

**ΑΝΤΙΜΕΤΑΘΕΤΙΚΗ ΑΛΓΕΒΡΑ**  
**ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ, 2013**  
**ΣΗΜΕΙΩΣΕΙΣ**

ΧΑΡΑ ΧΑΡΑΛΑΜΠΟΥΣ  
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ, ΑΠΘ

1. ΕΙΣΑΓΩΓΗ

**1.1. Απαρχές της Αντιμεταθετικής Άλγεβρας.**

1.1.1. Θεωρία Αριθμών. Θα σχολιάσουμε πρώτα τη σύνδεση με το Τελευταίο Θεώρημα τους Fermat (1637). Θυμίζουμε ότι η απόδειξη του TWF ολοκληρώθηκε το 1995 με τη δουλειά του Wiles: η εξίσωση  $x^n + y^n = z^n$  δεν μπορεί να λυθεί στους ακεραίους όταν  $n > 2$ .

Ο Gauss το 1832 στην εργασία *Theoria residuorum biquadraticorum* εισήγαγε το σύνολο

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}.$$

Ο δακτύλιος αυτός είναι γνωστός σήμερα ως δακτύλιος των ακεραίων του Gauss. Ο Gauss απέδειξε (ανόμεσα σε πολλά άλλα) ότι τα στοιχεία του  $\mathbb{Z}[i]$  ικανοποιούν την ιδιότητα της μοναδικής παραγοντοποίησης. Αυτό σημαίνει ότι αν  $x \in \mathbb{Z}[i]$  τότε  $x$  μπορεί να γραφτεί με μοναδικό τρόπο ως γινόμενο

$$x = u \prod_{i=1}^s p_i^{n_i}$$

όπου  $u$  είναι αντιστρέψιμο,  $p_i$  είναι ανάγωγο για κάθε  $i$  και  $p_i$  δεν είναι συναφές με το  $p_j$  για  $i \neq j$ . (Ένα μη αντιστρέψιμο  $q$  στοιχείο λέγεται ανάγωγο αν κάθε φορά που  $q = ab$  τότε ένα από τα  $a$  ή  $b$  είναι αντιστρέψιμα. Δύο ανάγωγα στοιχεία  $q_1, q_2$  λέγονται συναφή αν  $q_1 = aq_2$  όπου  $a$  αντιστρέψιμο). Με μοναδικό τρόπο σημαίνει ότι αν

$$x = u' \prod_{i=1}^t q_i^{m_i}$$

είναι μία άλλη έκφραση της παραπάνω μορφής τότε  $t = s$  και σε κάθε  $p_i$  αντιστοιχεί ένα συναφές  $q'_j$ .

Θυμίζουμε ότι αν  $D$  είναι μία ακεραία περιοχή, τότε ένα μη αντιστρέψιμο στοιχείο  $p \in D$  είναι πρώτο (prime) στοιχείο του  $D$  αν κάθε φορά που  $p|ab$  τότε  $p|a$  ή  $p|b$ . Είναι εύκολο να δείξει κανείς ότι κάθε πρώτο στοιχείο είναι και ανάγωγο. Ισχύει το αντίστροφο; Η  $D$  καλείται περιοχή μοναδικής παραγοντοποίησης ΠΜΜ (unique factorization domain UFD) αν για κάθε  $x \in D$  ισχύει η ιδιότητα της μοναδικής παραγοντοποίησης που περιγράψαμε παραπάνω.

