην επέκταση F/F_0. Έστω $Q_{3,j}$ η μοναδική θέση του F πάνω από $P_{3,j}$ (j σταθερό). Αφού $(m,p)=1$ έχουμε ότι η ομάδα ανάλυσης $G(Q_{3,1})$ είναι κυκλική τάξης nm. Συνεπώς $\beta(a) \equiv 1 \bmod n$. Παρατηρούμε ότι ο δείκτης $|G : G(Q_{3,1})| = 2$ άρα $G(Q_{3,1}) \lhd G$ και G είναι μία μετακυκλική ομάδα. Διαλέγουμε $S, R \in G$, τέτοια ώστε $\pi(R) = b, \pi(S) = a$. Μπορούμε να διαλέξουμε $S \in \pi^{-1}(a)$ τέτοιο ώστε $\langle S \rangle = G\left(Q_{3,1}\right)$. Αφού $G\left(Q_{3,1}\right) \lhd G$, υπάρχει ακέραιος r τέτοιος ώστε

$$RSR^{-1} = S^r. \tag{2.20}$$

Παρατηρούμε ότι η ομάδα C_n γεννάται από τον $\langle S^m \rangle$. Αρά από την (2.20) και την δράση του b στην C_n, έχουμε

$$S^{\beta(b)m} = RS^mR^{-1} = S^{rm},$$

το οποίο δίνει την σχέση

$$r \equiv \beta(b) \bmod n. \tag{2.21}$$

Ισχύει $G/C_n \cong D_n$ άρα από την (2.20) έχουμε

$$RSR^{-1}S = S^{r+1} \in \langle S^m \rangle$$

και αυτό οδηγεί στην σχέση

$$r \equiv -1 \bmod m. \tag{2.22}$$

Το σύστημα των εξισώσεων (2.21)(2.22) έχει λύσεις αν και μόνο αν $(n,m) | \beta(b)+1$. Διαχωρίζουμε δύο επιπλέον περιπτώσεις

(1) $\{P_{1,i}\}_{0 \le i < m} \cup \{P_{3,j}\}_{j=0,1} \subset A_R$, δηλαδή μία από τις θέσεις $P_{1,i}$, $i = 0, ..., m-1$, έστω η $P_{1,0}$, διακλαδίζεται πλήρως στην επέκταση F/F_0. Θα συμβολίζουμε με $Q_{1,0}$ την θέση υπεράνω της $P_{1,0}$. Όπως στην παρατήρηση 2.2.10 μπορούμε να υποθέσουμε ότι η $P_{1,0}$ σταθεροποιείται από το $b \in D_m$ (αν χρειαστεί διαλέγουμε σαν γεννήτορα b της D_m ένα άλλο στοιχείο τάξης δύο). Η ομάδα ανάλυσης $G(Q_{1,0})$ είναι κυκλική τάξης $2n$. Διαλέγουμε ένα γεννήτορα $R \in \pi^{-1}(b)$ της $G(Q_{1,0})$.

Η ομάδα C_n, είναι η μοναδική υποομάδα τάξης n της κυκλικής ομάδας $\langle R \rangle$, άρα παράγεται από το R^2. Συνεπώς $R^2 = S^{mi}$ για κάποιο $(i,n) = 1$. Απλοποιούμε τον συμβολισμό διαλέγοντας κατάλληλο γεννήτορα S της ομάδας $G(Q_{3,1})$ για τον οποίο $R^2 = S^m$. Επίσης παρατηρούμε ότι $\beta(b) \equiv 1 \bmod n$. Η ομάδα G σαν μετακυκλική ομάδα δέχεται την παρακάτω παράσταση σε γεννήτορες και σχέσεις

$$G = \langle R, S / R^2 = S^m, S^{nm} = 1, RSR^{-1} = S^r \rangle, \tag{2.23}$$

όπου το r ορίζεται να είναι λύση του συστήματος

$$\begin{aligned} r &\equiv 1 \bmod n \\ r &\equiv -1 \bmod m. \end{aligned} \tag{2.24}$$

Το παραπάνω σύστημα δέχεται (n,m) λύσεις αν και μόνο αν $(n,m)|2$. Στην περίπτωση $(n,m)=1$ η λύση r καθορίζεται μονοσήμαντα $\bmod nm$. Στην περίπτωση $(n,m)=2$ έχουμε δύο λύσεις $\bmod nm$ τις

$$r_0, r_1 = r_0 + \frac{nm}{2}.$$

Υποθέσαμε ήδη ότι οι θέσεις στην τροχιά του $P_{1,0}$ διακλαδίζονται πλήρως στην επέκταση F/F_0. Είναι ενδιαφέρον να δούμε πως ο τύπος διακλάδωσης των θέσεων $P_{2,i}$ καθορίζει την επιλογή της ρίζας r_0.

Έστω $P = P_{2,k}$ μία θέση του F_0 στην τροχιά του $P_{2,0}$, συνεπώς, σύμφωνα με την παρατήρηση 2.2.10, σταθεροποιείται από τον $ba^i \in D_m$, για κάποιο $i \equiv 1 \bmod 2$ (υπενθυμίζουμε ότι $2|m$). Σύμφωνα με το πόρισμα 2.2.4, η P αναλύεται (αντίστοιχα διακλαδίζεται) αν $G_\pi(P) = C_2 \times C_n$ (αντίστοιχα C_{2n}). Η συνάρτηση

$$\Phi_P \ : \left\{ \begin{array}{ccc} G_\pi(P) & \longrightarrow & G_\pi(P) \\ x & \longmapsto & x^2 \end{array} \right.$$

είναι ομομορφισμός ομάδων και αφού $2|n$ έχουμε $\ker \Phi_P = C_2 \times C_2$ αν η P αναλύεται, διαφορετικά (δηλαδή αν η P διακλαδίζεται) $\ker \Phi_P = C_2$. Υπολογίζουμε ότι

$$G_\pi(P) = \left\{ RS^{i+sm}, S^{sm} / s = 0, ..., n-1 \right\} \text{ για κάποιο } i \equiv 1 \bmod 2.$$

Τα στοιχεία $\left\{1, S^{nm/2}\right\}$ ανήκουν στον $\ker \Phi_P$. Επιπλέον χρησιμοποιώντας την (2.23) έχουμε

$$\left(RS^{i+sm}\right)^2 = S^{m(1+\frac{r+1}{m}(i+sm))}.$$

Συνεπώς η P αναλύεται στην επέκταση F/F_0 αν και μόνο αν η εξίσωση

$$-(r+1)s \equiv 1 + i\frac{r+1}{m} \bmod n$$

έχει λύση s. Η εξίσωση αυτή έχει $(r+1,n)=2$ διαφορετικές $\bmod n$ λύσεις αν και μόνο αν $(r+1,n) = 2|\ 1 + i\frac{r+1}{m}$. Αφού $i \equiv 1 \bmod 2$ έχουμε την ισοδυναμία

$$1 + i\frac{r+1}{m} \equiv 0 \bmod 2 \Longleftrightarrow \frac{r+1}{m} \not\equiv 0 \bmod 2.$$

Στην περίπτωση που $n \equiv 2 \bmod 4$ το $n/2$ είναι περιττό και το 2 διαιρεί ή το $\frac{r_0+1}{m}$ ή το $\frac{r_1+1}{m} = \frac{r_0+1}{m} + \frac{n}{2}$. Συνεπώς αν $n \equiv 2 \bmod 4$ οι δύο λύσεις του συστήματος (2.24) αντιστοιχούν στους διαφορετικούς τύπους διακλάδωσης των θέσεων $P_{2,i}$ στην επέκταση F/F_0.

Στην περίπτωση $n \equiv 0 \bmod 4$ έχουμε $\frac{r+1}{m} \not\equiv 0 \bmod 2$ και για τις δύο λύσεις του (2.24). Πράγματι αν $2|\frac{r+1}{m}$ τότε $4|r+1$ (υπενθυμίζουμε ότι $2|m$) και $4|n|r-1$ έτσι $4|(r+1)-(r-1)=2$, άτοπο. Λοιπόν, αν $n \equiv 0 \bmod 4$ τότε και για τις δύο λύσεις του (2.24) έχουμε ότι όλες οι θέσεις $P_{2,i}$ αναλύονται στην επέκταση F/F_0. Στην περίπτωση αυτή ο τύπος διακλάδωσης αδυνατεί να προσδιορίσει την δομή της ομάδας αυτομορφισμών.

Παράδειγμα: Σαν παράδειγμα θα δώσουμε δύο καμπύλες με τα ίδια σημεία διακλάδωσης, αλλά με διαφορετικές ομάδες αυτομορφισμών. Θεωρούμε τις καμπύλες V_1, V_2 ορισμένες υπέρανω του σώματος των μιγαδικών αριθμών $\mathbb{C}$ που δίνονται από τις σχέσεις

$$V_1 : y^4 = x(x^{10}-1) \quad \text{και} \quad V_2 : y^4 = x^3(x^{10}-1)$$

και έστω F_1, F_2 τα αντίστοιχα σώματα συναρτήσεων τους. Η θεωρία διακλάδωσης κυκλικών επεκτάσεων δίνει ότι στις επεκτάσεις $F_1/\mathbb{C}(x)$ και $F_2/\mathbb{C}(x)$ οι θέσεις που διακλαδίζονται είναι οι

$$\{P_{x=0}, P_{x=\zeta^i}, P_\infty\},$$

όπου το ζ^i διατρέχει τις 10 ρίζες της μονάδας. Το κριτήριο κανονικότητας του πορίσματος 1.1.3 δίνει ότι η ομάδα Galois

$$C_4 \cong Gal(F_1/\mathbb{C}(x)) \cong Gal(F_2/\mathbb{C}(x))$$

είναι κανονική σε ολόκληρη την ομάδα αυτομορφισμών G_i, και των δύο σωμάτων συναρτήσεων F_1 και F_2. Το πηλίκο $H_i = G_i/C_4$ είναι η μεγαλύτερη πεπερασμένη υποομάδα του $PGL(2,\mathbb{C})$ της οποίας τα στοιχεία μπορούν να επεκταθούν σε αυτομορφισμούς του σώματος F_i. Θα αποδείξουμε ότι η ομάδες H_i γεννούνται από τους παρακάτω μετασχηματισμούς Möbius

$$\tau : x \longmapsto 1/x, \sigma : x \longmapsto \zeta x,$$

όπου ζ είναι μία πρωταρχική 10-ρίζα της μονάδας, δηλαδή $H_i \cong D_{10}$.

Έστω c μία πρωταρχική 40-ρίζα της μονάδος. Οι αυτομορφισμοί:

$$R_1 : \left\{ \begin{array}{c} y \longmapsto c^5 y/x^3 \\ x \longmapsto 1/x \end{array} \right. , \quad S_1 : \left\{ \begin{array}{c} y \longmapsto cy \\ x \longmapsto c^4 x \end{array} \right. .$$

επεκτείνουν τους τ, σ στο F_1 και οι αυτομορφισμοί

$$R_2 : \left\{ \begin{array}{c} y \longmapsto c^{15} y/x^4 \\ x \longmapsto 1/x \end{array} \right. , \quad S_2 : \left\{ \begin{array}{c} y \longmapsto c^3 y \\ x \longmapsto c^4 x \end{array} \right. ,$$

επεκτείνουν τους τ, σ στην F_2 αντίστοιχα. Δηλαδή, $D_{10} < H_i$. Από τις δυνατές επιλογές των ομάδων αυτομορφισμών της $PGL(2,\mathbb{C})$ έχουμε ότι $H_i \cong D_{10i}$. Έστω ρ ένα στοιχείο τάξης $10i$ στην D_{10i} και $R \in G_i$ τέτοιο ώστε $R|_{\mathbb{C}(x)} = \rho$. Ο αυτομορφισμός ρ είναι της μορφής

$$\rho : x \longmapsto ax,$$

όπου a είναι μία πρωταρχική $10i$-ρίζα της μονάδας [27, σελ. 87]. Από την θεωρία των κυκλικών επεκτάσεων του Kummer έχουμε ότι $R(y) = y^\ell g$, $(\ell, 4) = 1, g \in k(x)$. Συνεπώς,

$$\left(\frac{R(y)}{y^\ell}\right)^4 = \frac{a^{k_i} x^{k_i} (a^{10} x^{10} - 1)}{x^{\ell k_i} (x^{10} - 1)^\ell}, \tag{2.25}$$

όπου $k_1 = 1, k_2 = 3$ και $R(y)/y^\ell = g \in k(x)$. Από την (2.25) παίρνουμε ότι

$$k_i(\ell - 1) \equiv 0 \bmod 4$$

και αφού $(\ell, 4) = 1$ έχουμε τελικά ότι $\ell = 1$. Συγκρίνοντας τις πολλαπλότητες των ριζών και των πόλων του δεξιού μέλους της (2.25) πέρνουμε ότι $\zeta = \zeta^i/a$, και συνεπώς η τάξη του ρ είναι 10 και $H_i \cong D_{10}$.

Από τους τύπους των R_i, S_i, μπορούμε να ελέγξουμε ότι οι ομάδες G_i, δέχονται παραστάσεις σε όρους γεννητόρων-σχέσεων ώς εξής:

$$G_1 = \langle R_1, S_1 | S_1^{40} = 1, R_1^2 = S_1^{10}, R_1 S_1 R_1^{-1} = S_1^{29} \rangle$$

και

$$G_2 = \langle R_2, S_2 | S_2^{40} = 1, R_2^2 = S_2^{10}, R_2 S_2 R_2^{-1} = S_2^{9} \rangle.$$

Οι ομάδες G_1 και G_2 δεν είναι ισόμορφες. Πράγματι, ας υποθέσουμε ότι υπάρχει ένας ισομορφισμός $\phi : G_1 \longrightarrow G_2$. Κάθε στοιχείο στην G_2 είναι της μορφής $R_2 S_2^j$ ή της μορφής S_2^j. Όμως

$$(R_2 S_2^j)^2 = S^{10+10j},$$

άρα $R_2 S_2^j$ έχει τάξη το πολύ 8 και αυτό αποδεικνύει ότι $\phi(S_1) = S_2^j$ $(j, 40) = 1$. Επιπλέον έχουμε

$$S_2^{29j} = \phi(S_1^{29}) = \phi(R_1 S_1 R_1^{-1}) = R_2 S_2^j R_2^{-1} = S_2^{9j}.$$

Δηλαδή πρέπει $20j \equiv 0 \bmod 40$, άτοπο αφού $(40, j) = 1$. □

(2) $A_R = \{P_{3,j}\}_{j=1,2}$. Σε αυτή την περίπτωση οι θέσεις $P_{i,j}$ $i = 1, 2$ $j = 0, ..., m-1$ του F_0 αναλύονται όλες στην επέκταση F/F_0. Σύμφωνα με το πόρισμα 2.2.4 έχουμε

$$G_\pi(P_{i,j}) \cong C_n \rtimes C_2.$$

Μπορούμε να διαλέξουμε $R \in \pi^{-1}(b)$ τέτοιο ώστε $R^2 = 1$. Η ομάδα G δίνεται από

$$\langle R, S / S^{nm} = 1, R^2 = 1, RSR^{-1} = S^r \rangle$$

όπου r είναι η λύση του συστήματος των εξισώσεων (2.21)(2.22),

$$r \equiv \beta(b) \bmod n, r \equiv -1 \bmod m. \tag{2.26}$$

Η ομάδα G είναι ένα ημιευθύ γινόμενο

$$C_{nm} \rtimes C_2,$$

με δράση να καθορίζεται από το r. Αν $(n, m) > 1$ τότε το σύστημα 2.26 μπορεί να έχει περισσότερες από μία λύσεις $\bmod\, nm$ οι οποίες οδηγούν σε περισσότερες από μία μη ισόμορφες ομάδες αυτομορφισμών G.

Ας υποθέσουμε ότι οι θέσεις $P_{3,j}$ $j = 1, 2$ δεν διακλαδίζονται στην επέκταση F/F_0. Από το πόρισμα 2.2.4 έχουμε ότι

$$G_\pi(P_{3,1}) \cong C_n \rtimes C_m$$

αφού η $D_m(P_{3,j}) = \langle a \rangle$ είναι κυκλική. Η ομάδα $G_\pi(P_{3,1})$ έχει δείκτη 2 στην G, άρα $C_n \rtimes C_m \lhd G$. Έστω T ένας γεννήτορας της κυκλικής ομάδας C_n, και S ένας γεννήτορας της C_m τέτοιος ώστε $\pi(S) = a$. Αν $R \in \pi^{-1}(b)$ αφού $|G : C_n \rtimes C_m| = 2$ το στοιχείο $R^2 \in C_n \rtimes C_m$ άρα $R^2 = T^\mu S^z$. Αλλά $\pi(R^2) = a^z$ έτσι $z \equiv 0 \bmod m$ και $R^2 = T^\mu$. Αυτό μας δίνει

$$R^2 S R^{-2} = T^\mu S T^{-\mu} = T^{\mu(1-\beta(a))} S. \tag{2.27}$$

Μπορούμε να υπολογίσουμε το αριστερό μέλος της (2.27) και με διαφορετικό τρόπο. Αφού $C_n \rtimes C_m \lhd G$ έχουμε

$$RSR^{-1} = T^\lambda S^r.$$

Από την άλλη $G/\langle T \rangle \cong D_m$ άρα

$$RSR^{-1}S = T^\lambda S^{r+1} \in \langle T \rangle \text{ συνεπώς } r \equiv -1 \bmod m \tag{2.28}$$

και αυτό μας δίνει

$$R^2 S R^{-2} = R T^\lambda S^{-1} R^{-1} = T^{\lambda(\beta(b) - \beta(a))} S. \tag{2.29}$$

Συνδυάζοντας τις (2.27) και (2.29) πέρνουμε

$$\mu(1 - \beta(a)) \equiv \lambda(\beta(b) - \beta(a)) \bmod n. \tag{2.30}$$

Οι γεννήτορες $T, R, S \in G$ ικανοποιούν τις παρακάτω σχέσεις:

$$S^m = 1, T^n = 1, R^2 = T^\mu, RTR^{-1} = T^{\beta(b)}, STS^{-1} = T^{\beta(a)}, RSR^{-1} = T^\lambda S^{-1}, \tag{2.31}$$

για κάποια λ, μ που ικανοποιούν την (2.30). Παρατηρούμε ότι δεν απαιτούνται επιπρόσθετες σχέσεις στον ορισμό της ομάδας G, γιατί οι σχέσεις (2.31) ορίζουν ομάδα τάξης $2nm$.

Θέλουμε να απλοποιήσουμε την σχέση $RSR^{-1} = T^\lambda S^{-1}$ διαλέγοντας ένα διαφορετικό γεννήτορα $S_1 = T^x S$. Υπολογίζουμε:

$$R S_1 R^{-1} = R T^x S R^{-1} = T^{x\beta(b)+\lambda} S^{-1} = T^{x(\beta(a)+\beta(b))+\lambda} S_1^{-1}. \tag{2.32}$$

Λήμμα 2.2.12 *Έστω P μία θέση του F_0 η οποία σταθεροποιείται από το ba. Επιπλέον υποθέτουμε ότι $R^2 = T^{\mu}$. Αν $2|n$ τότε*

$$(n, \beta(b)\beta(a)+1)|\lambda + \mu\beta(a), \tag{2.33}$$

αν και μόνο αν η θέση P αναλύεται στην επέκταση F/F_0. Αν $(2,n) = 1$ τότε η εξίσωση (2.33) ισχύει σε κάθε περίπτωση.

Απόδειξη: Υποθέτουμε πρώτα ότι $2|n$. Από το πόρισμα (2.2.4) έχουμε

$$G_\pi(P) = Gal(F/F_0^{\langle ba\rangle}) = \begin{cases} C_{2n} & \text{αν } P \text{ διακλαδίζεται στην } F/F_0 \\ C_n \rtimes C_2 & \text{αν } P \text{ αναλύεται στην } F/F_0 \end{cases}.$$

Στην πρώτη περίπτωση υπάρχει μόνο ένα στοιχείο τάξης δύο στην ομάδα $Gal(F/F_0^{\langle ba\rangle})$ ενώ στην δεύτερη περίπτωση υπάρχουν περισσότερα του ενός στοιχεία τάξης δύο στην $G_\pi(P)$. Υπενθυμίζουμε ότι η ομάδα $G_\pi(P)$ είναι η

$$G_\pi(P) = \{\sigma \in G/\pi(\sigma)P = P\} = \left\{RST^k, T^k/k = 0, ..., n-1\right\}.$$

Αφού το n είναι άρτιος, ένα στοιχείο τάξης δύο της $G_\pi(P)$ είναι το $T^{n/2}$. Αν το RST^k είναι ένα άλλο στοιχείο τάξης δύο τότε

$$1 = (RST^k)^2 = T^{k(\beta(b)\beta(a)+1)+\lambda+\mu\beta(a)} \tag{2.34}$$

άρα για κάποιο $k \in \{0, ..., n-1\}$

$$k(\beta(b)\beta(a)+1) + \lambda + \mu\beta(a) \equiv 0 \bmod n, \tag{2.35}$$

Όμως η εξίσωση (2.35) έχει λύσεις ως προς k αν και μόνο αν

$$(n, \beta(b)\beta(a)+1)|\lambda + \mu\beta(a).$$

Στην περίπτωση $(n,2) = 1$, το μοναδικό στοιχείο τάξης δύο στην ομάδα $Gal(F/F^{\langle ba\rangle})$ είναι της μορφής RST^k άρα η (2.34) έχει μία λύση, και το επιθυμητό αποτέλεσμα προκύπτει ακριβώς όπως και στην περίπτωση άρτιου n.□

Θα θεωρήσουμε τώρα τις τρείς τελευταίες περιπτώσεις του θεωρήματος

(3) $A_R = \{P_{1,i}\}_{0\le i<m-1} \cup \{P_{2,i}\}_{0=1,\dots,m-1}$ Όλες οι θέσεις $P_{i,j}$ διακλαδίζονται στην επέκταση F/F_0. Υποθέτουμε όπως και στην παρατήρηση 2.2.10 ότι $D_m(P_{1,0}) = \langle b\rangle$. Εξ αιτίας του πορίσματος 2.2.4 μπορούμε να διαλέξουμε $R \in \pi^{-1}(b)$ τέτοιο ώστε $R^2 = T$, δηλαδή $\mu = 1$. Επιπλέον η επέκταση είναι κεντρική σε αυτή την περίπτωση δηλαδή

$$\beta(a) \equiv \beta(b) \equiv 1 mod n.$$

Θεωρούμε δύο ακόμα υποπεριπτώσεις

- $(n,2) = 1$. Αφού η επέκταση είναι κεντρική έχουμε $H^2(D_m, C_n) = 1$, δηλαδή υπάρχει μόνο μία επέκταση της D_m με C_n, η

$$G \cong C_n \times D_m.$$

- $(n,2) = 2$. Η εξίσωση (2.32), σε αυτή την περίπτωση, έχει την μορφή

$$RS_1R^{-1} = T^{2x+\lambda}S_1^{-1}. \tag{2.36}$$

  Από το λήμμα 2.2.12 έχουμε ότι $(n, \beta(a)\beta(b)+1) = 2 \nmid \lambda + 1$, Συνεπώς $2|\lambda$ και έτσι η εξίσωση

$$2x + \lambda \equiv 0 \bmod n$$

έχει μία λύση x. Η σχέση (2.36) για την συγκεκριμένη αυτή λύση x γράφεται ως

$$RS_1R^{-1} = S_1^{-1}.$$

Έστω t η τάξη του S_1. Η ομάδα G είναι μία μετακυκλική ομάδα που δέχεται την παρακάτω παράσταση σε γεννήτορες και σχέσεις:

$$\langle R, S_1 | R^{2n} = 1, S_1^t = 1, RS_1R^{-1} = S_1^{-1} \rangle,$$

αλλά τότε $|G| = 2nt$, συνεπώς $t = m$.

(4) $A_R = \emptyset$. Όλες οι θέσεις $P_{i,j}$ αναλύονται στην επέκταση F/F_0. Ας υποθέσουμε ότι $D_m(P_{1,0}) = \langle b \rangle$. Εξ αιτίας του πορίσματος 2.2.4 μπορούμε να διαλέξουμε $R \in \pi^{-1}(b)$ τέτοιο ώστε $R^2 = 1$, και $\mu = 0$. Αφού όλες οι θέσεις του F_0 οι οποίες επεκτείνουν τις p_1, p_2 αναλύονται στην F/F_0 από το λήμμα 2.2.12 έχουμε ότι $(n, \beta(b)\beta(a) + 1)|\lambda$. Αλλά $(\beta(b), n) = 1$, έτσι $(n, \beta(ba) + 1) = (n, \beta(b)\beta(b)\beta(a) + \beta(b)) = (n, \beta(a) + \beta(b))|\lambda$. Συνεπώς υπάρχει ένα x τέτοιο ώστε

$$x(\beta(a) + \beta(b)) + \lambda \equiv 0 \bmod n$$

και για αυτό το x, η εξίσωση (2.32) γίνεται

$$RS_1R^{-1} = T^{x(\beta(a)+\beta(b))+\lambda} S_1^{-1} = S_1^{-1}.$$

Θα συμβολίζουμε με t την τάξη του $S_1 = T^x S$. Η ομάδα σε αυτή την περίπτωση δίνεται από τους παρακάτω γεννήτορες και σχέσεις

$$\langle R, T, S_1 | R^2 = 1, RTR^{-1} = T^{\beta(b)}, S_1TS_1^{-1} = T^{\beta(a)}, RS_1R^{-1} = S_1^{-1}, S_1^t = 1, T^n = 1 \rangle,$$

και είναι τάξης $2nt$, από όπου έχουμε $t = m$ και η ομάδα G είναι ισόμορφη με το ημιευθύ γινόμενο

$$C_n \rtimes D_m$$

όπου η δράση του D_m στην C_n καθορίζεται από τον μορφισμό β.

