Πολυώνυμα και Θεωρια Galois

Ανθή Ζερβού

Επιβλέπων Καθηγητής

Ιωάννης Α. Αντωνιάδης

Πτυχιακή εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης

Περιεχόμενα

Εισαγωγή

Έστω K σώμα με $chK \neq 2$ και $f(X) \in K[X]$ ένα διαχωρίσιμο πολυώνυμο με $degf(X) = n$. Είναι γνωστό ότι, αν το $f(X)$ είναι ανάγωγο υπέρ το σώμα K, τότε η ομάδα Galois $Gal(f(X)/K)$ είναι μία transitive υποομάδα της συμμετρικής ομάδας S_n. Ένα σημαντικό πρόβλημα της θεωρίας Galois είναι ο υπολογισμός της ομάδας Galois ενός δοθέντος πολυωνύμου. Για πολυώνυμα 3ου και 4ου βαθμού η απάντηση δίνεται στα πλαίσια ενός σχετικού μεταπτυχιακού μαθήματος και είναι η εξής:

Θεώρημα. *Έστω K σώμα με $chK \neq 2$ και $f(X)$ ένα ανάγωγο, διαχωρίσιμο πολυώνυμο 3ου βαθμού στο $K[X]$. Τότε:*
1) Άν η διακρίνουσα του $f(X)$, $disk(f)$, είναι τέλειο τετράγωνο στο K, τότε η ομάδα Galois του $f(X)$ υπέρ το K είναι η A_3.
2) Άν η διακρίνουσα του $f(X)$, $disk(f)$, δεν είναι τέλειο τετράγωνο στο K, τότε η ομάδα Galois του $f(X)$ υπέρ το K είναι η S_3.

Θεώρημα. *Έστω $f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ ένα ανάγωγο και διαχωρίσιμο πολυώνυμο 4ου βαθμού, και F το σώμα ανάλυσης του $f(X)$ υπέρ το K. Η κυβική επιλύουσα (cubic resolvent) του $f(X)$ είναι το πολυώνυμο 3ου βαθμού $r(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd)$ και έστω L το σώμα ανάλυσης του $r(X)$ υπέρ το K. Υποθέτουμε ότι $[L : K] = m$. Τότε:*
1) $r(X)$ είναι ανάγωγο υπέρ το K και η διακρίνουσα του $f(X)$, $disk(f)$, δέν είναι τέλειο τετράγωνο στο K αν και μόνο αν $m = 6$. Τότε η ομάδα Galois $Gal(f(X)/K) \cong S_4$.
2) $r(X)$ είναι ανάγωγο υπέρ το K και η διακρίνουσα του $f(X)$, $disk(f)$, είναι τέλειο τετράγωνο στο K αν και μόνο αν $m = 3$. Τότε η ομάδα Galois $Gal(f(X)/K) \cong A_4$.
3) Το $r(X)$ αναλύεται πλήρως υπέρ το K αν και μόνο αν $m = 1$. Τότε, η ομάδα Galois $Gal(f(X)/K) \cong V$, όπου V είναι η ομάδα του Klein.
4) Το $r(X)$ έχει μοναδική ρίζα $t \in K$ και $h(X) = (X^2 - tX + d)(X^2 + aX + (b - t))$ αναλύεται υπέρ το L αν και μόνο αν $m = 2$. Τότε η ομάδα Galois $Gal(f(X)/K) \cong \mathbb{Z}/4\mathbb{Z}$.

5) Το $r(X)$ έχει μοναδική ρίζα $t \in K$ και $h(X)$ δεν αναλύεται υπέρ το L αν και μόνο αν $m = 2$. Τότε η ομάδα Galois $Gal(f(X)/K) \cong D_4$, όπου D_4 είναι η διεδρική ομάδα.

Βέβαια θα επιθυμούσαμε να έχουμε αποτελέσματα γενικά, για κλάσεις πολυωνύμων και όχι για ένα συγκεκριμένο πολυώνυμο. Εδώ τα πράγματα είναι πολύ πιο δύσκολα. Η πιο απλή περίπτωση είναι όταν το πολυώνυμο είναι διώνυμο. Επειδή θα πρέπει το πολυώνυμο να είναι ανάγωγο, κατ' ανάγκη θα είναι της μορφής $f(X) = X^n - \alpha \in K[X]$, $n \in \mathbb{N}$.

Στο πρώτο κεφάλαιο της παρούσης εργασίας μελετάται αναλυτικά η θεωρία των διωνυμικών πολυωνύμων. Εξετάζονται κριτήρια αναγωγιμότητας και υπολογίζεται η ομάδα Galois αυτών. Ακολουθεί ένας χαρακτηρισμός για το πότε η ομάδα αυτή είναι αβελιανή. Επίσης, στο τέλος της παραγράφου μελετάται η αλγεβρική ανεξαρτησία αρρήτων αριθμών.
Στο δεύτερο κεφάλαιο ορίζεται η έννοια της πρώτης συνομολογίας πεπερασμένων ομάδων και αποδεικνύεται το Θεώρημα 90 του Hilbert. Τα αποτελέσματα αυτά είναι χρήσιμα στο επόμενο κεφάλαιο.
Στο επόμενο κεφάλαιο μελετώνται αναλυτικά οι επεκτάσεις του Kummer. Έστω F σώμα το οποίο για κάποιο φυσικό n, περιέχει τις n-ρίζες τις μονάδας. Η επέκταση K/F θα λέγεται n-επέκταση Kummer του F όταν είναι Galois, η ομάδα Galois είναι αβελιανή και $exp(G) \mid n$. Μία επέκταση K/F θα λέγεται επέκταση Kummer όταν είναι n-επέκταση Kummer για κάποιο φυσικό αριθμό n. Δίνεται ένας χαρακτηρισμός των επεκτάσεων αυτών. Για τον σκοπό αυτών χρησιμοποιείται η έννοια της διγραμμικής σύζευξης.
Η αμέσως επόμενη των διωνυμικών κλάση πολυωνύμων είναι αυτή των τριωνύμων. Πρόκειται για ανάγωγα πολυώνυμα της μορφής $X^n + aX^l + b \in K[X]$, $n, l \in \mathbb{N}$, $n > l > 0$. Η μελέτη αυτών των πολυωνύμων χρησιμοποιεί αρκετά πιο προχωρημένα εργαλεία, κυρίως Θεωρίας Αριθμών, και ως εκ τούτου δεν ενδείκνυται ως θέμα πτυχιακής εργασίας. Για λόγους πληρότητας όμως αναφέρουμε μερικά σχετικά αποτελέσματα, χωρίς αποδείξεις στο Παράρτημα.
Στο 4ο κεφάλαιο μελετάται η ομάδα Galois μιας κλάσεως πολυωνύμων, αυτών που ονομάζονται reciprocal. Για την μελέτη τους απαιτούνται προχωρημένες γνώσεις θεωρίας ομάδων όπως ημι-ευθύ γινόμενο ομάδων και wreath γινόμενα. Πρόκειται, για μία αρκετά γενική και ενδιαφέρουσα κλάση η οποία περιέχει τα κυκλοτομικά πολυώνυμα καθώς και τα L-πολυώνυμα της Ζήτα συνάρτησης αλγεβρικών καμπυλών ορι-

σμένων σε κάποιο πεπερασμένο σώμα.
Ως γνωστό, το αντίστροφο πρόβλημα της θεωρίας του Galois αναφέρεται στην ύπαρξη Galois επέκτασης $K/\mathbb{Q}$ της οποίας η ομάδα Galois είναι ισόμορφη προς δοθείσα πεπερασμένη ομάδα. Πρώτος ο Hilbert απέδειξε ότι η συμμετρική ομάδα S_n για κάθε $n \in \mathbb{N}$ είναι υλοποιήσιμη ως ομάδα Galois υπέρ το σώμα των ρητών αριθμών. Η απόδειξη του όμως ήταν υπαρξιακή (Γίνεται χρήση του λεγόμενου, Hilbert irreducibility theorem). Στις αρχές της δεκαετίας του 1930 ο I. Schur έδωσε παραδείγματα κλάσεων πολυωνύμων με ομάδα Galois υπέρ το $\mathbb{Q}$ την A_n ή την S_n $(n \in \mathbb{N})$. Μία απο αυτές τις κλάσεις είναι η κλάση των εκθετικών πολυωνύμων του Taylor.
Στα 1987 ο R.Coleman έδωσε για την κλάση αυτή των πολυωνύμων μία διαφορετική απόδειξη. Στο 5ο κεφάλαιο παρουσιάζουμε την απόδειξη του Coleman. Χρησιμοποιεί ένα θεώρημα θεωρίας ομάδων του Camille Jordan (βλ. θεώρημα 5.0.2), το αξίωμα του Bertrand (βλ. Παράρτημα Δ΄) και το p-αδικό πολύγωνο του Newton (βλ. Παράρτημα Ε΄).

Ηράκλειο, 15/6/2015

Κεφάλαιο 1

Ομάδα Galois διωνυμικών πολυωνύμων

Θα μελετήσουμε τα διώνυμα (binomials) προσδιορίζοντας συνθήκες που χαρακτηρίζουν την αναγωγιμότητα και διαχωρισιμότητα του διωνύμου της μορφής $X^n - u \in \mathbb{Q}[X]$ και θα υπολογίσουμε την ομάδα Galois αυτών.
Ειδικότερα αποδεικνύεται οτι, εάν $p_1, \ldots, p_m$ είναι διακριτοί πρώτοι αριθμοί τότε ο βαθμός της επέκτασης $\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$ υπέρ το $\mathbb{Q}$ είναι n^m, δηλαδή $[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}] = n^m$.Αυτό συνεπάγεται ότι το σύνολο των γινομένων της μορφής $\sqrt[n]{p_1^{e(1)}} \cdots \sqrt[n]{p_m^{e(m)}}$, όπου $0 \leq e(i) \leq n-1$, είναι γραμμικά ανεξάρτητο πάνω απ' το $\mathbb{Q}$. Για παράδειγμα, οι αριθμοί $1, \sqrt[4]{3} = \sqrt[60]{3^{15}}$, $\sqrt[5]{4} = \sqrt[60]{2^{24}}$, $\sqrt[6]{72} = \sqrt[60]{2^{30}3^{20}}$ είναι της παραπάνω μορφής όπου $p_1 = 2$ kai $p_2 = 3$. Οπότε, οποιαδήποτε έκφραση της μορφής $\alpha_1\sqrt[4]{3} + \alpha_2\sqrt[5]{4} + \alpha_3\sqrt[6]{72}$ με $\alpha_i \in \mathbb{Q}$ είναι άρρητη, εκτός αν $\alpha_i = 0$ για $i = 1, 2, 3$.

Συμβολισμός:
Το F θα συμβολίζει σώμα. Εάν $u \in F$ τότε $u^{1/n}$ συμβολίζει μια ειδική (σταθερή) ρίζα του διωνύμου $X^n - u \in F[X]$. Με Ω_n θα συμβολίζουμε το σύνολο των n-οστών ριζών της μονάδας και με ω_k θα συμβολίζουμε μία πρωταρχική k-ρίζα της μονάδας.

1.1 Αναγωγιμότητα

Ας θυμηθούμε πρώτα κάποια στοιχεία που ισχύουν γενικά.
Έστω $F < E$ πεπερασμένη επέκταση σωμάτων και $\alpha \in E$. Αφού η επέ-

κταση Ε υπέρ το F είναι πεπερασμένη, δηλαδή $[E : F] < \infty$, η επέκταση Ε υπέρ το F είναι αλγεβρική. Συνεπώς και το α είναι αλγεβρικό υπέρ το F.
Έστω $f(X) = Irr(\alpha, F) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in F[X]$ το ανάγωγο πολυώνυμο του α πάνω απο το F και $r_1, \ldots, r_d$ οι ρίζες του $f(X)$ (σε κάποια αλγεβρική θήκη του F).
Ορίζουμε:

$$N(\alpha) = \prod_{i=1}^{d} r_i = (-1)^d a_0, \text{ όπου } N := N_{F(\alpha)/F}$$

Προφανώς, $N(\alpha) \in F$.
Επίσης, για κάθε $\beta \in F(\alpha)$ και $a \in F$, ισχύουν τα εξής:
1) Η νόρμα είναι πολλαπλασιαστική, δηλαδή για κάθε $\beta, \gamma \in E$ ισχύει

$$N(\beta\gamma) = N(\beta)N(\gamma)$$

Ειδικότερα, ισχύει οτι $N(\beta^n) = N(\beta)^n$, $\forall n \in \mathbb{Z}_+$ και $N(1) = 1$
2) Για $a \in F$ ισχύει ότι

$$N(a\beta) = a^d N(\beta)$$

Συνεπώς, $N(a) = a^d$
3) Αν $F < E < L$ πεπερασμένες επεκτάσεις σωμάτων και $\alpha \in L$ τότε

$$N_{L/F}(\alpha) = N_{E/F}(N_{L/E}(\alpha))$$

Ο καθορισμός της αναγωγιμότητας του διωνύμου $f(X) = X^n - u$, με $u \in F$, είναι μία επαγωγική τεχνική. Θα ξεκινήσουμε με την περίπτωση που $n = p$ με p πρώτο αριθμό.

Θεώρημα 1.1.1. *Έστω p πρώτος αριθμός και F σώμα. Τα ακόλουθα είναι ισοδύναμα:*
1) $u \notin F^p$, όπου $u \in F$, $F^p = \{\alpha^p | \alpha \in F\}$
2) Το $f(X) = X^p - u$ δεν έχει ρίζες στο F
3) Το $f(X) = X^p - u$ είναι ανάγωγο υπέρ το F

Απόδειξη. $''(1) \Rightarrow (2)''$ Έστω $u \notin F^p$. Θα δείξουμε ότι το $f(X) = X^p - u$ δέν έχει ρίζες στο F. Έστω ότι το $f(X) = X^p - u$ έχει ρίζα στο F, δηλαδή υπάρχει $\alpha \in F$ τ.ω $f(\alpha) = 0$. Δηλαδή, $f(\alpha) = 0 \Rightarrow \alpha^p - u = 0 \Rightarrow u = \alpha^p \in F^p$. Άτοπο, αφού απο υπόθεση έχουμε ότι $u \notin F^p$. Άρα το $f(X)$ δεν έχει ρίζα στο F.
$''(2) \Rightarrow (1)''$ Έστω ότι το $f(X) = X^p - u$ δέν έχει ρίζες στο F. Θα δείξουμε

ότι, $u \notin F^p$. Άν $u \in F^p$ τότε συνεπάγεται ότι υπάρχει $\alpha \in F$ τ.ω $u = \alpha^p$. Δηλαδή, $\alpha^p - u = 0$. Δηλαδή, το $\alpha \in F$ είναι ρίζα του $f(X) = X^p - u$. Άτοπο, αφού το $f(X)$ δεν έχει ρίζες στο F.
$''(1) \Rightarrow (3)''$ Έστω ότι $u \notin F^p$. Θα δείξουμε ότι το $f(X) = X^p - u$ είναι ανάγωγο στο F. Έστω ότι α είναι ρίζα του $f(X) = X^p - u$ στο $\bar{F}$, όπου $\bar{F}$ είναι αλγεβρική θήκη του F. Προφανώς $[F(\alpha) : F] = d \leq p$. Θα δείξουμε ότι $d = p$. Εξ' υποθέσεως έχουμε ότι το α είναι ρίζα του $f(X) = X^p - u$. Άρα, $\alpha^p - u = 0 \Rightarrow u = \alpha^p$. Εφαρμόζοντας την norm $N = N_{F(\alpha)/F}$, προκύπτει ότι: $N_{F(\alpha)/F}(\alpha^p) = N_{F(\alpha)/F}(u)$. Δηλαδή, $N(\alpha^p) = N(u)$. Έχουμε ότι $u \in F$, και $[F(\alpha) : F] = d$. Άρα, σύμφωνα με τον ορισμό της $N = N_{F(\alpha)/F}$, έχουμε ότι: $N_{F(\alpha)/F}(u) = u^{[F(\alpha):F]} = u^d$, δηλαδή $N(u) = u^d$. Ακόμα ισχύει ότι $N(\alpha^p) = (N(\alpha))^p$. Δηλαδή $(N(\alpha))^p = u^d$, όπου $N(\alpha) \in F$. Άν $d < p$, δηλαδή $d \in \{1, 2, \ldots, p-1\}$, τότε ΜΚΔ(d,p)=1. Άρα, υπάρχουν $t, s \in \mathbb{Z}$ τ.ω $dt + sp = 1$. Συνεπώς, $u = u^1 = u^{dt+sp} = u^{dt}u^{sp} = (N(\alpha))^{pt}u^{sp} = (N(\alpha)^t u^s)^p$ και ισχύει ότι $(N(\alpha)^t u^s)^p \in F$, διότι το F είναι σώμα. Άρα, $u \in F^p$. Άτοπο, αφού από την υπόθεση έχουμε ότι $u \notin F^p$. Επομένως, $d = p$. Ακόμα, αφού $degf(X) = p$, τότε προκύπτει ότι $f(X) = Irr(\alpha, F)$. Συνεπώς, το $f(X)$ είναι ανάγωγο υπέρ το F.
$''(3) \Rightarrow (2)''$ Έστω ότι το $f(X) = X^p - u$ είναι ανάγωγο υπέρ το F. Θα δείξουμε ότι το f(X) δεν έχει ρίζες στο F. Προφανώς, αφού το f(X) είναι ανάγωγο υπέρ το F, τότε συνεπάγεται ότι το f(X) δεν έχει ρίζες στο F. □

Ας εξετάσουμε την γενική περίπτωση όπου ο εκθέτης δέν είναι πρώτος. Υποθέτουμε ότι $n = p_0 \cdots p_{t-1}$ όχι κατ' ανάγκη διακριτοί περιττοί πρώτοι αριθμοί. Θα εξετάσουμε αργότερα την περίπτωση όπου η ανάλυση του n σε πρώτους παράγοντες περιέχει άρτιο πρώτο παράγοντα.

Θεώρημα 1.1.2. *Έστω $n = p_0 \cdots p_{t-1}$, με $p_0, \ldots, p_{t-1}$ όχι αναγκαστικά διακριτοί περιττοί πρώτοι αριθμοί. Τότε, το διώνυμο $f(X) = X^n - \alpha_0 \in F(X)$ είναι ανάγωγο αν $\alpha_0 \notin F^{p_i}$, για κάθε $i = 0, \ldots, t-1$.*

Απόδειξη. Έστω β μία ρίζα του f(X) στο $\bar{F}$ και υποθέτουμε ότι $n = p_0 m_0$. Τότε $f(X) = (X^{m_0})^{p_0} - \alpha_0$. Αφού, β είναι ρίζα του f(X), προκύπτει ότι το $\alpha_1 = \beta^{m_0}$ είναι ρίζα του $h(X) := X^{p_0} - \alpha_0$. Προφανώς, το β είναι και ρίζα του $g_0(X) = X^{m_0} - \alpha_1$ υπέρ του $F(\alpha_1)$. Οπότε, προκύπτει η εξής αλυσίδα σωμάτων:

$$F = F(\alpha_0) \leq F(\alpha_1) \leq F(\beta)$$

Επαναλαμβάνουμε την παραπάνω διαδικασία για το $g_0(X)$. Άν $m_0 = p_1 m_1$ τότε έχουμε $g_0(X) = (X^{m_1})^{p_1} - \alpha_1$. Οπότε, το $\alpha_2 = \beta^{m_1}$ είναι ρίζα

του $h_2(X) := X^{p_1} - \alpha_1$. Επομένως, το β είναι ρίζα του $g_1(X) = X^{m_1} - \alpha_2$ στο $F(\alpha_2)$. Άρα, προκύπτει η παρακάτω αλυσίδα σωμάτων:

$$F(\alpha_0) \leq F(\alpha_1) \leq F(\alpha_2) \leq F(\beta)$$

Στην συνέχεια, επαναλαμβάνοντας την παραπάνω διαδικασία μετά απο πεπερασμένο πλήθος βημάτων, προκύπτει η εξής αλυσίδα σωμάτων:

$$F(\alpha_0) \leq F(\alpha_1) \leq \ldots \leq F(\alpha_t) = F(\beta)\,, \text{όπου}\, \beta = \alpha_t$$

και κάθε επέκταση $F(\alpha_i)/F(\alpha_{i+1})$ έχει την ιδιότητα ότι το α_{i+1} είναι ρίζα του διωνύμου $X^{p_i} - \alpha_i$ και η επέκταση του $F(\alpha_{i+1})/F(\alpha_i)$ έχει βαθμό ίσο με πρώτο αριθμό.
Ισχυριζόμαστε ότι, το διώνυμο $f(X) = X^n - \alpha_0$ είναι ανάγωγο άν και μόνο άν $[F(\beta) : F] = n = p_0 \cdots p_{t-1}$ άν και μόνο άν κάθε διώνυμο της μορφής $X^{p_i} - \alpha_i$ είναι ανάγωγο. Όμως, σύμφωνα με το Θεώρημα 1.1.1, ισχύει ότι κάθε διώνυμο $X^{p_i} - \alpha_i$ είναι ανάγωγο υπέρ το $F(\alpha_i)$, με $p_i \in \mathbb{P}$ άν και μόνο άν $\alpha_i \notin F(\alpha_i)^{p_i}$. Άρα, κάθε διώνυμο $X^{p_i} - \alpha_i$ είναι ανάγωγο άν και μόνο άν

$$\alpha_i \notin F(\alpha_i)^{p_i}, \text{ για κάθε } i = 0, \ldots, t-1 \tag{1.1}$$

Θα αποδείξουμε τις παραπάνω ισοδυναμίες. Αρχικά, αν $\alpha_i \in F(\alpha_i)^{p_i}$, δηλαδή $\alpha_i = \gamma^{p_i}$, με $\gamma \in F(\alpha_i)$, τότε ισχύει ότι:
$N_{F(\alpha_i)/F(\alpha_0)}(\alpha_i) = N_{F(\alpha_i)/F(\alpha_0)}(\gamma^{p_i}) = (N_{F(\alpha_i)/F(\alpha_0)}(\gamma))^{p_i} \in F^{p_i}$,
αφού $N_{F(\alpha_i)/F(\alpha_0)}(\gamma) \in F$. Από την εξίσωση 1.1 έχουμε ότι: $\alpha_i \notin F(\alpha_i)^{p_i}$, $\forall i = 0, \ldots, t-1$. Οπότε, σύμφωνα με τα παραπάνω έχουμε ότι

$$N_{F(\alpha_i)/F(\alpha_0)}(\alpha_i) \notin F^{p_i}, \text{ για κάθε } i = 0, \ldots, t-1 \tag{1.2}$$

Επομένως, σύμφωνα με αυτές τις συνθήκες κάθε διώνυμο $X^{p_i} - \alpha_i$ είναι ανάγωγο και το α_{i+1} είναι ρίζα του $X^{p_i} - \alpha_i$. Άρα,

$$N_{F(\alpha_{i+1})/F(\alpha_i)}(\alpha_{i+1}) = -(-1)^{p_i}\alpha_i \ \text{ για } i = 0, \ldots, t-1 \tag{1.3}$$

Άν υποθέσουμε ότι όλοι οι πρώτοι p_i είναι περιττοί ή ότι $ch(F) = 2$, τότε η εξίσωση 1.3 γράφεται ως εξής:

$$N_{F(\alpha_{i+1})/F(\alpha_i)}(\alpha_{i+1}) = \alpha_i \text{ για } i = 0, \ldots, t-1 \tag{1.4}$$

Για i=1, η εξίσωση 1.4 γράφεται: $N_{F(\alpha_2)/F(\alpha_1)}(\alpha_2) = \alpha_1$.
Αλλά έχουμε ότι $F(\alpha_0) \leq F(\alpha_1) \leq F(\alpha_2)$. Συνεπώς,

$$N_{F(\alpha_2)/F(\alpha_0)}(\alpha_2) = N_{F(\alpha_1)/F(\alpha_0)}(N_{F(\alpha_2)/F(\alpha_1)}(\alpha_2)) \ = \ N_{F(\alpha_1)/F(\alpha_0)}(\alpha_1) = \alpha_0$$

Γενικά, άν $N_{F(\alpha_i)/F(\alpha_0)}(\alpha_i) = \alpha_0$, τότε εφαρμόζοντας την norm στην σχέση 1.4 προκύπτει ότι:

$$N_{F(\alpha_{i+1})/F(\alpha_0)}(\alpha_{i+1}) = N_{F(\alpha_i)/F(\alpha_0)}(N_{F(\alpha_{i+1})/F(\alpha_i)}(\alpha_{i+1})) \overset{1.4}{=} N_{F(\alpha_i)/F(\alpha_0)}(\alpha_i) = \alpha_0$$

Δηλαδή, $N_{F(\alpha_{i+1})/F(\alpha_0)}(\alpha_{i+1}) = \alpha_0$, $\forall i = 0, \ldots, t-1$. Επομένως, αφού έχουμε ότι $N_{F(\alpha_i)/F(\alpha_0)}(\alpha_i) \notin F^{p_i}$, $\forall i = 0, \ldots, t-1$,τότε προκύπτει ότι $\alpha_0 \notin F^{p_i}$, $\forall i = 0, \ldots, t-1$. Συνεπώς, δείξαμε ότι το $f(X) = X^n - \alpha_0$ είναι ανάγωγο αν $\alpha_0 \notin F^{p_i}$, $\forall i = 0, \ldots, t-1$

□

Στήν συνέχεια θα εξετάσουμε την περίπτωση όπου $n = 2^s$. Έστω $f_s(X) = X^{2^s} - u$, με $u \in F$. Ο άρτιος πρώτος p=2 προκαλεί πολλά προβλήματα σε αυτήν την περίπτωση. Αυτό φαίνεται απο το εξής: Άν $b \in \mathbb{Q}, b \neq 0$, τότε για οποιοδήποτε $s \geq 2$ ισχύει ότι:

$$x^{2^s} + 4b^4 = (x^{2^{s-1}} + 2bx^{2^{s-2}} + 2b^2)(x^{2^{s-1}} - 2bx^{2^{s-2}} + 2b^2)$$

Οπότε, το διώνυμο $X^{2^s} + 4b^4$ δέν είναι ανάγωγο παρόλο που το $u = -4b^4 \notin \mathbb{Q}^2$. Άρα, για $s > 1$ θα πρέπει να έχουμε και σαν περιορισμό ότι $u \neq -4b^4$, $b \in F$, δηλαδή $u \notin -4F^4$, για να είναι ανάγωγο το πολυώνυμο.

Θεώρημα 1.1.3. *Έστω F σώμα και $u \in F, u \neq 0$.Τότε:*
1) Το $f(X) = X^2 - u$ είναι ανάγωγο άν και μόνο άν $u \notin F^2$
2)Για $s > 1$ το διώνυμο $f_s(X) = X^{2^s} - u$ είναι ανάγωγο άν και μόνο άν $u \notin F^2$ και $u \notin -4F^4$

Απόδειξη. 1) Από το Θεώρημα 1.1.1 έχουμε ότι για p πρώτο αριθμό $u \notin F^p$ άν και μόνο άν το $f(X) = X^p - u$ είναι ανάγωγο στο F. Οπότε, για τον πρώτο $p = 2$ ισχύει ότι το $f(X) = X^2 - u$ είναι ανάγωγο στο F άν και μόνο άν $u \notin F^2$.
2) Υποθέτουμε ότι το $f_s(X)$ είναι ανάγωγο με $s > 1$. Θα δείξουμε ότι $u \notin F^2$, και $u \notin -4F^4$.
Έστω ότι $u \in F^2$. Δηλαδή υπάρχει $\gamma \in F$ τ.ω $u = \gamma^2$. Άρα,

$$f_s(X) = X^{2^s} - u = X^{2^s} - \gamma^2 = (X^{2^{s-1}})^2 - \gamma^2 = (X^{2^{s-1}} - \gamma)(X^{2^{s-1}} + \gamma)$$

Οπότε, το $f_s(X)$ δεν είναι ανάγωγο, άτοπο, αφού υποθέσαμε το $f_s(X)$ είναι ανάγωγο για $s > 1$. Επομένως, $u \notin F^2$.
Ακόμα, έστω ότι $u \in -4F^4$. Δηλαδή, υπάρχει $\gamma \in F$ τ.ω $u = -4\gamma^4$. Τότε,

$$f_s(X) = X^{2^s} - u = X^{2^s} + 4\gamma^4 = (X^{2^{s-1}} + 2\gamma X^{2^{s-2}} + 2\gamma^2)(X^{2^{s-1}} - 2\gamma X^{2^{s-2}} + 2\gamma^2)$$

Δηλαδή, το $f_s(X)$ αναλύεται, άτοπο, αφού το $f_s(X)$ είναι εξ' υποθέσεως ανάγωγο για $s > 1$. Συνεπώς, $u \notin -4F^4$. Επομένως, $u \notin F^2$ και $u \notin -4F^4$.

Αντίστροφα, υποθέτουμε ότι $u \notin F^2$ και $u \notin -4F^4$. Θα δείξουμε ότι το $f_s(X) = X^{2^s} - u$ είναι ανάγωγο με $s \geq 1$.
Θα εφαρμόσουμε επαγωγή στο s. Θα αποδείξουμε ότι ισχύει για $s = 1$. Για $s = 1$: $f_1(X) = X^2 - u$. Το οποίο είναι ανάγωγο αφού $u \notin F^2$, (σύμφωνα με το Θεώρημα 1.3.1[1]). Υποθέτουμε ότι ισχύει για όλους τους θετικούς ακέραιους οι οποίοι είναι γνήσια μικρότεροι από τον $s > 1$ και θα αποδείξουμε ότι ισχύει για τον s.
Έστω β μία ρίζα του $f_s(X) = X^{2^s} - u = (X^{2^{s-1}})^2 - u$, σε κάποιο σώμα ανάλυσης του πολυωνύμου $f_s(X)$. Αφού, β είναι ρίζα του $f_s(X)$, τότε το $\alpha = \beta^{2^{s-1}}$ είναι ρίζα του $h(X) := -X^2 - u$. Το β είναι ρίζα του $g(X) = X^{2^{s-1}} - \alpha$. Άρα, προκύπτει η αλυσίδα σωμάτων

$$F \leq F(\alpha) \leq F(\beta)$$

Ακόμα, $[F(\alpha) : F] = 2$, αφού $Irr(\alpha, F) = X^2 - u$, το οποίο είναι ανάγωγο διότι $u \notin F^2$.
Άν $\alpha \notin F(\alpha)^2$ και $\alpha \notin -4F(\alpha)^4$, τότε σύμφωνα με την επαγωγική υπόθεση ισχύει ότι το $g(X)$ είναι ανάγωγο υπέρ το $F(\alpha)$. Δηλαδή, $g(X) = Irr(\beta, F(\alpha))$. Επομένως, $[F(\beta) : F(\alpha)] = degIrr(\beta, F(\alpha)) = degf(X) = 2^{s-1}$. Οπότε, $[F(\beta) : F] = [F(\beta) : F(\alpha)][F(\alpha) : F] = 2^{s-1}2 = 2^s$. Όμως, έχουμε ότι το β είναι ρίζα του $f_s(X)$ και $degf_s(X) = 2^s$. Οπότε, ισχύει ότι $Irr(\beta, F) = f_s(X)$. Δηλαδή, το $f_s(X)$ είναι ανάγωγο υπέρ το F. Επομένως, το $f_s(X)$ είναι ανάγωγο για $s \geq 1$.

Ας εξετάσουμε τώρα τις δύο περιπτώσεις που η υπόθεση αποτυγχάνει.
Άν $\alpha \in -4F(\alpha)^4$, δηλαδή υπάρχει $\gamma \in F(\alpha)$ τ.ω.

$$\alpha = -4\gamma^4 \tag{1.5}$$

τότε ισχυρίζομαι ότι $\alpha \in F(\alpha)^2$. Όμως υπάρχει πρόβλημα με το -1, διότι μπορεί το -1 να μην είναι τετράγωνο στο $F(\alpha)$, δηλαδή $-1 \notin F(\alpha)^2$. Εφαρμόζοντας, την norm $N = N_{F(\alpha)/F}$ στην σχέση 1.5 προκύπτει ότι: $N_{F(\alpha)/F}(\alpha) = N_{F(\alpha)/F}(-4\gamma^4)$, με $F < F(\alpha)$. Γνωρίζουμε ότι $Irr(\alpha, F) = X^2 - u$. Αφού το α είναι ρίζα του $Irr(\alpha, F)$, και το $-\alpha$ είναι ρίζα του. Οπότε, σύμφωνα με τον ορισμό της norm $N = N_{F(\alpha)/F}$ προκύπτει ότι

$$N(\alpha) = N_{F(\alpha)/F}(\alpha) = \prod_{i=1}^{2} t_i^{[F(\alpha):F(\alpha)]} = \prod_{i=1}^{2} t_i = \alpha(-\alpha) = -\alpha^2$$

με t_i οι ρίζες του $Irr(\alpha, F)$. Ακόμα, $N(-4\gamma^4) = N_{F(\alpha)/F}(-4\gamma^4)$. Ισχύει ότι $-4 \in F$, οπότε απο τις ιδιότητες της νόρμας έχουμε ότι

$$N_{F(\alpha)/F}(-4\gamma^4) = (-4)^{[F(\alpha):F]} N_{F(\alpha)/F}(\gamma^4) = (-4)^2 (N_{F(\alpha)/F}(\gamma))^4 = 16(N_{F(\alpha)/F}(\gamma))^4$$

Θέτουμε $a := 4(N_{F(\alpha)/F}(\gamma))^2$. Το $a \in F$, διότι $N_{F(\alpha)/F}(\gamma) \in F$. Οπότε,

$$N_{F(\alpha)/F}(\alpha) = N_{F(\alpha)/F}(-4\gamma^4) \Leftrightarrow -\alpha^2 = a^2 \Leftrightarrow -1 = \frac{a^2}{\alpha^2} \in F(\alpha)^2,$$
$$\text{αφού } \frac{a}{\alpha} \in F(\alpha)$$

Επομένως, αφού $\alpha = -4\gamma^4$ καί $-1 = \frac{a^2}{\alpha^2}$, έπεται ότι $\alpha = 4\frac{a^2}{\alpha^2}\gamma^4 \in F(\alpha)^2$, αφού $2\frac{a^2}{\alpha^2}\gamma^2 \in F(\alpha)$.
Φυσιολογικά θα έπρεπε να θεωρήσουμε δύο περιπτώσεις: i) $\alpha \in -4(F(\alpha))^4$ καί ii) $\alpha \in F(\alpha)^2$. Όμως, αποδείξαμε ότι ισχύει $\alpha \in -4(F(\alpha))^4 \Rightarrow \alpha \in F(\alpha)^2$. Οπότε, αρκεί να θεωρήσουμε μόνο την περίπτωση που $\alpha \in F(\alpha)^2$. Δηλαδή, εάν οποιαδήποτε απο τις δύο συνθήκες $\alpha \notin F(\alpha)^2$ καί $\alpha \notin -4F(\alpha)^4$ αποτυγχάνει, τότε υπάρχει $\gamma \in F(\alpha)$ τ.ω $\alpha = \gamma^2 \in F(\alpha)^2$.
Εμείς πρέπει να δείξουμε ότι η σχέση $u \notin F^2$ καί $u \notin -4F^4$ συνεπάγεται ότι το $f_s(X) = X^{2^s} - u$ είναι ανάγωγο υπέρ το F. Ισχύει ότι $Irr(\alpha, F) = X^2 - u$. Εφαρμόζοντας την norm $N = N_{F(\alpha)/F}$ προκύπτει ότι $N_{F(\alpha)/F}(\alpha) = ((-1)^2(-u))^{[F(\alpha):F(\alpha)]} = -u$. Και αφού $\alpha = \gamma^2$ τότε προκύπτει ότι $-u = N_{F(\alpha)/F}(\gamma^2) \Rightarrow -u = (N_{F(\alpha)/F}(\gamma))^2$. Θέτουμε $b = N_{F(\alpha)/F}(\gamma) \in F$. Δηλαδή, $-u = \beta^2 \in F^2$. Αφού, $u \notin F^2$ τότε $-1 \notin F^2$.
Το πολυώνυμο $h(X) := X^2 + 1 \in F[X]$ έχει ρίζες τις οποίες (κατ' αναλογία ως προς το $\mathbb{C}$) τις συμβολίζουμε i καί $-i$ στο $\bar{F}$. Ισχύει ότι $i \notin F$, διότι άν $i \in F \Rightarrow i^2 \in F$ καί το i ρίζα του $h(X)$, δηλαδή $h(i) = 0 \Leftrightarrow i^2 + 1 = 0 \Rightarrow i^2 = -1$, άρα $-1 \in F^2$, Άτοπο, αφού $-1 \notin F^2$. Άρα, $i \notin F$. Ακόμα, $[F(i) : F] = 2$. Στο $F(i)$ το $f_s(X)$ αναλύεται ώς εξής

$$f_s(X) = X^{2^s} - u = X^{2^s} + b^2 = (X^{2^{s-1}} + ib)(X^{2^{s-1}} - ib) \tag{1.6}$$

Διακρίνουμε περιπτώσεις:
1) Άν τα $X^{2^{s-1}} + ib, X^{2^{s-1}} - ib$ είναι ανάγωγα υπέρ το $F(i)$, τότε το $f_s(X)$ είναι ανάγωγο υπέρ το F. Διότι, άν το $f_s(X)$ δέν είναι ανάγωγο στο $F[X]$, τότε θα έχει τουλάχιστον δύο ανάγωγους παράγοντες, εστω $h_1(X)$ καί $h_2(X)$. Δηλαδή, το $h_j(X)$ με $j = 1, 2$ είναι ανάγωγο στο $F[X]$ καί $h_j(X) \mid_{F[X]} f_s(X)$. Τότε

$$degh_j(X) < deg((X^{2^{s-1}} + ib) \text{ ή } (X^{2^{s-1}} - ib))$$

για κάθε $j = 1, 2$. Όμως, το $h_j(X)$ μπορεί να μην είναι ανάγωγο στο $F(i)[X]$. Σε αυτήν την περίπτωση αναλύεται σε γινόμενα αναγώγων. Δηλαδή υπάρχει $h'_j(X) \mid_{F(i)[X]} h_j(X)$, όπου $degh'_j(X) \leq degh_j(X)$ καί $h'_j(X)$

ανάγωγο στο $F(i)[X]$ καί $h_i'(X) \mid f_s(X)$. Από υπόθεση έχουμε ότι, τα $X^{2^{s-1}}+ib$, $X^{2^{s-1}}-ib$ είναι ανάγωγα στο $F(i)[X]$, άρα το $h_i'(X)$ είναι πολλαπλάσιο του $X^{2^{s-1}}+ib$ ή $X^{2^{s-1}}-ib$. Άρα, $degh_i'(X) = deg($αναγώγου[1]$)$. Οπότε, $degh_1(X)h_2'(X) = degf_s(X)$. Αλλά, $degh_i'(X) \leq degh_i(X)$. Άρα, $deg(h_1'(X)h_2'(X)) < degf_s(X)$. Όμως, $h_1'(X)h_2'(X) = f_s(X)$. Αντίφαση. Άρα, το $f_s(X)$ ανάγωγο υπέρ το F.
2) Άν ένας από τους παράγοντες $X^{2^{s-1}}+ib$, $X^{2^{s-1}}-ib$ δέν είναι ανάγωγος, θα τον συμβολίζω ώς $h_s(X)$. Δηλαδή, $degh_s(X) < degf(X)$ καί $h_s(X)$ δέν είναι ανάγωγο. Άρα, απο επαγωγική υπόθεση συνεπάγεται ότι τα $ib, -ib$ ανήκουν είτε στο $F(i)^2$ είτε στο $-4F(i)^4$. Όμως, $-4F(i)^4 = 4i^2F(i)^4 \subseteq F(i)^2$. Άρα, $ib \in F(i)^2$ είτε $-ib \in F(i)^2$. Το $ib \in F(i)^2$ σημαίνει ότι υπάρχει $t \in F(i)$ τ.ω $ib = t^2$. Ισχύει ότι $F(i) = \{a+bi | a, b \in F\}$, άρα αφού $t \in F(i)$ τότε $t = c+di$ με $c, d \in F$. Δηλαδή, $ib = (c+di)^2 = c^2+2cdi-d^2$. Άρα, $c^2-d^2 = 0$ και $2cd = b$. Δηλαδή, $c^2 = d^2$ καί $4c^2d^2 = b^2$. Άρα, $4c^4 = b^2$. Όμως, $b^2 = -u$. Οπότε, $-u = 4c^4 \Rightarrow u = -4c^4$, $c \in F$. Δηλαδή, $u \in -4F^4$. Αντίφαση, αφού σύμφωνα με την υπόθεση ισχύει ότι $u \notin -4F^4$. Ομοίως, άν $-ib \in F(i)^2$ τότε καταλήγουμε σε αντίφαση. Επομένως, απορρίπτεται αυτή η περίπτωση.

□

Θεώρημα 1.1.4. *Έστω $n \in \mathbb{Z}, n \geq 2$ καί $u \in F, u \neq 0$. Τότε:*
1) Άν $4 \nmid n$ τότε το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F αν και μόνο αν $u \notin F^p$ για κάθε πρώτο αριθμό p με $p \mid n$.
2) Άν $4 \mid n$ τότε το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F αν και μόνο αν $u \notin F^p$ για κάθε πρώτο αριθμό p τ.ω. $p \mid n$ καί $u \notin -4F^4$.

