Θεωρία Galois

Θεοδώρα Θεοχαρη-Αποστολιδη

Χαρά Χαραλαμπους

Οι σημειωσεις αυτες θα συμπληρωνονται κατα τη διαρκεια των μαθηματων.

14 Ιανουαρίου 2015

Περιεχόμενα

Κεφάλαιο 4

Πεπερασμένα σώματα και εφαρμογές

4.1 Πεπερασμένα σώματα

Γνωρίζουμε ότι η χαρακτηριστική ενός σώματος ή είναι μηδέν (οπότε το σώμα είναι αναγκαστικά άπειρο) ή είναι πρώτος αριθμός. Όταν το σώμα είναι πεπερασμένο, είμαστε αναγκαστικά στη δεύτερη περίπτωση. Όταν η χαρακτηριστική του σώματος είναι μηδέν, τότε το σώμα περιέχει ισόμορφα το άπειρο σώμα $\mathbb{Q}$. Το σώμα $\mathbb{Z}_p$ είναι το ελάχιστο σώμα χαρακτηριστικής p και εμφυτεύεται σε κάθε σώμα χαρακτηριστικής p.

Έστω F μία πεπερασμένη επέκταση του $\mathbb{Z}_p$, έτσι ώστε $[F : \mathbb{Z}_p] = n$. Δηλαδή το σώμα F είναι $\mathbb{Z}_p$-διανυσματικός χώρος διάστασης n. Υπάρχει λοιπόν μία $\mathbb{Z}_p$-βάση $\{a_1, \ldots, a_n\}$ του F και $F = \{c_1a_1 + \cdots + c_na_n : \ a_i \in \mathbb{Z}_p, 1 \leq i \leq n\}$. Άρα υπάρχει ένας ισομορφισμός διανυσματικών χώρων $F \cong \mathbb{Z}_p^n$ και

$$|F| = |\mathbb{Z}_p|^n \ , \ \text{δηλαδή} \ \ |F| = p^n \ .$$

Συγκεντρώνουμε τις παρατηρήσεις αυτές στην παρακάτω πρόταση:

Πρόταση 4.1.1. *Κάθε πεπερασμένο σώμα F έχει πεπερασμένη χαρακτηριστική. Έστω p η χαρακτηριστική του F όπου p πρώτος φυσικός αριθμός. Τότε $|F| = p^n$ για κάποιο φυσικό αριθμό $n \geq 1$.*

Η πολλαπλασιαστική ομάδα $(F^*, \cdot)$ του σώματος F, όπου $F^* = F - \{0\}$ έχει $p^n - 1$ στοιχεία. Ως συνέπεια του θεωρήματος του Lagrange για τις πεπερασμένες ομάδες, γνωρίζουμε ότι κάθε στοιχείο μίας ομάδας υψούμενο στην τάξη της ομάδας ισούται με το μοναδιαίο στοιχείο στην ομάδα. Επομένως $\forall a \in F^*$ ισχύει

$$a^{p^n-1} = 1 \Rightarrow a^{p^n} = a \Rightarrow a^{p^n} - a = 0 \ ,$$

δηλαδή το a είναι ρίζα του πολυωνύμου

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x] \ .$$

Το 0 είναι και αυτό ρίζα του $f(x)$. Ισχύει λοιπόν η παρακάτω πρόταση:

Πρόταση 4.1.2. *Έστω F πεπερασμένο σώμα, $|F| = p^n$ όπου p πρώτος φυσικός αριθμός. Κάθε στοιχείο του F είναι ρίζα του πολυωνύμου $f(x) = x^{p^n} - x$ και F είναι σώμα ανάλυσης του $f(x)$.*

Θα αποδείξουμε τώρα ότι για κάθε φυσικό αριθμό $n > 1$ και για κάθε πρώτο φυσικό πρώτο αριθμό pυπάρχει ένα σώμα F με p^n στοιχεία. Η χαρακτηριστική του F θα είναι βέβαια p. Έστω $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Αφού $f'(x) = -1 \neq 0$ έπεται ότι $f(x)$ είναι διαχωρίσιμο. Από το Θεώρημα του Kronecker υπάρχει μία επέκταση L του $\mathbb{Z}_p$ που είναι σώμα ανάλυσης του $f(x) = x^{p^n} - x$. Θεωρούμε λοιπόν το σύνολο των ριζών M του $f(x)$ στο L, δηλαδή

$$M = \{a \in L : \ a^{p^n} = a\} \ .$$

Το M είναι υπόσωμα του L. Πράγματι αν $a, b \in M$ τότε αφού p διαιρεί $\binom{p^n}{i}$ για $1 \leq i \leq p^n - 1$, από το δυωνυμικό θεώρημα (ακόμα και για $p = 2$) προκύπτει ότι

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b \Rightarrow a - b \in M \ .$$

Ακόμη, αν $a, b \in M$, $b \in M - \{0\}$ τότε

$$(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1} \Rightarrow ab^{-1} \in M \ .$$

Άρα όντως M είναι υπόσωμα του L. Το πλήθος των στοιχείων του M είναι το πλήθος των διακεκριμένων ριζών του $f(x)$ που είναι ακριβώς p^n αφού $f(x)$ είναι διαχωρίσιμο. Άρα M είναι το ζητούμενο σώμα. Τα παραπάνω λοιπούν στοιχειοθετούν απόδειξη για το παρακάτω θεώρημα:

Θεώρημα 4.1.3. *Για κάθε πρώτο αριθμό p και για κάθε φυσικό αριθμό $n > 1$ υπάρχει πεπερασμένο σώμα με p^n στοιχεία.*

Παραδείγματα 4.1.4.

- Θα κατασκευάσουμε ένα σώμα με 4 στοιχεία. Έστω F ένα σώμα με $|F| = 4 = 2^2$. Είναι φανερό ότι η χαρακτηριστική του F είναι 2 και ότι το F είναι επέκταση του $\mathbb{Z}_2$ βαθμού 2. Έστω ακόμη ότι $F = \{0, 1, a, b\}$. Παρατηρούμε ότι το στοιχείο $a + 1 \in F$ και ότι $a + 1 = b$. Πράγματι αν $a + 1 = a$ τότε $1 = 0$, αδύνατον. Αν $a + 1 = 1$ τότε $a = 0$ αδύνατον. Αν $a + 1 = 0$ τότε $a = -1$ άρα $a = 1$ αδύνατον επίσης. Έτσι μπορούμε να βρούμε τον πίνακα πολλαπλασιασμού της προσθετικής ομάδας $(F, +)$:

	0	1	a	$a+1=b$
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
$b = a + 1$	b	a	1	0

  Η πολλαπλασιαστική ομάδα $(F^*, \cdot)$ του F έχει τρία στοιχεία, άρα είναι κυκλική και παράγεται είτε από το a είτε από το b. Έτσι $F^* = \{1, a, a^2 = b\}$. Ο πίνακας πολλαπλασιασμού της $(F^*, \cdot)$ είναι

	1	a	$a^2=b$
1	1	a	b
a	a	b	1
$b = a^2$	b	1	a

  .

  Παρατηρούμε ακόμη ότι αφού $a^2 = b$ έπεται ότι

$$a^2 = a + 1 \Rightarrow a^2 - a - 1 = 0 \Rightarrow a^+a + 1 = 0 \ ,$$

  αφού $1 = -1$ στον $\mathbb{Z}_2$. Δηλαδή το a είναι ρίζα του πολυωνύμου $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Όμως $x^2 + x + 1$ είναι ανάγωγο, βλ. Παράδειγμα **;;**. Άρα $F = \mathbb{Z}_2(a)$ και $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^2 + x + 1$. Οι ρίζες του $x^2 + x + 1$ είναι a, $a^2 = a + 1$.

- Έστω $x^8 - x = x^{2^3} - x \in \mathbb{Z}_2[x]$ και F το σώμα με 8 στοιχεία που κατασκευάζεται σύμφωνα με το Θεώρημα 4.1.3. Θα μελετήσουμε τη δομή του F. Παρατηρούμε καταρχήν ότι η πολλαπλασιαστική ομάδα $(F^*, \cdot)$ του F έχει 7 στοιχεία. Αφού 7 είναι πρώτος F^* είναι κυκλική ομάδα και μάλιστα κάθε στοιχείο $1 \neq b \in F^*$ παράγει την F^*. Έπεται ότι αν $0, 1 \neq b \in F$ τότε κάθε μη μηδενικό στοιχείο του F προκύπτει ως κάποια δύναμη του b και επομένως $F = Z_2(b)$, $0, 1 \neq b \in F$. Παρατηρούμε επίσης ότι $[F : \mathbb{Z}_2] = 3$. Η ανάλυση του $x^8 - x$ σε γινόμενο αναγώγων πολυωνύμων στο $\mathbb{Z}_2[x]$ είναι:

$$x^8 - x = x^8 + x = x(x + 1)(x^3 + x^2 + 1)(x^3 + x + 1) \ .$$

Έστω $a \in F$ ρίζα του x^3+x^2+1. Δηλαδή $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^3+x^2+1$ και $\mathbb{Z}_2(a) = F$. Τα στοιχεία $1, a, a^2$ είναι $\mathbb{Z}_2$-βάση του F. Αυτό σημαίνει ότι

$$F = \{c_0 + c_1 a + c_2 a^2 : \ a_i \in \mathbb{Z}_2, 0 \leq i \leq 2\}$$

$$= \{0, 1, a, 1+a, a^2, 1+a^2, a+a^2, 1+a+a^2\} \ .$$

Συγκεκριμένα αφού $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^3+x^2+1$ έπεται ότι

- $a^3 = a^2 + 1$,
- $a^4 = aa^3 = a^2 + a + 1$
- $a^5 = a^2 a^3 = a + 1$,
- $a^6 = aa^5 = a^2 + a$,
- $a^7 = 1$.

