Θεωρία Κλάσεων Σωμάτων και Εφαρμογές στην Κρυπτογραφία

Νίκος Γκερπινής

27/6/2005

Περιεχόμενα

Εισαγωγή

Σε αυτή την εργασία προσπαθούμε να δώσουμε μία εφαρμογή της αλγεβρικής θεωρίας αριθμών και της ακριβούς θεωρίας κλάσεων σωμάτων στην κρυπτογραφία. Ένα αποτελεσματικό κρυπτοσύστημα είναι αυτό που βασίζεται στο πρόβλημα του διακριτού λογαρίθμου σε μία πεπερασμένη ομάδα. Πολλές πεπερασμένες ομάδες έχουν χρησιμοποιηθεί στην βιβλιογραφία για την υλοποιήση της μεθόδου του διακριτού λογαρίθμου και μία από τις, κατά γενική παραδοχή, αποτελεσματικότερες είναι οι ομάδες των ρητών σημείων που ορίζονται πάνω από πεπερασμένα σώματα.

Οι ειδικοί της κρυπτοανάλυσης έχουν δώσει μία σειρά από «στρατηγικές» οι οποίες χρησιμοποιούνται για την αποκρυπτογράφιση κρυποσυστημάτων που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου. Προκειμένου να κατασκευάσουμε αποτελεσμάτικα κρυπτοσυστήματα βασισμένα στην μέθοδο του διακριτού λογάριθμου η τάξη της ομάδας της ελλειπτικής καμπύλης θα πρέπει να ικανοποιεί μία σειρά από συνθήκες. Θα πρέπει λοιπόν να κατασκευάσουμε ελλειπτικές καμπύλες οι οποίες να έχουν εκ των προτέρων γνωστή τάξη.

Το πρόβλημα του προσδιορισμού της τάξης των σημείων μίας ελλειπτικής καμπύλης είναι ένα δύσκολο και βαθύ πρόβλημα. Για μία ειδική κατηγορία ελλειπτικών καμπύλων, τις λεγόμενες ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό το πρόβλημα αυτό έχει λύση.

Πράγματι η j-αναλλοίωτη μίας ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό παράγει το λεγόμενο σώμα του Hilbert ενός μιγαδικού τετραγωνικού σώματος αριθμών. Αυτό το ανέλπιστο θεώρημα μας δίνει την δυνατότητα να κατασκεύασουμε την j-αναλλοίωτη ως ρίζα του πολυωνύμου Hilbert και να δώσουμε συνθήκες στην αριθμητική των ιδεωδών ενός μιγαδικού τετραγωνικού σώματος αριθμών, ώστε το πολυώνυμο Hilbert να έχει όλες του τις ρίζες σε ένα πεπερασμένο σώμα $\mathbb{F}_p$.

Προκειμένου να ορίσουμε και να χρησιμοποιήσουμε τα παραπάνω εργαλεία, κάνουμε στα έξι πρώτα κεφάλαια μία εισαγωγή σε μερικά στοιχεία της αλγεβρικής θεωρίας αριθμών.

Στο πρώτο κεφάλαιο δίνουμε τους βασικούς ορισμούς που θα χρησιμοποιήσουμε, όπως ενός ακέραιου αλγεβρικού αριθμού, ενός σώματος αριθμών K και του δακτύλιου ακεραίων του $\mathfrak{D}_K$. Επίσης περιγράφουμε τον τρόπο εύρεσης της βάσης ακεραιότητας ενός δακτυλίου ακεραίων. Τέλος γίνεται και ιδιαίτερη αναφορά στα τετραγωνικά μιγαδικά σώματα, δηλαδή σε επεκτάσεις του $\mathbb{Q}$ της μορφής $\mathbb{Q}(\sqrt{d})$, όπου d ένας αρνητικός αριθμός ελεύθερος τετραγώνων. Ένας δακτύλιος ακεραίων ενός σώματος αριθμών, είναι Noetherian ακέραια περιοχή, επομένως είναι δυνατή η ανάλυση σε πρώτα στοιχεία, χωρίς όμως να αποτελεί ΠΜΑ. Σε τέτοιους δακτυλίους ακεραίων θα προσπαθήσουμε να παραγοντοποιήσουμε ιδεώδη, κάνοντας χρήση της νόρμας τους. Με χρήση της θεωρίας των πλεγμάτων (lattice), θα ορί-

σουμε τον χώρο L^{st} και θα πάρουμε ένα πολυτιμότατο εργαλείο, το θεώρημα του Minkowski, το οποίο θα μας εξασφαλίσει ότι κάθε ιδεώδες $\mathfrak{a}$ που ανήκει στον $\mathfrak{D}_K$ είναι ισοδύναμο με ένα ιδεώδες νόρμας $\leq (2/\pi)^t\sqrt{\Delta}$, όπου Δ είναι η διακρίνουσα της βάσης ακεραιότητας του $\mathfrak{D}_K$. Αυτό το αποτέλεσμα, είναι που θα μας δώσει τη δυνατότητα να βρούμε την τάξη της class group του $\mathfrak{D}_K$.

Στη συνέχεια δίνουμε το θεώρημα ανάλυσης. Αν έχουμε μία επέκταση Galois $K \subset L = K(\alpha)$, και πάρουμε ένα πρώτο ιδεώδες $\mathfrak{p} \in \mathfrak{D}_K$ και αν το ελάχιστο πολυώνυμο του α αναλύεται πλήρως $\mathrm{mod}\mathfrak{p}$, έχουμε ότι το ιδεώδες $\mathfrak{p}$ είναι αδιακλάδωτο στον $\mathfrak{D}_L$ και μπορούμε εύκολα να το γράψουμε σαν γινόμενο πρώτων ιδεωδών του $\mathfrak{D}_L$. Η μέγιστη αδιακλάδωτη και αβελιανή επέκταση του K, ονομάζεται σώμα κλάσεων του Hilbert. Μέσω του ομομορφισμού του Artin, θα καταφέρουμε να φτάσουμε σε ένα από τα θεμελιώδη για τη δουλειά μας αποτελάσματα, ότι η class group $\mathcal{H}$ του $\mathfrak{D}_K$ είναι ισόμορφη με την ομάδα Galois της επέκτασης L/K. Επίσης ένα πρώτο ιδεώδες του K θα διασπάται πλήρως στο L, αν και μόνο αν είναι κύριο.

Στο έβδομο κεφάλαιο δίνονται μερικά βασικά στοιχεία της θεωρίας των ελλειπτικών καμπύλων, και ορίζονται οι ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό. Οι ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό αποτελούν μία πολύ ιδιαίτερη κλάση ελλειπτικών καμπύλων η οποία συνδέεται με την ακριβή κατασκευή του σώματος κλάσεων του Hilbert. Αφού ορίσουμε τις ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό, δείχνουμε πως μπορούμε να τις χρησιμοποιήσουμε για να υπολογίσουμε την j-αναλλοίωτη της ελλειπτικής καμπύλης που θέλουμε να κατασκευάσουμε. Η ιδέα είναι να κάνουμε αναγωγή modulo ένα κατάληλο κύριο ιδεώδες ενός τετραγωνικού σώματος αριθμών στο πολυώνυμο του Hilbert. Για να γίνει αυτό θα πρέπει να υπολογίσουμε την τιμή της j-αναλλοίωτης, την οποία την θεωρούμε ως μία modular συνάρτησης της $SL_2(\mathbb{Z})$. Το πολυώνυμο Hilbert κατασκευάζεται με την χρήση των τετραγωνικών μορφών οι οποίες εισάγονται στο όγδοο κεφάλαιο.

