Πεπερασμένα Σώματα και Εφαρμογές

25 Σεπτεμβρίου 2024

Κεφάλαιο 1

Αλγεβρικό υπόβαθρο

1.1 Ομάδες

Ορισμός 1.1 *Ένα μη κενό σύνολο G εφοδιασμένο με μία διμελή πράξη $*$ ονομάζεται ομάδα εάν ικανοποιούνται οι παρακάτω ιδιότητες:*

1. *(προσεταιριστική ιδιότητα) Για κάθε $a, b, c \in G$ ισχύει $(a * b) * c = a * (b * c)$*

2. *(ύπαρξη ουδέτερου) Υπάρχει $e \in G$ τέτοιο ώστε για κάθε $a \in G$ ισχύει $a * e = e * a = a$*

3. *(ύπαρξη συμμετρικού) Για κάθε $a \in G$ υπάρχει $a' \in G$ τέτοιο ώστε $a * a' = a' * a = e$*

Εάν ικανοποιείται επιπλέον το παρακάτω αξίωμα:

4. *(αντιμεταθετική ιδιότητα) Για κάθε $a, b \in G$ ισχύει $a * b = b * a$*

τότε η ομάδα $(G, *)$ ονομάζεται αντιμεταθετική ή αβελιανή.

Για λόγους συντομίας, όταν έχουμε μία ομάδα $(G, *)$ και η πράξη είναι σαφής από τα συμφραζόμενα, αναφερόμαστε στην «ομάδα G». Η ομάδα G ονομάζεται πεπερασμένη αν το σύνολο G είναι πεπερασμένο, διαφορετικά ονομάζεται άπειρη. Το πλήθος των στοιχείων του συνόλου G ονομάζεται *τάξη* της G. Όταν συμβολίζουμε την πράξη της ομάδας με $\cdot$ (αντίστοιχα $+$), συνηθίζεται να συμβολίζουμε το ουδέτερο στοιχείο με 1 (αντίστοιχα 0) και το συμμετρικό στοιχείο με a^{-1} (αντίστοιχα $-a$).

Ορισμός 1.2 *Έαν $(G, \cdot)$ είναι ομάδα, τότε ένα υποσύνολο H του G ονομάζεται υποομάδα της G έαν είναι το ίδιο ομάδα με πράξη τον περιορισμό της πράξης $\cdot$ στο σύνολο H. Συμβολίζουμε $H \leq G$.*

Μία ομάδα G ονομάζεται *κυκλική* αν υπάρχει κάποιο στοιχείο $a \in G$ τέτοιο ώστε $G = \{a^k : k \in \mathbb{Z}\}$. Τότε λέμε ότι το στοιχείο a παράγει την G και γράφουμε $G = \langle a \rangle$. Αν a είναι οποιοδήποτε στοιχείο μίας ομάδας G, εύκολα βλέπουμε ότι το σύνολο $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ είναι υποομάδα της G. Η τάξη της υποομάδας $\langle a \rangle$ ονομάζεται *τάξη του στοιχείου a* και τη συμβολίζουμε με $\mathrm{ord}(a)$.

Πρόταση 1.1 *Ἐστω G μία ομάδα και $H \subseteq G$. Τότε η H είναι υποομάδα της G αν και μόνο αν*

1. *$H \neq \varnothing$*

2. *Για κάθε $a, b \in G$ ισχύει $a \cdot b^{-1} \in G$.*

Πρόταση 1.2 *Αν H είναι υποομάδα μιας ομάδας G, τότε η σχέση $\sim_H$ που ορίζεται στην G ως $a \sim_H b$ αν και μόνο αν $ab^{-1} \in H$ είναι σχέση ισοδυναμίας. Η κλάση της $\sim_H$ που περιέχει το στοιχείο a είναι το σύνολο $aH = \{ah : h \in H\}$.*

Ορισμός 1.3 *Έστω G μία ομάδα, $H \leq G$. Για κάθε στοιχείο $a \in G$, ονομάζουμε το σύνολο $aH = \{ah : h \in H\}$ αριστερή πλευρική κλάση (ή αριστερό σύμπλοκο) της εντός της G (η οποία περιέχει το στοιχείο a). Οποιοδήποτε στοιχείο του συνόλου aH ονομάζεται αντιπρόσωπος του συμπλόκου. Το σύνολο των αριστερών συμπλόκων της H εντός της G συμβολίζεται G/H. Το πλήθος των αριστερών συμπλόκων (δηλαδή το πλήθος των στοιχείων του συνόλου G/H) ονομάζεται δείκτης της H στη G και συμβολίζεται $[G : H]$.*

Θεώρημα 1.1 (Lagrange) *Έστω μία πεπερασμένη ομάδα G και H μία υποομάδα της. Τότε $|G/H| = |G|/|H|$.*

Για οποιοδήποτε στοιχείο a μίας πεπερασμένης ομάδας G, εάν εφαρμόσουμε το Θεώρημα του Lagrange για την υποομάδα $\langle a\rangle$, βλέπουμε ότι $\mathrm{ord}(a) \mid |G|$ ή ισοδύναμα $a^{|G|} = 1$.

Πρόταση 1.3 *Κάθε υποομάδα μίας κυκλικής ομάδας είναι κυκλική.*

Θεώρημα 1.2 *Έστω μία ομάδα G και στοιχείο $a \in G$ πεπερασμένης τάξης n. Τότε*

1. $\mathrm{ord}(a^k) = \frac{n}{(k,n)}$.
2. *Η ομάδα $\langle a\rangle$ περιέχει ακριβώς μία υποομάδα τάξης d για κάθε $d \mid n$.*
3. *Η ομάδα $\langle a\rangle$ περιέχει $\phi(d)$ στοιχεία τάξης d για κάθε $d \mid n$.*

Ορισμός 1.4 *Έστω G μία πεπερασμένη αβελιανή ομάδα. Ο ελάχιστος θετικός ακέραιος m τέτοιος ώστε $a^m = 1$ για κάθε $a \in G$, ονομάζεται* **εκθέτης** *της G και τον συμβολίζουμε με* $\exp(G)$.

Θεώρημα 1.3 *Έστω G μία πεπερασμένη αβελιανή ομάδα. Τότε*

1. *Ο εκθέτης της G είναι ίσος με το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της G, δηλαδή* $\exp(G) = \mathrm{lcm}\,\{\mathrm{ord}(a) : a \in G\}$.
2. *Υπάρχει στοιχείο $a \in G$ με τάξη ίση με τον εκθέτη της ομάδας.*
3. *Η G είναι κυκλική αν και μόνο αν $|G| = \exp(G)$.*

Απόδειξη: Ας συμβολίσουμε $m = \exp(G)$ και $S = \{\mathrm{ord}(a) : a \in G\}$. Αφού $\mathrm{ord}(a) \mid m$ για κάθε $a \in G$, το m είναι κοινό πολλαπλάσιο του S. Άρα $\mathrm{lcm}\, S \mid m$. Επίσης, αν $\mathrm{ord}(a) \mid f$ για κάθε $a \in G$, τότε $a^f = 1$ για κάθε $a \in G$. Εκτελώντας Ευκλείδια διαίρεση του f με το m έχουμε $f = mq + r$ με $0 \leq r < m$. Βλέπουμε ότι $a^r = a^{f-qm} = 1$. Εάν ήταν $0 < r < m$ θα είχαμε αντίφαση στην υπόθεση ότι το m είναι ο ελάχιστος θετικός ακέραιος με την ιδιότητα $a^m = 1$. Άρα $r = 0$ και $m \mid f$. Αυτό αποδεικνύει την πρώτη πρόταση.

Για τη δεύτερη πρόταση, θεωρούμε την ανάλυση $m = p_1^{e_1} \cdots p_k^{e_k}$ σε πρώτους και παρατηρούμε ότι για κάθε $1 \leq i \leq k$ υπάρχει στοιχείο $b_i \in G$ τέτοιο ώστε $\mathrm{ord}(b_i) = \ell_i p_i^{e_i}$ με $(\ell_i, p_i) = 1$. Εάν τέτοιο στοιχείο δεν υπήρχε, η μέγιστη δύναμη του p_i που διαιρεί κάποιο από τα $\mathrm{ord}(a)$ για $a \in G$ θα ήταν $p_i^{f_i}$ με $f_i < e_i$ και τότε $p_i^{e_i} \nmid m$. Άρα τέτοιο στοιχείο b_i υπάρχει και το στοιχείο $a_i = b_i^{\ell_i}$ έχει τάξη $p_i^{e_i}$. Καθώς $(p_i^{e_i}, p_j^{e_j}) = 1$ για $i \neq j$, έχουμε $\mathrm{ord}(a_1 \cdots a_k) = p_1^{e_1} \cdots p_k^{e_k} = m$.

Η τρίτη πρόταση είναι άμεση συνέπεια της δεύτερης και της παρατήρησης ότι η G είναι κυκλική αν και μόνο αν υπάρχει στοιχείο τάξης $|G|$. □

Ορισμός 1.5 *Μία απεικόνιση $\phi : G \to H$ από μία ομάδα $(G, \cdot)$ σε μία ομάδα $(H, *)$ ονομάζεται ομομορφισμός ομάδων εάν για κάθε $a, b \in G$ ισχύει $\phi(ab) = \phi(a) * \phi(b)$. Έαν η ϕ είναι ένα-προς-ένα ονομάζεται μονομορφισμός και αν είναι επί της H ονομάζεται επιμορφισμός. Εάν η ϕ είναι συγχρόνως μονομορφισμός και επιμορφισμός ονομάζεται ισομορφισμός. Εάν η H ταυτίζεται με τη G, τότε η ϕ ονομάζεται ενδομορφισμός. Ένας ενδομορφισμός που είναι και ισομορφισμός ονομάζεται αυτομορφισμός.*

Ορισμός 1.6 *Έστω $\phi : G \to H$ ένας ομομορφισμός ομάδων. Το σύνολο $\ker \phi = \{a \in G : \phi(a) = e_H\}$, όπου e_H είναι το ουδέτερο στοιχείο της H ονομάζεται πυρήνας της ϕ. Το σύνολο $\operatorname{im} \phi = \{\phi(a) : a \in G\}$ ονομάζεται εικόνα της ϕ.*

Προκύπτει εύκολα ότι η ϕ είναι μονομορφισμός αν και μόνο αν $\ker \phi = \{e_G\}$.

Ορισμός 1.7 *Μία υποομάδα H της G ονομάζεται κανονική εάν $aha^{-1} \in H$ για κάθε $a \in G$ και κάθε $h \in H$. Συμβολίζουμε $H \trianglelefteq G$.*

Προκύπτει άμεσα από τον ορισμό, ότι κάθε υποομάδα μίας αβελιανής ομάδας είναι κανονική. Έστω H μία κανονική υποομάδα της G. Στο σύνολο G/H των πλευρικών κλάσεων της H στην G ορίζουμε την πράξη $aH \cdot bH = (ab)H$. Η πράξη είναι καλά ορισμένη (δεν εξαρτάται από την επιλογή των αντιπροσώπων) και επιπλέον ικανοποιεί τα αξιώματα της ομάδας. Με αυτή την πράξη το σύνολο G/H αποκτά δομή ομάδας, η οποία ονομάζεται ομάδα πηλίκο. Εάν η ομάδα G είναι αβελιανή τότε και η G/H είναι αβελιανή.

Θεώρημα 1.4 (Πρώτο Θεώρημα Ισομορφισμών) *Έστω $\phi : G \to S$ ένας ομομορφισμός ομάδων. Τότε ο $\ker \phi$ είναι κανονική υποομάδα της G και η απεικόνιση*

$$\begin{array}{rcl} \tilde{\phi} : G/\ker\phi & \to & \operatorname{im}\phi \\ a\ker\phi & \mapsto & \phi(a) \end{array}$$

είναι ισομορφισμός. Αν $N \trianglelefteq G$ τότε η απεικόνιση

$$\begin{array}{rcl} \pi : G & \to & G/N \\ a & \mapsto & aN \end{array}$$

είναι επιμορφισμός με $\ker \pi = N$.

1.2 Δακτύλιοι

Ορισμός 1.8 *Ένα μη κενό σύνολο R εφοδιασμένο με δύο πράξεις $+$ (πρόσθεση) και $\cdot$ (πολλαπλασιασμό) ονομάζεται δακτύλιος εάν ικανοποιούνται οι παρακάτω ιδιότητες:*

1. *Η $(R, +)$ είναι αβελιανή ομάδα.*
2. *(προσεταιριστική ιδιότητα του πολ/σμου) Για κάθε $a, b, c \in R$ ισχύει $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
3. *(επιμεριστική ιδιότητα) Για κάθε $a, b, c \in R$ ισχύει $a \cdot (b + c) = a \cdot b + a \cdot c$ και $(b + c) \cdot a = ba + ca$.*

Όπως και στην περίπτωση των ομάδων, αναφερόμαστε στον «δακτύλιο R», όταν οι πράξεις είναι σαφείς από τα συμφραζόμενα. Συμβολίζουμε με 0 το ουδέτερο στοιχείο της πρόσθεσης και με $-a$ το συμμετρικό του a ως προς την πρόσθεση (και το ονομάζουμε αντίθετο του a). Ένα μη μηδενικό στοιχείο a του δακτυλίου R ονομάζεται *μηδενοδιαιρέτης*, εάν υπάρχει $b \in R \setminus \{0\}$ τέτοιο ώστε $ab = 0$. Εάν ο πολλαπλασιασμός έχει ουδέτερο στοιχείο, το συμβολίζουμε με 1. Εάν το στοιχείο $a \in R$ έχει συμμετρικό ως προς τον πολλαπλασιασμό, το συμβολίζουμε a^{-1} και το ονομάζουμε αντίστροφο του a. Ένα αντιστρέψιμο στοιχείο δεν είναι μηδενοδιαιρέτης: αν $ab = 0$ τότε πολλαπλασιάζοντας κάθε μέλος με a^{-1} παίρνουμε $b = 0$.

Ορισμός 1.9 *Ένας δακτύλιος R ονομάζεται*

1. **μεταθετικός**, *εάν ο πολλαπλασιασμός είναι αντιμεταθετική πράξη.*
2. **δακτύλιος με μονάδα**, *εάν υπάρχει ουδέτερο στοιχείο του πολλαπλασιασμού και $1 \neq 0$.*
3. **ακέραια περιοχή**, *εάν είναι μεταθετικός δακτύλιος με μονάδα $1 \neq 0$ και δεν περιέχει μηδενοδιαιρέτες.*

4. **σώμα**, *εάν είναι ακέραια περιοχή και κάθε μη μηδενικό στοιχείο έχει αντίστροφο.*

Εάν R είναι ένας δακτύλιος με μονάδα, συμβολίζουμε το σύνολο των αντιστρέψιμων στοιχείων του με R^*. Προκύπτει άμεσα ότι το $(R^*, \cdot)$ είναι ομάδα. Ας υποθέσουμε επιπλέον, ότι ο R είναι μεταθετικός. Δύο στοιχεία $a, b \in R$ ονομάζονται συνεταιρικά και γράφουμε $a \sim b$ εάν υπάρχει $u \in R^*$ τέτοιο ώστε $a = ub$. Η σχέση $\sim$ είναι σχέση ισοδυναμίας στον R. Λέμε ότι το στοιχείο a διαιρεί το στοιχείο b και γράφουμε $a \mid b$ εάν υπάρχει $c \in R$ τέτοιο ώστε $b = ac$.

Πρόταση 1.4 *Κάθε πεπερασμένη ακέραια πειροχή είναι σώμα.*

Απόδειξη: Έστω R μία πεπερασμένη ακέραια περιοχή. Αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο $a \in R$ έχει αντίστροφο. Θεωρούμε την απεικόνιση

$$\begin{aligned} f : R \setminus \{0\} &\longrightarrow R \setminus \{0\} \\ b &\mapsto ab \end{aligned}$$

Η απεικόνιση f είναι 1-1, διότι ο R είναι ακέραια περιοχή και ισχύει ο νόμος της διαγραφής. Καθώς το σύνολο $R \setminus \{0\}$ είναι πεπερασμένο, η f είναι επί. Άρα υπάρχει κάποιο $b \in R \setminus \{0\}$ τέτοιο ώστε $ab = 1$. □

Ορισμός 1.10 *Ένα μη κενό υποσύνολο S ενός δακτυλίου R ονομάζεται* **υποδακτύλιος** *του R, εάν είναι δακτύλιος με πράξεις τους περιορισμούς των πράξεων του δακτυλίου R στο S.*

Πρόταση 1.5 *Ένα μη κενό υποσύνολο S ενός δακτυλίου R είναι υποδακτύλιος του R αν και μόνο αν ισχύουν*

1. *Για κάθε $a, b \in S$, $a - b \in S$.*

2. *Για κάθε $a, b \in S$, $ab \in S$.*

Ορισμός 1.11 *Έστω R μία ακέραια περιοχή.*

1. *Ένα στοιχείο $r \in R$ ονομάζεται* **ανάγωγο**, *εάν είναι μη μηδενικό, μη αντιστέψιμο και για κάθε $a, b \in R$ ισχύει $r = ab \;\Rightarrow\; a \in R^* \;\text{ή}\; b \in R^*$.*

2. *Ένα στοιχείο $p \in R$ ονομάζεται* **πρώτο**, *εάν είναι μη μηδενικό, μη αντιστέψιμο και για κάθε $a, b \in R$ ισχύει $p \mid ab \;\Rightarrow\; p \mid a \;\text{ή}\; p \mid b$.*

Θεώρημα 1.5 *Σε μία ακέραια περιοχή R κάθε πρώτο στοιχείο είναι ανάγωγο.*

Απόδειξη: Έστω $p \in R$ ένα πρώτο στοιχείο. Εξ' ορισμού, $p \neq 0$ και $p \notin R^*$. Έστω ότι $p = ab$ για κάποια $a, b \in R$. Τότε $p \mid ab$, οπότε από τον Ορισμό 1.11 έχουμε ότι $p \mid a$ ή $p \mid b$. Ας υποθέσουμε ότι $p \mid a$. Τότε $a = pc$ για κάποιο $c \in R$ και έχουμε $p = pcb$. Αφού $p \neq 0$ προκύπτει ότι $1 = cb$, άρα $b \in R^*$. Εντελώς ανάλογα προκύπτει ότι $a \in R^*$, αν υποθέσουμε ότι $p \mid b$. □

Ορισμός 1.12 *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Ένα μη κενό υποσύνολο I του R ονομάζεται ιδεώδες εάν ικανοποιούνται οι παρακάτω ιδιότητες:*

1. *Για κάθε $a, b \in I$ ισχύει $a - b \in I$.*

2. *Για κάθε $r \in R$ και κάθε $a \in I$ ισχύει $ra \in I$.*

Η έννοια του ιδεώδους ορίζεται σε κάθε δακτύλιο. Περιοριζόμαστε σε μεταθετικούς δακτυλίους με μονάδα, καθώς αυτοί οι δακτύλιοι εμφανίζονται σε αυτό το βιβλίο. Παρατηρούμε ότι κάθε ιδεώδες είναι υποδακτύλιος του R, με την επιπλέον ιδιότητα ότι είναι κλειστό ως προς πολλαπλασιασμό με στοιχεία από το R.