Οι ρίζες του x^3+x^2+1 είναι οι a, a^2, a^4 ενώ οι ρίζες του x^3+x+1 είναι οι a^3, a^5, a^6. Η αντίστοιχη ανάλυση μπορεί να γίνει και για $a \in F$ ρίζα του x^3+x+1 και επαφίεται στον αναγνώστη.

- Έστω τώρα F σώμα με $2^4 = 16$ στοιχεία. Θα δείξουμε ότι υπάρχει $a \in F$ έτσι ώστε $F = \mathbb{Z}_2(a)$. Πράγματι, αρκεί να δείξουμε ότι υπάρχει ένα στοιχείο $a \in F^*$ έτσι ώστε η τάξη του a στην πολλαπλασιαστική ομάδα F^* να είναι 15. Θα προσπαθήσουμε λοιπόν να μετρήσουμε τον αριθμό των στοιχείων του F^* με τάξη μικρότερη του 15. Σύμφωνα με το Θεώρημα του Lagrange, τα στοιχεία αυτά του F^* θα έχουν τάξη 5, 3 ή 1. Αφού όμως

  - 1) τα στοιχεία με τάξη 5 είναι ρίζες του πολυωνύμου $x^5 - 1$
  - 2) ένα πολυώνυμο βαθμού n πάνω από το σώμα F έχει το πολύ n ρίζες και
  - 3) το 1 είναι ρίζα του $x^5 - 1$ και 1 έχει τάξη 1,

  έπεται ότι υπάρχουν το πολύ 4 στοιχεία με τάξη 5 στο F^*. Αντίστοιχα υπάρχουν το πολύ 2 στοιχεία του F^* με τάξη 3. Υπάρχει βέβαια ακριβώς ένα στοιχείο με τάξη 1. Δηλαδή υπάρχουν το πολύ 7 στοιχεία στο F^* με τάξη μικρότερη του 15. Έπεται ότι υπάρχουν τουλάχιστον $15 - 7 = 8$ στοιχεία στο F^* με τάξη 15. Έστω a ένα τέτοιο στοιχείο. Άρα $F^* = \langle a \rangle$ και επομένως $F = \mathbb{Z}_2(a)$.

  Παρατηρούμε επίσης ότι γενικότερα για κάθε κυκλική ομάδα $G = \langle a \rangle$ έτσι ώστε $|G| = 15$ ισχύουν τα εξής:

- $1 \leq n \leq 14$ και $(n, 15) = 1$ τότε a^n έχει και αυτό τάξη 15. Δηλαδή υπάρχουν $\phi(15) = 8$ στοιχεία με τάξη 15 που προκύπτουν ως δυνάμεις του a.
- αν $1 \leq n \leq 14$ και $(n, 15) = 3$ τότε a^n έχει τάξη 5. Υπάρχουν 4 ($\phi(5)$) τέτοια n και $\langle a^3 \rangle = \langle a^6 \rangle = \langle a^9 \rangle = \langle a^{12} \rangle$. Πράγματι αφού $15 = 5 \cdot 3$ αν ξεκινήσουμε με $n = 3$, αρκεί στη συνέχεια να θεωρήσουμε τα πολλαπλάσια $3k$ όπου $1 \leq k \leq 5$, $(k, 5) = 1$.
- αν $1 \leq n \leq 14$ και $(n, 15) = 5$, τότε a^n έχει τάξη 3. Υπάρχουν 2 τέτοια n: $n = 5$, $n = 10$. Δηλαδή $2 = \phi(3)$. Είναι επίσης φανερό ότι $\langle a^5 \rangle = \langle a^{10} \rangle$.

Άρα ισχύει η παρακάτω σχέση:

$$15 = \phi(15) + \phi(5) + \phi(3) + \phi(1) \ .$$

4.2 Πρωταρχικά στοιχεία και πεπερασμένα σώματα

Θα γενικεύσουμε τις παρατηρήσεις που κάναμε στα προηγούμενα παραδείγματα. Έστω $\phi : \mathbb{N} \to \mathbb{N}$, η γνωστή συνάρτηση του Euler. Από τη βασική Θεωρία Ομάδων γνωρίζουμε ότι ισχύει το εξής:

Πρόταση 4.2.1. *Έστω $C = \langle a \rangle$ μία κυκλική ομάδα τάξης $n < \infty$. Τότε $C = \langle a^k \rangle$ ακριβώς όταν $(k, n) = 1$ και άρα το πλήθος των στοιχείων που παράγουν την C είναι $\phi(n) = \{k : \ 1 \leq k \leq n, (k, n) = 1\}$. Για κάθε d που διαιρεί το n υπάρχει ακριβώς μία υποομάδα της C τάξης d.*

Αν C είναι μία κυκλική ομάδα, θα συμβολίζουμε με $g(C)$ το σύνολο των στοιχείων που παράγουν την C: όταν $|C| = m$ τότε $|g(C)| = \phi(m)$. Έστω G μία τυχαία ομάδα και C_1, C_2 δύο κυκλικές υποομάδες της G. Αν $C_1 \neq C_2$ τότε $g(C_1) \cap g(C_2) = \emptyset$. Είναι φανερό ότι ισχύει

$$G = \bigcup_C g(C) \tag{4.1}$$

όπου C διατρέχει όλες τις κυκλικές υποομάδες της G.

Θα εφαρμόσουμε τη παραπάνω σχέση σε μία ειδική περίπτωση: $G = \mathbb{Z}_n$. Έστω λοιπόν n θετικός ακέραιος και $G = \mathbb{Z}_n$. Παίρνοντας τη πληθυκότητα και από τα δύο σκέλη της εξίσωσης 4.1 βρίσκουμε ότι

$$n = \sum_C |g(C)| \tag{4.2}$$

όπου C διατρέχει όλες τις κυκλικές υποομάδες της $\mathbb{Z}_n$. Αφού για κάθε d που διαιρεί το n υπάρχει ακριβώς μία κυκλική ομάδα C έτσι ώστε $|C| = d$ και $|g(C)| = \phi(d)$ προκύπτει ότι

$$n = \sum_{d \mid n} \phi(d) \ . \tag{4.3}$$

Παρατηρούμε ότι στη γενική περίπτωση μίας ομάδας G πληθυκότητας n είναι πιθανόν να υπάρχουν παραπάνω από μία κυκλικές ομάδες τάξης d όπου d διαιρεί το n ή και καμία. Παρακάτω αποδεικνύουμε το αντίστροφο της Πρότασης 4.2.1 χρησιμοποιώντας τις σχέσεις 4.1 και 4.3.

Θεώρημα 4.2.2. *Μία ομάδα G τάξης n είναι κυκλική αν και μόνο αν για κάθε διαιρέτη d του n υπάρχει το πολύ μία κυκλική υποομάδα τάξης d.*

Απόδειξη. Αν η G είναι κυκλική τότε το συμπέρασμα προκύπτει από την Πρόταση 4.2.1. Υποθέτουμε αντίστροφα ότι για κάθε διαιρέτη d του n υπάρχει το πολύ μία κυκλική υποομάδα τάξης d. Άρα όλα τα στοιχεία που έχουν τάξη d (αν υπάρχουν), παράγουν την ίδια υποομάδα και έτσι στη σχέση 4.2 μπορούμε ισοδύναμα να προσθέσουμε ως προς d, τους διαιρέτες του n. Επίσης αν υπάρχει κυκλική υποομάδα C της G τάξης d, τότε όπως είδαμε $|g(C)| = \phi(d)$. Άρα

$$n = \sum_{\substack{d \mid n, \\ |C| = d}} \phi(d)$$

όπου C είναι κυκλική ομάδα (αν υπάρχει). Εάν λοιπόν για κάποιο d δεν υπάρχει κάποια κυκλική υποομάδα τάξης d ο όρος $\phi(d)$ δε θα εμφανίζεται στο παραπάνω άθροισμα. Όμως από τη σχέση 4.3, για να επιτευχθεί η ισότητα προκύπτει ότι για κάθε d διαιρέτη του n υπάρχει ακριβώς μία κυκλική υποομάδα της G τάξης d. Αυτό συμβαίνει και για $d = n$, δηλαδή η G είναι κυκλική. □

Έτσι θα οδηγηθούμε στο επόμενο θεώρημα.

