Κεφάλαιο 2

Παραγοντοποίηση σε Ακέραιες Περιοχές

Γνωρίζουμε ότι στο $\mathbb{Z}$ κάθε στοιχείο εκτός από το 0 και τα ± 1 γράφεται ως γινόμενο πρώτων αριθμών κατά τρόπο ουσιαστικά μοναδικό. Από τη Βασική Άλγεβρα ξέρουμε ότι κάτι ανάλογο συμβαίνει στο δακτύλιο πολυωνύμων $F[x]$, όπου F είναι σώμα. Σκοπός μας εδώ είναι να μελετήσουμε συνοπτικά ακέραιες περιοχές που έχουν την ιδιότητα της "μοναδικής παραγοντοποίησης". Για να γίνουμε πιο σαφείς απαιτούνται μερικοί ορισμοί που παραθέτουμε αμέσως παρακάτω.

Όλοι οι δακτύλιοι στο κεφάλαιο αυτό θα είναι μεταθετικοί.

2.1 Ορισμοί και Παραδείγματα

Έστω R ένας δακτύλιος και $a, b \in R$.

2.1.1 Ορισμός *i) Θα λέμε ότι το a διαιρεί το b (συμβολισμός $a \mid b$) αν υπάρχει $c \in R$ τέτοιο ώστε $b = ac$.*

ii) Τα a και b ονομάζονται συντροφικά στο R αν $a = ub$ για κάποιο αντιστρέψιμο $u \in R$.

Η σχέση στο R που ορίζεται από $a \sim b \Leftrightarrow a$ και b είναι συντροφικά, είναι σχέση ισοδυναμίας.

Για παράδειγμα, τα μόνα συντροφικά στοιχεία του 3 στο $\mathbb{Z}$ είναι το 3 και -3. Τα συντροφικά στοιχεία του $f(x) \in F[x]$, όπου k είναι σώμα, είναι τα $uf(x)$ όπου $u \in k - \{0\}$.

2.1.2 Ορισμός *Έστω R μια ακέραια περιοχή και $p \in R$. Τότε το p ονομάζεται ανάγωγο στο R αν*

(i) το p δεν είναι μηδέν και δεν είναι αντιστρέψιμο, και

(ii) $p = ab$ με $a, b \in R$ ισχύει μόνο αν το a ή το b είναι αντιστρέψιμο.

Προφανώς οι πρώτοι αριθμοί είναι ανάγωγοι στο $\mathbb{Z}$. Όμως ο πρώτος αριθμός 5 δεν είναι ανάγωγο στοιχείο στο $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ αφού $5 = (1 + 2i)(1 - 2i)$ και τα στοιχεία $1 + 2i$, $1 - 2i$ δεν είναι αντιστρέψιμα στο $\mathbb{Z}[i]$. (Απόδειξη: $(1 + 2i)(m + ni) = 1 \Rightarrow m - 2n = 1$ και $2m + n = 0$ το οποίο δεν έχει ακέραιες λύσεις. Όμοια για το $1 - 2i$. .

2.1.3 Ορισμός *Μια ακέραια περιοχή R ονομάζεται περιοχή μοναδικής παραγοντοποίησης αν ισχύουν οι παρακάτω συνθήκες:*

(i) Κάθε στοιχείο του R που δεν είναι 0 ή αντιστρέψιμο γράφεται ως γινόμενο αναγώγων στοιχείων στο R.

(ii) Αν $a = p_1 \cdots p_r$ και $a = q_1 \cdots q_s$ είναι γινόμενα αναγώγων στοιχείων του R τότε $r = s$ και μετά από κάποια αρίθμηση, το p_i είναι συντροφικό του q_i για κάθε $i = 1, \ldots, r$.