Ένας τρόπος για να κατασκευάσουμε ένα ιδεώδες είναι να επιλέξουμε κάποια στοιχεία του R, έστω τα $a_1, \ldots, a_n$ και να θεωρήσουμε το σύνολο των γραμμικών συνδυασμών τους με συντελεστές από το R. Το σύνολο

$$\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$$

είναι ιδεώδες του R και ονομάζεται το «το ιδεώδες που παράγεται από το σύνολο $\{a_1, \ldots, a_n\}$». Η κατασκευή γενικεύεται άμεσα και για άπειρα υποσύνολα του R. Για οποιοδήποτε υποσύνολο $S \subseteq R$, το σύνολο

$$\langle S \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in S, n \in \mathbb{N}\}$$

είναι ιδεώδες του R και ονομάζεται το «το ιδεώδες που παράγεται από το σύνολο S». Ένα ιδεώδες που είναι της μορφής $\langle a \rangle$ για κάποιο $a \in R$, δηλαδή παράγεται από ένα στοιχείο, ονομάζεται *κύριο ιδεώδες*.

Δεδομένου ενός μεταθετικού δακτυλίου με μονάδα R και ενός ιδεώδους I του R, ορίζουμε στο σύνολο R τη σχέση ισοδυναμίας $\equiv_I$

$$a \equiv_I b \iff a - b \in I.$$

Συνηθίζεται να γράφουμε $a \equiv b \pmod{I}$ αντί για $a \equiv_I b$. Συμβολίζουμε το σύνολο των κλάσεων της σχέσης $\equiv_I$ με R/I. Η κλάση που περιέχει το στοιχείο $a \in R$ είναι το σύνολο $a + I = \{a + h : h \in I\}$. Για την κλάση $a + I$ χρησιμοποιούμε και τους συμβολισμούς $[a]_I$, $a \bmod I$ ή ακόμη και $\overline{a}$ εάν το ιδεώδες είναι σαφές από τα συμφραζόμενα.

Στο σύνολο R/I ορίζουμε πράξεις

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I\\(a+I)\cdot(b+I) &= (ab)+I\end{aligned}$$

Οι πράξεις είναι καλά ορισμένες. Στον ορισμό κάνουμε χρήση αντιπροσώπων των κλάσεων αλλά το αποτέλεσμα της πράξης δεν εξαρτάται από την επιλογή των αντιπροσώπων. Πραγματικά, εάν $a + I = a' + I$ και $b + I = b' + I$, έχουμε $a - a' = h \in I$ και $b - b' = f \in I$. Οπότε $(a + b) - (a' + b') = h + f \in I$, και προκύπτει ότι $(a + b) + I = (a' + b') + I$. Αντίστοιχα, για το πολλαπλασιασμό έχουμε $ab - a'b' = af + bh + hf \in I$ και προκύπτει ότι $ab + I = a'b' + I$. Στο σημείο αυτό φαίνεται ο λόγος που απαιτήσαμε το I να είναι ιδεωδες και όχι απλά υποδακτύλιος.

Το σύνολο R/I, εφοδιασμένο με τις παραπάνω πράξεις έχει τη δομή μεταθετικού δακτυλίου με μηδενικό στοιχείο το $0 + I = I$ και μονάδα το στοιχείο $1 + I$.

Παρατηρήσεις 1.1 *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Οι παρακάτω παρατηρήσεις είναι άμεσες από τους ορισμούς.*

1. *Τα υποσύνολα $\{0\}$ και R είναι ιδεώδη. Κάθε ιδεώδες διάφορο του $\{0\}$ ονομάζεται μημηδενικό και κάθε ιδεώδες διάφορο του R ονομάζεται γνήσιο.*

2. *Η κλάση $a + I$ είναι το μηδενικό στοιχείο του R/I αν και μόνο αν $a \in I$.*

3. *Έαν ένα ιδεώδες I περιέχει κάποιο αντιστρέψιμο στοιχείο $a \in R^*$, τότε $I = R$. Πραγματικά, για κάθε $r \in R$, έχουμε $r = ra^{-1}a \in I$, καθώς $a \in I$ και $ra^{-1} \in R$. Αντίστροφα, αν $I = R$ τότε $1 \in I$.*

4. *Από την προηγούμενη παρατήρηση προκύπτει άμεσα ότι ένας μεταθετικός δακτύλιος με μονάδα, R, είναι σώμα αν και μόνο αν τα μόνα ιδεώδη του είναι τα $\{0\}$ και R.*

Ορισμός 1.13 *Έστω R μεταθετικός δακτύλιος με μονάδα. Ένα μη μηδενικό, γνήσιο ιδεώδες I του R ονομάζεται*

1. **μεγιστικό** *εάν $I \neq R$ και για κάθε ιδεώδες J του R με $I \subsetneq J$ ισχύει $J = R$.*

2. **πρώτο** *εάν* $I \neq R$ *και για κάθε* $a, b \in R$*, αν* $ab \in I$ *τότε* $a \in I$ *ή* $b \in I$.

Θεώρημα 1.6 *Έστω* R *μεταθετικός δακτύλιος με μονάδα και* I *ιδεώδες του. Ισχύουν οι παρακάτω προτάσεις.*

1. *Το* I *είναι μεγιστικό αν και μόνο αν το* R/I *είναι σώμα.*

2. *Το* I *είναι πρώτο αν και μόνο αν το* R/I *είναι ακέραια περιοχή.*

Απόδειξη: Για την πρώτη πρόταση, υποθέτουμε ότι το I είναι μεγιστικό. Αρχικά παρατηρούμε ότι $1 + I \neq 0 + I$, διότι $1 \notin I$. Για να δείξουμε ότι ο δακτύλιος R/I είναι σώμα μένει να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R/I έχει αντίστροφο. Έστω $a + I \in R/I$ με $a \notin I$ (ισοδύναμα $a + I \neq I$). θεωρούμε το ιδεώδες που παράγεται από το σύνολο $I \cup \{a\}$, ας το ονομάσουμε J. Τότε $I \subsetneq J$ και η υπόθεση ότι το I είναι μεγιστικό συνεπάγεται ότι $J = R$. Αυτό σημαίνει ότι $1 \in J$, οπότε μπορεί να γραφεί ως $1 = h + ba$ για κάποιο $b \in R$. Άρα $ba - 1 \in I$ και

$$(b + I) \cdot (a + I) = ba + I = 1 + I,$$

δηλαδή το στοιχείο $a + I$ είναι αντιστρέψιμο.

Αντίστροφα, εάν ο δακτύλιος R/I είναι σώμα τότε το $a + I$ είναι αντιστρέψιμο για κάθε $a \in R \setminus I$. Ας υποθέσουμε ότι J είναι ένα ιδεώδες με την ιδιότητα $I \subsetneq J$. Τότε θα υπάρχει στοιχείο $a \in J \setminus I$. Η κλάση $a + I$ έχει αντίστροφο, έστω την $b + I$ και ισχύει

$$(a + I) \cdot (b + I) = 1 + I \implies ab + I = 1 + I$$

που σημαίνει ότι $ab - 1 = h \in I$. Όμως τότε $1 = ab - h \in J$ που σημαίνει ότι $J = R$.

Για τη δεύτερη πρόταση, υποθέτουμε ότι το I είναι πρώτο. Για να δείξουμε ότι ο δακτύλιος R/I είναι ακέραια περιοχή αρκεί να δείξουμε ότι $I \neq 1 + I$ και δεν περιέχει μηδενοδιαιρέτες. Εάν ήταν $I = 1 + I$, τότε $1 \in I$, οπότε $I = R$, που αποκλείεται από τον ορισμό του πρώτου ιδεώδους. Έστω ότι ισχύει $(a + I) \cdot (b + I) = I$ για κάποια $a, b \in R$. Τότε $ab \in I$, οπότε $a \in I$ ή $b \in I$, που γράφεται ισοδύναμα $a + I = I$ ή $b + I = I$.

Αντίστροφα, ας υποθέσουμε ότι ο δακτύλιος R/I είναι ακέραια περιοχή. Τότε περιέχει τουλάχιστον δύο διακεκριμένα στοιχεία I και $1 + I$. Αυτό σημαίνει ότι $I \neq R$ (διαφορετικά ο δακτύλιος R/I θα είχε ένα μοναδικό στοιχείο). Επίσης, εάν $ab \in I$ για κάποια $a, b \in R$, τότε $ab + I = (a + I) \cdot (b + I) = I$. Αφού ο R/I είναι ακέραια περιοχή θα πρέπει $a + I = I$ ή $b + I = I$, δηλαδή $a \in I$ ή $b \in I$. □

Πόρισμα 1.1 *Σε ένα* R *μεταθετικό δακτύλιο με μονάδα, κάθε μεγιστικό ιδεώδες είναι πρώτο.*

Απόδειξη: Κάθε σώμα είναι ακέραια περιοχή. □

Ορισμός 1.14 *Μία απεικόνιση* $\phi : R \to S$ *από ένα δακτύλιο* $(R, +, \cdot)$ *σε ένα δακτύλιο* $(S, +, \cdot)$ *ονομάζεται ομομορφισμός δακτυλίων εάν για κάθε* $a, b \in R$ *ισχύει* $\phi(a + b) = \phi(a) + \phi(b)$ *και* $\phi(ab) = \phi(a) \cdot \phi(b)$*. Έαν η* ϕ *είναι ένα-προς-ένα ονομάζεται μονομορφισμός και αν είναι επί του* S *ονομάζεται επιμορφισμός. Εάν η* ϕ *είναι συγχρόνως μονομορφισμός και επιμορφισμός ονομάζεται ισομορφισμός. Εάν ο* S *ταυτίζεται με τον* R*, τότε η* ϕ *ονομάζεται ενδομορφισμός. Ένας ενδομορφισμός που είναι και ισομορφισμός ονομάζεται αυτομορφισμός.*

Παρατηρήσεις 1.2 *Έστω* R *ακέραια περιοχή και* $\phi : R \to S$ *ομομορφισμός δακτυλίων.*

1. $\ker \phi$ *είναι ιδεώδες του* R.

2. *Αν* R *είναι σώμα, τότε* $\ker \phi = R$ *ή* $\ker \phi = \{0\}$*, που σημαίνει ότι* $\phi = 0$ *(ο μηδενικός ομομορφισμός) ή ο* ϕ *είναι μονομορφισμός.*

Θεώρημα 1.7 (Πρώτο Θεώρημα Ισομορφισμών) *Έστω R μεταθετικός δακτύλιος με μονάδα και $\phi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε ο $\ker\phi$ είναι ιδεώδες του R και η απεικόνιση*

$$\begin{aligned} \tilde{\phi} : R/\ker\phi &\to \operatorname{im}\phi \\ a + \ker\phi &\mapsto \phi(a) \end{aligned}$$

είναι ισομορφισμός. Αν I είναι ιδεώδες του R τότε η απεικόνιση

$$\begin{aligned} \pi : R &\to R/I \\ a &\mapsto a + I \end{aligned}$$

είναι επιμορφισμός με $\ker\pi = I$.

Ορισμός 1.15 *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Ονομάζουμε* **χαρακτηριστική** *του R και συμβολίζουμε $\mathrm{char}(R)$, τον ελάχιστο θετικό ακέραιο n με την ιδιότητα $n \cdot 1 = 1 + \cdots + 1 = 0$, εφόσον αυτός υπάρχει, διαφορετικά ορίζουμε $\mathrm{char}(R) = 0$.*

Πρόταση 1.6 *Η χαρακτηριστική μίας ακέραιας περιοχής είναι μηδέν ή πρώτος αριθμός.*

Απόδειξη: Έστω μία ακέραια περιοχή R. Αν $\mathrm{char}(R) = 0$ έχουμε τελειώσει. Έστω $\mathrm{char}(R) = n > 0$ και ας υποθέσουμε ότι $n = ab$ με $1 < a, b < n$. Τότε έχουμε $n \cdot 1 = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$. Όμως ο $\mathbb{Z}$ είναι ακέραια περιοχή, οπότε έχουμε $a \cdot 1 = 0$ ή $b \cdot 1 = 0$. Αυτό αντιβαίνει στην υπόθεση ότι ο n είναι *ο ελάχιστος* θετικός ακέραιος με την ιδιότητα $n \cdot 1 = 0$. Άρα τέτοια παραγοντοποίηση δεν υπάρχει και ο n είναι πρώτος. □

Πρόταση 1.7 *Έστω R ακέραια περιοχή με $\mathrm{char}(R) = p$. Τότε για κάθε $a \in R \setminus \{0\}$ ισχύει $n \cdot a = 0$ αν και μόνο αν $p \mid n$.*

Απόδειξη: Αφήνεται ως άσκηση. □

Λήμμα 1.1 *Έστω πρώτος αριθμός p. Για κάθε $1 \le k \le p - 1$ ισχύει $p \mid \binom{p}{k}$*

Απόδειξη: Από τον ορισμό του δυωνυμικού συντελεστή ξέρουμε ότι

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}.$$

Οπότε

$$p! = \binom{p}{k} k!(p-k)!$$

Το p διαιρεί το αριστέρο μέλος, άρα διαιρεί και το δεξί. Αφού το p είναι πρώτος και $1 \le k < p$ θα είναι $(p, k) = 1$. Για τον ίδιο λόγο είναι $(p, p-k) = 1$. Οπότε $p \mid \binom{p}{k}$. □

Θεώρημα 1.8 *Έστω ακέραια περιοχή R χαρακτηριστικής p. Τότε για κάθε $a_1, \ldots, a_n \in R$ ισχύει $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$.*

Απόδειξη: Για $a, b \in R$, από το δυωνυμικό θεώρημα έχουμε

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}. \tag{1.1}$$

Από το Λήμμα 1.1 προκύπτει ότι οι όροι του αθροίσματος για $1 \le k \le p - 1$ είναι ίσοι με 0.
□

1.2.1 Περιοχές κυρίων ιδεωδών

Ορισμός 1.16 *Μία ακέραια περιοχή R στην οποία κάθε ιδεώδες είναι κύριο, ονομάζεται* **περιοχή κυρίων ιδεωδών** *ή* ΠΚΙ *για συντομία.*

Πρόταση 1.8 *Έστω R μία ακέραια περιοχή και $a, b \in R$. Ισχύουν οι παρακάτω προτάσεις.*

1. *$\langle a \rangle \subseteq \langle b \rangle$ αν και μόνο αν $b \mid a$.*
2. *$\langle a \rangle = \langle b \rangle$ αν και μόνο αν υπάρχει $u \in R^*$ τέτοιο ώστε $b = ua$.*
3. *$\langle a \rangle = R$ αν και μόνο αν $a \in R^*$.*

Απόδειξη: Για την πρώτη πρόταση, βλέπουμε ότι $\langle a \rangle \subseteq \langle b \rangle$ αν και μόνο αν $a \in \langle b \rangle$. Η τελευταία συνθήκη ισχύει αν και μόνο αν $b \mid a$.

Για τη δεύτερη πρόταση, εξετάζουμε αρχικά την περίπτωση $a = 0$. Τότε $\langle a \rangle = \langle b \rangle = \{0\}$, οπότε $a = b = 0$ και η πρόταση ισχύει (παίρνοντας για παράδειγμα $u = 1$). Για $a \neq 0$, βλέπουμε ότι $\langle a \rangle = \langle b \rangle$ αν και μόνο αν $b \mid a$ και $a \mid b$. Χρησιμοποιώντας την πρώτη πρόταση οι δύο τελευταίες σχέσεις ισοδυναμούν με την ύπαρξη στοιχείων $u, v \in R$ τέτοιων ώστε $a = ub$ και $b = va$ αντίστοιχα, οπότε $a = uva$. Καθώς το a είναι μη μηδενικό στοιχείο ακέραιας περιοχής, ισχύει ο νόμος της διαγραφής και παίρνουμε ότι $uv = 1$, δηλαδή $u, v \in R^*$, όπως απαιτείται. Αντίστροφα, εάν $a = ub$ για κάποιο $u \in R^*$, έχουμε $b = u^{-1}a$. Οπότε $b \mid a$ και $a \mid b$ που ισοδυναμεί με $\langle a \rangle = \langle b \rangle$.