Θεώρημα 4.2.3. *Κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος F είναι κυκλική.*

Απόδειξη. Έστω G μία υποομάδα της $(F^*, \cdot)$ τάξης n και $d|n$. Αν C είναι μία κυκλική υποομάδα της G τάξης d τότε από το θεώρημα του Lagrange $c^d = 1, \forall\, c \in C$. Αν υπήρχε και δεύτερη κυκλική υποομάδα της G τάξης d τότε θα υπήρχαν τουλάχιστον $d+1$ στοιχεία x της G που ικανοποιούν την εξίσωση $x^d = 1$. Όμως το πολυώνυμο $x^d - 1$ έχει το πολύ d ρίζες σε ένα σώμα. Άρα υπάρχει το πολύ μία κυκλική υποομάδα τάξης d της G για κάθε d διαιρέτη του n. Από το Θεώρημα 4.2.2 προκύπτει ότι η G είναι κυκλική. □

Πόρισμα 4.2.4. *Αν F είναι ένα πεπερασμένο σώμα τότε η $(F^*, \cdot)$ είναι κυκλική ομάδα και $F = \mathbb{Z}_p(a)$ για κάποιον πρώτο p και για κάποιο στοιχείο a.*

Το παράγον στοιχείο της πολλαπλασιαστικής ομάδας $(F^*, \cdot)$ λέγεται *πρωταρχικό στοιχείο* του F. Σημειώνουμε ότι στη γενική περίπτωση δεν είναι γνωστή μία μέθοδος προσδιορισμού πρωταρχικών στοιχείων.

Παραδείγματα 4.2.5.

- Το $\overline{2}$ είναι πρωταρχικό στοιχείο του $\mathbb{Z}_{11}$.
- Το πολυώνυμο $f(x) = x^2 - 2$ είναι ανάγωγο πάνω από το $\mathbb{Z}_5$, αφού δεν έχει ρίζες στο $\mathbb{Z}_5$. Έστω $\Bbbk$ ένα σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Z}_5$. Αν $a \in \Bbbk$ είναι μία ρίζα του $f(x)$ τότε η άλλη ρίζα του $f(x)$ είναι το $-a$. Έπεται ότι $\Bbbk = \mathbb{Z}_5(a)$ και ότι $|K| = 25$. Τα στοιχεία του $\Bbbk$ είναι της μορφής $k + la$, όπου $k, l \in \mathbb{Z}_5$. Παρατηρούμε ότι a δεν είναι πρωταρχικό αφού $a^2 = 2$. Δεν είναι δύσκολο όμως να δείξει κανείς υπολογίζοντας διαδοχικά τις δυνάμεις του $b = \overline{2} + a$ ότι b είναι πρωταρχικό. Είναι φανερό ότι $\Bbbk = \mathbb{Z}_5(b)$.

Σημειώνουμε την παρακάτω χρήσιμη πρόταση.

Πρόταση 4.2.6. *Έστω $\Bbbk$ πεπερασμένο σώμα με p^n στοιχεία, a πρωταρχικό στοιχείο του K. Τότε το a είναι ρίζα ενός αναγώγου πολυωνύμου βαθμού n.*

Απόδειξη. Αφού $\Bbbk = \mathbb{Z}_p(a)$ έπεται ότι ο βαθμός $[\Bbbk : \mathbb{Z}_p]$ είναι ίσος με το βαθμό του $f(x) = \mathrm{irr}_{(\mathbb{Z}_p, a)}(x)$. Μιας και

$$|K| = |\mathbb{Z}_p|^{[\Bbbk : \mathbb{Z}_p]}$$

έπεται ότι $\deg f(x) = n$. □

Στη συνέχεια θα υπολογίσουμε την ομάδα Galois $\mathrm{Gal}(\Bbbk/\mathbb{Z}_p)$.

Θεώρημα 4.2.7. *Έστω $\Bbbk$ πεπερασμένο σώμα με p^n στοιχεία.*

$$\mathrm{Gal}(\Bbbk/\mathbb{Z}_p) \cong \mathbb{Z}_n$$

Απόδειξη. Έστω a πρωταρχικό στοιχείο του $\Bbbk$, $f(x) = \mathrm{irr}_{(\mathbb{Z}_p, a)}(x)$ και $G = \mathrm{Gal}(\Bbbk/\mathbb{Z}_p)$. Σύμφωνα με την Πρόταση 4.2.6 $\deg f(x) = n$. Άρα το $\Bbbk$ περιέχει το πολύ n ρίζες του $f(x)$. Αφού το σώμα μας έχει χαρακτηριστική p δεν γνωρίζουμε a priori ότι $f'(x) \neq 0$ και ότι $f(x)$ είναι διαχωρίσιμο. Έτσι δεν μπορούμε να χρησιμοποιήσουμε το Πόρισμα 3.3.3 για να συμπεράνουμε ότι $|G| = [\Bbbk : \mathbb{Z}_p] = n$. Παρατηρούμε όμως ότι αν $\sigma \in G$ τότε σ καθορίζεται πλήρως από το $\sigma(a)$. Πράγματι το τυχαίο μη μηδενικό στοιχείο του K είναι δύναμη

του a και $\sigma(a^i) = \sigma(a)^i$. Αφού το $\sigma(a)$ είναι ρίζα του $f(x)$, $\deg f(x) = n$, και $f(x)$ έχει το πολύ n διαφορετικές ρίζες, έπεται ότι $\sigma(a)$ μπορεί να ορισθεί το πολύ με n διαφορετικούς τρόπους. Άρα

$$|G| \leq n \ . \tag{4.4}$$

Στη συνέχεια θα δείξουμε ότι όχι μόνο $|G| = n$ αλλά και ότι η ομάδα G είναι κυκλική, προσδιορίζοντας έναν από τους γεννήτορες της G. Η συνάρτηση

$$\sigma : \ \Bbbk \to \Bbbk, \quad b \mapsto b^p$$

ανήκει στην G, δηλαδή είναι αυτομορφισμός του $\Bbbk$ που διατηρεί τα στοιχεία του $\mathbb{Z}_p$ σταθερά. Πράγματι αφού η πολλαπλαστιακή ομάδα $(\mathbb{Z}_p - \{0\}, \cdot)$ έχει $p-1$ στοιχεία έπεται ότι $\forall c \in \mathbb{Z}_p - \{0\}$, $c^{p-1} = 1$ και άρα $c^p = c$, $\forall c \in \mathbb{Z}_p$. Άρα τα στοιχεία του $\mathbb{Z}_p$ απεικονίζονται στον εαυτό τους. Εύκολα μπορεί να ελεγχθεί ότι η σ είναι ομομορφισμός δακτυλίων και ότι ο πυρήνας της είναι τετριμμένος. Άναγκαστικά αφού το σώμα $\Bbbk$ είναι πεπερασμένο ο μονομορφισμός σ είναι και επιμορφισμός, δηλαδή αυτομορφισμός του $\Bbbk$. Συμπεραίνουμε λοιπόν ότι $\sigma \in G$. Ακόμα τα στοιχεία $\sigma, \sigma^2, \ldots, \sigma^n$ είναι διακεκριμένα στοιχεία της G. Διαφορετικά για κάποιο $i < n$ θα είχαμε ότι $\sigma^i = \mathrm{id}_{\Bbbk}$ και $\forall b \in \Bbbk$ θα ίσχυε ότι

$$\sigma^i(b) = b \Rightarrow b^{p^i} = b \Rightarrow b^{p^i} - b = 0 \ .$$

Δηλαδή $\forall b \in \Bbbk$ θα ήταν ρίζα του πωλυωνύμου $x^{p^i} - x$ και αφού $|\Bbbk| = p^n$ ενώ $\deg x^{p^i} - x = p^i < p^n$ που είναι αδύνατον. Άρα $|\langle\sigma\rangle| \geq n$ και αφού $\langle\sigma\rangle \subset G$ έπεται ότι $|G| \leq n$. Συνδυάζοντας την ανισότητα της σχέσης 4.4 προκύπτει ότι $|G| = n$ και ότι $G = \langle\sigma\rangle$. Επομένως η G είναι κυκλική τάξης n, άρα είναι ισόμορφη με την $(\mathbb{Z}_n, +)$. □

Είδαμε ότι όταν $|\Bbbk| = p^n$, p πρώτος, τότε ο $\mathbb{Z}_p$-αυτομορφισμός του $\Bbbk$

$$\sigma : \Bbbk \to \Bbbk, \quad b \mapsto b^p$$

είναι γεννήτορας της $\mathrm{Gal}(\Bbbk/\mathbb{Z}_p)$. Ο αυτομορφισμός αυτός λέγεται αυτομορφισμός του Frobenius.

4.3 Πρωταρχικές ρίζες της μονάδας και πεπερασμένα σώματα

Θα ξεκινήσουμε με έναν ορισμό:

$$\mathbb{Z}_n^\sharp = \{\overline{a} \in \mathbb{Z}_n : \ (a, n) = 1\} \ .$$

Είναι εύκολο να δει κανείς ότι $\mathbb{Z}_n^\sharp$ είναι ομάδα και ότι $|\mathbb{Z}_n^\sharp| = \phi(n)$.