Γνωστά παραδείγματα είναι οι δακτύλιοι $\mathbb{Z}$ και $F[x]$, όπου F σώμα. Ο $\mathbb{Z}[i]$ είναι επίσης περιοχή μοναδικής παραγοντοποίησης όπως θα δούμε παρακάτω. Υπάρχουν πολλές περιοχές που δεν είναι περιοχές μοναδικής παραγοντοποίησης. Ένα τέτοιο παράδειγμα είναι το επόμενο.

2.1.4 Παράδειγμα Θα δείξουμε ότι στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ δεν ισχύει η συνθήκη (ii) του Ορισμού 1.1.3. Παρατηρούμε ότι

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Πρώτα δείχνουμε ότι τα στοιχεία 2, 3, $1 + \sqrt{-5}$, και $1 - \sqrt{-5}$ είναι ανάγωγα στο $\mathbb{Z}[\sqrt{-5}]$: Ορίζουμε μία συνάρτηση ("νόρμα")

$$N : \mathbb{Z}[\sqrt{-5}] \ni a + b\sqrt{-5} \mapsto a^2 + 5b^2 \in \mathbb{N}$$

και παρατηρούμε ότι $N(xy)=N(x)N(y)$ για κάθε $x,y\in\mathbb{Z}[\sqrt{-5}]$. Έστω τώρα ότι το $u\in\mathbb{Z}[\sqrt{-5}]$ είναι αντιστρέψιμο. Από τη σχέση $uv=1$ παίρνουμε $N(uv)=N(1)=1$, δηλαδή $N(u)N(v)=1$. Άρα $N(u)=1$, γιατί $N(u),N(v)\in\mathbb{N}$. Γράφοντας $u=u_0+u_1\sqrt{-5}$, παίρνουμε $u_0^2+5u_1^2=1$ ($u_0,u_1\in\mathbb{Z}$). Οι λύσεις της τελευταίας Διοφαντικής εξίσωσης είναι προφανώς $u_0=\pm1$, $u_1=0$. Συμπέρασμα: τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα ±1. Επομένως τα 2, 3, $1\pm\sqrt{-5}$ δεν είναι αντιστρέψιμα (συνθήκη i) του Ορισμού 2.1.2). Θα δείξουμε τώρα ότι ισχύει η συνθήκη ii) του Ορισμού 1.1.2 για καθένα από τα 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$. Έστω $2=ab$ με $a,b\in\mathbb{Z}[\sqrt{-5}]$. Έχουμε $N(2)=N(ab)$, δηλαδή $4=N(a)N(b)$. Επειδή $N(a),N(b)\in\mathbb{N}$, συμπεραίνουμε ότι $N(a)=1$ ή $N(a)=2$ ή $N(a)=4$. Η περίπτωση $N(a)=1$ αποκλείεται γιατί $N(a)=1\Rightarrow a=\pm1$. Όμοια η περίπτωση $N(a)=4$ αποκλείεται γιατί $N(a)=4\Rightarrow N(b)=1\Rightarrow b=\pm1$. Άρα έχουμε $N(a)=2$. Όμως γράφοντας $a_0+a_1\sqrt{-5}$ με $a_0,a_1\in\mathbb{Z}$ παρατηρούμε ότι $N(a)=2\Leftrightarrow a_0^2+5a_1^2=2$. Η τελευταία Διοφαντική εξίσωση δεν έχει λύσεις. Συνεπώς το 2 είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-5}]$. Με παρόμοιο τρόπο δείχνουμε ότι το 3, $1+\sqrt{-5}$, και $1-\sqrt{-5}$ είναι ανάγωγα στο $\mathbb{Z}[\sqrt{-5}]$. Τέλος είναι προφανές ότι από τα 2, 3, $1+\sqrt{-5}$, και $1-\sqrt{-5}$ οποιαδήποτε δύο δεν είναι συντροφικά, γιατί τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα ±1.

Υπενθυμίζουμε ότι ένα ιδεώδες I του δακτυλίου R ονομάζεται κύριο αν $I=(a)$ για κάποιο $a\in R$.

