Θεωρία Galois

Β. Μεταφτσής και Μ. Μπομπολάκης

Σημειώσεις Παραδόσεων
Μέρος Δεύτερο
Έκδοση 1.73205080756

Περιεχόμενα

8 Κανονικές Επεκτάσεις

ΟΡΙΣΜΟΣ 8.1. Έστω $L : K$ να είναι μια επέκταση σώματος. Η επέκταση $L : K$ θα λέγεται κανονική αν κάθε ανάγωγο πολυώνυμο επί του K που έχει μια ρίζα στο L, διασπάται στο L.

ΠΑΡΑΤΗΡΗΣΗ 8.1. Μια επέκταση $L : K$ είναι κανονική αν και μόνο αν για κάθε $\alpha \in L$ το ελάχιστο πολυώνυμο του α επί του K διασπάται στο L.

ΠΑΡΑΔΕΙΓΜΑ 8.1.

1. Οι επεκτάσεις $\mathbb{C} : \mathbb{R}$ και $\mathbb{C} : \mathbb{Q}$ είναι κανονικές καθώς από το Θεμελιώδες Θεώρημα της Άλγεβρας, κάθε πολυώνυμο διασπάται στο $\mathbb{C}$.

2. Η επέκταση $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ δεν είναι κανονική επέκταση καθώς το πολυώνυμο

$$f(x) = x^3 - 2$$

επί του $\mathbb{Q}$, έχει ρίζες τις $\sqrt[3]{2}$, $\sqrt[3]{2}\, e^{2\pi i/3}$, $\sqrt[3]{2}\, e^{4\pi i/3}$, από τις οποίες μόνο η $\sqrt[3]{2}$ ανήκει στο $\mathbb{Q}(\sqrt[3]{2})$, ενώ οι άλλες όχι.

ΘΕΩΡΗΜΑ 8.1. Μια επέκταση $L : K$ είναι κανονική και πεπερασμένη αν και μόνο αν το L είναι σώμα διάσπασης για κάποιο πολυώνυμο $f \in K[x]$.

Απόδειξη. ($\Longrightarrow$) Υποθέτουμε ότι η επέκταση $L : K$ είναι κανονική και πεπερασμένη. Από το Πόρισμα 5.2 θα έχουμε ότι υπάρχουν $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, αλγεβρικά επί του K ώστε $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Έστω $m_1, m_2, \ldots, m_n$ τα ελάχιστα πολυώνυμα των $\alpha_1, \alpha_2, \ldots, \alpha_n$ επί του K αντίστοιχα και έστω

$$f = m_1 m_2 \cdots m_n.$$

Καθένα από τα m_i είναι ανάγωγο επί του K και έχει μια ρίζα $\alpha_i \in L$. Επειδή η επέκταση $L : K$ είναι κανονική κάθε m_i διασπάται επί του L. Άρα το f διασπάται επί του L. Επειδή το L παράγεται από το K και τις ρίζες του f, θα είναι το σώμα διάσπασης του f.
($\Longleftarrow$) Τώρα υποθέτουμε ότι το L είναι το σώμα διάσπασης κάποιου πολυώνυμου f επί του K. Η επέκταση $L : K$ είναι πεπερασμένη καθώς προκύπτει από το K με τη προσθήκη των ριζών του f. Δηλαδή $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, όπου $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι οι ρίζες του f. Άρα τα $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι αλγεβρικά επί του K, συνεπώς από το Πόρισμα 5.2 η επέκταση $L : K$ είναι πεπερασμένη. Μένει να δείξουμε ότι η επέκταση $L : K$ είναι κανονική. Για να το κάνουμε αυτό θα πάρουμε ένα ανάγωγο πολυώνυμο g επί του K το οποίο έχει μια ρίζα στο L και θα δείξουμε ότι το g διασπάται στο L. Έστω M να είναι το σώμα διάσπασης του fg. Φανερά $L \subseteq M$ και τα f, g διασπώνται στο M. Έστω ϱ_1, ϱ_2 να είναι να είναι ρίζες του g επί του M. Το πολυώνυμο f διασπάται επί των $L(\varrho_1)$ και $L(\varrho_2)$. Επιπλέον, αν το f διασπάται επί ενός άλλου υποσώματος του M που περιέχει το $K(\varrho_1)$ τότε το υπόσωμα αυτό πρέπει να περιέχει και το L εφόσον το L είναι το σώμα διάσπασης του f επί του K και άρα θα πρέπει να περιέχει και το $L(\varrho_1)$. Άρα το $L(\varrho_1)$ είναι το σώμα διάσπασης του f επί του $K(\varrho_1)$. Όμοια, το $L(\varrho_2)$ είναι το σώμα διάσπασης του f επί του $K(\varrho_2)$.

Ισχυριζόμαστε ότι

$$[L(\varrho_1) : L] = [L(\varrho_2) : L].$$

Θεωρούμε την απεικόνιση $\sigma : K(\varrho_1) \longrightarrow K(\varrho_2)$ με

$$\sigma(k) = k \quad \forall k \in K \quad \text{και} \quad \sigma(\varrho_1) = \varrho_2.$$

Αρχικά θα δείξουμε ότι η σ είναι καλά ορισμένη. Έστω $h_1, h_2 \in K(\varrho_1)$ με $h_1(\varrho_1) = h_2(\varrho_1)$. Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο βρίσκουμε τον μέγιστο κοινό διαιρέτη του g και του $h_1 - h_2$, έστω ότι είναι το πολυώνυμο r. Τότε θα έχουμε ότι

$$q_1 g + q_2(h_1 - h_2) = r$$

άρα

$$r(\varrho_1) = q_1(\varrho_1)g(\varrho_1) + q_2(\varrho_1)(h_1 - h_2)(\varrho_1) = 0.$$

Αφού λοιπόν το πολυώνυμο r έχει ρίζα το ϱ_1, το r δεν μπορεί να είναι σταθερό πολυώνυμο, δηλαδή $\deg(r) > 0$. Τώρα όμως έχουμε ότι ένα μη σταθερό πολυώνυμο, διαιρεί το ανάγωγο πολυώνυμο g, το οποίο μπορεί να συμβαίνει μόνο αν το r είναι της μορφής cg, όπου $c \in K$. Άρα το g διαιρεί το $(h_1 - h_2)$, συνεπώς

$$h_1 - h_2 = qg,$$

άρα

$$(h_1 - h_2)(\varrho_2) = q(\varrho_2)g(\varrho_2) \Longrightarrow (h_1 - h_2)(\varrho_2) = 0 \Longrightarrow h_1(\varrho_2) = h_2(\varrho_2).$$

οπότε

$$\sigma\big(h_1(\varrho_2)\big) = \sigma\big(h_2(\varrho_2)\big).$$

Συνεπώς η απεικόνιση σ είναι καλά ορισμένη. Εύκολα βλέπει κανείς ότι η σ είναι $1-1$, επί και ότι $\sigma(x + y) = \sigma(x) + \sigma(y)$. Έτσι μας μένει μόνο να δείξουμε ότι $\sigma(xy) = \sigma(x)\sigma(y)$. Έστω $x = p_1(\varrho_1), y = p_2(\varrho_1)$ και $h(\varrho_1) = p_1(\varrho_1)p_2(\varrho_1)$. Τότε

$$(h - p_1 p_2)(\varrho_1) = 0.$$

Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο βρίσκουμε τον μέγιστο κοινό διαιρέτη του g και του $h - p_1 p_2$, έστω ότι είναι το πολυώνυμο $\hat{r}$. Τότε θα έχουμε

$$q_1 g + q_2(h - p_1 p_2) = \hat{r}$$

άρα

$$\hat{r}(\varrho_1) = q_1(\varrho_1)g(\varrho_1) + q_2(\varrho_1)(h - p_1 p_2)(\varrho_1) = 0.$$

Αφού λοιπόν το πολυώνυμο $\hat{r}$ έχει ρίζα το ϱ_1, το $\hat{r}$ δεν μπορεί να είναι σταθερό πολυώνυμο, δηλαδή $\deg(\hat{r}) > 0$. Τώρα όμως έχουμε ότι ένα μη σταθερό πολυώνυμο, διαιρεί το ανάγωγο πολυώνυμο g, το οποίο μπορεί να συμβαίνει μόνο αν το $\hat{r}$ είναι της μορφής cg, όπου $c \in K$. Άρα το g διαιρεί το $(h - p_1 p_2)$, συνεπώς

$$h - p_1 p_2 = \hat{q} g$$

άρα

$$h(\varrho_2) - p_1(\varrho_2)p_2(\varrho_2) = \hat{q}(\varrho_2)g(\varrho_2) \Longrightarrow h(\varrho_2) - p_1(\varrho_2)p_2(\varrho_2) = 0 \Longrightarrow h(\varrho_2) = p_1(\varrho_2)p_2(\varrho_2),$$

οπότε

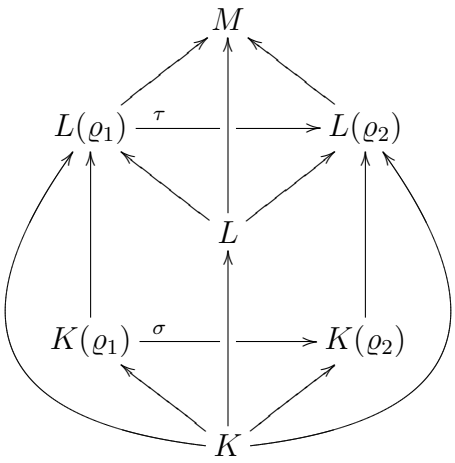
$$\sigma\big(h(\varrho_1)\big) = \sigma\big(p_1(\varrho_1)\big)\sigma\big(p_2(\varrho_1)\big).$$

Άρα ο $\sigma : K(\varrho_1) \longrightarrow K(\varrho_2)$ είναι ισομορφισμός. Επιπλέον, τα $L(\varrho_1)$ και $L(\varrho_2)$ είναι σώματα διάσπασης του f επί των $K(\varrho_1)$ Και $K(\varrho_2)$ συνεπώς από το Θεώρημα 7.3 ο σ επεκτείνεται σε ισομορφισμό $\tau : L(\varrho_1) \longrightarrow L(\varrho_2)$. Άρα οι επεκτάσεις $L(\varrho_1) : K$ και $L(\varrho_2) : K$ είναι ισομορφικές και $[L(\varrho_1) : K] = [L(\varrho_2) : K]$. Αλλά

$$[L(\varrho_1) : K] = [L(\varrho_1) : L][L : K] = [L(\varrho_2) : L][L : K] = [L(\varrho_2) : K]$$

δηλαδή $[L(\varrho_1) : L] = [L(\varrho_2) : L]$. Άρα $\varrho_1 \in L$ αν και μόνο αν $\varrho_2 \in L$. Με άλλα λόγια, αν μια ρίζα του ανάγωγου πολυωνύμου f ανήκει στο L τότε κάθε ρίζα του f ανήκει στο L και άρα η $L : K$ είναι κανονική επέκταση.

Το παρακάτω διάγραμμα δείχνει πως σχετίζονται μεταξύ τους τα υποσώματα του M.



□

8.1 Ασκήσεις

1. Δείξτε ότι τα μόνα υποσώματα του $\mathbb{Q}(i, \sqrt{5})$ είναι τα $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{5})$ και $\mathbb{Q}(i, \sqrt{5})$.

2. Προσδιορίστε τα σώματα διάσπασης επί του $\mathbb{Q}$ των πολυωνύμων $x^3 - 1$, $x^4 + 5x^2 + 6$, $x^6 - 8$.

3. Ποιες από τις παρακάτω επεκτάσεις είναι κανονικές?

   (i) $\mathbb{Q}(x) : \mathbb{Q}$.

   (ii) $\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}$.

(iii) $\mathbb{Q}(a) : \mathbb{Q}$ όπου a είναι η πραγματική έβδομη ρίζα του 5.

(iv) $\mathbb{R}(\sqrt{-7}) : \mathbb{R}$

4. Δείξτε ότι κάθε επέκταση ενός υποσώματος του $\mathbb{C}$ βαθμού 2 είναι κανονική. Ισχύει το παραπάνω για τις επεκτάσεις οποιουδήποτε βαθμού?

5. Εξηγήστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς.

(i) Κάθε πολυώνυμο επί του $\mathbb{Q}$ διασπάται σε κάποιο υπόσωμα του $\mathbb{C}$.

(ii) Τα σώματα διάσπασης στο $\mathbb{C}$ είναι μοναδικά.

(iii) Κάθε πεπερασμένη επέκταση είναι κανονική.

(iv) Η $\mathbb{Q}(\sqrt{19}) : \mathbb{Q}$ είναι κανονική επέκταση.

(v) Η $\mathbb{Q}(\sqrt[4]{19}) : \mathbb{Q}$ είναι κανονική επέκταση.

(vi) Η $\mathbb{Q}(\sqrt[4]{19}) : \mathbb{Q}(\sqrt{19})$ είναι κανονική επέκταση.

(vii) Κάθε κανονική επέκταση μιας κανονικής επέκτασης είναι κανονική επέκταση.

9 Διαχωρισιμότητα

ΟΡΙΣΜΟΣ 9.1. Έστω K σώμα και f πολυώνυμο με

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n, \quad c_i \in K.$$

Η παράγωγος Df του f ορίζεται ως

$$Df(x) = \sum_{i=1}^{n} j c_j x^{j-1}.$$

ΠΑΡΑΤΗΡΗΣΗ 9.1. Για κάθε πολυώνυμα $f, g \in K$ ισχύουν τα εξής:

- $D(f+g) = Df + Dg$
- $D(fg) = D(f)g + fD(g)$
- Αν το f είναι το σταθερό πολυώνυμο τότε $Df = 0$

Η απόδειξη των παραπάνω είναι απλή εφαρμογή του ορισμού 9.1.

ΟΡΙΣΜΟΣ 9.2. Έστω K σώμα, f πολυώνυμο επί του K και $L : K$ μια επέκταση. Ένα στοιχείο $\alpha \in L$ λέγεται πολλαπλή ρίζα του f επί του K αν το πολυώνυμο $(x-\alpha)^2$ διαιρεί το f.

ΠΡΟΤΑΣΗ 9.1. Έστω K σώμα και f πολυώνυμο επί του K. Το f έχει πολλαπλή ρίζα σε ένα σώμα διάσπασης του f επί του K αν και μόνο αν υπάρχει μη σταθερό πολυώνυμο επί του K το οποίο να διαιρεί το f και το Df στο K.
Απόδειξη. ($\Longrightarrow$) Αν το f έχει πολλαπλή ρίζα α στο σώμα διάσπασης L, τότε υπάρχει $g \in L[x]$ ώστε

$$f(x) = (x-\alpha)^2 g(x) \qquad \text{και} \qquad Df(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 Dg(x).$$

Άρα το ελάχιστο πολυώνυμο του α στο $K[x]$ διαιρεί και το f και το Df, διότι και τα δύο έχουν ρίζα το α.
($\Longleftarrow$) Έστω $f \in K[x]$ ώστε f και Df να διαιρούνται από ένα μη σταθερό πολυώνυμο $g \in K[x]$. Τότε θα υπάρχουν πολυώνυμα $q_1, q_2 \in K[x]$ ώστε

- $f(x) = q_1(x)g(x)$ και
- $Df(x) = q_2(x)g(x)$

Έστω L το σώμα διάσπασης του f επί του K, τότε και το g διασπάται στο L. Έστω $\varrho \in L$ μια ρίζα του g, τότε

$$f(\varrho) = 0 \Longrightarrow f(x) = (x-\varrho)p(x), \tag{1}$$

για κάποιο πολυώνυμο $p \in L[x]$, άρα

$$Df(x) = p(x) + (x-\varrho)Dp(x). \tag{2}$$

Όμως το g διαιρεί το Df, συνεπώς υπάρχει κάποιο $h \in L[x]$ ώστε

$$Df(x) = h(x)g(x) \Longrightarrow Df(\varrho) = h(\varrho)g(\varrho) = 0, \tag{3}$$

τώρα από τις (2) και (3) θα έχουμε ότι

$$0 = Df(\varrho) = p(\varrho),$$

άρα υπάρχει πολυώνυμο $l \in L[x]$ ώστε

$$p(x) = (x-\varrho)l(x), \tag{4}$$

έτσι από τις σχέσεις (1) και (4) θα έχουμε ότι

$$f(x) = (x-\varrho)^2 l(x),$$

συνεπώς το f έχει πολλαπλή ρίζα στο L.

□

ΟΡΙΣΜΟΣ 9.3. Ένα ανάγωγο πολυώνυμο f επί του K θα λέγεται διαχωρίσιμο επί του K αν δεν έχει πολλαπλές ρίζες στο σώμα διάσπασής του.

Αυτό σημαίνει ότι το f στο σώμα διάσπασής του γράφεται σαν γινόμενο πρωτοβάθμιων παραγόντων, δηλαδή στη μορφή

$$f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n), \text{ όπου } a_1,\ldots,a_n \text{ διακριτά.}$$

Θα δώσουμε ένα ισοδύναμο ορισμό.

ΟΡΙΣΜΟΣ 9.4. Ένα ανάγωγο πολυώνυμο f επί του K θα λέγεται διαχωρίσιμο επί του K αν όλοι οι ανάγωγοι παράγοντες του f είναι διαχωρίσιμοι στο σώμα διάσπασής του.

ΠΡΟΤΑΣΗ 9.2. Έστω K ένα σώμα. Ένα ανάγωγο πολυώνυμο $f \in K[x]$ δεν είναι διαχωρίσιμο αν και μόνο αν $Df = 0$

Απόδειξη. ($\Longrightarrow$) Έστω $f \in K[x]$ ένα ανάγωγο πολυώνυμο που δεν είναι διαχωρίσιμο. Συνεπώς το f έχει πολλαπλές ρίζες στο σώμα διάσπασής του, άρα από την Πρόταση 9.1 υπάρχει $g \in K[x]$ ώστε το g να διαιρεί το f και το Df, οπότε αφού το f είναι ανάγωγο, θα έχουμε ότι

$$g = cf \qquad \text{όπου} \qquad c \in K.$$

Όμως το cf διαιρεί το Df, οπότε και το f διαιρεί το Df. Αλλά $\deg(f) > \deg(Df)$ συνεπώς $Df = 0$.

($\Longleftarrow$) Υποθέτουμε ότι $Df = 0$ τότε το f διαιρεί και το f και το Df, έτσι από την Πρόταση 9.1 το f θα έχει πολλαπλές ρίζες στο σώμα διάσπασής του. Άρα το f δεν είναι διαχωρίσιμο. □

ΟΡΙΣΜΟΣ 9.5. Έστω $L : K$ να είναι μια επέκταση και $a \in L$ ένα αλγεβρικό στοιχείο επί του K. Θα λέμε ότι το a είναι διαχωρίσιμο επί του K αν το ελάχιστο πολυώνυμο του α επί του είναι διαχωρίσιμο επί του K.

ΟΡΙΣΜΟΣ 9.6. Μια αλγεβρική επέκταση $L : K$ θα λέγεται διαχωρίσιμη αν κάθε $a \in L$ είναι διαχωρίσιμο επί του K.

ΛΗΜΜΑ 9.1. Αν K είναι ένα σώμα χαρακτηριστικής 0, τότε κάθε f πολυώνυμο επί του K με $\deg(f) > 0$ είναι διαχωρίσιμο. Άρα και κάθε επέκταση $L : K$ είναι διαχωρίσιμη.

Απόδειξη. Το K έχει χαρακτηριστική 0, άρα

$$nx \neq 0 \qquad \forall n \in \mathbb{N}, \forall x \in K.$$

Έστω $f(x) \in K[x]$ και $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ ένας ανάγωγος παράγοντας του f επί του K με $\deg(g) > 1$. Τότε

$$Dg(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1} \neq 0.$$

Άρα από την Πρόταση 9.2 και τον ορισμό 9.4 το f είναι διαχωρίσιμο επί του K. Άρα η επέκταση είναι διαχωρίσιμη. □

10 Πεπερασμένα Σώματα

Λημμα 10.1. Έστω K ένα σώμα χαρακτηριστικής $p > 0$ (p πρώτος). Τότε η απεικόνιση $\phi : K \longrightarrow K$ με

$$\phi(x) = x^p, \qquad x \in K$$

είναι μονομορφισμός σωμάτων. Αν το K είναι πεπερασμένο τότε ο ϕ είναι αυτομορφισμός σωμάτων.

Απόδειξη. Αρχικά θα δείξουμε ότι ο ϕ είναι ομομορφισμός σωμάτων. Έστω $x, y \in K$, τότε

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y).$$

Επίσης από το διωνυμικό θεώρημα θα έχουμε ότι

$$\begin{aligned}\phi(x+y) &= (x+y)^p \\ &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p\end{aligned}$$

όμως

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(p-k+1)\ldots(p-1)p}{k!} = 1^{-1}2^{-1}\cdots k^{-1}(p-k+1)\cdots(p-1)p \equiv 0(\text{mod}p)$$

άρα

$$\begin{aligned}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p &= x^p + y^p \\ &= \phi(x) + \phi(y).\end{aligned}$$

Άρα η ϕ είναι ομομορφισμός. Τώρα θα δείξουμε ότι η ϕ είναι $1-1$. Εφόσον η ϕ είναι ομομορφισμός, ο πυρήνας $\text{Ker}(\phi)$ θα είναι ένα ιδεώδες του K. Όμως επειδή το K είναι σώμα, τα μόνα ιδεώδη που έχει είναι το τετριμμένο $\{0\}$ και ολόκληρο το K. Αλλά $\phi(1) = 1 \neq 0$, άρα $\phi \neq 0$, οπότε ο πυρήνας $\text{Ker}(\phi) \neq K$. Άρα $\text{Ker}(\phi) = \{0\}$ και συνεπώς η ϕ είναι $1-1$. Άρα η ϕ είναι ένας μονομορφισμός. Τώρα αν το K είναι πεπερασμένο, τότε κάθε μονομορφισμός $f : K \longrightarrow K$ είναι και επί, άρα ο ϕ είναι αυτομορφισμός. □

Ορισμος 10.1 (Frobenius Μονομορφισμός). Έστω K να είναι ένα σώμα χαρακτηριστικής $p > 0$. Τότε η απεικόνιση $\phi : K \longrightarrow K$ με

$$\phi(x) = x^p, \qquad x \in K$$

ονομάζεται Frobenius μονομορφισμός του K. Αν το K είναι πεπερασμένο τότε η ϕ θα λέγεται Frobenius αυτομορφισμός.

ΘΕΩΡΗΜΑ 10.1. Έστω p να είναι ένας πρώτος αριθμός και έστω $q = p^n$, όπου $n \in \mathbb{N}$. Ένα σώμα K έχει q στοιχεία αν και μόνο αν είναι το σώμα διάσπασης του πολυωνύμου $f(x) = x^q - x$ επί του $\mathbb{Z}_p$.