(5) $A_R = \{P_{1,i}\}_{0 \leq i < m}$. Σε αυτή την περίπτωση υποθέτουμε ότι το σύνολο των θέσεων $P_{1,i}$, υπέρ της p_1 διακλαδίζονται στην επέκταση F/F_0 και το σύνολο των θέσεων $P_{2,i}$ υπέρ της p_2 αναλύονται. Μπορούμε να διαλέξουμε $R \in \pi^{-1}(b)$ τέτοιο ώστε $R^2 = T$ συνεπώς $\mu = 1$. Επιπλέον $\beta(b) \equiv 1 \bmod n$.

Από το λήμμα 2.2.12 έχουμε ότι $(\beta(b)\beta(a) + 1, n) = (\beta(a) + 1, n) \,|\lambda + \beta(a)$. Άρα υπάρχει x έτσι ώστε

$$x(\beta(a) + 1) + \lambda \equiv -\beta(a) \bmod n$$

και για αυτό το x η εξίσωση (2.32) γράφεται

$$RS_1R^{-1} = T^{x(\beta(a)+\beta(b))+\lambda} S_1^{-1} = T^{-\beta(a)} S_1^{-1} = S_1^{-1} T^{-1}.$$

Αφού $T = R^2$ η παραπάνω σχέση είναι ισοδύναμη με την

$$(RS_1)^2 = 1.$$

Θα συμβολίζουμε με t την τάξη του S_1. Η ομάδα G δέχεται την παρακάτω παράσταση σε γενήτορες και σχέσεις:

$$G = \langle R, S_1 | R^{2n} = 1, S_1^t = 1, (RS_1)^2 = 1 \rangle.$$

Παρατηρούμε ότι η ομάδα που γεννάται από το R^2 είναι η ομάδα Galois $Gal(F/F_0)$ η οποία είναι κανονική υποομάδα της G. Το πηλίκο

$$\overline{G} := \frac{G}{\langle R^2 \rangle} = \langle \overline{R}, \overline{S}_1 | \overline{R}^2 = 1, \overline{S}_1^t = 1, (\overline{RS}_1)^2 = 1 \ \rangle$$

είναι ισόμορφο με μία διεδρική ομάδα τάξης $2t$. Συνεπώς η ομάδα G έχει τάξη $2nt$ και $t = m$. $\square$

Θα αποδείξουμε τώρα ότι οι παραπάνω τύποι διακλάδωσης υλοποιούνται, δηλαδή θα πρέπει να επιλέξουμε $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ βαθμού $0 \bmod n$.

(1) Ξεχωρίζουμε τις παρακάτω υποπεριπτώσεις:

- $n \equiv 2 \bmod 4$, $m \equiv 0 \bmod 2$. Σε αυτή την περίπτωση έχουμε στον φορέα του D το παρακάτω σύνολο A_R σταθερών θέσεων D_m

$$A_R = \{P_{3,1}, P_{3,2}, P_{1,0}, P_{1,1}, ..., P_{1,i-1}\}$$

  ή

$$A_R = \{P_{3,1}, P_{3,2}, P_{1,0}, P_{1,1}, ..., P_{1,i-1}, P_{2,0}, P_{2,1}, ..., P_{2,i-1}\}$$

  και φυσικά s τροχιές $O(P_j, D_m)$ όπου η θέση P_j δεν σταθεροποιείται από την D_m. Εδώ για απλοποίηση του συμβολισμού γράφουμε δύο περιπτώσεις μαζί, την δεύτερη εντός παρενθέσεων. Υπενθυμίζουμε ότι στην περίπτωση αυτή, η συνάρτηση δράσης β είναι τετριμμένη, οπότε παίρνοντας $\lambda(Q) = 1$ για όλα τα $Q \in \mathrm{supp}(D)$ έχουμε ότι

$$\deg(D) = 2 + m + 2ms \text{ ή } \deg(D) = 2 + 2m + 2ms.$$

  Αφού $(2m, n) = 2$ το οποίο διαιρεί το $2 + m$ ($2 + 2m$ αντίστοιχα), μπορούμε να διαλέξουμε το s έτσι ώστε $\deg(D) \equiv 0 \bmod n$.

- $n \equiv 0 \bmod 4, m \equiv 0 \bmod 2$. Στην περίπτωση αυτή έχουμε στον φορέα του D το παρακάτω σύνολο A_R σταθερών θέσεων D_m

$$A_R = \{P_{3,1}, P_{3,2}, P_{1,0}, P_{1,1}, ..., P_{1,i-1}\},$$

  και s τροχιές $O(P_j, D_m)$ όπου οι θέσεις P_j δεν σταθεροποιούνται από τον D_m. Παίρνουμε $\lambda(Q) = 1$ για όλα τα Q στο $\mathrm{supp}(D)$, έτσι

$$\deg(D) = 2 + m + 2ms.$$

  Στην περίπτωση αυτή $(2m, n) = 4$ το οποίο διαιρεί το $2 + m$ (υπενθυμίζουμε ότι αφού $(n, m) = 2$, $m \equiv 2 \bmod 4$), οπότε μπορούμε να διαλέξουμε το s έτσι ώστε $\deg(D) \equiv 0 \bmod n$.

Με όμοιο τρόπο μπορούμε να δείξουμε ότι μπορούμε να διαλέξουμε $\deg(D) \equiv 0 \bmod n$ στην περίπτωση $(n, m) = 1$.

(2) Στην περίπτωση αυτή έχουμε $A_R = \{P_{3,1}, P_{3,2}\}$. Αναλύουμε το n σε γινόμενο πρώτων παραγόντων $n = p_1^{a_1} \dots p_t^{a_t}$. Σύμφωνα με το λήμμα 2.2.8 γράφουμε $n = n^+(\beta(b)) \cdot n^-(\beta(b))$, και $(n^+(\beta(b)), n^-(\beta(b))) = 1$ ή 2. Η εξίσωση (2.14), μας δίνει $\deg(D) \equiv 0 \bmod p_i^{a_i}$ για $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ και για $p_i \mid n^-(\beta(b)), p_i \neq 2$. Αν $2 \mid n$, και $p_{i_0} = 2$ τότε $\deg(D) \equiv 0 \bmod p_{i_0}^{a'_{i_0}}$, όπου $a'_{i_0} = v_2(n^-\beta(b)) < a_{i_0}$. Ο τυχαίος divisor $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ γράφεται

$$D = \lambda(P_{3,1} + P_{3,2}) + \sum_{i=1}^{s} \lambda(P_i) \sum_{P \in O(P_i, D_m)} P.$$

Θα πρέπει να διαλέξουμε τον D έτσι ώστε $\deg(D) \equiv 0 \bmod n^+(\beta)$. Θέτουμε $\lambda = \lambda(P_i) \equiv 1 \bmod n$. Μπορούμε να διαλέξουμε τον αριθμό τον τροχιών s και τον divisor $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$, κατά τέτοιο τρόπο

$$\deg(D) = 2 + ms \equiv 0 \bmod n^+(\beta),$$

αφού $(n^+(\beta), m) \mid 2$ (υπενθυμίζουμε ότι $(n,m)|\beta(b)+1$).

(3) Έχουμε ότι $A_R = \{P_{i,j}/i = 1,2\ j = 0,...,m-1\}$. Συνεπώς διαλέγουμε D με s το πλήθος τροχίες $O(P_i, D_m)$ όπου P_i δεν σταθεροποιείται από την D_m, και θέτοντας $\lambda(Q_i) \equiv 1 \bmod n$ υπολογίζουμε

$$\deg(D) = 2m + s2m.$$

Μπορούμε να διαλέξουμε το s κατάλληλα ώστε ο παραπάνω βαθμός να είναι $0 \bmod n$.

(4) Έχουμε $A_R = \emptyset$ και η υλοποίηση προκύπτει από το λήμμα 2.1.7. **(5)** Έχουμε $A_R = \{P_{1,0}, ..., P_{1,m-1}\}$. Παρατηρούμε ότι $\beta(b) \equiv 1 \bmod n$. Αναλύουμε το n σε $n^+(\beta(a)), n^-(\beta(a))$ όπως μας δίνονται από το λήμμα 2.2.8. Από την εξίσωση (2.14) έχουμε ότι $\deg(D) \equiv 0 \bmod p_i^{a_i}$ για $p_i \mid n^-(\beta(a))$ και για όλους τους divisors $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$. Οπότε μπορούμε να διαλέξουμε τον D έτσι ώστε

$$\deg D \equiv 0 \bmod n^+\left(\beta(a)\right).$$

Υπολογίζουμε

$$\deg D = m + 2ms \bmod n^+(\beta(a)), \tag{2.37}$$

Από την εξίσωση (2.37) καταλήγουμε στο ότι η συνθήκη $(n^+(\beta(a)), 2m) \mid m$, είναι αναγκαία για να είναι η περίπτωση 3 υλοποιήσιμη.

Περίπτωση Β Σε αυτή την περίπτωση η χαρακτηριστική του σώματος k είναι 2. Έχουμε ότι $G/C_n = D_m$, $(2,m) = 1$. Από τον χαρακτηρισμό των πεπερασμένων ομάδων αυτομορφισμών του ρητού σώματος συναρτήσεων, στο θεώρημα 2.2.1 έχουμε ότι οι δύο θέσεις p_1, p_2 του $F^G = F_0^{D_m}$ διακλαδίζονται στην επέκταση $F_0/F_0^{D_m}$, με δείκτες διακλάδωσης 2 και m, αντίστοιχα. Έστω $P_{1,i}$ $i = 1,...,m$ ($P_{2,j}$ $j = 1,2$ αντίστοιχα) το σύνολο των θέσεων του F_0 υπέρ της p_1 (p_2 αντίστοιχα).

Θεώρημα 2.2.13 *Έστω ότι η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με την διεδρική ομάδα D_m, $p \nmid m, p = 2$. Ξεχωρίζουμε τις παρακάτω περιπτώσεις για την δομή της ομάδας G:*

1. *$A_R \supset \{P_{1,i}\}_{0 \le i < m}$. Τότε η β είναι τετριμμένη και $G \cong C_n \times D_m$.*
2. *$A_R = \{P_{2,j}\}_{j=1,2}$. Τότε $G \cong C_{nm} \rtimes C_2$.*
3. *$A_R = \emptyset$. Τότε $G \cong C_n \rtimes D_m$.*

Απόδειξη:

1 $A_R \supset \{P_{1,i}\}_{0 \le i < m}$. Στην περίπτωση αυτή οι θέσεις $P_{1,i}$ $i = 1,...,m$ που επεκτείνουν την p_1 διακλαδίζονται στην επέκταση F/F_0. Παρατηρούμε ότι αν μία από αυτές, ας πούμε η P_{1,i_0}, διακλαδίζεται τότε όλες οι $P_{1,i}$ διακλαδίζονται επίσης, αφού οι επέκτασεις F/F_0 και F_0/F^G είναι και οι δύο Galois. Παρατηρούμε επίσεις ότι η ομάδα Galois $Gal(F/F_0^{\langle ba^i \rangle})$ της επέκτασης $F/F_0^{\langle ba^i \rangle}$ είναι μία επέκταση της ομάδας $\langle ba^i \rangle \cong C_2$. Από την μελέτη των επεκτάσεων στοιχειωδών αβελιανών ομάδων, έχουμε ότι $\beta(ba^i) \equiv 1 \bmod n$, για όλα τα $i = 0,...,m-1$, αφού η μοναδική σταθερή θέση του ba^i διακλαδίζεται στην F/F_0. Αυτό ισχύει για όλα τα i έτσι η ομάδα G είναι μία κεντρική επέκταση του D_m με C_n. Αφού $n \equiv 1 \bmod 2$ έχουμε ότι $H^2(D_m, C_n) = 1$, συνεπώς

$$G \cong C_n \times D_m.$$

2 $A_R = \{P_{2,j}\}_{j=1,2}$. Οι δύο θέσεις $P_{2,i}$ του F_0 υπέρ της p_2 διακλαδίζονται πλήρως στην F/F_0. $D_m(P_{2,i}) = \langle a \rangle$, έτσι από το πόρισμα (2.2.4) μπορούμε να βρούμε $S \in \pi^{-1}(a)$ η οποία να έχει τάξη nm. Η δράση του a στην $Gal(F/F_0) \cong \langle S^m \rangle$ είναι τετριμμένη δηλαδή $\beta(a) \equiv 1 \bmod n$. Έστω $R \in \pi^{-1}(b)$. Παρατηρούμε ότι $|G : \langle S \rangle| = 2$ οπότε $\langle S \rangle \lhd G$. Συνεπώς υπάρχει r τέτοιο ώστε,

$$RSR^{-1} = S^r.$$

Παρατηρούμε ότι η S^m γεννά την ομάδα $Gal(F/F_0) \cong C_n$, οπότε

$$S^{\beta(b)m} = RS^mR^{-1} = S^{mr},$$

συνεπώς

$$\beta(b) = r \bmod n. \tag{2.38}$$

Από την άλλη, έχουμε

$$RSR^{-1}S = S^{r+1} \Rightarrow 1 = \pi(RSR^{-1}S) = \pi(S^{r+1}),$$

οπότε

$$r \equiv -1 \bmod m \tag{2.39}$$

Το σύστημα των (2.38)(2.39) έχει μία λύση r αν και μόνο αν $(n,m)|\beta(b)+1$ και η ομάδα δίνεται από τις παρακάτω σχέσεις:

$$\langle R, S | R^2 = 1, S^{nm} = 1, RSR^{-1} = S^r \rangle.$$

Παρατηρούμε ότι η G είναι ισόμορφη με την

$$G \cong C_{nm} \rtimes C_2.$$

3 $A_R = \emptyset$. Σε αυτή την περίπτωση όλες οι θέσεις, $P_{1,i}$, $P_{2,j}$ του F_0 υπέρ της p_1 και της p_2 αντίστοιχα, αναλύονται στην F/F_0. Παρατηρούμε ότι $(n,2) = (m,2) = 1$. Θα χρησιμοποιήσουμε την εμφύτευση της πρότασης 2.2.2,

$$\begin{array}{rcl} H^2(D_m, C_n) = \bigoplus_{p|2m} H^2(D_m, C_n)_p & \longrightarrow & \bigoplus_{p|2m} H^2(H_p, C_n) \\ a = \sum a_p & \longmapsto & \sum res_{D_m \to H_p}(a_p) \end{array}.$$

Αφού $(n,2) = 1$ από το θεώρημα του Zassenhaus ([14], σελ. 163) έχουμε ότι $H^2(H_2, C_n) = 1$. Αν $p \neq 2$, $p|m$ τότε η p-Sylow υποομάδα H_p είναι υποομάδα της κυκλικής υποομάδας $\langle a \rangle \cong C_m$ της D_m. Αφού η $\langle a \rangle$ σταθεροποιεί την $P_{2,j}$, η οποία αναλύεται στην F/F_0, η υποεπέκταση

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(\langle a \rangle) \longrightarrow \langle a \rangle \longrightarrow 1,$$

διασπάται. Όλες οι υποεπεκτάσεις που αντιστοιχούν στις p-Sylow υποομάδες του $\langle a \rangle$ διασπώνται επίσης, άρα $H^2(H_p, C_n) = 1$ για $p \neq 2$. Αυτό μας δίνει ότι $H^2(D_m, C_n) = 1$ και τελικά έχουμε

$$G \cong C_n \rtimes D_m$$

όπου η δράση της D_m στο C_n καθορίζεται από την συνάρτηση β. □

Για να αποδείξουμε ότι αυτός ο τύπος διακλάδωσης είναι υλοποιήσιμος θα πρέπει να διαλέξουμε $D \in \mathcal{D}_n(G_0, A_R \subset A, \beta)$ βαθμού $0 \bmod n$.

1 Παίρνουμε s τροχιές $O(P_i, D_m)$, έτσι ώστε η θέση P_i να μην σταθεροποιείται από την D_m και θέτουμε $\lambda(P_i) \equiv 1 \bmod n$. Έχουμε $A_R = \{P_{1,1}, ..., P_{1,m}, P_{2,1}, P_{2,2}\}$ (ή $A_R = \{P_{1,1}, ..., P_{1,m}\}$ άρα ο βαθμός του D είναι

$$\deg D = m + 2 + 2ms \text{ ή } \deg D = m + 2ms.$$

Προφανώς, αφού $(2m, n) = (n, m)$ μπορούμε να βρούμε s έτσι ώστε $\deg D \equiv 0 \bmod n$ στην περίπτωση $A_R = \{P_{1,1}, ..., P_{1,m},\}$. Στην περίπτωση $A_R = \{P_{1,1}, ..., P_{1,m}, P_{2,1}, P_{2,2}\}$, βλέπουμε ότι $(n,m) \mid 2$ είναι αναγκαία συνθήκη ώστε να υλοποιήται αυτός ο τύπος διακλάδωσης. Παρατηρούμε ότι η συνθήκη $(n,m) \mid 2$ είναι ισοδύναμη με $(n,m) = 1$ αφού $(n,2) = (m,2) = 1$.

2 Από το λήμμα 2.1.6 αρκεί να κατασκευάσουμε D βαθμού $0 \bmod n^{+}(b)$. Παίρνουμε s τροχιές $O(P_i, D_m)$, όπου η P_i δεν σταθεροποιείται από τον D_m και θέτουμε $\lambda(P) \equiv 1 \bmod n$ για όλα τα P στο $\mathrm{supp}(D)$. Έχουμε

$$\deg(D) = 2 + 2ms \bmod n^{+}(b).$$

Μπορούμε να διαλέξουμε s τέτοιο ώστε $\deg(D) \equiv 0 \bmod n^{+}(b)$, αφού $(n,2) = (n^{+}(b), 2) = 1$.

3 Ο τύπος διακλάδωσης σε αυτή την περίπτωση υλοποιήται από το λήμμα 2.1.7, αφού $A_R = \emptyset$.

2.2.7 Η ομάδα A_4

Υποθέτουμε ότι $G/C_n \cong A_4$. Από το θεώρημα ταξινόμησης 2.2.1 έχουμε ότι τρεις θέσεις του $F_1 := F^G = F_0^{A_4}$ διακλαδίζονται στην F_0/F_1, οι p_1, p_2, p_3 με δείχτες διακλάδωσης $e_1 = 2, e_2 = e_3 = 3$ αντίστοιχα. Επιπλέον θα πρέπει η χαρακτηριστική $p \neq 2, 3$. Θα συμβολίζουμε με $P_{1,i}$ $i = 1, ..., 6$, $P_{2,j}, P_{3,j}$ $j = 1, ..., 4$ το σύνολο των θέσεων του F_0 που επεκτείνουν τις p_1, p_2, p_3, αντίστοιχα.

Η ομάδα A_4 δέχεται μία παράσταση σε γεννήτορες και σχέσεις

$$A_4 = \langle a, b / a^2 = b^3 = 1, (ab)^3 = 1 \rangle.$$

Παρατηρούμε επίσεις ότι η ομάδα A_4 έχει μία κανονική 2-Sylow υποομάδα ισόμορφη με την ομάδα V_4 του Klein, η οποία σαν υποομάδα της A_4 μπορεί γραφεί σε όρους των γεννητόρων της A_4

$$V_4 = \left\{1, a, bab^{-1}, b^2ab^{-2}\right\}.$$

Τέλος, η ομάδα A_4 μπορεί να γραφεί και ως ημιευθές γινόμενο $A_4 \cong V_4 \rtimes \langle b \rangle$. Ο ομομορφισμός δράσης

$$\beta : A_4 \longrightarrow \mathbb{Z}_n^*$$

δεν γίνεται να είναι μονομορφισμός, αφού η A_4 δεν είναι αβελιανή. Έχουμε δύο δυνατότητες για τον $\ker\beta$:

$$\ker\beta = V_4, \text{ ή } \ker\beta = A_4 \text{ (κεντρική επέκταση)}$$

Σε κάθε περίπτωση, αφού $A_4/V_4 \cong \mathbb{Z}_3$ και το a έχει τάξη δύο στην A_4, έχουμε ότι $\beta(a) \equiv 1 \bmod n$.

Θεώρημα 2.2.14 *Έστω ότι $G_0 = G/C_n \cong A_4$, τότε η ομάδα αυτομορφισμών G είναι ισόμορφη κατά περίπτωση με:*

a) $A_R = \emptyset$ τότε $G \cong C_n \rtimes A_4$.

b) $A_R = \{P_{2,j}\}_{1 \leq j \leq 4}$ τότε $G \cong V_4 \rtimes C_{3n}$.

c) $A_R = \{P_{1,i}\}_{1 \leq i \leq 6}$ τότε $G \cong G' \rtimes C_3$, όπου G' ορίζεται μέσω γεννητόρων και σχέσεων:

$$G' := \langle R, S / R^2 = S^2, S^{2n} = 1, RSR^{-1} = S^r \rangle.$$

d) $\{P_{1,i}\}_{i=1,...,6} \subsetneq A_R$ τότε η ομάδα G δέχεται την παρακάτω αναπαράσταση μέσω γεννητόρων και σχέσεων:

$$G = \langle R, S | R^{2n} = 1, R^2 = S^3, (RS)^3 = R^{2k} \rangle,$$

για κάποιο $k \in \{1, ..., n\}$.