Θα πρέπει να τονίσουμε, ότι η προσέγγισή μας είναι καθαρά θεωρητική και δεν μας απασχολούν προβλήματα υλοποιήσης όπως το μέγεθος των συντελεστών του πολυωνύμου Hilbert, ούτε η μεγάλη ακρίβεια κινητής υποδιαστολής που απαιτείται για τον υπολογισμό της τιμής της modular συνάρτησης j πάνω στο πλέγμα που ορίζει ο δακτύλιος των ακεραίων αλγεβρικών του μιγαδικού τετραγωνικού σώματος.

Θα ήθελα εδώ, να εκφράσω τις ευχαριστίες μου στον δάσκαλο μου Αριστείδη Κοντογεώργη για τον χρόνο του και για το κουράγιο που μου έδωσε κατά την διάρκεια της εκπόνησης της πτυχιακής μου εργασίας. Επίσης θέλω να ευχαριστήσω τα υπόλοιπα μέλη της επιτροπής, τους κ. Μεταφτσή Β. και κ. Μπεληγιάννη Α. για τον χρόνο που διάθεσαν. Τέλος ευχαριστίες στον Σωτήρη για την δημιουργία των σχημάτων και φυσικά για τις ώρες που διαβαζαμε μαζί όλον αυτόν τον καιρό, και στην Χιονάτη για την παροχή του ηλεκτρονικού του υπολογιστή.

Νίκος Γκερπινής , Σάμος Ιούνιος 2005.

Κεφάλαιο 1

Αλγεβρικοί αριθμοί

1.1 Αλγεβρικοί αριθμοί

Κάτι που θα μας απασχολήσει σε μεγάλο βαθμό σε αυτήν την εργασία, είναι η παραγοντοποίηση ενός αριθμού. Είναι επίσης και το που θέλουμε να τον παραγοντοποιήσουμε. Γενικά δουλεύουμε σε κατάλληλους υποδακτύλιους του $\mathbb{C}$. Θα δούμε τα δύο πιο βασικά στοιχεία της δουλειάς μας, τα οποία είναι ένα αλγεβρικό σώμα αριθμών και ο δακτύλιος των αλγεβρικών ακεραίων αυτού του σώματος. Σε έναν τέτοιον δακτύλιο θα ψάξουμε για τρόπο να παραγοντοποιήσουμε. Δίνουμε πρώτα τον ορισμό ενός αλγεβρικού αριθμού.

Ορισμός 1.1 *Ένας μιγαδικός αριθμός a καλείται αλγεβρικός αν είναι αλγεβρικός πάνω από το $\mathbb{Q}$, το οποίο σημαίνει ότι ικανοποιεί κάποιο πολυώνυμο με ρητούς συντελεστές. Ισοδύναμα, αν διώξουμε τους παρανομαστές μπορούμε να υποθέσουμε ότι οι συντελεστές είναι στο $\mathbb{Z}$. Θα συμβολίζουμε από εδώ και πέρα με $\mathbb{A}$ το σύνολο των αλγεβρικών αριθμών.*

Θεώρημα 1.1 *Το σύνολο $\mathbb{A}$ των αλγεβρικών αριθμών, είναι ένα υπόσωμα του $\mathbb{C}$.*

Απόδειξη. Γνωρίζουμε ότι ένας αριθμός a είναι αλγεβρικός, αν και μόνο αν ο βαθμός της επέκτασης $[\mathbb{Q}(a) : \mathbb{Q}]$ είναι πεπερασμένος. Έστω ότι έχουμε δύο αλγεβρικούς αριθμούς a, b. Τότε θα έχουμε

$$[\mathbb{Q}(a,b) : \mathbb{Q}] = [\mathbb{Q}(a,b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}].$$

Αφού ο b είναι αλγεβρικός πάνω από το $\mathbb{Q}$, θα είναι αλγεβρικός και πάνω από το $\mathbb{Q}(a)$. Επομένως ο $[\mathbb{Q}(a,b) : \mathbb{Q}(a)]$ είναι πεπερασμένος. Επίσης, προφανώς ο $[\mathbb{Q}(a) : \mathbb{Q}]$ είναι πεπερασμένος, άρα τελικά ο $[\mathbb{Q}(a,b) : \mathbb{Q}]$ είναι πεπερασμένος. Αλλά κάθε $a+b, a-b, ab, a|b,\ (b \neq 0)$ ανήκει στο $\mathbb{Q}(a,b)$. Δηλαδή όλα αυτά θα ανήκουν στο $\mathbb{A}$.

Ορισμός 1.2 *Θα καλούμε ένα σώμα K, σώμα αριθμών αν είναι υπόσωμα του $\mathbb{C}$ και ο βαθμός επέκτασής του πάνω από το $\mathbb{Q}$ είναι πεπερασμένος.*

Αυτό μας λέει ότι κάθε στοιχείο του K είναι αλγεβρικό, οπότε θα έχουμε ότι $K \subseteq \mathbb{C}$.

Θεώρημα 1.2 *Αν K είναι ένα σώμα αριθμών, τότε $K = \mathbb{Q}(u)$ για κάποιον u αλγεβρικό αριθμό.*

Απόδειξη. Θα υποθέσουμε ότι αν $K = K_1(a, b)$ τότε $K = K_1(u)$. Έστω ότι p, q είναι τα ελάχιστα πολυώνυμα των a, b αντίστοιχα πάνω από το K_1. Έστω ότι η παραγοντοποίηση αυτών των πολυωνύμων πάνω από τους μιγαδικούς είναι

$$p(t) = (t - a_1)...(t - a_n)$$

$$q(t) = (t - b_1)...(t - b_m).$$

Επιλέγω να είναι $a = a_1, b = b_1$. Γνωρίζουμε επίσης ότι όλα τα a_i είναι διαφορετικά μεταξύ τους, όπως και τα b_j. Επομένως για κάθε i και κάθε $k \neq 1$ υπάρχει τουλάχιστον ένα στοιχείο x στο K_1, τέτοιο ώστε $a_i + xb_k = a_1 + xb_1$. Από την στιγμή που υπάρχουν πεπερασμένες το πλήθος τέτοιες εξισώσεις, μπορούμε να επιλέξουμε ένα $c \in K_1$ με $c \neq 0$, το οποίο να μην είναι ίσο με κανένα από αυτά τα x και τότε θα έχουμε

$$a_i + cb_k \neq a_1 + cb_1.$$

Θέτουμε $u = a + cb$. Θα αποδείξουμε ότι $K_1(u) = K_1(a, b)$. Το ότι $K_1(u) \subseteq K_1(a, b)$ είναι προφανές, άρα μένει να δείξουμε ότι $K_1(u) \supseteq K_1(a, b)$. Αρκεί να δείξουμε ότι $b \in K_u$ αφού $a = u - cb$. Έχουμε $p(u - cb) = p(a) = 0$, και ορίζουμε το πολυώνυμο $r(t) = p(u - ct) \in K_1(u)[t]$. Τότε το b είναι ρίζα και του $q(t)$ και του $r(t)$. Αυτά τα πολυώνυμα θα έχουν μόνο μία κοινή ρίζα, γιατί αν είχαμε και μία άλλη ρίζα ξ, με $q(\xi) = r(\xi) = 0$ τότε το ξ θα είναι ένα εκ των b_i και επίσης το $u - c\xi$ θα είναι ένα εκ των a_i. Είναι πλέον προφανές ότι πρέπει να είναι $\xi = b$. Έστω $h(t)$ το ελάχιστο πολυώνυμο του b πάνω από το $K_1(u)$. Τότε θα είναι $h(t) \mid q(t), h(t) \mid r(t)$. Και επειδή έχουμε ότι τα $q(t)$ και $r(t)$ έχουν μόνο μία κοινή ρίζα στο $\mathbb{C}$, πρέπει να είναι $\deg h(t) = 1$, έτσι $h(t) = t + l$ για κάποιο $l \in K_1(u)$. Τέλος θα έχουμε $0 = h(b) = b + l \Leftrightarrow b = -l \in K_1(u)$.