2.1.5 Ορισμός *Μια περιοχή R ονομάζεται περιοχή κυρίων ιδεωδών αν κάθε ιδεώδες του R είναι κύριο.*

2.1.6 Παράδειγμα Οι δακτύλιοι $\mathbb{Z}$ και $F[x]$, όπου F είναι σώμα, είναι περιοχές κυρίων ιδεωδών.

Απόδειξη. Έστω I ιδεώδες του $\mathbb{Z}$ διάφορο από το (0). Έστω $d \in I$ ο ελάχιστος μη μηδενικός φυσικός αριθμός του συνόλου $I \cap \mathbb{N}$. Θα αποδείξουμε ότι $I = (d)$. Προφανώς $(d) \subseteq I$. Έστω λοιπόν $m \in I$. Από την ταυτότητα διαίρεσης στο $\mathbb{Z}$ έχουμε

$$m = qd + r, \qquad 0 \le r < d .$$

Συνεπώς $r = m - qd \in I$, γιατί το I είναι ιδεώδες. Από την ανισότητα $0 \le r < d$ και τον ορισμό του d συμπεραίνουμε ότι $r = 0$. Τελικά $m = qd \in (d)$, δηλαδή $I \subseteq (d)$. Η απόδειξη για το $F[x]$ είναι πανομοιότυπη: χρησιμοποιήστε την ταυτότητα διαίρεσης πολυωνύμων.

Ένα παράδειγμα περιοχής που δεν είναι περιοχή κυρίων ιδεωδών είναι η $\mathbb{Z}[x]$. Πράγματι, το ιδεώδες $(2, x)$ του $\mathbb{Z}[x]$ δεν είναι κύριο (γιατί;). Ένα άλλο τέτοιο παράδειγμα είναι ο δακτύλιος $F[x, y]$ των πολυωνύμων δύο μεταβλητών πάνω στο σώμα F (γιατί;).

Έχοντας λοιπόν κατανοήσει τους προηγούμενους ορισμούς, μπορούμε να περιγράψουμε το στόχο αυτού του Κεφαλαίου, ο οποίος είναι να αποδείξουμε ότι: Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης (2.2.1 Θεώρημα).

2.2 Κύρια Ιδεώδη και Παραγοντοποίηση

Θα αποδείξουμε εδώ το ακόλουθο αποτέλεσμα.

2.2.1 Θεώρημα *Κάθε περιοχή κυρίων ιδεών είναι περιοχή μοναδικής παραγοντοποίησης.*

Το πρώτο βήμα στην απόδειξη του παραπάνω θεωρήματος είναι να δείξουμε ότι σε κάθε περιοχή κυρίων ιδεωδών κάθε μη μηδενικό, μη αντιστρέψιμο στοιχείο γράφεται ως γινόμενο αναγώγων στοιχείων (2.2.3 Πρόταση παρακάτω). Για το σκοπό αυτό χρειαζόμαστε το ακόλουθο λήμμα.

2.2.2 Λήμμα *Έστω R μια περιοχή κυρίων ιδεωδών και έστω*

$$I_1 \subseteq I_2 \subseteq \cdots$$

μια αύξουσα ακολουθία ιδεωδών του R. Τότε υπάρχει $m \in \mathbb{N}$ *τέτοιο ώστε*

$$I_m = I_{m+1} = I_{m+2} = \cdots .$$

Απόδειξη. Θεωρούμε την ένωση $I = \bigcup_{i=1}^{\infty} I_i$. Θα δείξουμε ότι το *I* είναι ιδεώδες του *R*. Πράγματι, έστω $a, b \in I$ και $r \in R$. Για κάποια *i* και *j* έχουμε $a \in I_i$, και $b \in I_j$ λόγω της υπόθεσης. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $i \le j$. Τότε $a, b \in I_j$. Κατά συνέπεια $a + b \in I_j$ και $ra \in I_j$. Άρα $a + b \in I$ και $ra \in I$. Συνεπώς το *I* είναι ιδεώδες. Τώρα, επειδή ο *R* είναι περιοχή κυρίων ιδεωδών, έχουμε $I = (c)$ για κάποιο $c \in I$. Όμως αφού $I = \bigcup_{i=1}^{\infty} I_i$, έχουμε $c \in I_m$ για κάποιο *m*. Άρα για κάθε $n \ge m$ έχουμε $I_m = I_n$. □