Για την τρίτη πρόταση, βλέπουμε ότι $R = \langle 1 \rangle$, οπότε χρησιμοποιώντας τη δεύτερη πρόταση, έχουμε $\langle a \rangle = \langle 1 \rangle$ αν και μόνο αν $a = u \in R^*$. □

Θεώρημα 1.9 *Έστω R μία ΠΚΙ και $a \in R$. Ισχύουν οι παρακάτω προτάσεις.*

1. *Το ιδεώδες $\langle a \rangle$ είναι μεγιστικό αν και μόνο αν το a είναι ανάγωγο.*
2. *Το ιδεώδες $\langle a \rangle$ είναι πρώτο αν και μόνο αν το a είναι πρώτο.*

Απόδειξη: Για την πρώτη πρόταση, υποθέτουμε ότι το ιδεώδες $\langle a \rangle$ είναι μεγιστικό. Τότε $\langle a \rangle \neq \{0\}$ και $\langle a \rangle \neq R$, που συνεπάγεται ότι $a \neq 0$ και $a \notin R^*$ αντίστοιχα. Έστω ότι $a = cb$ για κάποια $b, c \in R$ και ας υποθέσουμε ότι $b \notin R^*$. Από την Πρόταση 1.8 έχουμε ότι $\langle b \rangle \neq R$. Επίσης, $b \mid a$, οπότε από την ίδια πρόταση $\langle a \rangle \subseteq \langle b \rangle$. Καθώς το $\langle a \rangle$ είναι μεγιστικό, αυτό σημαίνει ότι $\langle a \rangle = \langle b \rangle$, δηλαδή $a = ub$ για κάποιο $u \in R^*$. Οπότε $c = u \in R^*$. Προσέξτε ότι από τη σχέση $cb = ub$ διαγράψαμε το b, αφού $b \neq 0$ και βρισκόμαστε σε ακέραια περιοχή.

Αντίστροφα, αν το a είναι ανάγωγο, τότε $a \neq 0$ και $a \notin R^*$, που σημαίνει ότι $\langle a \rangle \neq \{0\}$ και $\langle a \rangle \neq R$. Εάν $\langle a \rangle \subsetneq \langle b \rangle$, από την Πρόταση 1.8 έχουμε $a = cb$ και $c \notin R^*$. Από τον ορισμό του ανάγωγου στοιχείου, έπεται ότι $b \in R^*$, οπότε $\langle b \rangle = R$.

Για τη δεύτερη πρόταση, υποθέτουμε ότι το ιδεώδες $\langle a \rangle$ είναι πρώτο. Τότε $a \neq 0$ και $a \notin R^*$, ακριβώς όπως και στην πρώτη πρόταση. Αν $a \mid cd$ τότε $cd \in \langle a \rangle$ και από τον ορισμό του πρώτου ιδεώδους έχουμε $b \in \langle a \rangle$ ή $c \in \langle a \rangle$, ισοδύναμα $a \mid b$ ή $a \mid c$.

Αντίστροφα, αν το a είναι πρώτο, τότε $\langle a \rangle \neq \{0\}$ και $\langle a \rangle \neq R$. Αν $bc \in \langle a \rangle$ τότε $a \mid bc$ οπότε $a \mid b$ ή $a \mid c$ που σημαίνει ότι $b \in \langle a \rangle$ ή $c \in \langle a \rangle$. □

Πόρισμα 1.2 *Σε μία περιοχή κυρίων ιδεωδών τα ανάγωγα στοιχεία και τα πρώτα στοιχεία ταυτίζονται.*

Απόδειξη: Από το Θεώρημα 1.5 γνωρίζουμε ότι κάθε πρώτο στοιχείο είναι ανάγωγο. Έστω $a \in R$ ένα ανάγωγο στοιχείο. Τότε το ιδεώδες $\langle a \rangle$ είναι μεγιστικό, άρα από το Πόρισμα 1.1 είναι και πρώτο. Συνεπώς το $a \in R$ είναι πρώτο. □

Σε κάθε περιοχή κυρίων ιδεωδών ορίζεται η έννοια του μέγιστου κοινού διαιρέτη.

Ορισμός 1.17 *Έστω R μία ΠΚΙ και $a_1, \dots, a_n \in R$. Ονομάζουμε* **μέγιστο κοινό διαιρέτη** *των $a_1, \dots, a_n$ κάθε στοιχείο $d \in R$ με τις ιδιότητες:*

1. *$d \mid a_i$ για $1 \leq i \leq n$.*

2. *Για κάθε $f \in R$, αν $f \mid a_i$ για $1 \leq i \leq n$, τότε $f \mid d$.*

Πρόταση 1.9 *Έστω R μία ΠΚΙ και $a_1, \dots, a_n \in R$, τότε υπάρχει μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$. Εάν d είναι ένας μέγιστος κοινός διαιρέτης τότε υπάρχουν $t_1, \dots, t_n \in R$ τέτοια ώστε $d = t_1 a_1 + \cdots + t_n a_n$.*

Απόδειξη: Ας θεωρήσουμε το ιδεώδες $\langle a_1, \dots, a_n \rangle$. Καθώς ο R είναι ΠΚΙ, θα υπάρχει καποιο στοιχείο $d \in R$ τέτοιο ώστε $\langle a_1, \dots, a_n \rangle = \langle d \rangle$. Αυτό σημαίνει ότι $d \mid a_i$ για $1 \neq i \leq n$. Ας υποθέσουμε τώρα ότι κάποιο στοιχείο $f \in R$ ικανοποιεί $f \mid a_i$ για $1 \leq i \leq n$. Αυτό σημαίνει ότι $a_n \in \langle f \rangle$ για $1 \leq i \leq n$, οπότε $\langle a_1, \dots, a_n \rangle \subseteq \langle f \rangle$, δηλαδή $\langle d \rangle \subseteq \langle f \rangle$. Από την Πρόταση 1.8 συνεπάγεται ότι $f \mid d$. Η γραφή του $d = t_1 a_1 + \cdots + t_n a_n$ προκύπτει άμεσα, αφού $d \in \langle a_1, \dots, a_n \rangle$. □

Παρατηρήσεις 1.3 *Είναι σημαντικό να τονίσουμε ότι μέγιστος κοινός διαιρέτης υπάρχει αλλά δεν είναι μοναδικός. Ειδικότερα, εάν d είναι μέγιστος κοινός διαιρέτης κάποιων στοιχείων $a_1, \dots, a_n$, τότε και το σύνολο $\{ud : u \in R^*\}$ είναι το σύνολο των μέγιστων κοινών διαιρετών των $a_1, \dots, a_n$. Προκειμένου να μιλάμε για τον μέγιστο κοινό διαιρέτη, συχνά επιλέγουμε ένα από τα στοιχεία του συνόλου $\{ud : u \in R^*\}$ και το συμβολίζουμε με $\gcd(a_1, \dots, a_n)$. Ο τρόπος που γίνεται η επιλογή πρέπει να είναι σαφής για το δακτύλιο R. Για παράδειγμα, ο δακτύλιος $\mathbb{Z}$ είναι ΠΚΙ και τα αντιστρέψιμα στοιχεία του είναι τα $\{-1, 1\}$. Για δεδομένα $a_1, \dots, a_n \in \mathbb{Z}$ ονομάζουμε τον μέγιστο κοινό διαιρέτη $\gcd(a_1, \dots, a_n)$ το θετικό από τους δύο αριθμούς $-d, d$.*

Αντίστοιχα ορίζεται και η έννοια του ελάχιστου κοινού πολλαπλασίου.

Ορισμός 1.18 *Έστω R μία ΠΚΙ και $a_1, \dots, a_n \in R$. Ονομάζουμε* **ελάχιστο κοινό πολλαπλάσιο** *των $a_1, \dots, a_n$ κάθε στοιχείο $m \in R$ με τις ιδιότητες:*

1. *$a_i \mid m$ για $1 \leq i \leq n$.*

2. *Για κάθε $f \in R$, αν $a_i \mid f$ για $1 \leq i \leq n$, τότε $m \mid f$.*

Πρόταση 1.10 *Έστω R μία ΠΚΙ και $a_1, \dots, a_n \in R$, τότε υπάρχει ελάχιστο κοινό πολλαπλάσιο των $a_1, \dots, a_n$.*

Απόδειξη: Παρατηρούμε αρχικά ότι η τομή ιδεωδών είναι ιδεώδες. Θεωρούμε το ιδεώδες $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$. Ο R είναι ΠΚΙ, άρα υπάρχει $m \in R$ τέτοιο ώστε $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle m \rangle$. Έχουμε $\langle m \rangle \subseteq \langle a_i \rangle$ οπότε $a_i \mid m$ για $1 \leq i \leq n$. Έστω τώρα στοιχείο $f \in R$ τέτοιο ώστε $a_i \mid f$ για $1 \leq i \leq n$. Αυτό σημαίνει ότι $\langle f \rangle \subseteq \langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$. Οπότε $\langle f \rangle \subseteq \langle m \rangle$ που συνεπάγεται $m \mid f$. □

Ορισμός 1.19 *Μία ακέραια περιοχή R ονομάζεται* **περιοχή μοναδικής παραγοντοποίησης** *ή* **ΠΜΠ** *για συντομία, εάν για κάθε μη μηδενικό, μη αντιστρέψιμο στοιχείο $a \in R$*

1. *Υπάρχουν ανάγωγα $p_1, \dots, p_n \in R$ τέτοια ώστε $a = p_1 \cdots p_n$.*

2. *Εάν υπάρχουν ανάγωγα $q_1, \dots, q_m \in R$ τέτοια ώστε $a = q_1 \cdots q_m$, τότε $n = m$ και υπάρχει μετάθεση $f : \{1, \dots, n\} \to \{1, \dots, n\}$ τέτοια ώστε $p_i \sim q_{f(i)}$ για $1 \leq i \leq n$.*

Θεώρημα 1.10 *Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης.*

1.2.2 Ευκλείδιες περιοχές

Ορισμός 1.20 *Μία ακέραια περιοχή R ονομάζεται* **Ευκλείδια περιοχή** *αν ορίζεται απεικόνιση*

$$N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

με τις ιδιότητες:

1. *Για κάθε* $a, b \in R$*, με* $b \neq 0$*, υπάρχουν* $q, r \in R$ *τέτοια ώστε* $a = bq + r$*, με* $r = 0$ *ή* $N(r) < N(b)$*.*

2. *Για κάθε* $a, b \in R \setminus \{0\}$ *ισχύει* $N(a) \leq N(ab)$*.*

Η απεικόνιση N *ονομάζεται και Ευκλείδια βαθμίδα.*

Η επόμενη πρόταση δείχνει ότι η ελάχιστη τιμή της βαθμίδας επιτυγχάνεται από τα αντιστρέψιμα στοιχεία του δακτυλίου.

Πρόταση 1.11 *Έστω* R *μία Ευκλείδια περιοχή με Ευκλείδια βαθμίδα* N *και* $m = \min\{N(a) : a \in R \setminus \{0\}\}$*. Τότε για κάθε* $b \in R \setminus \{0\}$ *ισχύει* $N(b) = m$ *αν και μόνο αν* $b \in R^*$*.*

Απόδειξη: Έστω $c \in R \setminus \{0\}$ ένα στοιχείο με $N(c) = m$. Βλέπουμε ότι $N(1) \leq N(1 \cdot c) = m$, άρα $N(1) = m$. Ας υποθέσουμε τώρα ότι $b \in R^*$. Τότε υπάρχει $a \in R$ τέτοιο ώστε $ab = 1$, οπότε $N(b) \leq N(ab) = N(1) = m$. Οπότε $N(b) = m$.

Αντίστροφα, ας υποθέσουμε ότι $N(b) = m$. Για κάθε στοιχείο $a \in R$ υπάρχουν $q, r \in R$ τέτοια ώστε $a = bq + r$ και $r = 0$ ή $N(r) < N(b)$. Όμως $N(r) \geq m$, οπότε θα είναι $r = 0$ που σημαίνει ότι $a \in \langle b \rangle$. Αυτό συνεπάγεται ότι $\langle b \rangle = R$ και από την Πρόταση 1.8 έχουμε $b \in R^*$. □

Θεώρημα 1.11 *Κάθε Ευκλείδια περιοχή είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη: Έστω R μία Ευκλείδια περιοχή και $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ η αντίστοιχη απεικόνιση. Το μηδενικό ιδεώδες είναι κύριο. Έστω I ένα μη μηδενικό ιδεώδες του R. Το σύνολο $S = \{N(a) : a \in I \setminus \{0\}\}$ είναι μη κενό υποσύνολο του $\mathbb{Z}_{\geq 0}$, οπότε από την Αρχή του Ελαχίστου έχει ελάχιστο στοιχείο. Ας ονομάσουμε $b \in I$ ένα στοιχείο τέτοιο ώστε $N(b) = \min S$. Θα δείξουμε ότι $I = \langle b \rangle$. Είναι προφανές ότι $\langle b \rangle \subseteq I$. Για τον αντίστροφο εγκλεισμό, θεωρούμε $a \in I$. Τότε υπάρχουν $q, r \in R$ τέτοια ώστε $a = bq + r$ και $r = 0$ ή $N(r) < N(b)$. Όμως $r = a - bq \in I$ και αν ήταν $r \neq 0$ θα είχαμε $(r) \in S$ και $N(r) < N(b)$, που είναι άτοπο. Άρα $r = 0$ και $a \in \langle b \rangle$. □

Συνδυάζοντας το προηγούμενο θεώρημα και την Πρόταση 1.9 βλέπουμε ότι αν R είναι Ευκλείδια περιοχή και $a, b \in R$, τότε υπάρχει μέγιστος κοινός διαιρέτης των a, b. Η υπαρξη Ευκλείδιας διαίρεσης, μας δίνει ένα αλγόριθμο για τον υπολογισμό ενός μέγιστου κοινού διαιρέτη, εφόσον φυσικά υπάρχει αποτελεσματικός τρόπος, δεδομένων των $a, b \in R$ με $b \neq 0$ να υπολογίσουμε q, r με $a = bq + r$ και $r = 0$ ή $N(r) < N(b)$. Ο αλγόριθμος αυτός ονομάζεται *Ευκλείδιος αλγόριθμος*. Η ορθότητα του αλγορίθμου στηρίζεται στην επόμενη πρόταση.

Πρόταση 1.12 *Έστω* R *μία Ευκλείδια περιοχή και στοιχεία* $a, b, c, q \in R$ *τέτοια ώστε* $a = bq + c$*. Τότε ένας μέγιστος κοινός διαιρέτης των* b, c *είναι και μέγιστος κοινός διαιρέτης των* a, b*.*

Απόδειξη: Ας υποθέσουμε ότι d είναι ένας μέγιστος κοινός διαιρέτης των b, c. Τότε $d \mid b$ και $d \mid c$, οπότε $d \mid bq + c$, δηλαδή $d \mid a$. Άρα το d είναι κοινός διαιρέτης των a, b. Μένει να δείξουμε ότι κάθε κοινός διαιρέτης f των a, b διαιρεί το d. Εάν $f \mid a$ και $f \mid b$ τότε $f \mid a - bq$, δηλαδή $f \mid c$. Καθώς ο d είναι μέγιστος κοινός διαιρέτης των b, c, αυτό σημαίνει ότι $f \mid d$. □

Πρόταση 1.13 *Ο Ευκλείδιος αλγόριθμος υπολογίζει ένα μέγιστο κοινό διαιρέτη των* $a, b \in R$*, εφόσον* $b \neq 0$*.*

Απόδειξη: Κατ' αρχάς θα δείξουμε ότι ο αλγόριθμος τερματίζει. Παρατηρούμε ότι ο αλγόριθμος υπολογίζει μία ακολουθία υπολοίπων $r_0 = a, r_1 = b, r_{i-1} = r_i q_i + r_{i+1}$, για $i \geq 1$. Στο βήμα i υπολογίζει το υπόλοιπο r_{i+1}, σταματά εάν $r_{i+1} = 0$ και συνεχίζει διαφορετικά. Στη δεύτερη περίπτωση, έχουμε $N(r_{i+1}) < N(r_i)$. Εάν ο αλγόριθμος δεν τερμάτιζε, τότε θα

Algorithm 1 Ευκλείδιος αλγόριθμος

Precondition: $a, b \in R, b \neq 0$

```
function gcd(a, b)
    r_0 ← a
    r_1 ← b
    while r_1 ≠ 0 do
        r ← r_0 rem r_1
        (r_0, r_1) ← (r_1, r)
    end while
    return r_0
end function
```

είχαμε μία άπειρη γνησίως φθήνουσα ακολουθία μη αρνητικών ακεραίων, που είναι άτοπο.

Έστω ότι ο αλγόριθμος τερματίζει μετά από ℓ βήματα. Από την Πρόταση 1.13 έχουμε ότι ένας μέγιστος κοινός διαιρέτης των $r_\ell, 0$ είναι και μέγιστος κοινός διαιρέτης των $r_{\ell-1}, r_\ell$ και με μία εύκολη επαγωγή βλέπουμε ότι είναι μέγιστος κοινός διαιρέτης των r_0, r_1. Αρκεί να δείξουμε ότι ένας μέγιστος κοινός διαιρέτης των $r_\ell, 0$ είναι το r_ℓ, το οποίο είναι άμεσο από τον ορισμό του μέγιστου κοινού διαιρέτη. □

Ο Ευκλείδιος αλγόριθμος μπορεί να επεκταθεί ώστε δεδομένων $a, b \in R$, $b \neq 0$, να υπολογίζει ένα μέγιστο κοινό διαιρέτη d και συντελεστές $s, t \in R$, τέτοιους ώστε $d = sa + tb$.