Απόδειξη. Αρχικά υποθέτουμε ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. Τότε για κάθε πρώτο αριθμό p τέτοιο ώστε $p \mid n$ το πολυώνυμο $X^p - u$ είναι ανάγωγο υπέρ το F. Άν το πολυώνυμο $X^p - u$ δέν είναι ανάγωγο, δηλαδή αναλύεται μη τετριμμένα, τότε έστω ότι

$$X^p - u = a(X)b(X) \tag{1.7}$$

όπου η παραπάνω παραγοντοποίηση του $X^p - u$ είναι μη τετριμμένη. Τότε,

$$X^n - u = (X^{n/p})^p - u \overset{1.7}{=} a(X^{n/p})b(X^{n/p})$$

Δηλαδή, το $X^n - u$ αναλύεται μη τετριμμένα, άτοπο, αφού το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. Επομένως, το $X^p - u$ είναι ανάγωγο υπέρ το F για κάθε πρώτο p τέτοιο ώστε $p \mid n$. Συνεπώς, σύμφωνα με

[1] Δηλαδή του $X^{2^{s-1}}+ib$ ή του $X^{2^{s-1}}-ib$.

το θεώρημα 1.1.1 ισχύει ότι $u \notin F^p$ για κάθε πρώτο p τέτοιο ώστε $p \mid n$. Επίσης, αν $4 \mid n$ τότε το πολυώνυμο $X^4 - u$ είναι ανάγωγο υπέρ το F, διότι αν το $X^4 - u$ δέν είναι ανάγωγο, έστω ότι $X^4 - u = g_1(X)g_2(X)$, τότε

$$f(X) = X^n - u = (X^{n/4})^4 - u = g_1(X^{n/4})g_2(X^{n/4})$$

Δηλαδή, το $f(X)$ αναλύεται μη τετριμμένα στο F. Άτοπο, αφού το $f(X)$ είναι ανάγωγο υπέρ το F. Άρα, το $X^4 - u$ είναι ανάγωγο υπέρ το F. Αλλά ισχύει ότι $X^4 - u = X^{2^2} - u$. Οπότε, σύμφωνα με το Θεώρημα 1.3.1[2] προκύπτει ότι $u \notin -4F^4$. Αλλιώς, έχουμε ότι το $f(X)$ παραγοντοποιείται ως εξής

$$f(X) = X^n - u = X^{4d} + 4\gamma^4 = (X^{2d} + 2\gamma X^d + 2\gamma^2)(X^{2d} - 2\gamma X^d + 2\gamma^2)$$

διότι αν $u \in -4F^4$ τότε υπάρχει $\gamma \in F$ τέτοιο ώστε $u = -4\gamma^4$ καί αφού $4 \mid n$ τότε $n = 4d$, $d \in \mathbb{Z}$. Δηλάδη, το $f(X)$ αναλύεται μη τετριμμένα. Άτοπο, αφού το $f(X)$ είναι ανάγωγο υπέρ το F.
Επομένως, αν το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F, τότε ισχύουν τα εξής:
i) αν $4 \mid n$ τότε $u \notin F^p$ για κάθε πρώτο p τέτοιο ώστε $p \mid n$ και $u \notin -4F^4$.
ii) αν $4 \nmid n$ τότε $u \notin F^p$ για κάθε πρώτο p τέτοιο ώστε $p \mid n$.
Αντίστροφα, υποθέτουμε ότι $u \notin F^p$ για κάθε πρώτο p τέτοιο ώστε $p \mid n$. Επίσης, αν $4 \mid n$ υποθέτουμε ότι $u \notin -4F^4$. Θα δείξουμε ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. Θα το αποδείξουμε επαγωγικά ώς προς n. Θα δείξουμε ότι ισχύει για $n = 2$, δηλαδή ότι το $f(X) = X^2 - u$. Αφού έχουμε ότι $u \notin F^p$ καί $u \in F, u \neq 0$, τότε σύμφωνα με το Θεώρημα 1.3.1[1] προκύπτει ότι το $f(X) = X^2 - u$ είναι ανάγωγο υπέρ το F.
Υποθέτουμε ότι το $f(X) = X^t - u$ είναι ανάγωγο υπέρ το F για $2 \leq t \leq n$, $t \in \mathbb{Z}$. Θα αποδείξουμε ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. Διακρίνουμε τις εξής περιπτώσεις: 1) Εάν $n = 2^m$ με $m > 1$ τότε έχουμε ότι $u \notin F^p$ καί $4 \mid n = 2^m, m > 1$. Άρα $u \notin -4F^4$. Οπότε, σύμφωνα με το Θεώρημα 1.3.1[2] ισχύει ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. 2) Άν η ανάλυση του n σε πρώτους παράγοντες περιέχει κάποιο περιττό πρώτο παράγοντα, έστω p. Υποθέτουμε ότι $n = p^k m$ με ΜΚΔ$(p, m) = 1, k \geq 1$. Έστω β ρίζα του $f(X) = X^n - u = (X^{p^k})^m - u$. Άρα, το $\alpha = \beta^{p^k}$ είναι ρίζα του $h(X) = X^m - u$. Επίσης, το β είναι ρίζα του $g(X) = X^{p^k} - \alpha$. Οπότε, ορίζεται ο πύργος σωμάτων $F \leq F(\alpha) \leq F(\beta)$. Από την επαγωγική υπόθεση έχουμε ότι το $h(X) = X^m - u$ είναι ανάγωγο υπέρ το F, αφού $m < n$. Οπότε, $[F(\alpha) : F] = degh(X) = m$. Εξετάζουμε άν το $g(X)$ είναι ανάγωγο υπέρ το $F(\alpha)$. Θα εφαρμόσουμε την επαγωγική υπόθεση για να δείξουμε ότι το $g(X)$ είναι ανάγωγο. Αφού, το p είναι

περιττός πρώτος, αρκεί να δείξουμε ότι $\alpha \notin F(\alpha)^p$, σύμφωνα με το Θεώρημα 1.1.2. Εάν το $\alpha \in F(\alpha)^p$ τότε υπάρχει $\gamma \in F(\alpha)$ τέτοιο ώστε $\alpha = \gamma^p$. Εφαρμόζοντας την norm $N = N_{F(\alpha)/F}$ στην παραπάνω σχέση προκύπτουν τα εξής $N_{F(\alpha)/F}(\alpha) = N_{F(\alpha)/F}(\gamma^p)$, δηλαδή $N(\alpha) = N(\gamma^p)$. Έχουμε ότι $Irr(\alpha, F) = X^m - u$. Από τον ορισμό της norm $N = N_{F(\alpha)/F}$ έχουμε ότι $N(\alpha) = ((-1)^m(-u))^{[F(\alpha):F(\alpha)]} = (-1)^m(-u)$. Δηλαδή,

$$N(\alpha) = (-1)^m(-u) \Leftrightarrow (-1)^m N(\alpha) = (-1)^{2m}(-u) \Leftrightarrow (-1)^m N(\alpha) = -u$$

$$\Leftrightarrow -u = (-1)^m N(\gamma^p) \Leftrightarrow -u = (-1)^m (N(\gamma))^p$$

Άν m=περιττός τότε $-u = -(N(\gamma)^p) \Leftrightarrow u = N(\gamma)^p, N(\gamma) \in F$ Δηλαδή, $u \in F^p$. Άτοπο, αφού απο υπόθεση έχουμε ότι $u \notin F^p$.
Άν m=άρτιος τότε $-u = (N(\gamma))^p \Leftrightarrow u = (-N(\gamma))^p$, αφού p=περιττός. Όμως, $N(\gamma) \in F$. Άρα, $u \in F^p$. Αντίφαση, αφού από υπόθεση ισχύει ότι $u \notin F^p$.
Επομένως, $\alpha \notin F(\alpha)^p$. Άρα $g(X)$ ανάγωγο υπέρ το $F(\alpha)$. Οπότε, $[F(\beta) : F(\alpha)] = p^k$. Έτσι, $[F(\beta) : F] = [F(\beta) : F(\alpha)][F(\alpha) : F] = p^k m = n$. Και ισχύει ότι $degf(X) = n = mp^k$. Οπότε, $Irr(\beta, F) = f(X)$. Συνεπώς το $f(X)$ είναι ανάγωγο υπέρ το F. □

Απόδειξη. Η απόδειξη του είναι παρόμοια με την αποδειξη του Θεωρήματος 1.1.4 □

1.2 Η ομάδα Galois ενός Διωνύμου(Binomial)

Θα εξετάσουμε την ομάδα Galois του διωνύμου $X^n - u \in F[X]$ με $u \neq 0$ και n σχετικά πρώτος με την expchar(F).

Ορισμός 1.2.1. *Χαρακτηριστική του εκθέτη ενός σώματος F, expchar(F), ορίζεται ώς*

$$expchar(F) = \begin{cases} 1, & \alpha\nu\, char(F) = 0 \\ charF, & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

Θεώρημα 1.2.1. *Έστω n θετικός ακέραιος και ΜΚΔ*$(n, expchar(F)) = 1$. *Έστω S το σώμα ανάλυσης του $X^n - u \in F[X]$, με $u \in F, u \neq 0$ καί α ρίζα του $X^n - u$ καί $\omega \in \Omega_n$. Στην αλυσίδα σωμάτων $F \leq F(\omega) \leq F(\omega, \alpha) = S$ η επέκταση $F(\omega)/F$ είναι κυκλοτομική επέκταση καί η επέκταση $F(\omega) \leq S$ είναι κυκλική με $[S : F(\omega)] = d \mid n$ όπου $Irr(\alpha, F(\omega)) = X^d - \alpha^d$. Επίσης, η ομάδα $Gal(S/_F)$ είναι ισόμορφη με μια υποομάδα της ομάδας M_n, όπου $M_n = \{\begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix} | k \in \mathbb{Z}_n, j \in \mathbb{Z}_n^*\}$,*

μέσω της εμφύτευσης $\lambda : \sigma \mapsto \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix}$ *, όπου* $\sigma\alpha = \omega^{k(\sigma)}\alpha$ *και* $\sigma\omega = \omega^{j(\sigma)}$, $k(\sigma) \in \mathbb{Z}_d, j(\sigma) \in \mathbb{Z}_n^*$. *Η απεικόνιση* λ *είναι ισομορφισμός, οπότε* $Gal(S/_F) \approx M_n$ *αν και μόνο αν*
1) $[F(\omega) : F] = \varphi(n)$, *δηλαδή το* ω *είναι μια πρωταρχική* n*-ρίζα της μονάδας.*
2) $[F(\omega, \alpha) : F(\omega)] = n$ *ή ισοδύναμα το* $X^n - u$ *είναι ανάγωγο υπέρ το* $F(\omega)$
(Δηλαδή οι επεκτάσεις $F \leq F(\omega), F(\omega) \leq F(\omega, \alpha)$ *έχουν τους μέγιστους δυνατούς βαθμούς.)*

Απόδειξη. Έστω $f(X) = X^n - u \in F[X]$, με $u \neq 0$ καί ΜΚΔ$(n, expchar(F)) = 1$. Το α είναι ρίζα $f(X)$ καί $\omega \in \Omega_n$. Άρα, όλες οι ρίζες του $f(X)$ είναι οι εξής $\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha$. Ακόμα, το σώμα ανάλυσης S του $f(X) = X^n - u$ υπέρ το F είναι $S = F(\omega, \alpha)$. Οπότε προκύπτει η παρακάτω αλυσίδα σωμάτων

$$F \leq F(\omega) \leq F(\omega, \alpha) = S \tag{1.8}$$

Η επέκταση $F(\omega)/F$ είναι κυκλοτομική επέκταση. Άρα, η επέκταση $F \leq F(\omega)$ είναι αβελιανή, αφού κάθε κυκλοτομική επέκταση είναι αβελιανή, διότι η $Gal(F(\omega)/_F)$ είναι ισόμορφη με μία υποομάδα της $\mathbb{Z}_n^*$. Επομένως, η ομάδα $Gal(F(\omega)/_F)$ είναι αβελιανή, δηλαδή η επέκταση $F(\omega)$ υπέρ το F είναι αβελιανή.
Η επέκταση S υπέρ του $F(\omega)$ είναι καθαρού τύπου n (pure of type n), διότι ΜΚΔ$(n, expchar(F(\omega))) = 1$ [2] καί α ρίζα του διωνύμου $f(X) = X^n - u \in F[X]$. Ακόμα, το $F(\omega)$ περιέχει τις n-ρίζες της μονάδας. Άρα, σύμφωνα με το Θεώρημα 2[Παράρτημα] η επέκταση $F(\omega) \leq S$ είναι κυκλική βαθμού $d \mid n$. Ακόμα, ισχύει ότι $Irr(\alpha, F(\omega)) = X^d - \alpha^d$.
Θα περιγράψουμε την $Gal(S/_F)$ χρησιμοποιώντας το γεγονός ότι τα α, ω ικανοποιούν απλά πολυώνυμα πάνω απο το F. Επειδή κάθε $\sigma \in Gal(S/_F)$ πρέπει να μεταθέτει τις ρίζες του $X^d - \alpha^d$ προκύπτει ότι υπάρχει ακέραιος $k(\sigma) \in \mathbb{Z}_d \subseteq \mathbb{Z}_n$ τέτοιος ώστε $\sigma\alpha = \omega^{k(\sigma)}\alpha$. Ακόμα η επέκταση $F \leq F(\omega)$ είναι κανονική επέκταση. Άρα, ο περιορισμός της σ στο $F(\omega)$ ανήκει στην ομάδα $Gal(F(\omega)/_F)$, δηλαδή $\sigma|_{F(\omega)} \in Gal(F(\omega)/_F)$. Άρα $\sigma(\omega)$ είναι μία άλλη πρωταρχική n-ρίζα της μονάδας. Δηλαδή, $\sigma(\omega) = \omega^{j(\sigma)}$, όπου $j(\sigma) \in \mathbb{Z}_n^*$. Ο πολλαπλασιασμός στην $Gal(S/F)$ ορίζεται ως εξής: Έστω $\sigma, \tau \in Gal(S/F)$. Τότε, $\sigma\tau(\alpha) = \sigma(\omega^{k(\tau)}\alpha) = \sigma(\omega^{k(\tau)})\sigma(\alpha) = \sigma(\omega)^{k(\tau)}\sigma(\alpha) = \omega^{j(\sigma)k(\tau)}\omega^{k(\sigma)}\alpha = \omega^{j(\sigma)k(\tau)+k(\sigma)}\alpha$ καί $\sigma\tau(\omega) = \sigma(\omega^{j(\tau)}) =$

[2] ΜΚΔ$(n, expchar(F(\omega))) = 1$, διότι έχουμε ότι ΜΚΔ$(n, expchar(F) = 1, F \leq F(\omega)$. Άν $chF = 0$ τότε $\mathbb{Q} \leq F \leq F(\omega)$. Άρα, $chF(\omega) = 0$. Άν $chF = p$ τότε $\mathbb{F}_p \leq F \leq F(\omega)$. Άρα, $chF(\omega) = p$

$\sigma(\omega)^{j(\tau)} = \omega^{j(\tau)j(\sigma)}$. Παρατηρούμε ότι ο παραπάνω πολλαπλασιασμός μοιάζει με τον πολλαπλασιασμό πινάκων. Πράγματι, έστω M_n το σύνολο όλων των πινάκων της μορφής $M_n = \{\begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix} | k \in \mathbb{Z}_n, j \in \mathbb{Z}_n^*\}$, Ισχύει ότι

$$\begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix} \begin{bmatrix} 1 & 0 \\ k' & j' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k+jk' & jj' \end{bmatrix} \tag{1.9}$$

όπου $k + jk' \in \mathbb{Z}_n$, αφού $k, k' \in \mathbb{Z}_n$ καί $j \in \mathbb{Z}_n^*$, καί $jj' \in \mathbb{Z}_n^*$, αφού $j \in \mathbb{Z}_n^*, j' \in \mathbb{Z}_n^*$ καί $\mathbb{Z}_n^*$ πολλαπλασιαστική ομάδα.
Ακόμα, $\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_n$ καί για κάθε $A \in M_n$ ισχύει ότι $A^{-1} \in M_n$ διότι άν $A = \begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix}$ τότε $detA \neq 0$, διότι $j \in \mathbb{Z}_n^*$. Άρα, M_n είναι υποομάδα της γενικής γραμμικής ομάδας, $Gl_2(\mathbb{Z}_n)$, των αντιστρέψιμων 2×2 πινάκων πάνω από το $\mathbb{Z}_n$. Συγκρίνοντας το αποτέλεσμα του γινομένου της σχέσης 1.9 με την δράση του γινομένου $\sigma\tau$ προκύπτει ότι για την απεικόνιση

$$\lambda : Gal(S/F) \to M_n \text{ τέτοιο ώστε } \sigma \mapsto \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix}$$

ισχύουν τα παρακάτω:
Η λ είναι ομομορφισμός ομάδων, διότι

$$\lambda(\sigma\tau) = \begin{bmatrix} 1 & 0 \\ k(\sigma\tau) & j(\sigma\tau) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ j(\sigma)k(\tau) + k(\sigma) & j(\tau)j(\sigma) \end{bmatrix}$$

καί $\lambda(\sigma)\lambda(\tau) = \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ k(\tau) & j(\tau) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k(\sigma) + j(\sigma)k(\tau) & j(\sigma)j(\tau) \end{bmatrix}$, αφού $k(\sigma), k(\tau) \in \mathbb{Z}_d \subseteq \mathbb{Z}_n$ και $j(\sigma), j(\tau) \in \mathbb{Z}_n^*$. Οπότε $\lambda(\sigma\tau) = \lambda(\sigma)\lambda(\tau)$. Δηλαδή, η λ είναι ομομορφισμός ομάδων.
Ακόμα η λ είναι 1-1, διότι άν $\sigma, \tau \in Gal(S/F)$ τότε

$$\lambda(\sigma) = \lambda(\tau) \Leftrightarrow \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k(\tau) & j(\tau) \end{bmatrix} \Leftrightarrow k(\sigma) = k(\tau) \text{ καί } j(\sigma) = j(\tau)$$

$k(\sigma) = k(\tau) \Rightarrow \omega^{k(\sigma)} = \omega^{k(\tau)} \Rightarrow \omega^{k(\sigma)}\alpha = \omega^{k(\tau)}\alpha \Rightarrow \sigma(\alpha) = \tau(\alpha)$
καί $j(\sigma) = j(\tau) \Rightarrow \omega^{j(\sigma)} = \omega^{j(\tau)} \Rightarrow \sigma(\omega) = \tau(\omega)$
Εδώ αφού σ και τ είναι F-αυτομορφισμοί και $S = F(\omega, \alpha)$, έπεται ότι $\sigma = \tau$. Άρα η λ είναι 1-1. Οπότε, η λ είναι μονομορφισμός.
$card(M_n) = n\varphi(n)$, όπου φ είναι η συνάρτηση του Euler[3]. Ισχύει ότι η

[3] $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$

απεικόνιση λ είναι επί αν και μόνο αν $Card(Gal(S/F)) = Card(M_n)$ αν και μόνο αν $[S : F] = n\varphi(n)$. Και έχουμε ότι $F \leq F(\omega) \leq F(\omega, \alpha) = S$. Αλλά, ισχύει ότι $[F(\omega) : F] \leq \varphi(n)$ και $[F(\omega, \alpha) : F(\omega)] \leq n$. Άρα η απεικόνιση λ είναι επί και επομένως, η λ είναι ισομορφισμός αν και μόνο αν $[F(\omega) : F] = \varphi(n)$ και $[F(\omega, \alpha) : F(\omega)] = n$.

□

Παρατήρηση 1.2.1. *Παρόλο που η επέκταση $F \leq F(\omega)$ είναι αβελιανή και η επέκταση $F(\omega) \leq S$ είναι κυκλική, δέν συνεπάγεται ότι και η επέκταση $F \leq S$ είναι αβελιανή.*
Δηλαδή,

$$\begin{array}{ccc} S & \longleftrightarrow & \{1\} \\ | & & | \\ F(\omega) & \longleftrightarrow & H = Gal(S/F(\omega)) \\ | & & | \\ F & \longleftrightarrow & G = Gal(S/F) \end{array}$$

Ισχύει ότι $Gal(F(\omega)\_F) \cong \frac{G}{H}$ [4]. Δηλαδή, άν H κυκλική καί $G/_H$ αβελιανή τότε δεν συνεπάγεται ότι G είναι αβελιανή.

Στην συνέχεια θα εξετάσουμε δύο ζητήματα που προκύπτουν απο το προηγούμενο θεώρημα:
i) Το (2) του θεωρήματος 1.2.1 διατυπώθηκε στο $F(\omega)$. Πώς θα το διατυπώσουμε για να ισχύει στο F;
ii) Με ποιές προϋποθέσεις η ομάδα $Gal(S/F)$ είναι αβελιανή;
Υποθέτουμε ότι n είναι περιττός ακέραιος καί ΜΚΔ$(n, expchar(F)) = 1$. Η ιδιότητα (2) του θεωρήματος 1.2.1 θα διατυπωθεί ώς εξής "Το $X^n - u$ είναι ανάγωγο υπέρ το F".

Σχόλιο 1.2.1. *Άν n είναι πρώτος,έστω $n = p$, όπου p είναι πρώτος,τότε σύμφωνα με το Θεώρημα 1.1.1 ισχύει ότι $u \notin F^p$ άν καί μόνο άν το $f(X) = X^p - u$ δέν έχει ρίζες στο F άν καί μόνο άν το $f(X) = X^p - u$ είναι ανάγωγο υπέρ το F. Οπότε στο $F(\omega)$ το οποίο περιέχει όλες τις p-ρίζες της μονάδας, ισχύει ότι $[S : F(\omega)] = 1$ ή p.*

Απόδειξη. Αφού, ισχύει ότι $F \leq F(\omega) \leq F(\omega, \alpha) = S$ καί $[S : F(\omega)] = degIrr(\alpha, F(\omega))$, όπου α είναι ρίζα του $X^p - u$. Άρα, $Irr(\alpha, F(\omega)) \mid X^p - u$. Άν το $X^p - u$ είναι ανάγωγο τότε $[S : F(\omega)] = p$. Άν το $X^p - u$ δέν είναι ανάγωγο τότε σύμφωνα με το Θεώρημα 1.2.1 έχουμε αποδείξει ότι η

[4] Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois.

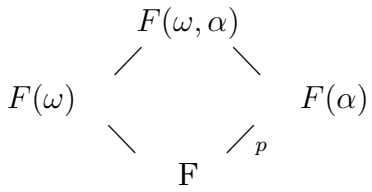
επέκταση $F(\omega) \leq S$ είναι κυκλική με $[S : F(\omega)] = d \mid p$ καί $Irr(\alpha, F(\omega)) = X^d - \alpha^d$. Δηλαδή, $d \mid p$ καί p είναι πρωτος αριθμός. Άρα, $d = 1$ ή $d = p$. Συνεπώς, $[S : F(\omega)] = 1$ή p. □

Παρατήρηση 1.2.2. *Έστω $\omega \in \Omega_p$, α ρίζα του $X^p - u \in F[X]$ καί S είναι σώμα ανάλυσης του $X^p - u$. Στο $F(\omega)$ τα ακόλουθα είναι ισοδύναμα:*
1)$[S : F(\omega)] = p$
2) $u \notin F(\omega)^p$
3) Το $X^p - u$ δέν έχει ρίζες στο $F(\omega)$
4) Το $X^p - u$ δέν αναλύεται στο $F(\omega)$
5) Το $X^p - u$ είναι ανάγωγο στο $F(\omega)$

Απόδειξη. $''(1) \Rightarrow (5)''$ Υποθέτουμε ότι $[S : F(\omega)] = p$. Το α είναι ρίζα του $X^p - u \in F[X]$. Άρα ισχύει ότι $Irr(\alpha, F(\omega)) = X^p - u$. Δηλαδή, το $X^p - u$ είναι ανάγωγο στο $F(\omega)$. Αλλά το p είναι πρώτος αριθμός και το $F(\omega)$ είναι σώμα. Επομένως, σύμφωνα με το θεώρημα 1.1.1 προκύπτει ότι ισοδύναμα το $X^p - u$ δέν έχει ρίζες στο $F(\omega)$. Ισοδύναμα, $u \notin F(\omega)^p$.
$''(5) \Rightarrow (1)''$ Έστω ότι το $X^p - u$ είναι ανάγωγο στο $F(\omega)$. Έχουμε ότι το α είναι ρίζα του $X^p - u$ καί S είναι σώμα ανάλυσης του $X^p - u$, όπου $S = F(\omega, \alpha)$. Άρα, $[S : F(\omega)] = degIrr(\alpha, F(\omega)) = deg(X^p - u) = p$.
Άρα δείξαμε ότι το (1) είναι ισοδύναμο με το (5). Όμως, σύμφωνα με το 1.1.1, αφού p είναι πρώτος αριθμός και το $F(\omega)$ είναι σώμα, ισχύουν ότι το $X^p - u$ είναι ανάγωγο στο $F(\omega)$ άν καί μόνο άν το $X^p - u$ δέν έχει ρίζες στο $F(\omega)$ άν καί μόνο άν $u \notin F(\omega)^p$. Επομένως, αποδείξαμε το ζητούμενο. □

Λήμμα 1.2.1. *Έστω p πρώτος αριθμός καί $\omega \in \Omega_p$. Τότε το $f(X) = X^p - u$ είναι ανάγωγο υπέρ το $F(\omega)$ άν καί μόνο άν το $f(X)$ είναι ανάγωγο υπέρ το F.*

Απόδειξη. $''\Rightarrow''$ Έστω οτι $f(X) = X^p - u$ είναι ανάγωγο υπέρ το $F(\omega)$. Θα δείξουμε ότι το $f(X)$ είναι ανάγωγο υπέρ το F. Όμως $F \leq F(\omega)$. Πράγματι, αφού το $f(X)$ είναι ανάγωγο υπέρ το $F(\omega)$, τότε το $f(X)$ είναι ανάγωγο υπέρ το F.
$''\Leftarrow''$ Έστώ ότι το $f(X)$ είναι ανάγωγο υπέρ το F. Θα δείξουμε ότι το $f(X)$ είναι ανάγωγο υπέρ το $F(\omega)$. Έστω α ρίζα του $f(X)$.Αφού, το $f(X)$ είναι ανάγωγο υπέρ το F, τότε $Irr(\alpha, F) = f(X) = X^p - u$. Έχουμε ότι $F \leq F(\omega) \leq F(\omega, \alpha)$. Οπότε, $[F(\alpha) : F] = p$. Ακόμα, ισχύει ότι $[F(\omega, \alpha) : F] = [F(\omega, \alpha) : F(\alpha)][F(\alpha) : F]$.



Άρα, $p \mid [F(\omega,\alpha):F]$. Επίσης, $[F(\omega):F] \leq \varphi(p) = p-1$, αφού η επέκταση $F \leq F(\omega)$ είναι κυκλοτομική επέκταση. Η επέκταση $F(\omega) \leq F(\omega,\alpha)$ είναι καθαρού τύπου p (pure of type p), διότι το α είναι ρίζα του $X^p - u$ καί ΜΚΔ$(p, expchar(F(\omega))) = 1$, αφού ΜΚΔ$(p, expchar(F)) = 1$. Άρα, αφού το $F(\omega)$ περιέχει τις p-ρίζες της μονάδας, ΜΚΔ$(p, expchar(F(\omega))) = 1$ καί η επέκταση $F(\omega) \leq F(\omega,\alpha)$ είναι καθαρού τύπου p (pure of type p), τότε σύμφωνα με το θεώρημα 2[Παράρτημα] προκύπτει ότι η επέκταση $F(\omega) \leq F(\omega,\alpha)$ είναι κυκλική βαθμού $d \mid p$. Δηλαδή $d = 1 ή p$. Άν $d = 1$, δηλαδή $[F(\omega,\alpha):F(\omega)] = 1$, τότε $F(\omega,\alpha) = F(\omega)$. Οπότε

$$[F(\omega,\alpha):F] = [F(\omega,\alpha):F(\omega)][F(\omega):F] = [F(\omega):F] \leq p-1$$

Όμως $p \mid [F(\omega,\alpha):F]$. Άτοπο. Άρα, $d = p$. Δηλαδή $[F(\omega,\alpha):F(\omega)] = p$ καί α ρίζα του $f(X) = X^p - u \in F[X]$. Άρα, $Irr(\alpha, F(\omega)) = X^p - u$. Οπότε το $X^p - u$ είναι ανάγωγο στο $F(\omega)$. □

Άν $n = p$, όπου p είναι πρώτος αριθμός, τότε η ομάδα $Gal(S/F)$ είναι αβελιανή αν κάποια απο τις επεκτάσεις $F \leq F(\omega)$ καί $F(\omega) \leq F(\omega,\alpha) = S$ είναι τετριμμένη. Αυτό ισχύει διότι οι επεκτάσεις $F \leq F(\omega)$ καί $F(\omega) \leq F(\omega,\alpha) = S$ είναι αβελιανές. Ισχύει $F \leq F(\omega) \leq F(\omega,\alpha) = S$. Άρα άν $\omega \in F$ ή $\alpha \in F(\omega)$ τότε η ομάδα $Gal(S/_F)$ είναι αβελιανή. Στην περίπτωση όπου $n = p$ ισχύει και το αντίστροφο.

Λήμμα 1.2.2. *Έστω p πρώτος αριθμός, $\omega \in \Omega_p$ καί S ένα σώμα ανάλυσης του $f(X) = X^p - u$ υπέρ το F. Τότε η ομάδα $Gal(S/F)$ είναι αβελιανή άν καί μόνο άν τουλάχιστον μία απο τις επεκτάσεις $F \leq F(\omega)$ καί $F(\omega) \leq F(\omega,\alpha) = S$ είναι τετριμμένη άν καί μόνο άν είτε $\omega \in F$ είτε το $f(X) = X^p - u$ δέν είναι ανάγωγο υπέρ το $F(\omega)$.*

Απόδειξη. Έχουμε ότι $F \leq F(\omega) \leq F(\omega,\alpha) = S$.

$$\begin{array}{rccc} & S = F(\omega,\alpha) & \longleftrightarrow & \{Id_s\} \\ \text{κυκλική} \Rightarrow \text{αβελιανή} \{ & | & & | \\ & F(\omega) & \longleftrightarrow & H = Gal(S/F(\omega)) \\ \text{κυκλοτομική, άρα Galois} \{ & | & & | \\ & \text{F} & \longleftrightarrow & G = Gal(S/F) \end{array}$$

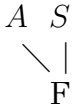
Άν κάποια απο τις επεκτάσεις $F \leq F(\omega)$ καί $F(\omega) \leq S$ είναι τετριμμένη, τότε η ομάδα $Gal(S/F)$ είναι αβελιανή. Πράγματι, έχουμε δείξει ότι οι επεκτάσεις $F \leq F(\omega)$ καί $F(\omega) \leq S$ είναι αβελιανές. Άν η επέκταση $F(\omega) \leq S$ είναι τετριμμένη,τότε $H = \{Id_s\}$, δηλαδή $S = F(\omega)$. Άρα, $Gal(S/F) = Gal(F(\omega)/F)$. Αλλά, η επέκταση $F \leq F(\omega)$ είναι κυκλοτομική, άρα η ομάδα $Gal(F(\omega)/_F)$ είναι κυκλική. Οπότε, η ομάδα $Gal(F(\omega)/F)$ είναι αβελιανή. Άν η επέκταση $F \leq F(\omega)$ είναι τετριμμένη, τότε $F(\omega) = F$. Η επέκταση $F \leq F(\omega)$ είναι Galois, άρα ισχύει ότι η ομάδα H είναι κανονική υποομάδα της G καί $Gal(F(\omega)/F) \cong \frac{G}{H}$.[5] Άρα $G = H = Gal(S/F(\omega))$. Αλλά, η επέκταση $F(\omega) \leq S$ είναι κυκλική, άρα η ομάδα $Gal(S/F(\omega))$ είναι κυκλική. Οπότε, η ομάδα $Gal(S/F(\omega))$ είναι αβελιανή. Έστω ότι $\omega \notin F$ και το $f(X)$ είναι ανάγωγο υπέρ το $F(\omega)$. Θα δείξουμε ότι η ομάδα $Gal(S/F)$ δέν είναι αβελιανή. Αφού $\omega \notin F$, τότε υπάρχει j τέτοιο ώστε $\omega^j \notin F$ καί $\omega^j \neq \omega$ [6]. έστω $\tau \in Gal(F(\omega)/F)$ τέτοιο ώστε $\tau(\omega) = \omega^j$. Επειδή το $f(X)$ είναι ανάγωγο υπέρ το $F(\omega)$ για κάθε $i \in \mathbb{Z}_p$, η μετάθεση τ μπορεί να επεκταθεί στην μετάθεση $\sigma_i \in Gal(S/_F)$, όπου $\sigma_i(\omega) = \omega^j$ καί $\sigma_i(\alpha) = \omega^i\alpha$. Για $i = 0$ καί 1 έχουμε ότι $\sigma_1\sigma_0(\alpha) = \sigma_1(\alpha) = \omega\alpha$ καί $\sigma_0\sigma_1(\alpha) = \sigma_0(\omega\alpha) = \sigma_0(\omega)\sigma_0(\alpha) = \omega^j\alpha$. Άρα, $\sigma_1\sigma_0(\alpha) \neq \sigma_0\sigma_1(\alpha)$, αφού $\omega \neq \omega^j$. Δηλαδή οι σ_1 καί σ_0 δέν αντιμετατίθεται. Οπότε η ομάδα $Gal(S/_F)$ δέν είναι αβελιανή. Επομένως, η ομάδα $Gal(S/_F)$ είναι αβελιανή άν καί μόνο άν είτε $\omega \in F$ είτε το $f(X)$ δέν είναι ανάγωγο υπέρ το $F(\omega)$.

□

Στην συνέχεια θα εξετάσουμε τα δύο ζητήματα στην γενική περίπτωση όπου ο n είναι περιττός ακέραιος.

Παρατήρηση 1.2.3. *Έστω $p(X) \in F[X]$ το οποίο παραγοντοποιείται (splits) υπέρ το F. Υποθέτουμε ότι το $p(X)$ έχει μια μη αβελιανή επέκταση $F \leq S$, (όπου S είναι σώμα ανάλυσης του $p(X)$). Τότε, αν η επέκταση $F \leq A$ είναι αβελιανή, το $p(X)$ δεν παραγοντοποιείται στον $A[X]$.*

Απόδειξη. Άν το $p(X)$ αναλυόταν στο A τότε θα υπήρχε ένα σώμα ανάλυσης T του $p(X)$ τέτοιο ώστε $F \leq T \leq A$.



[5] Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois.

[6] Γενικά άν $\omega^j \notin F$ τότε όλες οι πρωταρχικές p-ρίζες της μονάδας δέν ανήκουν στο F.

Αφού η επέκταση $F \leq A$ είναι αβελιανή, τότε και η επέκταση $F \leq T$ είναι αβελιανή. Αντίφαση, αφού όλα τα σώματα ανάλυσης του $f(X)$ υπέρ του F είναι ισόμορφα και η επέκταση $F \leq S$ δέν είναι αβελιανή. □

Θεώρημα 1.2.2. *Έστω n ένας περιττός θετικός ακέραιος, $\omega \in \Omega_n$ και ΜΚΔ$(n, expchar(F)) = 1$. Υποθέτουμε ότι το F δέν περιέχει τις n-ρίζες της μονάδας εκτός απο το 1. Έστω, επίσης, η επέκταση A/F να είναι οποιαδήποτε αβελιανή επέκταση. Τότε, το $f(X) = X^n - u \in F[X]$ είναι ανάγωγο υπέρ το F αν και μόνο αν το $f(X) = X^n - u \in F[X]$ είναι ανάγωγο υπέρ το A.*

Απόδειξη. $''\Leftarrow''$ Έστω ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το A. Θα δείξουμε ότι το $f(X)$ είναι ανάγωγο υπέρ το F.Πράγματι, αφού το $f(X)$ είναι ανάγωγο υπέρ το A καί $F \leq A$, τότε το $f(X)$ είναι ανάγωγο υπέρ το F.
$''\Rightarrow''$ Έστω ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F. Θα δείξουμε ότι το $f(X)$ είναι ανάγωγο υπέρ το A. Αφού, το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F, τότε για κάθε p πρώτο με $p \mid n$ το $X^p - u$ είναι ανάγωγο υπέρ το F. Πράγματι, αν το πολυώνυμο $X^p - u$ δέν είναι ανάγωγο υπέρ το F, δηλαδή αναλύεται μή τετριμμένα,τότε ας υποθέσουμε ότι $X^p - u = a(X)b(X) \in F[X]$[7]. Αλλά ισχύει ότι $X^n - u = (X^{n/p})^p - u = a(X^{n/p})b(X^{n/p})$. Δηλαδή, το $X^n - u$ αναλύεται μή τετριμμένα. Άτοπο, αφού το $X^n - u$ είναι ανάγωγο υπέρ το F. Οπότε, το $X^p - u$ είναι ανάγωγο υπέρ το F, για κάθε p πρώτο με $p \mid n$. Άρα,σύμφωνα με το λήμμα 1.2.1, το $X^p - u$, για κάθε p πρώτο με $p \mid n$ είναι ανάγωγο υπέρ το $F(\omega_p), \omega_p \in \Omega_p$.
Άν, το $X^p - u$ δέν είναι ανάγωγο υπέρ το A, τότε το $X^p - u$ θα έχει ρίζα στο A, σύμφωνα με το θεώρημα 1.1.1. Ακόμα, η επέκταση $F \leq A$ είναι κανονική, διότι είναι αβελιανή, αφού η ομάδα $Gal(A/F)$ είναι αβελιανή. Άρα, η επέκταση $F \leq A$ είναι Galois. Οπότε, η επέκταση $F \leq A$ είναι κανονική. Και αφού το $X^p - u$ έχει ρίζα στο A, τότε το $X^p - u$ αναλύεται υπέρ το A, για κάθε p πρώτο με $p \mid n$. Ακόμα,το F δεν περιέχει τις πρωταρχικές p-ρίζες της μονάδας (εκτός απο το 1), διότι το F δέν περιέχει τις πρωταρχικές n-ρίζες της μονάδας[8] καί $p \mid n$. Έστω, α_p ρίζα του $X^p - u$ σε κάποιο σώμα ανάλυσης. Ισχύει $F \leq F(\omega_p) \leq F(\omega_p, \alpha_p)$. Τότε οι επεκτάσεις $F \leq F(\omega_p)$ καί $F(\omega_p) \leq F(\omega_p, \alpha_p)$ δέν είναι τετριμμένες. Η επέκταση $F \leq F(\omega_p)$ δέν είναι τετριμμένη, διότι $\omega_p \notin F$, αφού

[7]Αυτή η παραγοντοποίηση είναι μη τετριμμένη.

[8]Άν το F περιέχει μία πρωταρχική p-ρίζα της μονάδας τότε αυτή θα αντιστοιχούσε σε μία πρωταρχική n-ρίζα της μονάδας, διότι $p \mid n$. Άτοπο, διότι το F περιέχει τις n-ρίζες της μονάδας.

το F δέν περιάχει τις n-ρίζες της μονάδας καί $p \mid n$. Για να δείξουμε ότι η επέκταση $F(\omega_p) \leq F(\omega_p, \alpha_p)$ δέν είναι τετριμμένη, αρκεί να δείξουμε ότι $\alpha_p \notin F(\omega_p)$. Δείξαμε ότι τα πολυώνυμα $X^p - u$, με p πρώτο αριθμό ,$p \mid n$ είναι ανάγωγα υπέρ το $F(\omega_p)$ καί το α_p είναι ρίζα του $X^p - u$. Άρα, $Irr(\alpha_p, F(\omega_p)) = X^p - u$. Δηλαδή, $[F(\omega_p.\alpha_p) : F(\omega_p)] = degIrr(\alpha_p, F(\omega_p)) = p$. Άρα η επέκταση $F(\omega) \leq F(\omega_p, \alpha_p)$ είναι μη τετριμμένη. Οπότε οι επεκτάσεις $F(\omega) \leq F(\omega_p, \alpha_p)$ καί $F \leq F(\omega_p)$ δέν είναι τετριμμένες. Ακόμα, έχουμε ότι $\omega_p \in \Omega_p$, με p πρώτο καί το $F(\omega_p, \alpha_p)$ είναι σώμα ανάλυσης του $X^p - u$. Οπότε, σύμφωνα με το λήμμα 1.2.2 προκύπτει ότι η ομάδα $Gal(F(\omega_p, \alpha_p)/F)$ δέν είναι αβελιανή. Αφού, η επέκταση $F \leq A$ είναι αβελιανή επέκταση, τότε σύμφωνα με την παρατήρηση 1.2.3 το $X^p - u$ δέν αναλύεται υπέρ το A. Αντίφαση. Άρα, το $X^p - u$ είναι ανάγωγο υπέρ το A, για κάθε p πρώτο με $p \mid n$. Οπότε, σύμφωνα με το θεώρημα 1.1.2 προκύπτει ότι το $f(X) = X^n - u$ είναι ανάγωγο υπέρ το A.

□

Έστω ότι $[F(\omega) : F] = \varphi(n)$. Τότε το F δέν περιέχει οποιαδήποτε πρωταρχική p-ρίζα της μονάδας για κάθε $p \mid n$. Άρα το F δέν περιέχει καμμία n-ρίζα της μονάδας εκτός απο το 1. Έτσι, αφού $F \leq F(\omega)$ είναι αβελιανή επέκταση, μπορούμε να ενισχύσουμε το θεώρημα 1.2.1, εφαρμόζοντας το θεώρημα 1.2.2, για n περιττό αριθμό.

Πόρισμα 1.2.1. *Έστω n περιττός θετικός ακέραιος και ισχύει ότι $ΜΚΔ(n, expchar(F)) = 1$. Τότε η ομάδα $Gal(S/F) \cong M_n$ αν και μόνο αν $[F(\omega) : F] = \varphi(n)$ και το πολυώνυμο $X^n - u$ είναι ανάγωγο υπέρ το F.*

Απόδειξη. Από το θεώρημα 1.2.1 έχουμε ότι η ομάδα $Gal(S/F) \cong M_n$ αν και μόνο αν $[F(\omega) : F] = \varphi(n)$ και το πολυώνυμο $X^n - u$ είναι ανάγωγο υπέρ το $F(\omega)$. Η επέκταση $F \leq F(\omega)$ είναι αβελιανή επέκταση. Οπότε, απο το θεώρημα 1.2.2 προκύπτει ότι το πολυώνυμο $f(X) = X^n - u$ είναι ανάγωγο υπέρ το F αν και μόνο αν το πολυώνυμο $f(X) = X^n - u$ είναι ανάγωγο υπέρ το $F(\omega)$. Επομένως, η ομάδα $Gal(S/F) \cong M_n$ αν και μόνο αν $[F(\omega) : F] = \varphi(n)$ και το πολυώνυμο $X^n - u$ είναι ανάγωγο υπέρ το F.