Απόδειξη:

a) $A_R = \emptyset$. Όλες οι θέσεις του F_0 που επεκτείνουν τις p_1, p_2, p_3 αναλύονται στην επέκταση F/F_0. Σε αυτή την περίπτωση ισχυριζόμαστε ότι

$$G \cong C_n \rtimes A_4$$

όπου η δράση του A_4 επί της C_n καθορίζεται από την συνάρτηση β. Για να αποδείξουμε τον ισχυρισμό παρατηρούμε ότι η A_4 είναι το ημιευθύ γινόμενο $V_4 \rtimes \langle b \rangle$ και ότι η V_4 είναι στοιχειώδης αβελιανή ομάδα της μορφής $\mathcal{E}_2(2)$. Σύμφωνα με την μελέτη επεκτάσεων διεδρικών ομάδων, αφού οι σταθερές θέσεις της $V_4 = D_2$ αναλύονται, έχουμε ότι η υποεπέκταση

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(V_4) \longrightarrow V_4 \longrightarrow 1, \tag{2.40}$$

διασπάται, και από το λήμμα 2.2.7 έχουμε $G \cong C_n \rtimes A_4$.

b) $A_R = \{P_{2,j}\}_{1 \leq j \leq 4}$. Δηλαδή το σύνολο των σταθερών θέσεων $P_{1,i}$ $i = 1, ..., 6$ αναλύεται και τουλάχιστον μία από τις θέσεις $P_{2,j}, P_{3,j}$, ας πούμε η $P_{2,j}$ $j = 1, ..., 4$ διακλαδίζεται στην F/F_0. Σύμφωνα με το πόρισμα 2.2.4, αφού οι σταθερές θέσεις του b διακλαδίζονται, έχουμε ότι $\beta(b) \equiv 1 \bmod n$ άρα η επέκταση είναι κεντρική. Η ομάδα A_4 είναι ένα ημιευθύ γινόμενο $V_4 \rtimes \langle b \rangle$ και όπως και στην περίπτωση **a)** έχουμε ότι η μικρή ακριβής ακολουθία (2.40) διασπάται. Χρησιμοποιόντας το λήμμα 2.2.7 έχουμε ότι

$$G \cong V_4 \rtimes C_{3n},$$

όπου η δράση του γεννήτορα R της κυκλικής ομάδας C_{3n} στο $x \in V_4$ δίνεται από

$$x^R := R^n x R^{-n} = x^{\beta(R^n)}.$$

Το δεξί μέλος έχει νόημα αφού $R^n \in C_3 < A_4$. Παρατηρούμε ότι αν οι θέσεις $P_{3,j}$ $j = 0, ..., 4$ του F_0 δεν διακλαδίζονται, τότε από την παρατήρηση 2.1.5 έχουμε ότι $(n, 3) = 1$.

c) $A_R = \{P_{1,i}\}_{1 \leq i \leq 6}$. Στην περίπτωση αυτή οι θέσεις $P_{1,i}$ $i = 1, ..., 6$ διακλαδίζονται και οι θέσεις $P_{i,j}$ $i = 1, 2,$ $j = 1, ..., 4$ αναλύονται. Από την μελέτη των διεδρικών επεκτάσεων έχουμε ότι η ομάδα $G' := \pi^{-1}(V_4)$ γράφεται μέσω γεννητόρων και σχέσεων ως

$$G' = \langle R, S / R^2 = S^2, S^{2n} = 1, RSR^{-1} = S^r \rangle,$$

όπου r είναι η μοναδική λύση του συστήματος $r \equiv 1 \bmod n, r \equiv -1 \bmod 2$ αν $(n, 2) = 1$, και η μοναδική λύση του συστήματος $r \equiv 1 \bmod n, r \equiv -1 \bmod 2$ έτσι ώστε $\frac{r+1}{2}$ να είναι άρτιος, διαφορετικά. Παρατηρούμε επίσης ότι στην περίπτωση $(n, 2) = 2$ αυτός ο τύπος διακλάδωσης εμφανίζεται μόνο αν $n \equiv 2 \bmod 4$. Ισχυριζόμαστε ότι $G \cong G' \rtimes \langle b \rangle \cong G' \rtimes C_3$. Παρατηρούμε ότι $G' \lhd G$ αφού $V_4 \lhd A_4$. Από την άλλη, από το πόρισμα 2.2.4 έπεται ότι η υποεπέκταση

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(\langle b \rangle) \longrightarrow \langle b \rangle \longrightarrow 1 \tag{2.41}$$

διασπάται, συνεπώς υπάρχει ένας ομομορφισμός

$$j : \langle b \rangle \hookrightarrow C_n \rtimes \langle b \rangle \hookrightarrow G$$

τέτοιος ώστε $j(\langle b \rangle) \cap C_n = \{1\}$. Για να αποδείξουμε τον ισχυρισμό θα πρέπει να δείξουμε ότι $j(\langle b \rangle) \cap G' = 1$. Έστω $x \in j(\langle b \rangle) \cap G'$. Αν $x \neq 1$ τότε $x \in (\langle b \rangle)$ έχει τάξη 3. Τέλος παρατηρούμε ότι το τετράγωνο κάθε στοιχείου της G' ανήκει στην $\langle S \rangle$. Αυτό μας δίνει ότι για το x, που γράφεται στην μορφή $R^i S^j$, έχουμε $x^3 = x x^2 = R^i S^j S^k$ άρα $x \in \langle S \rangle$ και $x^2 \in C_n$. Αφού $j(\langle b \rangle) \cap C_n = \{1\}$ έχουμε $x^2 = 1$ και $x = 1$.

d) $\{P_{1,i}\}_{i=1,...,6} \subsetneq A_R$. Στην περίπτωση αυτή όλες οι θέσεις $P_{1,i}$ $i = 1, ..., 6$ και τουλάχιστον μία από τις $P_{2,j}$ και $P_{3,j}$ $j = 1, ..., 4$ διακλαδίζεται στην επέκταση F/F_0. (Υπενθυμίζουμε ότι οι θέσεις $P_{2,j}$ $P_{3,j}$ έχουν διαφορετικό τύπο διακλάδωσης αν και μόνο αν

$(3,n)=1$. Υποθέτουμε ότι η $P_{1,1}$ σταθεροποιείται από το a και ότι $P_{2,1}$σταθεροποιείται από το b. Χρησιμοποιώντας το πόρισμα 2.2.4 έχουμε ότι ο ομομορφισμός β είναι τετριμμένος και η επέκταση ομάδων είναι κεντρική. Επιπλέον υπάρχουν στοιχεία $R \in \pi^{-1}(a)$ και $S \in \pi^{-1}(b)$ τέτοια ώστε

$$\langle R \rangle \cong C_{2n}, \langle S \rangle \cong C_{3n}.$$

Η ομάδα $Gal(F/F_0) \cong C_n$ είναι κοινή υποομάδα των $\langle R \rangle, \langle S \rangle$ οπότε, διαλέγοντας κατάλληλους γεννήτορες R, S, έχουμε τις παρακάτω σχέσεις μεταξύ των R, S,

$$R^{2n} = 1, R^2 = S^3.$$

Συμβολίζουμε με π την προβολή $G \to G/C_n$. Αφού το $\pi(RS) = ab$ έχει τάξη 3 στην A_4 έχουμε και την επιπρόσθετη σχέση $(RS)^3 = R^{2k}$ μεταξύ των R, S. Ορίζουμε την ομάδα G_1

$$G_1 := \langle R, S | R^{2n} = 1, R^2 = S^3, (RS)^3 = R^{2k} \rangle. \tag{2.42}$$

Προφανώς $\langle R^2 \rangle$ είναι μία κανονική υποομάδα της G_1 και $G_1/\langle R^2 \rangle \cong A_4$ άρα $G_1 \cong G$. Θα αποδείξουμε ότι υπάρχει μόνο μία ομάδα με τον τύπο διακλάδωσης της περίπτωσης d), δηλαδή υπάρχει μόνο μία ομάδα που να ορίζεται από τις σχέσεις της (2.42). Δυστυχώς, δεν μπορέσαμε να βρούμε ένα τρόπο προσδιορισμού του k σε κλειστή μορφή. Με την βοήθεια του προγράμματος υπολογιστικής άλγεβρας MAGMA [18] υπολογίσαμε την τιμή του k για διαφορετικές τιμές του n:

n	2	3	5	6	7	9	10	11	13	14	15	17	18	19
k	1	1	5	1	6	7	5	8	9	6	10	11	7	12

Θα αποδείξουμε τώρα ότι υπάρχει μόνο μία ομάδα G με τον τύπο διακλάδωσης της περίπτωσης d. Αφού η επέκταση στην περίπτωση d) είναι κεντρική έχουμε

$$H^2(A_4, C_n) \cong \mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,3)}.$$

Θα μετρήσουμε το πλήθος $i(A_4, C_n)$ των μη ισομόρφων ομάδων G, που παίρνουμε επεκτείνοντας την ομάδα A_4 με C_n. Στην περίπτωση $(n,3) = (n,2) = 1$ από τον παραπάνω τύπο συνομολογίας έχουμε ότι η επέκταση διασπάται και η ομάδα G είναι ισόμορφη με την $C_n \times A_4$. Στην περίπτωση $(n,2) = 1$, $(n,3) = 3$ η υποεπέκταση

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(V_4) \longrightarrow V_4 \longrightarrow 1$$

διασπάται από το θεώρημα Zassenhaus , ([14], σελ. 162) και, σύμφωνα με το λήμμα 2.2.7, έχουμε δύο δυνατότητες για την δομή της G:

$$G \cong C_n \rtimes A_4 \text{ ή } G \cong V_4 \rtimes C_{3n}.$$

Στην περίπτωση $(n,2) = 2, (n,3) = 1$ έχουμε $H^2(A_4, C_n) \cong \mathbb{Z}_2$. Οι δύο ομάδες που εμφανίζονται είναι ισόμορφες με τις δύο ομάδες που βρήκαμε στην περίπτωση c).

Ας υποθέσουμε ότι $(n,2) = 2, (n,3) = 3$. Θα αποδείξουμε ότι το πλήθος των μη ισόμορφων κεντρικών επεκτάσεων της A_4 με C_n είναι $i(A_4, C_n) = 4$. Γράφουμε το $n = 2^a 3^b m$ με $(m,2) = (m,3) = 1$. Υπάρχουν μόνο δύο μη ισόμορφες επεκτάσεις G'_i $i = 1,2$ της μορφής

$$1 \longrightarrow C_{3^b m} \longrightarrow G'_i \longrightarrow A_4 \longrightarrow 1,$$

όπως δείξαμε στην περίπτωση $(n,2) = 1$, $(n,3) = 3$. Η ομάδα G δίνεται σαν μία επέκταση των G'_i, δηλαδή

$$1 \longrightarrow C_{2^a} \longrightarrow G \longrightarrow G'_i \longrightarrow 1.$$

Ισχυριζόμαστε ότι η G έχει δύο δυνατότητες για κάθε επιλογή των G'_i $i=1,2$. Πράγματι,

$$H^1(C_{3^b m}, C_{2^a}) = Hom(C_{3^b m}, C_{2^a}) \cong 0$$

συνεπώς η παρακάτω ακολουθία (restriction - inflation)

$$0 \longrightarrow H^2\left(\frac{G'_i}{C_{3^b m}}, C_{2^a}\right) \longrightarrow H^2(G'_i, C_{2^a}) \longrightarrow H^2(C_{3^b m}, C_{2^a}) \cong 0$$

είναι ακριβής, το οποίο μας δίνει ότι $H^2(G'_i, C_{2^a}) \cong \mathbb{Z}_2$ αφού

$$H^2\left(\frac{G'_i}{C_{3^b m}}, C_{2^a}\right) = H^2(A_4, C_{2^a}) \cong \mathbb{Z}_2.\Box$$

Προκειμένου να αποδείξουμε ότι ο τύπος διακλάδωσης είναι υλοποιήσιμος κατά περίπτωση θα πρέπει να βρούμε ένα divisor $D \in \mathcal{D}_n(A_4, A_R \subset A, \beta)$ βαθμού $0 \bmod n$.

a) Ο τύπος διακλάδωσης σε αυτή την περίπτωση υλοποιήται από το λήμμα 2.1.7.

b) Αν $A_R = \{P_{2,1}, ..., P_{2,4}, P_{3,1}, ..., P_{3,4}\}$ παίρνουμε s τροχιές $O(P_i, A_4)$ όπου P_i δεν σταθεροποιείται από την A_4 και θέτουμε $\lambda(P_i) \equiv 1 \bmod n$, $\lambda(P_{2,j}) \equiv -\lambda(P_{3,j}) \bmod n$. Έτσι $\deg(D) = 12s$ και μπορούμε να διαλέξουμε το πλήθος των τροχιών s κατά τέτοιο τρόπο ώστε $\deg(D) \equiv 0 \bmod n$. Αν $A_R = \{P_{2,1}, ..., P_{2,4}\}$ παίρνουμε s τροχιές $O(P_i, A_4)$ όπου P_i δεν σταθεροποιείται από την A_4 και θέτουμε $\lambda(P) \equiv 1 \bmod n$ για όλα τα $P \in \mathrm{supp}(D)$. Ο βαθμός του D είναι

$$\deg(D) = 4 + 12s.$$

Συνεπώς, αφού $(n,3) = 1$ έχουμε ότι $(n,12) \mid 4$, άρα μπορούμε να βρούμε s τέτοιο ώστε $D \equiv 0 \bmod n$.

c) Έχουμε $A_R = \{P_{1,1}, ..., P_{1,6}\}$. Έστω n_0 το κομμάτι του n για το οποίο

$$\beta(b) \equiv 1 \bmod n_0.$$

Από το λήμμα 2.1.6 είναι αρκετό να αποδείξουμε ότι $\deg(D) \equiv 0 \bmod n_0$. Παίρνουμε s το πλήθος τροχιές $O(P_i, A_4)$ όπου P_i δεν παραμένει σταθερό από την A_4 και θέτουμε $\lambda(P) \equiv 1 \bmod n$ για όλα τα $P \in \mathrm{supp}(D)$. Υπολογίζουμε ότι

$$\deg(D) = 6 + 12s.$$

Αφού $n \equiv 2 \bmod 4$ ή $n \equiv 1 \bmod 2$ έχουμε ότι $(n_0, 12) \mid 6$, συνεπώς μπορούμε να βρούμε ένα s τέτοιο ώστε $\deg(D) \equiv 0 \bmod n_0$.

d) $\{P_{1,i}\}_{i=1,\dots,6} \subsetneq A_R$. Επιλέγουμε s τροχιές $O(P_i, A_4)$ όπου P_i δεν σταθεροποιείται από την D_m. Αν

$$A_R = \{P_{1,1}, ..., P_{1,6}, P_{2,1}, ..., P_{2,4}\}$$

τότε θέτουμε $\lambda(P_{1,i}) \equiv 1 \bmod n$ για $i = 1, ..., 6$, $\lambda(P_{2,j}) \equiv -1 \bmod n$ για $j = 1, ..., 4$. Αν $A_R = \{P_{1,1}, ..., P_{1,6}, P_{2,1}, ..., P_{2,4}, P_{3,1}, ..., P_{3,4}\}$ τότε θέτουμε $\lambda(P_{1,i}) \equiv 1 \bmod n$ και $\lambda(P_{2,i}) \equiv -\lambda(P_{3,i}) \bmod n$ $i = 1, ..., 6$, $j = 1, ..., 4$. Οι βαθμοί των παραπάνω divisors είναι

$$\deg(D) = 2 + 12s \text{ και } \deg(D) = 6 + 12s.$$

Μπορούμε να πάρουμε το s έτσι ώστε $\deg(D) \equiv 0 \bmod n$. Πράγματι, όπως στις περιπτώσεις, b) και c) παρατηρούμε $n \equiv 2 \bmod 4$ ή $n \equiv 1 \bmod 2$ και, αν οι θέσεις $P_{3,1}, ..., P_{3,4}$ δεν διακλαδίζονται στην F/F_0 τότε $(n,3) = 1$ από την παρατήρηση 2.1.5

2.2.8 Η ομάδα A_5

Η ομάδα A_5 εμφανίζεται ως ομάδα αυτομορφισμών του ρητού σώματος συναρτήσεων με τους παρακάτω τύπους διακλάδωσης, τους οποίους θα χειριστούμε ταυτόχρονα:

α) Στην επέκταση $F_0/F_0^{A_5}$ τρεις θέσεις p_1, p_2, p_3 της $F_0^{A_5}$ διακλαδίζονται, με δείκτες διακλάδωσης $e_1 = 2, e_2 = 3, e_3 = 5$ αντίστοιχα. Για την χαρακτηριστική p θα πρέπει να υποθέσουμε ότι $p \neq 2, 3, 5$.

β) Στην επέκταση $F_0/F_0^{A_5}$ δύο θέσεις p_1, p_2 διακλαδίζονται με βαθμούς διακλάδωσης $e_1 = 6, e_2 = 5$ αντίστοιχα. Σε αυτή την περίπτωση η χαρακτηριστική $p = 3$.

Θεώρημα 2.2.15 *Ας υποθέσουμε ότι η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με την A_5. Η συνομολογιακή κλάση $\alpha \in H^2(A_5, C_n)$ που περιγράφει την G καθορίζεται από την συνομολογιακή κλάση που αντιστοιχεί στην υποεπέκταση μιάς 2-Sylow υποομάδας H_2.*

Στην περίπτωση που $(n, 2) = 1$ ή που όλες οι θέσεις του F_0 υπέρ του p_1 αναλύονται στην επέκταση F/F_0 τότε $G \cong C_n \times A_5$. Διαφορετικά η ομάδα G δέχεται μία παράσταση μέσω γεννητόρων και σχέσεων ως εξής:

$$\left\langle \begin{array}{l|l} X,Y,Z,T & T^n = X^3 = 1, Y^2 = T, Z^2 = T, (XY)^3 = T^l, (YZ)^3 = T^o, \\ & (XZ)^2 = T^m, XTX^{-1} = T, ZTZ^{-1} = T, YTY^{-1} = T \end{array} \right\rangle,$$

για κάποιους ακέραιους $m, l, o \in \{1, ..., n\}$.

Απόδειξη:

Η ομάδα A_5 είναι μία απλή μη αβελιανή ομάδα άρα ο ομομορφισμός δράσης

$$\beta : A_5 \longrightarrow \mathbb{Z}_n^*$$

είναι τετριμμένος και η επέκταση

$$1 \longrightarrow C_n \longrightarrow G \longrightarrow A_5 \longrightarrow 1 \tag{2.43}$$

κεντρική. Υπολογίσαμε ότι $H^2(A_5, C_n) \cong \mathbb{Z}_{(n,2)}$. Αν ο n είναι περιττός τότε

$$G \cong C_n \times A_5.$$

Υποθέτουμε τώρα ότι ο n είναι άρτιος. Από τη πρόταση (2.2.2) έχουμε ότι η συνάρτηση περιορισμού

$$\begin{array}{rcl} \mathbb{Z}_2 \cong H^2(A_5, C_n) = H^2(A_5, C_n)_{(2)} & \xrightarrow{1-1} & H^2(H_2, C_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ \alpha & \longmapsto & res_{A_5 \to H_2}(\alpha) \end{array} \tag{2.44}$$

όπου $H_2 \cong V_4$ είναι η 2-Sylow υποομάδα της A_5, είναι «1-1».

Θεωρούμε την επέκταση $F_0/F_0^{H_2}$ η οποία είναι βαθμού 4. Οι θέσεις του $F_0^{H_2}$ που διακλαδίζονται στην επέκταση $F_0/F_0^{H_2}$ βρίσκονται υπεράνω της θέσης p_1. Για να μελετήσουμε την ομάδα $\pi^{-1}(H_2)$ θα ξεχωρίσουμε τις παρακάτω περιπτώσεις: είτε όλες οι θέσεις F_0 υπέρ την p_1 αναλύονται στην επέκταση F/F_0, είτε όλες οι θέσεις του F_0 υπέρ της p_1 διακλαδίζονται στην F/F_0.

Στην πρώτη περίπτωση από την μελέτη των διεδρικών επεκτάσεων έχουμε $(H_2 \cong V_4 \cong D_2)$ και η συνομολογιακή κλάση $res_{A_5 \to H_2}(a)$ στην $H^2(H_2, C_n)$ είναι τετριμμένη, και αφού η συνάρτηση περιορισμού (2.44) είναι «1-1» η συνομολογιακή κλάση a είναι επίσης τετριμμένη. Άρα

$$G \cong C_n \times A_5.$$

Στην περίπτωση που όλες οι θέσεις του F_0 υπέρ της p_1 διακλαδίζονται στην F/F_0, απο την μελέτη των επεκτάσεων διεδρικών ομάδων, έχουμε ότι η περίπτωση αυτή μπορεί να εμφανιστεί μόνο όταν $n \equiv 2mod4$. Θα εκφράσουμε την ομάδα G μέσω γεννητόρων και σχέσεων. Είναι γνωστό [14] σελ. 138 ότι η ομάδα A_5 δέχεται την παρακάτω παράσταση μέσω γεννητόρων και σχέσεων:

$$A_5 = \langle x, y, z \mid x^3 = y^2 = z^2 = (xy)^3 = (yz)^3 = (xz)^2 \rangle. \tag{2.45}$$

Έστω T ένας γεννήτορας της κυκλικής ομάδας C_n. Η ομάδα ανάλυσης των θέσεων του F που επεκτείνουν την θέση p_1 έχει μία κυκλική υποομάδα τάξης $2n$. Έστω X, Y στοιχεία τάξης $2n$, τέτοια ώστε $\pi(X) = x$, $\pi(Y) = y$. Μπορούμε να επιλέξουμε τα X, Y έτσι ώστε $Y^2 = X^2 = T$. Εφαρμόζοντας την π στα γινόμενα των X, Y και χρησιμοποιόντας τις σχέσεις μεταξύ των γεννητόρων της A_5 όπως αυτές δίνονται στην (2.45) καταλήγουμε στην παρακάτω παράσταση της G:

$$\left\langle \begin{array}{ll} X, Y, Z, T \mid & T^n = X^3 = 1, Y^2 = T, Z^2 = T, (XY)^3 = T^l, (YZ)^3 = T^o, \\ & (XZ)^2 = T^m, XTX^{-1} = T, ZTZ^{-1} = T, YTY^{-1} = T \end{array} \right\rangle,$$

όπου $m, l, o \in \{1, ..., n\}$. Οι τιμές των ακέραιων m, l, o μπορούν να υπολογιστούν κάνοντας χρήση της παράστασης της $\pi^{-1}(V_4)$ μέσω γεννητόρων και σχέσεων. Η πραγματοποίηση αυτών των υπολογισμών είναι δύσκολη, και δεν μπορέσαμε να βρούμε ένα τρόπο να τις πραγματοποιήσουμε γενικά. Κάνοντας χρήση του προγράμματος υπολογιστικής άλγεβρας MAGMA [18] για συγκεκριμένες τιμές του n, μπορέσαμε να υπολογίσουμε «πειραματικά» ότι μπορούμε να επιλέξουμε $m = 1 = l = 1$ για $n = 2$ και $m = 1, o = 3, l = 2 + \frac{n-2}{4}$ για $n > 2$, $n \equiv 2 \bmod 4$. □

Έστω D ένας divisor στο σύνολο $\mathcal{D}_n(A_5, A_R \subset A, \beta)$

$$D = \sum_{i=1}^{3} a_i \sum_{P|p_i} P + \sum_{i=1}^{s} \lambda(P_i) \sum_{P \in O(P_i, A_5)} P$$

όπου $a_i = 0$ αν οι θέσεις p_i δεν ανήκουν στο A_R και $a_i = \lambda(P_{i,j})$ αν οι θέσεις του F_0 υπέρ της p_i ανήκουν στο A_R. Με $P_{i,j}$ θα συμβολίζουμε μια τυχαία θέση p_i. Ο βαθμός του D στην περίπτωση α) είναι

$$\deg(D) = a_1 30 + a_2 20 + a_3 12 + 60 \sum_{i=1}^{s} \lambda_i(P_i),$$

Αυτό μας δίνει ότι η συνθήκη

$$(60, n) \mid a_1 30 + a_2 20 + a_3 12,$$

είναι αναγκαία και ικανή για να εμφανίζεται αυτός ο τύπος διακλάδωσης. Ομοίως στην περίπτωση b) η συνθήκη

$$(60, n) \mid a_1 10 + a_2 12,$$

είναι αναγκαία και ικανή για να εμφανίζεται ο τύπος διακλάδωσης της περίπτωσης b).

2.2.9 Η ομάδα S_4

Υποθέτουμε ότι $G/C_n \cong S_4$. Η περίπτωση αυτή εμφανίζεται μόνο στις χαρακτηριστικές $p \neq 2, 3$. Στην επέκταση $F_0/F_0^{S_4}$ διακλαδίζονται τρεις θέσεις q_1, q_2, q_3 του σώματος F_0, με βαθμούς διακλάδωσης $e_1 = 2, e_2 = 3, e_3 = 4$. Έστω $\{P_{1,i}\}_{1 \leq i \leq 12}$, $\{P_{2,j}\}_{1 \leq j \leq 8}$, $\{P_{3,k}\}_{1 \leq k \leq 6}$ τα σύνολα των θέσεων του F_0 που βρίσκονται υπεράνω των q_1, q_2, q_3, αντίστοιχα. Η ομάδα S_4 δέχεται την παρακάτω παράσταση σε γεννήτορες και σχέσεις:

$$S_4 = \langle x, y \mid y^2, x^4, (x^{-1}y)^3 = 1 \rangle, \tag{2.46}$$

ενώ η A_4 είναι η υποομάδα της S_4 που παράγεται απο τα στοιχεία x^2, yx.

Ο τύπος διακλάδωσης της S_4 συγκρινόμενος με αυτόν της A_4 δίνεται από το παρακάτω διάγραμμα

$$\begin{array}{cccc}
F_0 & P_{1,1},...,P_{1,12} & P_{2,1},...,P_{2,8} & P_{3,1},...,P_{3,6} \\
| & \backslash / & {}_3\backslash /\ \backslash /_3 & \backslash /_2 \\
F_0^{A_4} & * & p_2\ \ p_3 & p_1 \\
| & |_2 & \backslash / & |_2 \\
F_0^{S_4} & q_1 & q_2 & q_3
\end{array}$$

Θεώρημα 2.2.16 *Έστω ότι η ομάδα $G/C_n = G_0$ είναι ισόμορφη με την συμμετρική ομάδα S_4. Διακρίνουμε τις παρακάτω περιπτώσεις για την ομάδα αυτομορφισμών της G.*
a) $\{P_{1,i}\}_{1\leq i\leq 12} \cup \{P_{3,k}\}_{1\leq k\leq 6} \subset A_R$. Η δράση της S_4 επί της C_n είναι τετριμμένη. Αν $(n,2) = 1$ τότε $G \cong C_n \times S_4$ ενώ αν $(n,2) = 2$, $n \equiv 2mod4$ τότε η ομάδα G δέχεται την παρακάτω παράσταση σε όρους γεννητόρων σχέσεων

$$G = \langle X, Y, T \mid T^n = 1, Y^2 = X^4 = XTX^{-1} = YTY^{-1} = T, (X^{-1}Y)^3 = T^k\rangle,$$

για κάποιο $k \in \{1, ..., n\}$.
b) $G \cong C_n \rtimes S_4$ σε όλες τις υπόλοιπες περιπτώσεις.

Απόδειξη: Η συνάρτηση Φ της πρότασης 2.2.2

$$\begin{array}{rcl}
H^2(S_4, C_n) = \bigoplus_{p=2,3} H^2(S_4, C_n)_{(p)} & \xrightarrow{\Phi} & H^2(H_2, C_n) \oplus H^2(H_3, C_n) \\
\alpha = \alpha_2 + \alpha_3 & \longmapsto & res_{S_4\to H_2}(\alpha_2) + res_{S_4\to H_3}(\alpha_3)
\end{array},$$

είναι ένα προς ένα, όπου H_2 (αντις. H_3) είναι οποιαδήποτε 2-Sylow υποομάδα (αντις. 3-Sylow). Θα αποδείξουμε το παρακάτω

Λήμμα 2.2.17 *Αν $G/C_n \cong S_4$, τότε η συνάρτηση:*

$$\begin{array}{rcl}
H^2(S_4, C_n) = & \longrightarrow & H^2(H_2, C_n) \\
\alpha = \alpha_2 + \alpha_3 & \longmapsto & res_{S_4\to H_2}(\alpha_2)
\end{array},$$

είναι επίσης ένα προς ένα.