Απόδειξη. ($\Longrightarrow$) Έστω K να είναι ένα σώμα με q στοιχεία. Το $(K\backslash\{0\}, \cdot)$ είναι αβελιανή ομάδα τάξης $q-1$, έτσι αν $a \in K\backslash\{0\}$ τότε

$$a^{q-1} = 1 \Longrightarrow a^q = a \Longrightarrow a^q - a = 0.$$

Παρατηρήστε ότι τα a^s, $s = 0, \ldots, q-1$ είναι διακριτά. Άρα κάθε στοιχείο του K είναι ρίζα του πολυωνύμου $f(x) = x^q - x$. Καθώς το f είναι βαθμού q έχει q διακριτές ρίζες, οι οποίες είναι ακριβώς τα στοιχεία του K. Συνεπώς το σώμα διάσπασης του f είναι το K.
($\Longleftarrow$) Έστω ότι το K είναι το σώμα διάσπασης του πολυωνύμου $f(x) = x^q - x$, δηλαδή

$$K = \mathbb{Z}_p(\alpha_1, \alpha_2, \ldots, \alpha_q),$$

όπου $\alpha_1, \alpha_2, \ldots, \alpha_q$ είναι οι ρίζες του f. Άρα το K είναι πεπερασμένο. Τώρα επειδή

$$0 \neq Df(x) = qx^{q-1} - 1 \equiv -1 \pmod{q}$$

από την Πρόταση 9.2, το f είναι διαχωρίσιμο επί του K, δηλαδή όλες οι ρίζες του f είναι διακριτές, άρα το f έχει ακριβώς q ρίζες επί του K. Θεωρούμε την απεικόνιση $\phi : K \longrightarrow K$ με

$$\phi(x) = x^q.$$

Η ϕ είναι μονομορφισμός καθώς είναι πεπερασμένη σύνθεση Frobenius μονομορφισμών. Έστω $\alpha \in K$. Τότε το α είναι ρίζα του f αν και μόνο αν $\phi(\alpha) = \alpha$, άρα οι ρίζες του f ορίζουν υπόσωμα του K, το οποίο όμως είναι ίσο με το K εφόσον το K είναι σώμα διάσπασης. Άρα το K αποτελείται από τις ρίζες του f και συνεπώς $|K| = q$. □

ΠΑΡΑΤΗΡΗΣΗ 10.1. Θα δούμε ότι τα μόνα πεπερασμένα σώματα που μπορούμε να κατασκευάσουμε, είναι σώματα με p^n στοιχεία, όπου p πρώτος.

Πράγματι έστω K ένα πεπερασμένο σώμα χαρακτηριστικής p. Τότε το $\mathbb{Z}_p$ είναι υπόσωμα του K. Έστω n ο βαθμός της επέκτασης $K : \mathbb{Z}_p$ και $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ μια βάση του διανυσματικού χώρου K επί του $\mathbb{Z}_p$, όπου p πρώτος. Κάθε στοιχείο $s \in K$ γράφεται ως γραμμικός συνδυασμός των $\alpha_1, \alpha_2, \ldots, \alpha_n$, δηλαδή

$$s = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n, \qquad \text{όπου} \qquad r_1, r_2, \ldots, r_n \in \mathbb{Z}_p.$$

Άρα $|K| = p^n$.

ΟΡΙΣΜΟΣ 10.2. Ένα σώμα με p^n στοιχεία (p πρώτος) συμβολίζεται με $F(p^n)$ ή $\mathbb{F}_{p^n}$ ή $GF(p^n)$ (Galois Field) και λέγεται σώμα Galois με p^n στοιχεία.

ΛΗΜΜΑ 10.2. Έστω $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ η συνάρτηση Euler, δηλαδή

$$\varphi(n) = |\{x \in \mathbb{N} \mid 0 < x \leq n, \text{ ώστε } (x, n) = 1\}|$$

Για κάθε $n \in \mathbb{N}$ ισχύει

$$\sum_{d|n} \varphi(d) = n.$$

Απόδειξη. Θεωρώ το σύνολο $A = \{1, 2, 3, \ldots, n-1, n\}$. Αν ο d είναι διαιρέτης του n, τότε ο d διαιρεί τους

$$1d, 2d, \ldots, \Big(\frac{n}{d} - 1\Big)d, \frac{n}{d}d.$$

Έστω $\kappa \in \big\{1, 2, \ldots, \frac{n}{d} - 1, \frac{n}{d}\big\}$, τότε

$$(kd, n) = d \iff (k, n/d) = 1.$$

Άρα υπάρχουν $\phi(n/d)$ ακέραιοι στο $\{1, 2, \cdots, n/d\}$, που έχουν μέγιστο κοινό διαιρέτη με το n, d. Διαμερίζω το Α στα εξής υποσύνολα

$$\begin{aligned} A_1 &= \{x \in \mathbb{N} \mid 0 < x \leq n, (x, n) = 1\} \\ A_2 &= \{x \in \mathbb{N} \mid 0 < x \leq n, (x, n) = d_2\} \\ &\vdots \\ A_s &= \{x \in \mathbb{N} \mid 0 < x \leq n, (x, n) = d_s\} \end{aligned}$$

έτσι θα έχουμε ότι

$$\begin{aligned} |A_1| &= \phi(n) \\ |A_2| &= \phi(n/d_2) \\ &\vdots \\ |A_s| &= \phi(n/d_s) \end{aligned}$$

Τα σύνολα A_i είναι ξένα μεταξύ τους και αποτελούν διαμέριση του A, δηλαδή για κάθε $\alpha \in A$, υπάρχει $i = 1, 2, \ldots, s$ ώστε $\alpha \in A_i$. Είναι φανερό ότι

$$\sum_{i=1}^{s} |A_i| = n,$$

άρα

$$\sum_{d|n} \phi(n/d) = n$$

όμως

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

□

ΘΕΩΡΗΜΑ 10.2. Έστω G μια πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος. Τότε η G είναι κυκλική.

Απόδειξη. Έστω n να είναι η τάξη της ομάδας G και $d_1, d_2, \ldots, d_s$ να είναι όλοι οι διαιρέτες του n. Από το θεώρημα του Lagrange, έχουμε ότι η τάξη κάθε στοιχείου διαιρεί τη τάξη της ομάδας. Έτσι αν $\psi(d)$ είναι ο αριθμός των στοιχείων της G με τάξη d, τότε

$$\sum_{i=1}^{s} \psi(d_i) = n.$$

Έστω $g \in G$ ένα στοιχείο τάξης $d \in \{d_1, d_2, \ldots, d_s\}$. Τα $1, g, g^2, \ldots, g^{d-1}$ είναι διακριτά στοιχεία του G και είναι ρίζες του πολυωνύμου $x^d - 1$. Αλλά ένα πολυώνυμο βαθμού d έχει το πολύ d ρίζες και άρα κάθε στοιχείο x της G που ικανοποιεί την $x^d = 1$ είναι το g^k για μοναδικό k με $0 \leq k \leq d$.

Επιπλέον, $(k, d) = 1$ τότε το στοιχείο g^k έχει τάξη d. Αντίστροφα, αν $(d, k) = 1$ τότε το g^k έχει τάξη d. Άρα αν το $\psi(d) \neq 0$ τότε $\psi(d) = \phi(d)$ όπου $\phi(d)$ οι ακέραιοι $0 \leq k \leq< d$ με $(k, d) = 1$.

Σε κάθε περίπτωση

$$0 \leq \psi(d) \leq \phi(d).$$

Όμως

$$\sum_{i=1}^{s} \psi(d_i) = n = \sum_{i=1}^{s} \phi(d_i) \Longrightarrow \psi(d_i) = \phi(d_i) \quad \forall i = 1, 2, \ldots, s$$

άρα

$$\phi(n) = \psi(n) \geq 1$$

άρα υπάρχει στοιχείο τάξης n στην G οπότε η G είναι κυκλική. □

ΠΑΡΑΔΕΙΓΜΑ 10.1. Να κατασκευαστούν τα σώματα διάσπασης των πολυωνύμων

1. $f_1(x) = x^3 - 1 \in \mathbb{Q}[x]$,
2. $f_2(x) = x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$.

1. Το 1 είναι ρίζα του πολυωνύμου f_1, άρα θα υπάρχει πολυώνυμο $q \in \mathbb{Q}[x]$ ώστε

$$f(x) = (x - 1)q(x).$$

Ας βρούμε το πολυώνυμο q κάνοντας τη διαίρεση του f με το $(x - 1)$.

$$\begin{array}{r|l} x^3 + 0x^2 + 0x - 1 & x - 1 \\ \cline{2-2} -x^3 + x^2 & x^2 + x + 1 \\ \hline x^2 + 0x - 1 & \\ -x^2 - x + 0 & \\ \hline -x - 1 & \\ x + 1 & \\ \hline 0 & \end{array}$$

Γνωρίζουμε γενικότερα ότι $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$.
Άρα

$$f_1(x) = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Τώρα

$$x^2 + x + 1 = 0 \Longrightarrow x_{1,2} = \frac{-1 \pm i\sqrt{3}}{2}$$

Άρα

$$x^2 + x + 1 = \Big(x - \frac{-1 + i\sqrt{3}}{2}\Big)\Big(x + \frac{-1 - i\sqrt{3}}{2}\Big)$$

και έτσι

$$f_1(x) = (x-1)\Big(x - \frac{-1 + i\sqrt{3}}{2}\Big)\Big(x + \frac{-1 - i\sqrt{3}}{2}\Big)$$

Άρα το σώμα διάσπασης του f_1 είναι το

$$\mathbb{Q}\Big(\frac{-1 + i\sqrt{3}}{2}\Big) = \mathbb{Q}(i\sqrt{3}).$$

2. Θέτουμε $y = x^2$ και θα έχουμε ότι $f_2(x) = y^2 + 5y + 6$. Όμως

$$y^2 + 5y + 6 = (y+3)(y+2) = (x^2+3)(x^2+2),$$

άρα

$$f_2(x) = (x^2+3)(x^2+2) = (x - i\sqrt{3})(x + i\sqrt{3})(x - i\sqrt{2})(x + i\sqrt{2}).$$

Άρα το σώμα διάσπασης του f_2 είναι το

$$\mathbb{Q}(i\sqrt{2}, i\sqrt{3}).$$

ΠΑΡΑΔΕΙΓΜΑ 10.2. Να κατασκευαστεί το σώμα διάσπασης του $f(x) = x^3 + 2x + 1$ στο $\mathbb{Z}_3$. Εύκολα βλέπουμε ότι το f δεν έχει ρίζες στο $\mathbb{Z}_3$, άρα είναι ανάγωγο μιας και είναι βαθμού 3. Έστω $I = \langle x^3 + 2x + 1\rangle$ το ιδεώδες που παράγεται απ' το πολυώνυμο $f(x) = x^3 + 2x + 1$. Κατασκευάζουμε το σώμα

$$\mathbb{Z}_3[x]/I = \big\{c_2x^2 + c_1x + c_0 + I \mid c_0, c_1, c_2 \in \mathbb{Z}_3\big\} = \mathbb{F}_{27}.$$

Ξέρουμε ότι το πολυώνυμο f έχει μια ρίζα στο $\mathbb{F}_{27}$, την $x + I = \zeta$. Διαιρούμε το f με το $x - \zeta$

$$\begin{array}{r|l}
x^3 + 0x^2 + 2x + 1 & x - \zeta \\
\cline{2-2}
-x^3 + \zeta x^2 & x^2 + \zeta x + (2 + \zeta^2) \\
\hdashline
\zeta x^2 + 2x + 1 & \\
-\zeta x^2 + \zeta^2 x & \\
\hdashline
(2 + \zeta^2)x + 1 & \\
-(2 + \zeta^2)x + \zeta(2 + \zeta^2) & \\
\hdashline
\zeta^3 + 2\zeta + 1 = 0 &
\end{array}$$

Άρα το πολυώνυμο f γράφεται στη μορφή

$$f(x) = (x-\zeta)\big(x^2+\zeta x+(2+\zeta^2)\big)$$

Εύκολα βλέπουμε ότι το $\zeta+1$ είναι ρίζα του $x^2+\zeta x+(2+\zeta^2)$ στο $\mathbb{F}_{27}$ και τελικά έχουμε

$$x^3+2x+1 = (x-\zeta)(x-(\zeta+1))(x+(2\zeta+1))$$

οπότε το $\mathbb{F}_{27}$ είναι το σώμα διάσπασης του f. Να παρατηρήσουμε ότι στην ουσία το $\mathbb{F}_{27}$ κατασκευάστηκε προσαρτώντας στο $\mathbb{Z}_3$ μια ρίζα του πολυωνύμου f (την ζ), συνεπώς

$$\mathbb{F}_{27} = \mathbb{Z}_3(\zeta).$$

ΠΑΡΑΔΕΙΓΜΑ 10.3. Ποια από τα παρακάτω πολυώνυμα

1. $f_1(x) = x^3+1$
2. $f_2(x) = x^2+2x-1$
3. $f_3(x) = x^6+x^5+x^4+x^3+x^2+x+1$

είναι διαχωρίσιμα στο: $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$,$\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{19}$;

Από το Λήμμα 9.1 όλα τα παραπάνω πολυώνυμα είναι διαχωρίσιμα στα $\mathbb{Q}$ και $\mathbb{C}$ καθώς είναι σώματα χαρακτηριστικής 0. Θα εξετάσουμε τις παραγώγους των ανάγωγων παραγόντων των πολυωνύμων σε κάθε σώμα.

1. Το $f_1(x)$ έχει ρίζα το -1 και γράφεται σαν $(x+1)(x^2-x+1)$. Ο παράγοντας x^2-x+1 εύκολα βλέπουμε ότι στο $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ είναι ανάγωγος και $D(x^2-x+1) = 2x-1 \neq 0$ άρα το $f_1(x)$ είναι διαχωρίσιμο στα σώματα αυτά. Τι γίνεται με τα σώματα $\mathbb{Z}_7, \mathbb{Z}_{19}$;

2. Το x^2+2x-1 στο $\mathbb{Z}_2$ είναι το $x^2-1 = (x-1)^2$ και κάθε ανάγωγος παράγοντας έχει ορίζουσα 1 άρα είναι διαχωρίσιμο.

Εύκολα βλέπουμε ότι στο $\mathbb{Z}_3, \mathbb{Z}_5$ το πολυώνυμο είναι ανάγωγο και έχει $D(f_2) \neq 0$ άρα είναι διαχωρίσιμο στα σώματα αυτά. Τι γίνεται με το $\mathbb{Z}_7, \mathbb{Z}_{19}$;

3. Το $f_3(x)$ έχει ρίζα το 1 στο $\mathbb{Z}_7$ άρα δεν είναι ανάγωγο. Στην πραγματικότητα, στο $\mathbb{Z}_7$ ισχύει ότι $f_3(x) = (x+1)^7$.

ΘΕΩΡΗΜΑ 10.3 (Πρωταρχικών Στοιχείων). Κάθε πεπερασμένη και διαχωρίσιμη επέκταση σώματος είναι απλή.

Απόδειξη. Έστω $L : K$ να είναι μια πεπερασμένη και διαχωρίσιμη επέκταση σώματος.

- Αν το K είναι πεπερασμένο, τότε και το L είναι πεπερασμένο, αφού η επέκταση $L : K$ είναι πεπερασμένη. Έτσι από το Θεώρημα 10.2 η πολλαπλασιαστική ομάδα του L είναι πεπερασμένη κυκλική. Συνεπώς υπάρχει $j \in L$ ώστε

  $$\langle j \rangle = L \setminus \{0\}.$$

  Άρα $K(j) = L$.

- Αν το K είναι άπειρο.
  Έστω ότι $L = K(\alpha_1, \beta_1)$, αφού η επέκταση $L : K$ είναι πεπερασμένη από το Πόρισμα 5.2 τα α_1, β_1 είναι αλγεβρικά επί του K. Θεωρούμε f, g τα ελάχιστα πολυώνυμα επί του K, των α_1, β_1 αντίστοιχα. Υποθέτουμε ότι M είναι το σώμα διάσπασης του πολυώνυμου fg, οπότε προφανώς τα f και g διασπώνται στο M. Άρα τα f, g θα γράφονται στη μορφή

  $$f(x) = c_1(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$
  $$g(x) = c_2(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m).$$

  Επειδή η επέκταση $L : K$ είναι διαχωρίσιμη $\alpha_i \neq \alpha_j$ και $\beta_i \neq \beta_j$ για κάθε $i \neq j$. Καθώς το K είναι άπειρο μπορώ να βρω ένα $c \in K$ ώστε

  $$c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \tag{5}$$

  για κάθε $i = 1, \ldots, k$ και για κάθε $j = 2, \ldots, m$. Έστω

  $$h(x) = f(\theta - cx), \qquad \text{όπου} \quad \theta = \alpha_1 + c\beta_1$$

  ένα πολυώνυμο στο $K(\theta)$. Εύκολα βλέπουμε ότι

  $$h(\beta_1) = f(\alpha_1 + c\beta_1 - c\beta_1) = f(\alpha_1) = 0.$$

  Επίσης $h(\beta_i) \neq 0 \quad \forall i \neq 1$, διότι αν

  $$\begin{aligned} h(\beta_i) = 0 &\Longrightarrow f(\alpha_1 + c\beta_1 - c\beta_i) = 0 \\ &\Longrightarrow \alpha_1 + c(\beta_1 - \beta_i) = \alpha_r \qquad \text{για κάποιο } r \in \{1, \ldots, k\} \\ &\Longrightarrow c = \frac{\alpha_r - \alpha_1}{\beta_1 - \beta_i} \end{aligned}$$

  το οποίο είναι άτοπο από την σχέση (5).

  Άρα το β_1 είναι η μόνη κοινή ρίζα του g και του h, οπότε ο μέγιστος κοινός διαιρέτης των g, h στο $K(\theta)[x]$ είναι το $(x - \beta_1)$. Άρα $\beta_1 \in K(\theta)$ εφόσον $\alpha_1 = \theta - c\beta_1$ και $c \in K$. Άρα $L = K(\theta)$.

  Έστω τώρα $L = K(\alpha_1, \ldots, \alpha_m)$ όπου K άπειρο σώμα, $\alpha_1, \ldots, \alpha_m$ αλγεβρικά επί του K και $L : K$ διαχωρίσιμη. Για $m = 1$ δεν έχω τίποτε να δείξω και για $m = 2$ έχουμε ήδη δείξει ότι η επέκταση είναι απλή. Υποθέτουμε ότι το αποτέλεσμα ισχύει για $m-1$ και έστω $L_1 = K(\alpha_1, \ldots, \alpha_{m-1})$. Τότε η $L_1 : K$ είναι απλή και άρα υπάρχει $\beta \in L_1$ ώστε $L_1 = K(\beta)$. Άρα $L = K(\beta, \alpha_m)$ η οποία είναι επίσης διαχωρίσιμη και α_m, β αλγεβρικά επί του K. Άρα από επαγωγή η L είναι απλή.

□

ΠΑΡΑΔΕΙΓΜΑ 10.4. Η επέκταση $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}$ είναι απλή και μάλιστα

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) &= \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5}, \sqrt{7}) \\ &= \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}, \sqrt{7}) \\ &= \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7}). \end{aligned}$$

11 Ομάδα Galois

ΟΡΙΣΜΟΣ 11.1. Έστω $L : K$ μια επέκταση σωμάτων. Το σύνολο όλων των $K-$αυτομορφισμών της L αποτελεί ομάδα, ονομάζεται ομάδα Galois της επέκτασης και συμβολίζεται με $\Gamma(L : K)$. Δηλαδή

$$\Gamma(L : K) = \{\sigma : L \longrightarrow L \mid \sigma \text{ ένας } K-\text{αυτομορφισμός}\}.$$

ΠΑΡΑΔΕΙΓΜΑ 11.1. 1. Ποια η ομάδα Galois της επέκτασης $\mathbb{C} : \mathbb{R}$;

Έστω $f : \mathbb{C} \longrightarrow \mathbb{C}$ ένας $\mathbb{R}-$αυτομορφισμός. Τότε

$$\big(f(i)\big)^2 = f(i^2) = f(-1) = -1 \Longrightarrow f(i) = \pm i.$$

Άρα έχουμε δύο υποψήφιους $\mathbb{R}-$αυτομορφισμούς, τους

- $\sigma_1 : \mathbb{C} \longrightarrow \mathbb{C}$ με $\sigma_1(z) = z$ (ταυτοτικός)
- $\sigma_2 : \mathbb{C} \longrightarrow \mathbb{C}$ με $\sigma_2(z) = \overline{z}$ (συζυγής).

Ο σ_1 φανερά είναι $\mathbb{R}-$αυτομορφισμός. Ο σ_2 είναι $\mathbb{R}-$αυτομορφισμός λόγω των ιδιοτήτων της συζυγίας των μιγαδικών αριθμών

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} \qquad \text{και} \qquad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}.$$

Άρα

$$|\Gamma(\mathbb{C} : \mathbb{R})| = 2$$

και συνεπώς

$$\Gamma(\mathbb{C} : \mathbb{R}) \cong \mathbb{Z}_2.$$

2. Ποια η ομάδα Galois της επέκτασης $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$;

Έστω $f : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2})$ να είναι ένας $\mathbb{Q}-$αυτομορφισμός, τότε

$$f(\sqrt[3]{2})^3 = f\big((\sqrt[3]{2})^3\big) = f(2) = 2 \Longrightarrow f(\sqrt[3]{2}) = \sqrt[3]{2}$$

μιας και στο $\mathbb{Q}(\sqrt[3]{2})$ δεν υπάρχουν άλλες ρίζες της εξίσωσης $x^3 = 2$. Άρα ο μοναδικός αυτομορφισμός είναι ο ταυτοτικός και έτσι

$$\big|\Gamma\big(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big)\big| = 1.$$

Ο βαθμός της επέκτασης $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ είναι 3. Μπορούμε να παρατηρήσουμε ότι

$$\big|\Gamma\big(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big)\big| \leq \big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big].$$

ΛΗΜΜΑ 11.1. Αν $L : K$ είναι μια πεπερασμένη και διαχωρίσιμη επέκταση τότε

$$|\Gamma(L : K)| \leq [L : K].$$

Απόδειξη. Από το Θεώρημα 10.3, η επέκταση $L : K$ είναι απλή. Άρα υπάρχει $\alpha \in L$ ώστε $L = K(\alpha)$. Έστω $\lambda \in L$ ώστε

$$\lambda = g(\alpha),$$

για κάποιο $g \in K[x]$ και $\sigma \in \Gamma(L : K)$. Ο σ είναι K αυτομορφισμός συνεπώς

$$\sigma(\lambda) = \sigma\big(g(\alpha)\big) = g\big(\sigma(\alpha)\big).$$

Άρα η εικόνα του λ μέσω του σ προσδιορίζεται μοναδικά από το $\sigma(\alpha)$.

Έστω f το ελάχιστο πολυώνυμο του α επί του K. Τότε

$$f\big(\sigma(\alpha)\big) = \sigma\big(f(\alpha)\big) = 0,$$

άρα το $\sigma(\alpha)$ είναι ρίζα του f. Συνεπώς αν $\deg(f) = n$, έχουμε το πολύ n διαφορετικούς $K-$αυτομορφισμούς. Όμως n είναι ο βαθμός της επέκτασης $L : K$, άρα

$$|\Gamma(L : K)| \leq [L : K].$$

□

ΠΑΡΑΤΗΡΗΣΗ 11.1. Ας επισημάνουμε κάτι πολύ σημαντικό που ειπώθηκε στην παραπάνω απόδειξη.