Ας δούμε ένα παράδειγμα της χρησιμότητας του παραπάνω.

Παράδειγμα 1.1 *Θα δείξουμε με ελάχιστο κόπο, ότι $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$. Είναι*

$$a_1 = \sqrt{2}, a_2 = -\sqrt{2}$$

$$b_1 = \sqrt[3]{5}, b_2 = \omega\sqrt[3]{5}, b_3 = \omega^2\sqrt[3]{5}$$

με το ω να είναι μία μιγαδική κυβική ρίζα της μονάδας $\omega = 1/2(-1 + \sqrt[3]{-3})$. Για την τιμή τώρα του $c = 1$ παρατηρούμε ότι

$$a_i + cb_j \neq \sqrt{2} + c\sqrt[3]{5}$$

αφού το δεξί μέλος είναι πραγματικός αριθμός, ενώ το αριστερό είναι μιγαδικό για όλες τις περιπτώσεις ($k \neq 1$). Επομένως, όπως δείξαμε στην απόδειξη του προηγούμενου θεωρήματος και φτάνοντας σε αυτό που ζητήσαμε $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$.

1.2 Συζυγή και διακρίνουσες

Έστω ότι έχουμε ένα σώμα αριθμών $K = \mathbb{Q}(u)$. Το K μπορεί να εμφυτευτεί στο $\mathbb{C}$ με διαφορετικούς τρόπους, μέσω των μονομορφισμών $\sigma : K \to \mathbb{C}$. Για παράδειγμα, αν έχουμε $K = \mathbb{Q}(i)$ τότε θα έχουμε δύο περιπτώσεις.

$$\sigma(x + iy) = x + iy$$

$$\sigma(x+iy) = x - iy, x, y \in \mathbb{Q}.$$

Το σύνολο αυτών των μονομορφισμών θα μας απασχολήσει ιδιαίτερα στη συνέχεια.

Θεώρημα 1.3 *Έστω $K = \mathbb{Q}(u)$ σώμα αριθμών, με βαθμό επέκτασης n πάνω από το $\mathbb{Q}$. Τότε υπάρχουν ακριβώς n διαφορετικοί μονομορφισμοί $\sigma_i : K \to \mathbb{C}$. Επίσης, τα στοιχεία $\sigma_i(u) = u_i$, είναι οι διαφορετικές ρίζες στο $\mathbb{C}$, του ελάχιστου πολυωνύμου του u πάνω από το $\mathbb{Q}$.*

Απόδειξη. Έστω $u_1, ...u_n$ οι διαφορετικές ρίζες του ελάχιστου πολυωνύμου p του u. Τότε και το κάθε u_i θα έχει ελάχιστο πολυώνυμο το p, επειδή το p είναι ανάγωγο. Επομένως υπάρχει μοναδικός ισομορφισμός σωμάτων $\sigma_i : \mathbb{Q}(u) \to \mathbb{Q}(u_i)$, για τον οποίο $\sigma_i(u) = u_i$. Ουσιαστικά, αν πάρουμε ένα $a \in \mathbb{Q}(u)$ τότε θα έχουμε $a = r(u)$ για κάποιο μοναδικό πολυώνυμο $r(t) \in \mathbb{Q}[t]$, με $\deg r(t) < n$. Άρα τότε θα έχουμε $\sigma_i(a) = r(u_i)$. Αντίστροφα, αν ο $\sigma : K \to \mathbb{C}$ είναι ένας μονομορφισμός, τότε ο σ είναι ο ταυτοτικός στο $\mathbb{Q}$. Άρα θα είναι

$$\sigma(p(u)) = \sigma(0) = 0 = p(\sigma(u)).$$

Πράγμα το οποίο μας οδηγεί στο συμπέρασμα ότι το $\sigma(u)$ είναι μία εκ των u_i ριζών, άρα και ο σ είναι ένας εκ των σ_i.

Ορισμός 1.3 *Για κάθε $a \in K = \mathbb{Q}(u)$ ορίζουμε σαν πολυώνυμο σώματος του a πάνω από το K να είναι το*

$$f_a(t) = \prod_{i=1}^{n} (t - \sigma_i(a)).$$

Με τη βοήθεια του ορισμού του συμμετρικού πολυωνύμου, θα διατυπώσουμε ένα πόρισμα χωρίς την απόδειξή του, το οποίο θα μας φανεί χρήσιμο στο επόμενο θεώρημα.

Ορισμός 1.4 *Έστω $R[t_1, ..., t_n]$ δακτύλιος πολυωνύμων. Έστω S_n η συμμετρική ομάδα μεταθέσεων των n στοιχείων. Για κάθε μετάθεση $\sigma \in S_n$ και κάθε πολυώνυμο $f \in R[t_1, ..., t_n]$, ορίζουμε το πολυώνυμο*

$$f^\sigma(t_1, ..., t_n) = f(t_{\sigma(1)}, ..., t_{\sigma(n)}).$$

Ένα πολυώνυμο ονομάζεται συμμετρικό, αν και μόνο αν $f^\sigma = f$ για κάθε $\sigma \in S_n$.

Πόρισμα 1.1 *Έστω ότι έχουμε μία επέκταση L ενός σώματος K. Επίσης έστω πολυώνυμο $p \in K[t], \deg p(t) = n$ και οι ρίζες του p είναι οι $u_1, ..., u_n \in L$. Αν $h(t_1, ...t_n) \in K[t_1, ...t_n]$ είναι συμμετρικό, τότε $h(u_1, ..., u_n) \in K$.*

Απόδειξη. Βλέπε πόρισμα 1.10 [1].

Θεώρημα 1.4 *Οι συντελεστές του πολυωνύμου σώματος είναι ρητοί αριθμοί, δηλαδή $f_a(t) \in \mathbb{Q}[t]$.*

Απόδειξη. Όπως έχουμε πει, έχουμε $a = r(u), r(t) \in \mathbb{Q}[t]$ και $\deg r(t) < n$. Το πολυώνυμο σώματος παίρνει την εξής μορφή:

$$f_a(t) = \prod_{i} (t - r(u_i)).$$

Οι συντελεστές του $f_a(t)$ είναι της μορφής $h(u_1, ..., u_n)$, όπου το $h(t_1, ..., t_n)$ είναι ένα συμμετρικό πολυώνυμο στο $\mathbb{Q}[t_1, ..., t_n]$. Τέλος και με χρήση του πορίσματος 1.1, οι συντελεστές του πολυωνύμου σώματος $h(t_1, ..., h_t n) \in \mathbb{Q}$.