Απόδειξη: Αν $A_R \supset \{P_{2,j}\}_{1\leq j\leq 8} \cup \{P_{3,k}\}_{1\leq k\leq 6}$ή $A_R \supset \{P_{1,i}\}_{1\leq i\leq 12}$ τότε η δράση της S_4 επί της C_n είναι τετριμμένη, συνεπώς $H^2(S_4, C_n) = \mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$. Αν $A_R \cap \{P_{2,j}\}_{1\leq j\leq 8} = \emptyset$ τότε από την μελέτη των επεκτάσεων κυκλικών ομάδων, έχουμε ότι $res_{S_4\to H_3}(\alpha) = 0$. Τέλος αν $A_R \supset \{P_{2,j}\}_{1\leq j\leq 8}$ ανδ $A_R \cap \{P_{3,k}\}_{1\leq k\leq 6} = \emptyset$, τότε απο την μελέτη της περίπτωσης b) στην μελέτη της A_4 έχουμε ότι $(n, 3) = 1$, και συνεπώς $H^2(H_3, C_n) = 0$. □

Αποδείξαμε ότι η δομή της ομάδας G καθορίζεται από την δομή της υποεπέκτασης

$$1 \longrightarrow C_n \longrightarrow \pi^{-1}(D_4) \longrightarrow D_4 \longrightarrow 1.$$

Θεωρούμε τον παρακάτω πύργο επεκτάσεων:

$$\begin{array}{cccc}
F_0 & P_{1,1},\quad ,P_{1,12} & P_{2,1},...,P_{2,8} & P_{3,1},\quad ,P_{3,6} \\
| & {}_2\backslash|\qquad |/ & \backslash / & {}_2\backslash|\qquad {}_4|/ \\
F_0^{D_4} & p_1'\qquad * & * & p_2'\qquad p_3' \\
{}_3| & {}_1\backslash /_2 & {}_3| & {}_2\backslash /_1 \\
F_0^{S_4} & q_1 & q_2 & q_3
\end{array}$$

Ο τύπος διακλάδςσης του q_2 στην επέκταση $F_0/F_0^{S_4}$ δεν επηρεάζει τον τύπο διακλάδωσης της επέκτασης $F_0/F_0^{D_4}$. Θα πρέπει να θεωρήσουμε τις παρακάτω περιπτώσεις:

1. $A_R \cap \{P_{1,i}\}_{1\leq i\leq 12} = \emptyset$ και $\{P_{3,k}\}_{1\leq k\leq 6} \subset A_R$ ή
$A_R \cap \{P_{3,k}\}_{1\leq k\leq 6} = \emptyset$ και $\{P_{1,i}\}_{1\leq i\leq 12} \subset A_R$.

Και στις δύο παραπάνω περιπτώσεις, η δράση της S_4 στην C_n είναι τετριμμένη. Επιπλέον το $y \in S_4$ σταθεροποιεί μια θέση του F_0 υπέρ του q_1 και μια θέση του F_0 υπέρ του q_3. Συνεπώς από την παρατήρηση 2.1.5 έχουμε ότι $(n, 2) = 1$. Δηλαδή η ομάδα συνομολογίας $H^2(S_4, C_n) = 0$, και $G \cong C_n \times S_4$.

2. $A_R \cap \{P_{1,i}\}_{1 \le i \le 12} = A_R \cap \{P_{3,k}\}_{1 \le k \le 6} = \emptyset$. Σε αυτή την περίπτωση από την μελέτη των επεκτάσεων διεδρικών ομάδων έχουμε $res_{S_4 \to D_4}(\alpha) = 0$, δηλαδή $\alpha = 0$ και $G \cong C_n \rtimes S_4$.

3. $\{P_{1,i}\}_{1 \le i \le 12} \cup \{P_{3,k}\}_{1 \le k \le 6} \subset A_R$. Σε αυτή την περίπτωση η δράση του S_4 επί της C_n είναι τετριμμένη. Συνεπώς αν $(n, 2) = 1$ τότε $G \cong C_n \times S_4$. Αν $(n, 2) = 2$ τότε από την μελέτη των επεκτάσεων διεδρικών ομάδων, η περίπτωση αυτή μπορεί να εμφανιστεί μόνο $n \equiv 2 mod 4$.

Έστω T γεννήτορας της κυκλικής ομάδας C_n. Θεωρούμε στοιχεία X, Y στο G τάξεων $4n$ και $2n$ αντίστοιχα, τέτοια ώστε $\pi(X) = x$ και $\pi(Y) = y$. Μπορούμε να διαλέξουμε τα X, Y κατά τέτοιο τρόπο ώστε $X^4 = T$ και $Y^2 = T$. Επιπλέον, έχουμε τις σχέσεις $XTX^{-1} = T$ και $YTY^{-1} = T$. Εφαρμόζοντας την π στα γινόμενα των X, Y και κάνοντας χρήση της παράστασης (2.46) καταλήγουμε στην παρακάτω παράσταση για την G:

$$G = \langle X, Y, T \mid T^n = 1, Y^2 = X^4 = XTX^{-1} = YTY^{-1} = T, (X^{-1}Y)^3 = T^k, \rangle,$$

για κάποιο $k \in \{1, ..., n\}$. Αν και η δομή της G μπορεί να προσδιορισθεί από την δομή της $\pi^{-1}(V_4)$ είναι πολύ δύσκολο να υπολογίσουμε την ακριβή τιμή του k γενικά. Κάνοντας χρήση του προγράμματος MAGMA [18] υπολογίσαμε το k για διάφορες τιμές του n, $n \equiv 2 \bmod 4$. Σε όλα τις τιμές του n που υπολογίσαμε $k = 2 + \frac{n-2}{4}$. □

Προκειμένου να αποδείξουμε ότι οι παραπάνω τύποι διακλάδωσης είναι υλοποιήσιμοι θα πρέπει να βρούμε ένα divisor $D \in \mathcal{D}_n(S_4, A_R \subset A, \beta)$ με $degD \equiv 0 \bmod n$. Όπως και στην περίπτωση της ομάδας A_5 καταλήγουμε στην παρακάτω συνθήκη

$$(n_0, 24) \mid a_1 12 + a_2 8 + a_3 6,$$

ως ικανή και αναγκαία συκνθήκη για $\deg(D) \equiv 0 \bmod n_0$, όπου $a_i = 0$ αν οι θέσεις $P_{i,j}$ του F_0 που επεκτείνουν το p_i δεν διακλαδίζονται στην επέκταση και $a_i = \lambda(P_{i,j}) \neq 0$,, διαφορετικά.

2.2.10 Οι ομάδες $PSL(2, q)$ και $PGL(2, q)$.

Στην περίπτωση αυτή η ομάδα $G_0 = G/C_n$ είναι ισόμορφη με την $PSL(2, q)$ ή με την $PGL(2, q)$. Στην επέκταση $F_0/F_0^{G_0}$ διακλαδίζονται μόνο δύο θέσεις p_1, p_2. Είναι αδύνατον να δωθεί μία γενική παράσταση της G μέσω γεννητόρων και σχέσεων αφού δεν υπάρχει όσον γνωρίζουμε, ανάλογη γενική παράσταση των ομάδων $PSL(2, q)$ και $PGL(2, q)$ σε όρους γεννητόρων σχέσεων.

Θα αποδείξουμε το παρακάτω:

Θεώρημα 2.2.18 *Έστω $G_0 = G/C_n$ ομάδα ισόμορφη με την $PSL(2, q)$ ή με την $PGL(2, q)$, όπου q είναι δύναμη της χαρακτηριστικής. Η συνομολογιακή κλάση $\alpha \in H^2(G_0, C_n)$ καθορίζεται από τον περιορισμό $res_{G_0 \to H_2}(\alpha)$ σε μία 2-Sylow υποομάδας H_2.*

Ιδιαίτερα, όταν $(n, 2) = 1$, ή όταν οι θέσεις του F_0 που επεκτείνουν τις p_1, p_2 αναλύονται στην επέκταση F/F_0 τότε $G \cong C_n \rtimes G_0$.

Απόδειξη: Θα αποδείξουμε πρώτα το παρακάτω

Λήμμα 2.2.19 *Για $G_0 = PSL(2, q), PGL(2, q)$, η ομάδα $H^2(G_0, C_n)$ είναι μία 2-ομάδα.*

Απόδειξη: Ξεχωρίζουμε τις παρακάτω δύο περιπτώσεις:
Περίπτωση 1. $G_0 = PSL(2, q)$, $(q, 2) = 1$ ή $G_0 = PGL(2, 2^f) = PSL(2, 2^f)$.

Αφού $PSL(2, q)$, όπου $q = p^f$ είναι δύναμη της χαρακτηριστικής, είναι απλή ομάδα, η δράση της G_0 επί της C_n είναι τετριμμένη.

Υπολογίσαμε ότι

$$H^2(PSL(2,q),C_n) \cong \begin{cases} \mathbb{Z}_{(2,n)} & \text{αν} \quad p^f \neq 9 \\ \mathbb{Z}_{(6,n)} & \text{αν} \quad p^f = 9 \end{cases}.$$

Παρατηρούμε ότι αν $p^f = 9$ τότε $(n,6) = (n,2)$ αφού υποθέσαμε ότι η χαρακτηριστική p δεν διαιρεί το n, συνεπώς $H^2(PSL(2,q),C_n) = \mathbb{Z}_{(2,n)}$.

Περίπτωση 2. $G_0 = PGL(2,q)$, $(q,2)=1$. Ο πυρήνας του ομομορφισμού δράσης

$$\beta : PGL(2,q) \longrightarrow \mathbb{Z}_n^*$$

είναι ή $\ker\beta = PGL(2,q)$ ή $\ker\beta = PSL(2,q)$. Στην πρώτη περίπτωση η επέκταση είναι κεντρική και $H^2(PGL(2,q),C_n) = \mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,2)}$. Παρατηρούμε ότι

$$H^1(PSL(2,q),C_n) \cong Hom(PSL(2,q),C_n) = 0,$$

αφού η $PSL(2,q)$ είναι απλή και μη αβελιανή. Γράφουμε την ακολουθία inflation-restriction

$$0 \longrightarrow H^2\left(\frac{PGL(2,q)}{PSL(2,q)}, C_n\right) \longrightarrow H^2(PGL(2,q),C_n) \longrightarrow H^2(PSL(2,q),C_n) \cong \mathbb{Z}_{(2,n)}$$

και αφού $PGL(2,q)/PSL(2,q) \cong \mathbb{Z}_2$ έχουμε ότι $H^2(PGL(2,q),C_n)$ είναι μία 2-ομάδα. $\square$

Επιστρέφουμε στην απόδειξη του 2.2.18. Ο μονομορφισμός Φ της πρότασης 2.2.2

$$H^2(G_0,C_n) = \bigoplus_{t|q(q^2-1)} H^2(PGL(2,q),C_n)_{(t)} \xrightarrow{\Phi} \bigoplus_{t-Sylow} H^2(H_t,C_n)$$

όπου η H_t διατρέχει τις t-Sylow υποομάδες της G_0 είναι ένα προς ένα και συνεπώς η συνάρτηση περιορισμού

$$\begin{array}{rcl} H^2(G_0,C_n) & \longrightarrow & H^2(H_2,C_n) \\ \alpha & \longmapsto & \beta = res_{G_0 \to H_2}(\alpha) \end{array}$$

είναι επίσης ένα προς ένα. Η 2-Sylow υποομάδα H_2 είναι ισόμορφη με μία διεδρική ομάδα D_{2^K}, τάξης 2^{K+1}, όπου $K = \max\{v_2(e_1), v_2(e_2)\}$.

Επιπλέον αν $(n,2)=2$ τότε η ομάδα συνομολογίας μηδενίζεται, συνεπώς $G \cong C_n \rtimes G_0$, ενώ από την μελέτη των επεκτάσεων των διεδρικών ομάδων έχουμε ότι αν όλες οι θέσεις του F_0 υπεράνω των p_1, p_2 αναλύονται στην επέκταση F/F_0, τότε $\beta = res_{G_0 \to H_2}(\alpha) = 1$, συνεπώς $G \cong C_n \rtimes G_0$ επίσης. $\square$

Έστω D ένας divisor στο $\mathcal{D}_n(G_0, A_R \subset A, \beta)$, και n_0 ο μεγαλύτερος διαιρέτης του n, τέτοιος ώστε $\beta(\sigma) \equiv 1 \bmod n_0$. Σύμφωνα με το λήμμα 2.1.7 έχουμε ότι $\deg(D) \equiv 0 \bmod n \Leftrightarrow \deg(D) \equiv 0 \bmod n_0$. Συνεπώς η παρακάτω συνθήκη

$$(n_0, q(q-1)(q+1)) \mid a_1 q(q-1) + a_2(q+1)$$

είναι ικανή και αναγκαία για να έχουμε $\deg(D) \equiv 0 \bmod n_0$, όπου $a_i = 0$ αν οι θέσεις του F_0 υπεράνω των p_i ανήκουν στο A_R και $a_i = \lambda(P)$, $P \mid p_i$ διαφορετικά.

Κεφάλαιο 3

$x^n + y^m + 1 = 0$

3.1 Η περίπτωση $n = m$

Η περίπτωση αυτή μελετήθηκε στις αρχές της δεκαετίας του 70 από τον Leopold, αλλά δημοσιεύτηκε πρόσφατα. Η δε περίπτωση $n = q - 1$, όπου q είναι δύναμη της χαρακτηριστικής του σώματος είναι ιδιαίτερα ενδιαφέρουσα, αφού τα σώματα συναρτήσεων αυτών των καμπύλων είναι αμφίρητα ισοδύναμα με τα σώματα συναρτήσεων του Hermit, σώματα με υπερβολικά μεγάλο πλήθος αυτομορφισμών σε σχέση με το γένος τους, και μέγιστα όσων αφορά το πλήθος των $\mathbb{F}_q$ ρητών σημείων τους.

Ο Leopold απόδειξε ότι η ομάδα αυτομορφισμών G των σωμάτων συναρτήσεων των καμπύλων Fermat είναι ισόμορφη προς

$$G \cong \begin{cases} \mu(n)^2 \rtimes S_3 & \text{αν} \quad n - 1 \neq q \\ PGU(3, q^2) & \text{αν} \quad n - 1 = q \end{cases}$$

3.2 Η περίπτωση $n \neq m$

Στα επόμενα θα συμβολίζουμε με $F_{n,m}$ το σώμα συναρτήσεων μίας αλγεβρικής καμπύλης της μορφής $x^n + y^m + 1 = 0$, ορισμένης υπέρ το αλγεβρικά κλειστό σώμα k χαρακτηριστικής $p \geq 0$.

Παρατηρούμε ότι το σώμα $F_{n,m}$ αποτελεί κυκλική επέκταση του Kummer των σωμάτων $k(x)$ και $k(y)$. Έστω $P_{(x=a)}, (P_{(y=b)}$ αντίστοιχα) οι θέση του $k(x)$, ($k(y)$ αντίστοιχα) που αντιστοιχεί στο σημείο $x = a$,($y = b$ αντίστοιχα) του $\mathbb{P}^1(k)$. Θα συμβολίζουμε με v_p την εκτίμηση του $k(x)$ που αντιστοιχεί στην θέση P.

$$v_P(x^n + 1) = v_P\left(\prod_{i=1}^{n}(x - \zeta_i)\right) = \begin{cases} 1 & \text{αν} \quad P = P_{(x=\zeta_i)} \\ -n & \text{αν} \quad P = P_{(x=\infty)} \\ 0 & \quad\quad \text{διαφορετικά} \end{cases}$$

συνεπώς ο αριθμός r_P των θέσεων υπεράνω της P και οι αντίστοιχοι βαθμοί διακλάδωσης e_p υπολογίζονται:

$$r_P = \begin{cases} 1 & \text{αν} \quad P = P_{(x=\zeta_i)} \\ (n, m) & \text{αν} \quad P = P_{(x=\infty)} \\ m & \quad\quad \text{διαφορετικά} \end{cases} \qquad e_P = \begin{cases} m & \text{αν} \quad P = P_{(x=\zeta_i)} \\ \frac{m}{(n,m)} & \text{αν} \quad P = P_{(x=\infty)} \\ 1 & \quad\quad \text{διαφορετικά} \end{cases}$$

όπου $(\zeta_i)_{i=1,\ldots,n}$ είναι οι n-οστές ρίζες του -1. Εξ αιτίας της συμμετρίας ανάμεσα στα m

και n έχουμε:

$$r_P = \begin{cases} 1 & \text{αν} \quad P = P_{(y=\epsilon_j)} \\ (n,m) & \text{αν} \quad P = P_{(y=\infty)} \\ n & \qquad \text{διαφορετικά} \end{cases} \qquad e_P = \begin{cases} n & \text{αν} \quad P_{(y=\epsilon_j)} \\ \frac{n}{(n,m)} & \text{αν} \quad P_{(y=\infty)} \\ 1 & \qquad \text{διαφορετικά} \end{cases}$$

όπου $(\epsilon_j)_{j=1,\dots,m}$ είναι οι m-οστές ρίζες του -1. Οι κύριοι divisors των δύο γενοποιών συναρτήσεων x, y του σώματος $F_{n,m}$ είναι:

$$(x) = P_{(x=0)} - P_{(x=\infty)} = \sum_{i=1}^{m} \alpha_i - \frac{m}{(n,m)} \sum_{j=1}^{(n,m)} \gamma_j$$

$$(y) = P_{(y=0)} - P_{(y=\infty)} = \sum_{i=1}^{n} \beta_i - \frac{n}{(n,m)} \sum_{j=1}^{(n,m)} \delta_j,$$

όπου $\alpha_i, \gamma_j, \beta_i, \delta_j$ είναι οι επεκτάσεις, στο σώμα $F_{n,m}$, των θέσεων $P_{(x=0)}, P_{(x=\infty)} \in k(x)$ και $P_{(y=0)}, P_{(y=\infty)} \in k(y)$ αντίστοιχα. Υπολογίσαμε επίσεις ότι μία βάση του χώρου των ολόμορφων διαφορικών είναι η

$$x^i y^j \ \omega, \ \ (i,j) \in I.$$

όπου I είναι το σύνολο των δεικτών:

$$I := \left\{ (i,j) \in \ \mathbb{N}^2 : \frac{2g-2}{(n,m)} - \frac{im+nj}{(n,m)} \geq 0 \right\}. \tag{3.1}$$

και

$$\omega := \frac{dx}{my^{m-1}} = -\frac{dy}{nx^{n-1}}.$$

3.3 Υπολογισμός ημιομάδων του Weierstrass

Ορίζουμε για μία θέση P την ημιομάδα του Weierstrass

$$E(P) := \{\nu \in \mathbb{N} : \exists f \in F_{n,m}/(f)_\infty = \nu P\}.$$

Τα στοιχεία του $E(P)$ ονομάζονται πολικοί αριθμοί στο P και τα στοιχεία του $\mathbb{N} \backslash E(P)$ ονομάζονται πηδήματα στο P. Για κάθε divisor D του σώματος συναρτήσεων $F_{n,m}$ ορίζουμε τον πεπερασμένης διάστασης k διανυσματικό χώρο $\mathcal{L}(D) := \{f : (f) + D \geq 0\}$. Θέτουμε $\ell(D) := \dim_k \mathcal{L}(D)$. Παρατηρούμε ότι $s \in E(P)$ αν και μόνο αν $\ell(sP) = \ell((s-1)P) + 1$.

Σκοπός αυτής της παραγράφου είναι ο υπολογισμός ενός κομματιού του συνόλου $E(P)$ για τις θέσεις $P = \alpha_1$ ή β_1. Παρατηρούμε ότι οι θέσεις α_s, $s = 1, ..., m$, β_t, $t = 1, ..., n$ έχουν την ίδια ημιομάδα του Weierstrass. Τα σύνολα

$$x^i y_1^j \omega \text{ ή } x_1^i y^j \omega \ \ (i,j) \in I,$$

όπου $x_1 = x - \zeta_1$, $y_1 = y - \epsilon_1$, είναι επίσης βάσεις του χώρου των ολόμορφων διαφορικών. Επιπλέον ισχύει ότι:

$$v_{\alpha_1}(x^i y_1^j \omega) = i + nj, \quad v_{\beta_1}(x_1^i y^j \omega) = mi + j.$$

Από το θεώρημα Riemann-Roch έχουμε ότι

$$s \in E(P) \Leftrightarrow \ell(sP) = \ell((s-1)P) + 1 \Leftrightarrow \ell(W - (s-1)P) - \ell(W - sP) = 0,$$

όπου W είναι ένας κανονικός divisor του σώματος $F_{n,m}$. Διαλέγουμε για W τον divisor του ω. Η διάσταση του χώρου $\mathcal{L}(W - sP)$ μπορεί να θεαθεί σαν το πλήθος των γραμμικώς ανεξαρτήτων ολομόρφων διαφορικών που έχουν ρίζα στην θέση P τάξης $\geq s$, αφού

$$\mathcal{L}(W - sP) := \{f : (f) \geq -(\omega) + sP\} = \{(f\omega) \geq sP\}.$$

Από την άλλη, αφού 3.1) έχουμε $0 \leq i < n$ και $0 \leq j < m$, για $(i, j) \in I$, το οποίο αποδεικνύει ότι οι συναρτήσεις

$$\Phi_n : \left\{ \begin{array}{ccc} I & \longrightarrow & \mathbb{N} \\ (i,j) & \longmapsto & i + nj + 1 \end{array} \right. \quad \Psi_m : \left\{ \begin{array}{ccc} I & \longrightarrow & \mathbb{N} \\ (i,j) & \longmapsto & mi + j + 1 \end{array} \right.$$

είναι «ένα προς ένα». Συνεπώς οι εκτιμήσεις $v_{a_1}(x^i y_1^j \omega)$ παίρνουν διαφορετικές τιμές για διαφορετικά (i, j) και το ίδιο ισχύει και για τις εκτιμήσεις $v_{\beta_1}(x_1^i y^j \omega)$, άρα η εκτίμηση ενός ολόμορφου διαφορικού είναι

$$v_{a_1}\left\{\sum_{(i,j)\in I} \lambda_{i,j} x_1^i y^j \omega\right\} = \min_{\lambda_{i,j}\neq 0} v_{a_1}(\lambda_{i,j} x_1^i y^j \omega) = \min_{(i,j) \text{ τέτοια ώστε } \lambda_{i,j}\neq 0} \{i + nj\}.$$

Άρα

$$\ell(W - s\alpha_1) = |\{i + nj \geq s, (i, j) \in I\}|$$

και ομοίως

$$\ell(W - s\,\beta_1) = |\{mi + j \geq s, (i, j) \in I\}|$$

Συμπερένουμε ότι $\ell(W-(s-1)\alpha_1) \neq \ell(W-s\alpha_1)$ αν και μόνο αν υπάρχει $(i, j) \in I : i+nj = s-1$. Ο πληθάριθμος του συνόλου $\{i + nj + 1, (i, j) \in I\} = \Phi_n(I)$ είναι g, άρα τα πηδήματα στην θέση α_1 είναι $\Phi_n(I)$. Ομοίως τα πηδήματα στην θέση β_1 είναι $\Psi_n(I)$.