2.2.3 Πρόταση *Έστω R μια περιοχή κυρίων ιδεωδών. Τότε κάθε μη μηδενικό, μη αντιστρέψιμο στοιχείο του R είναι γινόμενο αναγώγων στοιχείων του R.*

Απόδειξη. Έστω $a \in R$ με $a \neq 0$ και *a* μη αντιστρέψιμο. Πρώτα θα αποδείξουμε ότι υπάρχει ανάγωγο $p \in R$ που διαιρεί το *a*. Αν το *a* είναι ανάγωγο, δεν υπάρχει τίποτε να αποδείξουμε. Έστω ότι το *a* δεν είναι ανάγωγο. Τότε υπάρχουν μη αντιστρέψιμα στοιχεία $a_1, b_1 \in R$ με την ιδιότητα $a = a_1 b_1$. Αυτό σημαίνει ότι

$$(a) \subsetneq (a_1) .$$

Πράγματι $a = a_1 b_1 \Rightarrow (a) \subseteq (a_1)$. Αν $(a) = (a_1)$ τότε $a = x a_1$ και $a_1 = ya$ για κάποια $x, y \in R$. Τότε $a = yab = ayb_1 \Rightarrow a(1 - yb_1) = 0 \Rightarrow 1 - yb_1 = 0 \Rightarrow b_1$ αντιστρέψιμο, που είναι άτοπο. Επαναλαμβάνουμε την προηγούμενη διαδικασία για το a_1 στη θέση του *a* κοκ. Λαμβάνουμε λοιπόν μια γνησίως αύξουσα ακολουθία ιδεωδών του *R*

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots .$$

Από το Λήμμα 2.2.2, η παραπάνω ακολουθία τερματίζει σε κάποιο (a_m). Το $p = a_m$ είναι ανάγωγο εξ ορισμού και διαιρεί το *a*.

Έχουμε αποδείξει ότι είτε το a είναι ανάγωγο είτε $a = p_1 c_1$, όπου p_1 ανάγωγο και c_1 μη αντιστρέψιμο. Στη δεύτερη περίπτωση έχουμε

$$(a) \subsetneq (c_1)$$

όπως και πριν. Αν το c_1 είναι ανάγωγο, δεν υπάρχει τίποτε να αποδείξουμε. Έστω ότι το c_1 δεν είναι ανάγωγο. Τότε $c_1 = p_2 c_2$ για κάποιο ανάγωγο p_2 και μη αντιστρέψιμο c_2. Επαναλαμβάνοντας τη διαδικασία λαμβάνουμε μια γνησίως αύξουσα ακολουθία ιδεωδών του R

$$(a) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots.$$

Από το Λήμμα 1.2.2, αυτή κάπου τερματίζει, έστω στο (c_m). Τότε το c_m είναι ανάγωγο και ισχύει $a = p_1 p_2 \cdots p_m c_m$. □

Το δεύτερο βήμα στην απόδειξη του Θεωρήματος 2.2.1 είναι να δείξουμε τη μοναδικότητα της παραγοντοποίησης που παρέχει η Πρόταση 2.2.3. Χρειαζόμαστε για περιοχές κυρίων ιδεωδών μια πρόταση ανάλογη με την ακόλουθη πρόταση για το $\mathbb{Z}$: αν ο πρώτος p διαιρεί το γινόμενο ab, τότε θα διαιρεί έναν τουλάχιστον από τα a και b. Αυτή η πρόταση είναι το κύριο βήμα στην απόδειξη της μοναδικότητας της παραγοντοποίησης στο $\mathbb{Z}$.