### Ασκήσεις 1.1.

- Να αποδείξετε ότι σε μία περιοχή μοναδικής παραγοντοποίησης, κάθε ανάγωγο στοιχείο είναι πρώτο.
- Να αποδείξετε ότι  $\mathbb{Z}[i]$  είναι ΠΜΜ. Δείξτε πρώτα ότι  $\mathbb{Z}[i]$  είναι Ευκλείδια περιοχή χρησιμοποιώντας πολλαπλασιαστικές ιδιότητες της νόρμας,  $N(a + bi) = a^2 + b^2$ .
- Σχολιάστε τη σχέση  $2 = (1+i)(1-i)$  στο  $\mathbb{Z}[i]$ . Είναι  $1 \pm i$  πρώτο (ανάγωγα) στοιχεία του  $\mathbb{Z}[i]$ ;
- Θεωρήστε τώρα την ακεραία περιοχή

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}$$

και την νόρμα  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ . Παρατηρείστε ότι

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

Είναι τα στοιχεία  $3, 2 \pm \sqrt{-5}$  πρώτα, ανάγωγα; Είναι η ακεραία περιοχή  $\mathbb{Z}[\sqrt{-5}]$  ΠΜΜ;

Τι σχέση έχουν όλα αυτά με το θεώρημα του Fermat; Για  $n = 2$  έχουμε ότι

$$x^2 + y^2 = (x + iy)(x - iy) .$$

Έστω λοιπόν ότι θέλουμε να βρούμε ακεραίους  $x, y$  έτσι ώστε  $x^2 + y^2 = z^2$ . Στον δακτύλιο  $\mathbb{Z}[i]$  αρκεί να βρούμε μία μη τετριμμένη παραγοντοποίηση του  $z^2$ . Για το θεώρημα του Fermat μας ενδιαφέρει η λύση της εξίσωσης

$$x^n + y^n = z^n$$

για  $n > 2$ . Τι κάνουμε λοιπόν σε αυτή τη περίπτωση; Η βασική ιδέα του Lame (1847) ήταν ότι αν υπάρχουν τέτοιες λύσεις, ( $\text{έστω } a, b, c$ ) τότε για το κατάλληλο  $\zeta$  ισχύει ότι

$$a^n + b^n = (a + b)(a + \zeta b) \cdots (a + \zeta^{n-1}b) = c^n .$$

Αφού οι παράγοντες σε αυτή τη παραγοντοποίηση είναι σχετικά πρώτοι στον δακτύλιο  $\mathbb{Z}[\zeta]$  ( χρησιμοποιώντας την ιδιότητα της μοναδικής παραγοντοποίησης) ο Lame έδειξε ότι κάθε ένας από αυτούς είναι ίσος με μία  $n$ -στη δύναμη. Επαναλαμβάνοντας κατέληξε σε άτοπο. Το πρόβλημα με την απόδειξη του, έγκειται στο ότι ο δακτύλιος  $\mathbb{Z}[\zeta]$  δεν είναι απαραίτητα ΠΜΜ. Αυτό το απέδειξε ο Kummer (επίσης το 1847).

Παρόλα αυτά οι Dedekind και Lasker στα τέλη του 19ου αιώνα με την έρευνά τους εισήγαγαν την έννοια των ιδεωδών όπου και ανέκτησαν την ιδιότητα της μοναδικής παραγοντοποίησης. Αντί για πρώτα στοιχεία μελετούμε πλέον πρώτα ιδεώδη. Αντί για ανάγωγα στοιχεία μελετούμε ανάγωγα ιδεώδη. Θυμίζουμε ότι ένα γνήσιο ιδεώδες  $P$  του δακτυλίου  $R$  λέγεται πρώτο εάν  $fg \in P$  τότε  $f$  ή  $g$  ανήκουν στο  $P$ , δηλαδή  $R/P$  είναι ακεραία περιοχή.

### Ασκήσεις 1.2.

- Να αποδείξετε ότι  $\langle 2 \rangle$  δεν είναι πρώτο ιδεώδες του  $\mathbb{Z}[\sqrt{-5}]$ .
- Να αποδείξετε ότι  $\langle 2, 1 + i\sqrt{5} \rangle$  είναι πρώτο ιδεώδες του  $\mathbb{Z}[\sqrt{-5}]$ . Υπόδειξη Χρησιμοποιείστε το τρίτο Θεώρημα Ισομορφίας Δακτυλίων για να δείξετε ότι  $\mathbb{Z}[\sqrt{-5}]/P \cong \mathbb{Z}_2$ .