- Έστω $K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K$ μια πεπερασμένη αλγεβρική επέκταση και $\Gamma\big(K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K\big)$ η ομάδα Galois της επέκτασης. Τότε ένας K-αυτομορφισμός σ της ομάδας Galois της $K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K$, καθορίζεται μοναδικά από τις εικόνες των στοιχείων $\alpha_1, \alpha_2, \ldots, \alpha_n$.

ΟΡΙΣΜΟΣ 11.2. Έστω L σώμα και G η ομάδα των αυτομορφισμών του L. Το σταθερό σώμα της G είναι το υπόσωμα του L,

$$\big\{\alpha \in L \mid \sigma(\alpha) = \alpha \quad \forall \sigma \in G\big\}.$$

ΠΡΟΤΑΣΗ 11.1. Έστω L σώμα, G μια πεπερασμένη υποομάδα της ομάδας αυτομορφισμών της L και K το σταθερό σώμα της G. Τότε κάθε στοιχείο $\alpha \in L$ είναι αλγεβρικό επί του K και το ελάχιστο πολυώνυμο του α επί του K είναι το

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$$

όπου α_i διακριτά με

$$\{\alpha_1, \ldots, \alpha_r\} = \{\sigma(\alpha) \mid \forall \sigma \in G\}.$$

Απόδειξη. Θεωρούμε το πολυώνυμο

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \ldots (x - \sigma_r(\alpha)).$$

Παρατηρήστε ότι το $\alpha \in \{\alpha_1, \ldots, \alpha_r\}$. Το f είναι αναλλοίωτο από τα στοιχεία της G δηλαδή

$$\sigma(f) = f, \quad \forall \sigma \in G \tag{6}$$

διότι κάθε σ θα μεταθέτει τους παράγοντες του f. Επιπλέον, το $f \in K[x]$. Πράγματι,

$$f(x) = x^r + (\sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_r(\alpha))x^{r-1} + \ldots + \sigma_1(\alpha)\ldots\sigma_r(\alpha)$$

και εύκολα βλέπω ότι οι συντελεστές του f ανήκουν στο σταθερό σώμα K. Επιπλέον, εφόσον το α είναι ρίζα του $f(x)$, το α είναι αλγεβρικό επί του K.

Τώρα για οποιαδήποτε ρίζα α_i του f υπάρχει $\sigma \in G$ ώστε $\sigma(\alpha) = \alpha_i$. Θεωρούμε $g \in K[x]$ με $g(\alpha) = 0$. Τότε

$$g(\alpha_i) = g(\sigma(\alpha)) = \sigma\big(g(\alpha)\big) = \sigma(0) = 0$$

άρα το α_i είναι και ρίζα του g για κάθε i. Συνεπώς το f διαιρεί το g, οπότε το f είναι το ελάχιστο πολυώνυμο του α επί του K. □

ΟΡΙΣΜΟΣ 11.3. Μια επέκταση σωμάτων λέγεται επέκταση Galois αν είναι πεπερασμένη, κανονική και διαχωρίσιμη.

ΘΕΩΡΗΜΑ 11.1. Έστω L σώμα, G μια πεπερασμένη υποομάδα της ομάδας αυτομορφισμών του L και K το σταθερό σώμα της G. Τότε η $L : K$ είναι επέκταση Galois. Επιπλέον

$$G = \Gamma(L : K) \qquad \text{και} \quad |G| = [L : K].$$

Απόδειξη. Από τη Πρόταση 11.1 αν $\alpha \in L$ τότε το ελάχιστο πολυώνυμο του α επί του K διασπάται στο L και δεν έχει πολλαπλές ρίζες. Άρα η επέκταση $L : K$ είναι διαχωρίσιμη και κανονική. Έστω M να είναι ένα σώμα με $K \subset M \subset L$ ώστε η επέκταση $M : K$ να είναι πεπερασμένη. Η επέκταση $M : K$ είναι διαχωρίσιμη, εφόσον η $L : K$ είναι διαχωρίσιμη. Άρα από το Θεώρημα 10.3 η επέκταση $M : K$ είναι απλή, δηλαδή υπάρχει $a \in L$ ώστε $M = K(a)$. Ξέρουμε ότι $[M : K] = \deg(f)$, όπου f είναι το ελάχιστο πολυώνυμο του a επί του K. Άρα από τη Πρόταση 11.1, για οποιοδήποτε ενδιάμεση πεπερασμένη επέκταση M το $[M : K]$ διαιρεί το $|G|$. Επιλέγουμε το ενδιάμεσο σώμα M ώστε η πεπερασμένη επέκταση $M : K$ να είναι η μέγιστη δυνατή και άρα το $[M : K]$ είναι το μέγιστο δυνατό. Αν πάρουμε ένα στοιχείο $\lambda \in L$, τότε το λ είναι αλγεβρικό επί του K, άρα η επέκταση $M(\lambda) : M$ είναι πεπερασμένη. Άρα από τον tower law, η $M(\lambda) : K$ είναι πεπερασμένη και

$$[M(\lambda) : K] = [M(\lambda) : M][M : K].$$

Μιας και το $M : K$ είναι το μέγιστο δυνατό $[M(\lambda) : K] = [M : K]$ δηλαδή $[M(\lambda) : M] = 1$ και άρα $\lambda \in M$ και $M = L$. Άρα η επέκταση $L : K$ είναι πεπερασμένη και $[L : K]$ διαιρεί το $|G|$. Επιπλέον η επέκταση $L : K$ είναι επέκταση Galois.

Τώρα επειδή $G \subseteq \Gamma(L : K)$, και $|\Gamma(L : K)| \leq [L : K]$ έχουμε ότι

$$|\Gamma(L : K)| \leq [L : K] \leq |G| \leq |\Gamma(L : K)|$$

(από το Λήμμα 11.1). Άρα $|G| = [L : K]$ και $|\Gamma(L : K)| = |G|$. □

ΠΑΡΑΤΗΡΗΣΗ 11.2. Από το προηγούμενο Θεώρημα βλέπουμε ότι αν έχουμε μια υποομάδα μιας ομάδας Galois, τότε παίρνουμε μια νέα επέκταση Galois.

ΠΑΡΑΔΕΙΓΜΑ 11.2. Έστω το σώμα $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ και G μια πεπερασμένη υποομάδα της ομάδας Galois $\Gamma(L : \mathbb{Q})$. Να βρεθούν τα σταθερά σώματα κάθε υποομάδας της ομάδας Galois.

Απόδειξη. Έστω $\sigma \in \Gamma(L : \mathbb{Q})$. Τότε

$$\begin{aligned} \big(\sigma(\sqrt{2})\big)^2 = \sigma\big(\sqrt{2}^2\big) = \sigma(2) = 2 \Longrightarrow \sigma(\sqrt{2}) = \pm\sqrt{2} \qquad \text{και} \\ \big(\sigma(\sqrt{3})\big)^2 = \sigma\big(\sqrt{3}^2\big) = \sigma(3) = 3 \Longrightarrow \sigma(\sqrt{3}) = \pm\sqrt{3}. \end{aligned}$$

Άρα

$$\Gamma(L : \mathbb{Q}) = \big\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\big\},$$

με

$$\begin{aligned} &\sigma_1(\sqrt{2}) = \sqrt{2} \qquad \text{και} \qquad \sigma_1(\sqrt{3}) = \sqrt{3}, \\ &\sigma_2(\sqrt{2}) = \sqrt{2} \qquad \text{και} \qquad \sigma_2(\sqrt{3}) = -\sqrt{3}, \\ &\sigma_3(\sqrt{2}) = -\sqrt{2} \qquad \text{και} \qquad \sigma_3(\sqrt{3}) = \sqrt{3}, \\ &\sigma_4(\sqrt{2}) = -\sqrt{2} \qquad \text{και} \qquad \sigma_4(\sqrt{3}) = -\sqrt{3}. \end{aligned}$$

Επειδή κάθε μη τετριμμένο στοιχείο της $\Gamma(L : \mathbb{Q})$ έχει τάξη 2, έχουμε ότι

$$\Gamma(L : \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Οι υποομάδες της $\Gamma(L : \mathbb{Q})$ είναι οι

1. $G_1 = \{\sigma_1, \sigma_2\}$
2. $G_2 = \{\sigma_1, \sigma_3\}$
3. $G_3 = \{\sigma_1, \sigma_4\}$.

Ξέρουμε ότι

$$\begin{aligned} L = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big) &= \big\{a_0 + a_1\sqrt{2} + (a_2 + a_3\sqrt{2})\sqrt{3} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\big\} \\ &= \big\{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\big\}. \end{aligned}$$

Άρα ένα στοιχείο x του $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ θα είναι της μορφής

$$x = a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}.$$

Οπότε

$$\begin{aligned}\sigma_4(x) &= \sigma_4(a_0+a_1\sqrt{2}+a_2\sqrt{3}+a_3\sqrt{6})\\ &= \sigma_4(a_0) + \sigma_4(a_1)\sigma_4(\sqrt{2}) + \sigma_4(a_2)\sigma_4(\sqrt{3}) + \sigma_4(a_3)\sigma_4(\sqrt{6})\\ &= a_0 + a_1\sigma_4(\sqrt{2}) + a_2\sigma_4(\sqrt{3}) + a_3\sigma_4(\sqrt{2}\sqrt{3})\\ &= a_0 - a_1\sqrt{2} - a_2\sqrt{3} + a_3(-\sqrt{2})(-\sqrt{3})\\ &= a_0 - a_1\sqrt{2} - a_2\sqrt{3} + a_3\sqrt{6}\end{aligned}$$

άρα

$$\begin{aligned}&\sigma(x) = x\\ \Longleftrightarrow &a_0 - a_1\sqrt{2} - a_2\sqrt{3} + a_3\sqrt{6} = a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}\\ \Longleftrightarrow &a_1 = a_2 = 0\end{aligned}$$

Άρα ο σ_4 κρατάει σταθερά τα σημεία της μορφής

$$x_1 = a_0 + a_3\sqrt{6}$$

και συνεπώς το σταθερό σώμα της G_3 είναι το $\mathbb{Q}(\sqrt{6})$.

Επιπλέον, επειδή

$$\sigma_2(\sqrt{6}) = \sigma_2(\sqrt{2}\sqrt{3}) = \sigma_2(\sqrt{2})\sigma_2(\sqrt{3}) = \sqrt{2}(-\sqrt{3}) = -\sqrt{6} \qquad \text{και} \qquad \sigma_2(a_0) = a_0,$$

συμπεραίνουμε ότι

$$\sigma_2(x_1) = \sigma_2(a_0 + a_3\sqrt{6}) = a_0 - a_3\sqrt{6}.$$

Άρα $\sigma_2(x_1) = x_1 \Longleftrightarrow a_3 = 0$ δηλαδή το x_1 είναι της μορφής

$$x_1 = a_0 \quad \text{με} \quad a_0 \in \mathbb{Q}.$$

Οπότε το σταθερό σώμα της $\Gamma(L:\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ είναι το $\mathbb{Q}$.

Με τον ίδιο τρόπο βλέπουμε ότι το σταθερό σώμα της G_1 είναι το $\mathbb{Q}(\sqrt{2})$ και ότι το σταθερό σώμα της G_2 είναι το $\mathbb{Q}(\sqrt{3})$.

ΘΕΩΡΗΜΑ 11.2. Έστω $L : K$ μια πεπερασμένη επέκταση και $\Gamma(L : K)$ η ομάδα Galois της επέκτασης $L : K$. Τότε η τάξη της ομάδας Galois $\Gamma(L : K)$, διαιρεί τον βαθμό της επέκτασης $L : K$. Επιπλέον $\left|\Gamma(L : K)\right| = [L : K]$ αν και μόνο αν η επέκταση $L : K$ είναι επέκταση Galois. Στην περίπτωση αυτή το K είναι το σταθερό σώμα της $\Gamma(L : K)$.

Απόδειξη. Έστω M το σταθερό σώμα της $\Gamma(L : K)$. Από το Θεώρημα 11.1 η επέκταση $L : M$, είναι επέκταση Galois και

$$\left|\Gamma(L : K)\right| = [L : M].$$

Τώρα από τον tower law έχουμε ότι

$$[L : K] = [L : M][M : K]$$

άρα η τάξη της $\Gamma(L : K)$, διαιρεί το $[L : K]$.
($\Longrightarrow$) Αν $\big|\Gamma(L : K)\big| = [L : K]$, τότε

$$[L : K] = [L : M][M : K] \Longrightarrow \big|\Gamma(L : K)\big| = \big|\Gamma(L : K)\big|[M : K] \Longrightarrow [M : K] = 1,$$

συνεπώς $M = K$. Άρα το σταθερό σώμα της $\Gamma(L : K)$ είναι το K, οπότε από το Θεώρημα 11.1 συμπεραίνουμε ότι η $L : K$ είναι επέκταση Galois.
($\Longleftarrow$) Υποθέτουμε ότι η επέκταση $L : K$ είναι επέκταση Galois. Συνεπώς η $L : K$ είναι πεπερασμένη και διαχωρίσιμη. Άρα υπάρχει $a \in L$ ώστε

$$L = K(a).$$

Έστω f το ελάχιστο πολυώνυμο του a επί του K. Το f είναι ανάγωγο στο K, διασπάται στο L και η $L : K$ είναι κανονική επέκταση. Αν $a = a_1, a_2, \ldots, a_r$ οι ρίζες του f στο L, τότε $r = \deg f$. Έστω σ ένας K-αυτομορφισμός της $\Gamma(L : K)$. Τότε

$$f\big(\sigma(a_j)\big) = \sigma\big(f(a_j)\big) = 0 \Longrightarrow \sigma(a_j) = a_i \quad \text{για κάποιο } i = 1, \ldots, r.$$

Δηλαδή, κάθε K-αυτομορφισμός της $\Gamma(L : K)$, μεταθέτει τις ρίζες του πολυωνύμου f. Θα δείξουμε ότι για κάθε a_j ρίζα του f, υπάρχει K-αυτομορφισμός $\sigma_j \in \Gamma(L : K)$ με

$$\sigma_j(a) = a_j.$$

Κάθε στοιχείο της επέκτασης $K(a) = L$ είναι της μορφής $p(a)$ για κάποιο $p \in K[x]$. Ορίζουμε την συνάρτηση $\sigma_j : L \longrightarrow L$ με $\sigma_j\big(p(a)\big) = p(a_j)$ για κάθε $p \in K[x]$. Η σ_j είναι καλά ορισμένη. Πράγματι αν $g(x), h(x) \in K[x]$ είναι πολυώνυμα επί του K με $g(a) = h(a)$, τότε το πολυώνυμο $g - h$ έχει ρίζα το a, άρα το $g - h$ διαιρείται από το ελάχιστο πολυώνυμο f του a, συνεπώς

$$g(a_j) - h(a_j) = 0 \Longrightarrow \sigma_j\big(g(a)\big) = \sigma_j\big(h(a)\big) \quad \text{για κάθε } j = 1, \ldots, r,$$

άρα η σ_j είναι καλά ορισμένη. Τώρα θα δείξουμε ότι η σ_j είναι ισομορφισμός για κάθε $j = 1, 2, \ldots, r$. Έχουμε

$$\sigma_j\big(p_1(a)+p_2(a)\big) = \sigma_j\big((p_1+p_2)(a)\big) = (p_1+p_2)(a_j) = p_1(a_j)+p_2(a_j) = \sigma_j\big(p_1(a)\big)+\sigma_j\big(p_2(a)\big)$$

και

$$\sigma_j\big(p_1(a)p_2(a)\big) = \sigma_j\big((p_1p_2)(a)\big) = (p_1p_2)(a_j) = p_1(a_j)p_2(a_j) = \sigma_j\big(p_1(a)\big)\sigma_j\big(p_2(a)\big),$$

άρα σ_j είναι ομομορφισμός.

Έστω $x \in L$. Υπάρχει $p \in K[x]$ με $p(a_j) = x$. Άρα $\sigma_j(p(a)) = p(a_j) = x$ άρα η σ_j είναι επί. Επιπλέον, αν $\sigma_j(p(a)) = \sigma_j(q(a))$ για $p, q \in K[x]$ τότε

$$\sigma_j(p(a) - q(a)) = 0 \Rightarrow \sigma_j((p-q)(a)) = 0 \Rightarrow (p-q)(a_j) = 0.$$

Άρα το f διαιρεί το $p - q$ συνεπώς $p - q(a) = 0$ δηλαδή $p(a) = q(a)$ και συνεπώς η σ_j είναι $1-1$. Φανερά η σ_j αφήνει αναλλοίωτο το K σημείο προς σημείο, δηλαδή

$$\sigma_j(k) = k \quad \text{για κάθε } k \in K.$$

Συνεπώς για κάθε j η σ_j είναι ένας K-αυτομορφισμός η μοναδικότητα του οποίου συνεπάγεται από τον ορισμό και το γεγονός ότι οι a_j είναι διακριτές.

Άρα η σ_j μεταθέτει τις ρίζες του πολυωνύμου f. Τώρα επειδή η επέκταση $L : K$ είναι διαχωρίσιμη και οι ρίζες του πολυωνύμου f είναι διακριτές, συμπεραίνουμε ότι το πλήθος των ριζών του f ισούται με το πλήθος των K-αυτομορφισμών σ_j εφόσον κάθε ρίζα προσδιορίζει μοναδικά ένα στοιχείο της ομάδας Galois. Άρα $|\Gamma(L : K)| = \deg f$. Όμως το f είναι το ελάχιστο πολυώνυμο του a επί του K και $L = K(a)$. Τελικά,

$$[L : K] = \deg f = |\Gamma(L : K)|.$$

□

ΠΡΟΤΑΣΗ 11.2. Έστω K, L, M να είναι σώματα με $K \subseteq M \subseteq L$. Αν η επέκταση $L : K$ είναι επέκταση Galois, τότε η επέκταση $L : M$ είναι επέκταση Galois. Επιπλέον αν η επέκταση $M : K$ είναι κανονική τότε η $M : K$ είναι επέκταση Galois.

Απόδειξη. Υποθέτουμε ότι η επέκταση $L : K$ είναι επέκταση Galois, άρα είναι πεπερασμένη, διαχωρίσιμη και κανονική. Από την Πρόταση 4.1 έχουμε ότι

$$[L : K] = [L : M][M : L],$$

συνεπώς αφού η $L : K$ είναι πεπερασμένη επέκταση και η $L : M$ είναι πεπερασμένη. Έστω $a \in L$ και f_K, f_M να είναι τα ελάχιστα πολυώνυμα του a επί των K και M αντίστοιχα. Επειδή η επέκταση $L : K$ είναι κανονική και διαχωρίσιμη και το $a \in L$ είναι μια ρίζα του f_K, το f_K διασπάται επί του L και όλες του ρίζες του f_K στο L είναι διακριτές, δηλαδή το f_K γράφεται στη μορφή

$$f_K(x) = (x - a_1)(x - a_2) \cdots (x - a_r),$$

με $a_1, a_2, \cdots, a_r \in L$. Τώρα έχουμε ότι $f_K(a) = 0$ και f_M είναι το ελάχιστο πολυώνυμο επί του M, άρα από το Λήμμα 5.3 το f_M διαιρεί το f_K στο M, οπότε για κάποιο πολυώνυμο $q \in M[x]$

$$f_K = q f_M.$$

Άρα το f_M διασπάται επί του L και οι ρίζες του είναι διακριτές, άρα η επέκταση $L : M$ είναι κανονική και διαχωρίσιμη και συνεπώς η επέκταση $L : M$ είναι επέκταση Galois.

Τώρα αν η επέκταση $M : K$ είναι κανονική και επειδή η επέκταση $L : K$ είναι πεπερασμένη και διαχωρίσιμη και η $M : K$ θα είναι και αυτή πεπερασμένη και διαχωρίσιμη, άρα είναι επέκταση Galois.

□

ΠΡΟΤΑΣΗ 11.3. Έστω $L : K$ μια επέκταση Galois και M σώμα με $K \subseteq M \subseteq L$. Τότε η επέκταση $M : K$ είναι κανονική αν και μόνο αν $\sigma(M) = M$, για κάθε $\sigma \in \Gamma(L : K)$.

Απόδειξη. Έστω $a \in M$ και f το ελάχιστο πολυώνυμο του a επί του K. Η επέκταση $L : K$ είναι επέκταση Galois, άρα το σταθερό σώμα της $\Gamma(L : K)$ είναι το K, άρα από την Πρόταση 11.1 το f διασπάται επί του L και οι ρίζες του f είναι ακριβώς οι $\sigma(a)$ για κάθε $\sigma \in \Gamma(L : K)$. Άρα το f διασπάται επί του M αν για κάθε $\sigma \in \Gamma(L : K)$ έχουμε ότι $\sigma(a) \in M$. Άρα η $M : K$ είναι κανονική αν και μόνο αν για κάθε $\sigma \in \Gamma(L : K)$ το $\sigma(M) \subseteq M$. Αλλά αν $\sigma(M) \subseteq M$ για κάθε $\sigma \in \Gamma(L : K)$ τότε $\sigma^{-1}(M) \subseteq M$ και $M = \sigma(\sigma^{-1}(M)) \subseteq \sigma(M)$.

Άρα $\sigma(M) = M$ για κάθε $\sigma \in \Gamma(L : K)$. Συνεπώς η επέκταση $M : K$ είναι κανονική αν και μόνο αν $\sigma(M) = M$ για κάθε $\sigma \in \Gamma(L : K)$. □

12 Αντιστοιχία Galois

ΘΕΩΡΗΜΑ 12.1 (Galois). Έστω $L : K$ μια επέκταση Galois. Τότε υπάρχει μία $1 - 1$ και επί αντιστοιχία μεταξύ των σωμάτων M με $K \subseteq M \subseteq L$ και των υποομάδων της ομάδας Galois. Πιο συγκεκριμένα

1. Αν M είναι σώμα με $K \subseteq M \subseteq L$ τότε η υποομάδα της $\Gamma(L : K)$ που αντιστοιχεί στο M είναι η $\Gamma(L : M)$.

2. Αν G είναι μια υποομάδα της $\Gamma(L : K)$ τότε το υπόσωμα του L που αντιστοιχεί στην G είναι το σταθερό σώμα της G.

3. Η επέκταση $M : K$ είναι κανονική αν και μόνο αν η $\Gamma(L : M)$ είναι κανονική υποομάδα της $\Gamma(L : K)$. Τότε $\Gamma(M : K) \cong \Gamma(L : K)/\Gamma(L : M)$.

Απόδειξη.

Έστω $\Gamma(L : K)$ ομάδα Galois της επέκτασης $L : K$ και G υποομάδα της. Αν M το σταθερό σώμα της G τότε από Θεώρημα 11.1 έχουμε $G = \Gamma(L : M)$ και $K \subseteq M \subseteq L$. Άρα σε κάθε υποομάδα της $\Gamma(L : K)$ αντιστοιχεί ένα ενδιάμεσο σώμα.

Από την άλλη, αν $K \subseteq M \subseteq L$ και $L : K$ πεπερασμένη και Galois, από την Πρόταση 11.2 η $L : M$ είναι επέκταση Galois και άρα από Θεώρημα 11.2 η $\Gamma(L : M)$ έχει σταθερό σώμα το M και εφόσον τα στοιχεία της $\Gamma(L : M)$ είναι M-αυτομορφισμοί και $K \subseteq M$ είναι και $K-$αυτομορφισμοί. Άρα η $\Gamma(L : M)$ είναι υποομάδα της $\Gamma(L : K)$. Άρα σε κάθε ενδιάμεσο σώμα αντιστοιχεί μια υποομάδα της ομάδας Galois.