Ορισμός 1.5 *Τα στοιχεία $\sigma_i(a)$ ονομάζονται K-συζυγή του a.*

Θεώρημα 1.5

1. *Το πολυώνυμο σώματος f_a είναι μία δύναμη του ελάχιστου πολυωνύμου p_a.*
2. *Τα K-συζυγή του a είναι οι ρίζες του p_a στο $\mathbb{C}$, με την καθεμιά να επαναλαμβάνεται n/m φορές, όπου m είναι ο βαθμός του πολυωνύμου p_a και διαιρέτης του n.*
3. *Το στοιχείο $a \in \mathbb{Q}$ αν και μόνο αν όλα του τα K-συζυγή, είναι ίσα.*
4. *Θα έχουμε $\mathbb{Q}(a) = \mathbb{Q}(u)$, αν και μόνο αν όλα τα K-συζυγή του a είναι διαφορετικά μεταξύ τους.*

*Απόδειξη.*Βλέπε θεώρημα 2.5 [1].

Ορισμός 1.6 *Αν έχουμε λοιπόν την επέκταση του $\mathbb{Q}$, $K = \mathbb{Q}(u)$ βαθμού n, και μία βάση του $(a_1, ..., a_n)$ αν το δούμε σα διανυσματικό χώρο πάνω από το $\mathbb{Q}$, ορίζουμε σα διακρίνουσα της βάσης αυτής να είναι:*

$$\Delta[a_1, ..., a_n] = [det(\sigma_i(a_j))]^2$$

Έστω ότι επιλέγουμε μία άλλη βάση $(b_1, ..., b_n)$. Τότε θα είναι:

$$b_k = \sum_{i=1}^{n} c_{ik} a_i$$

για $c_{ik} \in \mathbb{Q}, k = 1, ..., n$ και $det(c_{ik}) \neq 0$. Από την στιγμή που κάθε μονομορφισμό σ_i, αν τον περιορίσω στο $\mathbb{Q}$ είναι ο ταυτοτικός, θα πάρουμε:

$$\Delta[b_1, ..., b_n] = [det(c_{ik})]^2 \Delta[a_1, ..., a_n].$$

Θεώρημα 1.6 *Η διακρίνουσα κάθε βάσης για το $K = \mathbb{Q}(u)$ είναι ρητός αριθμός και μη μηδενικός. Επίσης αν όλα τα K-συζυγή του u είναι πραγματικοί αριθμοί, τότε η διακρίνουσα κάθε βάσης είναι και θετικός αριθμός.*

Απόδειξη. Επιλέγουμε τη βάση την οποία μας βολεύει, $(1, u, ..., u^{n-1})$. Αν τα συζυγή του u είναι οι $u_1, ..., u_n$ θα έχουμε $\Delta[1, u, ..., u^{n-1}] = (detu_i^j)^2$. Μία ορίζουσα αυτής της μορφής ονομάζεται Vandermonde ορίζουσα και αποδεικνύεται ότι η τιμή της δίνεται από

$$D = \sum_{1 \leq i < j \leq n} (t_i - t_j).$$

Επομένως θα έχουμε

$$\Delta = \Delta[1, u, ..., u^{n-1}] = [\prod (u_i - u_j)]^2.$$

Παρατηρούμε ότι το D σαν πολυώνυμο του t_i, είναι αντισυμμετρικό, άρα το D^2 θα είναι συμμετρικό. Επομένως, σύμφωνα με το πόρισμα 1.1, το Δ είναι ρητός αριθμός. Επίσης αφού τα u_i είναι διαφορετικά μεταξύ τους, το Δ θα είναι και

διάφορο του μηδέν. Έστω επίσης μία οποιαδήποτε βάση $(b_1, ..., b_n)$. Τότε σύμφωνα με τον τύπο που δείξαμε πριν θα είναι

$$\Delta[b_1, ..., b_n] = (detc_{ik})^2 \Delta$$

με c_{ik} ρητούς αριθμούς και $detc_{ik} \neq 0$, έτσι η $\Delta[b_1, ..., b_n]$ είναι ρητός αριθμός και διάφορος του μηδέν. Τέλος είναι προφανές ότι αν όλα τα u_i είναι πραγματικοί αριθμοί, το Δ θα είναι θετικός αριθμός και το ίδιο και η διακρίνουσα κάθε άλλης βάσης.

1.3 Ακέραιοι αλγεβρικοί αριθμοί

Ξεκινάμε την παράγραφο με τον ορισμό ενός ακέραιου αλγεβρικού αριθμού.

Ορισμός 1.7 *Ένας μιγαδικός αριθμός u θα ονομάζεται ακέραιος αλγεβρικός αν υπάρχει ένα μονικό πολυώνυμο $p(t)$ με ακέραιους συντελεστές, τέτοιο ώστε $p(u) = 0$. Δηλαδή θα ισχύει $u^n + a_{n-1}u^{n-1} + ... + a_0 = 0$ με τα $a_i \in \mathbb{Z}$.*

Παράδειγμα 1.2 *Σύμφωνα λοιπόν με τον παραπάνω ορισμό, ο αριθμός $u = \sqrt{-2}$ είναι ακέραιος αλγεβρικός αφού $u^2+2 = 0$. Ο αριθμός $t = 1/2(1+\sqrt{5})$ είναι επίσης ακέραιος αλγεβρικός αφού $t^2 - t - 1 = 0$. Ενώ αντίθετα, ο αριθμός $m = 23/2$ μπορεί να ικανοποιεί την εξίσωση $2m-23 = 0$, η οποία δεν είναι μονικό πολυώνυμο. Ικανοποιεί επίσης την $m - 23/2 = 0$, αλλά αυτή δεν έχει ακέραιους συντελεστές για να καθιστούν το m ακέραιο αλγεβρικό αριθμό.*

Από εδώ και πέρα θα συμβολίζουμε με $\mathbb{B}$ το σύνολο των ακέραιων αλγεβρικών αριθμών. Ο πρώτος στόχος θα είναι να δείξουμε ότι το $\mathbb{B}$ είναι υποδακτύλιος των αλγεβρικών αριθμών $\mathbb{A}$. Για να γίνει αυτό πρώτα δείχνουμε το ακόλουθο λήμμα.

Λήμμα 1.1 *Ένας μιγαδικός αριθμός u είναι ακέραιος αλγεβρικός, αν και μόνο αν η προσθετική ομάδα που γεννάται από όλες τις δυνάμεις $1, u, u^2, ...$ είναι πεπερασμένα παραγόμενη.*

Απόδειξη. Έστω πρώτα ότι ο αριθμός u είναι ακέραιος αλγεβρικός. Τότε σύμφωνα με τον ορισμό που δώσαμε θα είναι

$$u^n + a_{n-1}u^{n-1} + ... + a_0 = 0, a_i \in \mathbb{Z}. \tag{1.1}$$

Ισχυριζόμαστε ότι κάθε δύναμη του u βρίσκεται μέσα στην προσθετική ομάδα που παράγεται από τα $1, u, u^2, ..., u^{n-1}$. Θα συμβολίζουμε αυτήν την ομάδα, Γ. Από την σχέση 1.1, βλέπουμε ότι $u^n \in \Gamma$. Επαγωγικά, αν έχουμε $m \geq n$ και $u^m \in \Gamma$, θα είναι

$$u^{m+1} = u^{m+1-n}u^n = u^{m+1-n}(-a_{n-1}u^{n-1} - ... - a_0) \in \Gamma.$$

Δηλαδή κάθε δύναμη του u βρίσκεται μέσα στην Γ. Τώρα για το αντίστροφο. Υποθέτουμε ότι κάθε δύναμη του u ζει μέσα σε μία πεπερασμένα παραγόμενη προσθετική ομάδα G. Η υποομάδα $\Gamma \leq G$ που παράγεται από τις δυνάμεις $1, u, u^2, ..., u^n$ πρέπει και αυτή να είναι πεπερασμένα παραγόμενη. Οπότε θα θεωρήσουμε ότι η ομάδα Γ έχει γεννήτορες $v_1, v_2, ..., v_n$. Βλέπουμε αυτά τα v_i, σαν πολυώνυμα του

u, με ακέραιους συντελεστές. Επομένως και το uv_i θα είναι πολυώνυμο. Έτσι υπάρχουν ακέραιοι αριθμοί b_{ij} τέτοιοι ώστε

$$uv_i = \sum_{j=1}^{n} b_{ij} v_i.$$

Η παραπάνω σχέση μας οδηγεί σε ένα σύστημα ομογενών εξισώσεων για το v_i, που έχει την εξής μορφή.