□

Ακόμα, επειδή $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$ προκύπτει το εξής πόρισμα:

Πόρισμα 1.2.2. *Άν $F = \mathbb{Q}$ καί n είναι περιττός θετικός ακέραιος, τότε $Gal(S/\mathbb{Q}) \cong M_n$ αν και μόνο αν το πολυώνυμο $X^n - u$ είναι ανάγωγο υπέρ το $\mathbb{Q}$.*

Απόδειξη. Προκύπτει άμεσα απο το πόρισμα 1.2.1, εφαρμόζοντας όπου $F = \mathbb{Q}$ καί λαμβάνοντας υπόψιν ότι $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. □

Μέχρι στιγμής, έχουμε αποδείξει ότι όταν η επέκταση $F \leq F(\omega)$ έχει τον μεγαλύτερο βαθμό $\varphi(n)$ (όπου περιλαμβάνει την σημαντική περίπτωση όπου $F = \mathbb{Q}$), τότε ισχύει ότι η ομάδα $Gal(S/F) \cong M_n$ αν καΙ μόνο αν $[F(\omega) : F] = \varphi(n)$ και το πολυώνυμο $X^n - u$ είναι ανάγωγο υπέρ το F. Στην συνέχεια θα δείξουμε ότι η ομάδα $Gal(S/_F)$ είναι αβελιανή αν και μόνο αν το πολυώνυμο $X^n - u$ αναλύεται υπέρ το $F(\omega)$ αν και μόνο αν το πολυώνυμο $X^n - u$ έχει μία ρίζα στο F.

Παρατήρηση 1.2.4. *Για οποιουσδήποτε θετικούς ακεραίους a, b ισχύει ότι $F(\omega_a u^{1/a}) \leq F(\omega_{ab} u^{1/ab})$.*

Απόδειξη. Θέτουμε $K = F(\omega_a u^{1/a})$ καί $L = F(\omega_{ab} u^{1/ab})$. Το $u^{1/a}$ είναι ρίζα του πολυωνύμου $X^a - u$. Όμως $u^{1/a} = (u^{1/ab})^b$. Άρα, το $(u^{1/ab})^b$ είναι ρίζα του πολυωνύμου $X^a - u$. Οπότε το $u^{1/a} = (u^{1/ab})^b \in L$. Ακόμα το ω_a είναι πρωταρχική a-ρίζα της μονάδας, δηλαδή $(\omega_a)^a = 1$ καί $\omega_a^k \neq 1$ για κάθε $1 < k < a$. Θέτουμε $\omega_{ab} = J$. Το ω_{ab} είναι πρωταρχική ab-ρίζα της μονάδας, δηλαδή $(\omega_{ab})^{ab} = 1$, δηλαδή $J^{ab} = 1$. Το $J \in L$, άρα $J^b \in L$. Ισχύει ότι $(J^b)^a = J^{ab} = 1$. Θα δείξουμε ότι $(J^b)^k \neq 1$, για κάθε $1 < k < a$. Άν $(J^b)^k = 1 \Leftrightarrow J^{bk} = 1$. Άρα, το J είναι πρωταρχική m ρίζα της μονάδας με $m \leq bk < ab$. Άτοπο, αφού J πρωταρχική ab-ρίζα της μονάδας. Άρα το J^b είναι πρωταρχική a ρίζα της μονάδας, δηλαδή $J^b \in \Omega_a$, δηλαδή $(\omega_{ab})^b \in \Omega_a$. Δηλαδή, $(u^{1/ab})^b$ είναι ρίζα του πολυωνύμου $X^a - u$ καί $(\omega_{ab})^b \in \Omega_a$. Άρα όλες οι ρίζες του πολυωνύμου $X^a - u$ θα είναι οι $(u^{1/ab})^b, \omega_{ab}^b (u^{1/ab})^b, \ldots, (\omega_{ab}^b)^{a-1} (u^{1/ab})^b$. Δηλαδή, όλες οι ρίζες του πολυωνύμου $X^a - u$ ανήκουν στο $F(\omega_{ab}, u^{1/ab})$. Άρα, $F(\omega_a u^{1/a}) \leq F(\omega_{ab} u^{1/ab})$.

□

Θεώρημα 1.2.3. *Έστω n ένας περιττός θετικός ακέραιος και ισχύει ότι ΜΚΔ$(n, expchar(F)) = 1$. Έστω, επίσης, S ένα σώμα ανάλυσης του πολυωνύμου $X^n - u$ υπέρ το F, όπου $u \in F, u \neq 0$. Υποθέτουμε ότι $[F(\omega) : F] = \varphi(n)$, όπου $\omega \in \Omega_n$. Τότε τα ακόλουθα είναι ισοδύναμα:*
1) Η ομάδα $Gal(S/F)$ είναι αβελιανή.
2) Το πολυώνυμο $X^n - u$ έχει μία ρίζα στο F.
3) Το πολυώνυμο $X^n - u$ έχει μία ρίζα στο $F(\omega)$, (και συνεπώς αναλύεται στο $F(\omega)$).

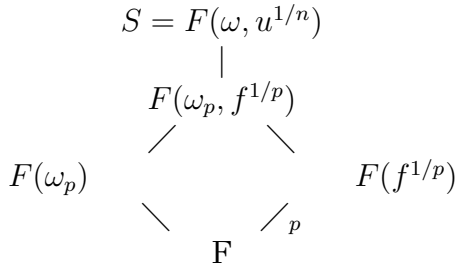
Απόδειξη. "2) ⇒ 3)" Έστω ότι το πολυώνυμο $X^n - u$ έχει μία ρίζα στο F και θα δείξουμε ότι το πολυώνυμο $X^n - u$ έχει μία ρίζα στο $F(\omega)$, (και συνεπώς αναλύεται στο $F(\omega)$). Προφανώς, αφού το $X^n - u$ έχει μία

ρίζα στο F και $F \leq F(\omega)$, τότε το $X^n - u$ έχει ρίζα στο $F(\omega)$.
$''3) \Rightarrow 1)''$

$$\begin{array}{ccc} S = F(\omega, \alpha) & \longleftrightarrow & \{Id_S\} \\ | & & | \\ F(\omega) & \longleftrightarrow & H = Gal(S/F(\omega)) \\ | & & | \\ \text{F} & \longleftrightarrow & G = Gal(S/F) \end{array}$$

Έστω ότι το πολυώνυμο $X^n - u$ έχει μία ρίζα στο $F(\omega)$ και θα δείξουμε ότι η ομάδα $Gal(S/F)$ είναι αβελιανή. Αφού, το πολυώνυμο $X^n - u$ έχει μία ρίζα στο $F(\omega)$, αυτό σημαίνει ότι το πολυώνυμο $X^n - u$ δέν είναι ανάγωγο υπέρ το $F(\omega)$. Ακόμα, αφού το πολυώνυμο $X^n - u$ έχει ρίζα στο $F(\omega)$ καί η επέκταση $F \leq F(\omega)$ είναι κυκλοτομική επέκταση, άρα η επέκταση $F \leq F(\omega)$ είναι κανονική, τότε το πολυώνυμο $X^n - u$ αναλύεται στο $F(\omega)$. Αυτό σημαίνει ότι το $F(\omega)$ είναι σώμα ανάλυσης του πολυωνύμου $X^n - u$. Όμως και το S είναι σώμα ανάλυσης του πολυωνύμου $X^n - u$. Άρα, $S \cong F(\omega)$. Δηλαδή, $S = F(\omega)$. Δηλαδή, η επέκταση $F(\omega) \leq S$ είναι τετριμμένη. Άρα, $H = \{Id_S\}$. Οπότε, $Gal(S/F) = Gal(F(\omega)/F)$. Η επέκταση $F \leq F(\omega)$ είναι επέκταση Galois, αφού η επέκταση $F \leq F(\omega)$ είναι κυκλοτομική επέκταση. Οπότε, $|Gal(F(\omega)/_F)| = [F(\omega) : F]$. Δηλαδή, $|Gal(F(\omega)/_F)| = \varphi(n)$ και ισχύει ότι η ομάδα $Gal(F(\omega)/_F)$ είναι υποομάδα της $\mathbb{Z}_n^*$ και $|\mathbb{Z}_n^*| = \varphi(n)$. Άρα, $Gal(F(\omega)/F) \cong \mathbb{Z}_n^*$. Όμως, η ομάδα $\mathbb{Z}_n^*$ είναι αβελιανή. Οπότε, η ομάδα $Gal(F(\omega)/F)$ είναι αβελιανή. Επομένως, η ομάδα $Gal(S/F)$ είναι αβελιανή.
$''1) \Rightarrow 2)''$ Έστω ότι η ομάδα $Gal(S/F)$ είναι αβελιανή. Θα δείξουμε ότι το πολυώνυμο $X^n - u$ έχει μία ρίζα στο F. Έστω $k \mid n$, με k να είναι ο μεγαλύτερος διαιρέτης του n τέτοιο ώστε $u \in F^k$, δηλαδή $u = f^k$ με $f \in F$. Αν $k = n$ τότε $u = f^n \Rightarrow f^n - u = 0$ με $f \in F$. Άρα, το πολυώνυμο $X^n - u$ έχει μία ρίζα στο F. Άν $k < n$ τότε: $\frac{n}{k} > 1$. Έστω p πρώτος αριθμός τέτοιος ώστε $p \mid \frac{n}{k}$, δηλαδή $\frac{n}{k} = ps$, $s \in \mathbb{Z}$, δηλαδή $n = kps$. Θεωρούμε την αλυσίδα σωμάτων $F \leq F(\omega_p) \leq F(\omega_p, f^{1/p}) \leq F(\omega, u^{1/n}) = S$. Πράγματι, $F(\omega_p, f^{1/p}) \leq F(\omega, u^{1/n})$, το οποίο προκύπτει απο την παρατήρηση 1.2.4. Ακόμα ισχύει ότι το πολυώνυμο $X^p - f$ είναι ανάγωγο υπέρ το F. Άν το πολυώνυμο $X^p - f$ δεν ήταν ανάγωγο υπέρ το F, τότε αφού το p είναι πρώτος αριθμός τότε σύμφωνα με το θεώρημα 1.1.1 προκύπτει ότι $f \in F^p$. Δηλαδή, $f = g^p$ με $g \in F$. Όμως, $u = f^k = g^{kp} \in F^{kp}$. Αντίφαση, αφού εξ' ορισμού το k είναι ο μεγαλύτερος διαιρέτης του n τέτοιος ώστε $u \in F^k$. Άρα, το πολυώνυμο $X^p - f$ είναι ανάγωγο υπέρ το F. Ακόμα, το $f^{1/p}$ είναι ρίζα του πολυωνύμου $X^p - f$. Άρα, $Irr(f^{1/p}, F) = X^p - f$. Δηλαδή, $[F(f^{1/p}) : F] = p$. Επίσης, $[F(\omega_p) : F] \leq \varphi(p) = p - 1$. Ισχύει ότι $[F(\omega) : F] = \varphi(n)$, δηλαδή η επέκταση $F \leq F(\omega)$ είναι μή τετριμμένη.

Άρα, $\omega \notin F$. Δηλαδή οι πρωταρχικές n- ρίζες της μονάδας δέν ανήκουν στο F. Ακόμα, $[F(\omega_p, f^{1/p}) : F] = [F(\omega_p, f^{1/p}) : F(\omega_p)][F(\omega_p) : F]$.



$[F(\omega_p) : F] = t \leq p-1$. Άρα, ΜΚΔ$(p,t) = 1$. Οπότε, $[F(\omega_p, f^{1/p}) : F(\omega_p)] = p$. Άρα η επέκταση $F(\omega_p) \leq F(\omega_p, f^{1/p})$ είναι μη τετριμμένη.
Απομένει να δείξουμε ότι η επέκταση $F \leq F(\omega_p)$ είναι μη τετριμμένη. Άν η επέκταση $F \leq F(\omega_p)$ είναι τετριμμένη, τότε $\omega_p \in F$. Αλλά τότε $[F(\omega) : F] < \varphi(n)$, άτοπο. Άρα, η επέκταση $F \leq F(\omega_p)$ είναι μη τετριμμένη.
Δηλαδή οι επεκτάσεις $F \leq F(\omega_p)$ καί $F(\omega_p) \leq F(\omega_p, f^{1/p})$ είναι μη τετριμμένες. Οπότε απο το λήμμα 1.2.2 προκύπτει ότι η ομάδα $Gal(F(\omega_p, f^{1/p})/_F)$ δέν είναι αβελιανή. Άτοπο, αφού απο υπόθεση έχουμε ότι η ομάδα $Gal(S/_F)$ είναι αβελιανή και $Gal(F(\omega_p, f^{1/p})/F) \cong \frac{Gal(S/_F)}{Gal(S/F(\omega_p, f^{1/p}))}$ [9].

□

Το θεώρημα 1.2.3 δεν ισχύει όταν το n είναι άρτιος.

Παράδειγμα 1.2.1. *$\sqrt{2} \in \mathbb{Q}(\omega)$ καί ω είναι πρωταρχική 8-ρίζα της μονάδας. Ακόμα, $[F(\omega) : F] = \varphi(8) = 4$. Το $S = \mathbb{Q}(i, \sqrt{2})$ είναι σώμα ανάλυσης του πολυωνύμου $f(X) = X^8 - 2 \in \mathbb{Q}[X]$. Ισχύει ότι η ομάδα $Gal(S/F)$ είναι αβελιανή. Όμως, το πολυώνυμο $f(X) = X^8 - 2$ είναι ανάγωγο υπέρ το $F = \mathbb{Q}$, σύμφωνα με το κριτήριο του Eisenstein για $p = 2$. Οπότε το θεώρημα 1.2.3 δεν ισχύει για n άρτιο αριθμό.*

Στην συνέχεια θα γενικεύσουμε το προηγούμενο θεώρημα προκειμένου να χαρακτηρίσουμε πότε η ομάδα $Gal(S/F)$ είναι αβελιανή. Το θεώρημα που θα ακολουθήσει αποτελεί ενδιαφέρον αποτέλεσμα επειδή δείχνει ότι η σχέση ανάμεσα στις n-ρίζες της μονάδας και το σώμα F, επηρεάζει την αντιμεταθετικότητα της ομάδας $Gal(S/F)$.
Αρχικά θα εξετάσουμε ένα άλλο ενδιαφέρον θεώρημα.

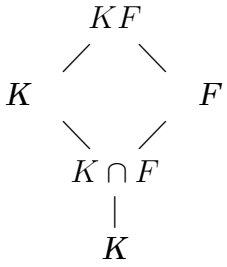
Θεώρημα 1.2.4. *Έστω ότι τα πολυώνυμα $X^n - a$ καί $X^n - b$ είναι ανάγωγα υπέρ το F και υποθέτουμε ότι το F περιέχει μία πρωταρχική*

[9] Προκύπτει απο το Θεμελιώδες Θεώρημα της Θεωρίας Galois.

n-ρίζα της μονάδας. Τότε τα πολυώνυμα $X^n - a$ *καί* $X^n - b$ *έχουν το ίδιο σώμα ανάλυσης υπέρ το* F *αν και μόνο αν* $b = c^n a^r$ *για κάποιο* $c \in F$ *και ΜΚΔ*$(r, n) = 1$.

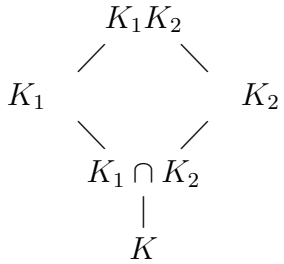
Για την απόδειξη του (βλ [6]),λήμμα 3.6, σελ. 437

Θεώρημα 1.2.5. *Έστω η επέκταση Galois* $K' \leq K$ *καί η τυχαία επέκταση* $K' \leq F$. *Τότε οι επεκτάσεις* $F \leq KF$ *και* $K \cap F \leq K$ *είναι επεκτάσεις Galois. Θέτουμε* $H = Gal(KF/F)$ *καί* $G = Gal(K/K')$. *Άν* $\sigma \in H$ *τότε* $Rest_K\sigma \in G$ *και η απεικόνιση όπου* $\sigma \mapsto Rest_K\sigma$ *επάγει ότι* $H \approxeq Gal(K/_{K\cap F})$.



Θεώρημα 1.2.6. *Έστω οι επεκτάσεις Galois* $K \leq K_1$ *καί* $K \leq K_2$, *με* $G_1 = Gal(K_1/K), G_2 = Gal(K_2/K)$. *Τότε η επέκταση* $K \leq K_1K_2$ *είναι επέκταση Galois, με* $G = Gal(K_1K_2/K)$. *Η απεικόνιση* $G \to G_1 \times G_2$ *όπου* $\sigma \mapsto (Rest_{K_1}\sigma, Rest_{K_2}\sigma)$ *είναι μονομορφισμός. Άν* $K_1 \cap K_2 = K$ *τότε η απεικόνιση αυτή είναι ισομορφισμός.*

Απόδειξη. Αφού οι επεκτάσεις $K \leq K_1$ και $K \leq K_2$ είναι επεκτάσεις Galois τότε καί η επέκταση $K \leq K_1K_2$ είναι επέκταση Galois.



Διότι αφού η επέκταση $K \leq K_1$ είναι επέκταση Galois τότε καί η επέκταση $K_2 \leq K_1K_2$ είναι επέκταση Galois. Ομοίως, αφού η επέκταση $K \leq K_2$ είναι επέκταση Galois, τότε καί η επέκταση $K_1 \leq K_1K_2$ είναι επέκταση Galois. Οπότε, η επέκταση $K \leq K_1K_2$ είναι επέκταση Galois.

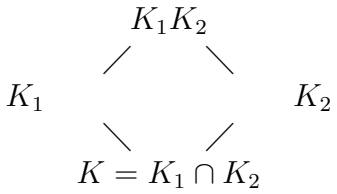
Η απεικόνιση $\varphi : G \to G_1 \times G_2$ είναι ομομορφισμός, διότι

$$\begin{aligned}\varphi(\sigma_1\sigma_2) &= (Rest_{K_1}\sigma_1\sigma_2, Rest_{K_2}\sigma_1\sigma_2)\\ &= (Rest_{K_1}\sigma_1 Rest_{K_1}\sigma_2, Rest_{K_2}\sigma_1 Rest_{K_2}\sigma_2)\\ &= (Rest_{K_1}\sigma_1, Rest_{K_2}\sigma_1)(Rest_{K_1}\sigma_2, Rest_{K_2}\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)\end{aligned}$$

Δηλαδή η φ είναι ομομορφισμός.

Έστω e_i το ταυτοτικό στοιχείο στην ομάδα G_i, για $i = 1, 2$. Στην συνέχεια θα δείξουμε ότι η απεικόνιση φ είναι ένα προς ένα. Έστω $\sigma \in Ker\varphi$. Ισχύει ότι $\sigma \in Ker\varphi \Leftrightarrow \varphi(\sigma) = (Rest_{K_1}e_1,\ Rest_{K_2}e_2) \Leftrightarrow \sigma = id$. Άρα η απεικόνιση φ είναι ένα πρός ένα. Επομένως, η απεικόνιση φ είναι μονομορφισμός.

Έστω τώρα ότι $K_1 \cap K_2 = K$. Θα δείξουμε ότι η απεικόνιση φ είναι ισομορφισμός. Απομένει να δείξουμε ότι η απεικόνιση φ είναι επί. Σύμφωνα με το θεώρημα 1.2.5 έχουμε ότι άν $\sigma_1 \in G_1 = Gal(K_1/_K)$ τότε υπάρχει $\sigma \in Gal(K_1K_2/_{K_2})$ τέτοιο ώστε $Res_{K_1}\sigma = \sigma_1 \in G_1$. Αλλά $\sigma \in G = Gal(K_1K_2/_K)$



Ακόμα ισχύει ότι $Gal(K_1K_2/K_2) \cong Gal(K_1/K)$, $\sigma \in Gal(K_1K_2/K)$ και $\sigma \in Gal(K_1/K)$. Άρα, $Rest_{K_2}\sigma = e_2$. Οπότε, $G_1 \times \{e_2\} \subseteq \varphi(G) = Im(\varphi)$. Ομοίως, $\{e_1\} \times G_2 \subset \varphi(G) = Im(\varphi)$. Άρα και το γινόμενο των $H_1 = G_1 \times \{e_2\}, H_2 = \{e_1\} \times G_2$ περιέχεται στην $Im(\varphi)$, δηλαδή $H_1H_2 = G_1 \times G_2 \leq Im(\varphi)$. Αλλά, $Im(\varphi) \leq G_1 \times G_2$. Άρα, $Im(\varphi) = G_1 \times G_2$. Οπότε, η απεικόνιση φ είναι επί. Επομένως, η απεικόνιση φ είναι ισομορφισμός. □

Σχόλιο 1.2.2. *Η απεικόνιση $\varphi : G \to G_1 \times G_2$ είναι μονομορφισμός. Άρα ταυτίζουμε πρότυπα με εικόνες, δηλαδή $G \cong \varphi(G) \leq G_1 \times G_2$.*

Παρατήρηση 1.2.5. *Έστω F σώμα και U_n είναι η ομάδα των n-ριζών της μονάδας υπέρ το F. Τότε το $U_n \cap F^*$ είναι μια κυκλική υποομάδα της U_n και συνεπώς είναι U_m για κάποιο $m \mid n$.*

Απόδειξη. Αρχικά θα δείξουμε ότι η $U_n \cap F^* = A$ είναι υποομάδα της U_n. Αρκεί να δείξουμε ότι i) $1_{U_n} \in A$. ii) Για κάθε $a, b \in A$ τότε $ab \in A$. iii) Για κάθε $a \in A$ τότε $a^{-1} \in A$.

F^* είναι το σύνολο των αντιστρέψιμων στοιχείων του F. Οπότε $F^* = F \setminus \{0\}$.
i) Το $1_{U_n} \in A$, διότι $1_{U_n} = 1 \in F^*$.
ii) Εστώ $a, b \in A$. $a \in A$ δηλαδή $a \in U_n$ καί $a \in F^*$. Δηλαδή $a^n = 1$ καί υπαρχεί $a' \in F$ τ.ω $aa' = 1 = a'a$. Ομοίως, $b \in A$, δηλαδή $b \in U_n$ καί $b \in F^*$. Δηλαδή, $b^n = 1$ καί υπάρχει $b' \in F$ τ.ω $bb' = 1 = b'b$. Τα $a, b \in F* = F \setminus \{0\}$ καί F είναι σώμα. Άρα $ab \in F^*$. Ακόμα, $a, b \in U_n$ καί η U_n είναι αβελιανή. $(ab)^n = a^n b^n = 1$. Άρα, $ab \in U_n$.
Δηλαδή, $ab \in U_n$ καί $ab \in F^*$. Άρα, $ab \in A$.
iii) Έστω $a \in A$. Δηλαδή, $a \in U_n$ καί $a \in F^*$. $a \in F^*$ δηλαδή υπάρχει $a' \in F$ τ.ω $aa' = 1 = a'a$. Άρα, $a' \in F^*$. Θέτουμε $a' = a^{-1}$. Έχουμε $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, αφού $a \in U_n$, άρα $a^{-1} \in U_n$ καί U_n αβελιανή. Άρα, $a^{-1} \in U_n$ καί $a^{-1} \in F^*$. Δηλαδή, $a^{-1} \in A$.
Οπότε, η ομάδα A είναι υποομάδα της U_n. Ακόμα, ισχύει ότι η ομάδα U_n είναι κυκλική(βλ.παρατήρηση 1[Παράρτημα]). Επομένως, η ομάδα $A = U_n \cap F^*$ είναι κυκλική υποομάδα της U_n. Άρα θα υπάρχει ω_n^a τ.ω $A =< \omega_n^a >$. Θέτουμε $\omega_m = \omega_n^a$. Άρα, $A =< \omega_m >, m \mid n$. Συνεπώς, $A = U_m, m \mid n$.

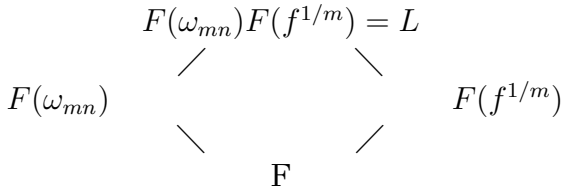
□

Θεώρημα 1.2.7. *Έστω n ένας περιττός θετικός ακέραιος και ισχύει ότι ΜΚΔ$(n, expchar(F)) = 1$. Έστω, επίσης, U_n είναι η ομάδα των n-ριζών της μονάδας υπέρ το F και $U_m = U_n \cap F^*$. Άν S είναι σώμα ανάλυσης του $X^n - u$, όπου $u \neq 0, u \in F$, τότε η ομάδα Galois $Gal(S/F)$ είναι αβελιανή αν και μόνο αν $u^m \in F^n$.*

Απόδειξη. Από την παρατήρηση 1.2.5 έχουμε ότι η U_m είναι κυκλική. Άρα, $U_m =< \omega_m >$. Έτσι, ισχύει ότι $\omega_i \in F \Leftrightarrow \omega_i \in U_n \cap F^* \Leftrightarrow \omega_i \in U_m \Leftrightarrow i \mid m$. Διότι $\omega_i \in U_m \Leftrightarrow \omega_i = \omega_m^\lambda$ με $\lambda \in \mathbb{N}$. Ισχύει ότι $\omega_i^i = 1 \Leftrightarrow \omega_m^{\lambda i} = 1$. Όμως, $ord(\omega_m) = m$. Άρα, $i \mid m$. Δηλαδή, $\omega_i \in F \Leftrightarrow i \mid m$.

$''\Leftarrow''$ Υποθέτουμε ότι $u^m \in F^n$. Θα δείξουμε ότι η ομάδα $Gal(S/F)$ είναι αβελιανή.
Έχουμε ότι $u^m \in F^n$, δηλαδή $u^m = f^n$, με $f \in F$. Ακόμα, το $u^{1/n}$ είναι ρίζα του $X^n - u$ καί το $f^{1/m}$ είναι ρίζα του $X^m - f$. Αλλά ισχύει ότι $(u^{1/n})^m = u^{m/n} = (u^m)^{1/n} = (f^n)^{1/n} = f$. Δηλαδή, $(u^{1/n})^m = f \Leftrightarrow (u^{1/n})^m - f = 0$. Αυτό σημαίνει ότι το $u^{1/n}$ είναι ρίζα του $X^m - f$. Οι ρίζες του $X^m - f$ είναι οι $f^{1/m}, \omega_m f^{1/m}, \ldots, \omega_m^{m-1} f^{1/m}$. Ακόμα, $F(\omega_m) \leq F(\omega_{mn})$. Άρα, θα

υπάρχει $k \in \mathbb{Z}$ τ.ω $u^{1/n} = \omega_{mn}^k f^{1/m}$. Αποδείξαμε ότι $m \mid m \Leftrightarrow \omega_m \in F$. Ακόμα, η επέκταση $F \leq F(f^{1/m})$ είναι καθαρού τύπου m (pure of type m), διότι ΜΚΔ$(m, expcharF) = 1$, $\omega_m \in F$ και το $f^{1/m}$ είναι ρίζα του $X^m - f$. Οπότε, σύμφωνα με την παρατήρηση ??[Παράρτημα] προκύπτει ότι η επέκταση $F \leq F(f^{1/m})$ είναι κυκλική. Άρα, η επέκταση $F \leq F(f^{1/m})$ είναι αβελιανή. Ακόμα, η επέκταση $F \leq F(\omega_{mn})$ είναι αβελιανή, διότι η ομάδα Galois $Gal(F(\omega_{mn})/F)$ είναι υποομάδα της $\mathbb{Z}_{mn}^*$. Όμως, η $\mathbb{Z}_{mn}^*$ είναι αβελιανή. Άρα και η ομάδα $Gal(F(\omega_{mn})/F)$ είναι αβελιανή. Οπότε, η επέκταση $F \leq F(\omega_{mn})$ είναι αβελιανή. Δηλαδή, οι επεκτάσεις $F \leq F(\omega_{mn})$ καί $F \leq F(f^{1/m})$ είναι αβελιανές. Ισχύει ότι $F \leq F(\omega_{mn})F(f^{1/m}) = F(\omega_{mn}, f^{1/m}) = F(\omega_{mn}, u^{1/n})$.



Η επέκταση $F \leq F(\omega_{mn})$ είναι αβελιανή, άρα ισχύει ότι η ομάδα Galois $Gal(F(\omega_{mn})/_F)$ είναι αβελιανή. Ακόμα, η ομάδα Galois $Gal(F(f^{1/m})/_F)$ είναι αβελιανή, διότι η επέκταση $F \leq F(f^{1/m})$ είναι αβελιανή. Οπότε, έχουμε ότι οι επεκτάσεις $F \leq F(\omega_{mn})$ καί $F \leq F(f^{1/m})$ είναι επεκτάσεις Galois. Επομένως, σύμφωνα με το θεώρημα 1.2.6 προκύπτει ότι η επέκταση $F \leq F(f^{1/m})F(\omega_{mn})$ είναι επέκταση Galois. Ακόμα, άν $G_1 = Gal(F(f^{1/m})/F)$, $G_2 = Gal(F(\omega_{mn})/F)$ και $G = Gal(L/F)$, τότε ισχύει ότι η απεικόνιση $\varphi : G \to G_1 \times G_2$, όπου $\sigma \mapsto (Rest_{K_1}\sigma\,,\, Rest_{K_2}\sigma)$ είναι μονομορφισμός. Ταυτίζουμε πρότυπα με εικόνες, $G \cong \varphi(G) \leq G_1 \times G_2$ και έτσι θεωρούμε ότι η G είναι υποομάδα της $G_1 \times G_2$. Όμως, η ομάδα $G_1 \times G_2$ είναι αβελιανή διότι έχουμε αποδείξει ότι οι ομάδες G_1, G_2 είναι αβελιανές.Οπότε, η ομάδα G είναι αβελιανή. Επομένως, η επέκταση $F \leq L$ είναι αβελιανή. Όμως, $L = F(\omega_{mn})F(f^{1/m}) = F(\omega_{mn}, u^{1/m})$. Άρα, η επέκταση $F \leq F(\omega_{mn}, u^{1/n})$ είναι αβελιανή. Ακόμα, ισχύει ότι $F \leq S \leq F(\omega_{mn}, u^{1/n})$. Άρα, η επέκταση $F \leq S$ είναι αβελιανή. Οπότε, η ομάδα Galois $Gal(S/F)$ είναι αβελιανή.
$''\Rightarrow''$ Έστω ότι η ομάδα Galois $Gal(S/F)$ είναι αβελιανή. Θα δείξουμε ότι $u^m \in F^n$.
Υποθέτουμε ότι k είναι ο μεγαλύτερος θετικός ακέραιος τέτοιος ώστε $m \mid k$ καί $k \mid n$ καί $u^m \in F^k$. Το $u^m \in F^k$ σημαίνει ότι $u^m = f^k$ με $f \in F$. Θα δείξουμε ότι $k = n$.Έστω ότι $k < n$ και p ένας πρώτος αριθμός όπου $p \mid \frac{n}{k}$. Υποθέτουμε ότι p^s να είναι η μεγαλύτερη δύναμη του p τέτοια

ώστε $p^s \mid m$ [10]. Αρχικά, θα δείξουμε ότι η επέκταση $F \leq F(\omega_{p^{s+1}}, f^{1/p^{s+1}})$ είναι αβελιανή. Θέτουμε $q = p^{s+1}$. Έχουμε, $p^s \mid m$ καί $m \mid k$, άρα $p^s \mid k$, δηλαδή $k = p^s\mu$, $\mu \in \mathbb{Z}$. Ακόμα, $p \mid \frac{n}{k} \Leftrightarrow \frac{n}{k} = p\lambda \Leftrightarrow n = kp\lambda$, $\lambda \in \mathbb{Z}$. Οπότε, $n = p^s\mu p\lambda \Leftrightarrow n = p^{s+1}\mu\lambda$, $\mu\lambda \in \mathbb{Z}$. Δηλαδή, $p^{s+1} \mid n \Leftrightarrow q \mid n$. Για να δείξουμε ότι η επέκταση $F \leq F(\omega_{p^{s+1}}, f^{1/p^{s+1}})$ είναι αβελιανή, αρκεί να ενσωματώσουμε αυτήν την επέκταση σε μια αβελιανή επέκταση. Ισχύει ότι $(f^{1/q})^{kq} = f^k = u^m = (u^{m/kq})^k q$. Το $u^{m/kq}$ είναι ρίζα του πολυωνύμου $X^{kq} - u^m$. Ακόμα, το $f^{1/q}$ είναι ρίζα του πολυωνύμου $X^{kq} - u^m$. Όμως οι ρίζες του $X^{kq} - u^m$ είναι οι $u^{m/kq}$, $u^{m/kq}\omega_{kq}, \ldots, u^{m/kq}\omega_{kq}^{kq-1}$. Άρα $f^{1/q} = \omega_{kq}^j u^{m/kq}$ για κάποιο j. Οπότε $F(\omega_q,\, f^{1/q}) \leq F(\omega_{kq}, f^{1/q}) = F(\omega_{kq}, u^{m/kq})$. Ακόμα, $p \mid \frac{n}{k}$, άρα υπάρχει $a \in \mathbb{Z}_+$ τ.ω $\frac{n}{k} = pa \Leftrightarrow n = apk$ καί $p^s \mid m$. Άρα, $\frac{mn}{kq} = \frac{mn}{kp^{s+1}} = \frac{mapk}{kp^{s+1}} = \frac{ma}{p^s}$. Αλλά $p^s \mid m$, έτσι το $\frac{ma}{p^s}$ είναι θετικός ακέραιος. Επίσης, το $\upsilon = (u^{1/n})^{\frac{nm}{kq}}$ είναι ρίζα του $X^{kq} - u^m$ καί το $\upsilon \in F(\omega_{kq}, u^{1/n})$. Άρα, όλες οι ρίζες του $X^{kq} - u^m$ ανήκουν στο $F(\omega_{kq}, u^{1/n})$. Οπότε, $F(\omega_{kq}, u^{m/kq}) \leq F(\omega_{kq}, u^{1/n})$. Επομένως,

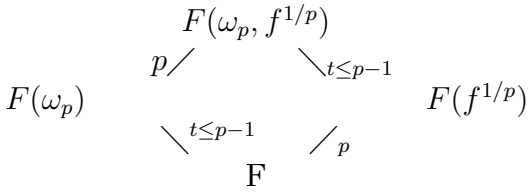
$$F \leq F(\omega_q, f^{1/q}) \leq F(\omega_{kq}, u^{m/kq}) \leq F(\omega_{kq}, u^{1/n}) \leq F(\omega_{kq})F(\omega_n, u^{1/n})$$

Η επέκταση $F \leq F(\omega_{kq})$ είναι αβελιανή, διότι η ομάδα Galois $Gal(F(\omega_{kq})/F)$ είναι υποομάδα της $\mathbb{Z}_{kq}^*$, αφού η επέκταση $F \leq F(\omega_{kq})$ είναι κυκλοτομική επέκταση καί η ομάδα $\mathbb{Z}_{kq}^*$ είναι αβελιανή. Άρα και η ομάδα $GalF(\omega_{kq})/F$ είναι αβελιανή. Οπότε η επέκταση $F \leq F(\omega_{kq})$ είναι αβελιανή.
Ακόμα, η επέκταση $F \leq F(\omega_n, u^{1/n})$ είναι αβελιανή, αφού από υπόθεση έχουμε ότι η ομάδα Galois $Gal(S/F)$ είναι αβελιανή.
Άρα, σύμφωνα με το θεώρημα 1.2.6 προκύπτει ότι η επέκταση $F \leq F(\omega_n, u^{1/n})$ είναι αβελιανή. Οπότε και η επέκταση $F \leq F(\omega_q, f^{1/q})$ είναι αβελιανή. Έπειτα θεωρούμε την αλυσίδα σωμάτων

$$F \leq F(\omega_q) \leq F(\omega_q, f^{1/q})$$

Παρατηρούμε ότι το πολυώνυμο $X^p - f$ είναι ανάγωγο υπέρ το F. Διότι, αν το πολυώνυμο $X^p - f$ δέν ήταν ανάγωγο υπέρ το F, τότε σύμφωνα με το θεώρημα 1.1.1, το πολυώνυμο $X^p - f$ θα είχε ρίζα στο F, έστω $g \in F$. Δηλαδή, $g^p - f = 0 \Leftrightarrow g^p = f$. Δηλαδή, $f = g^p \in F^p$ με $g \in F$. Όμως, $u^m = f^k = g^{pk} \in F^{pk}$. Άτοπο, αφού εξ' ορισμού το k είναι ο μεγαλύτερος θετικός ακέραιος τέτοιος ώστε $u^m \in F^k$. Άρα, το $X^p - f$ είναι ανάγωγο υπέρ το F. Εξετάζουμε την περίπτωση όπου $s = 0$. Άν $s = 0$ τότε $q = p^{s+1} = p$.

[10] Στο θεώρημα 1.2.3 οι υποθέσεις n να είναι περιττός αριθμός και $[F(\omega) : F] = \varphi(n)$ δίνουν ότι $m = 1$, έτσι $s = 0$.



Το $X^p - f$ είναι ανάγωγο υπέρ το F, άρα $[F(f^{1/p}) : F] = degIrr(f^{1/p}, F) = p$. Ισχύει ότι $t := [F(\omega_p) : F] \leq \varphi(p) = p - 1$. Ακόμα, $[F(\omega_p, f^{1/p}) : F] = [F(\omega_p, f^{1/p}) : F(\omega_p)][F(\omega_p) : F]$ καί ΜΚΔ$(p, t) = 1$. Άρα, $[F(\omega_p, f^{1/p}) : F(\omega_p)] = p$. Δηλαδή, $[F(\omega_p, f^{1/p}) : F] \leq p(p-1)$. Άρα, $[F(\omega_p, f^{1/p}) : F] \geq p$. Ακόμα, $p \nmid m$, διότι p^0 είναι η μεγαλύτερη δύναμη του p τέτοια ώστε $p^0 \mid m$. Οπότε, $\omega_p \notin F$. Άρα, η επέκταση $F \leq F(\omega_p)$ είναι μη τετριμμένη. Ακόμα, $[F(\omega_p, f^{1/p}) : F(\omega_p)] = p$. Άρα, η επέκταση $F(\omega_p) \leq F(\omega_p, f^{1/p})$ είναι μη τετριμμένη. Οπότε, σύμφωνα με το λήμμα 1.2.2 προκύπτει ότι η ομάδα Galois $Gal(F(\omega_p, f^{1/p})/F(\omega_p))$ δεν είναι αβελιανή. Δηλαδή, η επέκταση $F(\omega_p) \leq F(\omega_p, f^{1/p})$ δεν είναι αβελιανή. Άτοπο, αφού έχουμε αποδείξει ότι η επέκταση $F(\omega_q) \leq F(\omega_q, f^{1/q})$ είναι αβελιανή καί $q = p$. Εξετάζουμε τώρα την περίπτωση που $s > 0$. Δηλαδή, τώρα το $q = p^{s+1}$. Τότε, $p \mid m$ καί $p^s \mid m$. Θέτουμε $r = p^s$. Όμως, ισχύει ότι $p^{s+1} \nmid m$. Ισχύει ότι $p \mid m \Leftrightarrow \omega_p \in F$ καί $r \mid m \Leftrightarrow \omega_r \in F$ και $q = p^{s+1} \nmid m \Leftrightarrow \omega_q \notin F$. Επειδή, $\omega_r \in F$ τότε το διώνυμο $X^p - \omega_r$ είτε είναι ανάγωγο υπέρ το F, είτε αναλύεται πλήρως υπέρ το F [11]. Όμως, το ω_q είναι ρίζα του $X^p - \omega_r$ και $\omega_q \notin F$. Άρα, το $X^p - \omega_r$ είναι ανάγωγο υπέρ το F. Οι ρίζες του $X^p - \omega_r$ είναι οι $\omega_q, \omega_p\omega_q, \ldots, \omega_p^{p-1}\omega_q$.Άρα, για κάθε $j \in \mathbb{Z}_p$ υπάρχει $\sigma_j \in Gal(F(\omega_q)/F)$ τέτοιο ώστε $\sigma_j(\omega_q) = \omega_p^j\omega_q$. Θέλουμε να δείξουμε ότι η ομάδα Galois $Gal(F(\omega_q, f^{1/q})/F)$ δεν είναι αβελιανή. Αρκεί να δείξουμε ότι υπάρχουν $i, j \in \mathbb{Z}_p$ τέτοια ώστε $\sigma_i\sigma_j \neq \sigma_j\sigma_i$ με $\sigma_i, \sigma_j \in Gal(F(\omega_q, f^{1/q})/F)$. Έστω, $\sigma_0, \sigma_1 \in Gal(F(\omega_q)/F)$ όπου $\sigma_0 = id$ και $\sigma_1 : \omega_q \mapsto \omega_p\omega_q$. Υπάρχουν δύο περιπτώσεις: Άν το πολυώνυμο $X^q - f \in F[X]$ είναι ανάγωγο υπέρ το $F(\omega_q)$, τότε επεκτείνουμε τα σ_0 και σ_1 σε στοιχεία της ομάδας Galois $Gal(F(\omega_q, f^{1/q})/F)$ ορίζοντας

$$\sigma_{0,1} : \begin{cases} \omega_q \mapsto \omega_q \\ f^{1/q} \mapsto \omega_q f^{1/q} \end{cases} \quad \text{και} \quad \sigma_{1,0} : \begin{cases} \omega_q \mapsto \omega_p\omega_q \\ f^{1/q} \mapsto f^{1/q} \end{cases}$$

Έτσι $\sigma_{0,1}(\sigma_{1,0}(f^{1/q})) = \sigma_{0,1}(f^{1/q}) = \omega_q f^{1/q}$ καί $\sigma_{1,0}(\sigma_{0,1}(f^{1/q})) = \sigma_{1,0}(\omega_q)\sigma_{1,0}(f^{1/q}) = \omega_p\omega_q f^{1/q}$. Δηλαδή, $\sigma_{0,1}(\sigma_{1,0}(f^{1/q})) \neq \sigma_{1,0}(\sigma_{0,1}(f^{1/q}))$, αφού $\omega_r \neq 1$. Άρα, η ομάδα Galois $Gal(F(\omega_q, f^{1/q})/F)$ δεν είναι αβελιανή. Δηλαδή, η επέκταση $F \leq F(\omega_q, f^{1/q})$ δεν είναι αβελιανή. Άτοπο, αφού αποδείξαμε ότι η επέκταση $F \leq F(\omega_q, f^{1/q})$ είναι αβελιανή.