Algorithm 2 Επεκτεταμένος Ευκλείδιος αλγόριθμος

Precondition: $a, b \in R, b \neq 0$

```
function gcd(a, b)
    (r_0, r_1) ← (a, b)
    (s_0, s_1) ← (1, 0)
    (t_0, t_1) ← (0, 1)
    while r_1 ≠ 0 do
        r ← r_0 rem r_1
        q ← r_0 div r_1
        (r_0, r_1) ← (r_1, r)
        (s_0, s_1) ← (s_1, s_0 − q · s_1)
        (t_0, t_1) ← (t_1, t_0 − q · t_1)
    end while
    return (r_0, s_0, t_0)
end function
```

Πρόταση 1.14 *Ο επεκτεταμένος Ευκλείδιος αλγόριθμος, δεδομένων $a, b \in R$, με $b \neq 0$, υπολογίζει ένα μέγιστο κοινό διαιρέτη d και συντελεστές $s, t \in R$ τέτοιους ώστε $d = sa + tb$.*

Απόδειξη: Κατ' αρχάς βλέπουμε ότι ο αλγόριθμος υπολογίζει τρεις ακολουθίες στοιχείων του R:

$$\begin{aligned}
r_0 &= a, \quad r_1 = b, \quad r_{i+1} = r_{i-1} - q_i r_i, \quad \text{για } i \geq 1 \\
s_0 &= 1, \quad s_1 = 0, \quad s_{i+1} = s_{i-1} - q_i s_i, \quad \text{για } i \geq 1 \\
t_0 &= 0, \quad t_1 = 1, \quad t_{i+1} = t_{i-1} - q_i t_i, \quad \text{για } i \geq 1
\end{aligned}$$

Η συνθήκη τερματισμού είναι ίδια με αυτή του Ευκλείδιου αλγόριθμου, οπότε όπως δείξαμε στην Πρόταση 1.13 τερματίζει μετά από ℓ βήματα και δίνει αποτέσμα την τριάδα

(r_ℓ, s_ℓ, t_ℓ). Έχουμε ήδη δείξει ότι r_ℓ είναι ένας μέγιστος κοινός διαιρέτης των a, b. Θα αποδείξουμε με επαγωγή ότι

$$r_i = s_i a + t_i b \quad \text{για} \quad 0 \le i \le \ell.$$

Για $i = 0, 1$ η πρόταση ισχύει, όπως βλέπουμε από τις αρχικές συνθήκες. Υποθέτουμε ότι η πρόταση ισχύει για κάθε $0 \le i \le k$ και θα δείξουμε ότι $r_{k+1} = s_{k+1}a + t_{k+1}b$. Πραγματικά,

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_k r_k \\ &= s_{k-1}a + t_{k-1}b - q_k(s_k a + t_k b) \\ &= (s_{k-1} - q_k s_k)a + (t_{k-1} - q_k t_k)b \\ &= s_{k+1}a + t_{k+1}b. \end{aligned}$$

Εφαρμόζοντας την πρόταση για $i = \ell$ έχουμε $r_\ell = s_\ell a + t_\ell b$. □

1.2.3 Ο δακτύλιος των ακεραίων

Θεώρημα 1.12 (Ευκλείδια διαίρεση μη αρνητικών ακεραίων) *Για κάθε $a, b \in \mathbb{Z}_{\ge 0}$ με $b > 0$ υπάρχουν $q, r \in \mathbb{Z}_{\ge 0}$ τέτοιοι ώστε $a = bq + r$ και $0 \le r < b$.*

Θεώρημα 1.13 (Ευκλείδια διαίρεση ακεραίων) *Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι Ευκλείδια περιοχή με βαθμίδα τη συνήθη απόλυτη τιμή.*

Απόδειξη: Είναι γνωστό ότι το $\mathbb{Z}$ είναι ακέραια περιοχή. Επίσης, για $a, b \in \mathbb{Z} \setminus \{0\}$, $|a| \le |ab|$. Θα δείξουμε ότι για κάθε $a, b \in \mathbb{Z}$ με $b \neq 0$ υπάρχουν $q, r \in \mathbb{Z}$ τέτοιοι ώστε $a = bq + r$ και $r = 0$ ή $|r| < |b|$. Θα διακρίνουμε περιπτώσεις. Κάθε περίπτωση ανάγεται στο Θεώρημα 1.12.
Εάν $a, b \ge 0$, το ζητούμενο προκύπτει άμεσα από το Θεώρημα 1.12.
Εάν $a \ge 0$ και $b < 0$, υπάρχουν $q, r \in \mathbb{Z}_{\ge 0}$ τέτοιοι ώστε $a = (-b)q + r$ και $0 \le r < -b = |b|$. Παρατηρούμε ότι ισχύει $a = b(-q) + r$ και $r = 0$ ή $|r| < |b|$.
Εάν $a < 0$ και $b > 0$, υπάρχουν $q, r \in \mathbb{Z}_{\ge 0}$ τέτοιοι ώστε $-a = bq + r$ και $0 \le r < b = |b|$. Παρατηρούμε ότι ισχύει $a = b(-q) + (-r)$ και $-r = 0$ ή $|-r| < |b|$.
Εάν $a < 0$ και $b < 0$, υπάρχουν $q, r \in \mathbb{Z}_{\ge 0}$ τέτοιοι ώστε $-a = (-b)q + r$ και $0 \le r < -b = |b|$. Παρατηρούμε ότι ισχύει $a = bq + (-r)$ και $-r = 0$ ή $|-r| < |b|$. □

Παρατηρήσεις 1.4

1. *Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$ είναι τα $\mathbb{Z}^* = \{-1, 1\}$.*
2. *Από το Θεώρημα 1.11 προκύπτει ότι ο δακτύλιος $\mathbb{Z}$ είναι ΠΚΙ και τα ανάγωγα στοιχεία ταυτίζονται με τα πρώτα στοιχεία. Παραδοσιακά ονομάζουμε πρώτους τους αριθμούς $2, 3, 5, \ldots$, όμως σύμφωνα με τον Ορισμό 1.11 πρώτα στοιχεία του δακτυλίου $\mathbb{Z}$ είναι και οι $\{-2, -3, -5, \ldots\}$.*
3. *Δεδομένων ακεραίων $a, b \in \mathbb{Z}$ υπάρχει μέγιστος κοινός διαιρέτης του d και τότε οι μέγιστοι κοινοί διαιρέτες των a, b είναι τα $d, -d$. Κάτα σύμβαση, επιλέγουμε να ονομάζουμε τον μέγιστο κοινό διαιρέτη τον μη αρνητικό από τους δύο αριθμούς (παρατηρήστε ότι αν $a = b = 0$ ο μέγιστος κοινός διαιρέτης είναι μοναδικός και ίσος με 0)*
4. *Έαν $n \in \mathbb{Z}$ με $n \ge 2$, ο δακτύλιος $\mathbb{Z}/\langle n\rangle$ είναι μεταθετικός δακτύλιος με μονάδα και είναι πεπερασμένος με στοιχεία $\{\overline{0}, \ldots, \overline{n-1}\}$.*
5. *Για $a, b \in \mathbb{Z}$ έχουμε $\overline{a} = \overline{b}$ αν και μόνο αν $a \equiv b \pmod n$ δηλαδή ισοδύναμα αν $n \mid a - b$.*

Πρόταση 1.15 *Έαν $n \in \mathbb{Z}$ ο δακτύλιος $\mathbb{Z}/\langle n\rangle$ είναι σώμα αν και μόνο αν το n είναι πρώτος.*

Απόδειξη: Σύμφωνα με το Θεώρημα 1.6, ο δακτύλιος $\mathbb{Z}/\langle n\rangle$ είναι σώμα αν και μόνο αν το ιδεώδες $\langle n\rangle$ είναι μεγιστικό, το οποίο ισχύει αν και μόνο αν το n είναι ανάγωγο. Σε περιοχές κυρίων ιδεωδών τα ανάγωγα και οι πρώτοι ταυτίζονται. □

Παρατηρούμε ότι αν το $n \ge 2$ δεν είναι πρώτος, τότε ο δακτύλιος $\mathbb{Z}/\langle n\rangle$ απαραίτητα περιέχει μηδενοδιαιρέτες, διαφορετικά θα ήταν σώμα, σύμφωνα με την Πρόταση 1.4. Δώστε ένα παράδειγμα μηδενοδιαιρέτη όταν $n = ab$ και $a, b \geq 2$.

1.3 Πολυωνυμικοί δακτύλιοι

1.4 Αριθμητικές συναρτήσεις

Ονομάζουμε *αριθμητική συνάρτηση* κάθε συνάρτηση $f : \mathbb{N} \to \mathbb{C}$.

Ορισμός 1.21 *Μία αριθμητική συνάρτηση* $f : \mathbb{N} \to \mathbb{C}$ *ονομάζεται* **πολλαπλασιαστική** *αν* $f(1) = 1$ *και για κάθε* $n, m \in \mathbb{N}$ *με* $(n, m) = 1$ *ισχύει* $f(nm) = f(n) \cdot f(m)$.

Ορισμός 1.22 *Αν* f, g *είναι αριθμητικές συναρτήσεις, η* **συνέλιξη** *τους είναι η συνάρτηση*

$$f * g : \mathbb{N} \longrightarrow \mathbb{C}, \quad \textit{με} \quad f * g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b).$$

Στον προηγούμενο ορισμό, το τελευταίο άθροισμα εκτείνεται πάνω στα ζεύγη $(a, b) \in \mathbb{N} \times \mathbb{N}$ με την ιδιότητα $ab = n$.

Πρόταση 1.16 *Έστω* f, g, h *αριθμητικές συναρτήσεις. Ισχύουν οι παρακάτω προτάσεις.*

1. $f * g = g * f$,
2. $(f * g) * h = f * (g * h)$,
3. $f * I = I * f = f$, *όπου* $I(1) = 1$ *και* $I(n) = 0$ *για* $n > 1$.

Τα πρώτα παραδείγματα πολλαπλασιαστικών αριθμητικών συναρτήσεων είναι οι συναρτήσεις

$$I : \mathbb{N} \longrightarrow \mathbb{C} \quad \text{με} \quad I(n) = \begin{cases} 1 & , \text{αν } n = 1 \\ 0 & , \text{αν } n > 1. \end{cases}$$

και

$$u : \mathbb{N} \longrightarrow \mathbb{C} \quad \text{με} \quad u(n) = 1.$$

Πρόταση 1.17 *Αν οι αριθμητικές συναρτήσεις* f, g *είναι πολλαπλασιαστικές, τότε και η* $f * g$ *είναι πολλαπλασιαστική.*

Απόδειξη: Έστω $n, m \in \mathbb{N}$ με $(n, m) = 1$. Αφού $(n, m) = 1$, κάθε διαιρέτης d του nm γράφεται με μοναδικό τρόπο ως $d_1 d_2$, με $d_1 \mid n$ και $d_2 \mid m$ και τότε έχουμε $(d_1, d_2) = 1$ και $(n/d_1, m/d_2) = 1$. Εξ' ορισμού της συνέλιξης

$$\begin{aligned} f * g(nm) &= \sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) \\ &= \sum_{d_1|n} \sum_{d_2|m} f(d_1 d_2) g\left(\frac{n}{d_1} \frac{m}{d_2}\right) \\ &= \sum_{d_1|n} \sum_{d_2|m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right) \\ &= \sum_{d_1|n} f(d_1) g\left(\frac{n}{d_1}\right) \sum_{d_2|m} f(d_2) g\left(\frac{m}{d_2}\right) \\ &= f * g(n) \cdot f * g(m). \end{aligned}$$

□

Ως ειδική περίπτωση της τελευταίας πρότασης παίρνουμε ότι η αρθμητική συνάρτηση με τύπο $h(n) = \sum_{d|n} f(d)$ είναι πολλαπλασιαστική, όταν η f είναι πολλαπλασιαστική, καθώς $h = f * u$.

Πρόταση 1.18 *Αν f είναι πολλαπλασιαστική συνάρτηση για $n = \prod_{i=1}^{k} p_i^{e_i}$ ισχύουν*

1. $f(n) = \prod_{i=1}^{k} f\left(p_i^{e_i}\right)$,
2. $\sum_{d|n} f(d) = \prod_{i=1}^{k} \sum_{j=0}^{e_i} f\left(p_i^{j}\right)$.

Ορισμός 1.23 *Η συνάρτηση $\mu : \mathbb{N} \to \mathbb{C}$ του* **Moebius** *ορίζεται $\mu(1) = 1$ και για $n > 1$ με κανονική ανάλυση σε πρώτους $n = p_1^{e_1} \cdots p_k^{e_k}$,*

$$\mu(n) = \begin{cases} 0 & , \text{αν } e_i > 1 \text{ για κάποιο } 1 \leq i \leq k \\ (-1)^k & , \text{αν } e_i = 1 \text{ για κάθε } 1 \leq i \leq k. \end{cases}$$

Πρόταση 1.19 *Η συνάρτηση μ του Moebius είναι πολλαπλασιαστική και $\mu * u = I$, δηλαδή*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & , \text{αν } n = 1 \\ 0 & , \text{αν } n > 1. \end{cases}$$

Απόδειξη: Ισχύει $\mu(1) = 1$ από τον ορισμό της συνάρτησης μ. Έστω $n, m \in \mathbb{N}$ με $n = \prod_{i=1}^{s} p_i^{a_i}$ και $m = \prod_{j=1}^{t} q_j^{b_j}$, όπου p_i, q_j είναι διακεκριμένοι πρώτοι. Αν κάποιο από τα a_i είναι τουλάχιστον 2, τότε $\mu(nm) = 0$ και $\mu(n) = 0$, οπότε $\mu(nm) = \mu(n)\mu(m)$. Το ίδιο ισχύει αν κάποιο από τα b_j είναι τουλάχιστον 2. Ας υποθέσουμε τώρα ότι $n = \prod_{i=1}^{s} p_i$ και $m = \prod_{j=1}^{t} q_j$. Τότε $\mu(nm) = (-1)^{s+t} = (-1)^s(-1)^t = \mu(n)\mu(m)$.

Για να δείξουμε ότι $\sum_{d|n} = I(n)$, βλέπουμε αρχικά ότι $\sum_{d|1} \mu(d) = \mu(1) = 1$. Για $n = \prod_{i=1}^{k} p_i^{a_i}$, έχουμε

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \cdots p_k} \mu(d),$$

δίοτι κάθε διαιρέτης $d \min n$ ο οποίος δεν περιλαμβάνεται στο δεύτερο άθροισμα διαιρείται από το τετράγωνο κάποιου πρώτου και ο αντίστοιχος όρος $\mu(d) = 0$. Από αυτή την παρατήρηση και την πολλαπλσιαστικότητα της μ έχουμε

$$\sum_{d|n} \mu(d) = \prod_{i=1}^{k} \sum_{j=0}^{1} \mu(p_i^j) = \prod_{i=1}^{k} (1 + \mu(p_i)) = 0$$

αφού $\mu(p_i) = -1$ για κάθε i. □

Θεώρημα 1.14 (Αντιστροφή Moebius) *Έστω συναρτήσεις $f, g : \mathbb{N} \to \mathbb{C}$. Αν*

$$f(n) = \sum_{d|n} g(d) \quad \text{για κάθε} \quad n \in \mathbb{N}$$

τότε

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \quad \text{για κάθε} \quad n \in \mathbb{N}.$$

Απόδειξη: Από τον ορισμό της συνάρτησης f βλέπουμε ότι $f = g * u$. Επίσης, από την Προσταση 1.19 έχουμε $\mu * u = I$. Οπότε

$$\mu * f = \mu * (g * u) = \mu * (u * g) = (\mu * u) * g = I * g = g.$$

□

Κεφάλαιο 2

Στοιχεία θεωρίας σωμάτων

2.1 Βασικοί ορισμοί

Ένα σώμα K ονομάζεται επέκταση ενός σώματος F εάν το F είναι υποδακτύλιος του και συμβολίζουμε K/F. Το σώμα K έχει τη δομή διανυσματικού χώρου πάνω από το F με πράξεις την πρόσθεση $+$ και βαθμωτό πολλαπλασιασμό $\cdot$ που δίνονται από τις αντίστοιχες πράξεις του σώματος K:

$$\begin{array}{rcl} + : K \times K & \longrightarrow & K \\ (a, b) & \mapsto & a + b \end{array}$$

$$\begin{array}{rcl} \cdot : F \times K & \longrightarrow & K \\ (\lambda, a) & \mapsto & \lambda a \end{array}$$

Ορισμός 2.1 *Η διάσταση του F-χώρου K ονομάζεται* **βαθμός της επέκτασης** *και συμβολίζεται $[K : F]$. Αν η διάσταση είναι πεπερασμένη, η επέκταση ονομάζεται* **πεπερασμένη**, *διαφορετικά ονομάζεται* **άπειρη**. *Μία F-βάση του K ονομάζεται βάση της επέκτασης K/F.*

Θεώρημα 2.1 *Έστω οι επεκτάσεις σωμάτων $F \subseteq L \subseteq K$. Η επέκταση K/F είναι πεπερασμένη αν και μόνο αν οι επεκτάσεις K/L και L/F είναι πεπερασμένες. Σε αυτή την περίπτωση ισχύει $[K : F] = [K : L][L : F]$.*

Απόδειξη: Αν η επέκαταση K/F είναι πεπερασμένη, τότε ο F-χώρος K έχει πεπερασμένη διάσταση. Τότε και ο F-χώρος L έχει πεπερασμένη διάσταση, ως υπόχωρος του K και μάλιστα $[L : F] \leq [K : F]$. Επίσης, κάθε υποσύνολο του K που είναι γραμμικώς πάνω από το L, είναι επίσης γραμμικώς ανεξάρτητο πάνω από το F. Αυτό σημαίνει ότι $[K : L] \leq [K : F]$.