Παράδειγμα 4.3.1. $\mathbb{Z}_8^\sharp = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ ενώ $\phi(8) = 4$. Παρατηρούμε ότι $\mathbb{Z}_8^\sharp$ δεν είναι κυκλική αφού η τάξη των $\overline{3}$, $\overline{5}$, $\overline{7}\}$ είναι ίση με 2.

Πρόταση 4.3.2. *Όταν p πρώτος τότε $\mathbb{Z}_p^\sharp$ είναι κυκλική ομάδα.*

Απόδειξη. $\mathbb{Z}_p^\sharp$ είναι πολλαπλασιαστική υποομάδα του σώματος $\mathbb{Z}_p$. Το συμπέρασμα έπεται άμεσα από το Θεώρημα 4.2.3. □

Είναι επίσης φανερό ότι αν $\Bbbk$ είναι ένα σώμα και n ένας θετικός ακέραιος έτσι ώστε η χαρακτηρηστική του $\Bbbk$ να μη διαιρεί το n τότε το πολυώνυμο $f(x) = x^n - 1 \in \Bbbk[x]$ είναι διαχωρίσιμο. Σε αυτή τη περίπτωση έστω E ένα σώμα ανάλυσης του πολωνύμου $f(x)$. Το σύνολο των n ριζών του $f(x)$ είναι υποομάδα της πολλαπλασιαστικής ομάδας του $E - \{0\}$ και θα το καλούμε *ομάδα των n-ριζών της μονάδας πάνω από το σώμα* $\Bbbk$. Έτσι σύμφωνα με το Θεώρημα 4.2.3 έπεται ότι η υποομάδα αυτή είναι κυκλική. Ένα παράγον στοιχείο αυτής της ομάδας λέγεται *πρωταρχική ρίζα της μονάδας πάνω* από το $\Bbbk$.

Παράδειγμα 4.3.3. Το στοιχείο $e^{2\pi i/n}$ είναι πρωταρχική n-ρίζα της μονάδας πάνω από το $\mathbb{Q}$.

Θεώρημα 4.3.4. *Έστω $\Bbbk$ ένα σώμα έτσι ώστε η χαρακτηρηστική του K να μη διαιρεί το n, $f(x) = x^n - 1 \in \Bbbk[x]$ και L σώμα ανάλυσης του $f(x)$. Η ομάδα* $\mathrm{Gal}(L/\Bbbk)$ *είναι ισόμορφη με μία υποομάδα της $\mathbb{Z}_n^\sharp$.*

Απόδειξη. Έστω $G = \mathrm{Gal}(L/\Bbbk)$, ω μία πρωταρχική n-ρίζα της μονάδας στο L. Έπεται ότι το $L = \Bbbk(\omega)$. Αφού το σύνολο των n-ριζών της ομάδας στο L είναι η κυκλική ομάδα $\langle\omega\rangle$ έπεται ότι αν $\sigma \in G$ τότε $\sigma(\omega) = \omega^i$ για κάποιο $i \in \{1, \ldots, n\}$. Όμως

$$\tau = \sigma|_{\langle\omega\rangle} : \langle\omega\rangle \to \langle\omega\rangle$$

είναι ισομορφισμός ομάδων αφού είναι μονομορφισμός πεπερασμένης ομάδας. Επομένως το ω^i είναι επίσης παράγον στοιχείο της $\langle\omega\rangle$ αφού $\mathrm{Im}\tau = \langle\omega^j\rangle$. Άρα σύμφωνα με την Πρόταση 4.2.1 $(i, n) = 1$. Θεωρούμε τώρα την απεικόνιση

$$\psi : G \to \mathbb{Z}_n^\sharp, \quad \sigma \mapsto \overline{i}, \text{ όπου } \sigma(\omega) = \omega^i .$$

Είναι εύκολο να αποδειχθεί ότι η ψ είναι ομομορφισμός ομάδων. Ακόμη $\ker\psi = \{\sigma \in G : \overline{i} = \overline{1}\} = \{\sigma \in G : \sigma(\omega) = \omega\} = \{\mathrm{id}_L\}$ και η ψ είναι μονομορφισμός. □

Παράδειγμα 4.3.5. Έστω $\omega = e^{2\pi i/p}$ όπου p πρώτος. Έχουμε δει ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = \Phi_p(x) = x^{p-1} + \cdots + x + 1$. Άρα

$$|\,\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = p - 1 .$$

Σύμφωνα με το Θεώρημα 4.3.4 η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι υποομάδα της $\mathbb{Z}_p^\sharp$. Αφού $|\mathbb{Z}_p^\sharp| = p-1$ έπεται ότι

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_p^\sharp \ .$$

Σύμφωνα με τη Πρόταση 4.3.2 η ομάδα $\mathbb{Z}_p^\sharp$ είναι κυκλική άρα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι κυκλική ομάδα.

Θα εξετάσουμε στη συνέχεια το πολυώνυμο $f(x) = x^n - a \in \Bbbk[x]$ ως εφαρμογή των προηγουμένων, όπου η χαρακτηριστική του $\Bbbk$ δεν διαιρεί το n. Έστω ότι $\Bbbk$ περιέχει ω, μία πρωταρχική n-ρίζα της μονάδας. Έστω ακόμη L ένα σώμα ανάλυσης του $f(x)$. Θα εξετάσουμε την ομάδα $G = \mathrm{Gal}(L/\Bbbk)$. Οι ρίζες του $f(x)$ είναι οι $b, b\omega, \cdots, b\omega^{n-1}$ όπου b είναι μία ρίζα του $f(x)$. Έπεται ότι $L = \Bbbk(b)$. Αν σ είναι ένα στοιχείο της G τότε $\sigma(b) = b\omega^i$ για κάποιο i αφού το $\sigma(b)$ πρέπει να είναι ρίζα του $f(x)$. Έτσι το σ προσδιορίζεται από τον εκθέτη i. Θεωρούμε την αντιστοιχία

$$\psi : \ G \to \mathbb{Z}_n, \quad \sigma \mapsto \bar{i} \ .$$

Παρατηρούμε ότι αν

$$\sigma, \tau \in G \ \psi(\sigma) = \psi(\tau) \Rightarrow \sigma(b) = \tau(b) \ ,$$

δηλαδή η ψ είναι αμφιμονότιμη συνάρτηση. Είναι δε φανερό ότι η ψ είναι μορφισμός ομάδων. Άρα η G εμφυτεύεται στην $\mathbb{Z}_n$.

Έστω τώρα ότι $f(x)$ είναι ανάγωγο στο $\Bbbk[x]$. Τότε $\mathrm{irr}_{(\Bbbk,b)}(x) = f(x)$ και $|G| = [L:\Bbbk] = \deg f(x) = n$. Άρα G είναι ισόμορφη με την $\mathbb{Z}_n$. Αντίστροφα αν η G είναι ισόμορφη με την $\mathbb{Z}_n$ και ψ είναι επιμορφισμός, τότε η πρώτη παρατήρηση που κάνουμε είναι ότι όλες οι ρίζες του $f(x)$ είναι διακεκριμένες. Θα δείξουμε ότι $f(x)$ είναι ανάγωγο. Έστω λοιπόν ότι

$$f(x) = g(x)h(x), \ g(x), h(x) \in \Bbbk[x], \ (g(x), h(x)) = 1 \ .$$

Χωρίς περιορισμό της γενικότητας έστω ότι $g(b) = 0$ και $h(b\omega^i) = 0$ για κάποιο i. Αφού η ψ είναι επιμορφισμός, έπεται ότι υπάρχει $\sigma \in G$ έτσι ώστε $\sigma(b) = b\omega^i$. Αφού $g(b) = 0$, έπεται ότι $\mathrm{irr}_{(\Bbbk,b)}(x)$ διαιρεί το $g(x)$. Σύμφωνα με τη Πρόταση **;;** έπεται ότι

$$\mathrm{irr}_{(\Bbbk,\sigma(b))}(x) = \mathrm{irr}_{(\Bbbk,b)}(x).$$

Άρα $\mathrm{irr}_{(\Bbbk,b)}(x)$ διαιρεί τον μέγιστο κοινό διαιρέτη $(g(x), h(x))$ το οποίο είναι αδύνατον. Αποδείξαμε λοιπόν ότι:

Θεώρημα 4.3.6. *Αν το σώμα $\Bbbk$ περιέχει μία πρωταρχική n-ρίζα της μονάδας και L είναι σώμα ανάλυσης του $f(x) = x^n - a \in \Bbbk[x]$ τότε η $\mathrm{Gal}(L/\Bbbk)$ εμφυτεύεται στην $(\mathbb{Z}_n, +)$. Η $\mathrm{Gal}(L/\Bbbk)$ είναι ισόμορφη με την $\mathbb{Z}_n$ αν και μόνο αν το $f(x)$ είναι ανάγωγο.*