Αν τώρα $K \subseteq M \subseteq L$, η επέκταση $M : K$ είναι κανονική αν και μόνο αν $\sigma(M) = M$ για κάθε $\sigma \in \Gamma(L : K)$ από την προηγούμενη Πρόταση. Όμως το M και το $\sigma(M)$ είναι τα σταθερά σώματα του $\Gamma(L : M)$ και του $\sigma\Gamma(L : M)\sigma^{-1}$. Άρα $\sigma(M) = M$ αν και μόνο αν $\Gamma(L : M) = \sigma\Gamma(L : M)\sigma^{-1}$ και υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ των υποομάδων της $\Gamma(L : K)$ και των σταθερών σωμάτων τους. Άρα η επέκταση $M : K$ είναι κανονική αν και μόνο αν η $\Gamma(L : M)$ είναι κανονική υποομάδα της $\Gamma(L : K)$.

Τέλος, ας υποθέσουμε ότι η $M : K$ είναι κανονική επέκταση. Ορίσουμε $p : \Gamma(L : K) \to \Gamma(M : K)$ με $p(\sigma) = \sigma|_M$ ο περιορισμός του σ στο M. Η p είναι ομομορφισμός ($p(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_M = \sigma_1|_M(\sigma_2|_M) = p(\sigma_1)p(\sigma_2)$) και ο

$$\text{Ker}p = \{\sigma \in \Gamma(L : K) \mid p(\sigma) = \sigma|_M = \text{id}\}$$

όπου id η ταυτοτική απεικόνιση. Άρα τα στοιχεία του πυρήνα είναι τα στοιχεία της $\Gamma(L : K)$ που σταθεροποιούν το σώμα M δηλαδή τα στοιχεία της $\Gamma(L : M)$. Αλλά αν εφαρμόσουμε το Θεώρημα 11.1 στην επέκταση $M : K$ παίρνουμε ότι $p(\Gamma(L : K)) = \Gamma(M : K)$ εφόσον το σταθερό σώμα της $p(\Gamma(L : K))$ είναι το K. Άρα από το πρώτο θεώρημα ισομορφισμών έχουμε ότι $\Gamma(M : K) \cong \Gamma(L : K)/\Gamma(L : M)$. □

ΠΑΡΑΔΕΙΓΜΑ 12.1. Έστω $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ και έστω L το σώμα διάσπασής του. Θα προσπαθήσουμε να εφαρμόσουμε την αντιστοιχία Galois στο σώμα διάσπασης του $f(x)$ και άρα να απαντήσουμε στα παρακάτω.

1. Ποιο είναι το σώμα διάσπασης L και ποιος ο βαθμός της επέκτασης $L : \mathbb{Q}$;
2. Ποια είναι η ομάδα Galois της επέκτασης $L : \mathbb{Q}$;
3. Ποιες είναι οι υποομάδες της ομάδας Galois $\Gamma(L : \mathbb{Q})$;
4. Να βρείτε το σταθερό σώμα για κάθε υποομάδα της $\Gamma(L : \mathbb{Q})$.
5. Να βρείτε ποια από τα παραπάνω ενδιάμεσα σώματα αντιστοιχούν σε κανονικές επεκτάσεις.

1. Το f διασπάται στο $\mathbb{C}$ ως εξής:

$$f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Άρα $L = \mathbb{Q}(\sqrt[4]{2}, i)$. Η επέκταση $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ είναι κανονική, απλή και διαχωρίσιμη. Από τη Πρόταση 4.1 έχουμε ότι

$$\big[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}\big] = \big[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})\big]\big[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}\big],$$

όμως η επέκταση $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})$ προκύπτει με τη προσάρτηση του i στο $\mathbb{Q}(\sqrt[4]{2})$ και επειδή το ελάχιστο πολυώνυμο του i επί του $\mathbb{Q}$ είναι το $x^2 + 1$, ο βαθμός της επέκτασης $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})$ είναι 2. Όσον αφορά την επέκταση $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$, προκύπτει με την προσάρτηση της $\sqrt[4]{2}$ στο $\mathbb{Q}$ και επειδή το ελάχιστο πολυώνυμο της $\sqrt[4]{2}$ επί του $\mathbb{Q}$ είναι το $x^4 - 2$, ο βαθμός της επέκτασης $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ είναι 4. Άρα

$$\big[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}\big] = 2 \cdot 4 = 8.$$

2. Έστω $\sigma \in \Gamma(L : \mathbb{Q})$. Είναι

$$\big(\sigma(i)\big)^2 = \sigma(i^2) = \sigma(-1) = -1 \Longrightarrow \sigma(i) = \pm i$$

$$\big(\sigma(\sqrt[4]{2})\big)^4 = \sigma(\sqrt[4]{2}^4) = \sigma(2) = 2 \Longrightarrow \sigma(\sqrt[4]{2}) = \begin{cases} \pm\sqrt[4]{2} \\ \pm i\sqrt[4]{2} \end{cases}$$

Παρατηρήστε ότι αυτό το τελευταίο δεν είναι απαραίτητο. Γνωρίζω από την θεωρία ότι οι K-αυτομορφισμοί της ομάδας Galois μεταθέτουν τις ρίζες των ελαχίστων πολυωνύμων. Επομένως είναι άμεσο ότι ένας αυτομορφισμός της ομάδας Galois μεταθέτει τις ρίζες του x^2+1 και τις ρίζες του x^4-2.

Διαλέγω δυο αυτομορφισμούς $\sigma, \tau \in \Gamma(L:\mathbb{Q})$, όπου ο ένας θα δρα στο $\sqrt[4]{2}$ αφήνοντας αναλλοίωτο το i και ο άλλος θα δρα στο i αφήνοντας αναλλοίωτο το $\sqrt[4]{2}$. Επιλέγω τους $\sigma, \tau \in \Gamma(L:\mathbb{Q})$ ως εξής

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad \sigma(i) = i$$

και

$$\tau(i) = -i, \quad \tau(\sqrt[4]{2}) = \sqrt[4]{2}.$$

Τότε

$$\sigma^2(\sqrt[4]{2}) = \sigma\big(\sigma(\sqrt[4]{2})\big) = \sigma(i\sqrt[4]{2}) = \sigma(i)\sigma(\sqrt[4]{2}) = i^2\sqrt[4]{2} = -\sqrt[4]{2}$$

$$\sigma^3(\sqrt[4]{2}) = \sigma(-\sqrt[4]{2}) = \sigma(-1)\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$$

$$\sigma^4(\sqrt[4]{2}) = \sigma(-i\sqrt[4]{2}) = \sigma(-1)\sigma(i)\sigma(\sqrt[4]{2}) = -i^2\sqrt[4]{2} = \sqrt[4]{2}.$$

Ας δούμε τις δράσεις των αυτομορφισμών επάνω στα $\sqrt[4]{2},\ i$ στο παρακάτω πίνακα.

Αυτομορφισμοί	Δράση στο $\sqrt[4]{2}$	Δράση στο i
σ	$i\sqrt[4]{2}$	i
σ^2	$-\sqrt[4]{2}$	i
σ^3	$-i\sqrt[4]{2}$	i
$\sigma^4 = 1$	$\sqrt[4]{2}$	i
τ	$\sqrt[4]{2}$	$-i$
$\sigma\tau$	$i\sqrt[4]{2}$	$-i$
$\sigma^2\tau$	$-\sqrt[4]{2}$	$-i$
$\sigma^3\tau$	$-i\sqrt[4]{2}$	$-i$

Παρατηρούμε επίσης ότι

$$\tau\sigma = \sigma^3\tau$$

$$\tau\sigma^2 = \sigma^3\tau\sigma = \sigma^6\tau = \sigma^2\tau$$

$$\tau\sigma^3 = \sigma^3\tau\sigma^2 = \sigma^6\tau\sigma = \sigma^9\tau\sigma = \sigma\tau.$$

Άρα η ομάδα Galois της επέκτασης $\mathbb{Q}(\sqrt[4]{2}, i):\mathbb{Q}$ είναι η

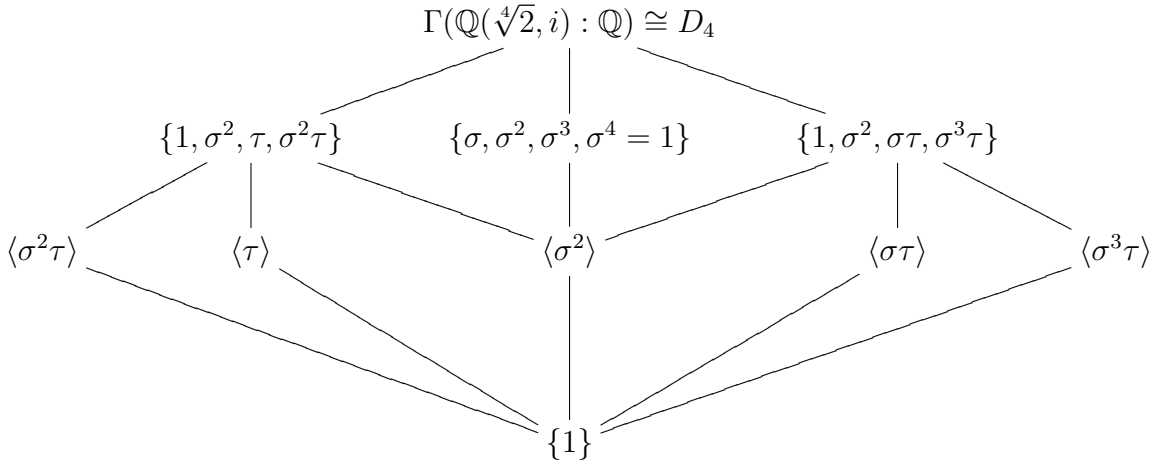
$$\Gamma(\mathbb{Q}(\sqrt[4]{2}, i):\mathbb{Q}) = \{\sigma, \sigma^2, \sigma^3, \sigma^4 = 1, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_4$$

όπου D_4 η διεδρική ομάδα με 8 στοιχεία.

3. Η υποομάδες της $\Gamma(\mathbb{Q}(\sqrt[4]{2}, i):\mathbb{Q})$ είναι οι εξής.

Υποομάδες Τάξης 4	Υποομάδες Τάξης 2
$\langle\sigma\rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4 = 1\} \cong \mathbb{Z}_4$	$\langle\sigma^2\rangle \cong \mathbb{Z}_2$
	$\langle\tau\rangle \cong \mathbb{Z}_2$
$\{1, \sigma^2, \tau, \sigma^2\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle\sigma\tau\rangle \cong \mathbb{Z}_2$
	$\langle\sigma^2\tau\rangle \cong \mathbb{Z}_2$
$\{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle\sigma^3\tau\rangle \cong \mathbb{Z}_2$

Ας δούμε το παρακάτω διάγραμμα των υποομάδων της D_4.



4.
Θέτουμε $\xi = \sqrt[4]{2}$ και έστω $x \in \mathbb{Q}(\sqrt[4]{2}, i)$ τότε το x θα είναι της μορφής

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3.$$

Αυτό γιατί μια βάση του $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i))$ είναι η $\{1, \xi, \xi^2, \xi^3\}$ και μια βάση του $\mathbb{Q}(i) : \mathbb{Q}$ είναι η $\{1, i\}$. Άρα μια βάση της $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$ είναι το γινόμενο των βάσεων (βλέπε απόδειξη του short tower law) δηλαδή η $\{1, \xi, \xi^2, \xi^3, i, i\xi, i\xi^2, i\xi^3\}$.
Παρατηρούμε επίσης ότι:

- το σταθερό σώμα της $\Gamma(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$ είναι το $\mathbb{Q}$.
- το σταθερό σώμα της $\{1\}$ είναι το $\mathbb{Q}(i, \sqrt[4]{2})$.
- το σταθερό σώμα της $\langle\sigma\rangle$ είναι το $\mathbb{Q}(i)$.
- Για το σταθερό σώμα της $\{1, \sigma^2, \tau, \sigma^2\tau\}$, βλέπουμε πως δρα ο $\mathbb{Q}$-αυτομορφισμός σ^2 στο x:

$$\begin{aligned}\sigma^2(x) &= \sigma^2(a_0) + \sigma^2(a_1\xi) + \sigma^2(a_2\xi^2) + \sigma^2(a_3\xi^3) + \sigma^2(a_4 i) + \sigma^2(a_5 i\xi) + \sigma^2(a_6 i\xi^2) + \sigma^2(a_7 i\xi^3)\\ &= a_0 + \sigma^2(a_1)\sigma^2(\xi) + \sigma^2(a_2)\big(\sigma^2(\xi)\big)^2 + \sigma^2(a_3)\big(\sigma^2(\xi)\big)^3 + \sigma^2(a_4)\sigma^2(i) +\\ &\qquad + \sigma^2(a_5)\sigma^2(i\xi) + \sigma^2(a_6)\sigma^2(i)\big(\sigma^2(\xi)\big)^2 + \sigma^2(a_7)\sigma^2(i)\big(\sigma^2(\xi)\big)^3\\ &= a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 + a_4 i - a_5 i\xi + a_6 i\xi^2 - a_7 i\xi^3\end{aligned}$$

Άρα

$$\begin{aligned}
&\sigma^2(x) = x \\
\iff & a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3 = \\
& \qquad = a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 + a_4 i - a_5 i\xi + a_6 i\xi^2 - a_7 i\xi^3 \\
\iff & a_1 = a_3 = a_5 = a_7 = 0
\end{aligned}$$

Δηλαδή ο σ^2 σταθεροποιεί το

$$x_0 = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2.$$

Τώρα θα εφαρμόσουμε τον τ στο x_0 (να επισημάνουμε ότι αναφερόμαστε σε ένα σημείο x_0 του $\mathbb{Q}(\sqrt[4]{2}, i)$ το οποίο σταθεροποιείται ήδη από τον σ^2) και έχουμε

$$\tau(x_0) = a_0 + a_2\xi^2 - a_4 i - a_6 i\xi^2,$$

άρα

$$\tau(x_0) = x_0 \iff a_4 = a_6 = 0.$$

Δηλαδή ο τ σταθεροποιεί το $x_1 = a_0 + a_2\xi^2$. Προφανώς και ο $\sigma^2\tau$ αφήνει αναλλοίωτο το $x_1 = a_0 + a_2\xi^2$, συνεπώς το σταθερό σώμα της $\{1, \sigma^2, \tau, \sigma^2\tau\}$ είναι το

$$\{a_0 + a_2\xi^2 \mid a_0, a_2 \in \mathbb{Q}\} = \mathbb{Q}(\xi^2) = \mathbb{Q}(\sqrt{2}).$$

- Για το σταθερό σώμα της $\{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$ θα εφαρμόσουμε παρόμοια διαδικασία με την παραπάνω. Ήδη έχουμε δει ότι ο σ^2 αφήνει αναλλοίωτο το $x_0 = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2$. Τώρα εφαρμόζοντας τον $\sigma\tau$ στο $x_0 = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2$ έχουμε ότι

$$\begin{aligned}
\sigma\tau(x_0) &= \sigma\tau(a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2) \\
&= a_0 + a_2(i\xi)^2 - a_4 i - a_6 i(i\xi)^2 \\
&= a_0 - a_2\xi^2 - a_4 i + a_6 i\xi^2,
\end{aligned}$$

άρα

$$\sigma\tau(x_0) = x_0 \iff a_2 = a_4 = 0.$$

έτσι βλέπουμε ότι ο $\sigma\tau$ αφήνει αναλλοίωτο το $x_1 = a_0 + a_6 i\xi^2$, το οποίο σταθεροποιείται και από τον $\sigma^3\tau$, άρα το σταθερό σώμα της $\{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$ είναι το:

$$\{a_0 + a_6 i\xi^2 \mid a_0, a_6 \in \mathbb{Q}\} = \mathbb{Q}(i\xi^2) = \mathbb{Q}(i\sqrt{2}).$$

- Για το σταθερό σώμα της $\langle\sigma^2\rangle$:
Είδαμε προηγουμένως ότι η σ^2 αφήνει αναλλοίωτο το $x_0 = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2$, συνεπώς το σταθερό σώμα της $\langle\sigma^2\rangle$ είναι το:

$$\{a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2 \mid a_0, a_2, a_4, a_6 \in \mathbb{Q}\} = \mathbb{Q}(\xi^2, i, i\xi^2) = \mathbb{Q}(\xi^2, i) = \mathbb{Q}(\sqrt{2}, i).$$

- Για το σταθερό σώμα της $\langle\tau\rangle$ Εφαρμόζουμε τον τ στο $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$, και έχουμε

  $$\tau(x) = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 - a_4 i + a_5 i\xi - a_6 i\xi^2 - a_7 i\xi^3,$$

  συνεπώς

  $$\tau(x) = x \iff a_4 = a_5 = a_6 = a_7 = 0$$

  άρα η τ αφήνει αναλλοίωτο το

  $$x_0 = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3,$$

  άρα το σταθερό σώμα της $\langle\tau\rangle$ είναι το:

  $$\{a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\} = \mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{2}).$$

- Για το σταθερό σώμα της $\langle\sigma^2\tau\rangle$ εφαρμόζουμε στο $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$ τον $\sigma^2\tau$ και έχουμε

  $\sigma^2\tau(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3) =$

  $= a_0 + a_1(-\xi) + a_2(-\xi)^2 + a_3(-\xi)^3 + a_4(-i) + a_5(-i)(-\xi) + a_6(-i)(-\xi)^2 + a_7(-i)(-\xi)^3$
  $= a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 - a_4 i + a_5 i\xi - a_6 i\xi^2 + a_7 i\xi^3.$

  άρα

  $$\sigma^2\tau(x) = x \iff a_1 = a_3 = a_4 = a_6 = 0.$$

  Συνεπώς ο $\sigma^2\tau$ αφήνει αναλλοίωτο το

  $$x = a_0 + a_2\xi^2 + a_5 i\xi + a_7 i\xi^3$$

  άρα το σταθερό σώμα της $\langle\sigma^2\tau\rangle$ είναι το:

  $\{a_0 + a_2\xi^2 + a_5 i\xi + a_7 i\xi^3 \mid a_0, a_2, a_5, a_7 \in \mathbb{Q}\} = \mathbb{Q}(\xi^2, i\xi, i\xi^3) = \mathbb{Q}(\xi^2, i\xi) = \mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}).$

  Όμως, $(i\xi)^2 = -\xi^2 = -\sqrt{2}$. Συνεπώς το $\xi^2 = \sqrt{2}$ παράγεται από το $i\sqrt[4]{2}$ και άρα $\mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}) = \mathbb{Q}(i\sqrt[4]{2})$.

- Για το σταθερό σώμα της $\langle\sigma\tau\rangle$ εφαρμόζουμε την $\sigma\tau$ στο $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$ τον $\sigma^2\tau$ και έχουμε

  $\sigma\tau(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3) =$

  $= a_0 + a_1 i\xi + a_2(i\xi)^2 + a_3(i\xi)^3 + a_4(-i) + a_5(-i)(i\xi) + a_6(-i)(i\xi)^2 + a_7(-i)(i\xi)^3$
  $= a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5\xi + a_6 i\xi^2 - a_7\xi^3.$

άρα

$$\begin{aligned}\sigma\tau(x) = x \iff & a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3 = \\ & = a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5\xi + a_6 i\xi^2 - a_7\xi^3\end{aligned}$$

$$\iff \begin{cases} a_1 = a_5 \\ a_2 = a_4 = 0 \\ a_3 = -a_7 \end{cases}$$

Άρα ο $\sigma\tau$ σταθεροποιεί το

$$\begin{aligned}x_0 &= a_0 + a_1\xi + a_3\xi^3 + a_1 i\xi + a_6 i\xi^2 - a_3 i\xi^3 \\ &= a_0 + (1+i)a_1\xi + (1-i)a_3\xi^3 + a_6 i\xi^2\end{aligned}$$

άρα το σταθερό σώμα της $\langle\sigma\tau\rangle$ είναι το

$$\mathbb{Q}\big((1+i)\xi, (1-i)\xi^3, i\xi^2\big).$$

Όμως βλέπω ότι $((1+i)\xi)^2 = (1+i)^2\xi^2 = 2i\xi^2$ και άρα το $i\xi^2$ παράγεται από το $(1+i)\xi$. Όμοια,

$$((1+i)\xi)^3 = (1+i)^3\xi^3 = (1+3i+3i^2+i^3)\xi^3 = (1+3i-3-i)\xi^3 = (2i-2)\xi^3 = -2(1-i)\xi^3$$

και άρα το $(1-i)\xi^3$ παράγεται από το $(1+i)\xi$. Επομένως

$$\mathbb{Q}\big((1+i)\xi, (1-i)\xi^3, i\xi^2\big) = \mathbb{Q}((1+i)\xi).$$

- Για το σταθερό σώμα της $\langle\sigma^3\tau\rangle$ εφαρμόζουμε τον $\sigma^3\tau$ στο $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$ και έχουμε

$$\begin{aligned}&\sigma^3\tau(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3) = \\ &\quad = a_0 - a_1 i\xi + a_2(-i\xi)^2 + a_3(-i\xi)^3 + a_4(-i) + a_5(-i)(-i\xi) + a_6(-i)(-i\xi)^2 + a_7(-i)(-i\xi)^3 \\ &\quad = a_0 - a_1 i\xi - a_2\xi^2 + a_3 i\xi^3 - a_4 i - a_5\xi + a_6 i\xi^2 + a_7\xi^3\end{aligned}$$

άρα

$$\begin{aligned}\sigma^3\tau(x) = x \iff & a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3 = \\ & = a_0 - a_1 i\xi - a_2\xi^2 + a_3 i\xi^3 - a_4 i - a_5\xi + a_6 i\xi^2 + a_7\xi^3\end{aligned}$$

$$\iff \begin{cases} a_1 = -a_5 \\ a_2 = a_4 = 0 \\ a_3 = a_7 \end{cases}$$

Άρα ο $\sigma^3\tau$ σταθεροποιεί το

$$\begin{aligned} x_0 &= a_0 + a_1\xi + a_3\xi^3 - a_1 i\xi + a_6 i\xi^2 + a_3 i\xi^3 \\ &= a_0 + (1-i)a_1\xi + (1+i)a_3\xi^3 + a_6 i\xi^2 \end{aligned}$$

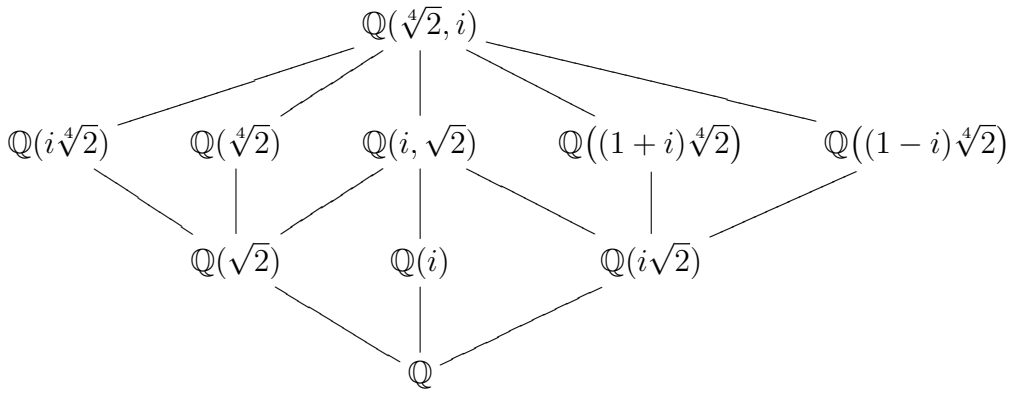
άρα το σταθερό σώμα της $\langle\sigma^3\tau\rangle$ είναι το

$$\mathbb{Q}\big((1-i)\xi, (1+i)\xi^3, i\xi^2\big).$$

Εύκολα βλέπουμε ότι $((1-i)\xi)^2 = -2i\xi^2$ άρα το $i\xi^2$ παράγεται από το $(1-i)\xi$. Όμοια, $((1-i)\xi)^3 = (1-i)^3\xi^3 = (-2i-2)\xi^3 = -2(1+i)\xi^3$ και άρα το $(1+i)\xi^3$ παράγεται από το $(1-i)\xi$. Τελικά

$$\mathbb{Q}\big((1-i)\xi, (1+i)\xi^3, i\xi^2\big) = \mathbb{Q}((1-i)\xi).$$

Τέλος ας φτιάξουμε και το διάγραμμα των σταθερών σωμάτων.