Αντίστροφα, ας υποθέσουμε ότι $[K : L] = n$ και $[L : F] = m$ και ας θεωρήσουμε μία L-βάση του K, $\{a_1, \ldots, a_n\}$ και μία F-βάση του L, $\{b_1, \ldots, b_m\}$. Θα δείξουμε ότι το σύνολο $\mathcal{B} = \{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ είναι F-βάση του K. Κάθε στοιχείο $\gamma \in K$ γράφεται ως

$$\gamma = c_1 a_1 + \cdots + c_n a_n, \quad \text{με} \quad c_1, \ldots, c_n \in L.$$

Επίσης, κάθε c_i γράφεται ως $c_i = \lambda_{i1} b_1 + \cdots + \lambda_{im} b_m$ με $\lambda_{ij} \in F$ για $1 \leq i \leq n$, $1 \leq j \leq m$. Συνδυάζοντας τις παραπάνω σχέσεις, έχουμε

$$\gamma = \sum_{i=1}^{n} c_i a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} b_j a_i.$$

Άρα το σύνολο $\mathcal{B}$ παράγει τον χώρο K πάνω από το F. Για να δείξουμε ότι είναι γραμμικώς ανεξάρτητο, θεωρούμε $\lambda_{1,1}, \ldots, \lambda_{n,m} \in F$ και υπολογίζουμε

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} a_i b_j = 0 \implies \sum_{i=1} \left(\sum_{j=1}^{m} \lambda_{ij} b_j \right) a_i = 0.$$

Αφού το $\{a_1, \ldots, a_n\}$ είναι γραμμικώς ανεξάρτητο πάνω από το L και $\sum_{j=1}^{m} \lambda_{ij} b_j \in L$, παίρνουμε $\sum_{j=1}^{m} \lambda_{ij} b_j = 0$ για $1 \leq i \leq n$. Το $\{b_1, \ldots, b_m\}$ είναι γραμμικώς ανεξάρτητο πάνω από το F, οπότε παίρνουμε $\lambda_{ij} = 0$ για $1 \leq j \leq n$, $1 \leq j \leq m$. □

Ορισμός 2.2 *Έστω K/F μία επέκταση σωμάτων.*

1. *Ορίζουμε το δακτύλιο που παράγεται από τα $\alpha_1, \ldots, \alpha_n \in K$ πάνω από το F*

$$F[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) : f \in F[x_1, \ldots, x_n]\}.$$

2. *Ορίζουμε το σώμα που παράγεται από τα $\alpha_1, \ldots, \alpha_n$ πάνω από το F*

$$F(\alpha_1, \ldots, \alpha_n) = \{f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n) : f, g \in F[x_1, \ldots, x_n] \text{ και } g(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

3. *Ορίζουμε το σώμα που παράγεται από το υποσύνολο $X \subseteq K$ πάνω από το F*

$$F(X) = \bigcup_{S \subseteq X} F(S),$$

όπου η ένωση είναι πάνω σε όλα τα πεπερασμένα υποσύνολα $S \subseteq X$.

Λήμμα 2.1 *Έστω K/F μία επέκταση σωμάτων, $X \subseteq K$ και $L \subseteq K$ σώμα με τις ιδιότητες $F \subseteq L$ και $X \subseteq L$. Τότε $F(X) \subseteq L$.*

Απόδειξη: Έστω $\beta \in F(X)$. Τότε υπάρχουν $\alpha_1, \ldots, \alpha_n \in X$ τέτοια ώστε $\beta = f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$. Εξ' υποθέσεως $F \subseteq L$ και $\alpha_1, \ldots, \alpha_n \in L$ και το L είναι κλειστό ως προς τις πράξεις της πρόσθεσης και του πολλαπλασιασμού του K. Άρα $\beta \in L$. □

Ορισμός 2.3 *Η τομή όλων των υποσωμάτων ενός σώματος F είναι σώμα και ονομάζεται* **πρώτο σώμα** *του F.*

Πρόταση 2.1 *Έστω σώμα F. Εάν* $\mathrm{char}(F) = 0$ *τότε το πρώτο σώμα του F είναι ισόμορφο με το $\mathbb{Q}$. Εάν* $\mathrm{char}(F) = p$ *τότε το πρώτο σώμα του F είναι ισόμορφο με το $\mathbb{F}_p$.*

Απόδειξη: Εάν $\mathrm{char}(F) = 0$, ο ομομορφισμός

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow F \\ n &\mapsto n \cdot 1 \end{aligned}$$

είναι 1-1 και $\mathrm{im}\,\phi \cong \mathbb{Z}$. Αφού $\mathrm{im}\,\phi$ είναι ακέραια περιοχή και περιέχεται στο σώμα F, το F περιέχει το σώμα κλασμάτων του $\mathrm{im}\,\phi$, που είναι ισόμορφο με το $\mathbb{Q}$.

Εάν $\mathrm{char}(F) = 0$, θεωρούμε τον ομομορφισμό

$$\begin{aligned} \psi : \mathbb{Z} &\longrightarrow F \\ n &\mapsto n \cdot 1 \end{aligned}$$

με $\ker \psi = \langle p \rangle$. Από το Πρώτο Θεώρημα Ισομορφισμών έχουμε ότι $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle \cong \mathrm{im}\,\psi$. □

2.2 Αλγεβρικές επεκτάσεις

Ορισμός 2.4 *Έστω K/F μία επέκταση σωμάτων. Ένα στοιχείο $\alpha \in K$ ονομάζεται* **αλγεβρικό** *πάνω από το F εάν υπάρχει μη μηδενικό πολυώνυμο $f \in F[x]$, το οποίο έχει ρίζα το α, διαφορετικά ονομάζεται* **υπερβατικό** *πάνω από το F.*

Ορισμός 2.5 *Έστω επέκταση σωμάτων K/F.*

1. *Λέμε ότι η επέκταση K/F είναι* **πεπερασμένα παραγόμενη**, *αν υπάρχει $n \in \mathbb{N}$ και στοιχεία $\alpha_1, \ldots, \alpha_n \in K$ τέτοια ώστε $K = F(\alpha_1, \ldots, \alpha_n)$.*

2. *Λέμε ότι η επέκταση K/F είναι* **αλγεβρική**, *αν κάθε στοιχείο $a \in K$ είναι αλγεβρικό πάνω από το F.*

Εάν $\alpha \in K$ είναι αλγεβρικό πάνω από το F, τότε το σύνολο $S = \{f \in F[x] : f \neq 0 \text{ και } f(\alpha) = 0\}$ περιέχει τουλάχιστον ένα πολυώνυμο. Αν g είναι ένα τέτοιο πολυώνυμο ελάχιστου βαθμού με συντελεστή μεγιστοβάθμιου όρου ίσο με $c \in F^*$, τότε το πολυώνυμο $f = c^{-1}g$ είναι ένα μονικό πολυώνυμο του συνόλου S ελάχιστου βαθμού. Υπάρχει ένα μοναδικό πολυώνυμο με αυτές τις δύο ιδιότητες στο σύνολο S (γιατί;)

Ορισμός 2.6 *Έστω K/F μία επέκταση σωμάτων και $\alpha \in K$ ένα αλγεβρικό στοιχείο πάνω από το F. Το μοναδικό μονικό πολυώνυμο ελάχιστου βαθμού $f \in F[x]$ το οποίο έχει ρίζα το α ονομάζεται* **ελάχιστο πολυώνυμο** *του α πάνω από το F και το συμβολίζουμε $\min(\mathbb{F}, \alpha)$. Ο βαθμός του $\min(F, \alpha)$ ονομάζεται και βαθμός του α πάνω από το F.*

Πρόταση 2.2 *Έστω K/F μία επέκταση σωμάτων και $\alpha \in K$ ένα αλγεβρικό στοιχείο πάνω από το F. Για κάθε $f \in F[x]$ ισχύει $f(\alpha) = 0$ αν και μόνο αν $\min(F, \alpha) \mid f$.*

Απόδειξη: Ας είναι $m_\alpha = \min(F, \alpha)$. Από τον αλγόριθμο της Ευκλείδιας διαίρεσης στο δακτύλιο $F[x]$ υπάρχουν πολυώνυμα $g, r \in F[x]$ με $r = 0$ ή $\deg(r) < \deg(m_\alpha)$ τέτοια ώστε $f = m_\alpha g + r$. Τότε $r(\alpha) = f(\alpha) - m_\alpha(\alpha)g(\alpha) = 0$. Οπότε πρέπει $r = 0$, διαφορετικά θα είχαμε μη μηδενικό πολυώνυμο του $F[x]$ με ρίζα το α και βαθμό $< \deg(m_\alpha)$. □

Πρόταση 2.3 *Κάθε πεπερασμένη επέκταση σωμάτων K/F είναι αλγεβρική.*

Απόδειξη: Ας θεωρήσουμε $\alpha \in K$ και ας θεωρήσουμε την ενδιάμεση επέκταση $F \subseteq F(\alpha) \subseteq K$. Τότε $[F(\alpha) : F] \leq [K : F] < \infty$, ας υποθέσουμε $[F(\alpha) : F] = n$. Το σύνολο $\{1, \alpha, \ldots, \alpha^n\}$ περιέχει $n + 1$ στοιχεία και άρα είναι γραμμικώς εξαρτημένο πάνω από το F. Επομένως υπάρχουν $c_0, c_1, \ldots, c_n \in F$, όχι όλα ίσα με μηδέν, τέτοια ώστε $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$. Αυτό σημαίνει ότι το α είναι ρίζα του μη μηδενικού πολυωνύμου $c_0 + c_1x + \cdots + c_nx^n \in F[x]$. □

Θεώρημα 2.2 *Έστω K/F μία επέκταση σωμάτων. Ισχύουν οι παρακάτω προτάσεις.*

1. *Αν το $\alpha \in K$ είναι αλγεβρικό πάνω από το F, τότε το $\min(F, \alpha)$ είναι ανάγωγο πάνω από το F.*

2. *Αν το $\alpha \in K$ είναι αλγεβρικό πάνω από το F, τότε $F[\alpha] = F(\alpha)$ και μία βάση της επέκτασης $F(\alpha)/F$ είναι η $\{1, \alpha, \ldots, \alpha^{n-1}\}$, όπου $n = \deg(\min(F, \alpha))$.*

3. *Το $\alpha \in K$ είναι αλγεβρικό πάνω από το F αν και μόνο αν $[F(\alpha) : F] < \infty$.*

Απόδειξη: Ας υποθέσουμε ότι το $\min(F, \alpha)$ δεν είναι ανάγωγο. Τότε υπάρχουν μονικά πολυώνυμα $f, g \in F[x]$ με $1 \leq \deg(f), \deg(g) < \deg(\min(F, \alpha))$ τέτοια ώστε $\min(F, \alpha) = fg$. Τότε $f(\alpha)g(\alpha) = 0$ που συνεπάγεται ότι $f(\alpha) = 0$ ή $g(\alpha) = 0$. Και οι δύο περιπτώσεις έρχονται σε αντίφαση με την υπόθεση ότι το $\min(F, \alpha)$ είναι το μονικό πολυώνυμο *ελάχιστου βαθμού* που έχει ρίζα το α.

Για την δεύτερη πρόταση, προφανώς ισχύει $F[\alpha] \subseteq F(\alpha)$. Θεωρούμε τον ομομορφισμό δακτυλίων

$$\begin{aligned} \phi : F[x] &\longrightarrow K \\ f &\mapsto f(\alpha) \end{aligned}$$

Βλέπουμε ότι $\ker\phi = \langle \min(F,\alpha)\rangle$ και $\operatorname{im}\phi = F[\alpha]$. Από το Πρώτο Θεώρημα Ισομορφισμών, έχουμε $F[x]/\langle \min(F,\alpha)\rangle \cong F[\alpha]$. Το πολυώνυμο $\min(F,\alpha)$ είναι ανάγωγο, άρα ο δακτύλιος $F[x]/\langle \min(F,\alpha)\rangle$ είναι σώμα, άρα σώμα είναι και ο δακτύλιος $F[\alpha]$, το οποίο περιέχει το F και το α. Από το Λήμμα 2.1 προκύπτει ότι $F(\alpha) \subseteq F[\alpha]$ και συνεπώς $F(\alpha) = F[\alpha]$. Επίσης, παρατηρούμε ότι

$$F[\alpha] = \{f(\alpha) : f \in F[x], \deg(f) < n\} = \left\{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_0, c_1, \ldots, c_{n-1} \in F\right\}.$$

Για να το δει κανείς, αρκεί να παρατηρήσει ότι για $g \in F[x]$ υπάρχουν $h, f \in F[x]$ με $f = 0$ ή $\deg(f) < n$ τέτοια ώστε $g = \min(F,\alpha)\cdot h + f$. Τότε $g(\alpha) = f(\alpha)$. Αυτό δείχνει ότι το σύνολο $\{1, \alpha, \ldots, \alpha^{n-1}\}$ παράγει το K ως F-διανυσματικό χώρο. Είναι επίσης γραμμικώς ανεξάρτητο πάνω από το F: αν $c_0, c_1, \ldots, c_{n-1} \in F$ είναι τέτοια ώστε $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0$ τότε το α είναι ρίζα του $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, το οποίο οφείλει να είναι το μηδενικό πολυώνυμο, διαφορετικά θα είχαμε αντίφαση στην υπόθεση ότι το α έχει βαθμό n πάνω από το F.

Η τρίτη πρόταση είναι άμεση συνέπεια της δεύτερης και της Πρότασης 2.3. □

Λήμμα 2.2 *Έστω επέκταση σωμάτων K/F και $\alpha_1, \ldots, \alpha_n \in K$ αλγεβρικά πάνω από το F. Τότε*

$$[F(\alpha_1, \ldots, \alpha_n) : F] \leq [F(\alpha_1) : F] \cdots [F(\alpha_n) : F].$$

Απόδειξη: Η απόδειξη είναι με επαγωγή πάνω στο πλήθος των γεννητόρων n. Για $n = 1$, το αποτέλεσμα ισχύει τετριμμένα. Υποθέτουμε ότι για οποιαδήποτε επέκταση σωμάτων K/F και οποιαδήποτε $n-1$ στοιχεία $\alpha_1, \ldots, \alpha_{n-1}$ ισχύει $[F(\alpha_1, \ldots, \alpha_{n-1}) : F] \leq [F(\alpha_1) : F] \cdots [F(\alpha_{n-1}) : F]$. Θεωρούμε τώρα μία επέκταση K/F και στοιχεία $\alpha_1, \ldots, \alpha_{n-1}, \alpha_n \in K$. Παρατηρούμε ότι $F(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = L(\alpha_n)$, όπου $L = F(\alpha_1, \ldots, \alpha_{n-1})$. Από το Θεώρημα 2.1 έχουμε $[F(\alpha_1, \ldots, \alpha_n) : F] = [L(\alpha_n) : L][L : F]$. Από την επαγωγική υπόθεση έχουμε

$$[L : F] \leq [F(\alpha_1) : F] \cdots [F(\alpha_{n-1}) : F].$$

Από το Θεώρημα 2.2 έχουμε $[L(\alpha_n) : L] = \deg(\min(L, \alpha_n))$ και γνωρίζουμε ότι $\min(F, \alpha_n) \in L[x]$ και έχει ρίζα το α_n, οπότε $\min(L, \alpha_n) \mid \min(F, \alpha_n)$ και έχουμε

$$[L(\alpha_n) : L] = \deg(\min(L, \alpha_n)) \leq \deg(\min(F, \alpha_n)) = [F(\alpha_n) : F]$$

Το ζητούμενο προκύπτει συνδυάζοντας τις δύο ανισότητες. □

Θεώρημα 2.3 *Έστω επέκταση σωμάτων K/F και $X \subseteq K$ τέτοιο ώστε κάθε στοιχείο του X είναι αλγεβρικό πάνω από το F. Τότε η επέκταση $F(X)/F$ είναι αλγεβρική. Επιπλέον, αν $|X| < \infty$ τότε $[F(X) : F] < \infty$.*

Απόδειξη: Ας θεωρήσουμε $\beta \in F(X)$. Τότε θα υπάρχουν $\alpha_1, \ldots, \alpha_n \in X$ τέτοια ώστε $\beta \in F(\alpha_1, \ldots, \alpha_n)$. Τα α_i είναι αλγεβρικά πάνω από το F, οπότε οι βαθμοί $[F(\alpha_i) : F]$ είναι πεπερασμένοι. Από το Λήμμα 2.2 έχουμε ότι $[F(\alpha_1, \ldots, \alpha_n) : F] < \infty$ οπότε η επέκταση $F(\alpha_1, \ldots, \alpha_n)/F$ είναι αλγεβρική, άρα το β είναι αλγεβρικό πάνω από το F. □

2.3 Κανονικές επεκτάσεις

Ορισμός 2.7 *Έστω επέκταση σωμάτων K/F και $f \in F[x]$. Το f* **διασπάται** *πάνω από το K εάν $f = c\prod_{i=1}^{n}(x - \alpha_i) \in K[x]$ για κάποια $\alpha_1, \ldots, \alpha_n \in K$ και $c \in F$.*

Έαν έχουμε ένα σώμα F και ένα πολυώνυμο $f \in F[x]$, για να μιλάμε για τις ρίζες του f πρέπει να υπάρχει κάποια επέκταση του F στην οποία το f να διασπάται. Το επόμενο θεώρημα εξασφαλίζει την ύπαρξη τέτοιας επέκτασης.