[11] Διότι άν είχε μία ρίζα,τότε θα τις είχε όλες, αφού οι ρίζες του $X^p - \omega_r$ θα έιναι τις μορφής $\omega_r^{1/p}\omega_p^i$ με $i = 0, \ldots, p-1$.

Άν τώρα το $X^p - f$ δεν είναι ανάγωγο υπέρ το σώμα $F(\omega_q)$, τότε σύμφωνα με το θεώρημα 1.1.1 προκύπτει ότι το $X^p - f$ έχει ρίζα στο $F(\omega_q)$, δηλαδή $f \in F(\omega_q)^p$. Άρα, $\beta^p - f = 0 \Leftrightarrow f = \beta^p$, για κάποιο $\beta \in F(\omega_q)$ και έτσι $F(\beta) \leq F(\omega_q)$. Έχουμε ότι τα πολυώνυμα $X^p - \omega_r$ και $X^p - f$ είναι ανάγωγα υπέρ το F. Το β είναι ρίζα του $X^p - f$, άρα $[F(\beta) : F] = p$. Το ω_q είναι ρίζα του $X^p - \omega_r$, άρα $[F(\omega_q) : F] = p$. Και έχουμε ότι $F(\beta) \leq F(\omega_q)$. Οπότε, $F(\beta) = F(\omega_q)$. Άρα, τα πολυώνυμα $X^p - \omega_r$ και $X^p - f$ έχουν το ίδιο σώμα ανάλυσης υπέρ το F. Ακόμα, το F περιέχει μια πρωταρχική p-ρίζα της μονάδας, την ω_p. Οπότε, απο το θεώρημα 1.2.4 έχουμε ότι $f = \omega_r^i \upsilon^p$ με $\upsilon \in F$ και ΜΚΔ$(j, n) = 1$. Έχουμε ότι $r = p^s \mid m$ και $m \mid k$, άρα $r = p^s \mid k$. Οπότε, $f = \omega_r^j \upsilon^p \to f^k = \omega_r^{kj} \upsilon^{kp} = \upsilon^{kp}$, αφού $r \mid k$. Όμως, $f^k = u^m$. Άρα, $u^m = \upsilon^{kp}$, με $\upsilon \in F$. Άτοπο, αφού k είναι ο μεγαλύτερος θετικός ακέραιος τέτοιος ώστε $u^m \in F^k$ και $kp > k$. Επομένως, $k = n$. Άρα, $u^m \in F^n$. □

1.3 Η Ανεξαρτησια των Άρρητων Άριθμών

Ισχύει ότι αν p πρώτος τότε $\sqrt{p} \notin \mathbb{Q}$. Διότι, αν $\sqrt{p} \in \mathbb{Q}$, τότε έστω $\sqrt{p} = \frac{a}{b}$, ΜΚΔ$(a, b) = 1$, $a, b \in \mathbb{Z}, b \neq 0$. Άρα, $p = \frac{a^2}{b^2} \Leftrightarrow a^2 = pb^2$. Άν $b = 1$ τότε $a^2 = p$. Άτοπο, αφού το p είναι πρώτος αριθμός και έτσι το p δεν είναι τετραγωνο ακεραίου. Άν $b \neq 1$ τότε υπάρχει p' πρώτος τέτοιος ώστε $p' \mid b \Rightarrow p' \mid b^2 \Rightarrow p' \mid pb^2$. Δηλαδή, $p' \mid a^2$ και αφού p' είναι πρώτος τότε $p' \mid a$. Δηλαδή, $p' \mid a$ και $p' \mid b$. Άρα, $p' \mid$ ΜΚΔ$(a, b) = 1$, δηλαδή $p' \mid 1$, άτοπο αφού το p είναι πρώτος. Οπότε το $\sqrt{p} \notin \mathbb{Q}$, δηλαδή το $\sqrt{p}$ είναι άρρητος. Επομένως, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

Σκοπός μας είναι να γενικεύσουμε το παραπάνω αποτέλεσμα για περισσότερους απο έναν πρώτο αριθμό p και για ρίζες βαθμού n με $n \geq 2$, δηλαδή για $\sqrt[n]{m}$, $m = p_1 \cdots p_k$. Θα περιοριστούμε στην περίπτωση όπου n είναι περιττός αριθμός.

Συμβολισμός: Άν $\alpha > 0$ είναι ρητός αριθμός, τότε το $\sqrt[n]{\alpha}$ ή $\alpha^{1/n}$ θα συμβολίζει την πραγματική θετική n-ρίζα του α.

Λήμμα 1.3.1. *Έστω $u = \frac{a}{b}$ ένας θετικός ρητός αριθμός όπου $a, b > 0$ και ΜΚΔ$(a, b) = 1$. Άν $n \geq 2$ είναι ένας ακέραιος, τότε ισχύει ότι $\sqrt[n]{\frac{a}{b}} \in \mathbb{Q}$ άν και μόνο άν $a = c^n$ καί $b = d^n$ με $c, d > 0$, $c, d \in \mathbb{Z}$.*

Ειδικά, άν p πρώτος αριθμός τότε $\sqrt[n]{p} \notin \mathbb{Q}$.

Απόδειξη. $''\Rightarrow''$ Έστω $\sqrt[n]{\frac{a}{b}} \in \mathbb{Q}$. Θα δείξουμε ότι $a = c^n$ και $b = d^n$, με $c, d \in \mathbb{Z}, c, d > 0$.
Ισχύει ότι $\sqrt[n]{\frac{a}{b}} \in \mathbb{Q} \Leftrightarrow \sqrt[n]{\frac{a}{b}} = \frac{c}{d}$, ΜΚΔ$(c, d) = 1$ και $c, d > 0$, $c, d \in \mathbb{Z}$ [12]. Δηλαδή, $\frac{a}{b} = \frac{c^n}{d^n} \Leftrightarrow ad^n = bc^n$. Άρα,$a \mid bc^n$. Όμως, ΜΚΔ$(a, b) = 1$. Άρα, $a \mid c^n \Leftrightarrow c^n = ax$, $x \in \mathbb{Z}$. Επίσης, $b \mid bc^n \Rightarrow b \mid ad^n$, αλλά ΜΚΔ$(a, b) = 1$. Οπότε, ισχύει ότι $b \mid d^n \Leftrightarrow d^n = b\psi$, $\psi \in \mathbb{Z}$. Άρα,

$$\frac{a}{b} = \frac{c^n}{d^n} \Rightarrow \frac{a}{b} = \frac{ax}{b\psi} \Leftrightarrow x = \psi$$

$c^n = ax \Leftrightarrow x \mid c^n$ και $d^n = b\psi \Leftrightarrow d^n = bx \Leftrightarrow x \mid d^n$. Δηλαδή, $x \mid c^n$ και $x \mid d^n$,άρα $x \mid$ ΜΚΔ$(c^n, d^n) = 1$, αφού ΜΚΔ$(c, d) = 1$. Δηλαδή, $x \mid 1 \Leftrightarrow x = 1$. Δηλαδή, $x = \psi = 1$. Οπότε, $c^n = ax \Leftrightarrow a = c^n$ και $d^n = b\psi \Leftrightarrow b = d^n$. Δηλαδή, $a = b^n$ και $b = d^n$.
$''\Leftarrow''$ Έστω $a = c^n$ και $b = d^n$ με $c, d \in \mathbb{Z}$, $cd > 0$. Θα δείξουμε ότι $\sqrt[n]{\frac{a}{b}} \in \mathbb{Q}$.

$$\sqrt[n]{\frac{a}{b}} = \sqrt[n]{\frac{c^n}{d^n}} = \sqrt[n]{(\frac{c}{d})^n} = |\frac{c}{d}| = \frac{c}{d}, \text{αφού } c, d > 0$$

Αλλά, το $\frac{c}{d} \in \mathbb{Q}$, διότι $c, d \in \mathbb{Z}$ και $c, d > 0$. Επομένως, $\sqrt[n]{\frac{a}{b}} \in \mathbb{Q}$.

□

Στην συνέχεια υποθέτουμε ότι το n είναι περιττός και p είναι πρώτος αριθμός. Ακόμα ισχύει ότι $p \in \mathbb{Q}$, $p \neq 0$ και $p \notin \mathbb{Q}^r$, για κάθε $r \mid n$ με r πρώτο αριθμό, δηλαδή το p δεν μπορεί να γραφτεί ώς $p = a^r$, $a \in \mathbb{Q}$ και r πρώτο αριθμό διότι p είναι πρώτος αριθμός.Επίσης, $4 \nmid n$ διότι το n είναι περιττός αριθμός, άρα σύμφωνα με το θεώρημα 1.1.4 προκύπτει ότι το $X^n - p$ είναι ανάγωγο υπέρ το $\mathbb{Q}$ [13]. Μία ρίζα του $X^n - p$ είναι το $p^{1/n}$. Άρα,$[\mathbb{Q}(p^{1/n}) : \mathbb{Q}] = n$, δηλαδή $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Θα γενικεύσουμε το παραπάνω αποτέλεσμα για περισσότερους απο έναν πρώτους αριθμούς.

Θεώρημα 1.3.1. *Έστω n περιττός ακέραιος με $n \geq 3$ και $p_1, \ldots, p_m$ διαφορετικοί πρώτοι αριθμοί. Τότε ισχύει ότι* $[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}] = n^m$.

Απόδειξη. Έστω ότι n είναι περιττός με $n \geq 3$ και $\omega \in \Omega_n$. Στη περίπτωση αυτή μπορούμε να αντικαταστήσουμε το $\mathbb{Q}$ με το $\mathbb{Q}(\omega)$. Ισχύει ότι $[\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}(\omega)] \leq [\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}] \leq n^m$. Διότι,

[12] Αφού $a, b \in \mathbb{Z}$, $a, b > 0$, ΜΚΔ$(a, b) = 1$.

[13] Το $X^n - p$ είναι ανάγωγο σύμφωνα με το κριτήριο του Eisenstein για τον πρώτο p. Το οποίο μας αποδεικνύει ότι το πολυώνυμο είναι ανάγωγο και για n άρτιο αριθμό.

$$\begin{array}{ccccc} & & \mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}) = L & & \\ & \swarrow & & \searrow & \\ \mathbb{Q}(\omega) & & & & \mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}) \\ & \searrow^{\varphi(n)} & & \swarrow & \\ & & \mathbb{Q} & & \end{array}$$

Ισχύουν ότι $[\mathbb{Q}(\omega):\mathbb{Q}] = \varphi(n)$ και $[\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}] \leq n^m$ και $[L:\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m})] \leq \varphi(n)$. Ακόμα ισχύει ότι

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}]$$

και

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m})][\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}]$$

Άρα,

$$[L:\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m})][\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}]$$

Δηλαδή, $[L:\mathbb{Q}(\omega)]\varphi(n) \leq \varphi(n)[\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}]$. Δηλαδή, $[L:\mathbb{Q}(\omega)] \leq [\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}]$. Άρα, $[L:\mathbb{Q}(\omega)] \leq [\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}] \leq n^m$.
Επομένως, αρκεί να δείξουμε ότι $[\mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}(\omega)] = n^m$. Θα το αποδείξουμε με επαγωγή ως προς m. Θα αποδείξουμε ότι ισχύει για $m = 1$. Έστω p ένας πρώτος αριθμός. Το $X^n - p$ είναι ανάγωγο υπέρ το $\mathbb{Q}$. Ακόμα, το $\mathbb{Q}$ δεν περιέχει τις n-ρίζες της μονάδας εκτός απο το 1, διότι $n \geq 3$, και n περιττός[14]. Έχουμε ότι ΜΚΔ$(n, expchar(\mathbb{Q})) = 1$, διότι $ch\mathbb{Q} = 0$ και έτσι $expchar(\mathbb{Q}) = 1$. Επίσης, η επέκταση $\mathbb{Q} \leq \mathbb{Q}(\omega)$ είναι αβελιανή, αφού η ομάδα Galois $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_n^*$ και $\mathbb{Z}_n^*$ είναι αβελιανή. Δηλαδή η ομάδα Galois $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι αβελιανή. Οπότε η επέκταση $\mathbb{Q} \leq \mathbb{Q}(\omega)$ είναι αβελιανή. Επομένως, απο το θεώρημα 1.2.2 προκύπτει ότι, το $X^n - p$ είναι ανάγωγο υπέρ το $\mathbb{Q}(\omega)$. Το $p^{1/n} = \sqrt[n]{p}$ είναι ρίζα του $X^n - p$. Άρα, $[\mathbb{Q}(\omega, \sqrt[n]{p}):\mathbb{Q}(\omega)] = n$. Δηλαδή, ισχύει για $m = 1$.
Υποθέτουμε ότι ισχύει για $m \in \mathbb{Z}$ και θα δείξουμε ότι ισχύει για $m+1$. Έχουμε ότι ισχύει για $m \in \mathbb{Z}$. Δηλαδή, $[\mathbb{Q}(\omega, \sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}(\omega)] = n^m$. Έστω, p πρώτος αριθμός διαφορετικός απο τους $p_1,\ldots,p_m$. Θέτουμε, $F = \mathbb{Q}(\omega)$ και $L = \mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m})$. Έτσι, $[L:F] = n^m$. Άν το $X^n - p$ είναι ανάγωγο υπέρ το L, τότε υπάρχει r πρώτος με $r \mid n$ ώστε $p^{1/r} \in L$, το οποίο ισχύει σύμφωνα με το θεώρημα 1.1.4, διότι $4 \nmid n$. Οπότε, το $p^{1/r}$ είναι γραμμικός συνδυασμός των στοιχείων $\sqrt[n]{p_1^{e(1)}},\ldots,\sqrt[n]{p_m^{e(m)}}$, όπου $0 \leq e(i) \leq n-1$, υπέρ του $\mathbb{Q}(\omega)$. Δηλαδή, $p^{1/r} = \sum a_1\cdots a_n(\sqrt[n]{p_1})^{e(1)}\cdots(\sqrt[n]{p_m})^{e(m)}$, όπου $a_1\cdots a_n \in \mathbb{Q}(\omega)$.

[14] Αν το $n = 2$ τότε στο $\mathbb{Q}$ θα άνηκαν το ∓ 1.

Διακρίνουμε δύο περιπτώσεις:
Περίπτωση 1: Άν ο γραμμικός συνδυασμός περιέχει μόνο έναν όρο, τότε $p^{1/r} = \sqrt[r]{p} = c\sqrt[n]{p_1^{e(1)}}\sqrt[n]{p_2^{e(2)}}\cdots\sqrt[n]{p_m^{e(m)}}$, όπου $c \in \mathbb{Q}(\omega)$ και όχι όλα τα $e(i)$ να είναι ίσα με μηδέν. Άν $n = rd \Rightarrow r = \frac{n}{d}$, τότε $\sqrt[r]{p} = p^{1/r} = p^{d/n} = \sqrt[n]{p^d}$. Άρα, $\sqrt[n]{p^d} = c\sqrt[n]{p_1^{e(1)}}\sqrt[n]{p_2^{e(2)}}\cdots\sqrt[n]{p_m^{e(m)}} \Leftrightarrow c = \sqrt[n]{\frac{p^d}{p_1^{e(1)}p_2^{e(2)}\cdots p_m^{e(m)}}} \in \mathbb{Q}(\omega)$. Θέτουμε $q = \frac{p^d}{p_1^{e(1)}p_2^{e(2)}\cdots p_m^{e(m)}}$. Άρα το q είναι ένας θετικός ρητός αριθμός και το $X^n - q$ έχει ρίζα στο $\mathbb{Q}(\omega)$, αφού ρίζα του $X^n - q$ είναι το $\sqrt[r]{q} = c \in \mathbb{Q}(\omega)$ και ισχύει ότι $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$, $\omega \in \Omega_n$. Οπότε, σύμφωνα με το θεώρημα 1.2.3, προκύπτει ότι το $X^n - q$ έχει μία ρίζα στο $\mathbb{Q}$. Άτοπο, διότι οι ρίζες του $X^n - q$ είναι οι $\sqrt[n]{q}, \omega\sqrt[n]{q}, \ldots, \omega^{n-1}\sqrt[n]{q}$. Το $\omega \notin \mathbb{Q}$, διότι $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Άρα, οι ρίζες $\omega^k\sqrt[n]{q} \notin \mathbb{Q}$ με $1 \leq k \leq n-1$. Απομένει να εξετάσουμε αν η $\sqrt[n]{q} \in \mathbb{Q}$. Από το λήμμα 1.3.1 έχουμε ότι $\sqrt[n]{q} \in \mathbb{Q} \Leftrightarrow p^d = a^n$ και $p_1^{e(1)}p_2^{e(2)}\cdots p_m^{e(m)} = b^n$, με $a, b \in \mathbb{Z}$, $a, b > 0$. Δηλαδή, $q = (\frac{a}{b})^n$ με ΜΚΔ$(a, b) = 1$. Όμως το q δεν μπορεί να γραφτεί στην μορφή $(\frac{a}{b})^n$ με ΜΚΔ$(a, b) = 1$, διότι $d \mid n$ και $0 \leq e(i) \leq n-1$. Οπότε, σύμφωνα με το λήμμα 1.3.1, προκύπτει ότι $\sqrt[n]{q} \notin \mathbb{Q}$. Άρα, όλες οι ρίζες του $X^n - q$ δέν ανήκουν στο $\mathbb{Q}$. Συνεπώς, η περίπτωση αυτή απορρίπτεται.
Περίπτωση 2: Έστω ότι τουλάχιστον δύο όροι στον γραμμικό συνδυασμό είναι μη μηδενικοί.
Δηλαδή, ένας απο τους πρώτους p_i, έστω ο p_m, εμφανίζεται με διαφορετικές δυνάμεις σε τουλάχιστον δύο διαφορετικούς όρους. Ομαδοποιώντας τους όρους με βάση τις δυνάμεις του p_m, προκύπτει ότι

$$p^{1/r} = A_0 + A_1 p_m^{1/n} + A_2 p_m^{2/n} + \cdots + A_{n-1} p_m^{\frac{n-1}{n}} \tag{1.10}$$

όπου $A_i \in \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_{m-1}})$ και τουλάχιστον δύο απο τα A_i είναι μη μηδενικά. Ισχύει ότι $\mathbb{Q}(\omega) \leq \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$. Η επέκταση $\mathbb{Q}(\omega) \leq \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$ είναι επέκταση Galois, διότι το $\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$ είναι σώμα ανάλυσης του $f(X) = (X^n - p_1)(X^n - p_2)\cdots(X^n - p_m)$ υπέρ του $\mathbb{Q}(\omega)$ και το $f(X)$ είναι διαχωρίσιμο στο $\mathbb{Q}(\omega)$ διότι $\mathbb{Q} \leq \mathbb{Q}(\omega)$ και $ch(\mathbb{Q}) = 0$. Άρα, η επέκταση $\mathbb{Q}(\omega) \leq L$ είναι επέκταση Galois. Επομένως, απο την επαγωγική υπόθεση ισχύει ότι $|Gal(\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})/\mathbb{Q}(\omega))| = n^m$. Θέτουμε $G = Gal(\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})/\mathbb{Q}(\omega))$. Έστω $\sigma \in G$. Η σ στέλνει ρίζες αναγώγων σε ρίζες των ίδιων αναγώγων. Άρα, η σ πρέπει να στέλνει ρίζες του $X^n - p_i$ σε άλλες ρίζες του. Το $X^n - p_i$ είναι ανάγωγο υπέρ το $\mathbb{Q}$, σύμφωνα με το κριτήριο του Eisenstein για τον πρώτο $p = p_i$. Ακόμα, οι ρίζες του $X^n - p_i$ είναι οι $p_i^{1/n}, \omega p_i^{1/n}, \omega^2 p_i^{1/n}, \ldots, \omega^{n-1} p_i^{1/n}$. Άρα, η σ δρά ως εξής

$$\sigma : p_i \mapsto \omega^{j_i} p_i^{1/n}, \text{ με } j_i \in \{0, \ldots, n-1\}$$

Οπότε, έχουμε n^m δυνατότητες[15] για την σ. Επειδή, $|G| = n^m$, τότε πρέπει να συνβαίνουν όλες αυτές οι επιλογές για την σ. Άρα, υπάρχει $\sigma \in G$ ώστε $\sigma = Id$ στο $\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$. Δηλαδή, $\sigma(B) = B$ για κάθε $B \in \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$ και $\sigma(p_m^{1/n}) = \omega p_m^{1/n}$. Ακόμα, $\sigma(p^{1/r}) = \omega^k p^{1/r}$, με $0 \leq k \leq n-1$ [16]. Εφαρμόζοντας την σ στην σχέση (1.10) προκύπτει ότι

$$\begin{aligned} \sigma(p^{1/r}) = \sigma(A_0 + A_1 p_m^{1/n} + A_2 p_m^{2/n} + \cdots + A_{n-1} p_m^{\frac{n-1}{n}}) \Leftrightarrow \\ \omega^k p^{1/r} = A_0 + A_1 \sigma(p_m^{1/n}) + A_2 \sigma(p_m^{2/n}) + \cdots + A_{n-1} \sigma(p_m^{\frac{n-1}{n}}) \Leftrightarrow \\ \omega^k p^{1/r} = A_0 + A_1 \omega p_m^{1/n} + A_2 \omega^2 p_m^{2/n} + \cdots + A_{n-1} \omega^{n-1} p_m^{\frac{n-1}{n}} \end{aligned} \tag{1.11}$$

διότι $\sigma(A_i) = A_i$, για κάθε $A_i \in \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_{m-1}})$.
Πολλαπλασιάζοντας την σχέση (1.10) με το ω^k και πρικύπτει ότι:

$$\omega^k p^{1/r} = \omega^k A_0 + \omega^k A_1 p_m^{1/n} + \omega^k A_2 p_m^{2/n} + \cdots + \omega^k A_{n-1} p_m^{\frac{n-1}{n}} \tag{1.12}$$

Αφαιρώντας κατα μέλη τις σχέσεις (1.12) και (1.11) έχουμε ότι

$$0 = (\omega^k - 1)A_0 + (\omega^k - \omega)A_1 p_m^{1/n} + (\omega^k - \omega^2)A_2 p_m^{2/n} + \cdots + (\omega^k - \omega^{n-1})A_{n-1} p_m^{\frac{n-1}{n}} \tag{1.13}$$

όπου τουλάχιστον ένας συντελεστής $(\omega^k - \omega^i)A_i$ είναι διάφορος του μηδενός, διότι έχουμε ότι τουλάχιστον δύο απο τα A_i είναι μη μηδενικά, έστω χωρίς βλάβη της γενικότητας ότι $A_0 \neq 0, A_1 \neq 0$ και $A_i = 0$, για κάθε $i \geq 2$. Άρα, $0 = (\omega^k - 1)A_0 + (\omega^k - \omega)A_1 p_m^{1/n} \Leftrightarrow (\omega^k - 1)A_0 = 0$ και $(\omega^k - \omega)A_1 = 0 \Leftrightarrow \omega^k = 1$ και $\omega^k = \omega \Leftrightarrow k = 0$ και $k = 1$. Άτοπο. Άρα, τουλάχιστον ένας συντελεστής $(\omega^k - \omega^i)A_i \neq 0$. Δηλαδή, στην σχέση (1.13) τουλάχιστον ένας απο τους συντελεστές $(\omega^k - \omega^i)A_i$ είναι μη μηδενικοί. Οπότε, το πολυώνυμο που προκύπτει απο την σχέση (1.13) είναι μη μηδενικό και το $p_m^{1/n}$ είναι ρίζα του. Όμως, ο βαθμός του είναι μικρότερος ή ίσος απο $n-1$. Άρα, $[L : F] < n^m$. Άτοπο, αφού από επαγωγική υπόθεση έχουμε ότι $[L : F] = n^m$.

Επομένως, το πολυώνυμο $X^n - p$ είναι ανάγωγο υπέρ το L. Το $p^{1/n} = \sqrt[n]{p}$ είναι ρίζα του $X^n - p$. Άρα, $[L(\sqrt[n]{p}) : L] = n$. Ακόμα, απο επαγωγική υπόθεση έχουμε ότι $[L : F] = n^m$. Οπότε,

$$[L(\sqrt[n]{p}) : F] = [L(\sqrt[n]{p}) : L][L : F] = nn^m = n^{m+1}$$

Δηλαδή, $[\mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}, \sqrt[n]{p}) : \mathbb{Q}(\omega)] = n^{m+1}$. Οπότε, δείξαμε το ζητούμενο. □

[15] n επιλογές για το j_i και m επιλογές για το i

[16] Το οποίο προκυπτει διότι, το $p^{1/r}$ είναι ρίζα του $X^r - p$, άρα υπό την δράση της σ το $p^{1/r}$ αντιστοιχίζεται σε κάποια άλλη ριζα του.

Σημείωση 1.3.1. *Το θεώρημα 1.3.1 ισχύει για κάθε ακέραιο n (βλ. [11]). Εδώ θα το αποδείξουμε για $n = 2$*

Απόδειξη. Έστω ότι το $n = 2$. Θα δείξουμε ότι $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$ με $p_1, \ldots, p_k$ διακριτοί πρώτοι.Θα το αποδείξουμε επαγωγικά.
Αρχικά θα δείξουμε ότι ισχύει για $k = 0$. Τότε $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) = \mathbb{Q}$. Άρα, $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1 = 2^0$.
Υποθέτουμε ότι ισχύει για k, δηλαδή $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$ και θα δείξουμε ότι ισχύει για $k + 1$.
Έστω p_{k+1} πρώτος διαφορετικός απο τους $p_1, \ldots, p_k$. Θέτουμε $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$. Έστω ότι το πολυώνυμο $X^2 - p_{k+1}$ δεν είναι ανάγωγο υπέρ το F. Τότε απο το θεώρημα 1.3.1 προκύπτει ότι $p_{k+1} \in F^2$, δηλαδή $p_{k+1}^{1/2} \in F$. Έστω $\{e_i\}$ να είναι το σύνολο των 2^k ριζικών της μορφής $\sqrt{p_1^{m(1)} \cdots p_k^{m(k)}}$, $0 \leq m(i) < 2$ και $1 \leq i \leq k$. Άρα, $p_{k+1}^{1/2} = \sum c_i e_i$, $c_i \in \mathbb{Q}$. Υπάρχουν δύο περιπτώσεις:
Περίπτωση 1: Έστω ότι υπάρχει ένας συντελεστής $c_i \neq 0$. Δηλαδή, $p_{k+1}^{1/2} = c_i e_i \Leftrightarrow \sqrt{p_{k+1}} = c_i \sqrt{p_1^{m(1)} \cdots p_k^{m(k)}} \Leftrightarrow c_i = \sqrt{\frac{p_{k+1}}{p_1^{m(1)} \cdots p_k^{m(k)}}}$, $0 \leq m(i) < 2$, $1 \leq i \leq k$. Θέτουμε $q = \frac{p_{k+1}}{p_1^{m(1)} \cdots p_k^{m(k)}}$. Το q είναι θετικός ρητός αριθμός. Δηλαδή, $c_i = \sqrt{q}$. Αλλά $c_i \in \mathbb{Q}$ και $\sqrt{q} \notin \mathbb{Q}$, διότι σύνφωνα με το λήμμα 1.3.1 έχουμε ότι το q δεν μπορεί να γραφτεί στην μορφή $(\frac{a}{b})^2$ με ΜΚΔ$(a, b) = 1$, διότι $0 \leq m(i) < 2$. Άτοπο, άρα απορρίπτεται αυτή η περίπτωση.
Περίπτωση 2: Έστω ότι υπάρχουν τουλάχιστον δύο όροι $c_i, c_j \neq 0$. Άρα, υπάρχει τουλάχιστον ένας απο τους p_i, έστω ο p_k, που εμφανίζεται με διαφορετικές δυνάμεις σε τουλάχιστον δύο διαφορετικούς όρους του αθροίσματος. Ομαδοποιώντας τους όρους με βάση τις δυνάμεις του p_k προκύπτει ότι

$$p_{k+1}^{1/2} = A + B p_k^{1/2} \text{ όπου } A, B \in \mathbb{Q}(p_1^{1/2}, \ldots, p_{k-1}^{1/2}),\ A, B \neq 0 \tag{1.14}$$

Υψώνουμε στο τετράγωγο την σχέση (1.14) και προκύπτει ότι

$$\begin{aligned} p_{k+1} &= (A + B p_k^{1/2})^2 \Leftrightarrow \\ p_{k+1} &= A^2 + 2AB p_k^{1/2} + B^2 p_k \Leftrightarrow \\ 2AB p_k^{1/2} &= p_{k+1} - (A^2 + B^2 p_k) \Leftrightarrow \\ p_k^{1/2} &= \frac{1}{2AB}(p_{k+1} - A^2 - B^2 p_k) \in \mathbb{Q}(p_1^{1/2}, \ldots, p_{k-1}^{1/2}) \end{aligned}$$

αφού $A, B \in \mathbb{Q}(p_1^{1/2}, \ldots, p_{k-1}^{1/2})$ και $p_k, p_{k+1} \in \mathbb{Q}$.
Άρα, $p_k^{1/2} \in \mathbb{Q}(p_1^{1/2}, \ldots, p_{k-1}^{1/2})$. Οπότε, $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] < 2^k$. Άτοπο,

αφού απο επαγωγική υπόθεση έχουμε ότι $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$.

Επομένως, το πολυώνυμο $X^2 - p_{k+1}$ είναι ανάγωγο υπέρ το F. Το $p_{k+1}^{1/2}$ είναι ρίζα του $X^2 - p_{k+1}$. Άρα, $[F(p_{k+1}^{1/2}) : F] = 2$. Οπότε,

$$[F(p_{k+1}^{1/2}) : \mathbb{Q}] = [F(p_{k+1}^{1/2}) : F][F : \mathbb{Q}] = 2 \cdot 2^k = 2^{k+1}$$

Δηλαδή, $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}, \sqrt{p_{k+1}}) : \mathbb{Q}] = 2^{k+1}$.

□

Κεφάλαιο 2

Το Θεώρημα Hilbert 90 και Συνομολογία

Ορισμός 2.0.1. *Έστω G πεπερασμένη ομάδα. Το σύνολο M θα λέγεται G-module αν και μόνο αν η $(M,+)$ είναι αβελιανή ομάδα και υπάρχει δράση της G στο M $\sigma : G \times M \to M$ ώστε*

$$\begin{aligned} \sigma(m+m') &= \sigma m + \sigma m' \\ (\sigma\tau)\cdot m &= \sigma\cdot(\tau(m)) \\ 1\cdot m &= m \end{aligned}$$

για κάθε $m, m' \in M$

Παρατήρηση 2.0.1. *Άν η επέκταση $K \leq L$ είναι επέκταση Galois με $G = Gal(L/K)$. Τότε οι $(L,+)$ και $(L^*,\cdot)$ είναι G-modules.*

Απόδειξη. • Η $(L,+)$ είναι G-module, διότι η $(L,+)$ είναι αβελιανή ομάδα και για κάθε $\sigma \in G$ ισχύει ότι

$$\begin{aligned} \sigma(m+m') &= \sigma m + \sigma m' \\ (\sigma\tau)\cdot m &= \sigma\cdot(\tau(m)) \\ 1\cdot m &= m \end{aligned}$$

για κάθε $m, m' \in M$

• Η $(L^*,\cdot)$ είναι G-module, διότι η $(L^*,\cdot)$ είναι αβελιανή ομάδα, $L^* = L\setminus\{0\}$ και ισχύει ότι $\sigma(a\cdot b) = \sigma a\cdot\sigma b$, $(\sigma\tau)(a) = \sigma(\tau(a))$ και $1\cdot a = a$. □

Ορισμός 2.0.2. *Έστω M ένα G-module. Σταυρωτός ομομορφισμός (crossed product) είναι μια απεικόνιση* $f : G \to M$ *ώστε* $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$, *για κάθε* $\sigma, \tau \in G$.

Προφανώς $f(1) = f(1) + 1 \cdot f(1) \Rightarrow f(1) = 0$.

Παρατήρηση 2.0.2. *Άν* $f : G \to M$ *σταυρωτός ομομορφισμός, τότε για κάθε* $\sigma \in G$ *ισχύει ότι*
$f(\sigma^2) = f(\sigma) + \sigma f(\sigma)$
$f(\sigma^3) = f(\sigma \cdot \sigma^2) = f(\sigma) + \sigma f(\sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma)$
$\vdots$
$f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma)$.

Επομένως άν G είναι κυκλική, δηλαδή $G =< \sigma >$, *τότε ο σταυρωτός ομομορφισμός* $f : G \to M$ *καθορίζεται πλήρως απο την τιμή στο* σ. *Δηλαδή, άν* $f(\sigma) = x$, *τότε το* x *επαληθεύει την εξίσωση*

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0 \tag{2.1}$$

Αντίστροφα, άν $x \in M$ *και επαληθεύει την εξίσωση 2.1, τότε η απεικόνιση* $f : G \to M$ *με* $G =< \sigma >$ *ώστε* $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$ *ορίζει έναν σταυρωτό ομομορφισμό. Διότι,* $f(\sigma^{i-1}) = x + \sigma x + \cdots + \sigma^{i-2} x$, *άρα* $f(\sigma^i) = f(\sigma^{i-1}) + \sigma^{i-1} x = f(\sigma^{i-1}) + \sigma^{i-1} f(\sigma)$, *το οποίο είναι σταυρωτός ομομορφισμός.*
Επομένως, για $G =< \sigma >$ *υπάρχει ένα-πρός-ένα καί επί απεικόνιση ανάμεσα στους σταυρωτούς ομομορφισμούς* $f : G \to M$ *και στα* $x \in M$ *τα οποία επαληθεύουν την εξίσωση (2.1).*

Παρατήρηση 2.0.3. *Για κάθε* $x \in M$ *η* $f(\sigma) = \sigma x - x$, *για κάθε* $\sigma \in G$ *ορίζει σταυρωτό ομομορφισμό.*

Απόδειξη. $f(\sigma\tau) = (\sigma\tau)x - x$ και $f(\sigma) + \sigma f(\tau) = \sigma x - x + \sigma(\tau x - x) = \sigma x - x + (\sigma\tau)x - \sigma x = (\sigma\tau)x - x = f(\sigma\tau)$. Άρα, είναι σταυρωτός ομομορφισμός. □

Ορισμός 2.0.3. *Οι σταυρωτοί ομομορφισμοί* $f : G \to M$ *ώστε* $f(\sigma) = \sigma x - x$, *για κάθε* $\sigma \in G$, *για κάθε* $x \in M$, *λέγονται κύριοι σταυρωτοί ομομορφισμοί*[1].

[1] Πολλαπλασιαστικά: $f(\tau) = \frac{\tau(a)}{a}$, για κάθε $\tau \in G$

Παρατήρηση 2.0.4. *i) Άν η G δρά τετριμμένα στο M, δηλαδή* $\sigma m = m$, *για κάθε* $\sigma \in G$ *και για κάθε* $m \in M$. *Τότε ο* $f : G \to M$ *είναι ομομορφισμός.*
ii) Άθροισμα και διαφορά απο σταυρωτούς ομομορφισμούς είναι σταυρωτός ομομορφισμός. Η ομάδα των σταυρωτών ομομορφισμών είναι αβελιανή.
iii) Άθροισμα και διαφορά κυρίων σταυρωτών ομομορφισμών είναι κύριος σταυρωτός ομομορφισμός. Η ομάδα των κυρίων σταυρωτών ομομορφισμών είναι αβελιανή.

Ορισμός 2.0.4. *Έστω G ομάδα και K σώμα. Ένας χαρακτήρας της G στο* K *είναι ένας ομομορφισμός ομάδων* $\chi : G \to K^*$.

Λήμμα 2.0.2. *(Λήμμα του Dedekind) Έστω* $\tau_1, \ldots, \tau_n$ *διακριτοί χαρακτήρες της G στο* K^*. *Τότε τα* $\tau_i, i = 1, \ldots, n$ *είναι γραμμικά ανεξάρτητα υπέρ το K, δηλαδή αν* $\sum_{i=1}^{n} c_i\tau_i(g) = 0$, *για κάθε* $g \in G, c_i \in K$, *τότε* $c_i = 0$, *για κάθε i.*

Απόδειξη. Έστω ότι δεν ισχύει. Δηλαδή, τα τ_i είναι γραμμικά εξαρτημένα. Έστω k να είναι ο ελάχιστος φυσικός αριθμός για τον οποίο ισχύει ότι k το πλήθος απο τα t_i είναι γραμμικά εξαρτημένα. Δηλαδή,

$$\sum_{i=1}^{k} c_i\tau_i(g) = 0, \text{ για κάθε } g \in G \text{ και όχι όλα τα } c_i = 0 \tag{2.2}$$

Έχουμε υποθέσει ότι το λήμμα δεν ισχύει, δηλαδή υπάρχουν $c_i \in K$ ώστε $\sum_{i=1}^{k} c_i\tau_i(g) = 0$ για κάθε $g \in G$, τότε $c_i \neq 0$, για κάθε i. Επειδή, $\tau_i \neq \tau_2$, τότε υπάρχει $h \in G$ με $\tau_1(h) \neq \tau_2(h)$. Ισχύει ότι,

$$\sum_{i=1}^{k} (c_i\tau_1(h))\tau_i(g) = 0 \tag{2.3}$$

Έχουμε ότι $gh \in G$, αφού G ομάδα καί $h, g \in G$. Άρα απο την σχέση (2.2) προκύπτει ότι

$$\sum_{i=1}^{k} c_i\tau_i(gh) = 0 \Rightarrow \sum_{i=1}^{k} (c_i\tau_i(h))\tau_i(g) = 0, \text{ αφού } \tau_i \text{ χαρακτήρας} \tag{2.4}$$

Αφαιρώντας κατα μέλη τις σχέσεις (2.3) και (2.4) προκύπτει ότι για κάθε $g \in G$ ισχύει ότι $\sum_{i=1}^{k} (c_i(\tau_1(h) - \tau_i(h)))\tau_i(g) = 0$

$\Rightarrow c_2(\tau_1(h)-\tau_2(h)))\tau_2(g)+\cdots+c_k(\tau_1(h)-\tau_k(h)))\tau_k(g)=0$ και $c_i(\tau_1(h)-\tau_i(h))\neq 0$ για κάθε $i=2,\ldots,k$. Δηλαδή είναι μία έκφραση που περιέχει $(k-1)$ το πλήθος απο τα τ_i και οι συντελεστές δεν είναι όλοι ίσοι με μηδέν. Άτοπο, διότι εξ' ορισμού k είναι ο ελάχιστος φυσικός αριθμός για τον οποίο ισχύει η παραπάνω ιδιότητα. Συνεπώς, το λήμμα ισχύει □

Ορισμός 2.0.5. *Η πρώτη ομάδα συνομολογίας του G-module M συμβολίζεται ως $H^1(G,M)$ και ορίζεται ως η ομάδα πηλίκο του συνόλου των σταυρωτών ομομορφισμών ως προς το σύνολο των κύριων σταυρωτων ομομορφισμών.*

Θεώρημα 2.0.2. *Άν η επέκταση $K\leq L$ είναι επέκταση Galois και $G=Gal(L/K)$ η οποία είναι κυκλική, τότε ισχύει ότι $H^1(G,L^*)=0$ (Δηλαδή κάθε σταυρωτός ομομορφισμός είναι κύριος σταυρωτός ομομορφισμός).*

Απόδειξη. Έστω $f:G\to L^*$ είναι σταυρωτός ομομορφισμός. Απο τον ορισμό ισχύει ότι $f(\sigma\tau)=f(\sigma)\cdot\sigma(f(\tau))$, για κάθε $\sigma,\tau\in G$. Θα πρέπει να αποδείξουμε ότι $f(\sigma)=\frac{\sigma(\gamma)}{\gamma}$, για κάποιο $\gamma\in L^*$ και για κάθε $\sigma\in G$. Έχουμε ότι $f(\tau)\neq 0$, διότι $f:G\to L^*$, όπου $L^*=L\setminus\{0\}$. Επειδή $f(\tau)\neq 0$, τότε απο το Λήμμα Dedekind (λήμμα 2.0.2), η απεικόνιση $\sum_{\tau\in G}f(\tau)\tau:L\to L$ είναι διάφορη της μηδενικής. Οπότε, υπάρχει $\alpha\in L$ ώστε $\beta:=\sum_{\tau\in G}f(\tau)\tau(\alpha)\neq 0$. Αλλά τότε για κάθε $\sigma\in G$ ισχύει ότι $\sigma(\beta)=\sum_{\tau\in G}\sigma(f(\tau))(\sigma\tau)(\alpha)$. Ισχύει $f(\sigma\tau)=f(\sigma)\cdot\sigma f(\tau)\Rightarrow\sigma(f(\tau))=f(\sigma)^{-1}f(\sigma\tau)$. Άρα, $\sigma(\beta)=\sum_{\tau\in G}\sigma(f(\tau))(\sigma\tau)(\alpha)=\sum_{\tau\in G}f(\sigma)^{-1}f(\sigma\tau)(\sigma\tau)(\alpha)=f(\sigma)^{-1}\sum_{\tau\in G}f(\sigma\tau)(\sigma\tau)(\alpha)$. Αλλά, όταν το τ διατρέχει την G, τότε το $\sigma\tau$ διατρέχει κι αυτό το G. Άρα, $\sigma(\beta)=f(\sigma)^{-1}\beta$, δηλαδή $f(\sigma)=\frac{\beta}{\sigma(\beta)}$. Θέτουμε $\gamma=\beta^{-1}$, τότε $f(\sigma)=\frac{\sigma(\gamma)}{\gamma}$, $\gamma\in L^*$. Άρα, κάθε σταυρωτό γινόμενο είναι κύριο σταυρωτό γινόμενο. □

Ορισμός 2.0.6. *Έστω η επέκταση Galois $K\leq L$ με $G=Gal(L/K)$ και $\alpha\in L^*$. Ορίζουμε $N_{L/K}:L^*\to K^*$ ώστε $\alpha\mapsto N_{L/K}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)$ και $KerN_{L/K}=\{\alpha\in L^*|N_{L/K}(\alpha)=1\}$.*

Σχόλιο 2.0.1. *Άν $G=\{\sigma_1,\ldots,\sigma_n$, $N_{L/K}(\alpha)=\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$. Έστω, $\tau\in G$ τυχαίο. Τότε $\tau(N_{L/K}(\alpha))=\tau\sigma_1(\alpha)\tau\sigma_2(\alpha)\cdots\tau\sigma_n\alpha=N_{L/K}(\alpha)$, διότι*

γνωρίζουμε ότι άν πολλαπλασιάσω τα στοιχεία της με ένα οποιοδήποτε στοιχείο της τότε θα πάρουμε όλα τα στοιχεία της ομάδας, δηλαδή $\{\sigma_1, \ldots, \sigma_n\} = \{\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_n\}$.