Θα δείξουμε ότι οι δύο παραγοντοποιήσεις του 6 στο  $\mathbb{Z}[\sqrt{-5}]$ ,

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

ανστιστοιχούν στην ίδια παραγοντοποίηση του  $\langle 6 \rangle$  σε γινόμενο πρώτων ιδεωδών. Έστω

$$P = \langle 2, 1 + i\sqrt{5} \rangle, Q = \langle 3, 1 + i\sqrt{5} \rangle, R = \langle 3, 1 - i\sqrt{5} \rangle$$

Μπορεί να αποδείξει κανείς ότι κάθε ένα από αυτά τα ιδεώδη είναι πρώτο. Επίσης

$$P^2 = \langle 2 \rangle, QR = \langle 3 \rangle, PQ = \langle 1 + i\sqrt{5} \rangle, PR = \langle 1 - i\sqrt{5} \rangle.$$

Παρακάτω θα ελέγξουμε ότι όντως  $P^2 = \langle 2 \rangle$ . Παρατηρούμε ότι

- $4 \in P^2$ ,
- $2 + 2i\sqrt{5} = 2(1 + i\sqrt{5}) \in P^2$ ,
- $(1 + i\sqrt{5})^2 = -4 + 2i\sqrt{5} \in P^2$ , άρα
- $2 = 4 - 2(1 + i\sqrt{5}) + (-4 + 2i\sqrt{5}) \in P^2$  και αφού  $\langle 2 \rangle \subset P^2$  έπειται ότι  $P^2 = \langle 2 \rangle$ .

Επομένως

$$\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = P^2(QR) = P^2QR$$

ενώ

$$\langle 6 \rangle = \langle 6 \rangle = \langle 1 + i\sqrt{5} \rangle \langle 1 - i\sqrt{5} \rangle = (PQ)(PR) = P^2QR.$$

Η E. Noether μία από τους πιο σπουδαίους μαθηματικούς του 20ου αιώνα ενοποίησε τις έννοιες των ιδεωδών των Dedekind και Lasker και έθεσε τις αξιωματικές βάσεις της αντιμεταθετικής άλγεβρας. Θα μιλήσουμε για παραγοντοποίηση ιδεωδών στις επόμενες διαλέξεις.

**1.1.2. Άλγεβρική Γεωμετρία.** Θα δούμε επίσης τη σύνδεση της Αντιμεταθετικής Άλγεβρας με την Άλγεβρική Γεωμετρία. Το Θεμελιώδες Θεώρημα της Άλγεβρας που πρωτοαπέδειξε ο Gauss το 1803 λέει ότι ένα μη μηδενικό πολυώνυμο  $f(x)$  με μιγαδικούς συντελεστές έχει ακριβώς  $\deg(f)$  ρίζες στο σώμα των μιγαδικών αριθμών. Θα αναζητήσουμε τη γενίκευση αυτού του θεωρήματος.

Έστω ότι έχουμε ένα σύνολο  $S$  πολυωνύμων με πολλές μεταβλητές στον δακτύλιο  $\mathbb{C}[x_1, \dots, x_n]$ . Τι μπορούμε να πούμε για τα κοινά μηδενικά αυτών των πολυωνύμων; Ορίζουμε

$$Z(S) = \{(a_1, \dots, a_n) \in \mathbb{C}^n : g(a_1, \dots, a_n) = 0, \forall g \in S\}.$$

Είναι το σύνολο  $Z(S)$  διάφορο του κενού; Αντίστροφα, έστω  $X$  ένα υποσύνολο του  $\mathbb{C}^n$ . Μπορούμε να αναγνωρίσουμε αν  $X$  ισούται με τα μηδενικά κάποιου συνόλου πολυωνύμων του  $\mathbb{C}[x_1, \dots, x_n]$ ; Έστω

$$\mathbb{I}(X) = \{f : f(a_1, \dots, a_n) = 0, \forall (a_1, \dots, a_n) \in X\}.$$