5. Τώρα για να μελετήσουμε τις κανονικές επεκτάσεις παρατηρούμε ότι όλες οι υποομάδες της D_4 που έχουν τάξη 4 είναι κανονικές μιας και έχουν δείκτη 2 στην D_4. Επομένως, οι επεκτάσεις $\mathbb{Q}(i) : \mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ και $\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}$ είναι κανονικές επεκτάσεις.

Επίσης, έχω $\tau\sigma^2\tau^{-1} = \tau\sigma^2\tau = \sigma^2$ και άρα η $\langle\sigma^2\rangle$ είναι κανονική υποομάδα της D_4 συνεπώς η επέκταση $\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q})$ είναι κανονική. Αντίθετα, παρατηρώ ότι

$$\sigma\tau\sigma^{-1} = \sigma^2\tau \notin \langle\tau\rangle$$

$$\sigma(\sigma\tau)\sigma^{-1} = \sigma^2\tau\sigma^{-1} = \sigma^3\tau \notin \langle\sigma\tau\rangle$$

$$\sigma(\sigma^2\tau)\sigma^{-1} = \sigma^3\tau\sigma^{-1} = \tau \notin \langle\sigma^2\tau\rangle$$

$$\sigma(\sigma^3\tau)\sigma^{-1} = \tau\sigma^{-1} = \sigma\tau \notin \langle\sigma^3\tau\rangle$$

συνεπώς οι υποομάδες $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma^2\tau\rangle$ και $\langle\sigma^3\tau\rangle$ δεν είναι κανονικές υποομάδες της D_4 και άρα οι επεκτάσεις $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, i\sqrt[4]{2}) : \mathbb{Q}$, $\mathbb{Q}((1+i)\sqrt[4]{2}) : \mathbb{Q}$ και $\mathbb{Q}((1-i)\sqrt[4]{2}) : \mathbb{Q}$ δεν είναι κανονικές επεκτάσεις.

13 Επιλυσιμότητα με ριζικά

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να συνδέσουμε τις ρίζες ενός πολυωνύμου με τους συντελεστές του.

13.1 Πολυώνυμα 2ου βαθμού.

Έστω $p(x) = \alpha x^2 + \beta x + \gamma$ ένα πολυώνυμο πάνω στο $\mathbb{R}$ τότε ξέρουμε ήδη από το γυμνάσιο ότι οι ρίζες του πολυωνύμου μπορούν να εκφραστούν με την βοήθεια των συντελεστών του πολυωνύμου σαν

$$x_{1,2} = \frac{-\beta \pm \delta}{2\alpha}$$

όπου

$$\delta^2 = \beta^2 - 4\alpha\gamma$$

Στην πραγματικότητα το παραπάνω ισχύει για κάθε σώμα K με χαρακτηριστική διάφορη του 2. Με άλλα λόγια, αν $p(x) = \alpha x^2 + \beta x + \gamma$ ένα πολυώνυμο πάνω στο σώμα K με χαρακτηριστική διάφορη του 2 αρκεί να επεκτείνουμε το K στο $K(\delta)$ και τότε το πολυώνυμο διασπάται στα

$$\Big(x - \frac{-\beta + \delta}{2\alpha}\Big)\Big(x - \frac{-\beta - \delta}{2\alpha}\Big).$$

13.2 Πολυώνυμα 3ου βαθμού.

Έστω $p(x) = y^3 + ay^2 + \beta y + \gamma$ ένα πολυώνυμο πάνω σε ένα σώμα K με χαρακτηριστική διάφορη του 3. Θέτουμε $y = x - a/3$ και έχουμε

$$\begin{aligned} p\Big(x - \frac{a}{3}\Big) &= \Big(x - \frac{a}{3}\Big)^3 + a\Big(x - \frac{a}{3}\Big)^2 + \beta\Big(x - \frac{a}{3}\Big) + \gamma \\ &= x^3 - 3\Big(\frac{a}{3}\Big)x^2 + 3\Big(\frac{a}{3}\Big)^2 x - \Big(\frac{a}{3}\Big)^3 + ax^2 - \frac{2}{3}a^2x + \frac{a^3}{9} + \beta x - \frac{\beta}{3}a + \gamma \\ &= x^3 - \Big(\frac{a^2}{3} - \beta\Big)x - \Big(\frac{\beta a}{3} - \gamma - \frac{2a^3}{27}\Big) \\ &= x^3 - \mu x - \lambda \end{aligned}$$

όπου

$$\mu = \frac{a^2}{3} - \beta \qquad \text{και} \qquad \lambda = \frac{\beta a}{3} - \gamma - \frac{2a^3}{27}$$

Αρκεί λοιπόν να μελετήσουμε το πολυώνυμο $x^3 - \mu x - \lambda$ με $\mu, \lambda \in K$. Έστω $u, v \in K$, τότε

$$\begin{aligned} p(u+v) &= (u+v)^3 - \mu(u+v) - \lambda \\ &= u^3 + 3u^2v + 3uv^2 + v^3 - \mu(u+v) - \lambda \\ &= u^3 + v^3 + (3uv - \mu)(u+v) - \lambda. \end{aligned}$$

Εάν υποθέσουμε ότι

$$3uv - \mu = 0 \iff uv = \frac{\mu}{3},$$

τότε θα έχουμε ότι

$$p(u+v) = p\Big(u + \frac{\mu}{3u}\Big) = 0 \iff u^3 + \Big(\frac{\mu}{3u}\Big)^3 - \lambda = 0$$

θέτουμε $x = u^3$ και έχουμε

$$x + \frac{\mu^3}{3x} - \lambda = 0 \iff x^2 - \lambda x + \frac{\mu^3}{27} = 0$$

Οι ρίζες αυτού του πολυωνύμου είναι οι

$$\frac{\lambda}{2} \pm \sqrt{\frac{\lambda^2}{4} - \frac{\mu^3}{27}}$$

και το γινόμενο των ριζών αυτών είναι $\mu^3/27$. Έτσι αν μια από τις ρίζες αυτές είναι το u^3 τότε η άλλη είναι το v^3, με $v = \lambda/(3u)$. Άρα οι ρίζες του αρχικού πολυωνύμου είναι οι

$$\sqrt[3]{\frac{\lambda}{2} + \sqrt{\frac{\lambda^2}{4} - \frac{\mu^3}{27}}} + \sqrt[3]{\frac{\lambda}{2} - \sqrt{\frac{\lambda^2}{4} - \frac{\mu^3}{27}}}$$

όπου οι δυο κυβικές ρίζες επιλέγονται έτσι ώστε το γινόμενό τους να είναι ίσο με $\frac{1}{3}\mu$.

Άρα το πολυώνυμο $x^3 - \lambda x - \mu$ διασπάται στο σώμα $K(\alpha_1, \alpha_2, \alpha_3)$ όπου $\alpha_1^2 = \frac{1}{4}\mu^2 - \frac{1}{27}\lambda^3$ και $a_2^3 = \frac{1}{2}\mu + \alpha_1$ και $a_3^3 = 1$ με $a_3 \neq 1$. Στην επέκταση αυτή οι ρίζες του πολυωνύμου είναι οι

$$\alpha_2 + \frac{\lambda}{3\alpha_2}, \quad \alpha_2\alpha_3 + \alpha_3^2\frac{\lambda}{3\alpha_2}, \quad \alpha_3^2\alpha_2 + a_3\frac{\lambda}{3\alpha_2}.$$

13.3 Πολυώνυμα 4ου βαθμού.

Με μια παρόμοια αντιμετώπιση, οι ρίζες των πολυωνύμων ανάγονται σε πολυώνυμα τρίτου βαθμού και λύνονται όπως παραπάνω.

Πράγματι, ας πάρουμε ένα πολυώνυμο τετάρτου βαθμού $f(x) = x^4 + ax^3 + bx^2 + cx + d$ σε ένα σώμα K χαρακτηριστικής μηδέν. Μια αντικατάσταση της μορφής $x \to x - c$ μετατρέπει το πολυώνυμο στο $f(x) = x^4 - px^2 - qx - r$ με $p, q, r \in K$. Αν $\alpha, \beta, \gamma, \delta$ είναι οι τέσσερις ρίζες του πολυωνύμου τότε αυτές ικανοποιούν την σχέση $\alpha + \beta + \gamma + \delta = 0$ εφόσον ο συντελεστής του x^3 στο $f(x)$ είναι μηδέν. Ορίζουμε

$$\lambda = (\alpha + \beta)(\gamma + \delta) = -(\alpha + \beta)^2$$

$$\mu = (\alpha + \gamma)(\beta + \delta) = -(a + \gamma)^2$$

$$\nu = (a+\delta)(\beta+\gamma) = -(\alpha+\delta)^2$$

Επιπλέον, $(\alpha+\beta)(\alpha+\gamma)(\alpha+\delta) = q$. Άρα οι ρίζες του f παίρνουν την μορφή $\frac{1}{2}(\sqrt{-\lambda} + \sqrt{-\mu} + \sqrt{-\nu}$ ώστε $\sqrt{-\lambda}\sqrt{-\mu}\sqrt{-\nu} = q$. Άρα μπορούμε να προσδιορίσουμε τις ρίζες του f αν εκφράσουμε τις ποσότητες λ, μ, ν ως προς τους συντελεστές του πολυωνύμου.

Ας πάρουμε τώρα το πολυώνυμο $g(x) = (x-\lambda)(x-\mu)(x-\nu)$. Το πολυώνυμο αυτό αναφέρεται ως resolvent cubic του αρχικού. Οποιαδήποτε μετάθεση των ριζών του πολυωνύμου f θα μεταθέσει τις ποσότητες λ, μ, ν και άρα θα μεταθέσει τους παράγοντες του g. Απευθείας υπολογισμοί δείχνουν ότι $\lambda+\mu+\nu = -2p$, $\lambda\mu+\lambda\nu+\mu\nu = p^2+4r$ και $\lambda\mu\nu = -q^2$. Άρα $g(x) = x^3 + 2px^2 + (p^2+4r)x + q^2$. Χρησιμοποιώντας του τύπους για τα πολυώνυμα τρίτου βαθμού μπορούμε να εκφράσουμε τις ρίζες λ, μ, ν του g ως προς τους συντελεστές του f, και άρα να προσδιορίσουμε τις ρίζες $\alpha, \beta, \gamma, \delta$ τους f ως προς τους συντελεστές του f.

14 Η ομάδα Galois ενός πολυωνύμου

ΟΡΙΣΜΟΣ 14.1. Έστω p πολυώνυμο με συντελεστές στο σώμα K. Η ομάδα Galois του πολυωνύμου p είναι η $\Gamma(L:K)$, όπου L είναι το σώμα διάσπασης του πολυωνύμου p επί του K και τη συμβολίζουμε $\Gamma_K(p)$.

ΠΑΡΑΤΗΡΗΣΗ 14.1. Με δεδομένο ότι όλα τα σώματα διάσπασης ενός πολυωνύμου επί ενός σώματος K είναι $K-$ισομορφικά, όλες οι Galois ομάδες όλων των διασπαστικών επεκτάσεων είναι ισόμορφες. Άρα η ομάδα Galois ενός πολυωνύμου f επί του K είναι καλά ορισμένη.

ΠΑΡΑΤΗΡΗΣΗ 14.2. Παρακάτω θα επισημάνουμε μερικά πράγματα για την ομάδα Galois $\Gamma(L:K)$ μιας επέκτασης $L:K$.

- Έστω L το σώμα διάσπασης ενός πολυωνύμου p επί του K. Αν σ είναι ένας $K-$αυτομορφισμός του L, τότε ο σ μεταθέτει τις ρίζες του p.
- Αν σ, τ είναι επίσης $K-$αυτομορφισμοί του L και $x_1, x_2, \ldots, x_n$ οι ρίζες του p, τότε αν

$$\sigma(x_i) = \tau(x_i) \quad \forall i = 1, \ldots, n \Longrightarrow \sigma = \tau,$$

άρα η $\Gamma(L:K)$ είναι ισόμορφη με κάποια υποομάδα της ομάδας μεταθέσεων S_n όπου n ο βαθμός του πολυωνύμου p.

ΟΡΙΣΜΟΣ 14.2. Ένα πολυώνυμο p επί του K λέγεται επιλύσιμο με ριζικά, αν οι ρίζες του p σε ένα σώμα διάσπασης μπορούν να κατασκευαστούν από τους συντελεστές του p σε πεπερασμένα βήματα με:

1. Πρόσθεση
2. Αφαίρεση

3. Πολλαπλασιασμό

4. Διαίρεση

5. Εξαγωγή n-οστής ρίζας, για κάποιο $n \in \mathbb{N}$.

Δηλαδή ένα πολυώνυμο p είναι επιλύσιμο αν υπάρχουν σώματα $K_0, K_1, \ldots, K_m$ ώστε το p να διασπάται στο K_m και και το K_i να προέρχεται από το K_{i-1} αν προσαρτήσουμε κάποιο a_i με την ιδιότητα

$$a_i^{p_i} \in K_{i-1} \quad \text{για κάποιο} \quad p_i \in \mathbb{N}.$$

Μπορούμε να υποθέσουμε ότι τα p_i είναι πρώτοι.

ΛΗΜΜΑ 14.1. Έστω $f \in K[x]$ με K σώμα και M επέκταση του K. Τότε το $\Gamma_M(f)$ είναι ισομορφικό με μια υποομάδα του $\Gamma_K(f)$.

Απόδειξη. Έστω N το σώμα διάσπασης του f επί του M. Τότε το N περιέχει και το σώμα διάσπασης L του f επί του K. Αν $\sigma \in \Gamma(N : M)$ τότε ο σ σταθεροποιεί και κάθε στοιχείο του K. Άρα ο περιορισμός του σ στο L, $\sigma|_L$ είναι και K αυτομορφισμός του L. Επιπλέον, για κάθε $\sigma, \tau \in \Gamma(N : M)$ έχουμε ότι $(\sigma \circ \tau)|_L = (\sigma_L) \circ (\tau_L)$. Συνεπώς υπάρχει ομομορφισμός $\phi : \Gamma(N : M) \to \Gamma(L : K)$ με $\phi(\sigma) = \sigma|_L$. Έστω τώρα σ στοιχείο του πυρήνα της ϕ δηλαδή $\sigma \in \Gamma(N : M)$ τέτοιο ώστε $\phi(\sigma) = \sigma|_L = id_L$. Όμως το f διασπάται επί του L άρα όλες οι ρίζες του f ανήκουν στο L. Άρα $\sigma(a) = a$ για κάθε ρίζα a του f. Τότε όμως το σταθερό σώμα της σ είναι ολόκληρο το N, εφόσον το M περιέχεται στο σταθερό σώμα του σ και το N είναι το σώμα διάσπασης του f επί του M. Άρα η σ είναι η ταυτοτική απεικόνιση, επομένως η ϕ είναι 1-1 και άρα απεικονίζει την $\Gamma(N : M)$ σε μια υποομάδα της $\Gamma(L : K)$. □

ΠΑΡΑΤΗΡΗΣΗ 14.3. Έχουμε αποδείξει ότι κάθε αυτομορφισμός στην ομάδα Galois ενός πολυωνύμου $f \in K[x]$ είναι K-αυτομορφισμός και άρα μεταθέτει τις ρίζες του πολυωνύμου. Έτσι, δύο τέτοιοι αυτομορφισμοί είναι ίδιοι αν επάγουν την ίδια μετάθεση στις ρίζες του f. Άρα η ομάδα Galois ενός πολυωνύμου είναι μια υποομάδα της ομάδας μεταθέσεων των ριζών του f. Επομένως, αν ο βαθμός του πολυωνύμου είναι n, έχουμε ότι $\Gamma_K(f) \leq S_n$.

14.1 Επιλύσιμες Ομάδες

ΟΡΙΣΜΟΣ 14.3. Μια ομάδα G λέγεται επιλύσιμη αν έχει μια πεπερασμένη ακολουθία υποομάδων $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ ώστε για κάθε i:

1. $G_i \trianglelefteq G_{i+1}$

2. G_{i+1}/G_i είναι αβελιανή.

Την ακολουθία αυτών των υποομάδων $\{G_i\}_{i=0}^n$ την λέμε κανονική σειρά.

Παρατηρήστε ότι το 1 παραπάνω δεν συνεπάγεται ότι $G_i \lhd G$ για κάθε i.

ΠΑΡΑΔΕΙΓΜΑ 14.1. 1. Όλες οι αβελιανές ομάδες είναι επιλύσιμες με σειρά την $1 \leq G$.

2. Η συμμετρική ομάδα S_3, η ομάδα όλων των 1-1 και επί απεικονήσεων από το $\{1,2,3\}$ στο $\{1,2,3\}$, είναι επιλύσιμη. Η σειρά της είναι η $1 \leq A_3 \leq S_3$. Το S_3/A_3 έχει τάξη 2 άρα είναι ισόμορφη με το $\mathbb{Z}_2$.

3. Η συμμετρική ομάδα S_4 είναι επιλύσιμη με σειρά $1 \leq V \leq A_4 \leq S_4$ όπου V η ομάδα του Klein $V = \{(12)(34), (13)(24), (14)(23), 1\} (\cong \mathbb{Z}_2 \times \mathbb{Z}_2)$ με $S_4/A_4 \cong \mathbb{Z}_2$, $A_4/V \cong \mathbb{Z}_3$ και $V/1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Τα παρακάτω Θεωρήματα είναι γνωστά σαν 2ο και 3ο Θεώρημα Ισομορφισμών και μας βοηθούν να κατασκευάζουμε νέες επιλύσιμες ομάδες από υπάρχουσες. Τα παραθέτουμε εδώ χωρίς απόδειξη.

ΘΕΩΡΗΜΑ 14.1 (2ο Θεώρημα Ισομορφισμών). Έστω G ομάδα, H υποομάδα της G και K κανονική υποομάδα της G. Τότε υπάρχει φυσικός ισομορφισμός

$$HK/K \longrightarrow H/(H \cap K) \quad \text{με} \quad hK \mapsto h(H \cap K).$$

ΘΕΩΡΗΜΑ 14.2 (3ο Θεώρημα Ισομορφισμών). Έστω G ομάδα, K κανονική υποομάδα της G και N υποομάδα της K η οποία είναι επίσης κανονική στην G. Τότε η K/N είναι κανονική υποομάδα της G/N και υπάρχει φυσικός ισομορφισμός

$$(G/N)/(K/N) \longrightarrow G/K \quad \text{με} \quad gN \cdot (K/N) \mapsto gK.$$

ΛΗΜΜΑ 14.2. Έστω G ομάδα, H μια υποομάδα της G και N μια κανονική υποομάδα της G. Τότε

1. Αν η G είναι επιλύσιμη $\Longrightarrow$ H είναι επιλύσιμη.

2. Αν G είναι επιλύσιμη $\Longrightarrow$ G/N είναι επιλύσιμη.

3. Αν οι $N, G/N$ είναι επιλύσιμες $\Longrightarrow$ G είναι επιλύσιμη.

Απόδειξη. 1. Η G είναι επιλύσιμη ομάδα οπότε υπάρχει μια κανονική σειρά $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n$ ώστε G_{i+1}/G_i αβελιανή. Θέτουμε $H_i = H \cap G_i$. Τότε και η ακολουθία των ομάδων

$$1 = H_0 \leq H_1 \leq H_2 \leq \ldots \leq H_n = H$$

είναι κανονική σειρά. Πράγματι

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i}.$$

Στην παραπάνω ο ισομορφισμός προκύπτει από το 2ο Θεώρημα Ισομορφισμών 14.1. Άρα η H_{i+1}/H_i αβελιανή άρα η H είναι επιλύσιμη.

2. Η G είναι επιλύσιμη ομάδα οπότε υπάρχει μια κανονική σειρά $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n$. Άρα στην G/N μπορώ να κατασκευάσω την σειρά

$$1 = \frac{N}{N} = \frac{G_0N}{N} \leq \frac{G_1N}{N} \leq \frac{G_2N}{N} \leq \ldots \leq \frac{G_nN}{N} = \frac{G}{N}.$$

Τα διαδοχικά πηλίκα της παραπάνω σειράς είναι τα

$$\frac{G_{i+1}N/N}{G_iN/N}$$

τα οποία από το 3ο Θεώρημα Ισομορφισμών 14.2 είναι

$$\frac{G_{i+1}N/N}{G_iN/N} = \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap G_iN} \cong \frac{G_{i+1}/G_i}{G_{i+1} \cap (G_iN))/G_i}$$

το οποίο είναι πηλίκο αβελιανής ομάδας άρα αβελιανή ομάδα.

3. Εφόσον οι N και G/N επιλύσιμες, υπάρχουν 2 κανονικές σειρές οι

$$1 = N_0 \lhd N_1 \lhd \ldots \lhd N_r = N$$

και

$$1 = N/N = G_0/N \lhd G_1/N \lhd \ldots \lhd G_s/N = G/N$$

με διαδοχικά αβελιανά πηλίκα. Θεωρούμε την σειρά

$$1 = N_0 \lhd N_1 \lhd \ldots \lhd N_r = N = G_0 \lhd G_1 \lhd \ldots \lhd G_s = G.$$

Τότε τα πηλίκα N_{i+1}/N_i είναι αβελιανά και τα πηλίκα $G_{i+1}/G_i \cong (G_{i+1}/N)/(G_i/N)$ είναι επίσης αβελιανά. Άρα η G είναι επιλύσιμη. □

ΠΟΡΙΣΜΑ 14.1. Έστω G ομάδα και N μη τετριμμένη κανονική υποομάδα της G. Η G είναι επιλύσιμη αν και μόνο αν η N και η G/N είναι επιλύσιμες.

ΟΡΙΣΜΟΣ 14.4. Μια ομάδα G λέμε ότι είναι μια επέκταση μιας ομάδας A με τη ομάδα B αν η G έχει μια κανονική υποομάδα N ισόμορφη με την A ώστε $G/N \cong B$.