Πόρισμα 2.0.1. *(Θεώρημα 90 του Hilbert) Έστω η κυκλική επέκταση* $K \leq L$ *με ομάδα Galois* $G = Gal(L/K) =< \sigma >$. *Τότε, άν* $\alpha \in L$ *ισχύει ότι* $N_{L/K}(\alpha) = 1$ *αν και μόνο αν* $\alpha = \frac{\sigma(\beta)}{\beta}$, *για κάποιο* $\beta \in L$.

Απόδειξη. Έστω $[L : K] = |G| = n$. $''\Leftrightarrow''$ Έστω ότι $\alpha = \frac{\sigma(\beta)}{\beta}$, για κάποιο $\beta \in L$. Τότε $N_{L/K}(\alpha) = N_{L/K}(\frac{\sigma(\beta)}{\beta}) = \frac{N_{L/K}(\sigma(\beta))}{N_{L/K}(\beta)}$. Επίσης, $N_{L/K}(\sigma(\beta)) = \prod_{\tau\in G} \tau(\sigma(\beta)) = \prod_{\tau\in G} (\tau\sigma)(\beta) = \prod_{\tau\in G} \tau(\beta) = N_{L/K}(\beta)$. Άρα, $N_{L/K}(\alpha) = \frac{N_{L/K}(\sigma(\beta))}{N_{L/K}(\beta)} = \frac{N_{L/K}(\beta)}{N_{L/K}(\beta)} = 1$.
$''\Rightarrow''$ Έστω ότι $N_{L/K}(\alpha) = 1$. Θα δείξουμε ότι $\alpha = \frac{\sigma(\beta)}{\beta}$, για κάποιο $\beta \in L$. Ορίζουμε $f : G \to L^*$ ώστε $f(id) = 1$, $f(\sigma) = \alpha$ και $f(\sigma^i) = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)$, με $i < n$.
Θα δείξουμε ότι ο f είναι σταυρωτό γινόμενο. Έστω $0 \leq i, j < n$.
Άν $i + j < n$ τότε

$$\begin{aligned} f(\sigma^i\sigma^j) &= f(\sigma^{i+j}) \\ &= \alpha\sigma(\alpha)\cdots\sigma^{i+j-1}(\alpha) \\ &= (\alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha))(\sigma^i(\alpha)\sigma^{i+1}(\alpha)\cdots\sigma^{i+j-1}(\alpha)) \\ &= (\alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha))\cdot\sigma^i(\alpha\sigma(\alpha)\cdots\sigma^{j-1}(\alpha)) \\ &= f(\sigma^i)\cdot\sigma^i(f(\sigma^j)) \end{aligned}$$

Άν $i + j \geq n$, τότε $0 \leq i + j - n < n$

$$\begin{aligned} f(\sigma^i\sigma^j) &= f(\sigma^{i+j}) = f(\sigma^{i+j-n+n}) = f(\sigma^{i+j-n})f(\sigma^n) \\ &= f(\sigma^{i+j-n})f(id) = f(\sigma^{i+j-n})\cdot 1 = f(\sigma^{i+j-n}) \\ &= \alpha\sigma(\alpha)\cdots\sigma^{i+j-n-1}(\alpha) \end{aligned}$$

$$\begin{aligned} f(\sigma^i)\cdot\sigma^i(f(\sigma^j)) &= (\alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha))\cdot\sigma^i(\alpha\sigma(\alpha)\cdots\sigma^{j-1}(\alpha)) \\ &= (\alpha\sigma(\alpha)\cdots\sigma^{i+j-n-1}(\alpha))\cdot\sigma^{i+j-n}(\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)) \\ &= f(\sigma^i\sigma^j)N_{L/K}(\alpha) \\ &= f(\sigma^i\sigma^j)\cdot 1 = f(\sigma^i\sigma^j) \end{aligned}$$

Οπότε, η f είναι σταυρωτό γινόμενο και σύμφωνα με το θεώρημα 2.0.2 έχουμε ότι f είναι κύριο σταυρωτό γινόμενο. Δηλαδή, υπάρχει $\beta \in L$ ώστε $f(\sigma^i) = \frac{\sigma^i(\beta)}{\beta}$ για κάθε i. Οπότε, υπάρχει $\beta \in L$ ώστε $f(\sigma) = \frac{\sigma(\beta)}{\beta}$. Όμως, $f(\sigma) = \alpha$. Άρα, $\alpha = \frac{\sigma(\beta)}{\beta}$, με $\beta \in L$.

□

Κεφάλαιο 3

Επεκτάσεις του Kummer

Στόχος μας είναι να χαρακτηρίσουμε επεκτάσεις Galois με αβελιανή ομάδα Galois, όταν το σώμα βάσης της επέκτασης, έστω F, περιέχει ικανό αριθμό n-ριζών της μονάδας.

Ορισμός 3.0.7. *Έστω F σώμα που περιέχει μια πρωταρχική n-ρίζα της μονάδας και $F \leq K$ είναι επέκταση Galois. Η επέκταση $F \leq K$ θα λεγεται n-επέκταση του Kummer υπεράνω του F, όταν η ομάδα Galois $G = Gal(K/_F)$ είναι αβελιανή και $exp(G) \mid n$* [1].
Άν η επέκταση $F \leq K$ είναι n-επέκταση του Kummer για κάποιο n, τότε η επέκταση $F \leq K$ είναι επέκταση του Kummer

Παράδειγμα 3.0.1. *Έστω F σώμα που περιέχει μια πρωταρχική n-ρίζα της μονάδας και η επέκταση $F \leq K$ είναι κυκλική επέκταση βαθμού n.*

Η επέκταση $F \leq K$ είναι κυκλική, άρα η επέκταση $F \leq K$ είναι αβελιανή. Οπότε, η ομάδα Galois $Gal(K/_F)$ είναι αβελιανή. Ακόμα, η ομάδα Galois $G = Gal(K/_F)$ είναι κυκλική βαθμού n. Και ισχύει ότι $exp(G) \mid n$. Άρα, επέκταση $F \leq K$ είναι μία n-επέκταση του Kummer. Άν, επίσης, το F περιέχει μια πρωταρχική m-ρίζα της μονάδας, για m πολλαπλάσιο του n, τότε επέκταση $F \leq K$ είναι επίσης μια m-επέκταση του Kummer.
Συνεπώς, άν μια επέκταση είναι n-επέκταση του Kummer, τότε το n δεν είναι μοναδικό.

Παράδειγμα 3.0.2. *Το $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ είναι σώμα ανάλυσης του πολυωνύμου $(X^2 - 2)(X^2 - 3)$ υπέρ του $\mathbb{Q}$.*

[1] Εκθέτης της G,Exp(G) είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων όλων των στοιχείων της G, δηλαδή άν $exp(G) = n$ τότε $a^n = 1, \forall a \in G$.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ |^2 \\ \mathbb{Q}(\sqrt{2}) \\ |^2 \\ \mathbb{Q} \end{array}$$

Άρα, $[K:\mathbb{Q}] = 2\cdot 2 = 4$. *Ακόμα,* $ch\mathbb{Q} = 0$, *άρα το πολυώνυμο* $(X^2-2)(X^2-3)$ *είναι διαχωρίσιμο πολυώνυμο. Οπότε, η επέκταση* $\mathbb{Q} \leq K$ *είναι επέκταση Galois, αφού το K είναι σώμα ανάλυσης διαχωρίσιμου πολυωνύμου. Δηλαδή,* $[K:\mathbb{Q}] = 4 = |Gal(K/_{\mathbb{Q}})|$ *και* $G = Gal(K/_{\mathbb{Q}}) = \{Id_K, \sigma, \tau, \sigma\tau\}$ *όπου*

$$Id_K : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \text{ και } \quad \sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$$

$$\tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \text{ και } \quad \sigma\tau : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Ισχύει ότι $ord(\sigma) = ord(\tau) = ord(\sigma\tau) = 2$. *Άρα,* $G \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. *Άρα, η ομάδα G είναι αβελιανή και* $Exp(G) = 2 \mid 4$. *Ακόμα,* $-1 \in \mathbb{Q}$ *και το* -1 *είναι πρωταρχική 2-ρίζα της μονάδας. Οπότε, η επέκταση* $\mathbb{Q} \leq K$ *είναι 2-επέκταση Kummer. Συνεπώς, η επέκταση* $\mathbb{Q} \leq K$ *είναι επέκταση Kummer.*

Λήμμα 3.0.3. *Έστω F σώμα που περιέχει μία πρωταρχική n-ρίζα της μονάδας, έστω* $\omega \in F$, *και η επέκταση* $F \leq K$ *είναι μία κυκλική επέκταση βαθμού n. Έστω, επίσης* $Gal(K/_F) =< \sigma >$. *Τότε υπάρχει* $a \in K$ *με* $\omega = \frac{\sigma(a)}{a}$.

Απόδειξη. Ο $\sigma \in Gal(K/_F)$ είναι F-γραμμικός μετασχηματισμός του K. Θέλουμε να δείξουμε ότι υπάρχει $a \in K$ ώστε $\sigma(a) = \omega a$. Δηλαδή θέλουμε να δείξουμε ότι το ω είναι ιδιοτιμή του σ. Άρα, αρκεί να δείξουμε ότι το ω είναι ρίζα του χαρακτηριστικού πολυωνύμου του σ.
Έχουμε ότι $Gal(K/_F) =< \sigma >$ και $[K:F] = |Gal(K/_F)| = n$, άρα $\sigma^n = id \Rightarrow \sigma^n - id = 0$. Δηλαδή το σ είναι ρίζα του πολυωνύμου $X^n - 1$. Ακόμα, αν υπάρχει $g(X) \in F[X]$ με $degg(X) = m < n$ ώστε $g(\sigma) = 0$, τότε ισχύει ότι οι αυτομορφισμοί $id, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ είναι γραμμικώς εξαρτημένοι υπέρ το F. Το οποίο είναι άτοπο, σύμφωνα με το Λήμμα του Detekind (λήμμα 2.0.2). Άρα, το $X^n - 1$ είναι το ελάχιστο πολυώνυμο της σ υπέρ το F. Επίσης, το χαρακτηριστικό πολυώνυμο της σ έχει βαθμό $n = [K:F]$ και ισχύει ότι το χαρακτηριστικό πολυώνυμο διαιρείται απο το ελάχιστο πολυώνυμο. Άρα, το $X^n - 1$ είναι το χαρακτηριστικό πολυώνυμο της σ υπέρ του F. Ακόμα, το ω είναι ρίζα του $X^n - 1$. Δηλαδή, το ω είναι ιδιοτιμή της σ. Οπότε, υπάρχει $a \in K$ ώστε $\sigma(a) = \omega a$. □

Θεώρημα 3.0.3. *Έστω F σώμα που περιέχει μια πρωταρχική n-ρίζα της μονάδας και η επέκταση $F \leq K$ μια κυκλική επέκταση Galois βαθμού n. Τότε υπάρχει $a \in K$ με $K = F(a)$ και $a^n = b \in F$, δηλαδή $K = F(\sqrt[n]{b})$.*

Απόδειξη. Έστω $Gal(K/_F) =< \sigma >$. Απο το λήμμα 3.0.3 έχουμε ότι υπάρχει $a \in K$ ώστε $\sigma(a) = \omega a$. Ακόμα, $\sigma^i(a) = \omega^i a$, αφού $\sigma \in Gal(K/_F)$. Άρα, το a παραμένει σταθερό απο την δράση της σ^i, όταν $n \mid i$. Αλλά, η τάξη του σ είναι n, δηλαδή $\sigma^n = id$. Οπότε, το a παραμένει σταθερό μόνο απο την δράση της id, δηλαδή $id(a) = a$. Άρα, $Gal(K/_{F(\alpha)}) =< id >$. Δηλαδή, $[K : F(a)] = 1$. Άρα, $K = F(\alpha)$. Ακόμα, ισχύει ότι $\sigma(a^n) = (\omega a)^n = \omega^n a^n = a^n$. Δηλαδή, το a^n παραμένει σταθερό απο την δράση της σ. Άρα, $a^n = b \in F$ [2]. Επομένως, $K = F(a) = F(\sqrt[n]{b})$. □

Θεώρημα 3.0.4. *Έστω F σώμα, ω πρωταρχική n-ρίζα της μονάδας ώστε $\omega \in F$ και η επέκταση $F \leq K$ είναι πεπερασμένη. Τότε ισχύει ότι η επέκταση $F \leq K$ είναι n-επέκταση Kummer αν και μόνο αν $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$, για κάποια $a_i \in F$.*

Απόδειξη. $''\Leftarrow''$ Έστω ότι $K = F(\alpha_1, \ldots, \alpha_r)$, όπου $\alpha_i^n = a_i \in F$. Για κάθε $i \in \{1, 2, \ldots, r\}$ οι ρίζες του $X^n - a_i$ υπέρ το K είναι οι εξής $\alpha_i, \omega\alpha_i, \ldots, \omega^{n-1}\alpha_i$. Επειδή $\omega \in F$ και $\alpha_i \in K$, τότε $\alpha_i, \omega\alpha_i, \ldots, \omega^{n-1}\alpha_i \in K$. Οι ρίζες $\alpha_i, \omega\alpha_i, \ldots, \omega^{n-1}\alpha_i$ είναι διακεκριμένες. Άρα $X^n - a_i \in F[X]$ είναι διαχωρίσιμο υπέρ το F (αφού σε κάποιο σώμα ανάλυσης του, έστω K, έχει απλές ρίζες) και αναλύεται πλήρως υπέρ το K. Οπότε, το K είναι σώμα ανάλυσης του συνόλου των διαχωρισίμων πολυωνύμων υπέρ το F $\{X^n - a_i | 1 \leq i \leq r\}$. Άρα, η επέκταση $F \leq K$ είναι επέκταση Galois. Άν $\sigma \in Gal(K/_F)$ τότε $\sigma(\alpha_i) = \omega^j \alpha_i$, για κάποιο $j \in \{0, \ldots, n-1\}$, διότι το $\sigma(\alpha_i)$ είναι επίσης ρίζα του πολυωνύμου $X^n - a_i$. Δηλαδή, $\sigma^k(\alpha_i) = \omega^{kj}\alpha_i$, για κάποιο k. Συνεπώς, $\sigma^n(\alpha_i) = \omega^{nj}\alpha_i = \omega^{n^j}\alpha_i = 1\dot{\alpha}_i = \alpha_i$, για κάθε $i = 1, \ldots, r$. Δηλαδή, $\sigma^n(\alpha_i) = \alpha_i$, για κάθε $i = 1, \ldots, r$. Αφού, τα α_i, $i = 1, \ldots, r$ παράγουν το K υπέρ το F και $\sigma^n(\alpha_i) = \alpha_i$ για κάθε $i = 1, \ldots, r$ τότε προκύπτει ότι $\sigma^n = Id_K$. Δηλαδή, $\sigma^n = Id_K$, για κάθε $\sigma \in Gal(K/_F) = G$. Οπότε, $Exp(G) \mid n$.
Απομένει να δείξουμε ότι η $G = Gal(K/_F)$ είναι αβελιανή. Έστω, $\sigma, \tau \in Gal(K/_F)$. Άρα, $\sigma(\alpha_i) = \omega^j \alpha_i$ και $\tau(\alpha_i) = \omega^k \alpha_i$, για κάποιο i. Έτσι, $\sigma\tau(\alpha_i) = \sigma(\tau(\alpha_i)) = \sigma(\omega^k \alpha_i) = \omega^k \sigma(\alpha_i) = \omega^k \omega^j \alpha_i = \omega^{k+j}\alpha_i$ και $\tau\sigma(\alpha_i) = \tau(\sigma(\alpha_i)) = \tau(\omega^j \alpha_i) = \omega^j \omega^k \alpha_i = \omega^{j+k}\alpha_i$. Άρα, τα $\sigma\tau$ και $\tau\sigma$ συμπίπτουν στους γεννήτορες της επέκτασης $F \leq K$. Δηλαδή, $\sigma\tau = \tau\sigma$. Επομένως, η ομάδα Galois $Gal(K/_F)$ είναι αβελιανή.

[2] $\sigma(f) = f$, $\forall f \in F$

Άρα, υπάρχει πρωταρχική n-ρίζα της μονάδας στο F, η ομάδα Galois $Gal(K/_F)$ είναι αβελιανή και $Exp(G) \mid n$. Οπότε, η επέκταση $F \leq K$ είναι n-επέκταση του Kummer. Επομένως, η επέκταση $F \leq K$ είναι επέκταση του Kummer.
$''\Rightarrow''$ Έστω ότι η επέκταση $F \leq K$ είναι μια n-επέκταση του Kummer. Θα δείξουμε ότι $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$, για κάποια $a_i \in F$. Αφού, η επέκταση $F \leq K$ είναι μια n-επέκταση του Kummer, τότε η επέκταση $F \leq K$ είναι επέκταση Galois και η $G = Gal(K/_F)$ είναι μια πεπερασμένη αβελιανή ομάδα. Έτσι, σύμφωνα με το Θεμελιώδες Θεώρημα των Πεπερασμένων Αβελιανών Ομάδων (Παρατήρηση 3[Παράρτημα]) ισχύει ότι $G \cong C_1 \times C_2 \times \cdots \times C_r$, όπου C_i είναι κυκλική για κάθε $i = 1, \ldots, r$ και $|C_i| \mid n$. Έστω $H_i = C_1 \times \cdots \times C_{i-1} \times C_{i+1} \times \cdots \times C_r$ υποομάδα της G ώστε $G/_{H_i} \cong C_i$, για κάθε $i \in \{1, 2, \ldots, r\}$. Έστω $L_i = \Phi(H_i)$ να είναι το σώμα των σταθερών στοιχείων της H_i. Η H_i είναι κανονική υποομάδα της G, αφού η G είναι αβελιανή. Οπότε, η επέκταση $F \leq L_i$ είναι επέκταση Galois[3] και ισχύει ότι $Gal(L_i/_F) \cong G/_{H_i} \cong C_i$. Άρα, η επέκταση $F \leq L_i$ είναι κυκλική επέκταση Galois. Έστω $[L_i : F] = m_i$, τότε $|C_i| = m_i$. Έχουμε ότι $|C_i| \mid n \Rightarrow m_i \mid n$. Το F περιέχει μια πρωταρχική m_i-ρίζα της μονάδας[4], την ω^{n/m_i}. Ακόμα, η επέκταση $F \leq L_i$ είναι κυκλική επέκταση Galois με $[L_i : F] = m_i$. Τότε,σύμφωνα με το θεώρημα 3.0.3 υπάρχει $\alpha_i \in L_i$ με $L_i = F(\alpha_i)$ και $\alpha_i^{m_i} \in F$. Άρα, $\alpha_i^n = \alpha_i^{m_i k} = (\alpha^{m_i})^k \in F$, διότι F σώμα και $\alpha_i^{m_i} \in F$. Θέτουμε $\alpha_i^n = a_i \in F$. Απο το θεμελιώδες θεώρημα της θεωρίας Galois προκύπτει ότι το $F(\alpha_1, \alpha_2, \ldots, \alpha_r) = L_1 \cdots L_r$ αντιστοιχεί στην ομάδα $H_1 \cap H_2 \cap \cdots \cap H_r =< id_K >$. Άρα, $K = F(\alpha_1, \alpha_2, \ldots, \alpha_r) = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$. □

Παράδειγμα 3.0.3. *Έστω $K = \mathbb{Q}(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$, $a_i \in \mathbb{Q}$. Τότε απο το θεώρημα (3.0.4) προκύπτει ότι η επέκταση $\mathbb{Q} \leq K$ είναι μια 2-επέκταση Kummer.*

Γενικά ισχύει ότι $[K : \mathbb{Q}] \leq 2^r$. Μπορεί να είναι γνήσια μικρότερο απο το 2^r, για παράδειγμα $[\mathbb{Q}(sqrt2, sqrt3, sqrt6) : \mathbb{Q}] = 4 \neq 8$. Ισχύει ότι $[K : \mathbb{Q}] = 2^r$ αν και μόνο αν οι a_i, $i = 1, \ldots, r$ είναι διακριτοί πρώτοι.

Παράδειγμα 3.0.4. *Έστω $F = \mathbb{Q}(i)$, με $i = \sqrt{-1}$ και $K = F(\sqrt[4]{12}, \sqrt[4]{3})$. Το i είναι πρωταρχική 4-ρίζα της μονάδας και $K = F(\sqrt[4]{12}, \sqrt[4]{3})$, με $12, 3 \in F$. Οπότε απο το θεώρημα (3.0.4), προκύπτει ότι η επέκταση $F \leq K$ είναι μια 4-επέκταση Kummer. Ακόμα, $K = F(\sqrt[4]{12}, \sqrt[4]{3}) = \mathbb{Q}(i)(\sqrt[4]{43}, \sqrt[4]{3}) = \mathbb{Q}(i, \sqrt[4]{3}, \sqrt[4]{4}) = \mathbb{Q}(i, sqrt[4]3, \sqrt{2}) = F(\sqrt[4]{3}, \sqrt{2})$. Άρα,*

[3] Το οποίο προκύπτει απο το Θεμελιώδες Θεώρημα της Θεωρίας Galois.
[4] Διότι το F περιέχει μια πρωταρχική n-ρίζα της μονάδας

$[K : F] = 2\dot{4} = 8 \neq 2^4 = 16$.
Επομένως, αν $K = F(\alpha_1, \ldots, \alpha_n)$ *είναι μια n-επέκταση Kummer του F με* $\alpha_i^n \in F$, *τότε υπάρχει περίπτωση* $\alpha_i^k \in F$, *με* $k < n$.

Πρόταση 3.0.1. *Έστω F σώμα το οποίο περιέχει μια πρωταρχική n-ρίζα της μονάδας και* $K = F(\sqrt[n]{b})$, *για κάποιο* $b \in F$. *Τότε η επέκταση* $F \leq K$ *είναι κυκλική επέκταση Galois. Επιπλέον, η* $[K : F] = m$ *είναι ίση με την τάξη του συμπλόκου* bF^{*n} *της ομάδας* F^*/F^{*n} *καί* $Irr(F, \sqrt[n]{b}) = X^m - d$, *για κάποιο* $d \in F$.

Απόδειξη. Έστω $a \in K$ με $a^n = b$. Άρα, το a είναι ρίζα του $X^n - b \in F[X]$. Το F περιέχει μια πρωταρχική n-ρίζα της μονάδας, έστω $\omega \in F$. Οι ρίζες του $X^n - b$ είναι οι $\sqrt[n]{b}, \omega\sqrt[n]{b}, \ldots, \omega^{n-1}\sqrt[n]{b}$. Δηλαδή, το $X^n - b$ αναλύεται υπέρ το K. Θέτουμε $f(X) = X^n - b$, τότε $f'(X) = nX^{n-1}$, άρα ΜΚΔ$(f, f') = 1$. Οπότε το $f(X)$ είναι διαχωρίσιμο υπέρ το F. Δηλαδή, το K είναι σώμα ανάλυσης του διαχωρισίμου πολυωνύμου $f(X) = X^n - b$. Άρα, η επέκταση $F \leq K$ είναι επέκταση Galois.
Απομένει να δείξουμε ότι η επέκταση $F \leq K$ είναι κυκλική. Αρκεί να δείξουμε ότι $Gal(K/_F) =< \sigma >$, δηλαδή το σ είναι γεννήτορας της $G = Gal(K/_F)$. Επειδή, $Irr(a, F) \mid X^n - b = f(X)$, τότε οι ρίζες του $Irr(a, F)$ ανήκουν στο σύνολο $\{\omega^j a : j \in \mathbb{Z}\}$. Οπότε, αν $\sigma \in Gal(K/_F)$, τότε αφού a ρίζα του $Irr(a, F)$, τότε και το $\sigma(a)$ είναι επίσης ρίζα του $Irr(a, F)$, δηλαδή $\sigma(a) = \omega^i a$, για κάποιο $i \in \mathbb{Z}$. Θεωρούμε το σύνολο $S = \{i(modn) : \frac{\sigma(a)}{a} = \omega^i$, για κάποιο $\sigma \in G\}$. Ορίζουμε την απεικόνιση $g : G \to \mathbb{Z}/_{n\mathbb{Z}}$ ώστε $\sigma \mapsto i(modn)$, όπου $\frac{\sigma(a)}{a} = \omega^i$. Η g είναι καλά ορισμένη, διότι άν $\sigma = \tau$, τότε $\frac{\sigma(a)}{a} = \frac{\tau(a)}{a} = \omega^i$, δηλαδή $g(\sigma) = g(\tau)$. Επίσης, η g είναι ομομορφισμός ομάδων, διότι $g(\sigma\tau) = k(modn)$, όπου $\frac{\sigma\tau(a)}{a} = \frac{\sigma(\tau(a))}{a} = \frac{\omega^i\tau(a)}{a} = \omega^i\omega^j = \omega^{i+j} = \omega^k$, αλλά $g(\sigma) = i(modn)$, όπου $\frac{\sigma(a)}{a} = \omega^i$ και $g(\tau) = j(modn)$, όπου $\frac{\tau(a)}{a} = \omega^j$ τότε $g(\sigma)+g(\tau) = i+j = k(modn)$, δηλαδή $g(\sigma\tau) = g(\sigma) + g(\tau)$. Ακόμα, η g είναι ένα-προς-ένα, διότι αν $\sigma(a) = \omega^i a$ και $\tau(a) = \omega^j a$, τότε έστω $g(\sigma) = g(\tau) \Rightarrow i \equiv j(modn) \Rightarrow n \mid (i - j) \Rightarrow i - j = n\dot{k} \Rightarrow i = j + nk$, $k \in \mathbb{Z}$. Τότε $\sigma(a) = \omega^i a = \omega^{j+nk} a = \omega^j \omega^{n^k} a = \omega^j a = \tau(a)$. Δηλαδή, $\sigma = \tau$. Άρα, η g είναι ένα-προς-ένα. Η G είναι μονομορφισμός, άρα $G \cong g(G)$ και $g(G)$ υποομάδα της $\mathbb{Z}/n\mathbb{Z}$. Όμως, $g(G) = S$. Δηλαδή $G \cong S$ και S υποομάδα της $\mathbb{Z}/n\mathbb{Z}$. Άρα, G είναι υποομάδα της $\mathbb{Z}/n\mathbb{Z}$. Οπότε, η G είναι κυκλική, αφού η $\mathbb{Z}/n\mathbb{Z}$ είναι κυκλική. Επόμένως, η επέκταση $F \leq K$ είναι επέκταση Galois. Δηλαδή, $[K : F] = |G|$. Έστω $Gal(K/_F) =< \tau >$ με $\tau(a) = \omega^t a$ και $|G| = m$. Τότε m είναι ο ελάχιστος θετικός ακέραιος ώστε $\omega^{t^m} = 1$. Θεωρούμε το πολυώνυμο $h(X) = \prod_{i=0}^{m-1}(X - \tau^i(a)) = (X - id(a))(X - \tau(a))(X - \tau^2(a)) \cdots (X - \tau^{m-1}(a)) =$

$(X-a)(X-\omega^t a)(X-\omega^{2t}a)\cdots(X-\omega^{(m-1)t}a)$. Ισχύει ότι $h(X)\in F[X]$, διότι
$\tau(h(X)) = \prod_{i=0}^{m-1}(\tau(X)-\tau^{i+1}(a)) = \prod_{k=1}^{m}(X-\tau^k(a)) = \prod_{i=0}^{m-1}(X-\tau^i(a)) = h(X)$
και $\tau(X)=X$, για κάθε $X\in F$. Άρα $h(X)\in F[X]$. Ο σταθερός όρος του $h(X)$ είναι $(-1)^m a\omega^t a\cdots\omega^{(m-1)t}a = (-1)^m a^m \omega^{\frac{1}{2}(m-1)mt} = (-1)^m a^m$ και ισχύει ότι $(-1)^m a^m\in F$. Δηλαδή, $a^m\in F$ και $b^m=(a^n)^m=(a^m)^n\in F^{*n}$, αφού $a^m\in F$ και F σώμα. 'Εστω ότι η τάξη του bF^{*n} στην F^*/F^{*n} είναι m', τότε $b^m\in F^{*n}\Leftrightarrow b^mF^{*n}=F^{*n}\Leftrightarrow (bF^{*n})^m=F^{*n}$. Δηλαδή $ord(bF^{*n})\mid m\Leftrightarrow m'\mid m$. Ακόμα $ord(bF^{*n})=m'\Leftrightarrow b^{m'}F^{*n}=F^{*n}\Leftrightarrow b^{m'}\in F^{*n}\Leftrightarrow b^{m'}=c^n$ με $c\in F^*$. Δηλαδή, $a^{nm'}=c^n\Leftrightarrow (a^{m'})^n-c^n=0$. Άρα, $a^{m'}=c\omega^i$, για κάποιο i. Όμως,$c\omega^i\in F$ διότι $\omega\in F$ και $c\in F$. Άρα, $a^{m'}\in F$. Τότε, $\tau(a^{m'})=a^{m'}$. Αλλά, $\tau(a^{m'})=(\tau(a))^{m'}=(\omega^t a)^{m'}=\omega^{tm'}a^{m'}$. Δηλαδή, $\omega^{tm'}a^{m'}=a^{m'}\Leftrightarrow(\omega^t)^{m'}=1$. Αλλά, $(\omega^t)^m=1$ και m είναι ο ελάχιστος θετικός ακέραιος στο F^*. Άρα, $m\mid m'$. Αλλά και $m'\mid m$. Οπότε, $m=m'$. Δηλαδή, $[K:F]=m=$τάξη του bF^{*n} της F^*/F^{*n}. Ισχύει $[K:F]=degIrr(a,F)=m$ και το a είναι ρίζα του $X^m-a^m\in F[X]$. Οπότε, $Irr(a,F)=X^m-a^m\in F[X]$. □

Πρόταση 3.0.2. *Έστω ω μια πρωταρχική n-ρίζα της μονάδας με $\omega\in F$ και $K=F(\sqrt[n]{a_1},\ldots,\sqrt[n]{a_r})$, δηλαδή η επέκταση $F\le K$ είναι n- επέκταση Kummer. Τότε $[K:F]\le n^r$.*

Στην προταση 3.0.1 αποδείξαμε ότι $[F(\sqrt[n]{a}):F]$ είναι η τάξη του aF^{*n} στην F^*/F^{*n}. Για να γενικεύσουμε αυτό το αποτέλεσμα χρειαζόμαστε την έννοια της διγραμμικής σύζευξης (bilinear pairing).

Ορισμός 3.0.8. *Έστω G,H πεπερασμένες αβελιανές ομάδες και C μια κυκλική ομάδα. Μια συνάρτηση $B: G\times H\to C$ ονομάζεται διγραμμική σύζευξη (bilinear pairing) άν B είναι ομομορφισμός ως προς κάθε συνιστώσα, δηλαδή $B(g_1g_2,h)=B(g_1,h)B(g_2,h)$, για κάθε $g_1,g_2\in G, h\in H$ και $B(g,h_1h_2)=B(g,h_1)B(g,h_2)$, για κάθε $g\in G$ και $h_1,h_2\in H$.*
Μάλιστα η σύζευξη B λέγεται μη-εκφυλισμένη (μη-ιδιάζουσα) αν $B(g,h)=e$, για κάθε $h\in H$ αν και μόνο αν $g=e$ και $B(g,h)=e$, για κάθε $g\in G$ αν και μόνο αν $h=e$.

Έστω ότι η επέκταση $F\le K$ είναι μια n-επέκταση Kummer και $\mu(F)$ είναι το σύνολο των n-ριζών της μονάδας στο F. Τότε το $\mu(F)$ είναι κυκλική ομάδα. Ακόμα ορίζουμε $KUM(K/_F)=\{a\in K^*: a^n\in F\}$ το οποίο λέγεται σύνολο του Kummer και ισχύει ότι $KUM(K/_F)\le K^*$. Ακόμα ισχύουν ότι 1) $F^*\le KUM(K/_F)$,
2) Άν $K=F(\sqrt[n]{a_1},\ldots,\sqrt[n]{a_r})$, τότε $\sqrt[n]{a_i}\in KUM(K/_F)$, για κάθε $i=1,\ldots,r$.

Ορισμός 3.0.9. *1) Ορίζουμε* $kum(K/_F) = KUM(K/_F)/F^*$ *η οποία λέγεται ομάδα του Kummer.*
2) Ορίζουμε Kummer pairing την απεικόνιση $B : Gal(K/_F) \times kum(K/_F) \to \mu(F)$ *ώστε* $B(\sigma, \alpha F^*) = \frac{\sigma(a)}{a}$.

Η απεικόνιση B είναι καλά ορισμένη, διότι αν $\alpha F^* = \beta F^*$ τότε $\alpha = a\beta$, με $a \in F^*$ και $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(a\beta)}{a\beta} = \frac{a\sigma(\beta)}{a\beta} = \frac{\sigma(\beta)}{\beta}$, αφού $\sigma(a) = a$, για κάθε $a \in F$. Δείξαμε ότι η B είναι μη εκφυλισμένη. Στην συνέχεια θα δείξουμε ότι η Kummer pairing μας βοηθάει στο να εξετάσουμε αν μια επέκταση είναι Kummer.

Λήμμα 3.0.4. *Έστω* $B : G \times H \to C$ *μια διγραμμική σύζευξη (pairing). Άν* $h \in H$, $B_h : G \to C$ *με* $B_h(g) = B(g, h)$. *Τότε η* $\varphi : h \mapsto B_h$ *είναι ομομορφισμός ομάδων απο το H στο* $hom(G, C)$. *Άν B είναι μη-εκφυλισμένη, τότε*
i) $exp(G) \mid |C|$
ii) Η φ *είναι ένα-πρός-ένα.*
iii) Η φ *επάγει ένα ισομορφισμό* $G \approxeq H$.

Απόδειξη. Αφού η $B : G \times H \to C$ είναι μια διγραμμική σύζευξη, τότε $B_{h_1h_2}(g) = B(g, h_1h_2) = B(g, h_1)B(g, h_2) = B_{h_1}(g)B_{h_2}(g)$, για κάθε $g \in G$ και $h_1, h_2 \in H$. Οπότε, $\varphi(h_1h_2) = B_{h_1h_2} = B_{h_1}B_{h_2} = \varphi(h_1)\varphi(h_2)$. Άρα, ο φ είναι ομομορφισμός. Ακόμα, $Ker\varphi = \{h \in H : \varphi(h) = 0\} = \{h \in H : B_h = 0\} = \{h \in H : B(g, h) = e,$ για κάθε $g \in G\}$. Άν η B είναι μη εκφυλισμένη τότε $Ker\varphi = \{h \in H : h = e\} = \{e\}$. Άρα, η φ είναι ένα-πρός-ένα. Υποθέτουμε ότι $|C| = m$. Τότε $e = B(e, h) = B(g, h)^m = B(g^m, h)$, για κάθε $h \in H$. Άρα, $g^m = e$, για κάθε $g \in G$, αφού η B είναι μη εκφυλισμένη διγραμμική σύζευξη. Οπότε $Exp(G) \mid m$, δηλαδή $Exp(G) \mid |C|$. Ισχύει ότι η ομάδα $hom(G, C)$ είναι ισόμορφη με τον χαρακτήρα $hom(G, \mathbb{C}^*)$ και $hom(G, \mathbb{C}^*) \approxeq G$. Η φ είναι ένα-πρός-ένα, άρα $H \approxeq \varphi(H) = im(\varphi) \approxeq hom(G, C) \approxeq G$. □

Θεώρημα 3.0.5. *Έστω ότι η επέκταση* $F \leq K$ *είναι μια n-επέκταση Kummer και* $B : Gal(K/_F) \times kum(K/_F) \to \mu(F)$ *μια Kummer pairing. Τότε η B είναι μη εκφυλισμένη και ισχύει ότι* $kum(K/_F) \approxeq Gal(K/_F)$.

Απόδειξη. Αρχικά θα δείξουμε ότι η B είναι διγραμμική σύζευξη (pairing). Έστω $\sigma, \tau \in Gal(K/_F)$ και $\alpha F^* \in kum(K/_F)$. Τότε $B(\sigma\tau, \alpha F^*) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha} \overset{5}{=} \frac{\tau\sigma(\alpha)}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha} = \tau(\frac{\sigma(\alpha)}{\alpha})\frac{\tau(\alpha)}{\alpha}$. Το $\alpha F^* \in kum(K/_F)$, δηλαδή $\alpha \in KUM(K\_F)$, άρα $\alpha \in K^*$ ώστε $\alpha^n \in F$. Αφού $\alpha^n \in F$, τότε $\sigma(\alpha^n) = \alpha^n$. Δηλαδή, $\sigma(\alpha)^n = \alpha^n \Leftrightarrow (\frac{\sigma(\alpha)}{\alpha})^n = 1$. Άρα, το $\frac{\sigma(\alpha)}{\alpha}$ είναι μια n-ρίζα

της μονάδας. Οπότε, το $\frac{\sigma(\alpha)}{\alpha} \in F$, διότι το F περιέχει μια πρωταρχική n-ρίζα της μονάδας, αφού η επέκταση $F \leq K$ είναι επέκταση Kummer. Άρα, $\tau(\frac{\sigma(\alpha)}{\alpha}) = \frac{\sigma(\alpha)}{\alpha}$. Επομένως, $B(\sigma\tau, \alpha F^*) = \tau(\frac{\sigma(\alpha)}{\alpha})\frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha} = B(\sigma, \alpha F^*)B(\tau, \alpha F^*)$. Δηλαδή, η B είναι ομομορφισμός ως προς την πρώτη συνιστώσα. Έστω $\alpha, \beta \in KUM(K/F)$. Τότε $B(\sigma, \alpha F^*\beta F^*) = B(\sigma, \alpha\beta F^*) = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)\sigma(\beta)}{\alpha\beta} = B(\sigma, \alpha F^*)B(\sigma, \beta F^*)$. Δηλαδή, η B είναι ομομορφισμός ως προς την δεύτερη συνιστώσα. Επομένως, η B είναι διγραμμική σύζευξη.
Έπειτα θα δείξουμε ότι η B είναι μη- εκφυλισμένη. Έστω $\sigma \in Gal(K/F)$ με $B(\sigma, \alpha F^*) = 1$, για κάθε $\alpha F^* \in kum(K/F)$. Ισχύει ότι $B(\sigma, \alpha F^*) = 1 \Leftrightarrow \frac{\sigma(\alpha)}{\alpha} = 1 \Leftrightarrow \sigma(\alpha) = \alpha$, για κάθε $\alpha \in KUM(K/F)$. Όμως, τα στοιχεία του $KUM(K/F)$ παράγουν το K ως μία επέκταση F. Οπότε, οι αυτομορφισμοί του K προσδιορίζονται απο την δράση τους σς αυτό το σύνολο. Άρα, $\sigma = id$. Δηλαδή, $B(\sigma, \alpha F^*) = 1$, για κάθε $\alpha F^* \in kum(K/F)$ αν καί μόνο αν $\sigma = id$. Ακόμα, έστω $B(\sigma, \alpha F^*) = 1$, για κάθε $\sigma \in Gal(K/F)$. Τότε, $B(\sigma, \alpha F^*) = 1 \Leftrightarrow \frac{\sigma(\alpha)}{\alpha} = 1 \Leftrightarrow \sigma(\alpha) = \alpha$, για κάθε $\sigma \in Gal(K/F)$. Δηλαδή $\alpha \in Fix(Gal(K/F))$. Αλλά, ισχύει ότι το σώμα των σταθερών στοιχείων της $Gal(K/F)$ είναι ίσο με F, δηλαδή $Fix(Gal(K/F) = F$. Δηλαδή, $\alpha \in F$. Άρα, $\alpha F^* = F^*$. Οπότε, $B(\sigma, \alpha F^*) = 1$, για κάθε $\sigma \in Gal(K/F) \Leftrightarrow \alpha F^* = F^*$. Επομένως, η B είναι μη εκφυλισμένη. Δηλαδή, η $B : Gal(K/F) \times kum(K/F) \to \mu(F)$ είναι μια μη-εκφυλισμένη διγραμμική συύευξη(pairing). Συνεπώς, σύμφωνα με το λήμμα 3.0.4 προκύπτει ότι $kum(K/F) \cong Gal(K/F)$. □

Άν η επέκταση $F \leq K$ είναι επέκταση Galois, τότε $[K : F] = |Gal(K/F)|$. Ακόμα, άν η επέκταση $F \leq K$ είναι επέκταση Kummer, τότε σύμφωνα με το θεώρημα 3.0.5 προκύπτει ότι $[K : F] = |kum(K/F)|$. Οπότε, αν προσδιορίσουμε την $kum(K/F)$, τότε προσδιορίζουμε και την $[K : F]$.