2.2.4 Πρόταση *Έστω R μια περιοχή κυρίων ιδεωδών και $p \in R$ ανάγωγο. Αν $p \mid ab$, όπου $a, b \in R$, τότε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Έστω ότι το p δεν διαιρεί το a. Θα δείξουμε ότι το p διαιρεί το b.
Αφού ο R είναι περιοχή κυρίων ιδεωδών, υπάρχει $d \in R$ τέτοιο ώστε $(p) + (a) = (d)$. Επειδή $p \in (d)$, έχουμε $p = cd$, όπου $c \in R$. Επειδή το p είναι ανάγωγο, έχουμε ότι το c ή το d είναι αντιστρέψιμο. Στην πρώτη περίπτωση οδηγούμεθα σε άτοπο γιατί $a \in (d) \Rightarrow d \mid a \Rightarrow cd \mid a \Rightarrow p \mid a$. Άρα το d είναι αντιστρέψιμο. Τότε $(p) + (a) = (d) = R \Rightarrow xp + ya = 1$ για κάποια $x, y \in R$. Επομένως έχουμε τη σχέση $xpb + yab = b$ από την οποία έπεται ότι το p διαιρεί το b. □

Με επαγωγή αποδείχνεται αμέσως το παρακάτω πόρισμα.

2.2.5 Πόρισμα *Έστω R μια περιοχή κυρίων ιδεωδών και $p \in R$ ανάγωγο. Αν $p \mid a_1 \cdots a_n$, όπου $a_1, ..., a_n \in R$, τότε για κάποιο i έχουμε $p \mid a_i$.*

Έχοντας υπόψη το προηγούμενο πόρισμα, η απόδειξη του δεύτερου βήματος είναι απλούστατη:

Απόδειξη του Θεωρήματος 2.2.1. Από την Πρόταση 2.2.3 αρκεί να δείξουμε τη συνθήκη (ii) του Ορισμού 2.1.3. Έστω λοιπόν $a = p_1 \cdots p_r$ και $a = q_1 \cdots q_s$ γινόμενα αναγώγων στοιχείων του R με $s \geq r$. Από τη σχέση $p_1 \cdots p_r = q_1 \cdots q_s$ και το Πόρισμα 2.2.5 συμπεραίνουμε ότι το p_1 διαιρεί κάποιο q_j. Μετά από κάποια αρίθμηση μπορούμε να υποθέσουμε ότι $p_1 \mid q_1$. Άρα $q_1 = u_1 p_1$ για κάποιο αντιστρέψιμο u_1, γιατί το q_1 είναι ανάγωγο. Άρα $p_1 \cdots p_r = u_1 p_1 q_2 \cdots q_s$ και αφού ο R είναι ακέραια περιοχή,

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s .$$

Συνεχίζοντας κατά αυτόν τον τρόπο καταλήγουμε σε μια σχέση της μορφής

$$1 = u_1 \cdots u_r q_{r+1} \cdots q_s .$$

Επειδή τα $q_{r+1}, ..., q_s$ είναι ανάγωγα και άρα μη αντιστρέψιμα θα ισχύει $r = s$. □

Από το Θεώρημα 2.2.1 και το Παράδειγμα 2.1.6 λαμβάνουμε και πάλι το ακόλουθο αποτέλεσμα.

2.2.6 Πόρισμα *Οι δακτύλιοι $\mathbb{Z}$ και $F[x]$ (F σώμα) είναι ακέραιες περιοχές μοναδικής παραγοντοποίησης.*

Αναφέρουμε χωρίς απόδειξη ότι το προηγούμενο πόρισμα γενικεύεται όπου στη θέση του σώματος F έχουμε τυχαία περιοχή μοναδικής παραγοντοποίησης.