Για τις ανάγκες μας είναι αρκετή η μελέτη ενός μικρού μόνο μέρους της ημιομάδας του Weierstrass. Θα περιοριστούμε στην μελέτη των πηδημάτων στην θέση α_1 τα οποία είναι εικόνες, της συνάρτησης Φ_n, του συνόλου $I_1 = \{(i, 0) \in I\}$. Σύμφωνα με την εξίσωση (3.1) το $(i, 0) \in I_1$ αν και μόνο αν

$$i \leq n - 1 - \frac{n + (n,m)}{m}. \tag{3.2}$$

Διαιρούμε το $n + (n,m)$ με m : $n + (n,m) = \kappa m + r$, όπου $0 \leq r < m$. Αν θέσουμε

$$t := \left\{ \begin{array}{lll} n-\kappa & \text{όταν} & r = 0 \\ n-\kappa-1 & \text{όταν} & r > 0 \end{array} \right. ,$$

τότε από την (3.2) έχουμε ότι $i \leq t - 1$. Επιπλέον $n + 1 = \Phi_n((0, 1))$ είναι ένα πήδημα για την θέση a_1. Τέλος, η δομή των πολικών αριθμών και των πηδημάτων στο α_1 μέχρι το $n+1$ είναι:

$$0,\ \underbrace{1,\ \ 2, \ldots.\ t}_{\text{πηδήματα}},\ \ \underbrace{t+1,\ \ \ldots\ldots\ n}_{\text{πολικοί αριθμοί}},\ \ \underbrace{n+1}_{\text{πήδημα}}, \ldots. \tag{3.3}$$

Ομοίως για την θέση $P = \beta_1$ υπολογίζουμε το κομμάτι του $E(\beta_1)$ το οποίο είναι της μορφής $\Psi_n((0, j))$, $(0, j) \in I$. Διαιρούμε το $m+(n,m)$ με n: $m+(n,m) = \lambda n+\upsilon, 0 \leq \upsilon < n$. Αφού $m < n$, το λ πρέπει να είναι μηδέν η ένα. Όπως και στην μελέτη του $E(\alpha_1)$ αν θέσουμε

$$t' := \left\{ \begin{array}{lll} m-\lambda & \text{όταν} & \upsilon\ = 0 \\ m-\lambda-1 & \text{όταν} & \upsilon\ > 0 \end{array} \right.$$

τότε $j \leq t' - 1$. Παρατηρούμε ότι $\lambda = 1$ αν και μόνο αν $\upsilon\ = 0$, συνεπώς $t' + 1 = m$ και η δομή της ημιομάδας του Weierstrass στην θέση β_1, μέχρι το $m + 1$ είναι:

$$0,\ \ \underbrace{1,\ \ 2,\ \ \ \ldots.. ,\ m-1}_{\text{πηδήματα}},\ \ \ \ \underbrace{m}_{\text{πολικός αριθμός}}\ \ ,\ \ \underbrace{m+1}_{\text{πήδημα}}, \ldots. \tag{3.4}$$

Λήμμα 3.3.1 *Έστω $n = m\kappa_1 + r_1, 0 \leq r_1 < m$, η διαίρεση του n με m. Ο αριθμός t ισούτε με $n - \kappa_1 - 1$. Επιπλέον αν $m + 1 < n$ τότε $m < t + 1$. Στην περίπτωση $m + 1 = n$ έχουμε $m = t + 1$.*

Απόδειξη: Θα εξετάσουμε δύο περιπτώσεις:

1. $m|n$ άρα $(n, m) = m$. Αυτό σημαίνει ότι $\kappa = \kappa_1 + 1$ και $r = 0$, συνεπώς $t = n - \kappa_1 - 1$.
2. $m \nmid n$ άρα $(n, m) < m$. Προφανώς
$$n + (n, m) = \kappa_1 m + r_1 + (n, m).$$
Διαχωρίζουμε τις παρακάτω υποπεριπτώσεις:
   - Αν $r_1 + (n, m) = m$, τότε $\kappa = \kappa_1 + 1, r = 0$ και συνεπώς $t = n - \kappa_1 - 1$.
   - Αν $r_1 + (n, m) < m$, τότε $\kappa = \kappa_1, r > 0$ και συνεπώς $t = n - \kappa_1 - 1$.
   - Η περίπτωση $r_1 + (n, m) > m$ δεν μπορεί να συμβεί αφού $(n, m)|r_1$.

Τελικά η ανισότητα $m < t + 1$ είναι ισοδύναμη με την $\frac{m-r_1}{m-1} < \kappa_1$, αφού $m > 1$. Το αριστερό μέρος της παραπάνω ανισότητας είναι μικρότερο της μονάδας εκτός αν $r_1 = 0, 1$. Συνεπώς $\frac{m-r_1}{m-1} \geq \kappa_1$ μόνο αν $\kappa_1 = 1$ και $r_1 = 0, 1$ ($n > m$ άρα $\kappa_1 \geq 1$). Άρα η ισότητα $t + 1 = m$ ισχύει αν και μόνο αν $n = m + 1$.□

Λήμμα 3.3.2 *Δεν υπάρχει αυτομορφισμός σ τέτοιος ώστε: $\sigma(\alpha_i) = \beta_j$.*

Απόδειξη: Για κάθε θέση P και για κάθε αυτομορφισμό $\sigma \in G$ $E(P) = E(\sigma P)$. Προκειμένου να αποδείξουμε τον παραπάνω ισχυρισμό παρατηρούμε ότι $E(\alpha_1) \neq E(\beta_1)$. Πράγματι, $m \in E(\beta_1)$ και αν $m + 1 < n$ τότε από το λήμμα 3.3.1 $m < t + 1$ άρα $m \notin E(\alpha_1)$. Στην περίπτωση που $m + 1 = n$, $n \notin E(\beta_1)$ άλλα $n \in E(\alpha_1)$.□

Λήμμα 3.3.3 *Αν P είναι μια θέση του $F_{n,m}$ και*
$$P \notin \left\{\{\alpha_i\}_{i=1,\dots,m} \cup \{\beta_j\}_{j=1,\dots,n} \cup \{\gamma_k\}_{k=1,\dots,(n,m)}\right\}$$
τότε για κάθε αυτομορφισμό $\sigma \in Aut(F_{n,m})$ ισχύει ότι $\sigma(P) \notin \{\beta_j\}_{j=1,\dots,n}$.

Απόδειξη: Θα αποδείξουμε ότι $E(P) \neq E(\beta_j)$. Για αυτό θα δουλέψουμε με τον χώρο των γραμμικών μορφών $\mathcal{L}(W)^*$ δηλαδή με τις μορφές
$$\Phi : \mathcal{L}(W) \longrightarrow k.$$
Η θέση P περιορίζεται στις πεπερασμένες θέσεις $P_{(x=a)}, P_{(y=b)}$ των σωμάτων συναρτήσεων $k(x), k(y)$ αντιστοίχως. Θέτουμε $\tilde{x} := x - a, \quad \tilde{y} := y - b$. Το σύνολο $\{\tilde{x}^i\tilde{y}^j\omega, (i, j) \in I\}$ σχηματίζει μία βάση του χώρου των ολόμορφων διαφορικών, άρα κάθε ολόμορφο διαφορικό ω_1 μπορεί να γραφεί σαν:
$$\omega_1 = \sum_{(i,j)\in I} \gamma_{i,j}\tilde{x}^i\tilde{y}^j\omega, \qquad \gamma_{i,j} \in k.$$
Έστω T μία τοπική παράμετρος του δακτυλίου εκτίμησης στην θέση P. Οι συναρτήσεις $\tilde{x}, \tilde{y}$ μπορούν να εκφραστούν σαν τυπικές δυναμοσειρές του T:
$$\tilde{x} = \sum_{k\geq 1} a_k T^k \ , \ \ \tilde{y} = \sum_{l\geq 1} b_l T^l.$$

Επιπλέον, αφού η θέση P δεν διακλαδίζεται σε καμία επέκταση $F_{n,m}/k(x), F_{n,m}/k(y)$ έχουμε ότι $a_1 b_1 \neq 0$. Οι s δυνάμεις των δυναμοσειρών $\tilde{x}, \tilde{y}$ συμβολίζονται με:

$$\tilde{x}^s = \sum_{k\geq 1} a_k^{(s)} T^k, \quad \tilde{y}^s = \sum_{l\geq 1} b_l^{(s)} T^l.$$

Από τον νόμο πολλαπλασιασμού δυναμοσειρών υπολογίζουμε:

$$\left\{ \begin{array}{lll} a_k^{(s)} = b_k^{(s)} = 0, & \text{αν} & k < s \neq 0 \\ a_s^{(s)} = a_1^s, b_s^{(s)} = b_1^s, & \text{αν} & k = s \neq 0 \end{array} \right. \qquad \left\{ \begin{array}{lll} a_k^{(0)} = b_k^{(0)} = 1 & \text{αν} & k = 0 \\ a_k^{(0)} = b_k^{(0)} = 0 & \text{αν} & k > 0 \end{array} \right. \tag{3.5}$$

Ορίζουμε τις γραμμικές μορφές:

$$\Phi^{(s)} := \left\{ \begin{array}{ccc} \mathcal{L}(W) & \longrightarrow & k \\ \omega_1 & \longmapsto & \langle \omega_1, \Phi^{(s)} \rangle := \sum_{(i,j)\in I} \gamma_{i,j} \phi_{i,j}^{(s)} \end{array} \right.$$

όπου

$$\phi_{i,j}^{(s)} := \sum_{k+l=s} a_k^{(i)} b_l^{(j)}, \qquad (i,j) \in I, \tag{3.6}$$

Το τυχαίο ολόμορφο διαφορικό γράφεται:

$$\omega_1 = \left(\sum_{s\geq 0} \langle \omega_1, \Phi^{(s)} \rangle T^s \right) \omega.$$

Από την επιλογή της θέσης P έχουμε ότι $P \nmid (\omega)$ άρα ο διανυσματικός χώρος $\mathcal{L}(W - sP)$ χαρακτηρίζεται από τις εξισώσεις: $0 = \langle \omega, \Phi^{(s_1)} \rangle, \forall\, 0 \leq s_1 \leq s-1$. Είναι σαφές ότι:

$$\mathcal{L}(W - s_1 P) = Ker\Phi^{(s_1-1)}|_{\mathcal{L}(W-(s_1-1)P)} < \mathcal{L}(W - (s_1 - 1)P).$$

Άρα $\mathcal{L}(W - (s-1)P) \neq \mathcal{L}(W - sP)$ αν και μόνο αν $\Phi^{(s-1)}$ είναι γραμμικά ανεξάρτητη από τις μορφές $\Phi^{(s_1)}$, $0 \leq s_1 \leq s-2$, συνεπώς:

$$s \in E(P) \Leftrightarrow \exists \xi_0, ..., \xi_{s-2} : \Phi^{(s-1)} = \sum_{k=0}^{s-2} \xi_k \Phi^{(k)}.$$

Παρατηρούμε ότι κάθε γραμμική μορφή $\Phi^{(s)}$ αντιστοιχεί σε ένα $1 \times g$ πίνακα, τον

$$\Phi^{(s)} \leftrightarrow (\phi_{(0,0)}^{(s)}, \phi_{(1,0)}^{(s)}, ..., \phi_{(t-1,0)}^{(s)}, ..., \phi_{(i,j)}^{(s)}, ...) \qquad (i,j) \in I$$

Από τις (3.6) και (3.5) έχουμε ότι

$$\phi_{i,0}^{(s)} = \sum_{k+l=s} = a_k^{(i)} b_l^{(0)} = a_s^{(i)},$$

άρα το αριστερό επάνω κομάτι του πίνακα των πρώτων $t-1$ μορφών είναι

	$(0,0)$	$(1,0)$	$\cdots$	$(t-1,0)$	$\cdots$
$s=0$	1	0	$\cdots$	0	
$s=1$	$*$	a_1		0	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	0	
$s=t-1$	$*$	$*$		a_1^{t-1}	$*$
$\vdots$	$*$	$*$		$\vdots$	$\ddots$

δηλαδή οι πρώτες $t-1$ μορφές $\Phi^{(s)}$ είναι γραμμικά ανεξάρτητες και έτσι $1,...,t \notin E(P)$. Στην περίπτωση που $m+1 < n$ ο ισχυρισμός μας έχει αποδειχτεί. Πράγματι, $m \in E(\beta_i)$ και από το λήμμα 3.3.1 έχουμε ότι $m < t+1$ άρα $m \notin E(P)$ και $E(P) \neq E(\beta_i)$.

Ας υποθέσουμε τώρα ότι $n = m+1$. Για να αποδείξουμε ότι $E(P) \neq E(\beta)$ θα πρέπει να υπολογίσουμε ένα μεγαλύτερο κομμάτι της ημιομάδας του Weierstrass $E(P)$. Ο υπολογισμός αυτός είναι αρκετά πολύπλοκος για τυχαία n, m. Θα χρησιμοποιήσουμε ένα θεώρημα του Leopoldt σχετικά με τα σώματα συναρτήσεων του γενικού τύπου Fermat.

Θεώρημα 3.3.4 *Έστω F/k ένα σώμα συναρτήσεων με ένα μοντέλο στο $\mathbb{A}^2(k)$ ορισμένο από ένα ανάγωγο πολυώνυμο δύο μεταβλητών $F_n(x,y) = 0$ βαθμού $n \geq 4$ χωρίς ιδιομορφίες σε πεπερασμένα σημεία ή στο άπειρο. Αν P είναι μία θέση τέτοια ώστε $P \nmid (x)_\infty, (y)_\infty, \mathrm{Diff}(F/k(y), \mathrm{Diff}(F/k(x))$ τότε $\ell(\nu P) = 1$ για $\nu = 0, ..., n-2$. Επιπλέον $\ell((n-1)P) = 2$ αν και μόνο αν*

$$\text{οποτεδήποτε } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^2 \text{ τότε } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^{n-1},$$

όπου $\theta \in k$, και $\tilde{x} = x - a, \tilde{y} = y - b, a = x(P), b = y(P)$.

Απόδειξη: Πρόκειται για την πρόταση 4 στο άρθρο του Leopoldt ([17], σελ. 267) μαζί με τον χαρακτηρισμό των σωμάτων συναρτήσεων του «γενικού τύπου Fermat », σε όρους των επιπέδων μοντέλων τους, όπως γίνεται στις σελίδες 262,263 του άρθρου του Leopoldt. □

Παρατηρούμε ότι τα σώματα συναρτήσεων $F_{m+1,m}$, είναι γενικού τύπου Fermat αφού το επίπεδο μοντέλο τους που δίνεται από την $x^{m+1} + y^m + 1 = 0$ δεν είναι ιδιόμορφο σε πεπερασμένα σημεία ή στο άπειρο. Για την θέση P έχουμε

$$P \nmid (x)_\infty, (y)_\infty, \mathrm{Diff}(F/k(y), \mathrm{Diff}(F/k(x))$$

οπότε από το θεώρημα 3.3.4 έχουμε ότι $t+1 = n-1 \in E(P)$ αν και μόνο αν

$$\text{όταν } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^2 \text{ τότε } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^{t+1}. \tag{3.7}$$

Θέτουμε $y_* := \tilde{y}\ /b$, $x_* := \tilde{x}/a$ όπου $a = x(P), b = y(P)$ τα αλγεβρικά σημεία που αντιστοιχούν στην θέση P. Το πολυώνυμο ορισμού $x^{m+1} + y^m + 1$ της καμπύλης μπορεί να μετασχηματισθεί

$$(1+y_*)^m - 1 = \theta_* \left[(1+x_*)^{m+1} - 1\right], \qquad \theta_* = -\frac{a^{m+1}}{b^m} \neq 0, \infty.$$

Συνεπώς, κάνοντας χρήση του διωνυμικού θεωρήματος έχουμε

$$my_* - \theta_*(m+1)x_* = -\sum_{\nu=2}^{m}\left[\binom{m}{\nu}y_*^\nu - \theta_*\binom{m+1}{\nu}x_*^\nu\right] + \theta_* x_*^n \tag{3.8}$$

Τα στοιχεία x_*, y_* είναι τοπικές παράμετροι στην θέση P, άρα από την (3.8)

$$y_* - \theta_*\frac{m+1}{m}x_* \equiv 0 \bmod P^2. \tag{3.9}$$

Υποθέτουμε ότι $n \geq 4$ και $t+1 = n-1 \in E(P)$ τότε από τις (3.7) και (3.9) έχουμε

$$y_* - \theta_*\frac{m+1}{m}x_* \equiv 0 \bmod P^{t+1}. \tag{3.10}$$

Επιπλέον από την (3.9) έχουμε $y_*^\nu - \theta_*^\nu\left(\frac{m+1}{m}\right)^\nu x_*^\nu \equiv 0 \bmod P^\nu$ συνεπώς κάνοντας χρήση του δεξιού μέρους της (3.8) καταλήγουμε στις παρακάτω συνθήκες:

$$\binom{m}{\nu}\frac{(m+1)^\nu}{m^\nu}\theta_*^\nu - \theta_*\binom{m+1}{\nu} = 0 \text{ για } \nu = 1, ..., t+1 = n-1 = m. \tag{3.11}$$

Η περίπτωση $m > 3$ (3.11) για $\nu = 2$ δίνει $\binom{m}{2}\frac{(m+1)^2}{m^2}\theta_*^2 - \theta_*\binom{m+1}{2} = 0$. Αφού $p \nmid m, m+1$, $\binom{m+1}{2} \neq 0$ συνεπώς $\binom{m}{2} \neq 0$. Αυτό δίνει $p \nmid m-1$ άρα $\theta_* = \frac{m^2}{(m-1)(m+1)}$. Συνεχίζουμε με τον επόμενο συντελεστή $\nu = 3$. Ισχύει ότι $\binom{m}{3}\frac{(m+1)^3}{m^3}\theta_*^3 - \theta_*\binom{m+1}{3} = 0$ από όπου έχουμε ότι $1 \equiv 0 \bmod p$, άτοπο. Έτσι $t+1 = n-1 = m \notin E(P)$ άρα $E(P) \neq E(\beta)$. Χρησιμοποιήσαμε ότι $p \neq 2, 3$ και ότι $3 < n-1$. Δηλαδή το επιχείρημα μας δεν ισχύει για τις καμπύλες $x^4 + y^3 + 1 = 0$, $x^3 + y^2 + 1 = 0$ και $x^2 + y + 1 = 0$. Οι δύο τελευταίες καμπύλες δεν μας απασχολούν αφού έχουν γένη 1 και 0 αντίστοιχα. Οι Klassen και Schaefer [16], απέδειξαν πρόσφατα ότι η καμπύλη $x^4 + y^3 + 1 = 0$ έχει 48 αυτομορφισμούς.

3.4 Τοπική μελέτη

Στην συνέχεια θα συμβολίζουμε με G την ομάδα των αυτομορφισμών, και με F το σώμα συναρτήσεων Fermat $F_{n,m}$ ενώ με $G(\beta)$ την ομάδα ανάλυσης της ομάδας G στην θέση β, όπου $\beta = \beta_i$ για κάποιο $i = 1, ..., n$. Θα συμβολίζουμε με P_ζ τον περιορισμό της θέσης β στο ρητό σώμα συναρτήσεων $k(x)$. Θυμίζουμε ότι η ομάδα ανάλυσης ισούτε με την ομάδα αδράνειας $G(\beta) = G_0(\beta)$, αφού το σώμα ορισμού k είναι αλγεβρικά κλειστό. Θα αποδείξουμε ότι:

$$G(\beta) = \begin{cases} C_m & \text{αν} \quad m \nmid n \\ C_{2m} & \text{αν} \quad m|n,\ n-1 \text{ δεν είναι } p-\text{δύναμη} \\ \mathcal{E}_q \rtimes C_{m(q-1)} & \text{αν} \quad m|n, n-1 = q \text{ είναι μια } p\text{-δύναμη} \end{cases},$$

όπου, C_x συμβολίζει μια κυκλική ομάδα τάξης x, και το $\mathcal{E}_q$ συμβολίζει μια στοιχειώδης αβελιανή ομάδα τάξης q.

Από την μελέτη των ημιομάδων του Weierstrass στην θέση β βλέπουμε ότι ο χώρος $\mathcal{L}(m\beta)$ είναι διδιάστατος και μια βάση δίνεται από τις συναρτήσεις $\left\{1, \frac{1}{x-\zeta}\right\}$. Η ομάδα $G(\beta)$ αφήνει το χώρο $\mathcal{L}(m\beta)$ αναλλοίωτο. Συνεπώς $\sigma(\frac{1}{x-\zeta}) = \mu + \lambda\frac{1}{x-\zeta}$, $\mu, \lambda \in k$. Το παραπάνω αποδεικνύει ότι κάθε αυτομορφισμός $\sigma \in G(\beta)$ αφήνει το σώμα $k(x)$ αναλλοίωτο. Θα συμβολίζουμε με $\overline{G}(P_\zeta)$ την εικόνα της συνάρτησης περιορισμού

$$Res : \begin{cases} G(\beta) & \longrightarrow & \overline{G}(P_\zeta) \\ \sigma & \longmapsto & Res_{k(x)}\sigma \end{cases}$$

Προφανώς ο πυρήνας του περιορισμού είναι $\mu(m) \lhd G(\beta)$.

Ένα γεννοποιόν ριζικό του F υπέρ το σώμα $k(x)$ είναι της μορφής $y^\ell z$ όπου $(\ell, m) = 1$ και $z \in k(x)$ ([12] σελ. 38). Για κάθε $\sigma \in G(\beta)$, $\sigma(k(x)) = k(x)$, έτσι $\sigma(y)$ είναι επίσης ένα γεννοποιόν ριζικό για την επέκταση $F/k(x)$. $\sigma(y) = y^{\ell_\sigma} z_\sigma$ για ένα στοιχείο z_σ στο $k(x)$. Έστω τ ένας γεννήτορας της κυκλικής ομάδας $\mu(m) = Gal(F/k(x))$. Παρατηρούμε ότι

$$\sigma^{-1}\tau\sigma = \tau^{\ell_\sigma} \ \forall \sigma \in G(\beta) \tag{3.12}$$

Θα συμβολίζουμε με $G_1(\beta)$ την πρώτη ομάδα διακλάδωσης της θέσης β. Η ομάδα $G(\beta) = G_0(\beta)$ μπορεί να γραφεί σαν ένα ημιευθές γινόμενο μιας κυκλικής ομάδας $E := G_0(\beta)/G_1(\beta)$ τάξεως πρώτης με το p με την $p-$ομάδα $G_1(\beta)$. Θα συμβολίζουμε με π την προβολή $G_0(\beta) \longrightarrow G_0(\beta)/G_1(\beta)$. Εφαρμόζοντας την π και στα δύο μέλη της (3.12)

$$\pi(\sigma^{-1}) \cdot \pi(\tau) \cdot \pi(\sigma) = \pi(\tau)^{\ell_\sigma} \quad \forall \sigma \in G(\beta).$$

Αφού E είναι αβελιανή και $ord(\pi(\tau)) = ord(\tau) = m$ έχουμε ότι $\ell_\sigma \equiv 1 \bmod m$ άρα

$$\sigma\tau = \tau\sigma.$$

Επιπλέον, αφού $\ell_\sigma \equiv 1 \bmod m$, όλοι οι αυτομορφισμοί σ του F που επεκτείνουν το τυχαίο $\sigma_0 \in \overline{G}(P_\zeta\ )$ είναι της μορφής

$$\sigma(y) = \theta_\sigma \cdot y \cdot z_{\sigma_0},\ \sigma(x) = \sigma_0(x) \tag{3.13}$$

όπου $z_{\sigma_0} \in k(x)$ και θ_σ διατρέχει τις m-οστές ρίζες της μονάδας. Τα παραπάνω αποδυκνείουν ότι

$$k(x) \ni z_\sigma^m = \left(\frac{\sigma(y)}{y}\right)^m = \frac{\sigma(x^n+1)}{x^n+1}.$$

Αντιστρόφως, αν $\sigma_0 \in PGL(2,k)$, $\sigma_0(P_\zeta\ ) = P_\zeta$ και $\frac{\sigma_0(x^n+1)}{x^n+1} = z_{\sigma_0}^m$ είναι μία m δύναμη για κάποιο $z_{\sigma_0} \in k(x)$, τότε οι αυτομορφισμοί σ του F που δίνονται από

$$\sigma(y) = \theta y z_{\sigma_0}, \sigma(x) = \sigma_0(x),$$

επεκτείνουν τον σ_0. Αποδείξαμε το παρακάτω:

Λήμμα 3.4.1 *Έστω P_ζ ο περιορισμός της θέσης β στο $k(x)$. Ένα στοιχείο $\sigma_0 \in PGL(2,k)$ τέτοιο ώστε $\sigma_0(P_\zeta\ ) = P_\zeta$ επεκτείνεται σε αυτομορφισμό του F αν και μόνο αν $\sigma_0(x^n+1)$ διαφέρει από το x^n+1 με ένα m-οστό παράγοντα z^m. Οι επεκτάσεις του σ_0 στο F δίνονται από την (3.13).*

Σύμφωνα με το λήμμα 3.4.1 θα πρέπει να προσδιορίσουμε τους αυτομορφισμούς σ του $k(x)$ οι οποίοι σταθεροποιούν το P_ζ και για τους οποίους

$$\sigma(x)^n + 1 = z^m \cdot (x^n+1) \text{ με } z \in k(x). \tag{3.14}$$

Αρκεί να γνωρίζουμε ότι η παραπάνω σχέση ισχύει μέχρι σταθερά στο $k(x)$, αφού το k είναι αλγεβρικά κλειστό και κάθε στοιχείο στο k είναι μία m δύναμη. Γι αυτό αντί της (3.14) απαιτούμε την σχέση

$$\sigma(x)^n + 1 = c \cdot z^m \cdot (x^n+1) \text{ με } c \in k, z \in k(x). \tag{3.15}$$

Αυτή είναι ισοδύναμη με την αντίστοιχη σχέση για τους κύριους divisors των συναρτήσεων. Ο κύριος divisor της x^n+1 είναι (θα συμβολίζουμε χάριν απλότητας $P_{\zeta_i} = P_{(x=\zeta_i)}$)

$$(x^n+1) = \sum_{1 \le i \le n} P_{\zeta_i}\ - nP_\infty. \tag{3.16}$$

Παρατηρούμε ότι κάθε αυτομορφισμός σ του $k(x)$ που είναι επεκτάσιμος στο F μεταθέτει τις θέσεις του $k(x)$ που διακλαδίζονται στην επέκταση $F/k(x)$ με τον ίδιο βαθμό.

Οι διακλαδιζόμενες θέσεις στην επέκταση $F/k(x)$, είναι τα σημεία P_{ζ_i} , τα οποία έχουν κοινό δείκτη διακλάδωσης m. Επίσεις, το σημείο στο άπειρο P_∞ έχει δείκτη διακλάδωσης $\frac{m}{(n,m)}$.