Θεώρημα 3.0.6. *Έστω η επέκταση $F \leq K$ είναι μια n-επέκταση Kummer. Τότε υπάρχει μονομορφισμός ομάδων $f : kum(K/F) \to F^*/F^{*n}$ ώστε $f(\alpha F^*) = \alpha^n F^{*n}$. Η εικόνα της f, Imf, είναι πεπερασμένη υποομάδα της F^*/F^{*n} με $|Imf| = [K : F]$.*

Απόδειξη. Αρχικά θα δείξουμε ότι η f είναι καλά ορισμένη. Ισχύει ότι $\alpha F^* = \beta F^* \Leftrightarrow \beta^{-1}\alpha \in F^*$. Δηλαδή, $(\beta^{-1}\alpha)^n \in F^{*n} \Leftrightarrow \beta^{-n}\alpha^n F^{*n} = F^{*n} \Leftrightarrow \alpha^n F^{*n} = \beta^n F^{*n} \Leftrightarrow f(\alpha F^*) = f(\beta F^*)$. Άρα, η f είναι καλά ορισμένη. Επίσης, η f είναι ομομορφισμός ομάδων, διότι $f(\alpha F^*\beta F^*) = f(\alpha\beta F^*) = (\alpha\beta)^n F^{*n} = \alpha^n\beta^n F^{*n} = \alpha^n F^{*n}\beta^n F^{*n} = f(\alpha F^*)f(\beta F^*)$. Έπειτα, θα δείξουμε ότι η f είναι ένα-προς-ένα. Έστω, $\alpha F^* \in Ker(f)$. Ισχύει ότι $Kerf = \{\alpha F^* \in kum(K/F) : f(\alpha F^* = F^{*n})\}$. Τότε, $\alpha F^* \in Ker(f) \Leftrightarrow$

$f(\alpha F^*) = F^{*n} \Leftrightarrow \alpha^n F^{*n} = F^{*n} \Leftrightarrow \alpha^n F^{*n} = F^{*n} \Leftrightarrow \alpha^n \in F^{*n} \Leftrightarrow$ υπάρχει $a \in F$ ώστε $\alpha^n = a^n \Leftrightarrow (\frac{\alpha}{a})^n = 1$. Δηλαδή,το $\frac{\alpha}{a}$ είναι μια n-ρίζα της μονάδας. Άρα το $\frac{\alpha}{a} \in F$, διότι το F περιέχει μια πρωταρχική n-ρίζα της μονάδας, αφού η επέκταση $F \leq K$ είναι επέκταση Kummer. Δηλαδή, το $\alpha \in F$, αφού $a \in F$, $\frac{\alpha}{a} \in F$ και F είναι σώμα. Άρα, $\alpha F^* = F^*$, δηλαδή $Kerf = \{F^*\}$, όπου F^* είναι το ουδέτερο στοιχείο της $kum(K/F)$. Οπότε, η f είναι ένα-προς-ένα. Επομένως, η f είναι μονομορφισμός ομάδων. Δηλαδή ισχύει ότι $kum(K/F) \cong Imf \leq F^*/F^{*n}$. Η επέκταση $F \leq K$ είναι επέκταση Kummer. Οπότε, σύμφωνα με το θεώρημα 3.0.5 προκύπτει ότι $kum(K/F) \cong Gal(K/F)$. Δηλαδή, $|kum(K/F)| = [K : F]$. Όμως, $kum(K/F) \cong Im(f)$. Δηλαδή, $|Im(f)| = [K : F]$. □

Το θεώρημα 3.0.6 μπορούμε να το χρησιμοποιήσουμε αντίστροφα, για την κατασκευή επεκτάσεων Kummer δοσμένου βαθμού. Έστω G μια πεπερασμένη αβελιανή υποομάδα της F^*/F^{*N}. Σταθεροποιούμε μια αλγεβρική θήκη του F. Ορίζουμε $F(G) = F(\{\sqrt[n]{a} : aF^{*n} \in G\})$ σε μια αλγεβρική θήκη του F. Τότε η επέκταση $F(G)/F$ είναι n-επέκταση Kummer με $Gal(F(G)/F) \cong G$. Άρα, $[F(G) : F] = |G|$.

Παράδειγμα 3.0.5. *Έστω $F = \mathbb{C}(x, y, z) = \{\frac{f(x,c,z)}{g(x,y,z)}, f, g \in \mathbb{C}[X, Y, Z]\}$ το σώμα των ρητών συναρτήσεων με τρείς μεταβλητές υπέρ το $\mathbb{C}$ και $K = F(\sqrt[4]{xyz}, \sqrt[4]{y^2z}, \sqrt[4]{xyz^2})$. Άρα σύμφωνα με το θεώρημα 3.0.4 ισχύει ότι η επέκταση $F \leq K$ είναι 4-επέκταση Kummer, αφού $xyz, y^2z, xyz^2 \in F$ και $K = F(\sqrt[4]{xyz}, \sqrt[4]{y^2z}, \sqrt[4]{xyz^2})$. Ακόμα, σύμφωνα νε το θεώρημα 3.0.6 προκύπτει ότι η εικόνα της $kum(K/F)$ είναι υποομάδα της F^*/F^{*4} και παράγεται απο τα σύμπλοκα $xyzF^{*4}$, y^2zF^{*4}, xyz^2F^{*4}. Στο K, υπάρχει $\alpha \in K$ ώστε $\sqrt[4]{xyz} = \alpha$ με $f(\alpha F^*) = \alpha^4 F^{*4} = xyzF^{*4}$, υπάρχει $\sqrt[4]{y^2z} = \beta \in K$ ώστε $f(\beta F^*) = \beta^4 F^{*4} = y^2zF^{*4}$ και υπάρχει $\sqrt[4]{xyz^2} = \gamma \in K$ ώστε $f(\gamma F^*) = \gamma^4 F^{*4} = xyz^2F^{*4}$. Αφού το σώμα K παράγεται απο τα $\sqrt[4]{xyz}, \sqrt[4]{y^2z}, \sqrt[4]{xyz^2}$, τότε η εικόνα της $kum(K/F)$ στο F^*/F^{*4} θα παράγεται απο τα σύμπλοκα(cosets) των εικόνων αυτών των στοιχείων, δηλαδή $Im(kum(K/F)) =< xyzF^{*4}, y^2zF^{*4}, xyz^2F^{*4} >$. Θέτουμε $a := xyzF^{*4}$, $b := y^2zF^{*4}$, $c := xyz^2F^{*4}$. Ισχυρίζομαι ότι η υποομάδα της F^*/F^{*4} που παράγεται απο τα a, b, c έχει τάξη 32, δηλαδή $| < a, b, c > | = 32$. Οπότε, απο το θεώρημα 3.0.6 ισχύει ότι $[K : F] = 32$. Θεωρούμε την υποομάδα που παράγεται απο τα a, b. Έστω $< a, b > \leq F^*/f^{*4}$. Τα στοιχεία της αβελιανής ομάδας $< a, b >$ είναι της μορφής a^ib^j, με $1 \leq i, j \leq 4$. Τα στοιχεία αυτά είναι όλα διαφορετικά, διότι άν δεν είναι όλα διαφορετικά, δηλαδή έστω ότι $a^ib^j = a^kb^l$. Τότε, υπάρχει $h \in F^*$ με $(xyz)^i(y^2z)^j = (xyz)^k(y^2z)^lh^4$. Ακόμα, $h \in F = \mathbb{C}(x, y, z)$, δηλαδή $h = \frac{f(x,y,z)}{g(x,y,z)}$, όπου $f(X, Y, Z), g(X, Y, Z) \in \mathbb{C}[X, Y, Z]$*

με $ΜΚΔ(f,g) = 1$. *Τότε* $(xyz)^i(y^2z)^jg^4(x,y,z) = (xyz)^k(y^2z)^lf^4(x,y,z)$. *Από μοναδικότητα της παραγοντοποίησης, εξισώνοντας τους εκθέτες των* x,z *προκύπτει ότι* $i \equiv k \pmod 4$ *και* $i+j \equiv k+l \pmod 4$. *Δηλαδή,* $j \equiv l \pmod 4$. *Οπότε, όλα τα στοιχεία* a^ib^j, *με* $1 \leq i,j \leq 4$ *είναι πράγματι διαφορετικά. Επομένως,* $| < a,b > | = 16$. *Παρατηρούμε ότι* $abc = x^2y^4z^4F^{*4}$, *τότε* $(abc)^4 = x^4y^8z^8F^{*4} = F^{*4}$, *δηλαδή* $(abc)^2 \in F^{*4} \Rightarrow (abc)^2 = t^4 \Rightarrow a^2b^2c^2 = t^4 \Rightarrow c^2 = a^{-2}b^{-2}t^4 = a^2b^2t^4$, *με* $t \in F^*$. *Δηλαδή,* $c^2F^{*4} = (ab)^2F^{*4}$, *δηλαδή* $c^2 = (ab)^2$. *Αυτό σημαίνει ότι* $c^2 \in < a,b >$. *Άρα* $c \in < a,b >$ *ή* $c \notin < a,b >$, *δηλαδή* $| < a,b,c > | = 16$ *ή* $| < a,b,c > | = 32$. *Άν* $c \in < a,b >$, *τότε* $c = a^ib^j$ *για κάποια* i,j. *Οπότε, επειδή είναι σύμπλοκα έχουμε ότι* $xyz^2f^4(x,y,z) = (xyz)^i(y^2z)^jg^4(x,y,z)$, *για κάποια πολυώνυμα* f,g. *Απο μοναδικότητα της παραγοντοποίησης, εξισώνοντας τους εκθέτες των* x,y , *έχουμε ότι* $1 \equiv i \pmod 4$ *και* $1 \equiv i+2j \pmod 4$. *Άρα,* $j \equiv 2 \pmod 4$. *Αλλά,* $ab^2 = xyzy^4z^2F^{*4} = xyz^3F^{*4} \neq c$. *Άρα,* $c \notin < a,b >$. *Οπότε,* $[< a,b,c > : < a,b >] = 2$.

$$\begin{array}{c} < a,b,c > \\ |_2 \\ < a,b > \\ |_{16} \\ \{1\} \end{array}$$

Επομένως, $| < a,b,c > | = 32$.

Κεφάλαιο 4

Θεωρία Galois των Reciprocal Πολυωνύμων

Ορισμός 4.0.10. *Έστω $f(X) \in k[X]$, όπου k σώμα με $chk = 0$.*
a) Το πολυώνυμο $f(X)$ ονομάζεται Reciprocal πολυώνυμο αν ισχύει ότι για κάθε ρίζα του a τότε και το $\frac{1}{a}$ είναι επίσης ρίζα του.
b) Το πολυώνυμο $f(X)$ ονομάζεται Gorenstein πολυώνυμο αν είναι reciprocal και έχει επιπλέον την ιδιότητα ότι οι ρίζες a και $\frac{1}{a}$ έχουν την ίδια πολλαπλότητα.

Παρατήρηση 4.0.5. *Άν $f(X) = \sum_{i=1}^{n} c_i X^i \in k[X]$ είναι πολυώνυμο βαθμού n με $c_0 c_n \neq 0$, τότε ορίζουμε*

$$f_s(X) := X^n f(\frac{1}{X}) = \sum_{i=1}^{n} c_{n-i} X^i$$

το οποίο είναι πολυώνυμο βαθμού n.
Το $f(X)$ είναι Gorenstein αν και μόνο αν $f(X) = f_s(X)$, το οποίο συμβαίνει αν και μόνο αν $c_i = c_{n-i}$, για $i = 0, \ldots, n$.

Παρατήρηση 4.0.6. *i) Κάθε ανάγωγο Reciprocal πολυώνυμο υπέρ το $\mathbb{Q}$ είναι Gorenstein. Επίσης, κάθε κυκλοτομικό πολυώνυμο υπέρ το $\mathbb{Q}$ είναι Gorenstein.*
ii) Ένα Gorenstein πολυώνυμο που έχει περιττό βαθμό έχει ρίζα το -1. Πράγματι, αν $f(X) \in k[X]$ είναι Gorenstein πολυώνυμο, τότε ισχύει ότι $f(X) = f_s(X)$. Άρα, $f(-1) = f_s(-1) = (-1)^n f(-1) = -f(-1) \Rightarrow f(-1) = -f(-1) \Rightarrow 2f(-1) = 0 \Rightarrow f(-1) = 0$. Δηλαδή, το -1 είναι ρίζα του $f(X)$. Οπότε, ένα μη γραμμικό ανάγωγο Gorenstein πολυώνυμο έχει άρτιο βαθμό.

Εμείς θα ασχοληθούμε με ανάγωγα πολυώνυμα, άρα υποθέτουμε ότι το n είναι άρτιος, δηλαδή $n = 2m$. Άν το $f(X)$ είναι Gorenstein, τότε οι ρίζες του είναι σε ζευγάρια, δηλαδή οι ρίζες του είναι $\cup_{1\leq i\leq m}\{r_i, r_i^{-1}\}$, όπου η ένωση δεν είναι απαραίτητα ξένη. Κάθε αυτομορφισμός σ της ομάδας Galois του $f(X)$ υπέρ το k, δηλαδή της $G := Gal(f(X)/k)$, μεταθέτει τα blocks $\{r_i, r_i^{-1}\}$, τα οποία είναι m στο πλήθος, άρα $\sigma(\{r_i, r_i^{-1}\}) = \{r_j, r_j^{-1}\}$ και η σ δρα στο r_i ως εξής

$$\sigma : r_i \mapsto r_j \text{ ή } r_j^{-1}$$

Η δράση της σ στο r_i^{-1} είναι $\sigma : r_i^{-1} \mapsto (\sigma(r_i))^{-1}$.

Πρόταση 4.0.3. *Η απεικόνιση*

$$\begin{aligned}\varphi : G &\to S_m \\ \sigma &\mapsto \varphi(\sigma) \quad \textit{όπου } \varphi(\sigma) : i \mapsto j, \textit{ αν } \sigma : r_i \mapsto r_j \text{ ή } r_j^{-1}\end{aligned}$$

είναι ομομορφισμός ομάδων με πυρήνα N ο οποίος αποτελείται από τους αυτομορφισμούς σ που ικανοποιούν $\sigma : r_i \mapsto r_i$ ή r_i^{-1}, για κάθε $i = 1, \ldots, m$.

Απόδειξη. Η φ είναι ομομορφισμός. Πράγματι, έστω $\sigma_1, \sigma_2 \in G$, τότε αν $\varphi(\sigma_1\sigma_2)(i) = j$, έχουμε ότι $\sigma_1\sigma_2 \cdot r_i = \sigma_1 \cdot (\sigma_2 \cdot r_i)$. Άρα, $\varphi(\sigma_1\sigma_2)(i) = \varphi(\sigma_1)\varphi(\sigma_2)(i)$. Δηλαδή, $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$.
Ο $Ker\varphi = \{\sigma \in G | \varphi(\sigma) = id\} = \{\sigma \in G | \varphi(\sigma) : i \mapsto i, \text{ για κάθε } i = 1, \ldots, m\} = \{\sigma \in G | \sigma : r_i \mapsto r_i \text{ ή } r_i^{-1}, \text{ για κάθε } i = 1, \ldots, m\} = N$.
Ισχύει ότι ο πυρήνας της φ, N, είναι ισόμορφος με μία υποομάδα της $(\mathbb{Z}/2\mathbb{Z})^m$, αφού όλα τα μη ταυτοτικά στοιχεία του πυρήνα έχουν τάξη ίση με 2. □

Αυτός ο ομομορφισμός φ θα αποτελέσει κύριο ατικείμενο στην μελέτη μας, διότι μας ενδιαφέρει η γνώση για το πότε η μικρή ακριβής ακολουθία (short exact sequence) $1 \to N \to G \xrightarrow{\varphi} Q \to 1$ διασπάται.

Πόρισμα 4.0.2. *Η ομάδα Galois του Gorenstein πολυωνύμου έχει τάξη το πολύ $2^m m!$.*

Απόδειξη. Σύμφωνα με την πρόταση 4.0.3 ισχύει ότι ο φ είναι ομομορφισμός. Οπότε, απο το θεώρημα ισομορφισμών ομάδων έχουμε ότι $G/Ker\varphi \cong \varphi(G) \leq S_m$, όπου $G = Gal(f(X)/K)$. Άρα, $\frac{|G|}{|Ker\varphi|} = |\varphi(G)| \Rightarrow |G| = |Ker\varphi| \cdot |\varphi(G)| \leq 2^m m!$

□

Στην συνέχεια θα δείξουμε ότι η γενική μορφή του Gorenstein πολυωνύμου έχει τάξη $2^m m!$ και θα αποδείξουμε ένα ανάλογο θεώρημα με το θεώρημα του Abel, το οποίο χαρακτηρίζει την ομάδα Galois της γενικής μορφής του Gorenstein πολυωνύμου.

4.1 Γενική Μορφή του Gorenstein Πολυωνύμου

Ορισμός 4.1.1. *Έστω k σώμα και $s_1, \ldots, s_m$ διακριτές, μη καθορισμένες μεταβλητές και $n = 2m$. Το πολυώνυμο*

$$\begin{aligned} g(X) &= X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^{m-1}s_{m-1}X^{n-m+1} + (-1)^m s_m X^m \\ &\quad +(-1)^{m-1}s_{m-1}X^{m-1} + \cdots + s_2X^2 - s_1X + 1 \\ &= X^n + 1 + \sum_{i=1}^{m}(-1)^i s_i(X^{n-i} + X^i) \in k(s_1, \ldots, s_m)[X] \end{aligned} \tag{4.1}$$

είναι η γενική μορφή του Gorenstein πολυωνύμου βαθμού n.

Το $g(X)$ είναι Gorenstein, γι αυτό και οι ρίζες του είναι σε ζευγάρια. Άν, $\{r_1, \frac{1}{r_1}, \ldots, r_m, \frac{1}{r_m}\}$ είναι το σύνολο των ριζών του $g(X)$, τότε το $L := k(r_1, \ldots, r_m)$ είναι σώμα ανάλυσης του $g(X)$ υπέρ το $K = k(s_1, \ldots, s_m)$. Θέτουμε $t_i = r_i + \frac{1}{r_i} \in L$. Ισχύει ότι $(X - r_i)(X - r_i^{-1}) = X^2 - t_iX + 1$. Οπότε, το $g(X)$ γράφεται ως

$$g(X) = \prod_{i=1}^{m}(X - r_i)(X - \frac{1}{r_i}) = \prod_{i=1}^{m}(X^2 - t_iX + 1) \tag{4.2}$$

Έστω $e_1, e_2, \ldots, e_m$ οι στοιχειώδεις συμμετρικές συναρτήσεις των $t_1, t_2, \ldots, t_m$. Δηλαδή, $e_1 = t_1 + t_2 + \cdots + t_m$, $e_2 = t_1t_2 + t_1t_3 + \cdots + t_1t_m + t_2t_3 + \cdots + t_2t_m + \cdots + t_{m-1}t_m = \sum_{i<j} t_it_j$, $\ldots$, $e_m = t_1t_2\cdots t_m$.
Συγκρίνοντας τους συντελεστές του $g(X)$ στις σχέσεις (4.1) και (4.2), προκύπτει ότι $s_1 = e_1$, $s_2 = e_2 + m$ και γενικά ισχύει ότι $s_i = e_i + \sum_{j<i} c_je_j$.
Οπότε, προκύπτει ότι $K = k(s_1, \ldots, s_m) = k(e_1, \ldots, e_m)$. Η επέκταση $k(t_1, \ldots, t_m)/K$, είναι επέκταση Galois και ισχύει ότι $Gal(k(t_1, \ldots, t_m)/K) \cong S_m$. Απο την άλλη ισχύει ότι, κάθε ρίζα r_i έχει ελάχιστο πολυώνυμο υπέρ το $k(t_1, \ldots, t_m)$ το οποίο είναι $Irr(r_i, k(t_1, \ldots, t_m)) = X^2 - t_iX + 1 = (X - r_i)(X - r_i^{-1})$. Είναι ανάγωγο διότι είναι 2ου βαθμού και οι ρίζες του $r_i, r_i^{-1} \notin k(t_1, \ldots, t_m)$. Άρα, η $\tau_i : r_i \leftrightarrow r_i^{-1}$ είναι αυτομορφισμός του L υπέρ το $k(t_1, \ldots, t_m)$. Οπότε, για κάθε $I \subset \{1, \ldots, m\}$ μπορούμε να ορίσουμε αυτομορφισμό τ_I της ομάδας Galois $G = Gal(L/K)$, δηλαδή $\tau_I \in Gal(L/K)$, ως εξής

$$\tau_I : r_i \mapsto \begin{cases} r_i^{-1}, & \text{αν } i \in I \\ r_i, & \text{αν } i \notin I \end{cases} \tag{4.3}$$

(Ειδικότερα, μπορούμε να ορίσουμε αυτομορφισμό τ_I της ομάδας Galois της L υπέρ το $k(t_1,\ldots,t_m)$, διότι αν $i \in I$ τότε $\tau_I(r_i) = r_i^{-1}$ και $\tau_I(r_i^{-1}) = r_i$, άρα $r_i + r_i^{-1} \mapsto r_i^{-1} + r_i$.) Άν $I = \{i\}$, τότε

$$\tau_i : \begin{cases} r_i \mapsto r_i^{-1} \\ r_j \mapsto r_j, \quad \text{για κάθε } j \neq i \end{cases} \tag{4.4}$$

Άρα, ο αυτομορφισμός τ_I είναι σύνθεση των αυτομορφισμών τ_i, για $i \in I$. Ισχύει ότι, αν $\tau_I(r_i) = r_i^{-1}$, τότε $\tau_I^2(r_i) = \tau_I(r_i^{-1}) = \tau_I^{-1}(r_i) = (r_i^{-1})^{-1} = r_i$ και αν $\tau_I(r_i) = r_i$, τότε $\tau_I^2(r_i) = r_i$. Άρα, για κάθε I ο αυτομορφισμός τ_I έχει την ιδιότητα ότι $\tau_I^2 = id$, δηλαδή για κάθε I ο αυτομορφισμός τ_I είναι involution. Ακόμα, για $I, J \subset \{1,\ldots,m\}$ έχουμε ότι $\tau_I \circ \tau_J = \tau_{I \triangle J}$, όπου $I \triangle J = (I \setminus J) \cup (J \setminus I)$ είναι η συμμετρική διαφορά των I και J. Πράγματι, αφού τα τ_i αντιμετατίθενται τότε για κάθε $i \in I \cap J$, το τ_i εξαφανίζεται διότι $\tau_i^2 = id$. Έτσι στην σύνθεση θα μείνουν μόνο αυτά τα τ_i για $i \in I \setminus J$ ή $i \in J \setminus I$.

Στην συνέχεια θεωρούμε το σύνολο

$$N = \{\tau_I | I \subset \{1,\ldots,m\}\} =< \tau_1, \tau_2, \ldots, \tau_m >$$

Έχουμε ότι η $\varphi : G \to S_m$ είναι ομομορφισμός με $\varphi(\sigma) \in S_m$ και $\varphi(\sigma) : i \mapsto j$, αν $\sigma : r_i \mapsto r_j$ ή r_j^{-1}. Τότε, $Ker\varphi = \{\sigma \in G | \varphi(\sigma) = id_{\{1,2,\ldots,m\}}\} = \{\sigma \in G | \varphi(\sigma) : i \mapsto i,\ r_i \mapsto r_i$ ή r_i^{-1}, για κάθε $i = 1,\ldots,m\} =< \tau_1,\ldots,\tau_m >= N$. Δηλαδή, $N = Ker\varphi$ και άρα $N \trianglelefteq G$. Επομένως έχουμε ότι $N \cong (\mathbb{Z}/2\mathbb{Z})^m$. Ακόμα, ισχύει ότι η επέκταση $L/k(t_1,\ldots,t_m)$ είναι επέκταση Galois, άρα το σώμα των σταθερών στοιχείων της ομάδας $Gal(L/k(t_1,\ldots,t_m))$ είναι το $k(t_1,\ldots,t_m)$. Ισχύει ότι $Gal(L/k(t_1,\ldots,t_m)) =< \tau_1,\ldots,\tau_m >= N$.

$$\begin{array}{ccc} L = k(r_1,\ldots,r_m) & \longleftrightarrow & \{Id_L\} \\ | & & | \\ k(t_1,\ldots,t_m) & \longleftrightarrow & Gal(L/k(t_1,\ldots,t_m)) = N \\ | & & | \\ K = k(s_1,\ldots,s_m) = k(e_1,\ldots,e_m) & \longleftrightarrow & G = Gal(L/K) \end{array}$$

Σύμφωνα με το θεμελιώδες θεώρημα της θεωρίας Galois, ισχύει ότι $Gal(L/K)/Gal(L/k(t_1,\ldots,t_m)) \cong Gal(k(t_1,\ldots,t_m)/K)$ αλλά έχουμε ότι $Gal(k(t_1,\ldots,t_m)/K) \cong S_m$. Άρα, $G/N \cong S_m$.
Οπότε, ορίζεται η μικρή ακριβής ακολουθία

$$1 \to N \xrightarrow{f} G \xrightarrow{\varphi} G/N \cong S_m \to 1$$

Στην συνέχεια ορίζουμε τον ομομορφισμό ομάδων

$$\begin{aligned}\theta : S_m \cong G/N &\to Aut(N)\\ \sigma N &\mapsto \theta(\sigma N)\\ \theta(\sigma N) : N &\to N, \ \text{με}\, \tau \mapsto \sigma\tau\sigma^{-1}\end{aligned}$$

Δηλαδή, $\theta : S_m \cong G/N \to Aut(N)$ ώστε για κάθε $\sigma \in S_m$ και για κάθε $\tau_I \in N$ ισχύει ότι $\theta_\sigma(\tau_I) = \sigma\tau_I\sigma^{-1}$. Το στοιχείο $\sigma \in S_m \cong G/N$ το ταυτίζουμε με το στοιχείο $\sigma N \in G/N$. Πράγματι, ο θ_σ είναι ομομορφισμός, διότι $\theta_{\sigma_1\sigma_2}(\tau) = \sigma_1\sigma_2\tau(\sigma_1\sigma_2)^{-1} = \sigma_1\sigma_2\tau\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\theta_{\sigma_2}(\tau)\sigma_1^{-1} = \theta_{\sigma_1}\theta_{\sigma_2}(\tau)$, δηλαδή $\theta_{\sigma_1\sigma_2} = \theta_{\sigma_1}\theta_{\sigma_2} \Rightarrow \theta(\sigma_1\sigma_2 N) = \theta(\sigma_1 N)\theta(\sigma_2 N)$.
Ο θ είναι συμβατός με τον ομομορφισμό φ, δηλαδή ισχύει ότι

$$\sigma\tau_I\sigma^{-1} = \tau_{\varphi(\sigma)(I)} \tag{4.5}$$

Πράγματι, η σχέση (4.5) ισχύει, διότι επαληθεύεται για τους γεννήτορες της $S_n =< (12), (12\dots m) >$. Οπότε, ο ομομορφισμός θ είναι στην ουσία η φυσική δράση της S_m στα υποσύνολα του $\{1, \dots, m\}$, αφού το N ταυτίζεται με το δυναμοσύνολο του $\{1, \dots, m\}$ ως εξής $\tau_I \leftrightarrow I$, για $\tau_I \in N$ και $I \subset \{1, \dots, m\}$.

Επιλέγουμε μία συγκεκριμένη ρίζα απο κάθε block $\{r_i, r_i^{-1}\}$, έστω την r_i, και ορίζουμε την απεικόνιση

$$\begin{aligned}\psi : S_m \cong G/N &\to G\\ \pi &\mapsto \psi(\pi)\\ \psi(\pi) : L &\to L, \ \text{με}\, r_i \mapsto r_{\pi(i)}\end{aligned}$$

Η ψ είναι ομομορφισμός. Πράγματι, αφού $\psi(\pi_1\pi_2)(r_i) = r_{\pi_1\pi_2(i)} = \psi(\pi_1)(r_{\pi_2(i)}) = \psi(\pi_1)\psi(\pi_2)(r_i)$, δηλαδή $\psi(\pi_1\pi_2) = \psi(\pi_1)\psi(\pi_2)$.
Ακόμα, θα δείξουμε ότι $\varphi \circ \psi = id_{G/N}$. Έστω $\pi \in S_m$ τυχαίο. Τότε, $\varphi \circ \psi(\pi) = \varphi(\psi(\pi))$. Αλλά, $\varphi(\psi(\pi))(i) = \pi(i)$, αφού $\psi(\pi) : r_i \mapsto r_{\pi(i)}$. Δηλαδή, $\varphi \circ \psi(\pi(i)) = \pi(i)$. Άρα, $\varphi \circ \psi = id_{G/N}$. Άρα, υπάρχει ομομορφισμός $\psi : G/N \to G$, με $\varphi \circ \psi = id_{G/N}$, όπου $\varphi : G \to G/N$ και $N \trianglelefteq G$. Οπότε, $G \cong N \rtimes_\theta G/N$ (το οποίο ισχύει, σύμφωνα με το θεώρημα 7[Παράρτημα]).

Θεώρημα 4.1.1. *Η ομάδα Galois της γενικής μορφής του Gorenstein πολυωνύμου βαθμού $2m$, είναι το ημιευθύ γινόμενο*

$$(\mathbb{Z}/2\mathbb{Z})^m \rtimes_\theta S_m$$

με δράση $\theta : S_m \to Aut((\mathbb{Z}/2\mathbb{Z})^m)$, η οποία δίνεται απο την ''φυσική'' δράση του S_m στα υποσύνολα του $\{1, \dots, m\}$.

Απόδειξη. Έχουμε G να είναι η ομάδα Galois της γενικής μορφής του Gorenstein πολυωνύμου. Αποδείξαμε ότι $N \trianglelefteq G$ και $G = N \rtimes_\theta G/N$. Καθώς επίσης δείξαμε ότι $N \cong (\mathbb{Z}/2\mathbb{Z})^m$ και $G/N \cong S_m$. Επομένως, $G \cong (\mathbb{Z}/2\mathbb{Z})^m \rtimes_\theta S_m$, όπου $\theta : S_m \to Aut((\mathbb{Z}/2\mathbb{Z})^m)$ είναι η "φυσική" δράση του του S_m στα υποσύνολα του $\{1, \ldots, m\}$. □

Σημείωση 4.1.1. *Η ομάδα Galois της γενικής μορφής του Gorenstein πολυωνύμου είναι μη αβελιανή για $n = 4$, επειδή αυτή είναι ισόμορφη με την διεδρική ομάδα D_4.*
Ο παραπάνω ισχυρισμός πράγματι ισχύει, για την απόδειξη του θα χρειαστούμε την έννοια του Wreath product.

Ορισμός 4.1.2. *Έστω A, B ομάδες και $m \in \mathbb{Z}_+$ και έστω $\rho : A \to S_m$ ομομορφισμός και H να είναι το ευθύ γινόμενο m αντίγραφων του B. Ακόμα, η $\psi : S_n \to Aut(H)$ είναι ομομορφισμός. Άρα, η $\psi \circ \rho : A \to Aut(H)$ είναι ομομορφισμός. Ορίζουμε Wreath product του B με το A, το οποίο συμβολίζεται $B \wr A$, να είναι το ημιευθύ γινόμενο $H \rtimes_{\psi\circ\rho} A$, δηλαδή $B \wr A = H \rtimes_{\psi\circ\rho} A$.*
Η ομάδα $H \leq B \wr A$ λέγεται βάση του wreath product.

Ισχύει ότι $D_4 = (\mathbb{Z}/2\mathbb{Z}) \wr (\mathbb{Z}/2\mathbb{Z})$. Στην περίπτωση μας $H = (\mathbb{Z}/2\mathbb{Z})^2$ και $\psi \circ \rho = \theta : S_2 \to Aut((\mathbb{Z}/2\mathbb{Z})^2)$. Άρα, $D_4 = (\mathbb{Z}/2\mathbb{Z}) \wr (\mathbb{Z}/2\mathbb{Z}) = H \rtimes_\theta (\mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\theta S_2$.
Αλλά η ομάδα Galois της γενικής μορφής του Gorenstein πολυωνύμου για $n = 4$, σύμφωνα με το παραπάνω θεώρημα, είναι $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\theta S_2$, με $\theta : S_2 \to Aut((\mathbb{Z}/2\mathbb{Z})^2)$. Οπότε, $G \cong D_4$. Η ομάδα αυτή ονομάζεται και hyperoctahedral ομάδα.

4.2 Άλλα Παραδείγματα Reciprocal Πολυωνύμων

Τα κυκλοτομικά πολυώνυμα είναι τα πιο σημαντικά Gorenstein πολυώνυμα. Το n-οστό κυκλοτομικό πολυώνυμο είναι το

$$\Phi_n(X) = \prod_\zeta (X - \zeta)$$

όπου το ζ διατρέχει το σύνολο των πρωταρχικών n-ριζών της μονάδας και ισχύει ότι $deg\Phi_n(X) = \varphi(n)$, με φ να είναι η συνάρτηση του Euler. Ακόμα ισχύει ότι η ομάδα Galois του n-οστού κυκλοτομικού πολυωνύμου υπέρ το $\mathbb{Q}$ είναι ισόμορφη με την ομάδα $U(\mathbb{Z}/n\mathbb{Z})$ των αντιστρέψιμων στοιχείων της $\mathbb{Z}/n\mathbb{Z}$, δηλαδή $Gal(\Phi_n(X)/\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z})$.

Ανάλογα με την περίπτωση της γενικής μορφής του Gorenstein πολυωνύμου, έτσι και στα κυκλοτομικά πολυώνυμα ορίζεται ένας επιμορφισμός $\phi : G \to H$, όπου H είναι υποομάδα της $S_{\varphi(n)/2}$. Οπότε ανάλογα αποδεικνύεται ότι στα κυκλοτομικά πολυώνυμα ισχύει το παρακάτω θεώρημα:

Θεώρημα 4.2.1. *Η ομάδα Galois G του n-οστού κυκλοτομικού πολυωνύμου $\Phi_n(X)$ υπέρ το $\mathbb{Q}$ είναι ίση με το ημιευθύ γινόμενο του $\phi(G)$ με την $\mathbb{Z}/2\mathbb{Z}$ αν και μόνο αν είτε $4 \mid n$ είτε υπάρχει ένας πρώτος διαιρέτης του n, έστω p, τέτοιος ώστε το 2 να είναι η μεγαλύτερη δύναμη του 2 που να διαιρεί το $p-1$.*

Τα Reciprocal πολυώνυμα εμφανίζονται σε πολλές περιοχές των μαθηματικών, συνήθως ως κανονικά πολυώνυμα αλγεβρικών ή γεωμετρικών αντικειμένων που έχουν κάποια δυϊκότητα. Θα αναφέρουμε άνα σημαντικό παράδειγμα.

Άν C μία καμπύλη ορισμένη σε κάποιο πεπερασμένο σώμα $\mathbb{F}_q$, τότε ορίζεται η Ζήτα συνάρτηση αυτής και μέσω της Ζήτα συνάρτησης το L-πολυώνυμο της $C|_{\mathbb{F}_q}$

$$L_{C/\mathbb{F}_q}(t) := (1-t)(1-qt)Z(t)$$

Το πολυώνυμο αυτό επαληθεύει την συνοριακή εξίσωση

$$L_{C/\mathbb{F}_q}(t) = q^g t^{2g} L_{C/\mathbb{F}_q}(\frac{1}{qt})$$

όπου g είναι το γένος της καμπύλης C.
Τότε, το $L_{C/\mathbb{F}_q}(q^{-\frac{1}{2}}t)$ είναι reciprocal.
Πράγματι, αν t_0 ρίζα του $L_{C/\mathbb{F}_q}(q^{-\frac{1}{2}}t)$, δηλαδή $L_{C/\mathbb{F}_q}(q^{-\frac{1}{2}}t_0) = 0$, τότε

$$\begin{aligned} L_{C/\mathbb{F}_q}(\frac{q^{-\frac{1}{2}}}{t_0}) &= q^g(\frac{q^{-\frac{1}{2}}}{t_0})^{2g} L_{C/\mathbb{F}_q}(\frac{1}{q\frac{q^{-1/2}}{t_0}}) \\ &= q^g(\frac{q^{-\frac{1}{2}}}{t_0})^{2g} L_{C/\mathbb{F}_q}(\frac{t_0}{q^{1/2}}) \\ &= q^g(\frac{q^{-\frac{1}{2}}}{t_0})^{2g} L_{C/\mathbb{F}_q}(t_0 q^{-1/2}) = 0 \end{aligned}$$

Επομένως,το $L_{C/\mathbb{F}_q}(q^{-\frac{1}{2}}t)$ είναι reciprocal.

Κεφάλαιο 5

Η ομάδα Galois των Εκθετικών Πολυωνύμων του Taylor

Έστω $f_n(X) = 1+X+\frac{X^2}{2!}+\cdots+\frac{X^n}{n!}$, το n-οστό πολυώνυμο του Taylor της εκθετικής συνάρτησης.

Θεώρημα. *(Θεώρημα του Schur) Έστω* $f_n(X) = 1+X+\frac{X^2}{2!}+\cdots+\frac{X^n}{n!} \in \mathbb{Q}[X]$. *Τότε ισχύει ότι* $Gal(f_n(X)/\mathbb{Q}) \cong A_n$, *αν* $4 \mid n$ *ή* $Gal(f_n(X)/\mathbb{Q}) \cong S_n$, *αλλιώς.*

Το 1930, ο Schur απέδειξε το παραπάνω θεώρημα. Για την απόδειξη του παραπάνω θεωρήματος θα ακολουθήσουμε την απόδειξη του R.Coleman [1].
Για την απόδειξη του θα πρέπει να δείξουμε ότι
1)Το $f_n(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$.
2) Η $G = Gal(f_n(X)/\mathbb{Q})$ περιέχει έναν p-κύκλο για κάθε πρώτο αριθμό p ώστε $\frac{n}{2} < p < n-2$.
3) Να υπολογίσουμε την διακρίνουσα του $f_n(X)$, $D_n = D(f_n(X))$, και να καθορίσουμε πότε είναι τέλειο τετράγωνο.
Για την απόδειξη των (1),(2),(3) θα χρειαστούμε τα ακόλουθα:
i) Το κύριο θεώρημα των p-αδικών πολυγώνων Newton.
ii) Το αξίωμα του Bertrand (το οποίο αποδείχθηκε από τον Tscebyshev[1]): Για κάθε $n \in \mathbb{Z}, n \geq 8$, υπάρχει p πρώτος τέτοιος ώστε $\frac{n}{2} < p < n-2$.
iii)Το θεώρημα του Jordan :

Θεώρημα 5.0.2. *(Θεώρημα του Jordan) Άν η ομάδα G είναι transitive υποομάδα της* S_n, *η οποία περιέχει έναν* p*-κύκλο για κάποιο πρώτο* p *τέτοιο ώστε* $\frac{n}{2} < p < n-2$, *τότε η ομάδα* A_n *περιέχεται στην G.(βλ. [5],*

[1]Γι αυτό τον λόγο είναι γνωστό και ως θεώρημα του Tscebyshev

Θεωρήματα 5.6.2 και 5.7.2)

iv) Η ομάδα Galois ενός πολυωνύμου βαθμού n περιέχεται στην A_n αν και μόνο αν η διακρίνουσα του είναι τέλειο τετράγωνο.

5.1 Πολύγωνο Newton

Έστω p κάποιος πρώτος αριθμός και $\bar{\mathbb{Q}}_p$ η αλγεβρική θήκη του σώματος των p-αδικών αριθμών $\mathbb{Q}_p$. Αν $a \in \bar{\mathbb{Q}}_p$, το $ord_p a$ ορίζεται απο την εξίσωση $|a|_p = p^{-ord_p a}$.

Ορισμός 5.1.1. *Το p-αδικό πολύγωνο του Newton του πολυωνύμου $f(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Q}_p[X]$ ορίζεται ως η αποκάτω κυρτή θήκη (convex hull) των σημείων $(0,0), (1, ord_p a_1), \ldots, (n, ord_p a_n)$. Άν $a_i = 0$, τότε $ord_p(a_i) = 0$. Τα σημεία στα οποία σχηματίζεται γωνία ονομάζονται κορυφές του πολυγώνου.*

Θέτουμε $(x_0, y_0) = (0,0), (x_1, y_1), \ldots, (x_s, y_s)$ αυτές τις κορυφές. Τότε οι αριθμοί $\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$ λέγονται κλίσεις (slopes).

Ισχύει το παρακάτω θεώρημα χωρίς απόδειξη.