2.2.7 Θεώρημα *Αν ο δακτύλιος R είναι περιοχή μοναδικής παραγοντοποίησης τότε και ο* $R[x]$ *είναι περιοχή μοναδικής παραγοντοποίησης.*

Συνεπώς οι δακτύλιοι $\mathbb{Z}[x_1,...,x_n]$, $F[x_1,...,x_n]$, όπου F είναι σώμα, είναι περιοχές μοναδικής παραγοντοποίησης.

2.3 Ευκλείδειες Περιοχές

Έχουμε διαπιστώσει ότι οι δακτύλιοι $\mathbb{Z}$ και $F[x]$ (F σώμα) έχουν πολλές κοινές ιδιότητες. Μία απ' αυτές είναι η ταυτότητα διαίρεσης συνέπεια της οποίας είναι ότι οι $\mathbb{Z}$ και $F[x]$ είναι περιοχές κυρίων ιδεωδών (Παράδειγμα 1.1.6). Εδώ θα μελετήσουμε περιοχές που έχουν μια "ταυτότητα διαίρεσης". Αυτές ονομάζονται Ευκλείδειες περιοχές. Ακριβέστερα έχουμε:

2.3.1 Ορισμός *Μια Ευκλείδεια περιοχή είναι μία ακέραια περιοχή R εφοδιασμένη με μία συνάρτηση* $\varphi : R-\{0\} \to \mathbb{N}$, *τέτοια ώστε*

(i) $a,b \in R$ *με* $a \mid b \Rightarrow \varphi(a) \le \varphi(b)$

(ii) $a \in R$ *και* $b \in R-\{0\}$. *Τότε υπάρχουν* $q,r \in R$ *με την ιδιότητα* $a = bq + r$ *και είτε* $r = 0$ *είτε* $\varphi(r) < \varphi(b)$.

Η συνάρτηση φ ονομάζεται Ευκλείδεια συνάρτηση του R.

Για παράδειγμα έχουμε $R = \mathbb{Z}$ με $\varphi(m) = \mid m \mid$ (απόλυτη τιμή), και $R = F[x]$ (F σώμα) με $\varphi(f(x)) = \deg f(x)$ (βαθμός πολυωνύμου). Σημειώνουμε ότι σε μια Ευκλείδεια περιοχή είναι δυνατόν να υπάρχουν πολλές Ευκλείδειες συναρτήσεις.

Το επόμενο αποτέλεσμα είναι σίγουρα αναμενόμενο.

2.3.2 Πρόταση *Κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Έστω I ιδεώδες της Ευκλείδειας περιοχής R με $I \neq (0)$. Έστω $b \in I$ με την ιδιότητα $\varphi(b)$ είναι ελάχιστο. Θα δείξουμε ότι $I = (b)$. Αρκεί να δείξουμε $I \subseteq (b)$. Έστω $a \in I$. Έχουμε $a = bq + r$ όπου είτε $r = 0$ είτε $\varphi(r) < \varphi(b)$. Από τον ορισμό του b συμπεραίνουμε ότι $r = 0$. Άρα $a = bq \in (a)$. □

Σημειώνουμε ότι δεν χρησιμοποιήσαμε την ιδιότητα (i) του ορισμού. Αυτή είναι συχνά χρήσιμη στον προσδιορισμό των αντιστρέψιμων στοιχείων μια Ευκλείδειας περιοχής, όπως δείχνει η παρακάτω πρόταση.

2.3.3 Πρόταση *Έστω R Ευκλείδεια περιοχή με Ευκλείδεια συνάρτηση φ. Τότε το* $u \in R$ *είναι αντιστρέψιμο αν και μόνο αν* $\varphi(u) = \varphi(1)$.