Το Θεώρημα αυτό μας οδηγεί στο επόμενο συμπέρασμα:

Πόρισμα 4.3.7. *Έστω p πρώτος φυσικός αριθμός, $\Bbbk$ σώμα που περιέχει μία p-ρίζα της μονάδας, $a \in \Bbbk[x]$. Αν $x^p - a$ δεν είναι ανάγωγο στο $\Bbbk[x]$ τότε $x^p - a$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\Bbbk[x]$.*

Απόδειξη. Έστω L σώμα ανάλυσης του $x^p - a$. Είδαμε ότι $\mathrm{Gal}(L/\Bbbk)$ εμφυτεύεται στο $\mathbb{Z}_p$. Άρα υπάρχουν ακριβώς δύο περιπτώσεις. Η πρώτη είναι $\mathrm{Gal}(L/\Bbbk) \cong \{0\}$ και η δεύτερη είναι $\mathrm{Gal}(L/\Bbbk) \cong \mathbb{Z}_p$. Η πρώτη περίπτωση είναι δυνατή μόνο όταν $L = \Bbbk$. Σύμφωνα με το Θώρημα 4.3.6 η δεύτερη περίπτωση ισχύει ακριβώς όταν $x^p - a$ είναι ανάγωγο. □

4.4 Επιλυσιμότητα με ριζικά

Είδαμε ότι τα πολυώνυμα του $\mathbb{Q}[x]$ με βαθμό ≤ 4 επιλύονται με ριζικά. Δηλαδή για αυτά τα πολυώνυμα, οι ρίζες τους δίνονται από έναν τύπο που εμπεριέχει μόνο τις συνήθεις πράξεις της πρόσθεσης, πολλαπλασιασμού και της εξαγωγή ριζών.

Υπάρχει και η έννοια της επιλυσιμότητας μίας ομάδας. Θα δώσουμε τον ορισμό και κάποιες σχετικές παρατηρήσεις που θα επιτρέψουν την σύνδεση αυτών των εννοιών.

Ορισμός 4.4.1. *Μία ομάδα G είναι επιλύσιμη αν και μόνο αν υπάρχει μία ακολουθία $G = G_0 \supset G_1 \ldots \supset G_n = \{e\}$ όπου $G_{i+1} \lhd G_i$ και G_i/G_{i+1} είναι αβελιανή ομάδα.*

Παρατηρήσεις 4.4.2. Μπορεί να αποδειχθεί ότι

- Κάθε αβελιανή ομάδα είναι επιλύσιμη.
- Αν G είναι επιλύσιμη ομάδα, τότε κάθε υποομάδα H της G είναι επιλύσιμη.
- Αν G είναι επιλύσιμη ομάδα και H είναι κανονική υποομάδα της G τότε η ομάδα G/H είναι επιλύσιμη.

Ισχύει το εξής:

Θεώρημα 4.4.3. *Έστω $f(x) \in \mathbb{Q}[x]$, E σώμα ανάλυσης του $f(x)$. Τότε το $f(x)$ επιλύεται με ριζικά αν και μόνο αν $\mathrm{Gal}(E/\mathbb{Q})$ είναι επιλύσιμη ομάδα.*

Για να μπορέσουμε να κάνουμε την σύνδεση των δύο εννοιών της επιλυσιμότητας θα χρειαστούμε τον παρακάτω ενδιάμεσο χαρακτηρισμό, που χρησιμεύει και ως επίσημος ορισμός της επιλυσιμότητας με ριζικά.

Πρόταση 4.4.4. *Έστω $f(x) \in F[x]$, E ένα σώμα ανάλυσης του $f(x)$. Το πολυώνυμο $f(x)$ επιλύεται με ριζικά αν και μόνο αν υπάρχει μία επέκταση B/E και $a_1, \ldots, a_t \in B$ έτσι ώστε αν $B_i = B_{i-1}(a_i)$ τότε $B_0 = F \subset B_1 \subset \cdots \subset B_t = B$, και $a_i^{m_i} \in B_{i-1}$ για $m_i \in \mathbb{N}$.*

Η απόδειξη της Πρότασης 4.4.4 επαφίεται ως άσκηση. Η μία κατεύθυνση είναι σχεδόν ταυτολογική. Το επόμενο παράδειγμα εξηγεί την άλλη κατεύθυνση της απόδειξης.

Θεώρημα 4.4.5. Έστω $f(x) = x^3 + q(x) + r \in \mathbb{Q}[x]$. Είναι γνωστό ότι οι ρίζες του $f(x)$ δίνονται από τους τύπους $y + z, \omega_3 y + \omega_3^2 z, \omega_3^2 y + \omega_3 z$ όπου

$$\omega_3 = e^{2\pi i/3} \ ,$$

$$y = (\frac{1}{2}\big(- r + \sqrt{r^2 + \frac{4q^3}{27}}\big))^{\frac{1}{3}}$$

και

$$z = (\frac{1}{2}\big(- r - \sqrt{r^2 + \frac{4q^3}{27}}\big))^{\frac{1}{3}} \ .$$

Παρατηρούμε ότι οι ρίζες του $f(x)$ εκφράζονται με την βοήθεια των πράξεων της πρόσθεσης και του πολλαπλασιασμού και με την εξαγωγή ριζών δευτέρου και τρίτου βαθμού. Το σώμα $L = \mathbb{Q}(y + z, \omega_3 y + om_3^2 z, \omega_3^2 y + \omega_3 z)$ είναι σώμα ανάλυσης του $f(x)$. Έστω

$$a_1 = e^{2\pi i/12}, \ a_2 = \sqrt{r^2 + \frac{4q^3}{27}}, \ a_3 = y, \ a_4 = z$$

και $B = \mathbb{Q}(a_1, \ldots, a_4)$. Είναι φανερό ότι $L \subset B$. Έστω $B_0 = \mathbb{Q}$, $B_1 = B_0(a_1)$, $B_2 = B_1(a_2)$, $B_3 = B_2(a_3)$, $B_4 = B_3(z) = L$. Αφού $\omega^3 = i$, $\omega^4 = \omega_3$ και

- $a_1^{12} \in \mathbb{Q}$,
- $a_2^2 = r^2 + \frac{4q^3}{27} \in \mathbb{Q} \subset B_1$,
- $a_3^3 = \frac{1}{2}(-r + \sqrt{r^2 + \frac{4q^3}{27}}) \in B_2$,
- $a_4^3 = \frac{1}{2}(-r - \sqrt{r^2 + \frac{4q^3}{27}}) \in B_2 \subset B_3$.

Δεν θα δώσουμε την αναλυτική απόδειξη του Θεωρήματος 4.4.3. Για την μία από τις δύο κατευθύνσεις σημειώνουμε τα εξής. Έστω $f(x) \in \mathbb{Q}[x]$ επιλύσιμο με ριζικά, E το σώμα ανάλυσης του $f(x)$ και έστω B η επέκταση της Πρότασης 4.4.4. Μπορούμε να επιλέξουμε τα a_i να είναι τέτοια ώστε m_i να είναι πρώτοι

αριθμοί και το B να είναι σώμα ανάλυσης που να περιέχει κατάλληλη πρωταρχική ρίζα της μονάδας. Τότε

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(B/\mathbb{Q})/\,\mathrm{Gal}(B/E)$$

και σύμφωνα με τις Παρατηρήσεις 4.4.2 αρκεί να αποδείξουμε ότι $\mathrm{Gal}(B/\mathbb{Q})$ είναι επιλύσιμη ομάδα. Αυτό όμως προκύπτει από το Θεμελιώδες Θεώρημα της Θεωρίας Galois, την αντιστοιχία των υποομάδων και των ενδιάμεσων σωμάτων, τις Παρατηρήσεις 4.4.2 και το Πόρισμα 4.3.7.