Ποια είναι η σχέση του  $X$  και του  $Z(\mathbb{I}(X))$ ; Αντίστροφα, αν θέσουμε  $X = Z(S)$ , ποια είναι η σχέση του  $\mathbb{I}(X)$  και του  $S$ ;

**Παραδείγματα 1.3.**

- Έστω  $S = \{x^2 - 4, x^2 - 5x + 6\}$ . Τότε  $Z(S) = \{2\}$  ενώ  $\mathbb{I}(\{2\}) = (x - 2)$ . Έστω  $\langle S \rangle$  το ιδεώδες του  $\mathbb{C}[x]$  που παράγεται από το  $S$ :

$$I = \{f(x)(x^2 - 4) + g(x)(x^2 - 5x + 6) : f(x), g(x) \in \mathbb{C}[x]\}.$$

Τότε  $\langle S \rangle = (x - 2)$ .

- Έστω  $S = \{x^2, y^2\}$ . Τότε  $Z(S) = \{(0, 0)\} = X$  ενώ  $\mathbb{I}(X) = (x, y)$ .

Το ριζικό radical του ιδεώδους  $I$  είναι το σύνολο

$$\text{rad}(I) = \{f : f^m \in I, \text{ για κάποιο } m\}.$$

Ο Hilbert απέδειξε ουσιαστικά ότι στο  $\mathbb{C}[x]$  ισχύει ότι  $\mathbb{I}(Z(S)) = \text{rad}(\langle S \rangle)$ . Έδειξε επίσης ότι αν τα πολυώνυμα  $f_1, \dots, f_m$  του  $\mathbb{C}[x_1, \dots, x_n]$  δεν έχουν κάποιο κοινό μηδενικό, τότε υπάρχουν πολυώνυμα  $g_1, \dots, g_m$  στο  $\mathbb{C}[x_1, \dots, x_n]$  έτσι ώστε

$$1 = g_1 f_1 + \dots + g_m f_m.$$

Τα υθεωρήματα αυτά είναι γνωστά ως το Θεώρημα των μηδενικών του Hilbert (Hilbert's Nullstellensatz) και είναι από τα βασικά υθεωρήματα αυτού του μαθήματος. Παρατηρείστε ότι το ανάλογο δεν ισχύει όταν έχουμε πολυώνυμα στο  $\mathbb{R}[x_1, \dots, x_n]$  και ερευνούμε τις ρίζες τους στο  $\mathbb{R}^n$  (με αντίστοιχους ορισμούς για  $Z(S)$  και  $\mathbb{I}(X)$ ).

**Παράδειγμα 1.4.** Έστω  $S = \{x^2 + 1\} \subset \mathbb{R}[x]$ . Τότε  $Z(S) = \emptyset$ ,  $\mathbb{I}(\emptyset) = \mathbb{R}[x]$  και  $\text{rad}(\langle x^2 + 1 \rangle) = \langle x^2 + 1 \rangle \neq \mathbb{R}[x]$ .

Δεν είναι δύσκολο να δει κανείς ότι η συνεπαγωγή  $\langle f_1, \dots, f_m \rangle \neq \mathbb{C}[x_1, \dots, x_n] \Rightarrow Z(\langle f_1, \dots, f_m \rangle) \neq \emptyset$  είναι άμεσο αποτέλεσμα της σχέσης  $\mathbb{I}(Z(S)) = \text{rad}(\langle S \rangle)$ .