$$(b_{11} - u)v_1 + b_{12}v_2 + ... + b_{1n}v_n = 0$$

$$b_{21}v_1 + (b_{22} - u)v_2 + ... + b_{2n}v_n = 0$$

$$.....$$

$$b_{n1}v_1 + ... + (b_{nn} - u)v_n = 0.$$

Από την στιγμή που υπάρχει λύση $v_1, ..., u_n \in \mathbb{C}$, οδηγούμαστε στο συμπέρασμα ότι η διακρίνουσα που σχηματίζουν οι συντελεστές των v_i στο παραπάνω σύστημα είναι ίση με μηδέν. Αν την ανοίξουμε, καταλήγουμε σε ένα πολυώνυμο μονικό, με ακέραιους συντελεστές που ικανοποιεί το u. Έτσι ο u θα είναι ακέραιος αλγεβρικός αριθμός.

Θεώρημα 1.7 *Οι ακέραιοι αλγεβρικοί αριθμοί σχηματίζουν υποδακτύλιο του σώματος των αλγεβρικών αριθμών.*

Απόδειξη. Έστω $l, m \in \mathbb{B}$. Πρέπει να δείξουμε ότι $l + m \in \mathbb{B}$ και ότι $lm \in \mathbb{B}$. Από το λήμμα 1.1, ξέρουμε ότι όλες οι δυνάμεις του l ζουν σε μία πεπερασμένα παραγόμενη προσθετική υποομάδα $\Gamma_l \leq \mathbb{C}$ και ότι όλες οι δυνάμεις του m ζουν σε μία πεπερασμένα παραγόμενη προσθετική υποομάδα $\Gamma_m \leq \mathbb{C}$. Επομένως, οι δυνάμεις των $l+m, lm$ είναι ακέραιοι γραμμικοί συνδυασμοί στοιχείων της μορφής $l^i m^j$, τα οποία ζουν μέσα στην $\Gamma_l\Gamma_m \subseteq \mathbb{C}$. Αν πούμε ότι η Γ_l έχει γεννήτορες $v_1, ..., v_n$ και η Γ_m τα $w_1, ..., w_s$, τότε η $\Gamma_l\Gamma_m$ είναι η προσθετική ομάδα που παράγεται από όλα τα $u_i w_j$ με $1 \leq i \leq n, 1 \leq j \leq s$. Επομένως όλες οι δυνάμεις του $l + m$ και του lm ζουν σε μία πεπερασμένα παραγόμενη υποομάδα του $\mathbb{C}$ και έτσι σύμφωνα με το λήμμα 1.1, τα $l + m$ και lm είναι ακέραιοι αλγεβρικοί αριθμοί.

Ακολουθώντας περίπου την ίδια τακτική με την προηγούμενη απόδειξη, θα δείξουμε το επόμενο θεώρημα.

Θεώρημα 1.8 *Έστω u ένας μιγαδικός αριθμός ο οποίος ικανοποιεί ένα μονικό πολυώνυμο, με συντελεστές ακέραιους αλγεβρικούς αριθμούς. Τότε ο u είναι ακέραιος αλγεβρικός.*

Απόδειξη. Υποθέτουμε ότι

$$u^n + y_{n-1}u^{n-1} + ... + y_0 = 0,$$

με τα $y_i \in \mathbb{B}$. Αυτά τα y_i γεννούν έναν υποδακτύλιο Y του $\mathbb{B}$. Από το λήμμα 1.1, ξέρουμε ότι όλες οι δυνάμεις του u ζουν σε ένα πεπερασμένα παραγόμενο Y-submodule M του $\mathbb{C}$, το οποίο γεννάται από τα $1, u, ..., u^{n-1}$. Από το θεώρημα 1.7, τα y_i και οι δυνάμεις τους ζουν σε μία πεπερασμένα παραγόμενη προσθετική ομάδα Γ_i. Έστω ότι αυτή έχει γεννήτορες g_{ij}, με $1 \leq j \leq n_i$. Επομένως το M ζει μέσα στην προσθετική ομάδα που παράγεται από όλα τα στοιχεία

$$g_{ij_1}, g_{2j_2}...g_{n-1,j_{n-1}}u^k, 1 \leq j_i \leq n_i, 0 \leq k \leq n-1,$$

το οποίο είναι πεπερασμένο σύνολο. Άρα και το M είναι πεπερασμένα παραγόμενο σαν προσθετική ομάδα. Σύμφωνα με το λήμμα 1.1, ο u είναι ακέραιος αλγεβρικός αριθμός.

Η χρησιμότητα των δύο τελευταίων θεωρημάτων που αποδείξαμε, είναι ότι μπορούμε να κατασκευάσουμε ακέραιους αλγεβρικούς αριθμούς από άλλους γνωστούς αριθμούς. Ας δούμε ένα παράδειγμα. Ξέρουμε ότι οι αριθμοί $\sqrt{5}$ και $\sqrt{7}$ είναι ακέραιοι αλγεβρικοί. Σύμφωνα τώρα με το θεώρημα 1.7, ακέραιοι αλγεβρικοί θα είναι και οι αριθμοί $\sqrt{5}+\sqrt{7}, 5\sqrt{5}+57\sqrt{7}, \sqrt{5}^5(1+\sqrt{7})^2$. Επίσης σύμφωνα με το θεώρημα 1.8, οι ρίζες ενός μονικού πολυωνύμου το οποίο έχει συντελεστές τους παραπάνω αριθμούς, θα είναι και αυτές ακέραιοι αλγεβρικοί αριθμοί. Συνεχίζουμε με τον ορισμό του δακτυλίου ακεραίων ενός σώματος αριθμών.

Ορισμός 1.8 *Για κάθε σώμα αριθμών K είναι $\mathfrak{D} = K \cap \mathbb{B}$, και ονομάζουμε το $\mathfrak{D}$ δακτύλιο των αλγεβρικών ακεραίων του K. Ο συμβολισμός που θα χρησιμοποιούμε θα είναι $\mathfrak{D}_K$, ή όταν είναι φανερό για ποιο σώμα μιλάμε, απλά θα γράφουμε $\mathfrak{D}$. Επίσης αφού τα $K, \mathbb{B}$ είναι υποδακτύλιοι του $\mathbb{C}$, το $\mathfrak{D}$ είναι υποδακτύλιος του K. Επιπλέον θα έχουμε $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ και $\mathbb{Z} \subseteq \mathbb{B}$, άρα $\mathbb{Z} \subseteq \mathfrak{D}$.*

Λήμμα 1.2 *Αν K είναι ένα σώμα αριθμών και $a \in K$, τότε για κάποιο $c \neq 0, c \in \mathbb{Z}$ θα έχουμε $ca \in \mathfrak{D}$.*

Απόδειξη. Η απόδειξη αυτού του λήμματος είναι τετριμμένη και απλά θα το χρησιμοποιήσουμε για να δείξουμε το ακόλουθο πόρισμα.