Θεώρημα 2.4 *Έστω σώμα F και $f \in F[x]$ βαθμού $n \geq 1$.*

1. *Υπάρχει επέκταση K του F, με $[K : F] \leq n$, η οποία περιέχει μία ρίζα του f.*
2. *Υπάρχει επέκταση L του F, με $[L : F] \leq n!$, στην οποία διασπάται το f.*

Απόδειξη: Έστω $p(x)$ ένας ανάγωγος παράγοντας του $f(x)$. Το σώμα $F[x]/\langle p(x)\rangle$ περιέχει μία ισόμορφη εικόνα του F, όπως φαίνται από τον μονομορφισμό

$$\begin{aligned} \phi : F &\longrightarrow F[x]/\langle p(x)\rangle \\ c &\mapsto c + \langle p(x)\rangle \end{aligned}$$

Ταυτίζοντας το F με την εικόνα του, θεωρούμε το F υπόσωμα του $K = F[x]/\langle p(x)\rangle$. Μία ρίζα του f είναι η $\alpha = x + \langle p(x)\rangle$, όπως φαίνεται από τον παρακάτω υπολογισμό.

$$f\left(x + \langle p(x)\rangle\right) = f(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle.$$

Για τη δεύτερη πρόταση χρησιμοποιούμε επαγωγή στο βαθμό n του f. Για $n = 1$ $f(x) = c(x - \alpha) \in F[x]$ και το f διασπάται στο F. Υποθέτουμε ότι για κάθε σώμα F και κάθε πολυώνυμο $f \in F[x]$ βαθμού $< n$ υπάρχει επέκταση F στην οποία διασπάται και $[K : F] \leq (n-1)!$. Έστω $f \in F[x]$ με βαθμό n. Από την πρώτη πρόταση, υπάρχει επέκταση K του F η οποία περιέχει μία ρίζα α_n του f. Τότε $f(x) = c(x - \alpha_n)g(x)$ για κάποιο $g(x) \in K[x]$. Από την επαγωγική υπόθεση για το σώμα K και το πολυώνυμο g έχουμε ότι υπάρχει κάποια επέκταση L του K στην οποία το g διασπάται και $[L : K] \leq (n-1)!$. Οπότε τελικά το f διασπάται στο σώμα L και $[L : F] = [L : K][K : F] \leq (n-1)! \cdot n = n!$. □

Ορισμός 2.8 *Έστω επέκταση σωμάτων K/F και $f \in F[x]$.*

1. *Το ονομάζεται* **σώμα διάσπασης** *του f πάνω από το F αν $K = F(\alpha_1, \ldots, \alpha_n)$ και $\alpha_1, \ldots, \alpha_n$ είναι οι ρίζες του f.*
2. *Αν S είναι ένα σύνολο μη σταθερών πολυωνύμων του $F[x]$, τότε το K ονομάζεται σώμα διάσπασης του S αν κάθε $f \in S$ διασπάται στο K και $K = F(X)$, όπου X είναι το σύνολο όλων των ριζών των όλων των πολυωνύμων του S.*

Από τον Ορισμό 2.8 και το Λήμμα 2.1, βλέπουμε ότι το σώμα διάσπασης K ενός συνόλου πολυωνύμων S είναι «η μικρότερη επέκταση» του F στην οποία διασπάται κάθε πολυώνυμο του S, με την εξής έννοια: αν κάθε πολυώνυμο του S διασπάται σε μία επέκταση L του F, τότε $K \subseteq L$.

Πόρισμα 2.1 *Έστω σώμα F και $f_1, \ldots, f_m \in F[x]$. Υπάρχει σώμα διάσπασης του συνόλου $\{f_1, \ldots, f_m\}$ πάνω από το F.*

Απόδειξη: Ένα σώμα διάσπασης του πολυωνύμου $f = f_1 \cdots f_m$ είναι και σώμα διάσπασης του $\{f_1, \ldots, f_m\}$. Από το Θεώρημα 2.4 υπάρχει επέκταση L του F, η οποία περιέχει όλες τις ρίζες $\alpha_1, \ldots, \alpha_n$ του f. Τότε το $F(\alpha_1, \ldots, \alpha_n)$ είναι σώμα διάσπασης του f. □

Πόρισμα 2.2 *Έστω σώμα F και $F \in F[x]$ πολυώνυμο βαθμού n. Αν K είναι ένα σώμα διάσπασης του f πάνω από το F, τότε $[K : F] \leq n!$.*

Απόδειξη: Από το Θεώρημα 2.4 υπάρχει επέκταση L στην οποία το f διασπάται και $[L : F] \leq n!$. Επίσης, $F \subseteq K \subseteq L$, οπότε $[K : F] \leq [L : F]$. □

Ορισμός 2.9 *Μία επέκταση σωμάτων K/F ονομάζεται* **κανονική** *αν το K είναι το σώμα διάσπασης πάνω από το F ενός συνόλου πολυωνύμων του $F[x]$.*

Παρατηρήστε ότι η απόδειξη του Πορίσματος 2.1 κάνει ουσιαστική χρήση της υπόθεσης ότι το σύνολο $\{f_1, \ldots, f_m\}$ είναι πεπερασμένο. Η πρόταση ισχύει και για άπειρα σύνολα πολυωνύμων, όμως η απόδειξη της απαιτεί την έννοια της *αλβερικής θήκης* ενός σώματος.

Πρόταση 2.4 *Έστω σώμα F. Οι παρακάτω προτάσεις είναι ισοδύναμες.*

1. *Η μοναδική αλγεβρική επέκταση του F είναι το ίδιο το F.*
2. *Η μοναδική πεπερασμένη επέκταση του F είναι το ίδιο το F.*
3. *Κάθε $f \in F[x]$ διασπάται στο F.*
4. *Κάθε $f \in F[x]$ έχει ρίζα στο F.*

Απόδειξη: (1) $\Rightarrow$ (2): Έστω K μία πεπερασμένη επέκταση του F. Τότε είναι αλγεβρική, άρα εξ' υποθέσεως $K = F$.
(2) $\Rightarrow$ (3): Υπάρχει πεπερασμένη επέκταση, K, του F στην οποία το f διασπάται. Εξ' υποθέσεως θα πρέπει να είναι $K = F$.
(3) $\Rightarrow$ (4): Προφανές.
(4) $\Rightarrow$ (1): Έστω K μία αλγεβρική επέκταση του F. Έστω $\alpha \in K$. Θα δείξουμε ότι $\alpha \in F$. Το πολυώνυμο $\min(F, \alpha) \in F[x]$ είναι ανάγωγο στον $F[x]$ και εξ' υποθέσεως έχει μία ρίζα στο F, άρα $\min(F, \alpha) = x - \alpha$ και $\alpha \in F$. □

Ορισμός 2.10 *Κάθε σώμα K που έχει μία από τις ιδιότητες της Πρότασης 2.4 ονομάζεται* **αλγεβρικά κλειστό**. *Μία αλγεβρική επέκταση K ενός σώματος F η οποία είναι αλγεβρικά κλειστή ονομάζεται* **αλγεβρική θήκη** *του F.*

Θεώρημα 2.5 *Κάθε σώμα F έχει αλγεβρική θήκη.*

Πόρισμα 2.3 *Έστω σώμα F και S ένα σύνολο πολυωνύμων του $F[x]$. Υπάρχει σώμα διάσπασης του S πάνω από το F.*

Απόδειξη: Έστω K μία αλγεβρική θήκη του F. Τότε το σύνολο S διασπάται στο K. Αν $X \subseteq K$ είναι το σύνολο των ριζών όλων των πολυωνύμων του S, τότε το $F(X)$ είναι ένα σώμα διάσπαση του S πάνω από το F. □

Από το προηγούμενο Πόρισμα βλέπουμε ένα χρήσιμο τρόπο να βλέπουμε την αλγεβρική θήκη ενός σώματος F: είναι το σώμα διάσπασης όλων των πολυωνύμων του $F[x]$.

2.4 Διαχωρίσιμες επεκτάσεις

Έστω πολυώνυμο $f \in F[x]$. Το α είναι ρίζα του f *με πολλαπλότητα* m αν $(x-\alpha)^m \mid f$ και $(x-\alpha)^{m+1} \nmid f$. Μία ρίζα ονομάζεται *απλή* αν έχει πολλαπλότητα 1.

Ορισμός 2.11 *Έστω σώμα F. Ένα ανάγωγο πολυώνυμο $f \in F[x]$ ονομάζεται* **διαχωρίσιμο** *πάνω από το F εάν όλες οι ρίζες του, σε οποιοδήποτε σώμα διάσπασης του f πάνω από το F, είναι απλές. Ένα πολυώνυμο $f \in F[x]$ ονομάζεται διαχωρίσιμο πάνω από το F εάν κάθε ανάγωγος παράγοντας του είναι διαχωρίσιμο πολυώνυμο πάνω από το F.*

Οι παρακάτω παρατηρήσεις είναι άμεσες συνέπειες του ορισμού.

Παρατηρήσεις 2.1 *Έστω σώμα F.*

1. *Αν το $f \in F[x]$ έχει απλές ρίζες σε κάθε σώμα διάσπασης πάνω από το F, τότε είναι διαχωρίσιμο πάνω από το F.*
2. *Το αντίστροφο δεν ισχύει. Εάν $p(x) \in F[x]$ είναι διαχωρίσιμο ανάγωγο πολυώνυμο, τότε και το $p(x)^m$ είναι διαχωρίσιμο για κάθε $m \in \mathbb{N}$.*

3. *Αν το $f \in F[x]$ είναι διαχωρίσιμο πάνω από το F και $g \in F[x]$ με $g(x) \mid f(x)$ τότε και το g είναι διαχωρίσιμο πάνω από το F.*

4. *Αν τα $f_1, \dots, f_n \in F[x]$ είναι διαχωρίσιμα πάνω από το F, τότε και το $f = f_1 \cdots f_n$ είναι διαχωρίσιμο πάνω από το F.*

Ένα χρήσιμο εργαλείο για τον έλεγχο της πολλαπλότητας των ριζών πολυωνύμων είναι η έννοια της (τυπικής) παραγώγου.

Ορισμός 2.12 *Έστω σώμα F και $f = \sum_{i=0}^{n} c_i x^i \in F[x]$. Η* **παράγωγος** *του f είναι το πολυώνυμο $f' = \sum_{i=1}^{n} i c_i x^{i-1} \in F[x]$.*

Λήμμα 2.3 *Για κάθε $f, g \in F[x]$ και κάθε $c \in F$ ισχύουν τα παρακάτω:*

1. $(cf)' = cf'$

2. $(f+g)' = f' + g'$

3. $(fg)' = fg' + f'g$

Απόδειξη: Αφήνεται ως άσκηση. □

Πρόταση 2.5 *Έστω σώμα F και $f \in F[x]$ ένα μη σταθερό πολυώνυμο. Κάθε ρίζα του f είναι απλή αν και μόνο αν $(f, f') = 1$*

Απόδειξη: Έστω K ένα σώμα διάσπασης του f πάνω από το F. Ας υποθέσουμε ότι κάθε ρίζα του f είναι απλή. Αν τα πολυώνυμα f, f' δεν είναι σχετικώς πρώτα, τότε το (f, f') έχει βαθμό τουλάχιστον 1 και έχει κάποια ρίζα $\alpha \in K$ (η οποία είναι και ρίζα του f). Τότε $f(x) = (x-\alpha)g(x)$ για κάποιο $g(x) \in K[x]$ και $f'(x) = (x-\alpha)g'(x) + g(x)$. Αφού $x - \alpha \mid f'(x)$ έχουμε ότι $x - \alpha \mid g(x)$, οπότε το α είναι ρίζα του f πολλαπλότητας τουλάχιστον 2, που είναι άτοπο.

Αντίστροφα, αν $(f, f') = 1$ και υποθέσουμε ότι $\alpha \in K$ είναι μία ρίζα του f πολλαπλότητας τουλάχιστον 2, έχουμε $f(x) = (x-\alpha)^2 g(x)$ για κάποιο $g(x) \in K[x]$ και $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Τότε $x - \alpha \mid (f, f')$, που είναι άτοπο. □

Θεώρημα 2.6 *Έστω σώμα F και ανάγωγο πολυώνυμο $f \in F[x]$.*

1. *Αν $\mathrm{char}(F) = 0$ τότε το f είναι διαχωρίσιμο.*

2. *Αν $\mathrm{char}(F) = p$ τότε το f είναι μη διαχωρίσιμο αν και μόνο αν $f(x) = g(x^p)$ για κάποιο $g \in F[x]$.*

Απόδειξη: Από την προηγούμενη πρόταση, έχουμε ότι το f είναι διαχωρίσιμο αν και μόνο αν $(f, f') = 1$. Το f είναι ανάγωγο οπότε (f, f') είναι 1 ή f. Μένει να χαρακτηρίσουμε την περίπτωση $(f, f') = f$. Αυτό σημαίνει ότι $f \mid f'$, το οποίο μπορεί να συμβεί αν και μόνο αν $f'(x) = 0$, γιατί διαφορετικά $\deg(f') < \deg(f)$. Αν $\mathrm{char}(F) = 0$ ισχύει πάντα $f'(x) \neq 0$. Αν $\mathrm{char}(F) = p$, και $f(x) = \sum_{i=0}^{n} c_i x^i$ τότε $f'(x) = \sum_{i=1}^{n} i c_i x^{i-1}$. Το τελευταίο πολυώνυμο είναι το μηδενικό αν και μόνο αν $c_i = 0$ για κάθε $i \not\equiv 0 \pmod p$. Άρα $f(x) = \sum_j c_{pj} x^{pj} = g(x^p)$ με $g(x) = \sum_j c_{pj} x^j$. □

Ορισμός 2.13 *Έστω αλγεβρική επέκταση σωμάτων K/F. Ένα στοιχείο $\alpha \in K$ ονομάζεται* **διαχωρίσιμο** *πάνω από το F αν το $\min(F, \alpha)$ είναι διαχωρίσιμο πάνω από το F. Η επέκταση ονομάζεται διαχωρίσιμη αν κάθε στοιχείο του K είναι διαχωρίσιμο πάνω από το F.*

Αν F είναι σώμα και $d \in \mathbb{N}$ συμβολίζουμε $F^d = \{a^d : a \in F\}$.

Πρόταση 2.6 *Έστω σώμα F χαρακτηριστικής p. Κάθε αλγεβρική επέκταση K του F είναι διαχωρίσιμη αν και μόνο αν $F^p = F$.*

Απόδειξη: Ας υποθέσουμε ότι $F^p = F$. Έστω K μία αλγεβρική επέκταση του F και $\alpha \in K$. Αν το $\min(F,\alpha)$ δεν είναι διαχωρίσιμο πάνω από το F τότε $\min(F,\alpha) = g(x^p)$ για κάποιο $g(x) = \sum_{i=0}^{n} c_i x^i \in F[x]$, οπότε $\min(F,\alpha) = \sum_{i=0}^{n} c_i x^{pi}$. Όμως εξ' υποθέσεως, $c_i = b_i^p$ για $0 \le i \le n$ και $b_i \in F$. Οπότε $\min(F,\alpha) = \sum_{i=0}^{n} b_i^p x^{pi} = \left(\sum_{i=0}^{n} b_i x^i\right)^p$, που είναι άτοπο, αφού το $\min(F,\alpha)$ είναι ανάγωγο.

Αντίστροφα, ας υποθέσουμε ότι κάθε αλγεβρική επέκταση του F είναι διαχωρίσιμη. Προφανώς $F^p \subseteq F$. Για το τυχόν $a \in F$, θεωρούμε το πολυώνυμο $f(x) = x^p - a \in F[x]$ και ένα σώμα ανάλυσης του K. Αν $\beta \in K$ είναι μία ρίζα του f, τότε $\beta^p = a$. Οπότε $f(x) = x^p - \beta^p = (x-\beta)^p$. Η επέκταση K/F είναι αλγεβρική, άρα εξ' υποθέσεως είναι διαχωρίσιμη. Άρα το $\min(F,\beta) \in F[x]$ έχει απλές ρίζες και $\min(F,\beta) \mid f(x)$. Αυτό σημαίνει ότι $\min(F,\beta) = x - \beta$, δηλαδή $\beta \in F$. □

Ορισμός 2.14 *Ένα σώμα F ονομάζεται* **τέλειο** *αν κάθε αλγεβρική του επέκταση είναι διαχωρίσιμη.*

Ορισμός 2.15 *Μία επέκαταση σωμάτων K/F ονομάζεται* **Galois** *αν είναι κανονική και διαχωρίσιμη.*

2.5 Αυτομορφισμοί

Έστω K/F και K'/F δύο επεκτάσεις του σώματος F. Ένας ομομορφισμός $\sigma : K \to K'$ ο οποίος σταθεροποιεί το σώμα F, δηλαδή τέτοιος ώστε $\sigma|_F = id$, ονομάζεται F-ομομορφισμός. Επίσης, $\ker\sigma$ είναι ιδεώδες του K. Κάθε σώμα έχει δύο μόνο ιδεώδη, τα $\{0\}$ και K. Στη δεύτερη περίπτωση, ο σ είναι ο μηδενικός ομομορφισμός. Στην πρώτη περίπτωση, ο σ είναι μονομορφισμός. Έαν $K' = K$ και ο σ είναι ισομορφισμός ονομάζεται *F-αυτομορφισμός*.

Λήμμα 2.4 *Έστω K/F επέκταση σωμάτων και $\mathrm{Gal}(K/F)$ το σύνολο των F-αυτομορφισμών του K.*

1. *Το $\mathrm{Gal}(K/F)$ είναι ομάδα με πράξη τη σύνθεση συναρτήσεων.*
2. *Κάθε $\sigma \in \mathrm{Gal}(K/F)$ είναι F-γραμμική απεικόνιση.*

Απόδειξη: Αφήνεται ως άσκηση. □

Παρατηρήσεις 2.2 *Έστω $K = F(\alpha_1, \ldots, \alpha_m)$ αλγεβρική επέκταση του F και $\sigma \in \mathrm{Gal}(K/F)$. Ο σ καθορίζεται από τις τιμές $\sigma(\alpha_i)$, για $1 \le i \le m$. Αρκεί να παρατηρήσουμε ότι αν $\gamma \in K$ υπάρχουν $c_{i_1,\ldots,i_m} \in F$ τέτοια ώστε $\gamma = \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} \alpha_1^{i_1} \cdots \alpha_m^{i_m}$, οπότε*

$$\begin{aligned}
\sigma(\gamma) &= \sigma\left(\sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} \alpha_1^{i_1} \cdots \alpha_m^{i_m}\right) \\
&= \sum_{i_1,\ldots,i_m} \sigma(c_{i_1,\ldots,i_m}) \sigma(\alpha_1)^{i_1} \cdots \sigma(\alpha_m)^{i_m} \\
&= \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} \sigma(\alpha_1)^{i_1} \cdots \sigma(\alpha_m)^{i_m}
\end{aligned}$$

αφού ο σ είναι αυτομορφισμός και σταθεροποιεί το F.