Απόδειξη. Έστω ότι  $\langle f_1, \dots, f_m \rangle \neq \mathbb{C}[x_1, \dots, x_n]$  και ότι  $Z(\langle f_1, \dots, f_m \rangle) = \emptyset$ . Άρα  $\mathbb{I}(Z(S)) = \mathbb{C}[x_1, \dots, x_n]$  και  $\text{rad}(\langle S \rangle) = \mathbb{C}[x_1, \dots, x_n]$ . Έπειτα ότι  $1 \in \text{rad}(\langle S \rangle)$ . Από τον ορισμό προκύπτει ότι για κάποιο  $t \in \mathbb{N}$  ισχύει ότι  $1^t = 1 \in \langle S \rangle$  και άρα  $\langle S \rangle = \mathbb{C}[x_1, \dots, x_n]$ , άτοπο.  $\square$

### Ασκήσεις 1.5.

- Να αποδείξετε ότι τα σύνολα  $\mathbb{I}(X)$  και  $\text{rad}(I)$  είναι ιδεώδη.
- Έστω  $f(x) = x^4 + 2x^2 + 1$  και  $I = (f(x))$ . Να υπολογίσετε  $\text{rad}(I)$ ,  $Z(I)$  και  $\mathbb{I}(Z(I))$  όταν υθεωρήσουμε το  $I$  σαν ιδεώδες του  $\mathbb{Z}_5[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$ .

1.1.3. **Θεωρία Αναλλοιώτων.** Οι απαρχές της Αντιμεταθετικής Άλγεβρας σηματοδοτήθηκαν επίσης τη σύνδεση με τη Θεωρία των Αναλλοιώτων (Invariant Theory). Θα ξεκινήσουμε με δύο παραδείγματα.

**Παραδείγματα 1.6.** Για τα δύο παραδείγματα που ακολουθούν,  $G$  είναι η ομάδα με δύο στοιχεία:  $G = \{e, g\}$ , όπου  $g^2 = e$  που δρα στον  $\mathbb{C}[x, y]$ .

- Θα υθεωρήσουμε τη παρακάτω δράση της  $G$ :  $g(x) = -x$ ,  $g(y) = -y$ , και έτσι  $g(f(x, y)) = f(gx, gy)$ . Το ερώτημα που θέτουμε αφορά τα πολυώνυμα που δεν επηρεάζονται από τη δράση της  $G$ . Ποια είναι εκείνα τα  $r \in \mathbb{C}[x, y]$  έτσι ώστε  $g(r) = r$ ? Μπορεί να αποδειχθεί ότι αναλλοιώτα από τη δράση της  $G$  είναι ακριβώς εκείνα τα πολυώνυμα που ανήκουν στον υποδακτύλιο  $\mathbb{C}[x^2, y^2, xy]$  και άρα ο υποδακτύλιος των αναλλοιώτων είναι πεπερασμένα παραγόμενος.
- Έστω ότι  $G$  δρα στον  $\mathbb{C}[x, y]$  ως εξής:  $g(x) = y$ ,  $g(y) = x$ . Μπορεί να αποδειχθεί ότι αναλλοιώτα από τη δράση της  $G$  είναι ακριβώς εκείνα τα πολυώνυμα που ανήκουν στον υποδακτύλιο  $\mathbb{C}[x+y, xy]$ , επίσης πεπερασμένα παραγόμενος.

Ένα από τα μεγάλα προβλήματα που απασχολούσε τους μαθηματικούς στο τέλος του 19ου αιώνα και αρχές του 20ου είναι η περιγραφή των αναλλοιώτων, (14o πρόβλημα του Hilbert). Ο Hilbert σε μία ευρεία κλάση περιπτώσεων έδειξε ότι η υποάλγεβρα

των αναλλοιώτων είναι πεπερασμένα παραγόμενη. Στηρίχτηκε σε αυτό που σήμερα είναι γνωστό ως το Θεώρημα Βάσης του Hilbert, δηλαδή ότι κάθε ιδεώδες στον  $\mathbb{C}[x_1, \dots, x_n]$  είναι πεπερασμένα παραγόμενο. Το Θεώρημα αυτό γενίκευσε μετέπειτα η Noether για τους δακτυλίους που είναι γνωστοί με το όνομά της και ανέπτυξε αξιωματικά την Αντιμεταθετική Άλγεβρα.