Πόρισμα 1.2 *Αν έχουμε K ένα σώμα αριθμών, τότε $K = \mathbb{Q}(u)$, για u κάποιον ακέραιο αλγεβρικό αριθμό.*

Απόδειξη. Όπως έχουμε δείξει στο θεώρημα 1.2, για κάποιον $b \in \mathbb{A}$ θα είναι $K = \mathbb{Q}(b)$. Από το λήμμα 1.2 θα ισχύει ότι $u = cb,\ c \in \mathbb{Z},\ c \neq 0$. Επομένως, είναι πλέον προφανές ότι $\mathbb{Q}(b) = \mathbb{Q}(u)$.

Για την απόδειξη του επόμενου λήμματος θα διατυπώσουμε το παρακάτω λήμμα που το οφείλουμε στον Gauss.

Λήμμα 1.3 *Έστω πολυώνυμο $p \in \mathbb{Z}[t]$ και έστω ότι $p = gh, g, h \in \mathbb{Q}[t]$. Τότε υπάρχει $\lambda \in \mathbb{Q}$ για τον οποίο θα έχουμε $\lambda g, \lambda^{-1}h \in \mathbb{Z}[t]$.*

Απόδειξη. Βλέπε λήμμα 1.4 από [1].

Λήμμα 1.4 *Ένας αλγεβρικός αριθμός a είναι ακέραιος αλγεβρικός, αν και μόνο αν το ελάχιστο πολυώνυμό του πάνω από το $\mathbb{Q}$, έχει ακεραίους συντελεστές.*

Απόδειξη. Έστω p το ελάχιστο πολυώνυμο του a πάνω από το $\mathbb{Q}$. Αυτό είναι μονικό και ανάγωγο στο $\mathbb{Q}[t]$. Αν το p ανήκει στο $\mathbb{Z}[t]$, τότε εξ ορισμού ο a είναι ακέραιος αλγεβρικός. Αντίστροφα, έστω a ακέραιος αλγεβρικός. Τότε για κάποιο μονικό πολυώνυμο $q(t) \in \mathbb{Z}[t]$ θα είναι $q(a) = 0$ και επίσης $p \mid q$. Κάποιο ρητό πολλαπλάσιο λp υπάρχει στο $\mathbb{Z}[t]$ το οποίο διαιρεί το q. Και επειδή τα δύο αυτά πολυώνυμα είναι μονικά θα έχουμε ότι $\lambda = 1$, επομένως σύμφωνα με το λήμμα 1.4, $p(t) \in \mathbb{Z}[t]$.

Λήμμα 1.5 *Ένας ακέραιος αλγεβρικός αριθμός θα είναι ρητός, αν και μόνο αν είναι ακέραιος αριθμός. Δηλαδή $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$.*

Απόδειξη. Ο εγκλεισμός $\mathbb{Z} \subseteq \mathbb{B} \cap \mathbb{Q}$ είναι προφανής. Έστω τώρα κάποιο $a \in \mathbb{B} \cap \mathbb{Q}$. Έχουμε ότι $a \in \mathbb{Q}$, άρα το ελάχιστο πολυώνυμό του πάνω από το $\mathbb{Q}$ θα είναι το $t-a$. Αφού είναι και ακέραιος αλγεβρικός, από το λήμμα 1.5, πρέπει οι συντελεστές του να ανήκουν στο $\mathbb{Z}$. Δηλαδή $-a \in \mathbb{Z}$ που προφανώς σημαίνει ότι $a \in \mathbb{Z}$.

1.4 Βάσεις ακεραιότητας

Έστω ότι έχουμε ένα σώμα αριθμών K, με βαθμό n πάνω από το $\mathbb{Q}$. Ξέρουμε ότι $K = \mathbb{Q}(u)$, όπου u ένας ακέραιος αλγεβρικός. Τότε το ελάχιστο πολυώνυμο p του u, έχει βαθμό n και μία βάση του K είναι η $\{1, u, u^2, ..., u^{n-1}\}$. Ο δακτύλιος ακεραίων $\mathfrak{D}$, του K, είναι αβελιανή ομάδα με πράξη την πρόσθεση (όλα αυτά θα αποδειχτούν στη συνέχεια). Η $\{a_1, ..., a_s\}$ είναι βάση ακεραιότητας, αν και μόνο αν όλα τα $a_i \in \mathfrak{D}$ και όλα τα στοιχεία του $\mathfrak{D}$ γράφονται μοναδικά στη μορφή $b_1a_1+...+b_sa_s, b_i \in \mathbb{Z}$. Στη συνέχεια θα δείξουμε ότι όντος βάση ακεραιότητας υπάρχει για κάθε δακτύλιο ακεραίων, αλλά δεν είναι αυτή που βιαστικά θα υποθέταμε. Δηλαδή για ένα $K = \mathbb{Q}(u)$ με u ακέραιο αλγεβρικό, μία $\mathbb{Q}$-βάση είναι η $\{1, u, u^2, ..., u^{n-1}\}$ αλλά δεν σημαίνει απαραίτητα ότι αυτή είναι και η βάση ακεραιότητας του K. Αν πάρουμε σαν παράδειγμα το $K = \mathbb{Q}(\sqrt{5})$ και το στοιχείο αυτού $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ το οποίο ικανοποιεί την εξίσωση $t^2 - t + 1 = 0$, βλέπουμε ότι ενώ είναι άλγεβρικός ακέραιος, δεν ανήκει στο $\mathbb{Z}[\sqrt{5}]$. Προχωρούμε τώρα σιγά σιγά να τα αποδείξουμε όλα αυτά και να τα δούμε στην πράξη.

Λήμμα 1.6 *Έστω K σώμα αριθμών και $\{a_1, ...a_n\}$ μία βάση του που αποτελείται από ακέραιους αλγεβρικούς. Τότε η διακρίνουσα $\Delta[a_1, ..., a_n]$ είναι ακέραιος αριθμός, διάφορος του μηδενός.*

Απόδειξη. Σύμφωνα με το θεώρημα 1.6 ξέρουμε ότι η Δ είναι ρητός αριθμός. Είναι και ακέραιος αλγεβρικός αφού είναι $a \in \mathbb{B}$. Επομένως, από το λήμμα 1.5 θα πάρουμε ότι είναι ακέραιος. Τέλος, το ότι δεν είναι μηδέν μας το εξασφαλίζει πάλι το θεώρημα 1.6.

Θεώρημα 1.9 *Κάθε δακτύλιος $\mathfrak{D}$, ενός σώματος αριθμών K, έχει βάση ακεραιότητας και η προσθετική ομάδα του $\mathfrak{D}$ είναι ελεύθερη αβελιανή, τάξης n, ίση με το βαθμό του K.*