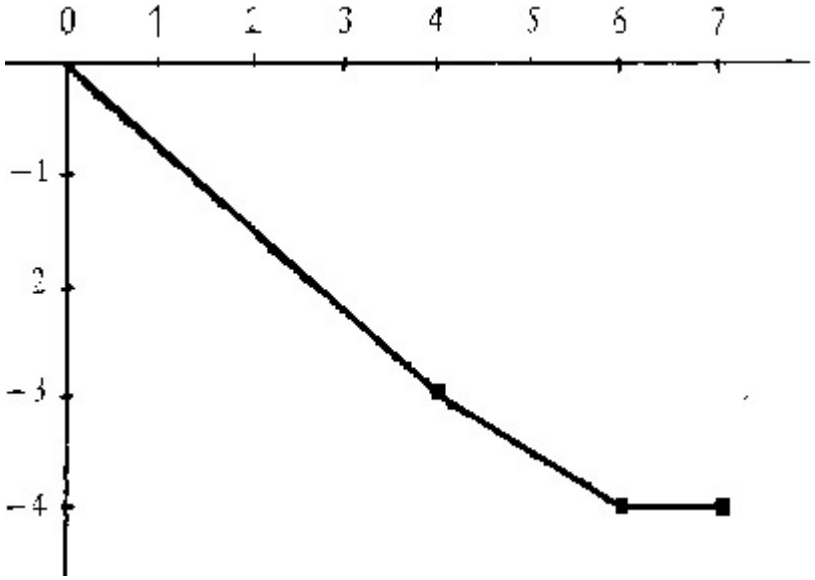
Θεώρημα 5.1.1. *(Θεώρημα p-αδικού πολύγωνου του Newton) Έστω $(x_0, y_0), (x_1, y_1), \ldots, (x_s, y_s)$ οι διαδοχικές κορυφές του πολυγώνου. Τότε το $f(X)$ παραγοντοποιείται υπέρ το $\mathbb{Q}_p$ ως $f(X) = f_1(X) \cdots f_s(X)$, όπου το $f_i(X)$ έχει βαθμό $x_i - x_{i-1}$ και όλες οι ρίζες α_i του $f_i(X)$ στο $\bar{\mathbb{Q}}_p$, έχουν $ord_p \alpha_i = -\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$.*

Για την απόδειξη του βλ. [9]. Ειδικότερα ισχύει ότι, αν το p-αδικό πολύγωνο του Newton έχει γωνίες, τότε το πολυώνυμο $f(X)$ αναλύεται υπέρ το $\mathbb{Q}_p$, δηλαδή δεν είναι ανάγωγο υπέρ το $\mathbb{Q}_p$.

Παράδειγμα 5.1.1. *Το πολύγωνο του Newton του $f_7(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^7}{7!}$ υπέρ το $\mathbb{Q}_2$.*
Αρχικά θα υπολογίσουμε τα σημεία $(i, ord_2(a_i))$, με $0 \leq i \leq 7$. Έχουμε ότι $a_0 = 1$, $a_1 = 1$ και $a_i = \frac{1}{i!}$, με $2 \leq i \leq 7$.
. $i = 0 : a_0 = 1$ τότε $ord_2(1) = 0$, δηλαδή $(0,0)$.
. $i = 1 : a_1 = 1$ τότε $ord_2(1) = 0$, δηλαδή $(1,0)$.
. $i = 2 : a_2 = \frac{1}{2} = 2^{-1}$ τότε $ord_2(a_2) = -1$, δηλαδή $(2,-1)$.
. $i = 3 : a_3 = \frac{1}{3!} = 2^{-1}3^{-1}$ τότε $ord_2(a_3) = -1$, δηλαδή $(3,-1)$.
. $i = 4 : a_4 = \frac{1}{4!} = 2^{-1}3^{-1}4^{-1} = 2^{-3}3^{-1}$ τότε $ord_2(a_4) = -3$, δηλαδή

$(4,-3)$.
▪ $i=5:\ a_5=\frac{1}{5!}=2^{-3}3^{-1}5^{-1}$ *τότε* $ord_2(a_5)=-3$, *δηλαδή* $(5,-3)$.
▪ $i=6:\ a_6=\frac{1}{6!}=2^{-3}3^{-1}5^{-1}6^{-1}=2^{-4}3^{-2}5^{-1}$ *τότε* $ord_2(a_6)=-4$, *δηλαδή* $(6,-4)$.
▪ $i=7:\ a_7=\frac{1}{7!}=2^{-4}3^{-2}5^{-1}7^{-1}$ *τότε* $ord_2(a_7)=-4$, *δηλαδή* $(7,-4)$.

Άρα οι κορυφές του πολυγώνου του Newton είναι οι εξής $(x_0,y_0)=(0,0)$, $(x_1,y_1)=(4,-3)$, $(x_2,y_2)=(6,-4)$, $(x_3,y_3)=(7,-4)$. *Οπότε οι κλίσεις των ευθειών είναι* $m_1=-\frac{3}{4}$, $m_2=-\frac{1}{2}$, $m_3=0$. *Άρα το* $f_7(X)$ *αναλύεται σε γινόμενο 3 παραγόντων υπέρ του* $\mathbb{Q}_2$ *υπέρ το* $\mathbb{Q}_2$ *οι οποίοι έχουν βαθμό* $4-0=4$, $6-4=2$, $7-6=1$ *αντιστοίχως.*
Παρατηρούμε ότι $7=2^2+2+1$. *Οπότε οι x-συντεταγμένες των κορυφών είναι τα "μερικά αθροίσματα" της 2-αδικής παράστασης του 7, δηλαδή* 2^2, $2^2+2=6$, $2^2+2+1=7$.



Από το παραπάνω παράδειγμα παρατηρούμε ότι γενικά ισχύει ότι, αν $n=b_1p^{n_1}+b_2p^{n^2}+\cdots$, *με* $n_1>n_2>\cdots$ *και* $1\le b_i\le p-1$. *Τότε οι x-συντεταγμένες των κορυφών του πολυγώνου Newton του* $f_n(X)=1+X+\frac{X^2}{2!}+\cdots+\frac{X^n}{n!}$ *είναι*

$$\begin{aligned} x_1 &= b_1 p^{n_1} \\ x_2 &= b_1 p^{n_1} + b_2 p^{n^2} \\ &\vdots \\ x_i &= b_1 p^{n_1} + b_2 p^{n^2} + \cdots + b_i p^{n_i} \\ &\vdots \end{aligned}$$

Οπότε οι κλίσεις είναι $m_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}} = \frac{y_i - y_{i-1}}{b_i p^{n_i}}$.

Υποθέτουμε ότι $n = b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_s p^{n_s}$, όπου $0 < b_i < p,\ n_1 > n_2 > \cdots > n_s$ και $x_i = b_1 p^{n_1} + \cdots + b_i p^{n_i}$, για $i = 1, 2, \ldots$.

Λήμμα 5.1.1. *Υποθέτουμε ότι* k *είναι ένας θετικός ακέραιος και* $k = a_0 + a_1 p + \cdots + a_s p^s$, *όπου* $0 \leq a_i < p$. *Τότε ισχύει ότι*

$$ord_p(k!) = \frac{k - (a_0 + a_1 + \cdots + a_s)}{p - 1}$$

Απόδειξη. Έστω ότι $p^e \mid m$ και $p^{e+1} \nmid m$, για κάποιο φυσικό αριθμό m. Αυτό σημαίνει ότι το p-αδικό ανάπτυγμα του m, έχει την μορφή $m = a_e p^e + a_{e+1} p^{e+1} + \cdots + a_r p^r$, για κάποιο r, με $0 \leq a_j < p$, για κάθε $j = e, e+1, \ldots, r$. Επομένως, επειδή οι συντελεστές πρεπει να είναι στο $\{0, 1, \ldots, p-1\}$ ισχύει ότι $m - 1 = (p-1) + (p_1)p + \cdots + (p-1) + (p-1)p^{e-1} + (a_e - 1)p^e + a_{e+1}p^{e+1} + \cdots + a_r p^r$. Θέτουμε r_m να είναι το άθροισμα των συντελεστών του m, δηλαδή $r_m := a_e + a_{e+1} + \cdots + a_r$. Τότε, $r_{m-1} = e(p-1) + a_e - 1 + a_{e+1} + \cdots + a_r$. Άρα, $\frac{r_{m-1} - r_m + 1}{p-1} = e = ord_p(m)$. Επομένως,

$$ord_p(k!) = ord_p(1 \cdots k) = \sum_{m=1}^{k} \frac{r_{m-1} - r_m + 1}{p-1} = \frac{1}{p-1} \sum_{m=1}^{k} (r_{m-1} - r_m + 1) =$$

$$\frac{1}{p-1}[(r_0 - r_1 + 1) + (r_1 - r_2 + 1) + \cdots + (r_{k-1} - r_k + 1)] = \frac{k - r_k}{p-1}. \qquad \square$$

Το παράδειγμα μας υποβάλλει την ιδέα της ισχύος της γενικότητας, δηλαδή οι κορυφές του πολυγώνου του Newton του πολυωνύμου $f_n(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$ θα είναι της μορφής $(x_i, -ord(x_i!))$ με $1 < i < s$. Θα υπολογίσουμε τις κλίσεις του πολυωνύμου $f_n(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$. Άρα,

$$m_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}} = \frac{-ord_p(x_i!) + ord_p(x_{i-1}!)}{x_i - x_{i-1}}$$

Ισχύει ότι

$$\begin{aligned} ord_p(x_i!) &= \frac{x_i - b_1 - \cdots - b_i}{p-1} = \frac{b_1 p^{n_1} + \cdots + b_i p^{n_i} - b_1 - \cdots - b_i}{p-1} \\ &= \frac{b_1(p^{n_1}-1) + b_2(p^{n_2}-1) + \cdots + b_i(p^{n_i}-1)}{p-1} \end{aligned}$$

Οπότε,

$$\begin{aligned} m_i &= \frac{-ord_p(x_i!) + ord_p(x_{i-1}!)}{x_i - x_{i-1}} \\ &= \frac{-b_1(p^{n_1}-1) - \cdots - b_i(p^{n_i}-1) + b_1(p^{n_1}-1) + \cdots + b_{i-1}(p^{n_{i-1}}-1)}{(p-1)b_i p^{n_i}} \\ &= -\frac{p^{n_i}-1}{p^{n_i}(p-1)} \end{aligned}$$

Πόρισμα 5.1.1. *Έστω d θετικός ακέραιος. Υποθέτουμε ότι το d διαιρεί τους παρανομαστές των κλίσεων του p-αδικού πολυγώνου του Newton του πολυωνύμου $f(X)$. Τότε το d διαιρεί τον βαθμό απο κάθε (ανάγωγο) παράγοντα του $f(X)$ υπέρ το $\mathbb{Q}_p$.*

Απόδειξη. Αρκεί να δείξουμε ότι το d διαιρεί τον βαθμό απο κάθε ανάγωγο παράγοντα του f υπέρ το $\mathbb{Q}_p$, αφού αν κάποιος παράγοντας δεν είναι ανάγωγος τότε θα αναλύεται σε γινόμενο αναγώγων. Έστω h ένας ανάγωγος παράγοντας του f υπέρ το $\mathbb{Q}_p$. Έστω επίσης $\alpha \in \bar{\mathbb{Q}}_p$ μια ρίζα του h. Έχουμε ότι το d διαιρεί τον παρανομαστή απο κάθε κλίση. Άρα, το d διαιρεί τον παρανομαστή της εκτίμησης του α, δηλαδή της $ord_p(\alpha)$, συμφωνα με το θεώρημα 5.1.1. Οπότε, το d διαιρεί τον δείκτη διακλάδωσης της επέκτασης $\mathbb{Q}_p \leq \mathbb{Q}_p(\alpha)$ (σύμφωνα με το θεώρημα 8[Παράρτημα][2]), ο οποίος διαιρεί τον βαθμό της επέκτασης $\mathbb{Q}_p \leq \mathbb{Q}_p(\alpha)$. Αλλά, το h είναι ανάγωγο και α ρίζα του h. Άρα, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = degh$. Επομένως, το d διαιρεί τον βαθμό του h. □

Πόρισμα 5.1.2. *Έστω ότι $p^m \mid n$. Τότε το p^m διαιρεί τον βαθμό κάθε παράγοντα του $f_n(X)$ υπέρ το $\mathbb{Q}_p$.*

Απόδειξη. Έστω ότι $n = b_1 p^{n_1} + \cdots + b_s p^{n_s}$. Αφού $p^m \mid n$, τότε $m \leq n_s < n_{s-1} < \cdots$. Άρα, απο το θεώρημα 5.1.1 προκύπτει ότι το p^m διαιρεί τους παρανομαστές απο κάθε m_i. Συνεπώς, σύμφωνα με το πόρισμα 5.1.1 ισχύει ότι το p^m διαιρεί τον βαθμό απο κάθε παράγοντα του $f_n(X)$ υπέρ το $\mathbb{Q}_p$. □

[2]Αυτό το θεώρημα εφαρμόζουμε για κάθε ρίζα α του $f(X)$ και κάθε ανάγωγο $h(X)$ που έχει ρίζα του το α.

Πόρισμα 5.1.3. *Έστω $p^k \leq n$. Τότε το p^k διαιρεί τον βαθμό της επέκτασης ενός σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}_p$.*

Απόδειξη. Έστω $n = b_1 p_1^{n_1} + \cdots + b_s p_s^{n_s}$. Αφού $p^k \leq n$, τότε $k \leq n_1$. Άρα το p^k διαιρεί τον παρανομαστή του m_1. Αλλά, όπως έχουμε δείξει και παραπάνω, ισχύει ότι το p^k διαιρεί τον βαθμό οποιασδήποτε επέκτασης του $\mathbb{Q}_p$ με την επισύναψη μιας ρίζας του $f_n(X)$ με εκτίμηση αυτής της ρίζας $-m_1$. Συνεπώς, το p^k διαιρεί τον βαθμό της επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}_p$. □

5.2 Θεώρημα του Schur

Ορισμός 5.2.1. *Άν το $f(X) \in K[X]$ αναλύεται σε κάποιο σώμα ανάλυσης του ως $f(X) = (X - r_1)(X - r_2)\cdots(X - r_n)$, τότε η διακρίνουσα του $f(X)$ ορίζεται ως $D(f(X)) := \prod_{i<j}(r_i - r_j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j}(r_i - r_j)$.*

Θεώρημα 5.2.1. *Έστω $f(X) \in K[X]$ ένα ανάγωγο, διαχωρίσιμο πολυώνυμο βαθμού n. Άν $chK \neq 2$, τότε η ομάδα Galois του $f(X)$ υπέρ το K είναι υποομάδα της A_n αν και μόνο αν η διακρίνουσα του f, $D(f(X))$, είναι τέλειο τετράγωνο στο K.*

Απόδειξη. Αφού το $f(X)$ είναι διαχωρίσιμο πολυώνυμο βαθμού n, τότε αν $r_1, r_2, \ldots, r_n$ είναι οι ρίζες του $f(X)$ ισχύει ότι $f(X) = (X - r_1)(X - r_2)\cdots(X - r_n)$ και $L = K(r_1, r_2, \ldots, r_n)$ είναι το σώμα ανάλυσης του f υπέρ το K. Θέτουμε $\delta = \prod_{i<j}(r_i - r_j) \neq 0$. Δηλαδή, $\delta \in L$ και $\delta^2 = D(f(X)) \in K$. Οπότε, η $D(f(X))$ είναι τέλειο τετράγωνο του K αν και μόνο αν $\delta \in K$. Για κάθε $\sigma \in Gal(L/K)$ ισχύει ότι $sign(\sigma) = \mp 1$, αφού σ είναι μετάθεση των ριζών του f. Οπότε, $\sigma(\delta) = \prod_{i<j}(\sigma(r_i) - \sigma(r_j)) = sign(\sigma)\prod_{i<j}(r_i - r_j) = sign(\sigma)\delta$. Άρα, $\sigma(\delta) = \mp\delta$. Αφού $\delta \neq 0$ και $chK \neq 2$, τότε $\delta \neq -\delta$. Ισχύει ότι $\sigma \in A_n \Leftrightarrow sign(\sigma) = 1$. Δηλαδή, $\sigma \in A_n \Leftrightarrow \sigma(\delta) = \delta$. Επομένως, $Gal(f(X)/K) \leq A_n$ αν και μόνο αν το δ παραμένει σταθερό απο την $Gal(f(X)/K)$, το οποίο είναι ισοδύναμο με το ότι $\delta \in K$. Άρα, $Gal(f(X)/K) \leq A_n$ αν και μόνο αν η $D(f(X))$ είναι τέλειο τετράγωνο στο K. □

Παρατήρηση 5.2.1. *Ισχύει ότι αν το πολυώνυμο f είναι μονικό ώστε $f(X) = (X - a_1)\cdots(X - a_n)$, τότε $D(f(X)) = (-1)^{\binom{n}{2}} \prod_{i \neq j}(a_i - a_j) =$*

$(-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(a_i)$.

Ορισμός 5.2.2. *Άν* $f(X) = a_n X^n + \cdots + a_1 X + a_0$ *και* $r_1, \ldots, r_n$ *ρίζες του* $f(X)$, *τότε*

$$D(f(X)) = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2 = (-1)^{\binom{n}{2}} a_n^{2n-2} \prod_{i \neq j} (r_i - r_j)$$

Θεώρημα 5.2.2. *(Θεώρημα του Schur) Έστω* $f_n(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!} \in \mathbb{Q}[X]$. *Τότε ισχύει ότι* $Gal(f_n(X)/\mathbb{Q}) \cong A_n$, *αν* $4 \mid n$ *ή* $Gal(f_n(X)/\mathbb{Q}) \cong S_n$, *αλλιώς.*

Απόδειξη. Στόχος μας είναι να δείξουμε ότι η ομάδα A_n περιέχεται στην ομάδα Galois $Gal(f_n(X)/\mathbb{Q})$ σε όλες τις περιπτώσεις. Το ζητούμενο θα προκύψει απο το γεγονός ότι $Gal(f(X)/\mathbb{Q}) \leq A_n$ αν και μόνο αν η $D(f(X))$ είναι τέλειο τετράγωνο στο $\mathbb{Q}$.
Αρχικά, θα υπολογίσουμε την διακρίνουσα του $f_n(X)$, δηλαδη την $D(f_n(X))$. Έστω ότι $a_1, \ldots, a_n$ ρίζες του $f_n(X)$ δηλαδή $f_n(X) = \frac{1}{n!}(X - a_1) \cdots (X - a_n)$ και $f_n'(X) = 1 + X + \cdots + \frac{X^{n-1}}{(n-1)!} = f_{n-1}(X)$.

$$\begin{aligned} D(f_n(X)) &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i \neq j} (a_i - a_j) = (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i=1}^{n} n! f_n'(a_i) \\ &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i=1}^{n} n! f_{n-1}(a_i) \end{aligned}$$

Ακόμα, $f_n(X) = f_{n-1}(X) + \frac{X^n}{n!}$ και το a_i είναι ρίζα του $f_n(X)$, δηλαδή $f_n(a_i) = 0 \Leftrightarrow f_{n-1}(a_i) = -\frac{a_i^n}{n!}$. Οπότε

$$\begin{aligned} D(f_n(X)) &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i=1}^{n} n! f_{n-1}(a_i) = (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i=1}^{n} n!(-\frac{a_i^n}{n!}) \\ &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}} \prod_{i=1}^{n} (-a_i^n) = (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}+n} \prod_{i=1}^{n} (a_i^n) \\ &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}+n} (\prod_{i=1}^{n} a_i)^n = (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}+n} ((-1)^n n! f_n(0))^n \end{aligned}$$

Τα a_i είναι ρίζες του $f_n(X)$. Άρα, $n!f_n(0) = (-1)^n \prod_{i=1}^{n} a_i \Rightarrow \prod_{i=1}^{n} a_i = n!f_n(0)(-1)^n$. Ακόμα, $f_n(0) = 1$. Οπότε,

$$\begin{aligned} D(f_n(X)) &= (\frac{1}{n!})^{2n-2}(-1)^{\binom{n}{2}+n}(-1)^{n^2}(n!)^n = (n!)^{2-n}(-1)^{\binom{n}{2}}(-1)^{n^2+n} \\ &= (-1)^{\binom{n}{2}}(n!)^{2-n} = (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2} \end{aligned}$$

Διότι, $(-1)^{n^2+n} = 1$, αφού άν $n = 2k$, $k \in \mathbb{Z}$, τότε $n^2 + n = 2(k + 2k^2)$ και αν $n = 2k + 1$, $k \in \mathbb{Z}$, τότε $n^2 + n = 2(k^2 + 3k + 1)$.
Επομένως, $D(f_n(X)) = (-1)^{\binom{n}{2}}(n!)^{2-n} = (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2}$.
Άν $n \equiv 0 \bmod 4$, τότε $n = 4k$, $k \in \mathbb{Z}$. Άρα, $D(f_n(X)) = (-1)^{\binom{4k}{2}}((4k)!)^{2-4k} = ((4k)!)^{2-4k} = ((4k)!^{1-2k})^2$, αφού $\binom{4k}{2} = 2k(4k-1)$. Οπότε, η $D(f_n)$ είναι τέλειο τετράγωνο ρητού αριθμού.
Άν $n \equiv 2 \bmod 4$, τότε: $4 \mid n-2 \Leftrightarrow n = 4k+2$, $k \in \mathbb{Z}$ και $\binom{n}{2} = 8k^2+6k+1$. Άρα, $D(f_n) = (-1)^{8k^2+6k+1}(n!)^{2-n} = -(n!)^{-4} = -(\frac{1}{n!})^{4k} < 0$. Οπότε, η $D(f_n(X))$ δεν είναι τέλειο τετράγωνο ρητού αριθμού.
Άν $n \equiv 3 \bmod 4$, τότε $4 \mid n-3 \Leftrightarrow n = 4k+3$, $k \in \mathbb{Z}$ και $\binom{n}{2} = 2(k^2+5k)+3$. Άρα, $D(f_n(X)) = (-1)^{\binom{4k+3}{2}}[(4k+3)!]^{2-4k-3} = -1[(4k+3)!]^{-4k-1} < 0$. Οπότε, η $D(f_n(X))$ δεν είναι τέλειο τετράγωνο ρητού αριθμού.
Άν $n \equiv 1 \bmod 4$, τότε $4 \mid n-1 \Leftrightarrow n = 4k+1$, $k \in \mathbb{Z}$ και $\binom{n}{2} = 2k(4k+1)$. Άρα, $D(f_n(X)) = (-1)^{2k(4k+1)}[(4k+1)!]^{1-4k}$. Αλλά απο το κριτήριο του Bertrand (θεώρημα του Tschebyshev), έχουμε ότι για κάθε ακέραιο n με $n \leq 8$ υπάρχει πρώτος p τέτοιος ώστε $\frac{n}{2} < p < n-2$ και έπεται ότι για κάθε ακέραιο $n > 1$ υπάρχει πρώτος p τέτοιος ώστε $\frac{n}{2} < p < n-2$ με $ord_p(n!) = 1$. Οπότε, η $D(f_n(X))$ δεν είναι τέλειο τετράγωνο ρητού αριθμού.
Επομένως, η $D(f_n)$ είναι τέλειο τετράγωνο στο $\mathbb{Q}$ αν και μόνο αν $4 \mid n$. Οπότε, σύμφωνα με το θεώρημα 5.2.1 ισχύει ότι $Gal(f(X)/_{\mathbb{Q}}) \leq A_n$ αν και μόνο αν $4 \mid n$.

Στην συνέχεια θα δείξουμε ότι το $f_n(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$. Υποθέτουμε ότι $n = \prod_p p^{n_p}$, όπου p πρώτος, είναι η ανάλυση του n σε πρώτους παράγοντες. Για κάθε πρώτο p ισχύει ότι $p^{n_p} \| n$. Άρα σύμφωνα με το πόρισμα 5.1.2 προκύπτει ότι το p^{n_p} διαιρεί τον βαθμό από κάθε παράγοντα του $f_n(X)$ υπέρ το $\mathbb{Q}_p$. Όμως, αυτό ισχύει για κάθε πρώτο p από την αναλύση του n. Οπότε, το p^{n_p} διαιρεί τον βαθμό από κάθε παράγοντα του $f_n(X)$ υπέρ το $\mathbb{Q}$. Ακόμα, $p^{n_p} \leq n$, για κάθε πρώτο p. Σύμφωνα με το πόρισμα 5.1.3 έχουμε ότι το p^{n_p} διαιρεί το βαθμό της

επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}_p$, ο οποίος διαιρεί το βαθμό της επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}$. Επομένως, το n διαιρεί τον βαθμό της επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}$. Όμως, $degf_n(X) = n$. Άρα, το $f_n(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$. Οπότε, η ομάδα Galois $Gal(f_n(X)/\mathbb{Q})$ είναι transitive.
Απομένει να δείξουμε ότι η ομάδα $Gal(f_n(X)/\mathbb{Q})$ περιέχει έναν p-κύκλο, για κάθε πρώτο p τέτοιο ώστε $\frac{n}{2} < p < n-2$.
Υποθέτουμε ότι p είναι πρώτος τέτοιο ώστε $\frac{n}{2} < p < n-2$. Θα αποδείξουμε ότι η ομάδα Galois $Gal(f_n(X)/\mathbb{Q})$ περιέχει κύκλο μήκους p. Οπότε, σύμφωνα με το πόρισμα 5.1.3, το p διαιρεί το βαθμό της επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}_p$, ο οποίος διαιρεί τον βαθμό της επέκτασης του σώματος ανάλυσης του $f_n(X)$ υπέρ το $\mathbb{Q}$. Δηλαδή, $p \mid |Gal(f_n(X)/\mathbb{Q})|$. Οπότε, απο το θεώρημα Cauchy προκύπτει ότι η ομάδα Galois $Gal(f_n(X)/\mathbb{Q}) = G$ περιέχει ένα στοιχείο τάξης p. Αλλά τα μόνα στοιχεία τάξης p στην S_n είναι οι κύκλοι μήκους p, αν $p > \frac{n}{2}$. Άρα, δείξαμε ότι η ομάδα $Gal(f_n(X)/\mathbb{Q})$ περιέχει έναν p-κύκλο. Οπότε, σύμφωνα με το θεώρημα Jordan (θεώρημα 5.0.2), έχουμε ότι για κάθε $n \geq 8$ η ομάδα A_n περιέχεται στην ομάδα G.
Ακόμα, αποδείξαμε ότι αν $4 \mid n$ τότε η $D(f_n(X))$ είναι τέλειο τετράγωνο, ισοδύναμα ισχύει ότι $Gal(f_n(X)/_{\mathbb{Q}}) \leq A_n$. Επομένως, αν $4 \mid n$ τότε $Gal(f_n(X)/_{\mathbb{Q}}) \cong A_n$, αλλιώς ισχύει $Gal(f_n(X)/_{\mathbb{Q}}) \cong S_n$, αφού $A_n < Gal(f_n(X)/\mathbb{Q})$, $[S_n : A_n] = 2$.

Για τις περιπτώσεις όπου το $n \leq 7$ το θεώρημα του Schur (θεώρημα 5.2.2) ισχύει. Στις περιπτώσεις αυτές το επαληθεύσαμε με την χρήση του προγράμματος Maple. Παραθέτουμε παρακάτω τα αποτελέσματα απο το πρόγραμμα Maple, από τα οποία διαπιστώνουμε ότι

$$Gal(f_2(X)/\mathbb{Q}) \cong S_2$$

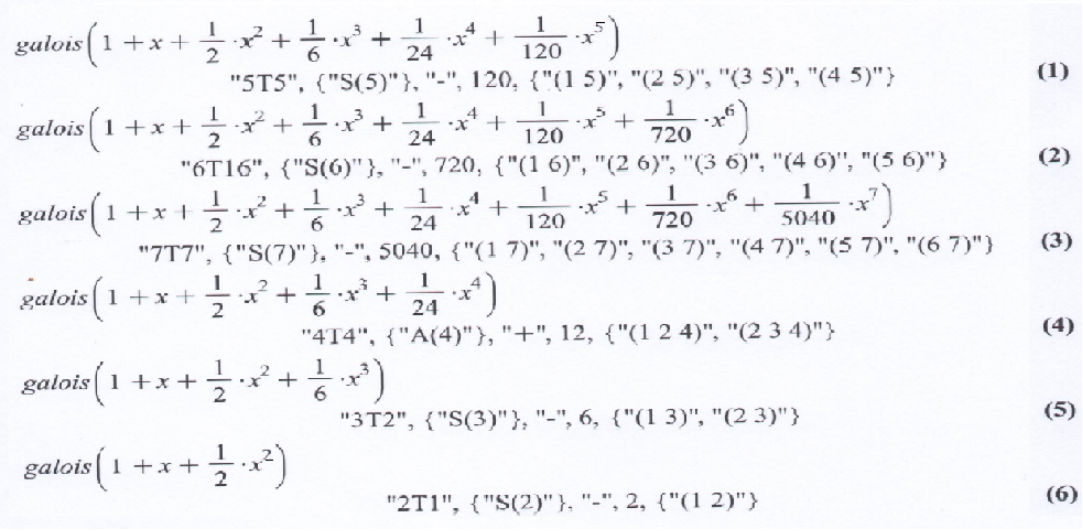
$$Gal(f_3(X)/\mathbb{Q}) \cong S_3$$

$$Gal(f_4(X)/\mathbb{Q}) \cong A_4$$

$$Gal(f_5(X)/\mathbb{Q}) \cong S_5$$

$$Gal(f_6(X)/\mathbb{Q}) \cong S_6$$

$$Gal(f_7(X)/\mathbb{Q}) \cong S_7$$



□

Παρατήρηση 5.2.2. *Τα ίδια επιχειρήματα με παραπάνω μπορούμε να χρησιμοποιήσουμε για να δείξουμε ότι το* $\sum_{j=0}^{n} a_j \frac{x^j}{j!}$, *με* $a_j = \pm 1$, *έχει ομάδα Galois* G *η οποία περιέχει την ομάδα* A_n.

Παράρτημα Α΄

Καθαρού τύπου (pure of type) επεκτάσεις

Θεώρημα 1. *Η πολλαπλασιαστική ομάδα των n-ριζών της μονάδας, έστω U_n, είναι κυκλική.*

Απόδειξη. Έστω $e = Exp(U_n)$ =εκθέτης της U_n, δηλαδή $e \in \mathbb{N}$ είναι ο ελάχιστος φυσικός αριθμός τ.ω $a^e = 1, \forall a \in U_n$. Δηλαδή όλα τα $a \in U_n$ είναι ρίζες του πολυωνύμου $g(X) = X^e - 1$. Όμως, το πολυώνυμο $g(X)$ έχει το πολύ e ρίζες. Άρα,

$$|U_n| \leq e \tag{Α΄.1}$$

Επίσης, ισχύει ότι $Exp(U_n) \leq |U_n|$, δηλαδή

$$e \leq |U_n| \tag{Α΄.2}$$

διότι ο εκθέτης μιας ομάδας δέν μπορεί να υπερβαίνει την τάξη της ομάδας.
Οπότε, από της σχέσεις (Α΄.1) καί (Α΄.2) προκύπτει ότι $e = |U_n|$. Ακόμα, η ομάδα U_n είναι πεπερασμένη, αφού αποτελείται απο τις n-ρίζες της μονάδας. Επομένως, η ομάδα U_n είναι πεπερασμένη αβελιανή ομάδα και ισχύει ότι $Exp(U_n) = |U_n|$. Άρα, η ομάδα U_n είναι κυκλική[1]. □

Ορισμός 1. *Έστω ΜΚΔ$(n, expchar(F)) = 1$. Μια επέκταση $F \leq F(\alpha)$ είναι καθαρού τύπου n (pure of type n), αν α είναι ρίζα του διωνύμου $X^n - u \in F[X]$, δηλαδή αν $\alpha^n \in F$.*

Ακόμα ισχύει ότι άν η επέκταση $F < E$ είναι καθαρού τύπου d (pure

[1]Διότι, ισχύει ότι άν G πεπερασμένη αβελιανή ομάδα τέτοια ώστε $Exp(G) = |G|$, τότε η ομάδα G είναι κυκλική.

of type d), με $d \mid n$, τότε η επέκταση $F < E$ είναι καθαρού τύπου n (pure of type n).

Θεώρημα 2. *Έστω ΜΚΔ$(n, expchar(F)) = 1$. Υποθέτουμε ότι το F περιέχει τις n-ρίζες της μονάδας και έστω $F \leq E$. Τα ακόλουθα είναι ισοδύναμα:*
1) Η επέκταση $F \leq E$ είναι καθαρού τύπου n (pure of type n)
2) Η επέκταση $F \leq E$ είναι κυκλική βαθμού $d \mid n$.
Σ΄αυτήν την περίπτωση, το $\alpha \in E$ είναι ρίζα του $X^n - u, u \in F$ αν και μόνο αν $Irr(\alpha, F) = X^d - \upsilon$, για κάποιο $\upsilon \in F$.

Απόδειξη. Υποθέτουμε ότι η επέκταση E/F είναι καθαρού τύπου n (pure of type n), άρα υπάρχει $\alpha \in E$ ρίζα του πολυωνύμου $X^n - u \in F[X]$. Οι ρίζες του πολυωνύμου είναι οι $\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha$, όπου ω είναι πρωταρχική n-ρίζα της μονάδας. Οπότε, η επέκταση E/F είναι πεπερασμένη επέκταση Galois. Έστω, $\sigma \in Gal(E/F) = G$. Η σ καθορίζεται πλήρως απο την δράση της στο α και η σ στέλνει ρίζες αναγώγων σε ρίζες των ίδιων αναγώγων, δηλαδή $\sigma\alpha = \omega^{k(\sigma)}\alpha$, με $k(\sigma) \in \mathbb{Z}_n$. Η απεικόνιση $\sigma \mapsto \omega^{k(\sigma)}$ είναι μια ενσωμάτωση της G στην U_n, δηλαδή η G είναι ισόμορφη με μια υποομάδα της U_n. Αλλά η ομάδα των n-ριζών της μονάδας, U_n, είναι κυκλική. Άρα, η G είναι κυκλική τάξης $d \mid n$.
Αντίστροφα, υποθέτουμε ότι η επέκταση E/F, είναι κυκλική βαθμού $d \mid n$, με ομάδα Galois $G =< \sigma >= \{id, \sigma, \ldots, \sigma^{d-1}\}$. Ψάχνουμε για ένα στοιχείο $\alpha \in E$, τέτοιο ώστε το α να είναι ρίζα του διωνύμου της μορφής $X^d - u$, με $u \in F$. Οι ρίζες οποιουδήποτε πολυωνύμου $p(X)$ είναι της μορφής $\alpha, \sigma\alpha, \ldots, \sigma^{d-1}\alpha$ και οι ρίζες του πολυωνύμου $X^d - u$ είναι της μορφής $\alpha, \omega_d\alpha, \ldots, \omega_d^{d-1}\alpha$, όπου ω_d είναι πρωταρχική d-ρίζα της μονάδας. Οπότε, αν βρούμε $\alpha \in F$ τέτοιο ώστε $\sigma\alpha = \omega_d\alpha$, τότε $Irr(\alpha, F) = \prod_{k=0}^{d-1}(X - \alpha\omega_d^k)$.
Θέτουμε $\beta := \alpha^d\omega_d^{d(d-1)/2} = \pm\alpha^d$. Αλλά το $\beta \in F$, διότι το β είναι ίσο με το γινόμενο των ριζών του $X^d - u$. Άρα, $\alpha^d \in F$ και έτσι $Irr(\alpha, F) = X^d - \alpha^d$. Δηλαδή, η επέκταση E/F είναι καθαρού τύπου n (pure of type n).
□

Θεώρημα 3. *(Θεμελιώδες Θεώρημα των Πεπερασμένων Αβελιανών Ομάδων) Έστω G πεπερασμένη, αβελιανή ομάδα. Τότε η G είναι ευθύ γινόμενο κυκλικών υποομάδων, δηλαδή $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$, για κάποιους ακεραίους n_i.*

Παρατήρηση 1. *Ισχύει ότι $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ αν και μόνο αν ο ΜΚΔ$(m, n) = 1$.*

Παράρτημα Β΄

Τριώνυμα και Θεωρία Galois

Ας θεωρήσουμε, κατ' αρχήν, τριώνυμα της μορφής

$$aX^n + bX^l + c$$

Το φθινόπωρο του 1967 ο Hans Zassenhaus παρατήρησε ότι, μέχρι τότε, ούτε ένα πολυώνυμο δεν ήταν γνωστό με ομάδα Galois υπέρ το $\mathbb{Q}$ την απλή ομάδα $PSL(3, \mathbb{F}_2)$, των αντιστρέψιμων 3×3- πινάκων με στοιχεία από το σώμα $\mathbb{F}_2$. Στα 1969 ο W. Trinks έδωσε ένα τέτοιο παράδειγμα. Πρόκειται για το πολυώνυμο

$$f(X) = X^7 - 7X + 3 \in \mathbb{Q}[X]$$

(βλ. [14])
Στα 1956, ο E.S. Selmer (βλ. [3]) απέδειξε ότι το πολυώνυμο

$$f(X) = X^n + X + 1 \in \mathbb{Q}[X]$$

για $n \not\equiv 2 \pmod 3$ είναι ανάγωγο υπέρ το $\mathbb{Q}$. Η απόδειξη είναι στοιχειώδης αλλά δύσκολη. Η ομάδα του Galois αυτού είναι η S_n, (βλ. [8]). Επίσης, στην ίδια εργασία του, ο Selmer απέδειξε ότι το $g(X) = X^n - X - 1 \in \mathbb{Q}[X]$ είναι ανάγωγο υπέρ το $\mathbb{Q}$, για κάθε $n \geq 2$.
Για την απόδειξη και των δύο παραδειγμάτων χρησιμοποιείται προχωρημένη Θεωρία Αριθμών.
Γενικά, έστω $f(X) = X^n + aX + b \in \mathbb{Z}[X]$, όπου $a = a_0c^n$ και $b = b_0c^n$. Η ομάδα Galois $Gal(f(X)/\mathbb{Q})$ ισόμορφη υπέρ το $\mathbb{Q}$ αν και μόνο αν όταν ισχύουν
1) Το $f(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$ και
2) ΜΚΔ$(a_0c(n-1), nb_0) = 1$
(βλ. [4])
Τέλος, ενδεικτικά αναφέρουμε την μεταπτυχιακή εργασία του S.C. Brown (βλ. [13]).

Παράρτημα Γ΄

Γ΄.1 Ημιευθέα Γινόμενα (Semidirect Products)

Το ημιευθύ γινόμενο (semidirect product)[βλ. [2]] δύο ομάδων Η και Κ είναι μία γενίκευση της έννοιας του ευθύ γινομένου των ομάδων Η και Κ στην οποία δεν απαιτείται και οι δύο ομάδες να είναι κανονικές. Αυτή η κατασκευή μας επιτρέπει (σε ορισμένες περιπτώσεις) να κατασκευάσουμε μια μεγαλύτερη ομάδα G, από τις Η και Κ, η οποία περιέχει υποομάδες ισόμορφες με τις Η και Κ αντίστοιχα, όπως αυτό συμβαίνει και στο ευθύ γινόμενο των δύο ομάδων. Στην περίπτωση του ημιευθέους γινομένου, η ομάδα Η θα είναι κανονική στην G, αλλά η Κ δεν είναι απαραίτητο να είναι κανονική στην G, σε αντίθεση με το ευθύ γινόμενο. Οπότε, θα μπορούμε να κατασκευάσουμε μη αβελιανές ομάδες ακόμη κι αν οι Η και Κ είναι αβελιανές. Το ημιευθύ γινόμενο αποτελεί χρήσιμο εργαλείο διότι μας επιτρέπει να μεγενθύνουμε σημαντικά το σύνολο των ομάδων που έχουμε στην διάθεση μας.

Ορισμός 2. *(Ευθύ Γινόμενο) Έστω ομάδα G και G_1, G_2 υποομάδες της G για τις οποίες ισχύει ότι $G = G_1G_2$. Η G είναι το (εσωτερικό) ευθύ γινόμενο των G_1, G_2 αν και μόνο αν οι G_1, G_2 είναι κανονικές υποομάδες της G και η τομή αυτών αποτελείται απο το μοναδιαίο στοιχείο της G.*

Ισχύει το παρακάτω θεώρημα:

Θεώρημα 4. *Έστω G ομάδα και H,K κανονικές υποομάδες της G για τις οποίες ισχύει ότι $H \cap K = e$, όπου e είναι το μοναδιαίο στοιχείο της G. Τότε, ισχύει ότι $H \times K \cong HK$, δηλαδή το εξωτερικό ευθύ γινόμενο των H και K είναι ισόμορφο με το εσωτερικό ευθύ γινόμενο των H και K.*

Σημείωση 1. *Υπάρχει αμφιμονοσήμαντη αντιστοιχία ανάμεσα στο HK*

και στο $H \times K$, η οποία δίνεται απο την $HK \to H \times K$ με $hk \mapsto (h,k)$. Οπότε, ισχύουν ότι $H \cong \{(h,1),\, h \in H\}$ και $K \cong \{(1,k),\, k \in K\}$.

Πρόταση 1. *Έστω G ομάδα και H,K υποομάδες του G. Το $HK = \{hk |\, h \in H,\, k \in K\}$ είναι υποομάδα της G αν και μόνο αν $HK = KH$.*

Πρόταση 2. *Έστω G ομάδα, H κανονική υποομάδα της G και K υποομάδα της G. Τότε η HK είναι υποομάδα της G. Αν επιπλέον και η K είναι κανονική υποομάδα της G, τότε HK είναι κανονική υποομάδα της G.*

Απόδειξη. $HK = \cup_{k\in K} Hk = \cup_{k\in K} kH = KH$, αφού Η κανονική υποομάδα της G. Οπότε, σύμφωνα με την πρόταση 1 ισχύει ότι η HK είναι υποομάδα της G.
Για να δείξουμε ότι HK είναι κανονική υποομάδα της G, αρκεί να δείξουμε ότι $g^{-1}HKg = HK$. Ορίζουμε $(HK)^g := g^{-1}HKg$. Τότε $(HK)^g = H^g K^g = HK$, αφού $^g = H$, διότι Η κανονική υποομάδα της G και $K^g = K$, διότι Κ είναι κανονική υποομάδα της G. □

Σχόλιο 1. *1) Για κάθε $\alpha \in HK$, ισχύει ότι γράφεται μοναδικά στην μορφή $\alpha = hk$, με $h \in H$, $k \in K$.*
2) Έστω $h_1k_1,\, h_2k_2 \in HK$ και $H \trianglelefteq G$, $K \leq G$ με $H \cap K = \{e\}$. Τότε,

$$(h_1k_1)(h_2k_2) = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_3k_3 \in HK \quad (\Gamma'.1)$$

αφού, $k_1h_2k_1^{-1} \in H$, διότι $H \trianglelefteq G$, δηλαδή $h_1k_1h_2k_1^{-1} := h_3 \in H$ και $k_1k_2 := k_3 \in K$.