4.5 Κατασκευάσιμοι αριθμοί και πολύγωνα

Θεωρούμε το επίπεδο $\mathbb{R}\times\mathbb{R}$ και αρχικά σημεία το $(0,0)$, $(1,0)$. Τα εργαλεία μας είναι ο κανόνας και ο διαβήτης. Ένα σημείο του επιπέδου $\mathbb{R}\times\mathbb{R}$ είναι *κατασκευάσιμο* αν προκύπτει ως σημείο τομής ευθειών και κύκλων. Θυμίζουμε ότι για να χαράξουμε μία ευθεία με τον κανόνα πρέπει να έχουμε προσδιορίσει δύο κατασκευάσιμα σημεία της ευθείας, ενώ για να χαράξουμε έναν κύκλο με τον διαβήτη πρέπει το κέντρο του να είναι κατασκευάσιμο και να έχουμε ήδη βρεί έναν κατασκευάσιμο σημείο στη περιφέρειά του. Ένας αριθμός $a\in\mathbb{R}$ θα λέγεται *κατασκευάσιμος* αν $(a,0)$ ή $(0,a)$ είναι κατασκευάσιμο. Έστω F το σύνολο των κατασκευάσιμων αριθμών. Στην εισαγωγή και στις ασκήσεις του πρώτου κεφαλαίου, είδαμε ότι F είναι υπόσωμα του $\mathbb{R}$ και ότι αν $a\in\mathbb{R}$ και $a^2\in\mathbb{Q}$ τότε $a\in F$. Ποιοί άλλοι πραγματικοί αριθμοί είναι κατασκευάσιμοι; Αν $K\subset F$ είναι σώμα, τότε θεωρούμε $K\times K$, το *επίπεδο* του K και τα αντίστοιχα κατασκευάσιμα σημεία του επιπέδου αυτού. Παρατηρούμε τα εξής:

1. αν c είναι κατασκευάσιμος αριθμός, τότε όλα τα στοιχεία του σώματος $\mathbb{Q}(c)$ είναι κατασκευάσιμα,

2. η εξίσωση μίας ευθείας στο $\mathbb{R}\times\mathbb{R}$ που περνά από δύο κατασκευάσιμα σημεία του επιπέδου του K είναι της μορφής $ax+by+c=0$ όπου $a,b,c\in K$,

3. η εξίσωση ενός κύκλου που το κέντρο του είναι κατασκευάσιμο σημείο του επιπέδου του K και που στη περιφέρειά του έχει προσδιοριστεί κατασκευάσιμο σημείο του επιπέδου του K(δηλ. ισοδύναμα, η ακτίνα του είναι κατασκευάσιμη) είναι της μορφής $x^2+y^2+ax+by+c=0$ όπου $a,b,c\in K$.

Έστω λοιπόν ότι K είναι υπόσωμα του $\mathbb{R}$ (και του F) που αποτελείται από κατασκευάσιμους αριθμούς, ($\mathbb{Q}\subset K$). Είναι φανερό ότι η τομή δύο ευθειών με συντελεστές από το K θα δώσει σημείο που ήδη βρίσκεται στο επίπεδο

του K. Επίσης είναι εύκολο να δει κανείς ότι το πρόβλημα εύρεσης σημείου τομής δύο κύκλων ανάγεται στο πρόβλημα εύρεσης τομής ενός κύκλου και μίας ευθείας. Ένα *νέο* λοιπόν κατασκευάσιμο στοιχείο του F εκτός του K μπορεί να προκύψει μόνο από τη τομή μίας ευθείας και ενός κύκλου με συντελεστές από το K. Είναι εύκολο να δει κανείς ότι οι συντεταγμένες του(ων) σημείου(ων) τομής μίας ευθείας $ax + by + c = 0$ και ενός κύκλου $x^2 + y^2 + dx + ey + f = 0$ (αντικαθιστώντας x ή y ανάλογα), θα προκύψουν από τη λύση μίας δευτεροβάθμιας εξίσωσης ως προς μία μεταβλητή. Δηλαδή το σημείο τομής θα προκύψει με τη βοήθεια του τύπου της δευτεροβάθμιας που συμπεριέχει ένα ριζικό: $\sqrt{q}$, όπου $q \in \mathbb{R}$ αφού ο κύκλος και η ευθεία τέμνονται. Έπεται λοιπόν ότι με αυτό το τρόπο προκύπτει ένα κατασκευάσιμο σημείο εκτός του K αν και μόνο αν $q \notin K$ και άρα αν και μόνο αν $[K(q) : K] = 2$. Αποδείξαμε λοιπόν το εξής:

Θεώρημα 4.5.1. *$c \in \mathbb{R}$ είναι κατασκευάσιμο αν και μόνο αν υπάρχει μία ακολουθία σωμάτων*

$$\mathbb{Q} = K_0 \subset K_1 \cdots \subset K_t$$

έτσι ώστε $c \in K_t$ και $[K_{i+1} : K_i] = 2$, $i = 1, \ldots, t-1$

Σημειώνουμε το παρακάτω πόρισμα:

Πόρισμα 4.5.2. *Αν c είναι κατασκευάσιμο, τότε c είναι αλγεβρικό πάνω από το $\mathbb{Q}$ και το ανάγωγο πολυώνυμό του πάνω από το $\mathbb{Q}$ έχει βαθμό μία δύναμη του 2.*

Απόδειξη. Έστω ότι c είναι κατασκευάσιμο και έστω $K_0, \ldots, K_t$ όπως στο Θεώρημα 4.5.1. Αφού $[K_t : \mathbb{Q}] = 2^t$ έπεται ότι $[\mathbb{Q}(c) : \mathbb{Q}]$ διαιρεί το 2^t. Αφού $\deg \operatorname{irr}_{\mathbb{Q},c}(x) = [\mathbb{Q}(c) : \mathbb{Q}]$ το συμπέρασμα έπεται. □

Πόρισμα 4.5.3. *Μία γωνία 60° δεν μπορεί να τριχοτομηθεί με κανόνα και διαβήτη.*

Απόδειξη. Έστω ότι ήταν δυνατόν να τριχοτομηθεί η γωνία των 60°. Τότε θα ήταν δυνατόν να κατασκευασθεί ένα ορθό τρίγωνο με γωνίες 20° και 70°. Επομένως θα ήταν δυνατόν να κατασκευασθεί και ο πραγματικός αριθμός $\cos(20)$ ως πηλίκο δύο κατασκευάσιμων αριθμών. Όμως από τη τριγωνομετρία έχουμε ότι

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$$

και αφού $\cos(60^\circ) = 1/2$, έχουμε ότι $\cos(20^\circ)$ είναι ρίζα του πολυωνύμου $8x^3 - 6x - 1$. Το πολυώνυμο αυτό δεν έχει ρίζες στο $\mathbb{Q}$ και είναι ανάγωγο στο $\mathbb{Q}[x]$. Αρα $[\mathbb{Q}(\cos(20^\circ)) : \mathbb{Q}] = 3$. Έπεται ότι $\cos(20^\circ)$ δεν είναι κατασκευάσιμος αριθμός και γωνία 60° δεν μπορεί να τριχοτομηθεί με κανόνα και διαβήτη. □

Πόρισμα 4.5.4. *Δεν είναι δυνατόν να διπλασιασθεί ένας κύβος που έχει πλευρά 1, με κανόνα και διαβήτη.*

Απόδειξη. Ο διπλασιασμένος κύβος θα είχε πλευρά ίση με $a = \sqrt[3]{2}$. Το ανάγωγο πολυώνυμο του a είναι $x^3 - 2$ και $[Q(a) : Q] = 3$, άρα a δεν είναι κατασκευάσιμος αριθμός. □

Πόρισμα 4.5.5. *Δεν είναι δυνατόν να τετραγωνίσουμε τον κύκλο με ακτίνα 1, με κανόνα και διαβήτη.*

Απόδειξη. Το τετράγωνο θα είχε εμβαδό π και πλευρά $\sqrt{\pi}$. Όμως π και κατά συνέπεια και $\sqrt{\pi}$ δεν είναι αλγεβρικοί αριθμοί υπεράνω του Q και άρα είναι μη κατασκευάσιμοι. □

Θα εξετάσουμε τώρα ποιά κανονικά p-γωνα είναι κατασκευάσιμα όταν p είναι περιττός πρώτος αριθμός. Παρατηρούμε ότι αυτό το πρόβλημα είναι ισοδύναμο με τη κατασκευή του μιγαδικού αριθμού $e^{2\pi i/p}$ ως σημείο του μοναδιαίου κύκλου. Από τη θεωρία ομάδων θα χρειαστούμε την επόμενη πρόταση:

Πρόταση 4.5.6. *Έστω G μία ομάδα έτσι ώστε $|G| = 2^{2^m}$. Τότε G έχει μία κανονική σειρά με παράγοντες ομάδες τάξης 2, δηλαδή υπάρχει κανονική σειρά της G*

$$G = G_t \lhd G_{t-1} \lhd \cdots \lhd \{e\}$$

με $[G_i : G_{i-1}] = 2, i = 1, \ldots, t$.

Το επόμενο Θεώρημα φέρει το όνομα του Gauss.