ΠΑΡΑΤΗΡΗΣΗ 14.4. Το παραπάνω λήμμα μας λέει ότι η κλάση των επιλύσιμων ομάδων είναι κλειστή ως προς υποομάδες, ομάδες πηλίκα και επεκτάσεις. Με άλλα λόγια μια επέκταση μιας επιλύσιμης ομάδας είναι επιλύσιμη. Το παραπάνω δεν ισχύει για αβελιανές ομάδες.

ΟΡΙΣΜΟΣ 14.5. Μια ομάδα λέγεται απλή αν οι μοναδικές κανονικές υποομάδες της είναι η τετριμμένη και ο εαυτός της.

Οι απλές ομάδες είναι οι δομικοί λίθοι με τους οποίους κατασκευάζουμε με τις υπόλοιπες πεπερασμένες ομάδες (Θεώρημα Jordan-Holder).

ΠΑΡΑΔΕΙΓΜΑ 14.2. Μια κυκλική ομάδα με τάξη πρώτο αριθμό είναι απλή, εφόσον κάθε μη τετριμμένο στοιχείο παράγει ολόκληρη της ομάδα. Μια τέτοια ομάδα είναι και επιλύσιμη, με κανονική σειρά την $1 \lhd \mathbb{Z}_p$. Το παρακάτω Θεώρημα μας δείχνει ότι αυτές είναι οι μοναδικές απλές και επιλύσιμες ομάδες.

ΘΕΩΡΗΜΑ 14.3. Μια επιλύσιμη ομάδα είναι απλή αν και μόνο αν είναι κυκλική με τάξη πρώτο αριθμό.

Απόδειξη. Αν η G είναι επιλύσιμη τότε έχει μια κανονική σειρά της μορφής

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

με $G_i \neq G_{i-1}$ για κάθε i. Εφόσον η G_{n-1} είναι κανονική στην G η οποία είναι απλή, έχουμε ότι $G_{n-1} = 1$. Επιπλέον, η G/G_{n-1} είναι αβελιανή συνεπώς η G αβελιανή. Όμως σε μια αβελιανή ομάδα κάθε υποομάδα της είναι κανονική, συνεπώς η G δεν έχει γνήσιες μη-τετριμμένες υποομάδες, άρα κάθε μη-τετριμμένο στοιχείο της G παράγει ολόκληρη την ομάδα. Συνεπώς η G είναι κυκλική με τάξη πρώτο αριθμό. □

ΘΕΩΡΗΜΑ 14.4. Η A_n είναι απλή για κάθε $n \geq 5$.

Απόδειξη. Η απόδειξη του Θεωρήματος βασίζεται στην παρακάτω τεχνική. Θα δείξουμε αρχικά ότι αν μια κανονική υποομάδα της A_n περιέχει έναν τρία κύκλο τότε περιέχει όλους τους τρία κύκλους και άρα είναι ολόκληρη η A_n. Στην συνέχεια θα δείξουμε ότι μια κανονική υποομάδα πρέπει να περιέχει οπωσδήποτε έναν τρία κύκλο.

Θεωρούμε N μη-τετριμμένη κανονική υποομάδα της A_n και υποθέτουμε ότι η N περιέχει τουλάχιστον έναν τρία κύκλο. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι ο κύκλος αυτός είναι ο (123). Δεδομένου ότι τοA_n περιέχει όλους τους τρία κύκλους, θα περιέχει και τον $(3k2)$ για κάθε δυνατό $k > 3$ και εφόσον η N κανονική έχουμε ότι

$$(3k2)^{-1}(123)(3k2) = (2k3)(123)(3k2) = (1k2) \in N.$$

Άρα η N περιέχει και το $(1k2)^2 = (12k)$ για κάθε $k \geq 3$. Θυμηθείτε ότι η S_n παράγεται από όλους του δύο κύκλους της μορφής $(1i)$ με $i = 2, \ldots, n$ και άρα η A_n παράγεται από όλα τα στοιχεία της μορφής $(1j)(1i) = (1ij)$. Αλλά για $i \neq 2$ έχουμε

$$(1ij) = (12j)^{-1}(12i)(12j)$$

και συνεπώς το A_n παράγεται από τα $(12k) \in N$. Επομένως $A_n = N$.

Θα δείξουμε στην συνέχεια ότι κάθε μη-τετριμμένη κανονική υποομάδα του A_n περιέχει ένα τουλάχιστον τρία κύκλο. Εξετάζουμε τις εξής περιπτώσεις.

1. Αν η N περιέχει ένα στοιχείο της μορφής $x = abc \ldots d$ όπου τα $a, b, c, \ldots, d$ είναι κύκλοι ξένοι μεταξύ τους και ο d είναι τουλάχιστον ένας 4-κύκλος, $d = (d_1 d_2 \ldots d_m)$ με $m \geq 4$. Τότε η N περιέχει το στοιχείο

$$(d_1d_2d_3)x(d_1d_2d_3)^{-1} = (d_1d_2d_3)abc \ldots d(d_1d_2d_3)^{-1} = abc \ldots (d_1d_2d_3)d(d_1d_2d_3)^{-1} = z$$

μιας και ξένοι κύκλοι μετατίθενται μεταξύ τους. Άρα το N περιέχει και το στοιχείο

$$x^{-1}z = d^{-1}\dots c^{-1}b^{-1}a^{-1}\cdot abc\dots(d_1d_2d_3)d(d_1d_2d_3)^{-1} = d^{-1}(d_1d_2d_3)d(d_1d_2d_3)^{-1} = (d_1d_3d_m)$$

και άρα η N περιέχει ένα 3-κύκλο.

2. Αν η N περιέχει ένα στοιχείο με τουλάχιστον δύο 3-κύκλους, δηλαδή χωρίς βλάβη της γενικότητας περιέχει το στοιχείο

$$x = (123)(456)y$$

όπου y ένα στοιχείο ξένο με τα $1, 2, \dots, 6$. Τότε η N περιέχει το στοιχείο

$$x^{-1}((234)x(234)^{-1}) = (654)(321)(234)(123)(456)(432) = (12436)$$

οπότε μπορούμε να εφαρμόσουμε την τεχνική της πρώτης περίπτωσης και να πάρουμε και πάλι έναν 3-κύκλο.

3. Αν κάθε στοιχείο του N περιέχει μόνο ένα 3-κύκλο. Τότε θεωρούμε το $x = (123)p$ όπου το p είναι γινόμενο 2-κύκλων. Τότε $p^2 = 1$ και το $x^2 = (123)p(123)p = (132)p^2 = (132)$ και άρα το N περιέχει έναν 3-κύκλο.

4. Αν κάθε στοιχείο του N είναι γινόμενο 2-κύκλων ξένων μεταξύ τους. Μιας και το $n \geq 5$, μπορούμε να υποθέσουμε ότι το N περιέχει ένα στοιχείο της μορφής $x = (12)(34)p$ όπου το p ξένο με τα $1, 2, 3, 4$. Τότε το N περιέχει το στοιχείο

$$x^{-1}(234)x(234)^{-1} = (12)(34)(234)(12)(34)(432) = (14)(23)$$

άρα και το στοιχείο

$$(145)(x^{-1}(234)x(234)^{-1})(145)^{-1} = (145)(14)(23)(541) = (45)(23).$$

Επομένως το N περιέχει και το γινόμενό τους

$$(14)(23)(45)(23) = (145)$$

άτοπο.

Άρα σε κάθε περίπτωση η N περιέχει ένα 3-κύκλο και συνεπώς από τα προηγούμενα είναι ολόκληρη η A_n. Συνεπώς η A_n είναι απλή. □

ΠΟΡΙΣΜΑ 14.2. Η S_n δεν είναι επιλύσιμη για $n \geq 5$.

Απόδειξη. Αν υποθέσουμε ότι για $n \geq 5$ η S_n είναι επιλύσιμη, τότε από το Λήμμα 14.2 και η A_n θα είναι επιλύσιμη. Κατά συνέπεια, εφόσον η A_n είναι απλή για κάθε $n \geq 5$, από το Θεώρημα 14.3, η $A_n \cong \mathbb{Z}_p$, όπου p πρώτος. Δηλαδή η A_n έχει τάξη p. Όμως η τάξη της A_n ξέρουμε ότι είναι $(1/2)n!$, η οποία για $n \geq 5$ δεν μπορεί να είναι πρώτος αριθμός. Άρα η S_n δεν είναι επιλύσιμη. □

14.2 p-ομάδες

ΟΡΙΣΜΟΣ 14.6. Τα στοιχεία $a, b \in G$ μιας ομάδας G λέγονται συζυγή αν υπάρχει $g \in G$ ώστε $a = gbg^{-1}$.

Η συζυγία είναι σχέση ισοδυναμίας και συζυγή στοιχεία ορίζουν κλάσεις ισοδυναμίας οι οποίες ονομάζονται και κλάσεις συζυγίας. Αν οι κλάσεις συζυγίας του G είναι οι $C_1, C_2, \ldots, C_r$ τότε μια από αυτές περιέχει το 1 και άρα $|C_1| = 1$. Επιπλέον, εφόσον οι κλάσεις ισοδυναμίας αποτελούν διαμέριση του G ισχύει η σχέση

$$|G| = 1 + |C_2| + \ldots + |C_r| \tag{7}$$

Η εξίσωση 7 είναι γνωστή και σαν εξίσωση κλάσης (class equation) της G.

ΟΡΙΣΜΟΣ 14.7. Αν G είναι μια ομάδα και $x \in G$ τότε η κεντροποιούσα του x στην G είναι η υποομάδα

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

ΛΗΜΜΑ 14.3. Αν η G ομάδα και $x \in G$ τότε ο αριθμός των στοιχείων στην κλάση ισοδυναμίας του x είναι ο δείκτης της $C_G(x)$ στην G.

Απόδειξη. Η εξίσωση $gxg^{-1} = hxh^{-1}$ ισχύει αν και μόνο αν $hg^{-1}x = xhg^{-1}$ δηλαδή αν και μόνο αν $hg^{-1} \in C_G(x)$ δηλαδή αν και μόνο αν $hC_G(x) = gC_G(x)$. Άρα ο αριθμός των διαφορετικών στοιχείων είναι ίδιος με τον αριθμό των διαφορετικών συμπλόκων της κεντροποιούσας. □

ΠΟΡΙΣΜΑ 14.3. Ο αριθμός των στοιχείων σε οποιαδήποτε κλάση συζυγίας μιας πεπερασμένης ομάδας G διαιρεί την τάξη του G.

ΟΡΙΣΜΟΣ 14.8. Έστω p πρώτος. Μια πεπερασμένη ομάδα G λέγεται p-ομάδα αν η τάξη της είναι μια δύναμη του p.

ΠΑΡΑΔΕΙΓΜΑ 14.3. Η ομάδα συμμετριών του τετραγώνου, D_4 είναι μια 2-ομάδα. Αντίθετα, για κάθε $n \geq 3$ η S_n δεν είναι ποτέ p-ομάδα για οποιονδήποτε πρώτο p.

ΟΡΙΣΜΟΣ 14.9. Το κέντρο $Z(G)$ μιας ομάδας G είναι το σύνολο των στοιχείων $x \in G$ ώστε $xg = gx$ για κάθε $g \in G$.

Από τον ορισμό φαίνεται εύκολα ότι το κέντρο μιας ομάδας είναι κανονική υποομάδα. Πολλές ομάδες έχουν τετριμμένο κέντρο, όπως για παράδειγμα η S_3. Από την άλλη όλες οι αβελιανές ομάδες έχουν κέντρο τον εαυτό τους.

ΘΕΩΡΗΜΑ 14.5. Αν G μια μη τετριμμένη πεπερασμένη p-ομάδα τότε η G έχει μη τετριμμένο κέντρο.

Απόδειξη. Η εξίσωση κλάσης της G μας λέει ότι

$$p^n = 1 + |C_2| + \ldots + |C_n|.$$

Από το Πόρισμα 14.3 έχουμε ότι $|C_i| = p^{n_i}$ για κάποιο $n_i \geq 0$ και για κάθε $i = 2, \ldots, r$. Εφόσον το p διαιρεί την αριστερή πλευρά της παραπάνω εξίσωσης θα πρέπει να διαιρεί και την δεξιά. Άρα τουλάχιστον $p-1$ τιμές του n_i πρέπει να είναι 1 διότι

$$p^n - 1 = |C_2| + \ldots + |C_n| \Leftrightarrow (p-1)(p^{n-1} + \ldots + 1) = |C_2| + \ldots + |C_n|.$$

Αλλά αν το x ανήκει σε μια κλάση συζυγίας με ένα στοιχείο τότε $gxg^{-1} = x$ για κάθε $g \in G$ συνεπώς το x ανήκει στο κέντρο της G και άρα $Z(G) \neq 1$. □

ΠΟΡΙΣΜΑ 14.4. Αν το G είναι μια πεπερασμένη p-ομάδα τάξης p^n τότε το G έχει μια σειρά από κανονικές υποομάδες

$$1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

έτσι ώστε $|G_i| = p^i$ για κάθε $i = 0, \ldots, n$.

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή στο n. Αν $n = 0$ δεν έχουμε τίποτε να δείξουμε. Διαφορετικά, έστω $Z(G) \neq 1$ το κέντρο της G. Εφόσον το $Z(G)$ είναι αβελιανή ομάδα τάξης p^m έχει στοιχείο g τάξης p. Έστω $K = \langle g \rangle$. Τότε $K \lhd Z(G)$. Τότε όμως το G/K είναι επίσης p-ομάδα, τάξης p^{n-1} και άρα από επαγωγική υπόθεση υπάρχει σειρά από κανονικές υποομάδες

$$K/K = G_1/K \lhd \ldots \lhd G_n/K = G/K$$

όπου $|G_i/K| = p^{i-1}$. Συνεπώς $|G_i| = p^i$ και $G_i \lhd G$. Αν θέσουμε $G_0 = 1$ έχουμε την ζητούμενη σειρά. □

ΠΟΡΙΣΜΑ 14.5. Κάθε πεπερασμένη p-ομάδα είναι επιλύσιμη.

ΛΗΜΜΑ 14.4. Έστω A μια πεπερασμένη αβελιανή ομάδα της οποίας η τάξη διαιρείται από έναν πρώτο p. Τότε η A έχει ένα στοιχείο τάξης p.

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή στην τάξη του A. Αν $|A|$ είναι πρώτος τότε η A είναι κυκλική και άρα έχουμε το ζητούμενο. Διαφορετικά, παίρνουμε μια γνήσια υποομάδα M της A με την μέγιστη δυνατή τάξη, έστω m. Αν το p διαιρεί το m τότε έχουμε το αποτέλεσμα από την επαγωγική υπόθεση. Αν το p δεν διαιρεί το m θεωρούμε $t \in A \setminus M$ και $T = \langle t \rangle$. Τότε η MT είναι υποομάδα του A, μεγαλύτερη από την M άρα $MT = A$ από την επιλογή της M σαν μέγιστης υποομάδας. Από Πρώτο Θεώρημα Ισομορφισμών έχουμε ότι $|MT| = |M| \cdot |T|/|M \cap T|$, άρα το p διαιρεί την τάξη r του T. Εφόσον η T είναι κυκλική που παράγεται από το t έχουμε ότι το $t^{r/p}$ έχει τάξη p. □

ΘΕΩΡΗΜΑ 14.6 (Sylow). Έστω G μια πεπερασμένη ομάδα τάξης $p^\alpha r$ όπου p πρώτος και p δεν διαιρεί το r. Τότε η G περιέχει τουλάχιστον μια υποομάδα τάξης p^α.

Απόδειξη. Χρησιμοποιούμε επαγωγή στην τάξη της G. Το θεώρημα ισχύει για $|G| = 1$ και 2. Έστω $C_1, \ldots, C_s$ οι κλάσεις συζυγίας του G και $c_i = |C_i|$. Η εξίσωση κλάση της G δίνει

$$p^a r = c_1 + \ldots + c_s \tag{8}$$

Έστω Z_i η κεντροποιούσα στην G κάποιου $x_i \in C_i$ και $n_i = |Z_i|$. Τότε από το Λήμμα 14.3 έχουμε

$$n_i = \frac{p^\alpha r}{c_i} \tag{9}$$

Ας υποθέσουμε αρχικά ότι $c_i > 1$ και p δεν διαιρεί το c_i. Τότε η εξίσωση 9 δίνει $n_i < p^\alpha r$ και n_i διαιρείται από το p^α. Άρα από επαγωγή η Z_i περιέχει υποομάδα τάξης p^α. Άρα μπορούμε να υποθέσουμε ότι για κάθε $i = 1, \ldots, s$ είτε $c_i = 1$ είτε p διαιρεί το c_i. Έστω $z = |Z(G)|$. Όπως και πριν το z είναι ο αριθμός των τιμών του i για τις οποίες $c_i = 1$. Άρα $p^\alpha r = z + kp$ για κάποιο ακέραιο k. Άρα το p διαιρεί το z και το G έχει μη τετριμμένο κέντρο $Z(G)$ ώστε p διαιρεί το $|Z(G)|$. Άρα από το Λήμμα 14.4 το $Z(G)$ έχει στοιχείο τάξης p που παράγει μια υποομάδα P του G τάξης p. Εφόσον $P \leq Z(G)$, η P είναι κανονική υποομάδα της G. Άρα από επαγωγή η G/P περιέχει υποομάδα S/P τάξης $p^{\alpha-1}$ και άρα η S είναι υποομάδα τάξης p^α. □

ΟΡΙΣΜΟΣ 14.10. Αν το G είναι μια ομάδα με τάξη $p^\alpha r$ όπου p πρώτος και p δεν διαιρεί το r τότε μια υποομάδα της G τάξης p^α λέγεται Sylow p-υποομάδα.

ΠΟΡΙΣΜΑ 14.6 (Θεώρημα Cauchy). Αν p πρώτος και p διαιρεί την τάξη μιας πεπερασμένης ομάδας G τότε η G έχει ένα στοιχείο τάξης p.

ΠΑΡΑΔΕΙΓΜΑ 14.4. Έστω $G = S_4$. Ξέρουμε ότι $|G| = 24$. Το Θεώρημα Cauchy μας λέει ότι η G πρέπει να έχει υποομάδες τάξης 3 και 8. Υποομάδες τάξης 3 είναι εύκολο να βρούμε. Όλες οι κυκλικές υποομάδες που παράγονται από 3-κύκλους, $\langle(123)>$, $\langle(234)\rangle$ κλπ.

Τι γίνεται όμως με τις υποομάδες τάξης 8; Έστω $V = \{1, (12)(34), (13)(24), (14)(23)\}$ η ομάδα του Klein που υπάρχει στην S_4. Αυτή έχει τάξη 4. Αν τώρα t ένας οποιοσδήποτε 2-κύκλος που παράγει μια υποομάδα τάξης 2, έστω T τότε $V \cap T = 1$ και άρα η VT είναι μια υποομάδα τάξης 8.

14.3 Πρωταρχικές Ρίζες

Παρακάτω θα υπενθυμίσουμε μερικά πράγματα για τις πρωταρχικές ρίζες της μονάδας.

Έστω L σώμα και p ένας πρώτος αριθμός, διαφορετικός από τη χαρακτηριστική του L. Υποθέτουμε ότι το πολυώνυμο

$$f(x) = x^p - 1$$

διασπάται στο L. Το f έχει διακριτές ρίζες, διότι η παράγωγός του, px^{p-1} είναι μη μηδενική. Αν $\omega \neq 1$ είναι μια ρίζα του f, τότε αυτή ονομάζεται πρωταρχική ρίζα της μονάδας. Οι πρωταρχικές ρίζες της μονάδας είναι οι ρίζες του πολυωνύμου

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

μιας και

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Εύκολα βλέπουμε ότι η ρίζα $w \neq 1$ λειτουργεί σαν γεννήτορας για τις υπόλοιπες ρίζες του f. Πράγματι, το w^k για $k = 1, \ldots, p-1$ διατρέχει όλες τις ρίζες του f. Άρα οι ρίζες της μονάδας αποτελούν τα στοιχεία μιας κυκλικής ομάδα τάξης p που παράγεται από οποιαδήποτε πρωταρχική ρίζα, δηλαδή

$$\langle \omega \rangle = \{\omega^k \mid k = 1, 2, \ldots, p-1\} \cong \mathbb{Z}_p.$$

Λημμα 14.5. Έστω K σώμα, p πρώτος διαφορετικός από την χαρακτηριστική του K και ω μια πρωταρχική p-οστή ρίζα της μονάδας. Τότε η ομάδα Galois της $K(\omega) : K$ είναι αβελιανή.

Απόδειξη. Έστω $L = K(\omega)$. Όπως είδαμε παραπάνω το ω είναι γεννήτορας όλων των ριζών του πολυωνύμου $x^p - 1$, άρα το L είναι το σώμα διάσπασης του πολυωνύμου $x^p - 1$. Θεωρούμε τους K-αυτομορφισμούς $\sigma, \tau \in \Gamma\big(K(\omega) : K\big)$. Τότε τα $\sigma(\omega), \tau(\omega)$ είναι ρίζες του $x^p - 1$, άρα υπάρχουν $m, r > 0$ ώστε

$$\sigma(\omega) = \omega^m \qquad \text{και} \qquad \tau(\omega) = \omega^r,$$

άρα

$$\sigma\big(\tau(\omega)\big) = \sigma(\omega^r) = \omega^{mr} = \tau(\omega^m) = \tau\big(\sigma(\omega)\big)$$

και $\sigma \circ \tau, \tau \circ \sigma \in \Gamma\big(K(\omega) : K\big)$. Άρα $\sigma \circ \tau = \tau \circ \sigma$ για κάθε $\sigma, \tau \in \Gamma\big(K(\omega) : K\big)$, συνεπώς η $\Gamma\big(K(\omega) : K\big)$ είναι αβελιανή. □

Λημμα 14.6. Έστω K σώμα χαρακτηριστικής μηδέν, p πρώτος και M το σώμα διάσπασης του πολυωνύμου $f(x) = x^p - c$, όπου $c \in K$. Τότε ομάδα Galois $\Gamma(M : K)$ είναι επιλύσιμη.

Απόδειξη. Αν $c = 0$, τότε $M = K$, άρα η ομάδα Galois $\Gamma(M : K) = \{1\}$ είναι επιλύσιμη. Αν $c \neq 0$ τότε οι ρίζες του f είναι διακριτές. Έστω ω να είναι μια πρωταρχική p-οστή ρίζα της μονάδας. Αν $\alpha \in M$ τέτοιο ώστε $\alpha^p = c$, οι ρίζες του $x^p - c$ είναι οι $\alpha\omega^k$, $k = 0, \ldots, p-1$. Επομένως κάθε δύναμη του ω μπορεί να γραφεί σαν λόγος δύο διακριτών ριζών του $x^p - c$. Άρα το $M = K(\alpha, \omega)$ όπου $\alpha^p = c$ και ω μια πρωταρχική ρίζα της μονάδας. Η $K(\omega) : K$ είναι κανονική επέκταση, διότι είναι το σώμα διάσπασης του πολυωνύμου $x^p - 1$ επί του K, οπότε από το θεώρημα της αντιστοιχίας Galois 12.1, έχουμε ότι

1. $\Gamma\big(M : K(\omega)\big) \trianglelefteq \Gamma(M : K)$ και
2. $\Gamma(M : K)/\Gamma\big(M : K(\omega)\big) \cong \Gamma\big(K(\omega) : K\big)$.