Ορισμός 2.16 *Έστω επέκταση σωμάτων K/F. Το σύνολο των F-αυτομορφισμών του K ονομάζεται* **ομάδα Galois** *της επέκτασης και συμβολίζεται $\mathrm{Gal}(K/F)$.*

Λήμμα 2.5 (Λήμμα του Dedekind) *Έστω ομάδα G, σώμα και $\rho_1, \ldots, \rho_m$ διακεκριμένοι ομομορφισμοί $G \to K^*$. Τότε οι $\rho_1, \ldots, \rho_m$ είναι γραμμικώς ανεξάρτητοι πάνω από το K. Δηλαδή εάν $\sum_{i=1}^{m} c_i \rho_i$ είναι η μηδενική απεικόνιση, τότε $c_i = 0$ για $1 \le i \le m$.*

Πρόταση 2.7 *Έστω K/F πεπερασμένη επέκταση. Τότε $|\mathrm{Gal}(K/F)| \le [K : F]$.*

Θεώρημα 2.7 *Μία απλή αλγεβρική επέκταση $F(\alpha)/F$ είναι Galois αν και μόνο αν* $|\mathrm{Gal}(F(\alpha)/F)| = [F(\alpha) : F]$. *Τότε το* $\min(F, \alpha)$ *έχει απλές ρίζες* $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_n$ *και*

$$\mathrm{Gal}(F(\alpha)/F) = \{\sigma_i : 0 \leq i \leq n-1\},$$

όπου $\sigma_i(\alpha) = \alpha_i$.

Κεφάλαιο 3

Πεπερασμένα σώματα

3.1 Βασική δομή

Πρόταση 3.1 *Έστω F ένα πεπερασμένο σώμα. Τότε* $\mathrm{char}(F) = p$ *πρώτος αριθμός.*

Απόδειξη: Το σύνολο $A = \{n \cdot 1 : n \in \mathbb{N}\}$ είναι πεπερασμένο, ως υποσύνολο του F. Άρα υπάρχουν $m, n \in \mathbb{N}$, με $m > n$ τέτοιοι ώστε $m \cdot 1 = n \cdot 1$. Αυτό σημαίνει ότι $(m - n) \cdot 1 = 0$ και $m - n > 0$, οπότε το F έχει θετική χαρακτηριστική. Από την Πρόταση 1.6 προκύπτει ότι η χαρακτηριστική του F είναι κάποιος πρώτος p. □

Θεώρημα 3.1 *Έστω p πρώτος αριθμός.*

1. *Υπάρχει σώμα $\mathbb{F}_p$ με p στοιχεία.*
2. *Κάθε σώμα με p στοιχεία είναι ισόμορφο με το $\mathbb{F}_p$.*

Απόδειξη: Έστω πρώτος αριθμός p. Από την Πρόταση 1.15 βλέπουμε ότι το $\mathbb{F}_p = \mathbb{Z}/\langle p\rangle$ είναι σώμα. Έστω F σώμα με p στοιχεία. Θεωρούμε τον ομομορφισμό

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow F \\ n &\mapsto n \cdot 1 \end{aligned}$$

Παρατηρούμε ότι $\{n \cdot 1 : 0 \le n < p\} \subseteq \mathrm{im}\,\phi$ και $|\{n \cdot 1 : 0 \le n < p\}| = p$, οπότε $\mathrm{im}\,\phi = F$. Επίσης,

$$\begin{aligned} n \in \ker\phi &\iff n \cdot 1 = 0 \\ &\iff p \mid n \\ &\iff n \in \langle p\rangle, \end{aligned}$$

δηλαδή $\ker\phi = \langle p\rangle$. Από το Πρώτο θεώρημα Ισομορφισμών έχουμε $\mathbb{Z}/\langle p\rangle \cong F$. □

Πρόταση 3.2 *Έστω F πεπερασμένο σώμα χαρακτηριστικής p. Τότε το F περιέχει το $\mathbb{F}_p$ και $|F| = p^n$ για κάποιο $n \in \mathbb{N}$.*

Απόδειξη: Θεωρούμε τον ομομορφισμό

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow F \\ a &\mapsto a \cdot 1 \end{aligned}$$

Από το Πρώτο Θεώρημα Ισομορφισμών, παίρνουμε τον μονομορφισμό

$$\begin{aligned} \tilde{\phi} : \mathbb{Z}/\langle p\rangle &\longrightarrow F \\ \overline{a} &\mapsto a \cdot 1 \end{aligned}$$

Άρα το F περιέχει ένα ισόμορφο αντίγραφο του $\mathbb{F}_p$. Από εδώ και στο εξής, θα ταυτίζουμε το $\phi(\mathbb{Z})$ με το $\mathbb{F}_p$.

Το σώμα F είναι επέκταση του $\mathbb{F}_p$ και αφού είναι πεπερασμένο, έχει πεπερασμένη διάσταση n πάνω από το $\mathbb{F}_p$. Αν $\{\alpha_1, \ldots, \alpha_n\}$ είναι μία $\mathbb{F}_p$-βάση του F, τότε κάθε στοιχείο του F γράφεται με μοναδικό τρόπο ως $c_1\alpha_1 + \cdots + c_n\alpha_n$, με $c_1, \ldots c_n \in \mathbb{F}_p$. Από απλή συνδυαστική παίρνουμε ότι $|F| = p^n$. □

Πρόταση 3.3 *Έστω πρώτος p και K ένα σώμα με $q = p^n$ στοιχεία. Τότε για κάθε $\alpha \in K$ ισχύει $\alpha^q = \alpha$.*

Απόδειξη: Η πολλαπλασιαστική ομάδα L^* περιέχει $q - 1$ στοιχεία, οπότε από το Θεώρημα του Lagrange έχουμε $\alpha^{q-1} = 1$ για κάθε $\alpha \in K \setminus \{0\}$. Οπότε $\alpha^q = \alpha$. Η τελευταία σχέση ικανοποιείται και από το 0. □

Θεώρημα 3.2 (Ύπαρξη και μοναδικότητα) *Έστω πρώτος αριθμός p και $n \in \mathbb{N}$. Αν $\overline{\mathbb{F}}_p$ είναι μια αλγεβρική θήκη του $\mathbb{F}_p$, υπάρχει ένα μοναδικό πεπερασμένο σώμα με p^n στοιχεία εντός της $\overline{\mathbb{F}}_p$. Το σώμα αυτό συμβολίζεται με $\mathbb{F}_{p^n}$ και είναι το σύνολο των ριζών του $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Απόδειξη: Σταθεροποιούμε μία αλγεβρική θήκη $\overline{\mathbb{F}}_p$ του $\mathbb{F}_p$ και θεωρούμε το πολυώνυμο $f(x) = x^q - x \in \mathbb{F}_p[x]$, όπου $q = p^n$. Το πολυώνυμο έχει παράγωγο $f'(x) = -1$, οπότε $(f, f') = 1$ και από την Πρόταση 2.5 προκύπτει ότι το $f(x)$ έχει απλές ρίζες. Στην αλγεβρική θήκη διασπάται, οπότε το σύνολο $K = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^q = \alpha\}$ έχει ακριβώς q στοιχεία. Μπορούμε εύκολα να διαπιστώσουμε ότι το K σώμα που περιέχει το $\mathbb{F}_p$: για $\alpha, \beta \in K$ έχουμε $\alpha^q = \alpha$ και $\beta^q = \beta$. Θα δείξουμε ότι $\alpha - \beta \in K$, $\alpha\beta \in K$ και $\alpha^{-1} \in K$ εφόσον $\alpha \neq 0$.

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta,$$

όπου χρησιμοποιήσαμε το Θεώρημα 1.8. Παρόμοια,

$$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$$

και

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}.$$

Επίσης, για κάθε $a \in \mathbb{F}_p$, έχουμε $a^p = a$. Μία απλή επαγωγή μας δίνει $a^{p^n} = a$, οπότε $a \in K$.

Για να δείξουμε τη μοναδικότητα, υποθέτουμε ότι $L \subset \overline{\mathbb{F}}_p$ είναι ένα σώμα με q στοιχεία. Τότε για κάθε $\gamma \in L$ έχουμε $\gamma^q = \gamma$, οπότε $\gamma \in K$, άρα $L \subseteq K$. Εξ' υποθέσεως $|K| = |L| = q$, οπότε $L = K$. □

Θεώρημα 3.3 *Έστω σώμα F. Κάθε πεπερασμένη υποομάδα της F^* είναι κυκλική.*

Απόδειξη: Έστω G μια υποομάδα της F^* με $|G| = n$ και ας είναι $\exp(G) = m$. Γνωρίζουμε από το Θεώρημα 1.3, ότι $m \mid n$. Από τον ορισμό του εκθέτη της G, έχουμε $a^m = 1$ για κάθε $a \in G$, άρα το πολυώνυμο $x^m - 1 \in F[x]$ έχει n διακεκριμένες ρίζες. Αυτό σημαίνει ότι $n \leq m$, οπότε $n = m$. Το Θεώρημα 1.3 μας δίνει το ζητούμενο. □

Πόρισμα 3.1 *Η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι κυκλική.*

Λήμμα 3.1 *Έστω $q, m, n \in \mathbb{N}$ και σώμα F. Ισχύουν οι παρακάτω προτάσεις.*

1. *$q^m - 1 \mid q^n - 1$ αν και μόνο αν $m \mid n$.*
2. *Στο δακτύλιο $F[x]$, $x^m - 1 \mid x^n - 1$ αν και μόνο αν $m \mid n$.*
3. *Στο δακτύλιο $F[x]$, $x^{q^m} - x \mid x^{q^n} - x$ αν και μόνο αν $m \mid n$.*

Απόδειξη: Έστω $q^m - 1 \mid q^n - 1$. Τότε $q^n \equiv 1 \pmod{q^m - 1}$, οπότε η τάξη του $q \bmod q^m - 1$ στην ομάδα $\mathbb{Z}/\langle q^m - 1\rangle$ διαιρεί το n. Όμως η τάξη αυτή είναι ίση με m (γιατί;). Αντίστροφα, αν $n = md$ με $d \in \mathbb{N}$ έχουμε

$$q^n - 1 = (q^m)^d - 1 = (q^m - 1)(q^{m(d-1)} + \cdots + q^m + 1).$$

Για τη δεύτερη πρόταση, υποθέτουμε $n = md$, με $d \in \mathbb{N}$. Τότε

$$x^n - 1 = (x^m)^d - 1 = (x^m - 1)(x^{m(d-1)} + \cdots + x^m + 1).$$

Αντίστροφα, υποθέτουμε $x^m - 1 \mid x^n - 1$. Εκτελώντας Ευκλείδια διαίρεση του n με το m, έχουμε $n = md + r$, με $0 \le r < m$, οπότε

$$x^n - 1 = x^{md+r} - x^r + x^r - 1 = x^r(x^{md} - 1) + x^r - 1.$$

Εξ' υποθέσεως $x^m - 1 \mid x^n - 1$ και έχουμε ήδη δείξει ότι $x^m - 1 \mid x^{md} - 1$, οπότε $x^m - 1 \mid x^r - 1$. Αφού $0 \le r < m$ αυτό μπορεί να συμβεί μόνο αν $r = 0$.

Η τρίτη πρόταση προκύπτει συνδυάζοντας τις δύο πρώτες:

$$\begin{aligned} x^{q^m} - x \mid x^{q^n} - x &\iff x^{q^m-1} - 1 \mid x^{q^n-1} - 1 \\ &\iff q^m - 1 \mid q^n - 1 \\ &\iff m \mid n. \end{aligned}$$

□

Πρόταση 3.4 *Έστω q δύναμη ενός πρώτου p και $m, n \in \mathbb{N}$. Τότε $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ αν και μόνο αν $m \mid n$. Σε αυτή την περίπτωση, $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] = n/m$.*

Απόδειξη: Αρχικά παρατηρούμε ότι το $\mathbb{F}_{q^m}$ είναι το σύνολο των ριζών του $x^{q^m} - x$ και το $\mathbb{F}_{q^n}$ είναι το σύνολο των ριζών του $x^{q^n} - x$. Επίσης, όπως έχουμε δει στην απόδειξη του Θεωρήματος 3.2, τα πολυώνυμα αυτά έχουν απλές ρίζες. Τότε $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ αν και μόνο αν κάθε ρίζα του $x^{q^m} - x$ είναι ρίζα του $x^{q^n} - x$, το οποίο ισχύει αν και μόνο αν $x^{q^m} - x \mid x^{q^n} - x$ που από το Λήμμα 3.1 είναι ισοδύναμο με $m \mid n$.

Ας υποθέσουμε τώρα ότι $m \mid n$ και $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] = d$. Το συνδυαστικό επιχείρημα της απόδειξης της Πρότασης 3.2 δείχνει ότι το πλήθος των στοιχείων του $\mathbb{F}_{q^n}$ είναι $q^n = (q^m)^d$. Άρα $n = md$. □

Πόρισμα 3.2 *Έστω q δύναμη ενός πρώτου p και $n \in \mathbb{N}$. Υπάρχει μοναδική επέκταση βαθμού n του $\mathbb{F}_q$.*

Απόδειξη: Από το Θεώρημα 3.2 είναι σαφές ότι υπάρχουν τα σώματα $\mathbb{F}_q$ και $\mathbb{F}_{q^n}$ και από την Πρόταση 3.4 έχουμε $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$. Κάθε επέκταση K του $\mathbb{F}_q$ βαθμού n έχει κάποια $\mathbb{F}_q$-βάση $\{\gamma_1, \ldots, \gamma_n\}$, οπότε κάθε στοιχείο του K γράφεται μοναδικά ως $c_1\gamma_1 + \cdots + c_n\gamma_n$, με $c_1, \ldots, c_n \in \mathbb{F}_q$. Άρα $|K| = q^n = |\mathbb{F}_{q^n}|$ και η μοναδικότητα προκύπτει από το Θεώρημα 3.2. □

Πόρισμα 3.3 *Αν q είναι δύναμη πρώτου p και $n \in \mathbb{N}$, τότε $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ για κάποιο $\alpha \in \mathbb{F}_{q^n}$ με $\deg(\min(\mathbb{F}_q, \alpha)) = n$. Ειδικότερα, υπάρχει ανάγωγο πολυώνυμο βαθμού n πάνω από το $\mathbb{F}_q$ για κάθε $n \in \mathbb{N}$.*

Απόδειξη: Αρχικά από την Πρόταση 3.4 έχουμε $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$. Επίσης, αν $\alpha \in \mathbb{F}_{q^n}$ είναι ένας γεννήτορας της $\mathbb{F}_{q^n}^*$, τότε κάθε μη μηδενικό στοιχείο του $\mathbb{F}_{q^n}$ γράφεται ως δύναμη του α. Άρα $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Επίσης,

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(\min(\mathbb{F}_q, \alpha)).$$

□

Πρόταση 3.5 *Έστω q δύναμη ενός πρώτου p και $f \in \mathbb{F}_q[x]$ ανάγωγο βαθμού d.*

1. *Όλες οι ρίζες του f είναι απλές.*

2. *Αν $f(\alpha) = 0$, τότε το σύνολο των ριζών του f είναι το $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\} \subseteq \mathbb{F}_q(\alpha)$.*

Απόδειξη: Αν $f(x) = x$, τότε $\alpha = 0$ και το θεώρημα ισχύει. Υποθέτουμε $f(x) \neq x$. Έστω $f(x) = \sum_{i=0}^m c_i x^i \in \mathbb{F}_q[x]$. Τότε για $0 \leq j \leq d-1$ έχουμε $c_i^{q^j} = c_i$ και υπολογίζουμε

$$f\left(\alpha^{q^j}\right) = \sum_{i=0}^{m} c_i \alpha^{iq^j} = \sum_{i=0}^{m} c_i^{q^j} \alpha^{iq^j} = \left(\sum_{i=0}^{m} c_i \alpha^i\right)^{q^j} = 0$$

Οπότε το f έχει τις ρίζες α^{q^j} για $0 \leq j \leq d-1$ οι οποίες ανήκουν στο $\mathbb{F}_q(\alpha)$. Θα δείξουμε ότι είναι διακεκριμένες.

Αν $\alpha^{q^i} = \alpha^{q^j}$ για κάποια $0 \leq i < j \leq d-1$, έχουμε $\alpha^{q^j - q^i} = 1$ οπότε $\alpha^{q^i(q^{j-i}-1)} = 1$. Όμως $\mathrm{ord}(\alpha) \mid q^d - 1$, άρα $(\mathrm{ord}(\alpha), q^i) = 1$ και υπάρχουν $s, t \in \mathbb{Z}$ τέτοιοι ώστε $s\,\mathrm{ord}(\alpha) + t\,q^i = 1$. Τότε $\alpha^{tq^i} = \alpha^{1-s\,\mathrm{ord}(\alpha)} = \alpha$. Υπολογίζουμε

$$\begin{aligned} \alpha^{q^i(q^{j-i}-1)} &= 1 \Longrightarrow \\ \alpha^{tq^i(q^{j-i}-1)} &= 1 \Longrightarrow \\ \alpha^{q^{j-i}-1} &= 1 \Longrightarrow \\ \alpha^{q^{j-i}} &= \alpha. \end{aligned}$$

Αυτό σημαίνει ότι $\alpha \in \mathbb{F}_{q^{j-i}}$, οπότε $\mathbb{F}_q \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^{j-i}}$. Άρα $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] \mid [\mathbb{F}_{q^{j-i}} : \mathbb{F}_q]$ ή ισοδύναμα $d \mid j - i$, το οποίο είναι άτοπο, αφού $0 < j - i < d$. □

Θεώρημα 3.4 *Έστω q δύναμη ενός πρώτου p και $n \in \mathbb{N}$. Η επέκταση $\mathbb{F}_{q^n}/\mathbb{F}_q$ είναι Galois και*

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \left\{\phi^i : 0 \leq i \leq n-1\right\},$$

όπου

$$\begin{aligned} \phi : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ \beta &\mapsto \beta^q \end{aligned}$$

είναι ο αυτομορφισμός του Frobenius.