Θεώρημα 4.5.7. *Αν p είναι περιττός πρώτος, τότε ένα κανονικό p-γωνο είναι κατασκευάσιμο αν και μόνο αν*

$$p = 2^{2^m} + 1,\ m \in \mathbb{N}\ .$$

Απόδειξη. Έστω p περιττός πρώτος, $\omega = e^{2\pi i/p}$. Σύμφωνα με το Θεώρημα 4.5.2, αν z είναι κατασκευάσιμο τότε $[\mathbb{Q}(z) : \mathbb{Q}]$ θα είναι μία δύναμη του 2. Αφού

$$\mathrm{irr}_{(\mathbb{Q},\omega)} = x^{p-1} + \cdots + x + 1$$

έπεται ότι $p - 1 = 2^s$ για κάποιο s. Θα πρέπει τότε και το s να είναι δύναμη του 2. Πράγματι αν υπάρχει περιττός αριθμός k τέτοιος ώστε $s = k\lambda$ τότε ο αριθμός

$$p = 2^s + 1 = (2^\lambda)^k + 1$$

έχει ως παράγοντα το $2^\lambda + 1$, αδύνατον αφού p πρώτος. Άρα $p - 1 = 2^{2^m}$ για κάποιο $m \geq 0$. Αντίστροφα αν για τον p ισχύει ότι

$$p = 2^{2^m} + 1\ m \in \mathbb{N}\ ,$$

τότε

$$|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(z):\mathbb{Q}] = p-1 = 2^{2^m} .$$

Σύμφωνα με τη Πρόταση 4.5.6 η ομάδα $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ έχει μία κανονική σειρά με παράγοντες ομάδες τάξης 2:

$$G = G_t \lhd G_{t-1} \lhd \cdots \lhd \{e\} .$$

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois έπεται ότι υπάρχει μία ακολουθία σωμάτων

$$\mathbb{Q} = K_0 \subset K_1 \cdots \subset K_t = \mathbb{Q}(\omega)$$

με $[K_{i+1} : K_i] = 2$, $i = 1, \ldots, t-1$. Άρα ω είναι κατασκευάσιμο. □

Οι πρώτοι αριθμοί της μορφής $2^{2^m}+1$ λέγονται πρώτοι αριθμοί του Fermat. Αναφέρουμε χωρίς απόδειξη το Θεώρημα που αφορά τη περίπτωση του κανονικού n-γώνου.

Θεώρημα 4.5.8. *Ένα κανονικό n-γωνο είναι κατασκευάσιμο αν και μόνο αν*

$$n = 2^s p_1 \cdots p_r,$$

για κάποιον φυσικό s, όπου $p_1, \ldots, p_r$ είναι διακεκριμένοι πρώτοι αριθμοί του Fermat.

4.6 Θεμελιώδες Θεώρημα της Άλγεβρας

Η απόδειξη που δίνουμε σε αυτήν την ενότητα για το Θεμελιώδες Θεώρημα της Άλγεβρας είναι κατά κυριότητα αλγεβρικού χαρακτήρα: χρησιμοποιεί το Θεώρημα της Μέσης Τιμής για πολυώνυμα με πραγματικούς συντελεστές, αλλά ο κύριος κορμός της σύντομη (σχετικά) απόδειξης του Θεμελιώδους Θεωρήματος της Άλγεβρας στηρίζεται στην αντιστοιχία ανάμεσα στις υποομάδες μία ομάδας Galois και τα ενδιάμεσα σώματα. Θα δεχτούμε ότι κάθε μιγαδικός αριθμός $z \in \mathbb{C}$ μπορεί να γραφεί στη μορφή $re^{i\theta}$ όπου $r \in \mathbb{R}^+$. Θα χρειαστούμε το παρακάτω αποτέλεσμα από τη Θεωρία Ομάδων το οποίο και παραθέτουμε χωρίς απόδειξη. Αναφέρουμε απλά ότι προκύπτει άμεσα από τα Θεωρήματα του Sylow.

Θεώρημα 4.6.1. *Έστω G πεπερασμένη ομάδα και έστω ότι η μέγιστη δύναμη του 2 που διαιρεί το G είναι 2^m: δηλαδή $|G| = 2^m k$, όπου $(m,k) = 1$. Τότε για κάθε $1 \le n \le m$, η G έχει μία υποομάδα H έτσι ώστε $|H| = 2^n$.*

Έστω τώρα $f(x) \in \mathbb{R}[x]$. Σύμφωνα με το Θεώρημα της Μέσης Τιμής:*εάν υπάρχουν* $a, b \in \mathbb{R}$ *έτσι ώστε* $f(a) > 0$ *και* $f(b) < 0$ *τότε υπάρχει* $c \in \mathbb{R}$ *έτσι ώστε* $f(c) = 0$. Σημειώνουμε τις παρακάτω συνέπειες:

Πρόταση 4.6.2. *Έστω* $a \in \mathbb{R}^+$. *Τότε υπάρχει* $r \in \mathbb{R}^+$ *έτσι ώστε* $r^2 = a$.

Απόδειξη. Έστω $f(x) = x^2 - a \in \mathbb{R}[x]$. Τότε $f(1 + a) = 1 + a^2 + a$ και $f(1 + a) > 0$. Ακόμη $f(0) = -a < 0$. Έπεται ότι υπάρχει r έτσι ώστε $f(r) = 0$. Αν $r < 0$ τότε $-r$ είναι επίσης ρίζα. □

Πρόταση 4.6.3. *Αν* $f(x) = ax^2 + bx + c \in \mathbb{C}[x]$ *τότε υπάρχει* $z \in \mathbb{C}$ *έτσι ώστε* $f(z) = 0$.

Απόδειξη. Οι ρίζες του $f(x)$ προκύπτουν από τον τύπο της διακρίνουσας

$$(-b \pm \sqrt{b^2 - 4c})/2a \ .$$

Αρκεί λοιπόν να δείξουμε ότι $\sqrt{z}$ έχει νόημα για κάθε $z \in \mathbb{C}$. Πράγματι, έστω ότι $z = re^{i\theta}, r \in \mathbb{R}^+$. Σύμφωνα με τη Πρόταση 4.6.2, υπάρχει $\sqrt{r} \in \mathbb{R}^+$ και άρα $w = \sqrt{r}e^{i\theta/2} \in \mathbb{C}$ και $w^2 = z$. □

Πρόταση 4.6.4. *Το σώμα* $\mathbb{C}$ *δεν έχει επέκταση βαθμού 2.*

Απόδειξη. Έστω $[E : \mathbb{C}] = 2$. Υπάρχει $a \in E \setminus \mathbb{C}$ και αναγκαστικά $E = \mathbb{C}(a)$. Έπεται ότι $\deg \mathrm{irr}_{\mathbb{C},a}(x) = 2$. Προκύπτει άτοπο από την Πρόταση 4.6.3. □

Πρόταση 4.6.5. *Έστω* $f(x) \in \mathbb{R}[x]$ *ανάγωγο. Τότε* $\deg f(x) = 2k$.

Απόδειξη. Αρκεί να αποδείξουμε ότι αν $\deg f(x)$ είναι περιττός τότε $f(x)$ έχει τουλάχιστον μία ρίζα στο $\mathbb{R}$. Παρατηρούμε ότι $c_0 + c_1x + \cdots + c_nx^n$ έχει πραγματική ρίζα αν και μόνο αν $c_0/c_n + c_1/c_nx + \cdots + x^n$ έχει πραγματική ρίζα. Έστω λοιπόν $f(x) = a_0 + a_1x + \cdots + x^n \in R[x]$ όπου $\deg f(x)$ περιττός. Θέτουμε

$$t = 1 + \sum_{i=0}^{i=n-1} |a_i|.$$

Τότε $t - 1 = \sum_{i=0}^{i=n-1} |a_i|$ και $|a_i| \leq t - 1, i = 1, \ldots, n - 1$. Άρα

$$|a_0 + a_1t + \cdots + a_{n-1}t^{n-1}| \leq (t - 1) + (t - 1)t + \cdots (t - 1)t^n =$$

$$(t - 1)(1 + t + \cdots + t^{n-1}) = t^n - 1$$

Άρα $|a_0 + a_1t + \cdots + a_{n-1}t^{n-1}| < t^n$ και

$$f(t) = (a_0 + a_1t_1 + \cdots + a_{n-1}t^{n-1}) + t^n > 0.$$

Αφού το n είναι περιττός έπεται ότι $(-t)^n = (-1)t^n < 0$ και οι προηγούμενοι υπολογισμοί οδηγούν στη σχέση $f(-t) < 0$. Σύμφωνα με το θεώρημα της μέσης τιμής $f(x)$ έχει μία πραγματική ρίζα. □

Πρόταση 4.6.6. *Έστω ότι* $\mathbb{R} \subsetneq L$ *εγκλεισμός σωμάτων και έστω ότι* $[L : \mathbb{R}] < \infty$. *Τότε* $[L : \mathbb{R}] = 2n$

Απόδειξη. Έστω $a \in L/\mathbb{R}$. Τότε από την Πρόταση 4.6.5 ο βαθμός του $\mathrm{irr}_{(\mathbb{R},a)}(x)$ πρέπει να είναι άρτιος. Έπεται ότι

$$[L : \mathbb{R}] = [L : \mathbb{R}(a)][\mathbb{R}(a) : \mathbb{R}]$$

είναι άρτιος. □

Δίνουμε έμφαση στα συμπεράσματα των Προτάσεων 4.6.4, 4.6.6. Έχουμε δείξει ως τώρα ότι δεν υπάρχει επέκταση L του C έτσι ώστε $[L : \mathbb{C}] = 2$ ενώ έχουμε επίσης δείξει ότι κάθε πεπερασμένη επέκταση του $\mathbb{R}$ πρέπει να είναι άρτιου βαθμού. Είμαστε έτοιμοι για την απόδειξη του κυρίου θεωρήματος της ενότητας.