Απόδειξη. Έστω u ακέραιος αλγεβρικός και $K = \mathbb{Q}(u)$. Υπάρχει μία βάση του K, έστω η $\{1, u, ..., u^{n-1}\}$, η οποία αποτελείται από ακέραιους αλγεβρικούς, αλλά χωρίς να είναι απαραίτητα βάση ακεραιότητας. Από το λήμμα 1.5, έχουμε ότι $\Delta[1, ..., u^{n-1}] \in \mathbb{Z}^*$. Επομένως, επιλέγουμε μία βάση που αποτελείται από ακέραιους αλγεβρικούς $\{\omega_1, ..., \omega_n\}$ και για την οποία να ισχύει ότι η $|\Delta[\omega_1, ..., \omega_n]|$, να είναι η ελάχιστη δυνατή. Ισχυριζόμαστε ότι αυτή είναι μία βάση ακεραιότητας. Έστω ότι δεν είναι. Τότε θα υπάρχει κάποιος αλγεβρικός ακέραιος $\omega \in \mathbb{Q}(u)$, ο οποίος γράφεται $\omega = a_1\omega_1 + ... + a_n\omega_n$ με τα $a_i \in \mathbb{Q}$ και κάποια από αυτά τα x_i, όχι απαραίτητα όλα, να είναι ακέραιοι. Έστω ότι $a_1 \notin \mathbb{Z}$. Τότε θα είναι

$$a_1 = a + r, a \in \mathbb{Z}, 0 < r < 1.$$

Θέτουμε

$$y_1 = \omega - a\omega_1, y_i = \omega_i, i = 2, ..., n.$$

Και τώρα η $\{y_1, ..., y_n\}$, είναι μία βάση που αποτελείται από ακέραιους αλγεβρικούς. Η ορίζουσα που είναι σχετική με την αλλαγή βάσης από τα ω στα y, είναι η

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & ... & a_n \\ 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ .. & .. & .. & .. & .. \\ 0 & 0 & 0 & ... & 1 \end{vmatrix} = r.$$

Επομένως θα έχουμε

$$\Delta[y_1, ..., y_n] = r^2 \Delta[\omega_1, ..., \omega_n].$$

Από την στιγμή που έχουμε υποθέσει ότι για το r ισχύει $0 < r < 1$, φτάνουμε σε αντίθεση σε ότι αφορά την επιλογή μας για τη $\{\omega_1, ..., \omega_n\}$, ότι η $|\Delta[\omega_1, ..., \omega_n]|$ είναι ελάχιστη. Επομένως ο ισχυρισμός μας ήταν σωστός, δηλαδή η βάση $\{\omega_1, ..., \omega_n\}$ είναι βάση ακεραιότητας. Οπότε η $(\mathfrak{D}, +)$ είναι ελεύθερη αβελιανή ομάδα, τάξης n.

Μετά την απόδειξη αυτού του θεωρήματος φτάνουμε στο ερώτημα της εύρεσης βάσης ακεραιότητας, για περιπτώσεις όπως αυτή του $\mathbb{Q}(\sqrt{5})$, όπου βάση ακεραιότητας δεν είναι η $\mathbb{Q}$-βάση $\{1, \sqrt{5}\}$. Έστω ένα στοιχείο το οποίο να ανήκει στο $\mathbb{Q}(\sqrt{5})$. Αυτό θα έχει μορφή $p + q\sqrt{5},\ p, q \in \mathbb{Q}$. Αυτό το στοιχείο έχει ελάχιστο πολυώνυμο

$$t = p + q^2 \Leftrightarrow t^2 - 2pt + p^2 = 5q^2 \Leftrightarrow t^2 - 2pt + (p^2 - 5q^2).$$

Ο αριθμός $p + q\sqrt{5}$ θα είναι ακέραιος αλγεβρικός, αν και μόνο αν οι συντελεστές αυτού του πολυωνύμου είναι ακέραιοι αριθμοί. Δηλαδή $p, p^2 - 5q^2 \in \mathbb{Z}$. Επομένως $p = 1/2P,\ P \in \mathbb{Z}$. Για P άρτιο, έχουμε ότι ο p^2 είναι ακέραιος, που σημαίνει ότι και ο $5q^2$ είναι ακέραιος, που κάνει τον q να είναι ακέραιο επίσης. Αν ο P είναι περιττός αριθμός, βρίσκουμε ότι $q = 1/2Q$, όπου Q είναι επίσης περιττός ακέραιος. Επομένως βλέπουμε ότι ο δακτύλιος ακεραίων είναι ο $\mathfrak{D} = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{5}]$ και η βάση ακεραιότητας είναι η $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$.

Λήμμα 1.7 *Έστω G ελεύθερη αβελιανή ομάδα τάξης n, με βάση $\{a_1, ..., a_n\}$. Έστω ότι έχουμε τον πίνακα (b_{ij}) με $b_{ij} \in \mathbb{Z}$. Τότε τα στοιχεία*

$$y_i = \sum_i b_{ij} a_j$$

αποτελούν μία βάση για την G, αν και μόνο αν ο (b_{ij}) είναι unimodular.

Απόδειξη. Τα y_i αποτελούν βάση για την G. Άρα και τα a_i γράφονται σαν γραμμικοί συνδυασμοί των y_i. Είναι

$$a_i = \sum_j c_{ij} y_j.$$

Αν (c_{ij}) ο πίνακας των στοιχείων c_{ij}, παρατηρούμε ότι $(b_{ij})(c_{ij}) = I_d$, έτσι οι πίνακες αυτοί θα είναι αντιστρέψιμοι και θα πρέπει να έχουν αντιστρέψιμη ορίζουσα στο $\mathbb{Z}$, δηλαδή $det\ (b_{ij}) = \pm 1$.

Θεώρημα 1.10 *Έστω ότι $\{a_1, ..., a_n\}$ είναι μία $\mathbb{Q}$-βάση για ένα σώμα αριθμών K. Αν η διακρίνουσα $\Delta[a_1, ..., a_n]$ είναι αριθμός ελεύθερος τετραγώνων, τότε η $\{a_1, ..., a_n\}$ θα είναι βάση ακεραιότητας.*

Απόδειξη. Έστω μία βάση ακεραιότητας $\{b_1, ..., b_n\}$. Τότε θα ισχύει

$$\Delta[a_1, ..., a_n] = (detc_{ij})^2 \Delta[b_1 ..., b_n].$$

Αφού η $\Delta[a_1, ..., a_n]$ είναι αριθμός ελεύθερος τετραγώνων από την υπόθεση, θα πρέπει η ορίζουσα $detc_{ij} = \pm 1$, δηλαδή ο πίνακας b_{ij} να είναι unimodular. Επομένως από το λήμμα 1.7 η βάση $\{a_1, ..., a_n\}$ θα είναι βάση ακεραιότητας.

Παράδειγμα 1.3 *Έστω ότι έχουμε το προηγούμενο παράδειγμα, δηλαδή* $K = \mathbb{Q}(\sqrt{5})$. *Έστω επίσης η* $\mathbb{Q}$*-βάση του* $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$. *Παίρνουμε τους δύο μονομορφισμούς* $\sigma_i : \mathbb{Q}(\sqrt{5}) \to \mathbb{C}, i = 1, 2$. *Είναι:*

$$\sigma_1(p + q\sqrt{5}) = p + q\sqrt{5}$$

$$\sigma_2(p + q\sqrt{5}) = p - q\sqrt{5},$$

για $p, q \in \mathbb{Q}$. *Επομένως η διακρίνουσα αυτής της βάσης θα είναι*

$$\Delta[1, \frac{1}{2} + \frac{1}{2}\sqrt{5}] = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{5} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{5} \end{vmatrix}^2 = 5.$$

Όπου το 5 είναι αριθμός ελεύθερος τετραγώνων, επομένως σύμφωνα με το θεώρημα 1.10 η βάση $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$, *είναι βάση ακεραιότητας.*

Παρατήρηση: Βλέπουμε ότι το αντίστροφο του θεωρήματος 1.10 δεν ισχύει σε αυτήν την περίπτωση.

1.5 Νόρμα και ίχνος

Σε αυτή την παράγραφο θα ασχοληθούμε με τη νόρμα και το ίχνος ενός στοιχείου $a \in K$. Ξεκινάμε δίνοντας τους ορισμούς.