Απόδειξη. Αν $uv = 1$ τότε $\varphi(u) \le \varphi(1)$. Από την άλλη μεριά έχουμε $1 \mid u$ και άρα $\varphi(1) \le \varphi(u)$. Άρα $\varphi(u) = \varphi(1)$. Αντίστροφα, έστω $\varphi(u) = \varphi(1)$. Τότε υπάρχουν $q, r \in R$ με την ιδιότητα $1 = uq + r$ και είτε $r = 0$ είτε $\varphi(r) < \varphi(u)$. Αν $r \neq 0$, τότε $1 \mid r$ και $\varphi(1) \le \varphi(r)$ άτοπο. Άρα $r = 0$ και $1 = uq$. □

Το αντίστροφο της Πρότασης 2.3.2 δεν ισχύει, δηλαδή υπάρχουν περιοχές κυρίων ιδεωδών που δεν είναι Ευκλείδειες περιοχές. Ένα τέτοιο παράδειγμα είναι ο δακτύλιος $\left\{ \frac{a}{2} + \frac{b}{2}\sqrt{-19} \mid a, b \in \mathbb{Z} \quad \text{και} \quad a \equiv b \bmod 2 \right\}$. Η απόδειξη χρησιμοποιεί μέσα που ξεφεύγουν από τις σημειώσεις αυτές και παραλείπεται.

2.3.4 Πρόταση *Οι ακέραιοι του Gauss* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *είναι Ευκλείδεια περιοχή. Τα αντιστρέψιμα στοιχεία του* $\mathbb{Z}[i]$ *είναι* $\{\pm 1, \pm i\}$.

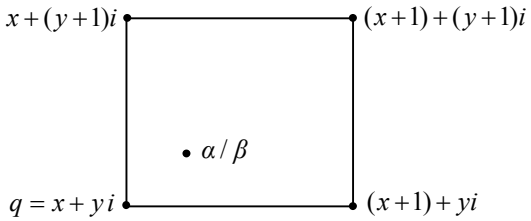
Απόδειξη. Έστω $\varphi(a + b) = (a + bi)(a - bi) = a^2 + b^2$. Τότε $\varphi((a + bi)(c + di)) = \varphi(a + bi)\varphi(c + di)$. Κατά συνέπεια ισχύει η συνθήκη (i) του Ορισμού 2.3.1. Για τη συνθήκη (ii) τώρα, έστω $\alpha, \beta \in \mathbb{Z}[i]$ με $\beta \neq 0$. Θεωρούμε τον μιγαδικό αριθμό α / β. Στο επίπεδο απεικονίζουμε τα στοιχεία του $\mathbb{Z}[i]$ στα σημεία με ακέραιες συντεταγμένες. Έτσι δημιουργούνται πολλά τετράγωνα με κορυφές τα παραπάνω σημεία και μήκος πλευράς 1. Επειδή το μήκος κάθε διαγωνίου είναι $\sqrt{2}$, συμπεραίνουμε ότι υπάρχει κορυφή που απέχει από το α / β απόσταση $\le \frac{\sqrt{2}}{2}$.

Έστω q μια τέτοια κορυφή. Τότε $|\alpha/\beta - q| \le \sqrt{2}/2 < 1$. Θέτοντας $r = \alpha - \beta q$ έχουμε

$$\alpha = \beta q + r \quad \text{και} \quad |r| = |\alpha - \beta q| = |\beta|\,|\alpha/\beta - q| < |\beta|.$$

Επομένως $\varphi(r) = |r|^2 < |\beta|^2 = \varphi(\beta)$.

Για τις μονάδες έχουμε : u μονάδα $\Leftrightarrow \varphi(u) = \varphi(1) = 1$. Άρα $u = \pm 1$ και $\pm i$