Θεμελιώδες Θεώρημα της Άλγεβρας *Κάθε μη σταθερό πολυώνυμο του* $\mathbb{C}[x]$ *έχει μία μιγαδική ρίζα.*

Απόδειξη. Έστω $f(x) = \sum a_i x^i \in \mathbb{C}[x]$. Με $\overline{f(x)}$ συμβολίζουμε το πολυώνυμο $\sum \overline{a_i} x^i$. Παρατηρούμε ότι

$$\overline{f(x)\overline{f(x)}} = f(x)\overline{f(x)}$$

και άρα $f(x)\overline{f(x)} \in \mathbb{R}[x]$. Ακόμη παρατηρούμε ότι

$$f(z) = 0 \Leftrightarrow \overline{f(\overline{z})} = 0 \ .$$

Άρα $f(x)$ έχει μιγαδική ρίζα αν και μόνο αν $f(x)\overline{f(x)} \in \mathbb{R}[x]$ έχει μιγαδική ρίζα. Αρκεί λοιπόν να αποδείξουμε ότι το θεώρημα για πολυώνυμα με πραγματικούς συντελεστές. Αφού κάθε πολυώνυμο γράφεται μοναδικά ως γινόμενο αναγώγων, θα αποδείξουμε το θεώρημα για ανάγωγα πολυώνυμα του $\mathbb{R}[x]$.

Έστω λοιπόν $p(x) \in \mathbb{R}[x]$ ανάγωγο. Θα θεωρήσουμε το πολυώνυμο $q(x) = (x^2 + 1)p(x)$ ως στοιχείο του $\mathbb{C}[x]$ και θα πάρουμε L το σώμα ανάλυσης του $q(x)$ πάνω από το $\mathbb{C}$. Θα δείξουμε ότι $L = \mathbb{C}$ και άρα το πολυώνυμο $q(x)$ και κατά συνέπεια και το $p(x)$ διασπώνται πλήρως στο $\mathbb{C}$.

Αφού L έχει χαρακτηριστική 0, το πολυώνυμο $q(x)$ είναι διαχωρίσιμο και L είναι επέκταση Galois πάνω από το $\mathbb{C}$ και πάνω από το $\mathbb{R}$. Έστω $G = \mathrm{Gal}(L/\mathbb{R})$ και έστω ότι $|G| = 2^m k$, όπου $(2, k) = 1$. Σύμφωνα με το Θεώρημα 4.6.1 υπάρχει μία υποομάδα H της G έτσι ώστε $|H| = 2^m$. Έπεται ότι $[G : H] = k$. Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois (Ενότητα 3.5) έπεται ότι $[L^H : \mathbb{R}] = k$. Αν $k > 1$, αυτό μας οδηγεί σε άτοπο σύμφωνα με τη Πρόταση 4.6.6. Επομένως $k = 1$ και $|G| = 2^m$. Έπεται ότι και η υποομάδα

$G' = \mathrm{Gal}(L/\mathbb{C})$ της G έχει τάξη κάποια δύναμη του 2. Έστω ότι $|G'| = 2^n$ όπου $n > 0$. Σύμφωνα πάλι με το Θεώρημα 4.6.1, η ομάδα G' έχει μία υποομάδα J έτσι ώστε $|J| = 2^{n-1}$ και άρα $[G' : J] = 2$. Σύμφωνα πάλι με το Θεμελιώδες Θεώρημα της Θεωρίας Galois έπεται ότι $[L^J : \mathbb{C}] = 2$. Αυτό οδηγεί σε άτοπο σύμφωνα με τη Πρόταση 4.6.4. Άρα $n = 0$, δηλ. $|G'| = |\mathrm{Gal}(L/\mathbb{C})| = 1$ και επομένως $[L : \mathbb{C}] = 1$, δηλαδή $L = \mathbb{C}$. □

4.7 Απλές επεκτάσεις

Θεώρημα 4.7.1. *Έστω E επέκταση Galois υπεράνω του F, και L ενδιάμεσο σώμα. Τότε υπάρχει $a \in L$ έτσι ώστε $L = F(a)$.*

Απόδειξη. Αν $|F| < \infty$ τότε $|E| < \infty$. Έπεται ότι $E^* =< a >$ και επομένως $E = F(a)$.

Έστω ότι F είναι άπειρο σώμα. Αφού $[E : F] < \infty$ έπεται ότι $[L : F] < \infty$ και με απλή επαγωγή στον βαθμό $[L : F]$ βρίσκουμε ότι υπάρχουν $b_1, \ldots, b_n$ έτσι ώστε $L = F(b_1, \ldots, b_n)$: (αν $L \neq F(b_1, \ldots, b_{i-1})$ τότε υπάρχει $b_i \in L \setminus F(b_1, \ldots, b_{i-1})$, και συγκρίνουμε L με το υπόσωμα $F(b_1, \ldots, b_i)$). Αρκεί λοιπόν να αποδείξουμε το θεώρημα όταν $L = F(b, c)$.

Θα ξεκινήσουμε με τα ανάγωγα πολυώνυμα των b, c: έστω λοιπόν $f(x) \in F[x]$ το ανάγωγο πολυώνυμο με $f(b) = 0$, $b = b_1, \ldots, b_n \in E$ οι ρίζες του $f(x)$ και $f(x) = \prod(x - b_i) \in E[x]$. Αντίστοιχα έστω $g(x) \in F[x]$ το ανάγωγο πολυώνυμο με $g(c) = 0$, $c = c_1, \ldots, c_m \in E$ οι ρίζες του $g(x)$ και $g(x) = \prod(x - c_i) \in E[x]$. (Σημειώνουμε ότι οι ρίζες b_i και c_j είναι όλες απλές.)

Θεωρούμε τα $n \times m - 1$ στοιχεία

$$\frac{b_i - b}{c - c_j},$$

$i = 1, \ldots, n$, $j = 2, \ldots, m$. Αφού F άπειρο, υπάρχει $d \in F$ διαφορετικά από αυτά. Έτσι

$$d(c - c_j) \neq b_i - b \Leftrightarrow b + dc \neq b_i + dc_j, \ \forall i = 1, \ldots, n, \forall j = 2, \ldots, m.$$

Θέτουμε

$$a = b + dc \in L.$$

Από τα προηγούμενα συνεπάγεται ότι

$$a \neq b_i + dc_j$$

Θα δείξουμε ότι $F(a) = L$. Έστω $h(x) = f(a - dx) \in F(a)[x]$. Τότε $h(d) = f(a - dc) = f(b) = 0$. Επίσης για $j = 2, \ldots, m$, $h(c_j) \neq 0$: διαφορετικά

$0 = h(c_j) = f(a - dc_j)$ και επομένως $a - dc_j = b_i$, άρα $a = b_i + dc_j$, άτοπο. Ο μέγιστος κοινός διαιρέτης των $h(x)$, $g(x)$ στους δακτυλίους $F(a)[x]$ και $E[x]$ υπολογίζεται και στις δύο περιπτώσεις με τον Ευκλείδιο αλγόριθμο, και άρα είναι ο ίδιος, έστω $q(x)$. Έτσι αφού $q(x)$ διαιρεί το $g(x)$, $q(x)$ παραγοντοποείται ως εξής στο $E[x]$: $q(x) = (x - c)\prod(x - c_{j_s})$, $j_s \neq 1$. Όμως $q(x)$ διαιρεί το $h(x)$ και $h(c_{j_s}) \neq 0$, άρα $q(x) = x - c$. Αφού $q(x) \in F(a)[x]$ έπεται ότι $c \in F(a)$. Επομένως $b = a - dc \in F(a)$ και $F(a) = F(b, c)$. □

4.8 Ασκήσεις

1. Έστω $f(x) = x^3 + x^2 + 2x$.
   - Να βρείτε ένα σώμα ανάλυσης E του $f(x)$ υπεράνω του $\mathbb{Z}_3[x]$.
   - Να περιγράψετε τα στοιχεία του E.
   - Να βρείτε ένα στοιχείο a έτσι ώστε $E = \mathbb{Z}_3(a)$.
2. Να δείξετε ότι υπάρχει ανάγωγο πολυώνυμο βαθμού 6 υπεράνω του $\mathbb{Z}_5$
3. Έστω F ένα σώμα ανάλυσης του πολυωνύμου $f(x) = x^{3^{15}} - x$ υπεράνω του $\mathbb{Z}_3$. Να αποδείξετε ότι σύνολο E των ριζών του $f(x)$ είναι σώμα με 3^{15} στοιχεία που περιέχει το $\mathbb{Z}_3$. Να βρείτε τον βαθμό $[E : \mathbb{Z}_3]$.
4. Έστω $|E| = 2^8$, $G = \mathrm{Gal}(E/\mathbb{Z}_2)$.
   - Να δείξετε αναλυτικά ότι η συνάρτηση $\sigma : E \to E$, $\sigma(b) = b^2$ είναι αυτομορφισμός του E και $\sigma \in G$.
   - Να δείξετε αναλυτικά ότι η τάξη του σ είναι 8 και επομένως $G = \langle\sigma\rangle \cong Z_8$.