Από το Λήμμα 14.5 η $\Gamma\big(K(\omega) : K\big)$ είναι αβελιανή.

Από την άλλη, το M προκύπτει από το $K(\omega)$ προσαρτώντας το α και άρα κάθε $\sigma \in \Gamma(M : K(\omega))$ προσδιορίζεται μοναδικά από την τιμή του $\sigma(\alpha)$. Επιπλέον, το $\sigma(\alpha) = \alpha\omega^j$ μιας και είναι ρίζα του $x^p - c$. Άρα αν $\sigma, \tau \in \Gamma(M : K(\omega))$ τότε $\sigma(\alpha) = \alpha\omega^j$, $\tau(\alpha) = \alpha\omega^k$ και

$\sigma \circ \tau(\alpha) = \alpha\omega^{j+k} = \tau \circ \sigma(\alpha)$, εφόσον οι σ, τ είναι $K(\omega)-$αυτομορφισμοί του M και άρα $\sigma(\omega) = w = \tau(\omega)$. Άρα η $\Gamma(M : K(\omega))$ είναι αβελιανή και συνεπώς η σειρά

$$\{1\} \leq \Gamma\big(M : K(\omega)\big) \leq \Gamma(M : K)$$

είναι κανονική και τα διαδοχικά πηλίκα είναι αβελιανές ομάδες. Άρα η $\Gamma(M{:}K)$ είναι επιλύσιμη. □

15 Επιλύσιμα πολυώνυμα

ΛΗΜΜΑ 15.1. Έστω $f \in K[x]$ με K σώμα χαρακτηριστικής μηδέν, $a \in K(a) = K'$ ώστε $a^p \in K$, όπου p πρώτος. Τότε η $\Gamma_K(f)$ είναι επιλύσιμη αν και μόνο αν η $\Gamma_{K'}(f)$ είναι επιλύσιμη.

Απόδειξη. Θεωρούμε το πολυώνυμο $q(x) = f(x)(x^p - c)$ όπου $c = a^p$. Το $q(x) \in K[x]$ και έστω N είναι το σώμα διάσπασης του q επί του K. Το N περιέχει το σώμα διάσπασης του f επί του K, έστω L και το σώμα διάσπασης του $x^p - c$ επί του K, έστω M.

Οι επεκτάσεις $N : K, M : K, L : K$ είναι επεκτάσεις Galois και από το θεώρημα της αντιστοιχίας Galois 12.1 έχουμε ότι

1. $\Gamma(N : L) \lhd \Gamma(N : K)$,
2. $\Gamma(N : M) \lhd \Gamma(N : K)$
3. $\Gamma(N : K)/\Gamma(N : L) \cong \Gamma(L : K)$ και
4. $\Gamma(N : K)/\Gamma(N : M) \cong \Gamma(M : K)$.

Τα M, N είναι τα σώματα διάσπασης του $x^p - c$ επί των K και L αντίστοιχα. Άρα από το προηγούμενο Λήμμα, οι $\Gamma(M : K)$ και $\Gamma(N : L)$ είναι επιλύσιμες. Άρα από Λήμμα 14.2 η $\Gamma(N : K)$ είναι επιλύσιμη αν και μόνο αν η $\Gamma(N : M)$ είναι επιλύσιμη. Όμοια η $\Gamma(N : K)$ είναι επιλύσιμη αν και μόνο αν η $\Gamma(L : K)$ είναι επιλύσιμη. Αλλά η $\Gamma(N : M) \cong \Gamma_M(f)$ και $\Gamma(L : K) \cong \Gamma_K(f)$ εφόσον τα L, N είναι σώματα διάσπασης του f επί των K και M αντίστοιχα. Συνεπώς η $\Gamma_M(f)$ είναι επιλύσιμη αν και μόνο αν η $\Gamma_K(f)$ είναι επιλύσιμη.

Το M είναι σώμα διάσπασης του $x^p - c$ επί του K'. Άρα από το παραπάνω, $\Gamma_M(f)$ επιλύσιμη αν και μόνο αν $\Gamma_{K'}(f)$ επιλύσιμη και συνεπώς $\Gamma(f)$ επιλύσιμη αν και μόνο αν $\Gamma_{K'}(f)$ επιλύσιμη. □

ΘΕΩΡΗΜΑ 15.1. Έστω K σώμα χαρακτηριστικής μηδέν και $f \in K[x]$. Αν το f είναι επιλύσιμο με ριζικά, τότε η ομάδα Galois $\Gamma_K(f)$ είναι επιλύσιμη.

Απόδειξη. Το f είναι επιλύσιμο με ριζικά, άρα υπάρχει μια ακολουθία σωμάτων $K_0 = K, K_1, \ldots, K_m$ ώστε

$$K_i = K_{i-1}(a_i), \quad \text{όπου} \quad a_i^{p_i} \in K_{i-1} \quad \text{και} \quad p_i \quad \text{πρώτος για κάθε } i = 1, 2, \ldots, m.$$

Έχουμε ότι $\Gamma_{K_m}(f) = \{1\}$, η οποία είναι επιλύσιμη. Όμως

$$K_m = K_{m-1}(a_m) \quad \text{με} \quad a_m^{p_m} \in K_{m-1},$$

άρα από το Λήμμα 15.1 και η $\Gamma_{K_{m-1}}(f)$ είναι επιλύσιμη. Επίσης

$$K_{m-1} = K_{m-2}(a_{m-1}) \quad \text{με} \quad a_{m-1}^{p_{m-1}} \in K_{m-2},$$

άρα πάλι από το Λήμμα 15.1 η $\Gamma_{K_{m-2}}(f)$ είναι επιλύσιμη. Με μια απλή επαγωγή βλέπουμε ότι και $\Gamma_K(f)$ είναι επιλύσιμη. □

Λημμα 15.2. Έστω K σώμα, p πρώτος διαφορετικός από τη χαρακτηριστική του K και $L : K$ μια επέκταση Galois βαθμού p. Αν το πολυώνυμο $x^p - 1$ διασπάται επί του K, τότε υπάρχει $a \in L$ ώστε $L = K(a)$ και $a^p \in K$.

Απόδειξη. Η επέκταση $L : K$ έχει βαθμό p και είναι επέκταση Galois και συνεπώς η $\Gamma(L : K)$ είναι κυκλική τάξης p. Έστω σ ένας γεννήτορας της $\Gamma(L : K)$ και $\beta \in L \backslash K$. Ορίζουμε

$$a_j = \beta_0 + \beta_1\omega^j + \beta_2\omega^{2j} + \cdots + \beta_{p-1}\omega^{(p-1)j}$$

όπου $\beta_0 = \beta$, $\beta_i = \sigma(\beta_{i-1})$, $i = 1, \ldots, p-1$ και ω μια πρωταρχική $p-$οστή ρίζα της μονάδας που ανήκει το K. Τότε

$$\begin{aligned}
\sigma(a_j) &= \sigma(\beta_0) + \sigma(\beta_1)\omega^j + \cdots + \sigma(\beta_{p-1})\omega^{(p-1)j} \\
&= \beta_1 + \beta_2\omega^j + \cdots + \beta_0\omega^{(p-1)j} \\
&= \beta_0\omega^{-pj}\omega^{-j} + \beta_1 + \beta_2\omega^j + \cdots + \beta_{p-1}\omega^{(p-2)j} \\
&= \beta_0\omega^{-j} + \beta_1 + \beta_2\omega^j + \cdots + \beta_{p-1}\omega^{(p-2)j} \\
&= \omega^{-j}(\beta_0 + \beta_1\omega^j + \beta_2\omega^{2j} + \cdots + \beta_{p-1}\omega^{(p-1)j}) \\
&= \omega^{-j}a_j,
\end{aligned}$$

άρα

$$\sigma\big(a_j^p\big) = (\omega^{-j}a_j)^p = a_j^p$$

και άρα $a_j^p \in K$ για $j = 0, \ldots, p-1$. Όμως,

$$a_0 + \ldots + a_{p-1} = \sum_{j=0}^{p-1} \beta_0 + w^j\beta_1 + \ldots + w^{j(p-1)}\beta_{p-1}$$

$$= p\beta_0 + (1 + w + w^2 + \ldots + w^{p-1})\beta_1 + \ldots + (1 + w^{p-1} + w^{2(p-1)} + \ldots + w^{(p-1)(p-1)})\beta_{p-1}$$

$$= p\beta_0 = p\beta$$

εφόσον το w είναι ρίζα του πολυωνύμου $1+x^2+\ldots+x^{p-1}$. Το $p\beta \in L \setminus K$ εφόσον $\beta \in L \setminus K$ και $p \in K$. Άρα ένα τουλάχιστον από τα a_j, έστω το a_1 ανήκει στο $\in L \setminus K$. Από τον tower law έχουμε ότι το $[K(a_1) : K]$ διαιρεί το $[L : K] = p$. Συνεπώς $L : K = K(a_1) : K$ και $a_1^p \in K$. □

ΘΕΩΡΗΜΑ 15.2. Έστω K ένα σώμα χαρακτηριστικής μηδέν και $f \in K[x]$. Αν $\Gamma_K(f)$ είναι επιλύσιμη τότε το f είναι επιλύσιμο με ριζικά.

Απόδειξη. Έστω ω είναι μια $p-$οστή πρωταρχική ρίζα της μονάδας. Η $\Gamma_{K(w)}(f)$ είναι ισομορφική με μια υποομάδα της $\Gamma_K(f)$ (Λήμμα 14.1) και άρα είναι επιλύσιμη. Όμως το f είναι επιλύσιμο με ριζικά επί του K αν και μόνο αν το f είναι επιλύσιμο με ριζικά επί του $K(w)$ μιας και το $K(w)$ προκύπτει από το K με την προθήκη ενός στοιχείου, του οποίου η p-οστή δύναμη ανήκει στο K. Άρα χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι το K περιέχει μια πρωταρχική p-οστή ρίζα της μονάδας για κάθε πρώτο p που διαιρεί την $|\Gamma_K(f)|$.

Θα αποδείξουμε το αποτέλεσμα με επαγωγή στην τάξη της $\Gamma_K(f)$. Το αποτέλεσμα ισχύει αν $|\Gamma(f)| = 1$ εφόσον στην περίπτωση αυτή το f διασπάται. Ας υποθέσουμε ότι το αποτέλεσμα ισχύει όταν η τάξη της ομάδας Galois είναι μικρότερη από $|\Gamma_K(f)|$ και έστω L το σώμα διάσπασης του f επί του K. Φυσικά, $L : K$ επέκταση Galois με ομάδα Galois την $\Gamma(L : K) \cong \Gamma_K(f)$. Επιπλέον, η $\Gamma(L : K)$ είναι επιλύσιμη και περιέχει μια κανονική υποομάδα H για την οποία η ομάδα πηλίκο $\Gamma(L : K)/H$ είναι κυκλική τάξης p για κάποιο πρώτο p που διαιρεί την τάξη της $\Gamma_K(f)$. Έστω M το σταθερό σώμα της H. Τότε $\Gamma(L : M) = H$ και $\Gamma(M : K) \cong \Gamma(L : K)/H$. Άρα $[M : K] = |\Gamma(L : K)/H| = p$. Συνεπώς, από το προηγούμενο Λήμμα έχουμε ότι $M = K(\alpha)$ για κάποιο $\alpha \in M$ με $\alpha^p \in K$. Επίσης, $\Gamma_M(f) \cong H$ και η H είναι επιλύσιμη μιας και είναι υποομάδα μιας επιλύσιμη ομάδας. Άρα από επαγωγή το f είναι επιλύσιμο με ριζικά αν θεωρηθεί σαν πολυώνυμο επί του M και άρα οι ρίζες του ανήκουν σε μια επέκταση του M που προκύπτει προσθέτοντας διαδοχικά ριζικά. Αλλά και το M προκύπτει από το K προσθέτοντας την ρίζα α. Επομένως το f είναι επιλύσιμο με ριζικά και σαν πολυώνυμο επί του K. □

ΘΕΩΡΗΜΑ 15.3. Έστω K σώμα χαρακτηριστικής μηδέν και $f \in K[x]$. Το f είναι επιλύσιμο με ριζικά επί του K αν και μόνο αν η ομάδα Galois $\Gamma_K(f)$ επί του K είναι επιλύσιμη.

Απόδειξη. Άμεση συνέπεια των Θεωρημάτων 15.1 και 15.2. □

ΠΟΡΙΣΜΑ 15.1. Έστω p πρώτος και f πολυώνυμο τάξης p με συντελεστές στο $\mathbb{Q}$. Υποθέτουμε ότι το f έχει ακριβώς $p-2$ πραγματικές ρίζες και είναι ανάγωγο επί του $\mathbb{Q}$. Τότε η ομάδα Galois του f επί του $\mathbb{Q}$ είναι η S_p. Ειδικότερα, αν $p \geq 5$ οι ρίζες του f δεν είναι επιλύσιμες με ριζικά.

Απόδειξη. Αν το α είναι ρίζα του f τότε $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ εφόσον το f είναι ανάγωγο και $\deg f = p$. Άρα αν το L είναι το σώμα διάσπασης του f επί του $\mathbb{Q}$ τότε $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$ και άρα το $[L : \mathbb{Q}]$ διαιρείται από το p. Αλλά το $[L : \mathbb{Q}]$ είναι η τάξη της ομάδας Galois, έστω G, του f άρα η $|G|$ διαιρείται από το p. Από το Θεώρημα Cauchy έχουμε ότι η G έχει ένα στοιχείο τάξης p. Επιπλέον, τα στοιχεία της G καθορίζονται από την δράση του στις ρίζες του f. Άρα ένα στοιχείο του G έχει τάξη p αν και μόνο αν μεταθέτει κυκλικά τις ρίζες του f. Εφόσον το f είναι ανάγωγο έχει διακριτές ρίζες . Αν α_1, α_2 οι δύο ρίζες του f που δεν είναι πραγματικές. Τότε οι α_1, α_2 είναι μιγαδικές. Εφόσον η G περιέχει στοιχείο τάξης p που μεταθέτει τις ρίζες, υπάρχει κατάλληλη δύναμη του στοιχείου αυτού

που στέλνει την α_1 στην α_2. Έστω $\alpha_3, \alpha_4, \ldots, \alpha_p$ οι πραγματικές ρίζες του f ώστε $\alpha_j = \sigma(\alpha_{j-1})$ για $j = 2, 3, \ldots, p$. Τότε $\sigma(\alpha_p) = \alpha_1$. Επειδή έχω ακριβώς δυο μιγαδικές συζυγείς ρίζες υπάρχει $\mathbb{Q}$ αυτομορφισμός τ του L ώστε $\tau(\alpha_1) = \alpha_2$, $\tau(a_2) = \alpha_1$ και $\tau(a_i) = a_i$ για $i \geq 3$. Τότε $\langle \sigma, \tau \rangle \cong S_p$. Άρα $G \cong S_p$. □

ΠΑΡΑΔΕΙΓΜΑ 15.1. Έστω $f(x) = x^5 - 6x + 3$ επί του $\mathbb{Q}$. Το πολυώνυμο αυτό είναι ανάγωγο από το κριτήριο του Eisenstein. Όμως, $f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$ και $f(2) = 23$. Το Θεώρημα ενδιαμέσων τιμών μας εγγυάται ότι το f έχει τουλάχιστον 3 διακριτές πραγματικές ρίζες. Αν τώρα έχω 4 πραγματικές ρίζες τότε από το Θεώρημα Rolle οι διακριτές ρίζες του f' και f'' θα ήταν τουλάχιστον 3 και 2 αντίστοιχα. Όμως $f''(x) = 20x^3$ το οποίο έχει μοναδική πραγματική ρίζα το 0. Άρα το f έχει ακριβώς 3 πραγματικές ρίζες και 2 μιγαδικές και επομένως η ομάδα Galois είναι η S_5. Συνεπώς το f δεν είναι επιλύσιμο με ριζικά.

ΠΑΡΑΤΗΡΗΣΗ 15.1. Ένα από τα άλυτα προβλήματα της Θεωρίας Galois είναι το περίφημο Inverse Galois Problem: Αποτελεί κάθε πεπερασμένη ομάδα μια ομάδα Galois μιας πεπερασμένης επέκτασης του $\mathbb{Q}$; Το πρόβλημα αυτό είναι άλυτο στην γενικότητά του, παρόλα αυτά ξέρουμε τι γίνεται για πολλές οικογένειες ομάδων. Για παράδειγμα γνωρίζουμε ότι το αποτέλεσμα ισχύει για τις A_n και S_n (Hilbert), για τις p-ομάδες (A. Scholz and H. Reichardt, 1937) και για τις επιλύσιμες ομάδες (Shafarevich). Επιπλέον, έχει αποδειχθεί (????? 1978) ότι αν δεν απαιτήσουμε η επέκταση να είναι Galois τότε κάθε πεπερασμένη ομάδα μπορεί να υλοποιηθεί σαν ομάδα αυτομορφισμών μια πεπερασμένης επέκτασης.

16 Κυκλοτομικές επεκτάσεις

Το σώμα διάσπασης L του $x^n - 1$ επί του K λέγεται κυκλοτομική επέκταση τάξης n. Αν η χαρακτηριστική του K είναι p διαφορετική από το μηδέν και $n = mp^t$ όπου $(p, m) = 1$ τότε $x^n - 1 = (x^m - 1)^{p^t}$ άρα η κυκλοτομική επέκταση τάξης n ταυτίζεται με την κυκλοτομική επέκταση τάξης m. Άρα γενικά μπορούμε να θεωρούμε ότι η χαρακτηριστική είναι σχετικά πρώτη με το n.

Η βαθμός μιας κυκλοτομικής επέκτασης τάξης n σχετίζεται με την συνάρτηση ϕ του Euler.

ΘΕΩΡΗΜΑ 16.1. Έστω n θετικός ακέραιος, K σώμα χαρακτηριστικής p με $(p, n) = 1$ και L η κυκλοτομική επέκταση του K τάξης n. Τότε

1. $L = K(\zeta)$ όπου ζ μια πρωταρχική n-οστή ρίζα της μονάδας.
2. η ομάδα Galois της επέκτασης είναι αβελιανή με τάξη d όπου d διαιρεί το $\phi(n)$.

Απόδειξη.

1. Από υπόθεση έχουμε ότι $nx^{n-1} \neq 0$ άρα $x^n - 1$ είναι σχετικά πρώτο με την παράγωγό του. Άρα το $x^n - 1$ έχει n διακριτές ρίζες στο σώμα διάσπασης L. Άρα η κυκλική ομάδα των n-οστών ριζών της μονάδας στο L έχει τάξη n άρα το L περιέχει μια πρωταρχική ρίζα $\zeta \in L$. Συνεπώς $1, \zeta, \zeta^2, \ldots, \zeta^{n-1} \in K(\zeta)$ δηλαδή $L = K(\zeta)$.

2. Αν $\sigma \in \Gamma(L:K)$ τότε η σ προσδιορίζεται μοναδικά από το $\sigma(\zeta)$. Όμως $\sigma(\zeta) = \zeta^i$ για κάποιο $1 \leq i \leq n-1$. Όμοια $\sigma^{-1}(\zeta) = \zeta^j$. Αλλά $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$ δηλαδή $ij \equiv 1 \pmod{n}$. Άρα η συνάρτηση $\sigma \mapsto i$ ορίζει μονομορφισμό $\Gamma(L:K) \to A$ όπου A η πολλαπλασιαστική ομάδα των μονάδων της $\mathbb{Z}_n$. Όμως $|A| = \phi(n)$. Συνεπώς $\Gamma(L:K) \cong \mathrm{Im} f \leq A$ αβελιάνη. Άρα έχει τάξη d που διαιρεί το $\phi(n)$. □

Αν τώρα K σώμα, n φυσικός πρώτος με την χαρακτηριστική του σώματος και F η κυκλοτομική επέκταση τάξης n του K. Το n-οστό κυκλοτομικό πολυώνυμο του K είναι το μονικό πολυώνυμο

$$g_n(x) = (x-\zeta_1)(x-\zeta_2)\dots(x-\zeta_r)$$

όπου $\zeta_1, \dots, \zeta_r$ είναι οι διακριτές *πρωταρχικές* n-οστές ρίζες της μονάδας στο F.

ΠΑΡΑΔΕΙΓΜΑ 16.1.

$$g_1(x) = x - 1.$$

$$g_2(x) = (x-(-1)) = x+1.$$

Αν $K = \mathbb{Q}$ τότε $g_3(x) = (x-\zeta_1)(x-\zeta_2)$ όπου $\zeta_1, \zeta_2 = \frac{-1 \pm i\sqrt{3}}{2}$, $g_4(x) = (x-i)(x+i) = x^2+1$.

ΠΡΟΤΑΣΗ 16.1. Έστω $n > 0$ ακέραιος, K σώμα χαρακτηριστική p με $(p,n) = 1$ και $g_n(x)$ το n-οστό κυκλοτομικό πολυώνυμο επί του K. Τότε

1. $x^n - 1 = \prod_{d|n} g_d(x)$.

2. Οι συντελεστές του $g_n(x)$ ανήκουν στο πρώτο υπόσωμα P του K. Επιπλέον, αν η χαρακτηριστική του K είναι 0 τότε οι συντελεστές του $g_n(x)$ είναι ακέραιοι.

3. $\deg(g_n(x)) = \phi(n)$.

Απόδειξη.

1. Έστω F η κυκλοτομική επέκταση του K τάξης n και $\zeta \in F$ μια πρωταρχική n-οστή ρίζα της μονάδας. Τότε η $\langle\zeta\rangle = G$ περιέχει όλες τις n-οστές ρίζες της μονάδας και όλες τις d-οστές ρίζες της μονάδας για κάθε διαιρέτη d του n. Τώρα η $\eta \in \langle\zeta\rangle = G$ είναι πρωταρχική d-οστή ρίζα της μονάδας ($d|n$) αν και μόνο αν η τάξη της είναι d. Άρα για κάθε διαιρέτη d του n

$$g_d(x) = \prod_{\substack{\eta\in G \\ |\eta|=d}} (x-\eta).$$

Άρα

$$x^n - 1 = \prod_{\eta\in G}(x-\eta) = \prod_{\substack{d \\ d|n}} \Big(\prod_{\substack{\eta\in G \\ |\eta|=d}} (x-\eta) \Big) = \prod_{\substack{d \\ d|n}} g_d(x).$$

2. Θα χρησιμοποιήσουμε επαγωγή στο n. Προφανώς $g_1(x) = x-1 \in P[x]$. Υποθέτουμε ότι το αποτέλεσμα ισχύει για κάθε $k < n$ και έστω

$$f(x) = \prod_{\substack{d|n \\ d<n}} g_d(x).$$

Από επαγωγική υπόθεση το $f(x) \in P[x]$ και $x^n - 1 = f(x)g_n(x)$. Όμως το $x^n - 1 \in P[x]$ και το f είναι μονικά. Άρα από αλγόριθμο διαίρεσης πολυωνύμων στο $P[x]$ έχουμε $x^n - 1 = f \cdot h + r$ για $h, r \in P[x] \subset F[x]$. Άρα, από μοναδικότητα υπολοίπου, $r = 0$ και $g_n(x) = h \in P[x]$. Παρατηρήστε ότι αν $P = \mathbb{Q}$ τότε εφαρμόζω τον αλγόριθμο της διαίρεσης πολυωνύμων στο $\mathbb{Z}[x]$ και $\mathbb{Q}[x]$.