2.3.5 Παράδειγμα Ποια είναι η ανάγωγη παραγοντοποίηση του $-1+7i \in \mathbb{Z}[i]$; (Ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης από την Πρόταση 2.3.4 και το Θεώρημα 2.2.1). Πρώτα μια γενική παρατήρηση: αν $\alpha \in \mathbb{Z}[i]$ είναι τέτοιο ώστε $\varphi(\alpha) = p$ πρώτος αριθμός στο $\mathbb{Z}$, τότε το α είναι ανάγωγο. Πράγματι, αν $\alpha = \beta\gamma$, τότε $\varphi(\alpha) = \varphi(\beta)\varphi(\gamma) = p$ και άρα $\varphi(\beta) = 1$ ή $\varphi(\gamma) = 1$ δηλαδή β αντιστρέψιμο ή γ αντιστρέψιμο (Πρόταση 2.3.3). Τώρα στο συγκεκριμένο παράδειγμα. Έχουμε $\varphi(-1+7i) = 50$. Αν ο $\alpha \in \mathbb{Z}[i]$ διαιρεί το $-1+7i$ θα πρέπει το $\varphi(\alpha)$ να διαιρεί το 50. Εξαιρώντας τις τετριμμένες περιπτώσεις, αναζητούμε τα α που ικανοποιούν $\varphi(\alpha) = 2, 5, 10, 25$. Κάποια απ' αυτά (όχι αναγκαστικά όλα) θα είναι διαιρέτες του $-1+7i$. Για $\varphi(\alpha) = 2$ δοκιμάζουμε αν το $1+i$ είναι διαιρέτης του $-1+7i$. Εκτελώντας τη διαίρεση στο $\mathbb{C}$, βλέπουμε ότι το πηλίκο είναι στο $\mathbb{Z}[i]$, $-1+7i = (1+i)(3+4i)$. Το $1+i$ είναι ανάγωγο. Εκτελούμε την ίδια διαδικασία για το $3+4i$. Τελικά $-1+7i = (1+i)(2+i)^2$ είναι ανάγωγη παραγοντοποίηση.

Ασκήσεις

1. Η ακέραια περιοχή $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.

(Υπόδειξη $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$).

2. Έστω k σώμα. Ο δακτύλιος $k[x, y]$ δεν είναι περιοχή κυρίων ιδεωδών.

3. Εξετάστε αν η πρόταση 'R περιοχή κυρίων ιδεωδών $\Rightarrow R[x]$ περιοχή κυρίων ιδεωδών' είναι σωστή.

4. Έστω R ακέραια περιοχή και $p \in R$ ένα μη μηδενικό μη αντιστρέψιμο στοιχείο. Το p λέγεται πρώτο αν: $p \mid ab \Rightarrow p \mid a$ ή $p \mid b$.

(i) Αποδείξτε ότι κάθε πρώτο στοιχείο είναι ανάγωγο

(ii) Αν ο R είναι περιοχή μοναδικής παραγοντοποίησης, τότε κάθε ανάγωγο στοιχείο είναι πρώτο.

5. Έστω R περιοχή κυρίων ιδεωδών, S ακέραια περιοχή και $\varphi : R \to S$ επιμορφισμός δακτυλίων. Τότε ο φ είναι ισομορφισμός ή το S είναι σώμα.

6. Γνωρίζουμε ότι R σώμα $\Rightarrow R[x]$ περιοχή κυρίων ιδεωδών. Δείξτε το αντίστροφο: Έστω R δακτύλιος μεταθετικός με 1. Αν ο δακτύλιος $R[x]$ είναι περιοχή κυρίων ιδεωδών, τότε το R είναι σώμα. (Υπόδειξη: θεωρήστε έναν επιμορφισμό $R[x] \to R$).

7. Έστω R περιοχή κυρίων ιδεωδών και $a, b \in R$ όχι και τα δύο μηδέν. Τότε $(a, b) = (d)$, όπου $d = \text{μ.κ.δ.}(a, b)$.

8. Βρείτε το $m \in \mathbb{N}$ έτσι ώστε $\mathbb{Z}[i]/(1 + 3i) \cong \mathbb{Z}_m$.

9. Στο $\mathbb{Z}[i]$ ισχύει $10 = 2 \cdot 5 = (1 + 3i)(1 - 3i)$ αλλά ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης. Εξηγήσετε.