Λήμμα 3.4.2 *Κάθε αυτομορφισμός $\sigma \in G(\beta)$ που σταθεροποιεί το P_∞ είναι ο ταυτοτικός.*

Απόδειξη: : Έστω $\sigma_0 = \sigma|_{k(x)}$, τέτοιος ώστε $\sigma(P_\infty) = P_\infty$. Από την (3.16) έχουμε ότι οι κύριοι divisors των συναρτήσεων $\sigma(x^n+1), x^n+1$ είναι ίσοι, συνεπώς η (3.15) ισχύει με $z \in k$. Επιπλέον αφού ο σ_0 κρατάει το P_∞ σταθερό έχουμε

$$\sigma_0(x) = a + bx \text{ όπου } a, b \in k, b \neq 0.$$

Συνπεπώς,

$$\sigma(x)^n + 1 = (a+bx)^n + 1 = c \cdot (x^n+1).$$

Αναλύουμε το αριστερό μέλος της παραπάνω εξίσωσης χρησιμοποιώντας το δυονιμικό θεώρημα. Αφού $p \nmid n$ υπάρχει τουλάχιστον ένας δυονιμικός συντελεστής $\binom{n}{i} \neq 0$, όπου $0 < i < n$. Συγκρίνοντας τους συντελεστές του x^i και στις δύο πλευρές της παραπάνω εξίσωσης βλέπουμε ότι

$$\binom{n}{i} a^{n-i} b^i = 0$$

από όπου έχουμε $a = 0$, δηλαδή $\sigma(x) = bx$. Άρα ο σ εκτός από το P_∞ σταθεροποιεί και το P_0. Άρα ο σ_0 σταθεροποιεί τρία σημεία του ρητού σώματος συναρτήσεων $k(x)$ και συνεπώς $\sigma = 1$.□

Προκειμένου να μελετήσουμε την ομάδα $\overline{G}(P_\zeta\ )$ θα διακρίνουμε τρεις περιπτώσεις:

Περίπτωση (i): $1 < (n, m) < m$. Στην περίπτωση αυτή, η P_∞ είναι η μοναδική θέση του $k(x)$ η οποία έχει βαθμό διακλάδωσης $\frac{m}{(n,m)}$, συνεπώς η θέση P_∞ σταθεροποιείται από όλους τους επεκτάσιμους αυτομορφισμούς σ_0 που σταθεροποιούν P_ζ. Το λήμμα 3.4.2 εξασφαλίζει ότι $\overline{G}(P_\zeta) = 1$.

Περίπτωση (ii): $(n, m) = m$, δηλαδή $m|n$. Στην περίπτωση αυτή ένας μη τετριμμένος επεκτάσιμος αυτομορφισμός σ του $k(x)$ που σταθεροποιεί το P_ζ δίνεται από την

$$\sigma(x) = \frac{\zeta^2}{x} \tag{3.17}$$

όπου $\zeta^n = -1$. Πράγματι, αφού $\zeta^{2n} = 1$ έχουμε

$$\sigma(x)^n + 1 = \frac{1}{x^n} + 1 = \frac{1 + x^n}{x^n}.$$

Παρατηρούμε ότι η (3.15) ισχύει με $c = 1$ και $z = \frac{1}{x^{n/m}}$· θυμίζουμε ότι $m|n$ στην περίπτωση (ii). Επίσης ο αυτομορφισμός που δίνεται από την (3.17) αντιμεταθέτει τις θέσεις P_∞ και P_0.

Κάθε άλλος αυτομορφισμός $\sigma \in \overline{G}(P_\zeta\ )$ μεταθέτει τις θέσεις P_{ζ_i} αφού αυτές είναι ακριβώς οι θέσεις που διακλαδίζονται στην F, με βαθμό διακλάδωσης m. Θέτουμε

$$P_\eta = \sigma(P_\infty)$$

με $\eta \notin \{\zeta_1, ..., \zeta_n\}$. Υποθέτουμε επίσεις ότι $\eta \neq \infty$ γιατί διαφορετικά η θέση P_∞ θα σταθεροποιούνταν από τον σ και από το λήμμα 3.4.2 θα είχαμε $\sigma = 1$. Υπολογίζουμε

$$\sum_{1 \le i \le n} \sigma(P_{\zeta_i}) - n\sigma(P_\infty) = \sum_{1 \le i \le n} P_{\zeta_i} - nP_\eta\ = n(P_\infty - P_\eta\ ) + \sum_{1 \le i \le n} P_{\zeta_i} - nP_\infty.$$

Εδώ, $P_\infty - P_\eta$ είναι ο κύριος divisor της συνάρτησης $\frac{1}{x-\eta}$. Άρα η συνθήκη (3.15) ισχύει με $z = \left(\frac{1}{x-\eta}\right)^{n/m}$. (Υπενθυμίζουμε ότι στην περίπτωση αυτή $m|n$.) Από την άλλη, αφού $\sigma(P_\infty) = P_\eta$ έχουμε ότι ο σ είναι της μορφής

$$\sigma(x) = \frac{a + bx}{x - \eta}. \tag{3.18}$$

Αντικαθιστώντας στην (3.15) και πολλαπλασιάζοντας με $(x - \eta)^n$ βλέπουμε ότι η

$$(a + bx)^n + (x - \eta)^n = c \cdot (x^n + 1) \tag{3.19}$$

είναι αναγκαία και ικανή συνθήκη για να επεκτείνεται ο αυτομορφισμός σ σε αυτομορφισμό του F. Όπως και παραπάνω, θέτουμε $0 < i < n$ τέτοιο ώστε $\binom{n}{i} \neq 0$. Συγκρίνοντας τους συντελεστές του x^i και στα δυο μέλη της (3.19) βλέπουμε ότι

$$a^{n-i} b^i = -(-\eta)^{n-i}. \tag{3.20}$$

Αν $\eta = 0$ τότε $a \neq 0$ (διαφορετικά $\sigma = 1$) και συνεπώς $b = 0$. Αφού ο σ αφήνει το P_ζ σταθερό, η specialization $x \longmapsto \zeta$ δίνει ότι $\sigma(x) \longmapsto \zeta$ το οποίο με την σειρά του δίνει $a = \zeta^2$. Συνεπώς αν $\eta = 0$ παίρνουμε την involution που ήδη γράψαμε στην (3.17).

Υποθέτουμε τώρα ότι $\eta \neq 0$· τότε $a \neq 0$ και $b \neq 0$ σύμφωνα με την (3.20). Ας υποθέσουμε ότι υπάρχει ένα i τέτοιο ώστε και οι δύο συντελεστές $\binom{n}{i} \neq 0$ και $\binom{n}{i+1} \neq 0$. Τότε η εξίσωση (3.20) ισχύει ταυτόχρονα για i και για $i+1$. Περνώντας στο πηλίκο έχουμε ότι $ab^{-1} = -\eta$ και συνεπώς λόγω της (3.18) έχουμε $\sigma(x) = \frac{b(x-\eta)}{x-\eta} = b$, άτοπο. Άρα, αν υπάρχει ένας επιπλέον μη τετριμμένος αυτομορφισμός $\sigma \in \overline{G}(P_\zeta)$, ο οποίος να διαφέρει από την involution (3.17) δεν υπάρχουνε δυο διαδοχικοί ενδιάμεσοι διονυμικοί συντελεστές $\binom{n}{i}$, $\binom{n}{i+1}$ που να είναι ταυτόχρονα $\neq 0$.

Λήμμα 3.4.3 *Αν για όλα τα $i = 1, ..., n-2$*

$$\binom{n}{i} \neq 0 \Longrightarrow \binom{n}{i+1} = 0$$

και $p \not| n$ τότε $n = 1 + q$ όπου q είναι μία p-δύναμη.

Απόδειξη: Συμβολίζουμε με $a = \sum a_i p^i, b = \sum b_i p^i$, $0 \leq a_i, b_i < p$, το p-αδικό ανάπτυγμα δύο ακαιρέων αριθμών a, b. Αν $a_i \leq b_i$ για όλα τα i τότε γράφουμε $a \leq_p b$. Είναι γνωστό ότι $\binom{n}{i} \neq 0$ αν και μόνο αν $i \leq_p n$,[22] σελ. 73. Έστω $n = n_0 + n_1 q_1 + ... + n_s q_s$ το p-αδικό ανάπτυγμα του n, όπου $q_i = p^{s_i}$ και $0 < n_i < 0$. Παρατηρούμε ότι $q_i \leq_p n$ και $1 + q_1 \leq_p n$ άρα $\binom{n}{q_i} \neq 0$ και $\binom{n}{1+q_i} \neq 0$. Από την συνθήκη του λήμματος έχουμε ότι $n - 2 < q_i$. Αφού δε η χαρακτηριστική είναι πρώτη προς το $n, s = 1$ και $n - 1 = q_1$. □

Κάνοντας χρήση του λήμματος 3.4.3 παίρνουμε ότι

Στην περίπτωση (ii), αν $n-1$ δεν είναι δύναμη της χαρακτηριστικής p, τότε $\overline{G}(P_\zeta)$ είναι τάξης 2, και περιέχει μόνο την involution που δίνεται από την (3.17).

Απομένει να μελετήσουμε την περίπτωση (ii) όταν $n - 1 = q$ είναι μία p-δύναμη. Είναι βολικό να αντικαταστήσουμε το ριζικό του Kummer με ένα άλλο ριζικό για την επέκταση $F/k(x)$ το οποίο θα είναι ευκολότερο στο χειρισμό.

Θέτουμε

$$t := \frac{\zeta}{x - \zeta}, \qquad \text{άρα } x = \zeta \cdot \frac{t+1}{t} \tag{3.21}$$

και

$$u := -t^n(x^n + 1). \tag{3.22}$$

Αφού $m|n$, έχουμε ότι t^n είναι μία m δύναμη και συνεπώς το u είναι ένα επιτρεπτό ριζικό για την επέκταση του Kummer $F/k(x)$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\zeta = \zeta_1$. Ο κύριος divisor του u είναι

$$\begin{aligned}(u) &= n \cdot (t) + (x^n + 1) = n(P_\infty - P_\zeta\ ) + \sum_{1 \leq i \leq n} P_{\zeta_i} - \ nP_\infty = \\ &= \sum_{2 \leq i \leq n} P_{\zeta_i} - (n-1)P_\zeta\end{aligned}$$

Από την άλλη γνωρίζουμε ότι στην περίπτωση (ii) οι θέσεις P_{ζ_i} μετατίθενται κάτω από την δράση του $\sigma \in \overline{G}(P_\zeta)$, και η θέση P_ζ παραμένει σταθερή. Δηλαδή ο κύριος divisor του u μένει σταθερός από το σ.

Εξ ορισμού του t έχουμε ότι $k(x) = k(t)$, και ότι ο πόλος του t είναι P_ζ. Το στοιχείο u έχει την θέση P_ζ σαν μοναδικό πόλο, με τάξη $n - 1 = q$. Συνεπώς το u είναι ένα πολυώνυμο του t, βαθμού q. Το πολυώνυμο αυτό μπορεί να υπολογιστεί ακριβώς, χρησιμοποιόντας την (3.21) και την (3.22), έχοντας φυσικά υπόψην ότι $n = q + 1$:

$$u = -t^n \left(\frac{\zeta^n (t+1)^n}{t^n} + 1 \right) = (t+1)^n - t^n = t^q + t + 1.$$

Είναι βολικό να ξαναλλάξουμε την μεταβλητή t ώστε να απλοποίησουμε την μορφή του παραπάνω πολυωνύμου. Θέτουμε λοιπόν $t = a_1 + b_1 t_1$ με $a_1, b_1 \in k$ τέτοια ώστε $a_1^q + a_1 = -1$ και $b_1^q = -b_1$, όπου $b_1 \neq 0$. Στην συνέχεια θέτουμε $u_1 = -b_1^{-1} u$ και τελικά καταλήγουμε στην

$$u_1 = t_1^q - t_1.$$

Από εδώ και στο εξής θα γράφουμε t αντί για t_1 και u αντί για u_1. Αποδείξαμε ότι

Στην περίπτωση (ii) με $n = q+1$ υπάρχει ένας γεννήτορας t του $k(x) = k(t)$ ο οποίος έχει την θέση P_ζ σαν μοναδικό πόλο, και επιπλέον το πολυώνυμο $u = t^q - t$ είναι ένα ριζικό για την επέκταση $F/k(t)$. Ο κύριος divisor του u παραμένει αναλλοίωτος κάτω από κάθε $\sigma \in \overline{G}(P_\zeta)$.

Αφού κάθε $\sigma \in \overline{G}(P_\zeta)$ αφήνει τον πόλο του t σταθερό είναι της μορφής

$$\sigma(t) = a + bt,$$

με $a, b \in k$ και $b \neq 0$. Ένας τέτοιος αυτομορφισμός ανήκει στο $\overline{G}(P_\zeta)$ αν και μόνο αν $\sigma(u) = cu$ όπου $0 \neq c \in k$, το οποίο σημαίνει

$$\sigma(t)^q - \sigma(t) = (a+bt)^q - (a+bt) = c \cdot (t^q - t)$$

με $c \neq 0 \in k$. Δηλαδή ισχύουν οι συνθήκες

$$a^q = a, c = b, b^q = b$$

Καταλήξαμε στο παρακάτω συμπέρασμα:

Στην περίπτωση (ii)με $n = q+1$, η ομάδα $\overline{G}(P_\zeta)$ αποτελείται ακριβώς από τους μετασχηματισμούς $t \longmapsto a+bt$ των οποίων οι συντελεστές a, b περιέχονται στο σώμα $\mathbb{F}_q$ με q-στοιχεία. Η ομάδα αυτή είναι ισόμορφη με την ομάδα των πινάκων

$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \qquad \text{με } a, b \in \mathbb{F}_q, b \neq 0.$$

Ιδιαίτερα η τάξη του$\overline{G}(P_\zeta)$ είναι $(q-1)q$.

Περίπτωση (iii): $(n, m) = 1$. Στην περίπτωση αυτή οι $n+1$ θέσεις $P_{\zeta_1}, ..., P_{\zeta_n}, P_\infty$ είναι ακριβώς οι θέσεις που διακλαδίζονται στο F, όλες με βαθμό διακλάδωσης m. Κάθε $\sigma \in \overline{G}(P_\zeta)$ αφήνει το P_ζ αναλλοίωτο και συνεπώς μεταθέτει τα $P_{\zeta_2}, ..., P_{\zeta_n}, P_\infty$.

Έστω $\sigma(P_\infty) = P_\eta$. Αν $\eta = \infty$ τότε από το λήμμα 3.4.2 έχουμε ότι $\sigma = 1$. Υποθέτουμε τώρα ότι $\sigma \neq 1$ το οποίο σημαίνει ότι $\eta \in \{\zeta_2, ..., \zeta_n\}$. Ο κύριος divisor του x^n+1 απεικονίζεται μέσω της σ στον divisor

$$\sum_{1 \leq i \leq n} \sigma(P_{\zeta_i}) - nP_\eta .$$

Στο παραπάνω άθροισμα δεν εμφανίζεται ο όρος P_η , ενώ εμφανίζεται ένας όρος P_∞. Αν από αυτό αφαιρέσουμε τον κύριο divisor του $x^n + 1$ τότε παίρνουμε

$$\left(\frac{\sigma(x^n+1)}{x^n+1} \right) = (n+1)(P_\infty - P_\eta). \tag{3.23}$$

Το δεξί μέλος είναι ο κύριος divisor της συνάρτησης $(\frac{1}{x-\eta})^{n+1}$. Από την άλλη, γνωρίζουμε ότι το δεξί μέλος είναι ο divisor μιας m δύναμης. Έτσι καταλήγουμε

$$m | n+1$$

σαν μια αναγκαία συνθήκη ώστε να υπάρχει ένας μη τετριμμένος αυτομορφισμός στην $\overline{G}(P_\zeta)$.

Η εξίσωση (3.23) μας δίνει ότι

$$\sigma(x)^n = \frac{c(x^n+1)-(x-\eta)^{n+1}}{(x-\eta)^{n+1}}, \text{ όπου } c \in k.$$

Ο κύριος divisor του πολυωνύμου $f(x) := c(x^n+1)-(x-\eta)^{n+1}$, το οποίο είναι βαθμού $n+1$, είναι

$$\sum_{1\le i\le n} A_i + P_\eta - (n+1)P_\infty,$$

όπου A_i, P_η είναι οι θέσεις, όχι κατ ανάγκην διαφορετικές, που αντιστοιχούν στις ρίζες του $f(x)$. Από την άλλη, ο κύριος divisor του $(x-\eta)^{n+1}$ είναι $(n+1)(P_\eta - P_\infty)$ και αυτό μας δίνει ότι ο κύριος divisor του $\sigma(x)^n$ είναι

$$(\sigma(x)^n) = \sum_{1\le i\le n} A_i - nP_\eta \,.$$

Συνεπώς το πολυώνυμο $f(x)$ έχει μία πολλαπλή ρίζα τάξης n. Αν ρ είναι αυτή η ρίζα, τότε

$$f(x) = c(x^n+1)-(x-\eta)^{n+1} = c_1\cdot(x-\eta)(x-\rho)^n, \tag{3.24}$$

για κάποιο $c_1 \in k$. Ξεχωρίζουμε δυο περιπτώσεις:

α) $\rho = 0$. Τότε η (3.24) γίνεται

$$c(x^n+1)-(x-\eta)^{n+1} = c_1(x-\eta)x^n = c_1x^{n+1} - c_1\eta x^n. \tag{3.25}$$

Αναπτύσουμε το αριστερό μέλος χρησιμοποιόντας τον διονυμικό τύπο

$$c(x^n+1)-(x-\eta)^{n+1} =$$

$$= -x^{n+1} + \left(-(n+1)(-\eta)+c\right)x^n - \sum_{i=1}^{n-1}\binom{n+1}{i}(-\eta)^{n+1-i}x^i + c - (-\eta)^{n+1}.$$

Συγκρίνοντας τους συντελεστές του x^{n+1} στα δύο μέλη της (3.25) παίρνουμε $c_1 = -1$, ενώ συγκρίνοντας τους συντελεστές του x^n και του σταθερού όρου παίρνουμε $c = \eta$. Επιπλέον για κάθε $i = 1, ..., n$ έχουμε ότι

$$\binom{n+1}{i} = 0$$

το οποίο μαζί με το κριτήριο μηδενισμού ενός διονυμικού συντελεστή που δώθηκε στο λήμμα 3.4.3, δίνει ότι $n+1 = q$ είναι μία δύναμη της χαρακτηριστικής p. Αυτό όμως είναι αδύνατον αφού $m|n+1$ και $(m,p)=1$.

β) $\rho \neq 0$. Παρατηρούμε ότι το $(x-\rho)^{n-1}$ διαιρεί το πολυώνυμο

$$g(x) := (n+1)f(x) - \frac{df(x)}{dx}(x-\eta) = c\left(x^n + n\eta x^{n-1} + (n+1)\right).$$

Επιπλέον έχουμε ότι το η είναι μία ρίζα του $g(x)$, αφού $\eta^n = -1$, έτσι για μία σταθερά c' έχουμε

$$c\left(x^n + n\eta x^{n-1} + (n+1)\right) = c'(x-\eta)(x-\rho)^{n-1}. \tag{3.26}$$

Συγκρίνοντας τους συντελεστές του x^n και στα δύο μέλη της (3.26) καταλήγουμε στο ότι $c' = c$. Συγκρίνοντας τους συντελεστές του x και x^2 και στα δύο μέλη της (3.26) παίρνουμε

$$(-\rho)^{n-2}(-\rho - \eta(n-1)) = 0 \Rightarrow -\rho = (n-1)\eta \tag{3.27}$$

και

$$(-\rho)^{n-3}\left(-\eta\binom{n-1}{2}-\rho(n-1)\right)=0. \tag{3.28}$$

Αντικαθιστούμε την (3.27) στην (3.28) για να πάρουμε

$$(-\rho)^{n-3}\eta\frac{(n-1)n}{2}=0,$$

το οποίο είναι άτοπο, αφού από την (3.27) $n-1\neq 0$ (υπενθυμίζουμε ότι έχουμε υποθέσει για την χαρακτηριστική ότι $p\neq 2$ και $p\nmid n$).

Έχουμε υπολογίσει όλα τα στοιχεία στην ομάδα $G(\beta)$. Η ομάδα αυτή είναι τάξης

$$|\ \overline{G}(P_\zeta\ )|\cdot|\mu(m)|=\begin{cases} m & \text{αν} \quad m\nmid n \\ 2m & \text{αν} \quad m\mid n \text{ και } n-1 \text{ δεν είναι μία } p \text{ δύναμη} \\ mq(q-1) & \text{αν} \quad m\mid n \text{ και } n-1=q \text{ είναι μία } p \text{ δύναμη}\end{cases}.$$

Επιπλέον στις πρώτες δύο περιπτώσεις η τάξη του $G(\beta)$ είναι πρώτη προς την χαρακτηριστική του σώματος p (υπενθυμίζουμε ότι έχουμε υποθέσει ότι $p\neq 2$), συνεπώς η ομάδα $G(\beta)$ είναι ισόμορφη με μία κυκλική ομάδα τάξης m (αντίστοιχα $2m$). Στην τρίτη περίπτωση η ομάδα $G(\beta)$ είναι το ημιευθές γινόμενο μιας κυκλικής ομάδας τάξης $m(q-1)$ με μία κανονική υποομάδα τάξης q[20, σελ. 68].

3.5 Δομή της ομάδας αυτομορφισμών

Θα συμβολίζουμε με $O(\beta,G)$ την τροχιά της θέσης β κάτω από την δράση της G. Θα υπολογίσουμε την τάξη του $|G|$ υπολογίζοντας την τάξη της $O(\beta,G)$. Έχουμε καθορίσει ποιες θέσεις του F δεν γίνεται να ανήκουν στην τροχιά β (λήμματα 3.3.2 και 3.3.3), συνεπώς

$$O(\beta,G)\subseteq\{\beta_1,\beta_2,...,\beta_n,\gamma_1,\gamma_2,...,\gamma_{(n,m)}\}.$$

Παρατηρούμε ότι τα $\beta_i\in O(\beta,G)$ για $i=1,...,n$ και ότι αν $\gamma_{i_0}\in O(\beta,G)$ για κάποιο i_0 τότε $\gamma_i\in O(\beta,G)$ για όλες τις θέσεις γ_i $i=1,...,(n,m)$ που επεκτείνουν την P_∞.

Περίπτωση 1) Υποθέτουμε ότι $m\nmid n$. Τότε $|O(\beta,G)|=n$ ή $n+(n,m)$. Ας υποθέσουμε ότι $|O(\beta,G)|=n+(n,m)$ και έστω $H:=\mu(n)\times\mu(m)$. Προφανώς η τάξη της τροχιάς της β υπό την δράση της H είναι $|O(\beta,H)|=|H:H(\beta)|=n$. Έχουμε αποδείξει ότι $|G(\beta)|=\mu(m)=|H(\beta)|$ έτσι

$$\frac{n+(n,m)}{n}=\frac{|G:G(\beta)|}{|H:H(\beta)|}=\frac{|G|}{|H|}\in\mathbb{N}.$$

Από το αριστερό μέρος της παραπάνω εξίσωσης παίρνουμε ότι $n|(n,m)$, το οποίο εί ναι άτοπο αφού $n>m$. Δηλαδή $|O(\beta,G)|=n$ και η ομάδα G έχει τάξη

$$|G|=|O(\beta,G)|\cdot|G(\beta)|=nm.$$

Περίπτωση 2) Υποθέτουμε ότι $m|n$. Η involution σ που δίνεται από την (3.17) στέλνει μία θέση γ_i που επεκτείνει την P_∞ σε μία θέση α_j υπέρ το P_0. Αυτό μας δίνει ότι $O(\beta,G)=\{\beta_1,\beta_2,...,\beta_n\}$, γιατί αν υπήρχε ένα $\tau\in G$ τέτοιο ώστε $\tau(\beta)=\gamma_i$ τότε $\tau\sigma(\beta)=\alpha_j$ το οποίο είναι αδύνατον από το λήμμα 3.3.2. Συνεπώς η τάξη του G, σε αυτή την περίπτωση υπολογίζεται:

$$|G|=|G:G(\beta)|\cdot|G(\beta)|=|O(\beta,G)|\cdot|G(\beta)|=$$

$$=\begin{cases} 2nm & \text{αν} \quad n-1 \text{ δεν είναι μία δύναμη του } p \\ nmq(q-1) & \text{αν} \quad n-1 \text{ είναι μία δύναμη του } p\end{cases}$$

Θα μελετήσουμε τώρα την δομή της ομάδας των αυτομορφισμών. Υποθέτουμε καταρχήν ότι $m \nmid n$. Σε αυτή την περίπτωση η ομάδα G είναι το ευθύ γινόμενο των ομάδων $\mu(n)$ και $\mu(m)$, αφού $|G| = n \cdot m$ και $\mu(n) \times \mu(m) \leq G$.