3. Ο αριθμός των πρωταρχικών n-οστών ριζών της μονάδας είναι ίσος με $\deg g_n$. Αν ζ είναι μια τέτοια ρίζα τότε κάθε άλλη ρίζα (και άρα και οι πρωταρχικές) είναι δυνάμεις του ζ. Άρα το ζ^i είναι πρωταρχική ρίζα αν και μόνο αν $(i, n) = 1$ και άρα το πλήθος των πρωταρχικών ριζών είναι ίσο με $\phi(n)$. □

ΠΑΡΑΤΗΡΗΣΗ 16.1. Το παραπάνω θεώρημα μας δίνει ένα τρόπο να προσδιορίσουμε αναδρομικά το $g_n(x)$ εφόσον

$$g_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} g_d(x)}.$$

Για παράδειγμα, αν p πρώτος τότε

$$g_p(x) = \frac{x^p - 1}{g_1(x)} = x^p - 1x - 1 = x^{p-1} + \ldots + x + 1.$$

Αν $K = \mathbb{Q}$ τότε

$$g_6(x) = \frac{x^6 - 1}{g_1(x)g_2(x)g_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.$$

Όμοια,

$$g_{12}(x) = \frac{x^{12} - 1}{g_1(x) \ldots g_6(x)} = \frac{x^{12} - 1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)} = x^4 - x^2 + 1.$$

Το παραπάνω γενικεύεται για $K = \mathbb{Q}$.

ΠΡΟΤΑΣΗ 16.2. Έστω F κυκλοτομική επέκταση τάξης n επί του $\mathbb{Q}$ και $g_n(x)$ το n-οστό κυκλοτομικό πολυώνυμο επί του $\mathbb{Q}$. Τότε

1. το $g_n(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.
2. $[F : \mathbb{Q}] = \phi(n)$.

3. $\Gamma(F:\mathbb{Q})$ είναι η πολλαπλασιαστική ομάδα των μονάδων στο $\mathbb{Z}_n$.

Απόδειξη.

1. Αρκεί να δείξω ότι το $g_n(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$. Έστω h ένας ανάγωγος παράγοντας του $g_n(x)$ στο $\mathbb{Z}[x]$ με $\deg h \geq 1$. Τότε $g_n(x) = f(x)h(x)$ με $f, h \in \mathbb{Z}[x]$ μονικά πολυώνυμα. Αν ζ μια ρίζα του h και p πρώτος ώστε $(p,n) = 1$ τότε το ζ είναι και ρίζα του $g_n(x)$ και άρα η ζ είναι πρωταρχική n-οστή ρίζα της μονάδας. Όμως τότε και η ζ^p είναι πρωταρχική n-οστή ρίζα της μονάδας και άρα είτε ρίζα του f είτε του h. Αν η ζ^p δεν είναι ρίζα του h αλλά του $f(x) = \sum_{i=0}^{r} a_i x^i$ και άρα το ζ είναι ρίζα του $f(x^p) = \sum_{i=0}^{r} a_i x^{ip}$. Εφόσον το h είναι ανάγωγο στο $\mathbb{Q}[x]$ και το ζ ρίζα, το h πρέπει να διαιρεί το $f(x^p)$ και άρα $f(x^p) = h(x)k(x)$ με $k(x) \in \mathbb{Q}[x]$. Από τον αλγόριθμο της διαίρεσης των πολυωνύμων στο $\mathbb{Z}[x]$ έχουμε $f(x^p) = h(x)k_1(x) - r_1(x)$ με $k_1, r_1 \in \mathbb{Z}[x]$. Λόγω της μοναδικότητας του του αλγορίθμου διαίρεσης έχουμε $k(x) = k_1(x)$. Δεδομένου ότι η κανονική προβολή $\mathbb{Z} \to \mathbb{Z}_p$ επάγει ομομορφισμό δακτυλίων $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, έχουμε $\overline{f}(x^p) = \overline{h}(x)\overline{k}(x)$ στο $\mathbb{Z}_p[x]$. Αλλά στο $\mathbb{Z}_p[x]$ έχουμε $\overline{f}(x^p) = (\overline{f}(x))^p$ και άρα $(\overline{f}(x))^p = \overline{h}(x)\overline{k}(x) \in \mathbb{Z}_p[x]$. Συνεπώς κάποιος ανάγωγος παράγοντας τους $\overline{h}$ με θετικό βαθμό πρέπει να διαιρεί το $(\overline{f}(x))^p$ και άρα $\overline{f}(x) \in \mathbb{Z}_p[x]$. Από την άλλη, εφόσον το $g_n(x)$ διαιρεί το $x^n - 1$ έχουμε

$$x^n - 1 = g_n(x)r(x) = f(x)h(x)r(x)$$

για κάποιο $r(x) \in \mathbb{Z}[x]$. Άρα στο $\mathbb{Z}[x]$ έχουμε

$$x^n - 1 = \overline{f}(x)\overline{h}(x)\overline{r}(x).$$

Εφόσον $\overline{f}$ και $\overline{h}$ έχουν κοινό παράγοντα το $x^n - 1 \in \mathbb{Z}_p[x]$ έχει πολλαπλή ρίζα. Αυτό έρχεται σε αντίθεση με το γεγονός ότι οι ρίζες του $x^n - 1$ στο $\mathbb{Z}_p[x]$ είναι διακριτές μιας και $(p,n) = 1$. Άρα το ζ^p είναι ρίζα του $h(x)$.

Αν $r \in \mathbb{Z}$ με $1 \leq r \leq n$ και $(r,n) = 1$ τότε $r = p_1^{k_1} \dots p_s^{k_s}$ με $k_i > 0$ και κάθε p_i πρώτο με $(p_i, n) = 1$. Αν εφαρμόσουμε πολλές φορές το γεγονός ότι το ζ^p είναι ρίζα του h παίρνουμε ότι και το ζ είναι ρίζα του h και τέλος ότι το ζ^r είναι ρίζα του h. Αλλά τα ζ^r για $1 \leq r \leq n$ και $(r,n) = 1$ είναι ακριβώς οι πρωταρχικές ρίζες της μονάδας. Άρα το $h(x)$ διαιρείται από το $\prod_{\substack{1 \leq r < n \\ (r,n)=1}} (x - \zeta^r) = g_n(x)$ και άρα $g(x) = h(x)$. Άρα το $g(x)$ είναι ανάγωγο.

2. Από γνωστά έχουμε ότι $F = \mathbb{Q}(\zeta)$ άρα

$$[F:\mathbb{Q}] = [\mathbb{Q}(\zeta):\mathbb{Q}] = \deg g_n = \phi(n).$$

3. Άμεσα από το 2.

ΠΑΡΑΤΗΡΗΣΗ 16.2. Ένα σπουδαίο θεώρημα του Kronecker μας λέει ότι κάθε αβελιανή επέκταση του $\mathbb{Q}$ περιέχεται σε μια κυκλοτομική επέκταση.

17 Θεμελιώδες Θεώρημα της Άλγεβρας

ΟΡΙΣΜΟΣ 17.1. Ένα διατεταγμένο σώμα είναι ένα σώμα K με μια σχέση $\leq$ τέτοια ώστε

1. $k \leq k$ για κάθε $k \in K$.
2. αν $k \leq l$ και $l \leq m$ τότε $k \leq m$ για κάθε $k, l, m \in K$.
3. αν $k \leq l$ και $l \leq k$ τότε $k = l$ για κάθε $k, l \in K$.
4. αν $k, l \in K$ τότε είτε $k \leq l$ είτε $l \leq k$.
5. αν $k, l, m \in K$ και $k \leq l$ τότε $k + m \leq l + m$.
6. αν $k, l, m \in K$ και $k \leq l$ και $0 \leq m$ τότε $km \leq lm$.

Η σχέση $\leq$ είναι μια διάταξη στο K.

ΠΑΡΑΔΕΙΓΜΑ 17.1. Τα σώματα $\mathbb{Q}, \mathbb{R}$ είναι προφανώς διατεταγμένα σώματα.

ΛΗΜΜΑ 17.1. Έστω K ένα διατεταγμένο σώμα. Για κάθε $k \in K$ έχουμε ότι $k^2 \geq 0$. Επομένως η χαρακτηριστική του K είναι μηδέν.

Απόδειξη. Αν $k \geq 0$ τότε $k^2 \geq 0$ λόγω του 6 του ορισμού. Άρα μπορούμε να υποθέσουμε ότι $k < 0$. Αν και το $-k < 0$ τότε $0 = k + (-k) < k + 0 = k$, άτοπο. Άρα $-k \geq 0$ και $k^2 = (-k)^2 \geq 0$.

Επομένως $1 = 1^2 > 0$ και συνεπώς για κάθε πεπερασμένο n ο αριθμός $n \cdot 1 = 1 + \ldots + 1 > 0$ άρα $n \cdot 1 \neq 0$. Δηλαδή το K έχει χαρακτηριστική 0. □

ΠΑΡΑΤΗΡΗΣΗ 17.1. Θυμηθείτε ότι το $\mathbb{R}$ έχει τις παρακάτω ιδιότητες.

- Το $\mathbb{R}$ είναι διατεταγμένο σώμα.
- Κάθε θετικό στοιχείο του $\mathbb{R}$ έχει τετραγωνική ρίζα στο $\mathbb{R}$.
- Κάθε πολυώνυμο περιττού βαθμού στο $\mathbb{R}$ έχει μια ρίζα στο $\mathbb{R}$.

ΛΗΜΜΑ 17.2. Έστω K σώμα χαρακτηριστικής μηδέν τέτοιο ώστε για κάποιο πρώτο p κάθε πεπερασμένη επέκταση M του K με $M \neq K$ έχει βαθμό $[M : K]$ διαιρετό με το p. Άρα κάθε πεπερασμένη επέκταση του K έχει βαθμό μια δύναμη του p.

Απόδειξη. Έστω N μια επέκταση του K. Εφόσον η χαρακτηριστική είναι μηδέν, η επέκταση είναι διαχωρίσιμη. Αν χρειάζεται, μπορούμε να περάσουμε σε μια μεγαλύτερη επέκταση, οπότε χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι η $N : K$ είναι κανονική και άρα να ισχύει η αντιστοιχία Galois. Έστω G η ομάδα Galois της $N : K$ και P μια Sylow p-υποομάδα της G για κάποιο πρώτο p. Το σταθερό σώμα της P, έστω P^*, έχει βαθμό $[P^* : K]$ ίσο με τον δείκτη της P στην G. Αυτός είναι πρώτος με το p. Όμως από υπόθεση $P^* = K$ άρα $P = G$. Συνεπώς $[N : K] = |G| = p^n$ για κάποιο n. □

ΘΕΩΡΗΜΑ 17.1. Έστω K ένα διατεταγμένο σώμα στο οποίο κάθε θετικό στοιχείο έχει τετραγωνική ρίζα και κάθε πολυώνυμο περιττού βαθμού έχει ρίζα στο K. Τότε το $K(i)$ είναι αλγεβρικά κλειστό, δηλαδή κάθε μη σταθερό πολυώνυμο του $K(i)[x]$ έχει ρίζα στο $K(i)[x]$, όπου $i^2 = -1$.

Απόδειξη. Θα δείξουμε αρχικά ότι το K δεν μπορεί να έχει πεπερασμένες επεκτάσεις περιττού βαθμού. Υποθέτουμε ότι M πεπερασμένη επέκταση του K με $[M : K] = r > 1$ με r περιττό. Έστω $a \in M \setminus K$ με ελάχιστο πολυώνυμο m. Τότε ο βαθμός τους m, $\deg m$, διαιρεί το r άρα είναι περιττός. Από την υπόθεση, το m έχει μια ρίζα στο K άρα είναι παραγοντοποιήσιμο, άτοπο διότι το m είναι ελάχιστο πολυώνυμο και άρα ανάγωγο.

Άρα κάθε πεπερασμένη επέκταση του K έχει άρτιο βαθμό. Επιπλέον, από το Λήμμα 17.1 η χαρακτηριστική του K είναι μηδέν και άρα από το Λήμμα 17.2 κάθε πεπερασμένη επέκταση του K έχει βαθμό μια δύναμη του 2.

Έστω $M \neq K(i)$ μια πεπερασμένη επέκταση του $K(i)$. Πηγαίνοντας σε μια μεγαλύτερη επέκταση αν χρειάζεται μπορούμε να υποθέσουμε ότι η $M : K(i)$ κανονική, άρα η ομάδα Galois είναι μια 2-ομάδα. Από την αντιστοιχία Galois, υπάρχει επέκταση N του $K(i)$ βαθμού $[N : K(i)] = 2$. Προφανώς, $N = K(i)(\zeta)$ όπου ζ ρίζα πολυωνύμου δευτέρου βαθμού με $\zeta^2 \in K(i)$. Αλλά, αν $a, b \in K$ με $\zeta^2 = a + bi$ τότε

$$\sqrt{a+bi} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

όπου $\sqrt{a^2+b^2}$ θετικός. Επιπλέον οι ποσότητες κάτω από τις ρίζες είναι θετικές άρα ανήκουν στο K. Άρα το $z \in K$ δηλαδή $N = K(i)$ άτοπο. Άρα $M = K(i)$ και συνεπώς το $K(i)$ δεν έχει επεκτάσεις βαθμού μεγαλύτερου του 1. Άρα το μόνα ανάγωγα πολυώνυμα στο $K(i)$ είναι πολυώνυμα βαθμού 1 και συνεπώς το $K(i)$ είναι αλγεβρικά κλειστό. □

ΠΟΡΙΣΜΑ 17.1 (Θεμελιώδες Θεώρημα της Άλγεβρας). Το σώμα $\mathbb{C}$ είναι αλγεβρικά κλειστό.

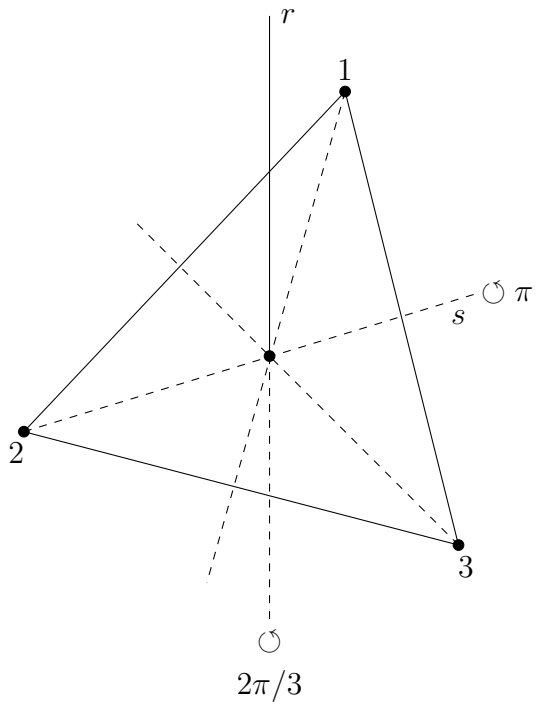
Απόδειξη. Από το προηγούμενο θεώρημα για $K = \mathbb{R}$. □

Α′ Η Διεδρική Ομάδα

Α′.1 Η πεπερασμένη Διεδρική Ομάδα

Ας θεωρήσουμε ένα κανονικό (ισόπλευρο) τρίγωνο. Πόσες συμμετρίες έχει; Με τον όρο συμμετρίες εννοούμε περιστροφικές συμμετρίες, δηλαδή με πόσους τρόπους μπορούμε να στρίψουμε το τρίγωνο ώστε να παραμείνει ίδιο (όχι σημείο προς σημείο).

Οι συμμετρίες που έχουμε για το κανονικό τρίγωνο είναι οι εξής: στροφές ως προς κάθετο άξονα που περνά από το κέντρο του τριγώνου κατά $2\pi/3$ και ανακλάσεις (στροφές κατά π) ως προς άξονα που περνά από μια κορυφή και το μέσο της απέναντι πλευράς.



Αν ονομάσουμε r την στροφή κατά $2\pi/3$ βλέπουμε ότι μπορούμε να πάρουμε τις συμμετρίες $1, r, r^2$ μιας και $r^3 = 1$.

Επίσης βλέπουμε ότι υπάρχουν συνολικά τρεις ανακλάσεις s_1, s_2, s_3 ως προς άξονες που περνούν από τις τρεις κορυφές του τριγώνου και τα μέσα των απέναντι πλευρών. Εύκολα όμως διαπιστώνουμε ότι $s_2 = rs_1$ και $s_3 = r^2 s_1$. Επίσης $s_1^2 = 1$. Αν θέσουμε $s_1 = s$ τελικά έχουμε ότι υπάρχουν 6 συμμετρίες του κανονικού τριγώνου οι

$$1, r, r^2, s, rs, r^2 s$$

οι οποίες ορίζουν ομάδα με πράξη την σύνθεση, την ομάδα συμμετριών του κανονικού τριγώνου. Την ομάδα αυτή την συμβολίζουμε με D_3.

Τα παραπάνω μπορεί να τα δει κανείς χρησιμοποιώντας και τις ομάδες μεταθέσεων. Ας ονομάσουμε τις κορυφές του κανονικού τριγώνου με $1, 2, 3$ αντίστοιχα. Βλέπουμε ότι η r αντιστοιχεί στην μετάθεση (123) και η s στην μετάθεση (13). Επιπλέον, όλες οι δυνατές συμμετρίες του τριγώνου θα είναι όλες οι δυνατές μεταθέσεις σε τρία στοιχεία, δηλαδή όλα τα στοιχεία της $S_3 = \{1, (12), (13), (23), (123), (132)\}$.

Παρατηρήστε γεωμετρικά ότι $sr = r^2 s$ (ή αλγεβρικά ότι $((13)(123) = (132)(13)$). Αυτό μαζί με το γεγονός ότι $r^3 = 1 = s^2$ μας επιτρέπει να υπολογίσουμε οποιοδήποτε άλλο στοιχείο της ομάδας συμμετριών και να δείξουμε ότι αυτά είναι ακριβώς τα 6 στοιχεία της D_3. Για παράδειγμα

$$(r^2 s)(rs) = r^2(s(rs)) = r^2((sr)s) = r^2((r^2 s)s) = r^2(r^2 s^2) = r^4 s^2 = r.$$

Χρησιμοποιώντας κανείς τους τρεις παραπάνω κανόνες μπορεί εύκολα να υπολογίσει τα 6 στοιχεία της D_3 και να κατασκευάσει τον πίνακα πολλαπλασιασμού της ομάδας.

Η διαδικασία αυτή μπορεί να γενικευτεί. Ορίζουμε D_n να είναι η ομάδα συμμετριών του κανονικού n-γώνου. Η ομάδα αυτή μπορεί να περιγραφεί με τον ίδιο τρόπο με την D_3. Πράγματι, έστω r η στροφή του n-γώνου κατά γωνία $2\pi/n$ ως προς άξονα κάθετο στο κέντρο του n-γώνου και s ανάκλαση (στροφή κατά π) ως πρός άξονα συμμετρίας που βρίσκεται πάνω στο επίπεδο του n-γώνου. Ένας τέτοιος άξονας μπορεί να περνά από δύο κορυφές του n-γώνου ή από τα μέσα δύο απέναντι πλευρών (αν το n είναι άρτιος) ή από μια κορυφή και το μέσο της απέναντι πλευράς (αν το n περιττός). Τότε τα στοιχεία της D_n είναι τα

$$1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s.$$

Προφανώς $r^n = 1$, $s^2 = 1$ και μπορούμε γεωμετρικά να επαληθεύσουμε ότι $sr = r^{n-1}s$. Η τελευταία αυτή σχέση συνήθως γράφεται $sr = r^{-1}s$ εφόσον $r^n = 1$ και άρα $r^{n-1} = r^{-1}$. Όπως και πριν, όλα τα υπόλοιπα γινόμενα υπολογίζονται με τον παραπάνω τρόπο. Άρα κάθε στοιχείο της D_n είναι της μορφής r^a ή r^as με $0 \leq a \leq 1$. Εύκολα βλέπουμε ότι

$$r^a r^b = r^k, \;\; k \equiv a + b \pmod{n}$$

$$r^a(r^b s) = r^k s, \;\; k \equiv a + b \pmod{n}$$
$$(r^a s)r^b = r^c s, \;\; c = a + (n - b) \pmod{n}$$
$$(r^a s)(r^b s) = r^c, \;\; c = a + (n - b) \pmod{n}.$$

Λέμε ότι τα r, s παράγουν την D_n και οι $r^n = s^2 = 1$ και $sr = r^{-1}s$ είναι ένα πλήρες σύνολο σχέσεων στην D_n. Επιπλέον η

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s \rangle$$

είναι μια παράσταση της D_n. Επιπλέον, η τάξη της D_n είναι $2n$.

Α΄.2 Η άπειρη Διεδρική Ομάδα

Ας πάρουμε τώρα την ευθεία των πραγματικών αριθμών πάνω στην οποία σημειώνουμε τους ακεραίους. Ας ονομάσουμε G το σύνολο όλων των συναρτήσεων από την ευθεία στον εαυτό της που διατηρούν την απόσταση και στέλνουν τους ακεραίους σε ακεραίους. Το G είναι ομάδα με πράξη την σύνθεση των συναρτήσεων και κάθε στοιχείο της G είναι είτε μεταφορά κατά ακέραια απόσταση είτε ανάκλαση με άξονα κάθετο στην ευθεία που περνά από ακέραιο, είτε ανάκλαση ως προς άξονα κάθετο στην ευθεία που περνά από το μέσο μεταξύ δύο διαδοχικών ακεραίων. Ας ονομάσουμε t την μεταφορά κατά 1. Τότε $t(x) = x+1$ και αν ονομάσουμε s την ανάκλαση ως προς άξονα κάθετο στην ευθεία, που περνά από το 0 έχουμε $s(x) = -x$. Τότε τα στοιχεία της G είναι τα

$$\begin{array}{c} \ldots, t^{-2}, t^{-1}, 1, t, t^2, \ldots \\ \ldots, t^{-2}s, t^{-1}s, s, ts, t^2s, \ldots \end{array} \qquad (*)$$

Για παράδειγμα η ανάκλαση ως προς $1/2$ είναι η $ts(x) = t(-x) = -x + 1$. Τα t, s παράγουν την G. Παρατηρήστε ότι

$$st(x) = s(x + 1) = -x - 1$$

$$t^{-1}s(x) = t^{-1}(-x) = -x - 1$$

και άρα $st = t^{-1}s$. Γνωρίζοντας ότι $s^2 = 1$ και $st = t^{-1}s$ μας επιτρέπει να πολλαπλασιάσουμε δύο οποιαδήποτε στοιχεία της λίστας $(*)$ και να δείξουμε ότι το αποτέλεσμα εξακολουθεί να ανήκει στην $(*)$. Η παραπάνω ομάδα αποτελεί γενίκευση της D_n όπου η στροφή r πεπερασμένης τάξης έχει αντικατασταθεί με την μεταφορά t που έχει άπειρη τάξη. Η G λέγεται άπειρη διεδρική ομάδα και συμβολίζεται με D_∞.