Οι παραπάνω υπολογισμοί στο σχόλιο 1(2), στηρίζονται στο γεγονός ότι ήδη υπάρχει ομάδα G που περιέχει υποομάδες Η και Κ με $H \trianglelefteq G$ και $H \cap K = \{e\}$. Η βασική ιδέα του ημιευθέους γινομένου είναι ότι ξεκινώντας με δύο ομάδες Η και Κ να ορίσουμε μία ομάδα η οποία να περιέχει ισομορφικά αντίγραφα των Η και Κ τέτοια ώστε η τομή αυτών να είναι η τετριμμένη και ένα εκ' των δύο να είναι κανονική υποομάδα της G. Για να συμβεί αυτό, εφαρμόζουμε την εξίσωση (Γ΄.1), η οποία ορίζει τον πολλαπλασιασμό των στοιχείων της ομάδας μας κατά τέτοιο τρόπο ώστε να έχει νόημα ακόμη κι αν δεν γνωρίζουμε αν υπάρχει ομάδα που να περιέχει τις Η και Κ. Στην εξίσωση (Γ΄.1) το k_3, προκύπτει απο τον πολλαπλασιασμό στοιχείων της Κ και το h_3 προκύπτει από τον πολλαπλασιασμό του h_1 και του $k_1h_2k_1^{-1}$ στην Η. Εάν εμείς μπορούμε να καταλάβουμε που ανήκει το στοιχείο $k_1h_2k_1^{-1}$ με βάση τις Η και Κ, χωρίς αναφορά στην G, τότε η ομάδα HK θα μπορεί να περιγραφεί

εξ' ολοκλήρου απο τις Η και Κ. Μπορούμε να χρησιμοποιήσουμε αυτήν την περιγραφή για να ορίσουμε την ομάδα HK, χρησιμοποιώντας την εξίσωση(Γ΄.1) για να ορίσουμε τον πολλαπλασιασμό.

Παρατήρηση 2. *Επειδή $H \trianglelefteq G$, η ομάδα Κ δρα στην Η με συζυγία (conjugation), δηλαδή $k \cdot h = khk^{-1}$, για $k \in K$, $h \in H$.*

Οπότε, η εξίσωση (Γ΄.1), μπορεί να γραφτεί ως

$$(h_1k_1)(h_2k_2) = (h_1k_1 \cdot h_2)k_1k_2 \qquad (\Gamma'.2)$$

Η δράση της Κ στην Η με συζυγία δίνει τον ομομορφισμό

$$\varphi : K \to Aut(H)$$

Οπότε, από την εξίσωση (Γ΄.2) προκύπτει ότι ο πολλαπλασιασμός στην HK εξαρτάται μόνο απο τον πολλαπλασιασμό στην Η, απο τον πολλαπλασιασμό στην Κ και από τον ομομορφισμό φ. Δηλαδή, ο πολλαπλασιασμός στην HK ορίζεται απο τις Η και Κ.

Θεώρημα 5. *Έστω Η, Κ ομάδες και $\varphi : K \to Aut(H)$ ομομορφισμός. Ας συμβολίσουμε $\cdot$ την (αριστερή) δράση της Κ στην Η, η οποία ορίζεται απο την φ. Έστω G το σύνολο όλων των διατεταγμένων ζευγών (h, k) με $h \in H$ και $k \in K$ και ορίζουμε τον πολλαπλασιασμό στην G ως:*

$$(h_1, k_1)(h_2, k_2) = (h_1k_1 \cdot h_2, k_1k_2)$$

Τότε:
1) Αυτός ο πολλαπλασιασμός καθιστά την G μία ομάδα με τάξη $|G| = |H||K|$.
2) Τα σύνολα $\{(h, 1)|\, h \in H\}$ και $\{(1, k)|\, k \in K\}$ είναι υποομάδες της G και οι απεικονίσεις $h \mapsto (h, 1)$, με $h \in H$ και $k \mapsto (1, k)$, με $k \in K$ είναι ισομορφισμοί αυτών των υποομάδων με τις ομάδες H και K, αντιστοίχως. Δηλαδή, $H \cong \{(h, 1)|h \in H\}$ και $K \cong \{(1, k)|k \in K\}$.

Ταυτίζοντας τις Η και Κ με τα ισόμορφα αντίγραφα τους στην G που περιγράφονται στο (2), προκύπτει ότι
3) $H \trianglelefteq G$
4) $H \cap K = \{e\}$
5) Για κάθε $h \in H$ και $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Απόδειξη. 1) Είναι απλό να ελέγξουμε ότι η G είναι ομάδα με τον πολλαπλασιασμό που ορίσαμε, χρησιμοποιώντας το γεγονός ότι η $\cdot$ είναι

δράση του Κ στην Η.
$G = \{(h,k), h \in H,\ k \in K\}$ Προσεταιριστική ιδιότητα της G:
Έστω $(a,x),(b,y),(c,z) \in G$, τότε:

$$\begin{aligned}((a,x)(b,y))(c,d) &= (ax \cdot b, xy)(c,z) = (ax \cdot b(xy) \cdot c, xyz)\\ &= (ax \cdot bx \cdot (y \cdot c), xyz) = (axbx^{-1}x \cdot (y \cdot c), xyz)\\ &= (axbx^{-1}x(y \cdot c)x^{-1}, xyz) = (axbycy^{-1}x^{-1}, xyz)\\ &= (ax(by \cdot c)x^{-1}, xyz) = (ax \cdot (by \cdot c), xyz)\\ &= (a,x)(by \cdot c, yz) = (a,x)((b,y)(c,z))\end{aligned}$$

Άρα, $((a,x)(b,y))(c,d) = (a,x)((b,y)(c,z))$, για κάθε $(a,x),(b,y),(c,z) \in G$.
Ύπαρξη μοναδιαίου:
Το $(1,1)$ είναι το μοναδιαίο της G, διότι $(1,1)(a,x) = (1 \cdot a, x) = (a,x)$, για κάθε $(a,x) \in G$.
Ύπαρξη αντοστρόφου:
Έστω $(h,k),(h_1,k_1) \in G$. Τότε: $(h,k)(h_1,k_1) = (1,1) \Rightarrow (hk \cdot h_1, kk_1) = (1,1) \Rightarrow hk \cdot h_1 = 1$ και $kk_1 = 1 \Rightarrow hkh_1k^{-1} = 1$ και $k_1 = k^{-1} \Rightarrow kh_1 = h^{-1}k$ και $k_1 = k^{-1} \Rightarrow h_1 = k^{-1}h^{-1}k$ και $k_1 = k^{-1} \Rightarrow h_1 = k^{-1} \cdot h^{-1}$, και $k_1 = k^{-1}$. Άρα, $(h,k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$, για κάθε $(h,k) \in G$.
Τέλος, η G είναι κλειστή ως προς τον πολλαπλασιασμό που ορίσαμε, διότι ισχύει ότι $(h_1,k_1)(h_2,k_2) = (h_1k_1 \cdot h_2, k_1k_2) \in G$, αφού $k_1,k_2 \in K$ και $h_1k_1 \cdot h_2 \in H$.
Επομένως, η G είναι ομάδα και προφανώς ισχύει ότι $|G| = |H||K|$.
2) Έστω $\tilde{H} = \{(h,1)|h \in H\}$ και $\tilde{K} = \{(1,k)|k \in K\}$.
$\tilde{H} \leq G$. Πράγματι, αφού $(1,1) \in \tilde{H}$, αν $(a,1),(b,1) \in \tilde{H}$ τότε $(a,1)(b,1) = (a1 \cdot b, 1) = (ab,1) \in \tilde{H}$, αφού $ab \in H$ και αν $(a,1) \in \tilde{H}$, τότε $(a,1)^{-1} = (1 \cdot a^{-1}, 1) = (a^{-1},1) \in \tilde{H}$, αφού $a^{-1} \in H$.
Ακόμα, $\tilde{K} \leq G$. Πράγματι, αφού $(1,1) \in \tilde{K}$. Άν $(1,x),(1,y) \in \tilde{K}$, τότε $(1,x)(1,y) = (1x \cdot 1, xy) = (x \cdot 1, xy) = (x1x^{-1}, xy) = (1,xy) \in \tilde{K}$, αφού $xy \in K$ και αν $(1,x) \in \tilde{K}$, τοτε $(1,x)^{-1} = (x^{-1} \cdot 1, x^{-1}) = (x^{-1}1x, x^{-1}) = (1,x^{-1}) \in \tilde{K}$, αφού $x^{-1} \in K$.
Απομένει να δείξουμε ότι $H \cong \tilde{H}$ και $K \cong \tilde{K}$. Ορίζουμε $T_1 : H \to \tilde{H}$, με $h \mapsto (h,1)$. Η T_1 είναι ομομορφισμός, διότι $T_1(h_1h_2) = (h_1h_2,1) = (h_11 \cdot h_2, 1) = (h_1,1)(h_2,1) = T_1(h_1)T_1(h_2)$. Επίσης, η T_1 είναι ένα-προς-ένα. Πράγματι, $T_1(h_1) = T_2(h_2) \Rightarrow (h_1,1) = (h_2,1) \Rightarrow h_1 = h_2$. Ακόμα, η T_1 είναι επί, διότι αν $(h,1) \in \tilde{H}$, τότε $T_1(h) = (h,1)$. Οπότε, η T_1 είναι ισομορφισμός, δηλαδή $H \cong \tilde{H}$. Ανάλογα, ορίζουμε $T_2 : K \to \tilde{K}$, με $k \mapsto (1,k)$ και προκύπτει ότι η T_2 είναι ισομορφισμός, δηλαδή $K \cong \tilde{K}$.
4) Προφανώς ισχύει ότι $\tilde{H} \cap \tilde{K} = \{1\} = \{(1,1)\}$ και αφού $H \cong \tilde{H}$ και $K \cong \tilde{K}$, τότε $H \cap K = \{1\}$.

5)Έστω $(1,k) \in \tilde{K}$, $(h,1) \in \tilde{H}$. Τότε, $(1,k)(h,1)(1,k)^{-1} = ((1,k)(h,1))(k^{-1}\cdot 1, k^{-1}) = (k\cdot h, k)(k^{-1}k, k^{-1}) = (khk^{-1}, k)(1,k^{-1}) = (khk^{-1}k\cdot 1, kk^{-1}) = (khk^{-1}kk^{-1}, 1) = (khk^{-1}, 1) = (k\cdot h, 1)$, με $k\cdot h \in H$. Οπότε, ταυτίζοντας το $(1,k)$ με το k και το $(h,1)$ με το h, λόγω των ισομορφισμών που αποδείξαμε στο (2), προκύπτει ότι $khk^{-1} = k\cdot h$, με $k \in K$, $h \in H$.
3) Αποδείξαμε ότι $khk^{-1} = k\cdot h$ και ισχύει ότι $k\cdot h \in H$. Δηλαδή, $khk^{-1} \in H$. Άρα, $kHk^{-1} = H$ και έπεται ότι $k \in N_G(H)$, για κάθε $k \in K$ [1]. Οπότε, $K \leq N_G(H)$ και ισχύει ότι $H \leq N_G(H)$, άρα $HK \leq N_G(H)$. Ακόμα, ισχύει ότι $N_G(H) \leq G$ και $G = HK$, έτσι έπεται ότι $G = N_G(H)$. Επομένως, $H \trianglelefteq G$.

□

Ορισμός 3. *Έστω H,K ομάδες και $\varphi : K \to Aut(H)$ ομομορφισμός. Η ομάδα που περιγράφεται στο θεώρημα 5, ονομάζεται ημιευθύ γινόμενο (semidirect product) των H, K ως προς την φ και συμβολίζεται ως $H \rtimes_\varphi K$.*
(Αν η φ είναι προφανής τότε δεν την αναφέρουμε, δηλαδή γράφουμε $H \rtimes K$.)

Σχόλιο 2. *Ο συμβολισμός του ημιευθέους γινομένου (semidirect product) είναι έτσι ώστε να υπενθυμίζει ότι το ισομορφικό αντίγραφο της H στο $H \ltimes K$ είναι ο κανονικός παράγοντας και ότι η κατασκευή του ημιευθέους γινομένου δεν είναι συμμετρική ως προς την H και την K, σε αντίθεση με το ευθύ γινόμενο.*
Στην συνέχεια, θα διαπιστώσουμε πότε το ημιευθύ γινόμενο των H και K ταυτίζεται με το ευθύ γινόμενο τους. Ισχύει ότι το ευθύ γινόμενο είναιειδική περίπτωση του ημιευθέους γινομένου.

Πρόταση 3. *Έστω H,K ομάδες και $\varphi : K \to Aut(H)$ ένας ομομορφισμός. Τότε τα ακόλουθα είναι ισοδύναμα:*
1) Η ταυτοτική απεικόνιση μεταξύ του $H \rtimes K$ και του $H \times K$ είναι ένας ομομορφισμός ομάδων (και επομένως ισομορφισμός)
2) Η φ είναι ο τετριμμένος ομομορφισμός από το K στην $Aut(H)$.
3) $K \trianglelefteq H \rtimes K$.

Απόδειξη. (1) $\Rightarrow$ (2) Υποθέτουμε ότι η ταυτοτική απεικόνιση είναι ομομορφισμός. Απο τον ορισμό της πράξης της ομάδας στο $H \rtimes K$, έχουμε ότι

$$(h_1,k_1)(h_2,k_2) = (h_1k_1\cdot h_2, k_1k_2), \text{για κάθε} h_1,h_2 \in H \text{ και για κάθε} k_1,k_2 \in K \quad (\Gamma'.3)$$

[1] $N_G(H) = \{g \in G | H^g = H\} = \{g \in G | gHg^{-1} = H\}$

Αφού, η ταυτοτική απεικόνιση μεταξύ του $H \ltimes K$ και του $H \times K$ είναι ένας ομομορφισμός ομάδων, τότε

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2) \qquad (\Gamma'.4)$$

Εξισώνοντας τις (Γ΄.3) και (Γ΄.4) κατά συντεταγμένες έχουμε ότι $k_1 \cdot h_2 = h_2$, για κάθε $h_2 \in H$ και για κάθε $k_1 \in K$. Άρα, η Κ δρα τετριμμένα στην Η, δηλαδή $K \times H \to H$, με $(k, h) \mapsto k \cdot h = h$. Οπότε, ο φ είναι ο τετριμμένος ομομορφισμός από το Κ στην $Aut(H)$.

(2) $\Rightarrow$ (3) Υποθέτουμε ότι ο φ είναι ο τετριμμένος ομομορφισμός από το Κ στην $Aut(H)$. Τότε, η δράση της Κ στην Η είναι τετριμμένη. Οπότε, σύμφωνα με το θεώρημα 5(5), ισχύει ότι για κάθε $k \in K$ και για κάθε $h \in H$, $khk^{-1} = k \cdot h = h$, δηλαδή $khk^{-1} = h \Rightarrow kh = hk \Rightarrow k = hkh^{-1}$. Άρα, $h \in N_G(K)$, για κάθε $h \in H$. Δηλαδή, $H \leq N_G(K)$. Ακόμα, $K \leq N_G(K)$. Άρα, $HK \leq N_G(K)$, με $G = HK$ και ισχύει ότι $N_G(K) \leq G$. Οπότε, έπεται ότι $G = N_G(K)$. Επομένως, $K \trianglelefteq G$, δηλαδή $K \trianglelefteq H \rtimes K$.

(3) $\Rightarrow$ (1) Έστω ότι $K \trianglelefteq H \rtimes K$. Έχουμε ότι $[h, k] = hkh^{-1}k^{-1} \in K$, αφού $hkh^{-1} \in K$, διότι $K \trianglelefteq H \ltimes K$ αλλά και $[h, k] = hkh^{-1}k^{-1} \in H$, αφού $kh^{-1}k^{-1} \in H$, διότι $H \trianglelefteq G$. Δηλαδή, $[h, k] \in H \cap K = \{1\}$. Άρα, $[h, k] = 1 \Rightarrow hkh^{-1}k^{-1} = 1 \Rightarrow hk = kh \Rightarrow h = khk^{-1}$. Οπότε, η δράση της Κ στην Η είναι τετριμμένη και άρα ο πολλαπλασιασμός στο ημιευθύ γινόμενο ταυτίζεται με αυτόν του ευθέους γινομένου, το οποίο σημαίνει ότι $(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2) = (h_1 h_2, k_1 k_2)$, για κάθε $h_1, h_2 \in H$ και $k_1, k_2 \in K$. Αλλά, $id : H \rtimes K \to H \times K$, με $id((h_1, k_1)(h_2, k_2)) = id(h_1 h_2, k_1 k_2) = (h_1 h_2, k1k_2) = (h_1, k_1)(h_2, k_2) = id(h_1, k_1) id(h_2, k_2)$. Άρα, ο id είναι ομομορφισμός ομάδων. □

Παράδειγμα 1. *Ισχύουν ότι Η,Κ ομάδες και $\varphi : H \to Aut(H)$ ομομορφισμός και Κ δρα στο Η με $k \cdot h \in H$. Έστω $G = H \rtimes K$ και υπάρχουν $\tilde{H}, \tilde{K}$, τέτοια ώστε $H \cong \tilde{H}$ και $K \cong \tilde{K}$.*
Έστω Η αβελιανή ομάδα (μπορεί να είναι και άπειρης τάξης) και $K =< x >\cong \mathbb{Z}_2$. Ορίζουμε $\varphi : K \to Aut(H)$, με $k \mapsto f_k(h) = h^{-1}$, δηλαδή $k \cdot h = h^{-1}$, για κάθε $h \in H$. Τότε, η G περιέχει την υποομάδα Η με δείκτη 2 και $khk^{-1} = h^{-1}$, για κάθε $h \in H$.
Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση που η Η είναι κυκλική, διότι τότε αν $H = \mathbb{Z}_n$, τότε $G \cong D_{2n}$ και αν $H = \mathbb{Z}$, τότε ορίζουμε $G = D_\infty$.

Στην συνέχεια, θα αποδείξουμε ένα θεώρημα αναγνώρισης (recognition theorem) για τα ημιευθέα γινόμενα. Το θεώρημα αυτο μας βοηθάει να

διασπάσουμε ή να αναλύσουμε όλες τις ομάδες συγκεκριμένων τάξεων, με αποτέλεσμα να ταξινομήσουμε τις ομάδες με συτές τις τάξεις.

Θεώρημα 6. *Έστω G ομάδα και H,K υποομάδες της G τέτοιες ώστε* $H \trianglelefteq G$ *και* $H \cap K = \{1\}$. *Έστω* $\varphi : K \to Aut(H)$, *με* $k \mapsto f_k$, *όπου* $f_k(h) = k \cdot h = khk^{-1}$ *ομομορφισμός ομάδων. Τότε,* $HK \cong H \rtimes K$. *Ειδικότερα, αν* $G = HK$ *με* $H \trianglelefteq G$ *και* $H \cap K = \{1\}$, *τότε η G είναι το ημιευθύ γινόμενο των H,K.*

Απόδειξη. Αφού $H \trianglelefteq G$, τότε HK υποομάδα της G και ισχύει ότι κάθε στοιχείο της HK γράφεται μοναδικά στην μορφή hk, με $h \in H$ και $k \in K$.
Η απεικόνιση $T : HK \to H \rtimes K$, με $hk \mapsto (h, k)$ είναι ισομορφισμός. Πράγματι, η T είναι ομομορφισμός, διότι $T(h_1k_1h_2k_2) = T(h_1k_1h_2, k_1k_2) = (h_1k_1h_2k_2^{-1}, k_1k_2) = (h_1k_1 \cdot k_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = T(h_1k_1)T(h_2k_2)$, αφού $H \trianglelefteq G$. Επίσης, η T είναι ένα-προς-ένα, διότι $T(h_1k_1) = T(h_2k_2) \Rightarrow (h_1, k_1) = (h_2, k_2) \Rightarrow h_1 = h_2$ και $k_1 = k_2$. Δηλαδή, $h_1k_1 = h_2k_2$. Ακόμα, η T είναι επί εκ' κατασκευής, διότι αν $(h, k) \in H \rtimes K$, τότε $T(hk) = (h, k)$. Επομένως, $HK \cong H \rtimes K$. □

Ορισμός 4. *Έστω H υποομάδα της G. Μία υποομάδα K της G λέγεται συμπλήρωμα (complement) της H στην G αν ισχύει ότι* $G = HK$ *και* $H \cap K = \{1\}$.

Με την παραπάνω ορολογία, το κριτήριο για την αναγνώριση του ημιευθέους γινομένου είναι ότι πρέπει να υπάρχει ένα συμπλήρωμα για κάποια γνήσια κανομ=νική υποομάδα της G. Επιπλέον, δεν είναι κάθε ομάδα ημιευθύ γινίμενο δύο γνήσιων υποομάδων της. Χαρακτηριστικό παράδειγμα αποτελούν οι απλές ομάδες. Αλλά, η έννοια του ημιευθέους γινομένου αυξάνει σημαντικά τον κατάλογο των γνωστών μας ομάδων.

Θεώρημα 7. *Άν K είναι κανονική υποομάδα της G, τότε τα επόμενα είναι ισοδύναμα:*
i) H G είναι το ημιευθύ γινόμενο των K και G/K, δηλαδή $G = K \rtimes G/K$.
ii) Υπάχει ομομορφισμός $s : G/K \to G$, *με* $vs = 1_{G/K}$, *όπου* $v : G \to G/K$ *είναι η φυσική απεικόνιση.*

Γ΄.2 Ακριβείς Ακολουθίες (Exact Sequences)

Ορισμός 5. *Μία ακολουθία ομάδων της μορφής*

$$\cdots G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} G_{i+2} \to \cdots$$

όπου f_i είναι ομομορφισμοί ομάδων, ονομάζεται ακριβής ακολουθία αν η εικόνα κάθε ομομορφισμού είναι ίση με τον πυρήνα του επόμενου, δηλαδή $Imf_i = Kerf_{i+1}$.

Ορισμός 6. *Μικρή ακριβής ακολουθία (Short exact sequence) ονομάζεται μία ακριβής ακολουθία με την παρακάτω μορφή*

$$1 \to N \xrightarrow{f} G \xrightarrow{\varphi} Q \to 1$$

Δηλαδή, η f είναι ένα-προς ένα, η g είναι επί και $Imf = Kerg$.

Μας ενδιαφέρει η γνώση για το πότε η μικρή ακριβής ακολουθία $1 \to N \xrightarrow{f} G \xrightarrow{\varphi} Q \to 1$ διασπάται ή ισοδύναμα πότε η φ αντιλαμβάνεται την G ως ημιευθύ γινόμενο των N και $\varphi(G)$ (Αλλά η φ είναι επί, άρα $\varphi(G) = Q$).

Παρατήρηση 3. *Άν $G = H \rtimes K$, τότε η ακολουθία $1 \to H \xrightarrow{f} G = H \rtimes K \xrightarrow{\varphi} K \to 1$, με $f : h \mapsto (h, 1)$ και $\varphi : (h, k) \mapsto k$, είναι ακριβής. Άν συμβαίνει αυτό, τότε λέμε ότι η μικρή ακριβής ακολουθία διασπάται. Αλλά υπάρχουν ακριβείς ακολουθίες που η G δεν είναι το ημιευθύ γινόμενο των H,K.*

Παράρτημα Δ΄

Το αξίωμα του Bertrand

Απόσπασμα απο το βιβλίο των Ιωάννη Αντωνιάδη και Αριστείδη Κοντογεώργη "Θεωρία Αριθμών και Εφαρμογές" (Σε ηλεκτρονική μορφή, http://eclass.uoa.gr/modules/document/file.php/MATH443/workingcopy.pdf).

Αν $n > 0$, ύπάρχει πάντα πρώτος p τέτοιος ώστε $n < p \leq 2n$

Σημείωση Αν είχα $n > 1$ τότε $n < p < 2n$. Για $n = 1$, $1 < p \leq 2 \cdot 1 \Rightarrow p = 2$ χρειάζεται την ισότητα.

Παρατήρηση Συνήθως η απόδειξη είναι αναλυτικής μορφής και αποτελεί μέρος της απόδειξης του prime number theorem [?]. Εδώ θα δώσουμε μία απόδειξη περισσότερο συνδιαστική, η οποία οφείλεται στον Erdös.

Λήμμα 1. *Αν $n \geq 1$, τότε:*

1. $2^n \leq \binom{2n}{n} < 2^{2n}$.
2. $\prod_{n<p\leq 2n} p$ *διαιρεί το* $\binom{2n}{n}$.
3. *Αν $r(p)$ ο εκθέτης του p, έτσι ώστε*
$$p^{r(p)} \leq 2n < p^{(r(p)+1)}$$
τότε $\binom{2n}{n} \mid \prod_{p\leq 2n} p^{r(p)}$.
4. *Αν $n > 2$ και $\frac{2n}{3} < p \leq n$, τότε $p \nmid \binom{2n}{n}$.*
5. $\prod_{p\leq n} p < 4^n$.

Απόδειξη. 1. $2n - k \geq 2(n - k)$ για κάθε k, $0 \leq k < n$.

Επομένως $2^n \leq \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{n} = \binom{2n}{1}$. Από την άλλη μεριά, ο αριθμός $\binom{2n}{n}$ είναι ο μεγαλύτερος συντελεστής του $(1+1)^{2n}$, $\binom{2n}{n} < (1+1)^{2n} = 2^{2n}$.

2. $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Για κάθε $p \in \P$, $n < p \leq 2n$ ισχύει ότι $p \mid (2n)!$ αλλά

$$p \nmid n! \Rightarrow \prod_{n<p\leq 2n} p \mid \binom{2n}{n}.$$

3. Ο εκθέτης του p στο $n!$ είναι $\sum_{j=1}^{r(p)} \left[\frac{n}{p^j}\right]$ (θα το δούμε, στις ασκήσεις).

   Επομένως, ο εκθέτης του p στο $\binom{2n}{n}$ είναι

$$\sum_{j=1}^{r(p)} \left\{ \left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] \right\} \leq \sum_{j=1}^{r(p)} 1 = r(p)$$

   Εδώ χρησιμοποιούμε την ιδιότητα

$$[x] + [y] \leq [x+y]$$

$$2\left[\frac{n}{p^j}\right] = \left[\frac{n}{p^j}\right] + \left[\frac{n}{p^j}\right] \leq \left[\frac{2n}{p^j}\right]$$

   και

$$\left\{ \left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] \right\} = 0 \text{ ή } 1$$

   και συνεπώς

$$\prod_{p\leq 2n} p^{r(p)} \geq \binom{2n}{n}.$$

4. Αν $\frac{2n}{3} < p \leq n$ τότε το p εμφανίζεται μια φορά στην παραγοντοποίηση του $n!$ και δύο φορές, αφού $3p > 2n$, στην παραγοντοποίηση του $(2n)!$. Επομένως, αφού $n > 2$ και $p > 2$, ισχύει

$$\frac{2n}{3} < p \Rightarrow p \nmid \binom{2n}{n}.$$

5. Έστω $P(n)$ η προς απόδειξη πρόταση

   $P(1)$ $\quad 0 \leq 4^1$, ισχύει

   $P(2)$ $\quad 2 < 4^2$, ισχύει

   $P(3)$ $\quad 3 < 4^3$, ισχύει

   Τώρα, αν $m > 1$, Τότε $P(2m-1) \Rightarrow P(2m)$. Πράγματι,

$$\prod_{p\leq 2m} p = \prod_{p\leq 2m-1} p < 4^{2m-1} < 4^{2m}.$$

Επομένως, μπορούμε να υποθέσουμε ότι $n = 2m + 1$, όπου $m \geq 2$. Για κάθε $p \in \P$, $m + 2 \leqq p \leq 2m + 1$, έχουμε $p \mid \binom{2m+1}{m}$. Αν λοιπόν υποθέσουμε ότι η $P(m + 1)$ ισχύει, τότε:

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}.$$

Αλλά $\binom{2m+1}{m}$ είναι ο (κεντρικός) συντελεστής του αναπτύγματος $(1 + 1)^{2m+1}$ οπότε

$$\binom{2m+1}{m} < \frac{1}{2}(1+1)^{2m+1} = 4^m.$$

Συνεπώς αποδείξαμε ότι $P(m + 1) \Rightarrow P(2m + 1)$. Χρησιμοποιώντας την αλήθεια της πρότασης για $1, 2, 3$ και την αλήθεια των συνεπαγωγών $P(2m - 1) \Rightarrow P(2m)$ και $P(m + 1) \Rightarrow P(2m + 1)$ διαπιστώνουμε την αλήθεια της πρότασης για κάθε φυσικό αριθμό.

□

Απόδειξη. (του αξιώματος του Bertrand). Το αξίωμα ισχύει για $n \leq 3$ αφού για $n = 1$, $1 < 2 \leq 2$, και για $n = 2$, $2 < 3 \leq 4$, για $n = 3$, $3 < 5 \leq 6$.

Θα υποθέσουμε ότι είναι λάθος για $n > 3$ και θα καταλήξουμε σε άτοπο.

Από το (4) του λήμματος 1 όλοι οι πρώτοι παράγοντες p του $\binom{2n}{n}$ επαληθεύουν την ανισότητα

$$p \leq \frac{2n}{3}.$$

Έστω $s(p)$ η πιο μεγάλη δύναμη του p η οποία διαιρεί το $\binom{2n}{n}$. Από το (3) του λήμματος 1 έχουμε:

$$p^{s(p)} \mid \binom{2n}{n} \mid \prod_{p \leq 2n} p^{r(p)} \Rightarrow s(p) \leq r(p)$$

και καταλλήγουμε στην ανισότητα

$$p^{s(p)} \leq p^{r(p)} \leq 2n. \tag{Δ′.1}$$

Επομένως, αν $s(p) > 1$ τότε $p \leq \sqrt{2n}$. Συνεπώς δεν υπάρχουν περισσότεροι από $[\sqrt{2n}]$ πρώτοι διαιρέτες του $\binom{2n}{n}$ με εκθέτη > 1. Αυτό έχει ως συνέπεια λόγω της (Δ′.1) ότι

$$\binom{2n}{n} \leq (2n)^{[\sqrt{2n}]} \prod_{p \leq \frac{2n}{3}} p. \tag{Δ′.2}$$

Όμως

$$\binom{2n}{n} > \frac{4^n}{2n+1}, \tag{Δ΄.3}$$

(Εδώ $\binom{2n}{n}$ είναι ο μεγαλύτερος συντελεστής του $(1+1)^{2n} = 4^n$, το οποίο ανάπτυγμα έχει $(2n+1)$- όρους). Από τις εξισώσεις (Δ΄.2), (Δ΄.3) και το (5) του λήμματος 1 έχουμε:

$$\frac{4^n}{2n+1} < (2n)^{[\sqrt{2n}]} \prod_{p \le \frac{2n}{3}} p < 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{2n}}.$$

Προφανώς $2n+1 < (2n)^2$, οπότε απλοποιώντας με $4^{2n/3}$ έχουμε

$$4^{n/3} < (2n)^{2+\sqrt{2n}}.$$

Λογαριθμίζουμε, $\frac{n \ln 4}{3} < (2+\sqrt{2n}) \ln 2n$ Αυτό όμως δεν ισχύει για μεγάλα n.

Για παράδειγμα για $n = 750$ έχουμε (χρησιμοποιούμε τις ανισότητες $1,\ 3 < \ln 4$ και $\ln 1500 < 7.5$

$$325 = \frac{750 \cdot 1.3}{3} < (2 + \sqrt{1500}) \ln 1500 < 41 \cdot 7.5 < 308, \text{ άτοπο}$$

Συνεπώς το αξίωμα ισχύει για $n \ge 750$. Για $n < 750$ ισχύει επίσης, αφού οι πρώτοι $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 751$ είναι, κάθε φορά, ο καθένας τους <2 φορές του προηγούμενου του. □

Παράρτημα Ε΄

Ε΄.1 Το πολύγωνο του Νεύτωνα (Newton)

Ο Νεύτωνας ανέπτυξε μία μέθοδο προσέγγισης της πραγματικής λύσης μιας εξίσωσης, $f(X) = c$ (π.χ. Thomas και Finney, Απειροστικός Λογισμός, σελίδες 200-204). Την ιδέα αυτή εκμεταλευτήκαμε και στην θεωρία των τοπικών σωμάτων και έτσι δημιουργήθηκε η έννοια του πολυγώνου του Νεύτωνα.

Έστω K ένα σώμα. Θα λέμε ότι το σώμα αυτό είναι εφοδιασμένο με μία (μη-αρχιμήδεια) εκτίμηση V, όταν η V είναι μία συνάρτηση $V : K^* \to \mathbb{R}$ τέτοια ώστε $V(ab) = V(a) + V(b)$ και $V(a + b) \geq min\{V(a), V(b)\}$.

Σημείωση 2. *Συχνά στον ορισμό η εκτίμηση* $V : K \to \mathbb{R} \cup \{\infty\}$ *και ισχύει επιπλέον ότι* $V(X) = 0 \Leftrightarrow X = 0$.

Μία εκτίμηση επάγει μία μετρική στο σώμα K, $d(a, b) = exp(-V(a - b))$. Οπότε, μπορούμε να αναφερθούμε στην πλήρωση του K ως προς αυτήν την μετρική.

Παράδειγμα 2. *Αν* $K = \mathbb{Q}$ *και* $V = V_p = ord_p$ *η* p*-αδική εκτίμηση του* $\mathbb{Q}$*, τότε η πλήρωση του* $\mathbb{Q}$ *ως προς την εν λόγω εκτίμηση είναι το σώμα των* p*-αδικών αριθμών,* $\mathbb{Q}_p$.

Έστω τώρα K σώμα, πλήρες ως προς κάποια εκτίμηση V. Υποθέτουμε ότι L/K είναι μία πεπερασμένη επέκταση του K. Υπάρχει μοναδική εκτίμηση $W : L^* \to \mathbb{R}$ του σώματος L η οποία αποτελεί επέκταση αυτής του σώματος K και ορίζεται ως εξής:
Άν $\alpha \in L^*$, τότε

$$W(\alpha) := \frac{1}{[L : K]} V(N_{L/K}(\alpha))$$

όπου $N_{L/K}(\alpha)$ είναι η norm του στοιχείου α.
Μάλιστα και το σώμα L είναι πλήρες ως προς την εκτίμηση αυτή.

Έστω τώρα ένα πολυώνυμο $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, $a_0a_n \neq 0$, όπου το σώμα K είναι ένα σώμα πλήρες ως προς κάποια εκτίμηση V αυτού. Η θεωρία του πολυγώνου Newton μας εκφράζει τις τιμές $V(\alpha)$ των ριζών του $f(X)$ σε μία αλγεβρική θήκη $\bar{K}$, του K, συναρτήσει των τιμών $V(a_i)$, των συντελεστών του $f(X)$.
Θεωρούμε τα σημεία $(i, V(a_i))$ του πραγματικού επιπέδου. Αν κάποιο $a_i = 0$, τότε $V(0) = +\infty$. Τα σημεία αυτά παραλείπονται.
Το πολύγωνο του Newton του πολυωνύμου $f(X)$ ορίζεται ως η αποκάτω κυρτή θήκη (lower convex hall) του συνόλου των σημείων

$$\{(0, V(a_0)), (1, V(a_1)), \ldots, (n, V(a_n))\}$$

Ας συμβολίσουμε $(x_0, y_0), (x_1, y_1), \ldots, (x_k, y_k)$ τις διαδοχικές κορυφές του πολυγώνου Newton και με $m_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}}$, για $i = 1, 2, \ldots, k$ την κλίση του i-στού ευθυγράμμου τμήματος.
Το θεώρημα του πολυγώνου του Newton μας εξασφαλίζει ότι υπάρχουν ακριβώς $x_i - x_{i-1}$ ρίζες του πολυωνύμου $f(X)$ στο $\bar{K}$, οι οποίες έχουν την ίδια εκτίμηση $-m_i$, για $i = 1, 2, \ldots, k$ (Απόδειξη: βλ [9], σελίδες 150).
Άμεσο συμπέρασμα του θεωρήματος είναι ότι $f(X) = a_n \prod_{j=1}^{k} f_j(X)$, όπου

$$f_j(X) := \prod_{W(\alpha_i) = m_j} (X - \alpha_i) \in K[X].$$

Ε΄.2 Σύντομη αναφορά στην θεωρία διακλαδώσεων

Έστω K σώμα πλήρες ως προς μία εκτίμηση V και L πεπερασμένη επέκταση αυτού, βαθμού $n = [L : K]$. Όπως προαναφέρθηκε ήδη υπάρχει μονοσήμαντα ορισμένη εκτίμηση W του L η οποία επεκτείνει την V και μάλιστα το σώμα L είναι πλήρες ως προς την εκτίμηση αυτή. Ισχύει $V(K^*) \leq W(L^*)$. Αν τώρα συμβολίσουμε με $\mathcal{K}$ και $\mathcal{L}$ τα αντίστοιχα σώματα πηλίκων (Εδώ έχουμε τον δακτύλιο εκτίμησης modulo το αντίστοιχο μοναδικό πρώτο ιδεώδες), τότε $\mathcal{K} \subseteq \mathcal{L}$.

Ορισμός 7. *Ο δείκτης $e = e(W/V) := [W(L^*) : V(K^*)]$ λέγεται δείκτης διακλαδώσεως της επέκτασης L/K.*
Ο βαθμός $f = f(W/V) := [\mathcal{L} : \mathcal{K}]$ της επέκτασης $\mathcal{L}/\mathcal{K}$ θα λέγεται βαθμός αδρανείας της επέκτασης L/K.

Τώρα υποθέτουμε ότι επιπλέον η εκτίμηση V του σώματος K είναι διακεκριμένη, δηλαδή υπάρχει ένας ελάχιστος φυσικός αριθμός s τέτοιος ώστε $V(K^*) = s\mathbb{Z}$ τότε ισχύει ότι $n = [L : K] = ef$.

Επίσης, αν $\tilde{\mathcal{O}}$, P, π και $\mathcal{O}$, Q, Π, ο δακτύλιος εκτίμησης, το maximal ιδεώδες και ένα πρώτο στοιχείο των σωμάτων $\mathcal{K}$ και $\mathcal{L}$ αντίστοιχα, τότε

$$e := [W(\Pi)\mathbb{Z} : V(\pi)\mathbb{Z}]$$

$$\pi = \varepsilon\Pi^e, \text{ όπου } \varepsilon \in \mathcal{O}^*$$

$$\text{και } P = Q^e$$

Θεώρημα 8. *Έστω K ένα σώμα πλήρες ως προς την διακριτή εκτίμηση V. Αν α είναι ρίζα ενός πολυωνύμου $f(X) \in K[X]$ και $V(\alpha) = \frac{a}{n}$, με ΜΚΔ$(a, n) = 1$, τότε η επέκταση $K(\alpha)/K$ έχει δείκτη διακλαδώσεως e διαιρετό από το n. Συνεπώς και $n \mid [K(\alpha) : K] = ef$.*

Απόδειξη. Αφού $\pi = \varepsilon\Pi^e$, έπεται $eW(\Pi) = V(\pi) = 1 \Rightarrow W(\Pi) = \frac{1}{e}$. Το α διαφέρει από κάποια δύναμη του Π κατά μία μονάδα ($\alpha = \varepsilon_1 \cdot \Pi^t$). Επομένως, $W(\alpha) = tW(\Pi)$, δηλαδή

$$\frac{a}{n} \in \frac{1}{e}\mathbb{Z} \Rightarrow \frac{a}{n} = \frac{1}{e}\beta \text{ με } \beta \in \mathbb{Z}$$

$$\Rightarrow ea = n\beta \in n\mathbb{Z} \Rightarrow n \mid ea$$

Όμως, ΜΚΔ$(a, n) = 1$. Επομένως, το n διαιρεί το e και επειδή $[K(\alpha) : K] = ef$ έπεται ότι $n \mid [K(\alpha) : K]$. □

Βιβλιογραφία

[1] Coleman, R. On the Galois groups of the exponential Taylor polynomials. *Enseign.Math*, 33(2):183–189, (1987).

[2] Richard M. Foote David S. Dummit. *Abstract Algebra*. John Wiley and Sons, Inc.

[3] E. Selmer. On the irreducibility of certain trinomials. *Math Scand 4*, pages 287–302, 1956.

[4] H. Osada. The Galois Groups of the Polynomials $X^n + aX^l + b$. *Journal of Number Theory*, pages 230–238, 1987.

[5] Marshall Hall. *Theory of Groups*. Macmillan.

[6] G. Karpilovsky. *Topics in Field Theory*. North - Holland.

[7] Patrick Morandi. *Field and Galois Theory*. Springer.

[8] M. Ram Murty. *Introduction to p-adic Analytic Number Theory*.

[9] Jurgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992.

[10] Paulo Vianna and Paula Murgel Veloso. Galois Theory of Reciprocal Polynomials. *The Mathematical Association of A merica*, pages 466–471.

[11] Richards, I. An application of Galois theory to elementary arithmetic. *Advances in Mathematics*, 13:268–273, (1974).

[12] Steven Roman. *Field Theory*. Springer-Verlag.

[13] S. C. Brown. On the Galois Groups of Sextic Trinomials . *University of British Columbia*, 2011.

[14] Wolfgang Trinks. *Arithmetisch ähnliche Zahlkörper*. Diplomarbeit, Karlsruhe, 1964.