Ας υποθέσουμε ότι $m|n$. Παρατηρούμε ότι $\mu(m) < Z(G)$. Πράγματι, έστω G_1 η υποομάδα του G που παράγεται από όλα τα γινόμενα $x \cdot y$, $x \in G(\beta), y \in \mu(n)$. Η ομάδα $G_1 < G$ έχει τουλάχιστον $|G(\beta)| \cdot |\mu(n)| = |G|$ στοιχεία, αφού $G(\beta) \cap \mu(n) = 1$. Άρα $|G_1| = |G|$ και τελικά $G_1 = G$. Αυτό αποδεικνύει το επιθυμητό αποτέλεσμα, αφού τα στοιχεία του $\mu(m)$ αντιμετατίθενται με τα στοιχεία του $G(\beta)$ και $\mu(n)$.

Αφού δε $\mu(m) \lhd G$ κάθε αυτομορφισμός $\sigma \in G$ περιορίζεται σε ένα αυτομορφισμό του ρητού σώματος συναρτήσεων $k(x) = F^{\mu(m)}$. Άρα η συνάρτηση περιορισμού της σελίδας 51 μπορεί να επεκταθεί σε μία συνάρτηση

$$\mathcal{F} : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathcal{F}(G) < PGL(2,k) \\ \sigma & \longmapsto & res_{k(x)}\sigma. \end{array} \right.$$

Προφανώς ο πυρήνας της $\mathcal{F}$ είναι $\ker \mathcal{F} = \mu(m)$. Θα ξεχωρίσουμε ακόμα δύο περιπτώσεις:

i) Το $n-1$ δεν είναι δύναμη του p. Τότε σύμφωνα με τον υπολογισμό της τάξης του G, η τάξη του $\mathcal{F}(G)$ είναι $2n$. Παρατηρούμε ότι η ομάδα $\mathcal{F}(G)$ περιέχει την κυκλική ομάδα $\mu(n)$ που παράγεται από το $\tau_0 : x \longmapsto \zeta^2 x$ και την involution $\sigma_0 : x \longmapsto \zeta^2/x$. Αφού $\sigma_0 \notin \langle \tau_0 \rangle = \mu(n)$ και $\sigma_0\tau_0 = \tau_0^{-1}\sigma_0$, η ομάδα που γεννάται από τα σ_0, τ_0 είναι μία διεδρική ομάδα τάξης $2 \cdot n$. Αυτή είναι η τάξη της $\mathcal{F}(G)$, άρα $\mathcal{F}(G) \cong D_n$ και η ομάδα G δίνεται σαν κεντρική επέκταση της D_n με αβελιανό πυρήνα $\mu(m)$.

Η ομάδα ανάλυσης γενάται από τους αυτομορφισμούς

$$\sigma : \left\{ \begin{array}{ccc} y & \longmapsto & \frac{y}{x^{n/m}} \\ x & \longmapsto & \frac{\zeta^2}{x} \end{array} \right.$$

αφού σ έχει τάξη $2m$. Η ομάδα $\mu(n) < G$ γεννάται από τον

$$\tau : \left\{ \begin{array}{ccc} y & \longmapsto & y \\ x & \longmapsto & \zeta^2 x \end{array} \right.$$

και μπορούμε να ελέγξουμε ότι η ομάδα G δέχεται μία παράσταση

$$\langle \sigma, \tau / \sigma^{2m} = 1, \tau^n = 1, \sigma^3\tau^{-1} = \tau\sigma, \sigma^2\tau = \tau\sigma^2 \rangle.$$

Παρατηρούμε ότι αν μία κεντρική επέκταση διασπάται, δηλαδή αντιστοιχεί στην τετριμμένη συνομολογιακή κλάση, τότε είναι το ευθύ γινόμενο των παραγόντων της. Θα αποδείξουμε ότι η επέκταση

$$1 \longrightarrow \mu(n) \longrightarrow G \longrightarrow D_n \longrightarrow 1 \tag{3.29}$$

διασπάται ή ισοδύναμα $G \cong \mu(n) \times D_n$ αν και μόνο αν το m είναι περιττό.

Έστω m περιττό. Η συνάρτηση

$$\begin{array}{rcl} H^2(D_n, \mu(m)) = \bigoplus_{p|2n} H^2(D_n, \mu(m))_p & \longrightarrow & \bigoplus_{p|2n} H^2(H_p, \mu(m)) \\ \alpha = \sum_{p|2n} \alpha_p & \longmapsto & \sum_{p|2n} res_{(D_n \to H_p)}\alpha_p \end{array}$$

όπου το H_p διατρέχει τις p-Sylow υποομάδες της D_n είναι «1-1» [32, σελ. 93]. Αν $p = 2$ τότε $(|H_2|, m) = 1$ άρα $res_{(D_n \to H_2)}\alpha_2 = 1$ από το θεώρημα του Zassenhaus[14, σελ. 126]. Από την άλλη αν H_p είναι μία p-Sylow υποομάδα για $p \neq 2$, τότε $res_{(D_n \to H_p)}\alpha_p = 1$ αφού $H_p < \mu(n)$ και η υποεπέκταση

$$1 \longrightarrow \mu(m) \longrightarrow G_1 \longrightarrow \mu(n) \longrightarrow 1$$

διασπάται.

Έστω m άρτιος. Θεωρούμε την υποομάδα που γεννάτε από την involution σ που δίνεται από την (3.17) και την υποεπέκταση που δίνεται από το παρακάτω διάγραμμα

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu(m) & \longrightarrow & G & \xrightarrow{\pi} & D_n & \longrightarrow & 1 \\ & & || & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mu(m) & \longrightarrow & \pi^{-1}(\langle\sigma\rangle) & \longrightarrow & \langle\sigma\rangle & \longrightarrow & 1 \end{array}$$

Έστω $\alpha \in H^2(D_n, \mu(m))$ η συνομολογιακή κλάση που αντιστοιχεί στην επέκταση G. Στην υποεπέκταση $\pi^{-1}(\langle\sigma\rangle)$ αντιστοιχεί η συνομολογιακή κλάση $res_{(D_n\to\langle\sigma\rangle)}\alpha$. Αλλά $\pi^{-1}(\langle\sigma\rangle) = G(\beta)$ η οποία είναι μία κυκλική ομάδα τάξης $2m$. Συνεπώς $res_{(D_n\to\langle\sigma\rangle)}\alpha \neq 1$ αφού μία κυκλική ομάδα τάξης $2m$ δεν είναι ισόμορφη με το γινόμενο $\mu(m) \times \langle\sigma\rangle$ όταν $2|m$.

ii) Σε αυτή την περίπτωση το $n - 1 = p^s = q$, είναι δύναμη της χαρακτηριστικής. Ισχυριζόμαστε ότι $\mathcal{F}(G) < PGL(2, q^2)$. Παίρνουμε σαν γεννήτορα του σώματος $k(x)$ το στοιχείο t όπως αυτό ορίστηκε στην σελίδα 55. Έχουμε αποδείξει ότι $\mathcal{F}(G(\beta)) = \overline{G}(P_\zeta)$ είναι μία ομάδα από Möbius μετασχηματισμούς της μορφής $t \longmapsto a + bt$, $a, b \in \mathbb{F}_q \subset \mathbb{F}_{q^2}$. Τα στοιχεία στην $\mu(n)$ ορίζονται υπέρ το $\mathbb{F}_{q^2}$ επίσης. Πράγματι, η αλλαγή μεταβλητών $x \longmapsto t$ εμπλέκει τα ζ, a_1, b_1 τα οποία ανήκουν στο σώμα $\mathbb{F}_{q^2}$ αφού

$$b_1^q = -b_1 \Rightarrow b_1^{q^2} = b_1 \text{ (το } q \text{ είναι περιττό)}$$
$$\zeta^n = -1 \Rightarrow \zeta^{q+1} = -1 \Rightarrow \zeta^q = -\tfrac{1}{\zeta} \Rightarrow \zeta^{q^2} = \zeta$$
$$a_1^q = -1 - a_1 \Rightarrow a_1^{q^2} = (-1 - a_1)^q = (-1)^q + (-1)^q a_1^q = a_1$$

και συνεπώς η αλλαγή μεταβλητών $x \longmapsto t$ είναι ένας Möbius μετασχηματισμός στο $PGL(2, q^2)$. Από την άλλη η $\mathcal{F}(\mu(n))$ γεννάται από τους αυτομορφισμούς $x \longmapsto \zeta^2 x$ που ανήκουν στην $PGL(2, q^2)$.

Η τάξη της $\mathcal{F}(G)$ είναι $q(q-1)(q+1)$. Θα αποδείξουμε ότι η μοναδική υποομάδα της $PGL(2, q^2)$ με τάξη $q(q-1)(q+1)$ είναι η $PGL(2, q)$. Για αυτό θα χρησιμοποιήσουμε τον χαρακτηρισμό των υποομάδων της $PGL(2, p^f)$ ο οποίος προκύπτει από το θεώρημα 2.2.1.

Θεώρημα 3.5.1 *Η ομάδα $PGL(2, p^f)$ έχει τις παρακάτω υποομάδες*

1. *Στοιχειώδεις αβελιανές p-ομάδες*
2. *Κυκλικές ομάδες τάξης t όπου $t|p^f \pm 1$.*
3. *Διεδρικές ομάδες τάξης $2t$, $t|p^f \pm 1$.*
4. *Ομάδες ισόμορφες με A_4, S_4, A_5.*
5. *Ημιευθέα γινόμενα από στοιχειώδεις αβελιανές ομάδες τάξης p^r με κυκλικές ομάδες τάξης t, όπου $t|p^r - 1$ και $t|p^f - 1$.*
6. *Ομάδες ισόμορφες με την $\mathrm{PSL}(2, p^r)$ και $\mathrm{PGL}(2, p^r)$ όπου $r|f$.*

Θα χρησιμοποιήσουμε το παραπάνω θεώρημα και το γεγονός ότι $|\mathcal{F}(G)| = q(q^2-1)$, όπου $q = p^s$ είναι δύναμη της χαρακτηριστικής, για να περιγράψουμε την δομή ομάδας της $\mathcal{F}(G)$. Παρατηρούμε ότι $\mathcal{F}(G)$ δεν είναι p-ομάδα, και κατά συνέπεια ούτε στοιχειώδης αβελιανή. Ας υποθέσουμε ότι $\mathcal{F}(G)$ είναι ισόμορφη με μία κυκλική ομάδα τάξης t, $t|p^f \pm 1$. Τότε $|\mathcal{F}(G)| = p^s(p^{2s} - 1)$ διαιρεί το $p^f \pm 1$, άτοπο αφού $p \nmid 1$. Για τον ίδιο λόγο η $\mathcal{F}(G)$ δεν είναι διεδρική ομάδα. Οι τρεις ομάδες A_4, S_4, A_5 έχουν τάξη μικρότερη η ίση του 60, ενώ από την άλλη $|\mathcal{F}(G)| = q(q^2-1) \geq 120$ αφού $p \geq 5$. Δηλαδή $\mathcal{F}(G) \ncong A_4, S_4, A_5$. Ας υποθέσουμε τώρα ότι $\mathcal{F}(G)$ είναι το ημιευθύ γινόμενο μίας στοιχειώδους αβελιανής ομάδας τάξης p^r με μία κυκλική ομάδα τάξης $t = p^{s-r}(p^{2s} - 1)$. Ο αριθμός t θα πρέπει να διαιρεί και το $p^r - 1$ και το $p^f - 1$, άτοπο. Τέλος αν $\mathcal{F}(G) \cong \mathrm{PSL}(2, p^r)$ τότε $r|f = 2s$ και $|\mathrm{PSL}(2, r)| = \frac{(p^{2r}-1)p^r}{2} = (p^{2s}-1)p^s$, άτοπο. Η μόνη δυνατή περίπτωση είναι $\mathrm{Im}(\mathcal{F}) \cong \mathrm{PGL}(2, q)$.

Η ομάδα G είναι μία κεντρική επέκταση της $\mathrm{PGL}(2, q)$ με πυρήνα $\mu(m)$ που να δίνεται από την παρακάτω ακριβή ακολουθία:

$$1 \longrightarrow \mu(m) \longrightarrow G \xrightarrow{\pi} \mathrm{PGL}(2, q) \longrightarrow 1 \tag{3.30}$$

Χρησιμοποιώντας το παγκόσμιο θεώρημα συντελεστών, τις τιμές του πολλαπλασιαστή του Schur $H_2(\mathrm{PGL}(2, q), \mathbb{Z})$ και την αβελιανοποίηση του $\mathrm{PGL}(2, q)$ [3, σελ. 26] μπορούμε να υπολογίσουμε

$$H^2(\mathrm{PGL}(2, q), \mu(m)) = \begin{cases} 0 & \text{αν} \quad m \equiv 1 \bmod 2 \\ \mathbb{Z}_2 \oplus Z_2 & \text{αν} \quad m \equiv 0 \bmod 2 \end{cases}.$$

Αυτό μας δίνει ότι για περιττό m η ομάδα G είναι ισόμορφη με

$$G \cong \mu(m) \times \mathrm{PGL}(2, q).$$

Για m άρτιο, η κατάσταση είναι περισσότερο πολύπλοκη. Για να περιγράψουμε την δομή της ομάδας G, είναι αρκετό να καθορίσουμε την συνομολογιακή κλάση

$$\alpha \in H^2(\mathrm{PGL}(2, q), \mu(m))$$

η οποία αντιστοιχεί στην κεντρική επέκταση (3.30). Αυτό τον υπολογισμό όμως τον κάναμε στο προηγούμενο κεφάλαιο όταν εξετάζαμε κυκλικές επεκτάσεις της $PGL(2, q)$.

Κεφάλαιο 4

Ομάδες αυτομορφισμών των modular καμπύλων $X(N)$

Ο J.P. Serre σε ένα γράμμα του στον Ribet υπολόγισε ότι οι ομάδες αυτομορφισμών των modular καμπύλων $X(p)$ για p πρώτο $p \geq 7$, είναι ισόμορφες με τις απλές ομάδες $PSL(2,p)$. Σκοπός αυτού του κεφαλαίου είναι η επέκταση του αποτελέσματος του Serre και η μελέτη της ομάδας των αυτομορφισμών των καμπύλων $X(N)$, όπου N οποιοσδήποτε θετικός ακέραιος. Όπως προέκειψε μετά από επικοινωνία με τον J.P. Serre, το αποτέλεσμα που έστειλε στον Ribet, όπως και η γενίκευση του, ήταν γνωστό στους ειδικούς της περιοχής.

Υπενθυμίζουμε ότι οι καμπύλες $X(N)$ είναι οι επιφάνειες Riemann που ορίζονται ως χώροι τροχιών $\Gamma(N)\backslash\mathbb{H}^*$, όπου $\Gamma(N)$ είναι ο πυρήνας του επιμορφισμού

$$PSL(2,\mathbb{Z}) \longrightarrow PSL\left(2,\mathbb{Z}/N\mathbb{Z}\right)$$

Η καμπύλη $X(1)$ είναι ισόμορφη με την προβολική ευθεία $\mathbb{P}^1$, και το κάλυμμα $X(N) \to X(1)$ είναι Galois με ομάδα Galois την $PSL(2,\mathbb{Z}/N\mathbb{Z})$. Ο βαθμός αυτού του καλύμματος είναι

$$\mu_N := \begin{cases} N^3/2\prod_{p|N}(1-p^{-2}) & \text{αν } N>2 \\ 6 & \text{αν } N=2 \end{cases}$$

Επιπλέον το γένος g_N της $X(N)$ είναι [23, σελ. 23]

$$g_N = 1 + \mu_N \frac{N-6}{12N}. \tag{4.1}$$

Από τον παραπάνω τύπο βλέπουμε ότι οι καμπύλες $X(2), X(3), X(4), X(5)$ είναι ρητές ενώ η $X(6)$ είναι ελλειπτική. Όλες οι άλλες καμπύλες έχουν γένος μεγαλύτερο του δύο και συνεπώς οι ομάδες αυτομορφισμών τους είναι πεπερασμένες και φραγμένες από τον τύπο του Hurwitz:

$$|Aut(X(N)| \leq 84(g_N - 1). \tag{4.2}$$

Είναι επίσης γνωστό ότι στο κάλυμμα $X(N) \to X(1)$ ακριβώς τρία σημεία του $X(1)$, διακλαδίζονται, τα $j(i), j(\omega), j(\infty)$ με δείκτες διακλάδωσης $2, 3$ και N αντίστοιχα.

Αν $PSL(2,\mathbb{Z}/N\mathbb{Z}) \lhd AutX(N)$ τότε κάθε αυτομορφισμός στην $AutX(N)$ περιορίζεται σε αυτομορφισμό της $X(1) \cong \mathbb{P}^1$, που σταθεροποιεί τρία σημεία, και συνεπώς είναι ο ταυτοτικός. Δηλαδή σε αυτή την περίπτωση έχουμε $AutX(N) \cong PSL(2,\mathbb{Z}/N\mathbb{Z})$.

Έστω m ο δείκτης της $PSL(2,\mathbb{Z}/N\mathbb{Z}) = Gal(X(N)/X(1))$ στην $AutX(N)$. Η εξίσωση (4.1) για $N \neq 2$ μπορεί να γραφεί ως

$$84(g_N - 1) = |PSL(2,\mathbb{Z}/N\mathbb{Z})| \left(7 - \frac{42}{N}\right) \tag{4.3}$$

και αυτή συνδυασμένη με την (4.2) μας δίνει τα παρακάτω φράγματα για τον δείκτη m:

$$\begin{array}{lll} m \leq 2 & \text{για} & 7 \leq N < 11 \\ m \leq 3 & \text{για} & 11 \leq N < 14 \\ m \leq 4 & \text{για} & 14 \leq N < 21 \\ m < 7 & \text{για} & 21 \leq N \end{array}. \tag{4.4}$$

Συνεπώς για $7 \leq N < 11$ έχουμε ότι $AutX(N) \cong PSL(2, \mathbb{Z}/N\mathbb{Z})$. Προκειμένου να αποδείξουμε γενικά ότι $PSL(2, \mathbb{Z}/N\mathbb{Z}) \lhd AutX(N)$ θα θεωρήσουμε την παράσταση

$$\beta : PSL(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow S_m$$

όπου $\sigma \mapsto \{\sigma a_1 PSL(2, \mathbb{Z}/N\mathbb{Z}), \sigma a_2 PSL(2, \mathbb{Z}/N\mathbb{Z}), ..., \sigma a_m PSL(2, \mathbb{Z}/N\mathbb{Z})\}$, και

$$\{a_1 PSL(2, \mathbb{Z}/N\mathbb{Z}), ..., a_m PSL(2, \mathbb{Z}/N\mathbb{Z})\}$$

είναι η διάσπαση της ομάδας $AutX(N)$ σε cosets της $PSL(2, \mathbb{Z}/N\mathbb{Z})$. Παρατηρούμε ότι $PSL(2, \mathbb{Z}/N\mathbb{Z}) \lhd AutX(N)$ αν και μόνο αν ο β είναι ο τετριμμένος ομομορφισμός.

Ας υποθέσουμε ότι $N = p$ είναι ένας πρώτος, $p \geq 7$. Αφού $PSL(2, p)$ είναι απλή ομάδα έχουμε ότι $\ker \beta$ είναι ή $PSL(2, p)$ ή $\{1\}$. Η τελευταία περίπτωση είναι αδύνατη αφού δεν υπάρχουν στοιχεία τάξης p στην S_m, για $m \leq 6$.

Ας θεωρήσουμε τώρα τις καμπύλες $X(p^e)$, όπου p είναι πρώτος, $p \geq 7$. Θεωρούμε τον παρακάτω πύργο καλυμμάτων

$$PSL(2, \mathbb{Z}/p^e\mathbb{Z}) \left\{ \begin{array}{c} \left.\begin{array}{c} X(p^e) \\ \downarrow \\ X(p) \end{array}\right\} H \\ \left.\begin{array}{c} X(p) \\ \downarrow \\ X(1) \end{array}\right\} PSL(2, p) \end{array} \right.$$

Έστω $H := Gal(X(p^e)/X(p))$, τότε $|H| = p^{3(e-1)}$, και αφού $p \geq 7$ έχουμε $H < \ker \beta$. Συνεπώς μπορούμε να ορίσουμε τον ομομορφισμό $\tilde{\beta}$

$$\tilde{\beta} : PSL(2, p) \cong PSL\,(2, \mathbb{Z}/N\mathbb{Z})/H \longrightarrow S_m.$$

Αυτό μας δίνει ότι $\tilde{\beta} = 1$ και σαφώς το ίδιο ισχύει για την β.

Έστω N θετικός ακέραιος πρώτος με τους $2, 3, 5$. Ο ομομορφισμός β είναι τετριμμένος και σε αυτή την περίπτωση, αφού

$$PSL(2, \mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_{i=1}^{s} PSL(2, \mathbb{Z}/p_i^{a_i}\mathbb{Z}),$$

όπου $N = \prod_{i=1}^{s} p_i^{a_i}$ είναι η διάσπαση του N σε γινόμενο πρώτων παραγόντων.

Προκειμένου να μελετήσουμε την περίπτωση τυχαίου N θα χρειαστούμε τα καλύτερα φράγματα για τον δείκτη m. Θεωρούμε τον πύργο καλυμμάτων

$$\begin{array}{cccc} X(N) & & & \\ \downarrow & 2\,| & 3\,| & N\,| \\ X(1) & j(i) & j(\omega) & j(\infty) \\ \downarrow & & & \\ X(N)^{AutX(N)} & & & \end{array}$$

Παρατηρούμε ότι αν $PSL(2, \mathbb{Z}/N\mathbb{Z})$ δεν είναι μία κανονική υποομάδα στην $AutX(N)$ τότε το κάλυμμα $X(1) \cong \mathbb{P}^1 \to X(N)^{AutX(N)}$ δεν είναι Galois. Από την απόδειξη του φράγματος του Hurwitz (4.2) για την ομάδα των αυτομορφισμών αλγεβρικής καμπύλης [6, σελ. 260] βλέπουμε ότι αν το πλήθος r των σημείων της $X(1)$ που διακλαδίζονται στο κάλυμμα $X(N) \to X(N)^{AutX(N)}$ είναι $r > 3$ τότε το φράγμα του Hurwitz βελτιώνεται στο

$$|AutX(N)| \leq 12(g_N - 1).$$

Αυτό μας δίνει ότι $m \leq 1$, και συνεπώς $PSL(2, \mathbb{Z}/N\mathbb{Z}) \lhd AutX(N)$, άτοπο. Συνεπώς το πλήθος των σημείων διακλάδωσης είναι $r = 3$. Ο τύπος του Hurwitz για το κάλυμμα $X(N) \longmapsto X(N)^{AutX(N)}$ δίνει την

$$2(g_N - 1) = |AutX(N)| \left(1 - \frac{1}{\nu_1} + 1 - \frac{1}{\nu_2} + 1 - \frac{1}{\nu_3} - 2\right), \tag{4.5}$$

όπου ν_i είναι οι δείκτες διακλάδωσης των σημείων που διακλαδίζονται. Ξεχωρίζουμε τις παρακάτω περιπτώσεις:

- Τα τρία σημεία $j(i), j(\omega), j(\infty)$ περιορίζονται σε διαφορετικά σημεία p_1, p_2, p_3 των οποίων οι δείκτες διακλάδωσης είναι $e(j(i)/p_1) = \kappa, e(j(\omega)/p_2) = \lambda, e(j(\infty)/p_3) = \mu$. Ή (4.5) σε αυτή την περίπτωση γράφεται

$$2(g_N - 1) = |AutX(N)| \left(1 - \frac{1}{2\kappa} + 1 - \frac{1}{3\lambda} + 1 - \frac{1}{N\mu} - 2\right) \geq$$
$$\geq |AutX(N)| (1 - 1/2 + 1 - 1/3 + 1 - 1/N - 2) \geq$$
$$\geq |AutX(N)| (1/6 - 1/N)$$

  η οποία μας δίνει και το επιθυμητό αποτέλεσμα

$$|Aut(X)| \leq \frac{12N}{N-6}(g_N - 1) = \mu_N.$$

- Κάποια από τα τρία σημεία $j(i), j(\omega), j(\infty)$ περιορίζονται στο ίδιο σημείο της $X(N)^{AutX(N)}$. Θα θεωρήσουμε την περίπτωση $11 \leq N$. Τα σημεία $j(i)$ και $j(\infty)$ δεν γίνεται να περιορίζονται στο ίδιο σημείο της $X(N)^{AutX(N)}$. Αφού το κάλυμμα $X(N) \to X(N)^{AutX(N)}$ είναι Galois θα πρέπει να έχουμε $2\kappa = N\lambda$, όμως ο βαθμός του καλύμματος $X(1) \to X(N)^{AutX(N)}$ είναι το πολύ 6, συνεπώς $\kappa \leq 6, \lambda = 1$, δηλαδή τα $j(i)$ και $j(\infty)$ δεν περιορίζονται στο ίδιο σημείο, εκτός αν $N \leq 12$. Αλλά αν $N \leq 12$ τότε $m \leq 3$, και συνεπώς $N \leq 6$, το οποίο αντιτίθεται στην αρχική υπόθεση $N \geq 11$. Με τα ίδια επιχειρήματα μπορούμε να δείξουμε ότι τα σημεία $j(\omega)$ και $j(\infty)$ περιορίζονται σε διαφορετικά σημεία του $X(N)^{AutX(N)}$.