Απόδειξη: Έστω $\beta \in \mathbb{F}_{q^n}$. Το $\min(\mathbb{F}_q, \beta)$ έχει απλές ρίζες, άρα το β είναι διχωρίσιμο πάνω από το $\mathbb{F}_q$. Άρα η επέκταση $\mathbb{F}_{q^n}/\mathbb{F}_q$ είναι διαχωρίσιμη.

Γνωρίζουμε ότι $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ για κάποιο $\alpha \in \mathbb{F}_{q^n}$, με $\deg(\min(\mathbb{F}_q, \alpha)) = n$. Τότε όλες οι ρίζες του $\min(\mathbb{F}_q, \alpha)$ ανήκουν στο $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Άρα το $\mathbb{F}_{q^n}$ είναι το σώμα διάσπασης του $\min(\mathbb{F}_q, \alpha)$ πάνω από το $\mathbb{F}_q$. Άρα η επέκταση $\mathbb{F}_{q^n}/\mathbb{F}_q$ είναι κανονική.

Από το Θεώρημα 2.7 έχουμε ότι η ομάδα $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ έχει $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ αυτομορφισμούς:

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \{\phi_i : 0 \leq i \leq n-1\},$$

οπου $\phi_i(\alpha) = \alpha^{q^i}$, για $0 \leq i \leq n-1$. Τότε για το τυχόν $\beta = \sum_{j=0}^m c_j \alpha^j \in \mathbb{F}_{q^n}$ με $c_j \in \mathbb{F}_q$, έχουμε

$$\begin{aligned} \phi_i(\beta) &= \sum_{j=0}^{m} c_j \phi_i(\alpha)^j = \sum_{j=0}^{m} c_j \alpha^{q^i j} \\ &= \left(\sum_{j=0}^{m} c_j \alpha^j\right)^{q^i} = \beta^{q^i} \end{aligned}$$

Τέλος βλέπουμε ότι $\phi^i(\alpha) = \alpha^{q^i} = \phi_i(\alpha)$, οπότε $\phi_i = \phi^i$ για $0 \leq i \leq n-1$. □

3.2 Ανάγωγα πολυώνυμα

Ορισμός 3.1 *Έστω q δύναμη πρώτου p και $n \in \mathbb{N}$. Συμβολίζουμε με $\mathbb{I}_q(n)$ το σύνολο των μονικών αναγώγων πολυωνύμων του $\mathbb{F}_q[x]$ βαθμού n. Συμβολίζουμε με $\pi_q(n)$ το πλήθος τους, δηλαδή $\pi_q(n) = |\mathbb{I}_q(n)|$.*

Θεώρημα 3.5 *Έστω q δύναμη πρώτου p και $n \in \mathbb{N}$. Τότε το πολυώνυμο $x^{q^n} - x$ είναι ίσο με το γινόμενο όλων των μονικών αναγώγων του $\mathbb{F}_q[x]$ βαθμού $d \mid n$. Δηλαδή*

$$x^{q^n} - x = \prod_{d|n} \prod_{f \in \mathbb{I}_q(d)} f.$$

Απόδειξη: Έχουμε δει με το κριτήριο της παραγώγου, ότι το πολυώνυμο $F(x) = x^{q^n} - x \in \mathbb{F}_q[x]$ έχει απλές ρίζες. Έστω $f \in \mathbb{F}_q[x]$ ένα μονικό ανάγωγο στην κανονική ανάλυση του F βαθμού d. Αν α είναι μία ρίζα του f, τότε είναι και ρίζα του F, δηλαδή $\alpha^{q^n} = \alpha$, οπότε $\alpha \in \mathbb{F}_{q^n}$. Αυτό σημαίνει

$$\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}.$$

Από την Πρόταση 3.4 συμπεραίνουμε ότι $d \mid n$.

Μένει να δείξουμε ότι *κάθε* μονικό ανάγωγο βαθμού $d \mid n$ διαιρεί το F. Έστω $f \in \mathbb{I}_q(d)$ για κάποιο $d \mid n$. Αν α είναι μία ρίζα του f, τότε $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(f) = d$, δηλαδή $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$. Αφού $d \mid n$ έχουμε $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, οπότε $\alpha \in \mathbb{F}_{q^n}$. Προκύπτει ότι $\alpha^{q^n} = \alpha$, δηλαδή $F(\alpha) = 0$, οπότε $f \mid F$. □

Θεώρημα 3.6 *Έστω q δύναμη πρώτου p και $n \in \mathbb{N}$. Τότε ισχύουν τα παρκάτω:*

1. $\pi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}$,
2. $\left|\pi_q(n) - \frac{q^n}{n}\right| < \frac{2}{n}\, q^{\frac{n}{2}}$.

Απόδειξη: Από το Θεώρημα 3.5 συγκρίνοντας τους βαθμούς του αριστερού και του δεξιού μέλους της ισότητας έχουμε

$$q^n = \sum_{d|n} d\pi_q(n).$$

Με αντιστροφή Moebius, παίρουμε τον τύπο της πρώτη πρότασης

$$n\, \pi_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Για τη δεύτερη πρόταση έχουμε

$$n\, \pi_q(n) = q^n + \sum_{\substack{d|n \\ d>1}} \mu(d) q^{\frac{n}{d}}$$

και υπολογίσουμε το φράγμα για το άθροισμα του δεύτερου μέλους:

$$\Big|\sum_{\substack{d|n \\ d>1}} \mu(d) q^{\frac{n}{d}}\Big| \le \sum_{\substack{d|n \\ d>1}} q^{\frac{n}{d}} \le \sum_{j=1}^{n/2} q^j = q\frac{q^{\frac{n}{2}} - 1}{q-1} < 2q^{\frac{n}{2}},$$

διότι $q/(q-1) \le 2$ για κάθε $q \ge 2$. □

3.3 Κυκλοτομικά πολυώνυμα

Ένα στοιχείο ζ ενός σώματος F ονομάζεται n-οστή **ρίζα της μονάδας** αν $\zeta^n = 1$ και **πρωταρχική** n-οστή ρίζα της μονάδας αν $\zeta^n = 1$ και $\zeta^k \neq 1$ για κάθε $1 \leq k < n$. Βλέπουμε άμεσα ότι κάθε μη μηδενικό στοιχείο ενός πεπερασμένου σώματος $\mathbb{F}_q$ είναι $q-1$ τάξης ρίζα της μονάδας και είναι πρωταρχική n-οστή ρίζα της μονάδας, όπου n είναι η τάξη του στοιχείου στην ομάδα $\mathbb{F}_q^*$.

Πρόταση 3.6 *Έστω πρώτος p και $n \in \mathbb{N}$. Υπάρχει πρωταρχική n-οστή ρίζα της μονάδας στο $\overline{\mathbb{F}}_p$ αν και μόνο αν $(n,p) = 1$. Αν $(n,p) = 1$ τότε υπάρχει πρωταρχική n-οστή ρίζα της μονάδας $\zeta_n \in \overline{\mathbb{F}}_p$ και $\mathbb{F}_p(\zeta_n) = \mathbb{F}_{p^d}$, όπου d είναι η τάξη του p modulo n. Το σύνολο των n-οστών ριζών της μονάδας είναι το $\{\zeta_n^j : 0 \leq j < n\}$ και το σύνολο των πρωταρχικών n-οστών ριζών της μονάδας είναι το $\{\zeta_n^j : 0 \leq j < n, (j,n) = 1\}$.*

Απόδειξη: Ένα στοιχείο $\zeta \in \mathbb{F}_{p^k}$ είναι n-οστή ρίζα της μονάδας αν και μόνο αν η τάξη του ζ στην ομάδα $\mathbb{F}_{p^k}^*$ είναι ίση με n. Η τάξη του ζ διαιρεί την τάξη της ομάδας, η οποία είναι $p^k - 1$ και άρα πρώτη προς το q. Επομένως, αν υπάρχει στοιχείο $\zeta \in \mathbb{F}_{p^k}$ με τάξη n τότε $(n,p) = 1$. Αντίστροφα, αν $(n,p) = 1$, τότε υπάρχει κάποιο $k \in \mathbb{N}$ τέτοιο ώστε $n \mid p^k - 1$. Το ελάχιστο τέτοιο k είναι η τάξη d του p modulo n, η οποία ορίζεται αφού $(n,p) = 1$. Τότε αν α είναι ένας γεννήτορας της ομάδας $\mathbb{F}_{p^d}^*$, το στοιχείο $\zeta_n = \alpha^{(q^d-1)/n}$ έχει τάξη n.

Έχουμε $\zeta_n \in \mathbb{F}_{p^d}$, δηλαδή $\mathbb{F}_p(\zeta_n) \subseteq \mathbb{F}_{p^d}$. Επίσης, αν $\mathbb{F}_p(\zeta_n) = \mathbb{F}_{p^k}$, τότε $\zeta_n^{p^k-1} = 1$, άρα $p^k \equiv 1 \pmod{n}$. Αυτό σημαίνει ότι $d \mid k$, οπότε $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^k} = \mathbb{F}_p(\zeta_n)$.

Είναι σαφές ότι κάθε στοιχείο του συνόλου $\{\zeta_n^j : 0 \leq j < n\}$ είναι n-οστή ρίζα της μονάδας. Αντίστροφα, αν β είναι μία n-οστή ρίζα της μονάδας στο $\overline{\mathbb{F}}_p$, τότε $\beta^{q^d-1} = 1$ και συνεπώς $\beta \in \mathbb{F}_{p^d}$ και μάλιστα ανήκει στη μοναδική κυκλική υποομάδα τάξης n της $\mathbb{F}_{p^d}^*$, η οποία είναι η $\langle \zeta_n \rangle$. Οι προωταρχικές n-οστές ρίζες της μονάδας είναι οι γεννήτορες της $\langle \zeta_n \rangle$, δηλαδή οι ζ_n^j για $0 \leq j < n$ και $(j,n) = 1$. □

Ορισμός 3.2 *Έστω πρώτος p και $n \in \mathbb{N}$ με $(n,p) = 1$ και $\zeta_n \in \mathbb{F}_{p^d}$ μία πρωταρχική n-οστή ρίζα της μονάδας. Το πολυώνυμο $\Psi_n(x) = \prod_{\substack{0 \leq j < n \\ (j,n)=1}} \left(x - \zeta_n^j\right)$ είναι το n-οστό κυκλοτομικό πολυώνυμο.*

Πρόταση 3.7 *Έστω q δύναμη ενός πρώτου p και $m = np^e$, με $(n,p) = 1$. Τότε για το πολυώνυμο $x^m - 1 \in \mathbb{F}_p[x]$ ισχύει*

$$x^m - 1 = \prod_{d \mid n} \Psi_d(x)^{p^e}.$$

Απόδειξη: Αρχικά βλέπουμε ότι $x^m - 1 = (x^n - 1)^{p^e}$, διότι p είναι η χαρακτησριστική του $\mathbb{F}_p$. Οι ρίζες του $x^n - 1$ είναι ακριβώς οι n-οστές ρίζες της μονάδας στο $\overline{\mathbb{F}}_q$. Αν ζ_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας, τότε

$$x^n - 1 = \prod_{i=0}^{n-1} \left(x - \zeta_n^j\right).$$

Για κάθε $d \mid n$, θεωρούμε το σύνολο $A_d = \{0 \leq i < n : (i,n) = \frac{n}{d}\}$. Το $\{A_d,\ d \mid n\}$ αποτελεί μία διαμέριση του $\{0, 1, \ldots, n-1\}$, οπότε

$$x^n - 1 = \prod_{d \mid n} \prod_{\substack{0 \leq i < n \\ (i,n)=\frac{n}{d}}} \left(x - \zeta_n^i\right).$$

Τέλος, βλέπουμε ότι $0 \leq i < n,\ (i,n) = \frac{n}{d}$ αν και μόνο αν $i = j\frac{n}{d}$ με $0 \leq j < d, (j,d) = 1$, οπότε $A_d = \{j\frac{n}{d} : 0 \le j < d,\ (j,d) = 1\}$ και έχουμε

$$\prod_{\substack{0\le i<n\\(i,n)=\frac{n}{d}}} \left(x - \zeta_n^i\right) = \prod_{\substack{0\le j<d\\(j,n)=1}} \left(x - \zeta_n^{j\frac{n}{d}}\right) = \prod_{\substack{0\le j<d\\(j,n)=1}} \left(x - \zeta_d^j\right) = \Psi_d(x),$$

όπου $\zeta_d = \zeta_n^{\frac{n}{d}}$ είναι μία πρωταρχική d-οστή ρίζα της μονάδας. □

Λήμμα 3.2 *Έστω q δύναμη πρώτου p και $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Η απεικόνιση*

$$\begin{array}{rcl} \tilde{\sigma} : \mathbb{F}_q[x] & \longrightarrow & \mathbb{F}_q[x] \\ \displaystyle\sum_{i=0}^{n} c_i x^i & \mapsto & \displaystyle\sum_{i=0}^{n} \sigma(c_i) x^i \end{array}$$

είναι ισομορφισμός δακτυλίων.

Απόδειξη: Αφήνεται ως άσκηση. □

Θεώρημα 3.7 *Έστω πρώτος p, $n \in \mathbb{N}$ με $(n,p) = 1$ και ζ_n μία πρωταρχική n-οστή ρίζα της μονάδας. Ισχύουν τα παρακάτω:*

1. $\deg(\Psi_n) = \varphi(n)$, *όπου φ είναι η συνάρτηση του Euler,*
2. $\Psi_n \in \mathbb{F}_p[x]$,
3. *Η κανονική ανάλυση του Ψ_n σε ανάγωγα είναι $\Psi_n = f_1 \cdots f_r$, όπου οι βαθμοί $\deg(f_i)$ είναι όλοι ίσοι με την τάξη d του p modulo n και $r = \varphi(n)/d$.*

Απόδειξη: Η πρώτη πρόταση είναι προφανής από τον ορισμό του Ψ_n. Για τη δεύτερη πρόταση, έχουμε αρχικά $\Psi_n \in \mathbb{F}_{p^d}[x]$, όπου d είναι η τάξη του p modulo n και πρέπει να δείξουμε $\Psi_n \in \mathbb{F}_p[x]$, δηλαδή ότι κάθε συντελεστής του Ψ_n ανήκει στο $\mathbb{F}_p$. Εφαρμόζουμε το Λήμμα 3.2 με τον αυτομορφισμό του Frobenius και έχουμε

$$\tilde{\phi}_p(\Psi_n) = \prod_{\substack{0\le j<n\\(j,n)=1}} \tilde{\phi}_p\left(x - \zeta_n^j\right) = \prod_{\substack{0\le j<n\\(j,n)=1}} \left(x - \phi_p\left(\zeta_n^j\right)\right) = \prod_{\substack{0\le j<n\\(j,n)=1}} \left(x - \zeta_n^{pj}\right).$$

Βλέπουμε τώρα ότι η απεικόνιση

$$\begin{array}{rcl} \phi_p : \{\zeta_n^j : 0 \le j < n,\ (j,n) = 1\} & \longrightarrow & \{\zeta_n^j : 0 \le j < n,\ (j,n) = 1\} \\ \zeta & \mapsto & \zeta^p \end{array}$$

είναι 1-1 και επί, είναι δηλαδή μία μετάθεση του συνόλου $\{\zeta_n^j : 0 \le j < n,\ (j,n) = 1\}$ (γιατί;). Συνεπώς, ο ισομορφισμός $\tilde{\phi}_p$ κάνει μία μετάθεση των παραγόντων $x - \zeta_n^j$ του πολυωνύμου Ψ_n και επομένως $\tilde{\phi}_p(\Psi_n) = \Psi_n$. Αυτό σημαίνει ότι ο αυτομορφισμός ϕ_p σταθεροποιεί κάθε συντελεστή Ψ_n, δηλαδή $\Psi_n \in \mathbb{F}_p[x]$.

Για την τρίτη πρόταση, είναι σαφές ότι το πολυώνυμο Ψ_n έχει απλές ρίζες, οπότε η ανάλυση του σε ανάγωγα είναι $\Psi_n = f_1 \cdots f_r$. Θεωρούμε μία ρίζα α_i για κάθε ανάγωγο f_i και χωρίς βλάβη της γενικότητας υποθέτουμε $\alpha_1 = \zeta_n$. Τότε το $f_i = \min(\mathbb{F}_p, \alpha_i)$. Επίσης, $\alpha_i \in \mathbb{F}_p(\zeta_n)$, οπότε $\mathbb{F}_p(\alpha_i) \subseteq \mathbb{F}_p(\zeta_n)$. Το α_i είναι πρωταρχική n-οστή ρίζα της μονάδας, οπότε $\zeta_n = \alpha_i^{k_i}$ για κάποιο $k_i \in \mathbb{Z}$. Οπότε $\mathbb{F}_p(\zeta_n) \subseteq \mathbb{F}_p(\alpha_i)$. Αυτό σημαίνει ότι

$$\deg(f_i) = [\mathbb{F}_p(\alpha_i) : \mathbb{F}_p] = [\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = \deg\left(\min\left(\mathbb{F}_p, \zeta_n\right)\right).$$

Τέλος, έχουμε ήδη δει ότι ο βαθμός $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p]$ είναι ίσος με την τάξη d του p modulo n. □