  Ας υποθέσουμε τώρα ότι τα $j(i)$ και $j(\omega)$ περιορίζονται στο ίδιο σημείο της $X(N)^{AutX(N)}$. Θα πρέπει να υπάρχει ένα σημείο p της $X(N)^{AutX(N)}$ το οποίο διακλαδίζεται μόνο στο κάλυμμα $X(1) \to X(N)^{AutX(N)}$ με δείκτη διακλάδωσης $2 \leq \nu \leq 6$. Από τον τύπο του Hurwitz παίρνουμε

$$2(g_N - 1) = |AutX(N)| \left(1 - \frac{1}{6\psi} + 1 - \frac{1}{\phi N} + 1 - \frac{1}{\nu} - 2\right) \overset{\nu \geq 2, \psi = 1 \text{ ή } 2}{\geq}$$
$$|AutX(N)| \left(\frac{1}{3} - \frac{1}{N}\right) \overset{N \geq 11}{\geq} |AutX(N)| \left(\frac{1}{3} - \frac{1}{11}\right)$$

  το οποίο μας δίνει σε αυτή την περίπτωση

$$|AutX(N)| \leq 33/4\,(g_N - 1)$$

  το οποίο με την σειρά του δίνει το επιθυμητό αποτέλεσμα $m \leq 1$,.

Παρατήρηση 4.0.2 *Είναι ενδιαφέρον να παρατηρήσουμε ότι αφού* $X(2), X(4), X(3), X(5)$, *είναι ρητές καμπύλες, η ταξινόμηση των πεπερασμένων υποομάδων αυτομορφισμών του ρητού σώματος συναρτήσεων αποδεικνύει το γνωστό αποτέλεσμα*

$$PSL(2,2) \cong \mathbb{Z}_3, PSL(2,\mathbb{Z}/4\mathbb{Z}) \cong S_4, PSL(2,3) \cong A_4, PSL(2,5) \cong A_5$$

Κεφάλαιο 5

Ομάδες αυτομορφισμών των υπερεπιφανειών Fermat

Οι ομάδες αυτομορφισμών των μη-ιδιομόρφων υπερεπιφανειών Fermat του $\mathbb{P}^r(k)$ ορίζονται από τις εξισώσεις

$$F_{r,n} : X_0^n + ... + X_r^n = 0,$$

όπου το k, είναι αλγεβρικά κλειστό, χαρακτηριστικής $p \geq 0$. Μπορούμε να υποθέσουμε ότι $p \nmid n$, αφού αν $p \mid n$ τότε το πολυώνυμο $\sum_{\nu=0}^{r} X_\nu^n$ είναι δύναμη του p και συνεπώς οι αντίστοιχες υπερεπιφάνειες είναι ιδιόμορφες. Οι υπερεπιφάνειες αυτές έχουν μία προφανή ομάδα αυτομορφισμών που παράγεται από τους αυτομορφισμούς

$$(X_0, ..., X_r) \longmapsto (\zeta^{i_0} X_0, ..., \zeta^{i_r} X_r),\ \zeta^n = 1$$

και από την συμμετρική ομάδα S_{r+1} που μεταθέτει τις μεταβλητές X_i. Η παραπάνω ομάδα είναι ισόμορφη με το ημιευθύ γινόμενο $\mathbb{Z}_n^r \rtimes S_{r+1}$. Ο A. Weil [32] διατύπωσε την εικασία ότι η ομάδα

$$N_{r,n} := \mathbb{Z}_n^r \rtimes S_{r+1}$$

είναι η πλήρης ομάδα αυτομορφισμών των υπερεπιφανειών του Fermat .

Στην αρχή της δεκαετίας του 70, ο Leopoldt [17] μελέτησε την ομάδα αυτομορφισμών των σωμάτων συναρτήσεων του Fermat , ή ισοδύναμα τους αυτομορφισμούς των προβολικών καμπύλων $F_{2,n}$ και απέδειξε ότι η εικασία του A. Weil δεν είναι σωστή αν το $n-1$ είναι δύναμη της χαρακτηριστικής.

Ο Leopoldt δεν ενδιαφέρθηκε να δημοσιεύσει τους υπολογισμούς πριν από το 1996, και μετά από μία εργασία του Π. Τζερμιά [29], ο οποίος ανεξάρτητα από τον Leopoldt υπολόγισε τους αυτομορφισμούς των καμπύλων Fermat, στην χαρακτηριστική 0.

Το πρόβλημα της δομής της ομάδας αυτομορφισμών των $F_{n,r}$ λύθηκε από τον T.Shioda [24] το 1987. Η μέθοδος του Shioda εφαρμόζεται και στην περίπτωση των καμπύλων Fermat, και δίνει ένα τρίτο τρόπο υπολογισμού των αυτομορφισμών των καμπύλων Fermat ανεξάρτητο από τις μεθόδους των Leopoldt, Τζερμιά.

Η εργασία του Shioda μου έγινε γνωστή από τον T. Katsura και αφού η διδακτορική μου διατριβή είχε ποιά ολοκληρωθεί. Η μέθοδος υπολογισμού των αυτομορφισμών που παρουσιάζω σε αυτό το κεφάλαιο είναι μία παραλαγή της μεθόδου του Shioda. Συγκεκριμένα θα αποδείξουμε το παρακάτω

Θεώρημα 5.0.3 *Η ομάδα των γραμμικών αυτομορφισμών $G_{r,n}$ των υπερεπιφανειών Fermat $F_{r,n}$, $r \geq 2$, $n \geq 3$ είναι*

$$G_{r,n} = \begin{cases} N_{r,n} = \mathbb{Z}_n^r \rtimes S_{r+1} & \text{αν } n-1 \text{ δεν είναι δύναμη της χαρακτηριστικής} \\ PGU(r+1, p^{2h}) & \text{αν } n-1 = p^h \end{cases}$$

Επιπλέον για $n \neq r+1$ και $r \geq 4$ κάθε αυτομορφισμός του $F_{n,r}$ είναι γραμμικός.

Προκειμένου να υπολογίσουμε την ομάδα αυτομορφισμών των υπερεπιφανειών του Fermat θα αποδείξουμε πρώτα, ότι κάτω από συγκεκριμένες συνθήκες, κάθε αυτομορφισμός μίας προβολικής μη ιδιόμορφης υπερεπιφάνειας $V \subset \mathbb{P}^r(k)$ επάγεται από ένα γραμμικό αυτομορφισμό του $\mathbb{P}^r(k)$. Η απόδειξη που θα δώσουμε ακολουθεί την απόδειξη των Griffiths-Harris για μιγαδικές υπερεπιφάνειες [8, σελ. 177], και την επεκτείνει στην περίπτωση θετικής χαρακτηριστικής.

5.1 Υπολογισμοί

Πρόταση 5.1.1 *Έστω $V \subset \mathbb{P}^r(k)$ μία μη ιδιόμορφη προβολική υπερεπιφάνεια, βαθμού $n \neq r+1$, όπου k είναι ένα αλγεβρικά κλειστό σώμα χαρακτηριστικής $p \geq 0$. Αν $r \geq 4$ τότε κάθε αυτομορφισμός του V επάγεται από ένα αυτομορφισμό του $\mathbb{P}^r(k)$.*

Απόδειξη: Έστω $\mathcal{O}(1)$ το αντιστρέψιμο sheaf του $\mathbb{P}^r(k)$ που αντιστοιχεί στο hyperplane bundle, και $\mathcal{O}_V(1)$ ο περιορισμός του $\mathcal{O}(1)$ στο V. Θα συμβολίζουμε με $\mathcal{L}(-V)$ το αντιστρέψιμο sheaf που αντιστοιχεί στον divisor $-V$. Η μικρή ακριβής ακολουθία των sheaves

$$1 \longrightarrow \mathcal{O}(1) \otimes \mathcal{L}(-V) \longrightarrow \mathcal{O}(1) \longrightarrow \mathcal{O}_V(1) \longrightarrow 0,$$

επάγει την μακρά ακριβή ακολουθία στην συνομολογία

$$H^0(\mathbb{P}^r(k), \mathcal{O}(1)) \xrightarrow{r} H^0(V, \mathcal{O}_V(1)) \longrightarrow H^1(\mathbb{P}^r(k), \mathcal{O}(1-n)) \cong 0,$$

η οποία δίνει ότι ο περιορισμός r είναι επί, και συνεπώς το γραμμικό σύστημα στο V,

$$L = |H^0(V, \mathcal{O}_V(1))|$$

το οποίο επάγεται από τις τομές με υπερεπίπεδα είναι πλήρες.

Έστω $\omega_V = \bigwedge^{\dim V} \Omega_{V/k}$ το κανονικό αντιστρέψιμο sheaf του V. Έχουμε ότι [13, σελ. 183]

$$\omega_V = \mathcal{O}_V(1)^{\otimes d-n-1}.$$

Κάθε αυτομορφισμός ϕ του V αφήνει το κανονικό sheaf αναλλοίωτο, συνεπώς

$$\phi^* \omega_V = \omega_V \Rightarrow \phi^*(\mathcal{O}_V(1)^{\otimes d-n-1}) = \mathcal{O}_V(1)^{\otimes d-n-1}.$$

Το θεώρημα του Lefschetz [9], το οποίο εξασφαλίζει ότι $Pic(V) \cong \mathbb{Z}$ για $r \geq 4$, επάγει ότι

$$\phi^*(\mathcal{O}_V(1)) = \mathcal{O}_V(1)$$

και συνεπώς ϕ^* επάγει ένα αυτομορφισμό στους divisors του L, δηλαδή στο $\mathbb{P}(L) \cong \mathbb{P}^r(k)$.□

Η ομάδα των γραμμικών αυτομορφισμών είναι η υποομάδα της $PGL(r+1,k)$ η οποία αφήνει την εξίσωση $F_{r,n}$ αναλλοίωτη, δηλαδή πίνακες (a_{ij}) τέτοιες ώστε

$$\sum_{i=0}^{r} \left(\sum_{j=0}^{r} a_{ij} X_j \right)^n = \sum_{j=0}^{r} X_j^n. \tag{5.1}$$

Αντί να εργαστούμε με την $PGL(2,k)$, θα εργαστούμε με τον αφινικό κώνο της, δηλαδή με την $GL(2,k)$ η οποία είναι ένα βασικό αφινικό σύνολο, με αφινικό δακτύλιο

$$R := k[X_{ij}/i,j = 0,...,r]_{\det()^{-1}}.$$

Ο R είναι η τοπικοποίηση του πολυωνυμικού δακτυλίου σε n^2 μεταβλητές ως προς την ορίζουσα. Η εξίσωση (5.1) σε αυτή την περίπτωση γίνεται

$$\sum_{i=0}^{r}\left(\sum_{j=0}^{r} a_{ij}X_j\right)^n = c(a_{ij})\sum_{j=0}^{r} X_j^n, \tag{5.2}$$

όπου

$$c : G_{r,n} \longrightarrow k^*$$

είναι μία μονοδιάστατη παράσταση της $G_{r,n}$. Επεκτείνοντας την (5.1) χρησιμοποιόντας τον τύπο του διωνύμου παίρνουμε

$$\sum_{i=0}^{r}\sum_{n_0+\ldots+n_r=n}\binom{n}{n_0,\ldots,n_r} a_{i0}^{n_0}a_{i1}^{n_1}\cdots a_{ir}^{n_r}X_0^{n_0}X_1^{n_1}\cdots X_r^{n_r} = c(a_{ij})\sum_{j=0}^{r} X_j^n,$$

το οποίο με την σειρά του δίνει

$$\binom{n}{n_0,\ldots,n_r}\sum_{i=0}^{r} a_{i0}^{n_0}a_{i1}^{n_1}\cdots a_{ir}^{n_r} = 0 \text{ αν } n_i < n \text{ για όλα τα } i \tag{5.3}$$

και

$$\sum_{i=0}^{r} a_{i\kappa}^n = \sum_{i=0}^{r} a_{i\lambda}^n \text{ για όλα τα } \kappa,\lambda = 0,\ldots,r \tag{5.4}$$

Θέτοντας $n_\kappa = 1$, $n_\lambda = n-1$ στην (5.3) καταλήγουμε

$$\begin{aligned} n\sum_{i=0}^{r} a_{i\kappa}a_{i\lambda}^{n-1} &= 0 \text{ για } \kappa\neq\lambda \\ \sum_{i=0}^{r} a_{i\kappa}a_{i\kappa}^{n-1} &= c(a_{ij}) \end{aligned}$$

η οποία δίνει ότι

$$(a_{ij})^t(a_{ij}^{n-1}) = c(a_{ij})\cdot I \Rightarrow (a_{ij}^{n-1}) = c(a_{ij})\cdot(a_{ij})^{-1t}.$$

Συνεπώς, η ύψωση όλων των στοιχείων ενός πίνακα $(a_{ij}) \in G_{r,n}$ στην $n-1$ δύναμη, επάγει ένα μορφισμό ομάδων από την $G_{r,n}$ στην $G_{r,n}$. Σταθεροποιούμε ένα στοιχείο (b_{ij}) στην $G_{r,n}$. Για όλα τα $(a_{ij}) \in G_{r,n}$ έχουμε

$$\begin{aligned} \sum_{\nu=0}^{r} a_{i\nu}^{n-1}b_{\nu j}^{n-1} &= \left(\sum_{\nu=0}^{r} a_{i\nu}b_{\nu j}\right)^{n-1} = \\ &= \sum_{\nu=0}^{r} a_{i\nu}^{n-1}b_{\nu j}^{n-1} + \sum_{\substack{k_1+\cdots+k_r=n-1\\ k_i<n-1}}\binom{n-1}{k_1,\ldots,k_r}(a_{i0}b_{0j})^{k_0}\cdots(a_{ir}b_{rj})^{k_r} \end{aligned}$$

Συνεπώς, το πολυώνυμο

$$T_{ij}(X_{i0},\ldots,X_{ir}) := \sum_{\substack{k_1+\cdots+k_r=n-1\\ k_i<n-1}}\binom{n-1}{k_1,\ldots,k_r} b_{0j}^{k_0}\cdots b_{rj}^{k_r}X_{i0}^{k_0}\cdots X_{ir}^{k_r}$$

μηδενίζονται ταυτοτικά στο αλγεβρικό σύνολο του $\mathbb{A}^{n^2+1}(k)$, που ορίζεται από (5.3) και (5.4). Από το θεώρημα Nullstellensatz του Hilbert έχουμε ότι για κάποιο ακέραιο μ

$$T_{ij}^{\mu} \in I,$$

όπου I είναι το ιδεώδες του R που γεννάται από τα πολυώνυμα

$$f_{n_0,\ldots,n_r} := \binom{n}{n_0,\ldots,n_r} \sum_{i=0}^{r} X_{i0}^{n_0} X_{i1}^{n_1} \cdots X_{ir}^{n_r}$$

και

$$f_{\kappa,\lambda} := \sum_{i=0}^{r} X_{i\kappa}^{n} - \sum_{i=0}^{r} X_{i\lambda}^{n}$$

Θα αποδείξουμε, ότι το παραπάνω είναι αδύνατον εκτός αν $T_{ij} = 0$. Πράγματι, υποθέτουμε ότι για κατάλληλα πολυώνυμα $g_{n_0,\ldots,n_r} \in R$ έχουμε

$$T_{ij}^{\mu} = \sum_{n_0,\ldots,n_r} g_{n_0,\ldots,n_r} \cdot f_{n_0,\ldots,n_r} + \sum_{\kappa,\lambda} g_{\kappa,\lambda} \cdot f_{\kappa,\lambda}.$$

Παρατηρούμε ότι T_{ij}^{μ} είναι ένα ομογενές πολυώνυμο βαθμού $(n-1)\mu$ στις n μεταβλητές $X_{i0},\ldots,X_{ir}$.

Έστω a ένας μονωνυμικός προσθεταίος κάπου $g_{n_0,\ldots,n_r}$ ή $g_{\kappa,\lambda}$ βαθμού $\neq (n-1)\mu - n$. Το πολυώνυμο $a \cdot f_{n_0,\ldots,n_r}$ απαλλοίφεται από γινόμενα μονωνυμικών προσθεταίων άλλων πολυωνύμων $g_{n_0',\ldots,n_r'}$ ή $g_{\kappa',\lambda'}$ με $f_{n_0',\ldots,n_r'}$ ή $f_{\kappa',\lambda'}$. Συνεπώς μπορούμε να υποθέσουμε ότι $g_{n_0,\ldots,n_r}$ είναι ομογενή βαθμού $(n-1)\mu - n$.

Από την άλλη, αφού τα T_{ij} είναι ομογενή πολυώνυμα στις n-μεταβλητές $X_{i0},\ldots,X_{ir}$ μόνο, θα πρέπει να υπάρχει ένα ομογενές μονώνυμο a βαθμού $(n-1)\mu - n$ μόνο στις $X_{i0},\ldots,X_{ir}$ μεταβλητές, το οποίο είναι προσθεταίος κάποιου από τα $g_{n_0,\ldots,n_r}$ ή $g_{\kappa,\lambda}$. Ας υποθέσουμε πρώτα ότι το a είναι ένας προσθεταίος κάποιου $g_{n_0,\ldots,n_r}$. Οι όροι $a \cdot X_{j_0}^{n_0} X_{j_1}^{n_1} \cdots X_{j_r}^{n_r}$ $j \neq i$ μπορούν να διαγραφούν μόνο αν το a είναι ένας προσθεταίος κάποιου $f_{n_0,\ldots,n_r}$ το οποίο συμβαίνει μόνο στην περίπτωση $(n-1)\mu - n = n \Rightarrow \mu = 2\frac{n}{n-1}$, άτοπο αφού $n \geq 3$. Το ίδιο επιχείρημα δείχνει ότι το a δεν μπορεί να είναι προσθεταίος ούτε κάποιου $g_{\kappa,\lambda}$.

Οι πίνακες (b_{ij}) στο $N_{r,n}$, οι οποίοι είναι προφανείς λύσεις της (5.3) και (5.4), είναι της μορφής

$$b_{ij} = \lambda \zeta^{i} \delta_{i,\sigma(j)},$$

όπου $\zeta^n = 1$, λ είναι μία μη μηδενική σταθερά και σ είναι μία μετάθεση του S_{r+1}. Υποθέτουμε ότι υπάρχει ένα $(b_{ij}) \in G_{r,n} \backslash N_{r,n}$ συνεπώς υπάρχει ένα $j \in \{0,\ldots,r\}$ τέτοιο ώστε

$$b_{i_1 j} \neq 0 \text{ και } \; b_{i_2 j} \neq 0 \text{ για } j_1, j_2 \in \{0,\ldots,r\}.$$

$T_{ij} = 0$ συνεπώς

$$\binom{n-1}{k_1,\ldots,k_r} b_{0j}^{k_0} b_{1j}^{k_1} \cdots b_{rj}^{k_r} = 0.$$

Στον παραπάνω τύπο θέτουμε $k_{i_1} = \nu$, $k_{i_2} = n - \nu - 1$, και αφού $b_{i_1 j} \neq 0, b_{i_2 j} \neq 0$ έχουμε ότι $\binom{n-1}{\nu} = 0$ για όλα τα $\nu = 1,\ldots,n-2$ το οποίο δίνει [5, σελ. 352] τότε $n-1$ είναι μία δύναμη της χαρακτηριστικής. Συνεπώς, όταν $n-1$ δεν είναι δύναμη της χαρακτηριστικής $G_{r,n} = N_{r,n}$.

Στην περίπτωση $n - 1 = p^h$, η (5.1) δίνει

$$\sum_{i=0}^{r} \sum_{j=0}^{r} \sum_{\nu=0}^{r} a_{ij}^{p^h} a_{i\nu} X_j^{p^h} X_\nu = \sum_{i=0}^{r} X_j^n. \tag{5.5}$$

Συγκρίνοντας συντελεστές και στα δύο μέλη της (5.5) παίρνουμε

$$\sum_{i=0}^{r} a_{ij}^{p^h} a_{i\nu} = \delta_{j\nu}. \tag{5.6}$$

Έστω F ο αυτομορφισμός του Frobenius, ο οποίος στέλνει τον πίνακα $A = (a_{ij})$ στον $F(A) = (a_{ij}^{p^h})$. Η εξίσωση (5.6) μας δίνει ότι

$$F(A) \cdot A^t = I, \tag{5.7}$$

και

$$A \cdot F(A)^t = I. \tag{5.8}$$

Εφαρμόζοντας τον F και στα δύο μέλη της (5.7) πέρνουμε

$$F^2(A) \cdot F(A)^t = I,$$

ενώ από την (5.8) έχουμε ότι $F^2(A) = A$. Συνεπώς η ομάδα αυτομορφισμών ταυτίζεται με την $PGU(r+1, p^{2h})$ αν $n - 1 = p^h$.

Βιβλιογραφία

[1] Accola R. D.M. *Strongly Branched Coverings of Closed Riemann Surfaces* Proc. Amer. Math. Soc. **26** (1970), 315–322,

[2] Arbarello E. - Cornalba M., *Footnotes to a Paper of Beniamino Segre,* Math. Ann. 341-362 (1981)

[3] Brandt R. *Über die Automorphismengruppen von algebraischen Funktionenkörper,* PhD Thesis, Universität-Gesamthochschule Essen 1988.

[4] Brandt R., Stichtenoth H. *Die Automorphismengruppen hyperelliptischer Kurven,* manuscripta math. **55** (1986), 83-92.

[5] Eisenbud D. *Commutative Algebra* Springer Verlag, New York 1994

[6] Farkas H. M. and Kra I. , *Riemann surfaces*, Second edition, Springer-Verlag, New York, New York, 1992

[7] Gonzalez Victor - Rodriguez Rubi *On Automorphism of Curves and Linear Series*, Complex Geometry Seminar (vol III). Chile 1994

[8] Griffiths P. Harris J., *Principles of Algebraic Geometry,* Wiley Classics Library Edition, New York 1994

[9] Grothendieck, A. *Séminaire de Géométrie Algébrique 2, Cohomologie Locale des Faisceaux Cohérent et Théorèmes de Lefschetz Locaux et Globaux,* North-Holland, Amsterdam (1968)

[10] Henn H.W. *Funktionenkörper mit großer Automorphismengruppe* , J. Reine Angew. Math. **302** (1978), 96-115 .

[11] Hartshorne R., *Algebraic Geometry,* Graduate Texts in Mathematics, Springer Verlag, New York 1977.

[12] Hasse, H. *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper,* J. Reine Angewandte Math. 172, 37-54 (1934)

[13] Hasse H. *Zahlentheorie* , Akademie-Verlag, Berlin 1969.

[14] Huppert B., *Endliche Gruppen I* , Grundlehren der Mathematischen Wissenschaften, Band **134,** Springer-Verlag, Berlin 1967.

[15] Jacobson N. *Basic algebra. II*, Second edition, W. H. Freeman and Company, New York, New York, 1989

[16] Klassen M.J., Schaefer E.F. *Arithmetic and geometry of the curve* $y^3 + 1 = x^4$, Acta Arithmetika LXXIV.3 (1996), 241-257.

[17] Leopoldt H.W. *Über die Automorphismengruppe des Fermatkörpers* , Journal of Number Theory **56** (1996), 256-282.

[18] Magma Algebra System, Computational Algebra Group, University of Sydney. `http://www.maths.usyd.edu.au:8000/u/magma/`

[19] Namba M. *Equivalence problem and automorphism groups of certain compact Riemann surfaces,* Tsukuba J. Math. 5 Nr. 2 319-338 (1981).

[20] Serre J.P., *Local Fields* , Graduate Texts in Mathematics 67, Springer-Verlag, New York, 1979.

[21] Serre J.P., Letter to Prof. Ribet 1996.

[22] Schmidt F.K. *Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern* Math. Z. **45**, (1939),62-74

[23] Shimura G. *Introduction to the Arithmetic Theory of Automorphic Functions,* Publications of the Mathematical Society of Japan, Princeton University Press 1971

[24] Shioda, T. *Arithmetic and Geometry of Fermat Curves,* Proc. of the Algebraic Geometry Seminar, Singapore 1987

[25] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986

[26] Stichtenoth H. *Algebraic Function Fields and Codes* , Universitext, Springer-Verlag, Berlin 1993.

[27] Stichtenoth Henning *Algebraische Funktionenkörper einer Variablen*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen 1978

[28] Towse C.W. *Weierstrass Points on Cyclic Covers of the Projective Line* , Ph.D. Thesis, Brown University, Brown (1993).

[29] Tzermias P. *The Group of Automorphisms of the Fermat Curve* , Journal of Number Theory **53,** (1995), 173-178.

[30] Valentini C. R. - Madan L. M. *A Hauptsatz of L.E. Dickson and Artin-Schreier extensions* J. Reine Angewandte Math. 318, 156-177 (1980)

[31] Weil A. *Sommes de Jacobi et charactères de Hecke,* Ouevres Scentifiques, Collected Papers Vol. III, p 329-342 Springer-Verlag, New York-Heidelberg, 1979.

[32] Weiss E. *Cohomology of Groups* , Academic Press, New York 1969.