Ορισμός 1.9 *Για κάθε* $a \in K$ *ορίζουμε νόρμα να είναι η*

$$N(a) = \prod_{i=1}^{n} \sigma_i(a)$$

και ίχνος

$$T(a) = \sum_{i=1}^{n} \sigma_i(a).$$

Ξέρουμε ότι το πολυώνυμο σώματος είναι μία δύναμη του ελάχιστου πολυωνύμου του a. Επομένως, και σύμφωνα με αυτά που έχουμε πει ως τώρα, ο a θα είναι ακέραιος αλγεβρικός, αν και μόνο αν το πολυώνυμο σώματός του, έχει συντελεστές ακέραιους αριθμούς. Αφού το πολυώνυμο σώματος είναι

$$f_a(t) = \prod_{i=1}^{n} (t - \sigma_i(a)),$$

θα έχουμε ότι αν ο a είναι ακέραιος αλγεβρικός, τότε η νόρμα του και το ίχνος του θα είναι ακέραιοι αριθμοί. Είναι επίσης προφανές, ότι αφού οι σ_i είναι μονομορφισμοί έχουμε, $N(ab) = N(a)N(b), a, b \in K$ και ότι αν $a \neq 0$ τότε $N(a) \neq 0$.

Πρόταση 1.1 *Έστω* $K = \mathbb{Q}(u)$ *ένα σώμα αριθμών και το* u *να έχει ελάχιστο πολυώνυμο* p, $\deg p = n$. *Τότε η* $\mathbb{Q}$*-βάση* $\{1, u, ..., u^{n-1}\}$ *έχει διακρίνουσα* $\Delta[1, u, ..., u^{n-1}] = (-1)^{n(n-1)/2} N(Dp(u))$, *όπου* Dp *είναι η παράγωγος του* p.

Απόδειξη. Όπως έχουμε δει στην απόδειξη του θεωρήματος 1.6, είναι

$$\Delta = \Delta[1, u, ..., u^{n-1}] = \prod_{1 \le i < j \le n} (u_i - u_j)^2,$$

όπου $u_1, ..., u_{n-1}$ είναι τα συζυγή του u. Έχουμε

$$p(t) = \prod_{i=1}^{n} (t - u_i),$$

$$Dp(t) = \sum_{j=1}^{n} \prod_{i=1, i \ne j}^{n} (t - u_i)$$

επομένως

$$Dp(u_j) = \prod_{i,j=1, i \ne j}^{n} (u_i - u_j).$$

Πολλαπλασιάζουμε τώρα όλες αυτές τις εξισώσεις για $j = 1, ..., n$ και παίρνουμε

$$\prod_{j=1}^{n} Dp(u_j) = \prod_{i,j=1, i \ne j}^{n} (u_j - u_i).$$

Το αριστερό μέλος της εξίσωσης είναι η $N(Dp(u_j))$. Για το δεξί μέλος έχουμε τον παράγοντα $u_i - u_j$ να εμφανίζεται δύο φορές, μία σαν $u_i - u_j$ και μία σαν $u_j - u_i$. Το γινόμενο δύο τέτοιων παραγόντων είναι $-(u_i - u_j)^2$. Όπως είπαμε πιο πριν στην απόδειξη, αυτό είναι η διακρίνουσα πολλαπλασιασμένη με $(-1)^s$ όπου s είναι το πλήθος των ζευγών (i, j) το οποίο είναι $s = \frac{1}{2}n(n-1)$. Καταλήξαμε λοιπόν στο ζητούμενο

$$\Delta[1, u, ..., u^{n-1}] = (-1)^{n(n-1)/2} N(Dp(u)).$$

1.6 Δακτύλιοι ακεραίων

Σε αυτήν την παράγραφο θα δούμε τον τρόπο με τον οποίο θα βρίσκουμε δακτύλιους ακεραίων, για ένα σώμα αριθμών. Αυτό απαιτεί αρκετές πράξεις, αλλά με διάφορες τεχνικές θα τις μειώσουμε όσο μπορούμε περισσότερο. Επίσης θα δούμε ότι δεν έχουν όλα τα σώματα αριθμών βάση ακεραιότητας της μορφής $\{1, u, ..., u^{n-1}\}$.

Θεώρημα 1.11 *Κάθε υποομάδα H μιας ελεύθερης αβελιανής ομάδας G τάξης n, είναι και αυτή ελεύθερη και έχει τάξη $s \le n$. Επιπλέον υπάρχει μία βάση $b_1, ..., b_n$ της G και θετικοί ακέραιοι αριθμοί $a_1, ..., a_n$, τέτοιοι ώστε η $a_1 b_1, ..., a_n b_n$ να είναι μία βάση για την H.*

Απόδειξη. Βλέπε θεώρημα 1.12 [1].

Θεώρημα 1.12 *Έστω G μία προσθετική υποομάδα του $\mathfrak{D}$, τάξης όσο ο βαθμός του K, με βάση ακεραιότητας $\{a_1, ..., a_n\}$. Τότε η τάξη $|\mathfrak{D}/G|$ διαιρεί την $\Delta[a_1, ..., a_n]$.*

Απόδειξη. Σύμφωνα με το θεώρημα 1.11 θα υπάρχει μία βάση ακεραιότητας $\{b_1, ..., b_n\}$ για το $\mathfrak{D}$, τέτοια ώστε η υποομάδα της G να έχει βάση ακεραιότητας $\{m_1 b_1, ..., m_n b_n\}$, για κατάλληλα $m_i \in \mathbb{Z}$. Αφού κάθε αλλαγή βάσης έχει unimodular πίνακα, θα ισχύει ότι $\Delta[a_1, ..., a_n] = \Delta[m_1 b_1, ..., m_n b_n]$. Είναι

$$\Delta[m_1 b_1, ..., m_n b_n] = (m_1 ... m_n)^2 \Delta[b_1, ..., b_n] = (m_1 ... m_n)^2 \Delta,$$

όπου Δ είναι η διακρίνουσα του K δηλαδή ακέραιος αριθμός. Έχουμε όμως και ότι $|m_1 ... m_n| = |\mathfrak{D}/G|$. Επομένως η $|\mathfrak{D}/G|$ διαιρεί την $\Delta[a_1, ..., a_n]$.

Προχωρούμε με μία πρόταση η οποία ουσιαστικά είναι μία γενίκευση του προηγούμενου θεωρήματος.

Πρόταση 1.2 *Έστω ότι $\mathfrak{D} \neq G$. Τότε υπάρχει ακέραιος αλγεβρικός αριθμός της μορφής*

$$\frac{1}{p}(l_1 a_1 + ... + l_n a_n)$$

όπου $0 \leq l_i \leq p-1,\ l_i \in \mathbb{Z}$ και p είναι πρώτος αριθμός, τέτοιος ώστε το p^2 να διαιρεί Δ_G.

Απόδειξη. Αφού $G \neq \mathfrak{D}$ τότε $|\mathfrak{D}/G| > 1$. Τότε από τη θεωρία των πεπερασμένων αβελιανών ομάδων, θα υπάρχει ένας p πρώτος ο οποίος θα διαιρεί το $|\mathfrak{D}/G|$ και ένα στοιχείο $u \in \mathfrak{D}/G$ τέτοιο ώστε $g = pu \in G$. Από το θεώρημα 1.12, έχουμε ότι p^2 διαιρεί την Δ_G. Επιπλέον,

$$u = \frac{1}{p} g = \frac{1}{p}(l_1 a_1 + ... + l_n a_n),$$

αφού τα $\{a_i\}$ αποτελούν βάση ακεραιότητας για την G.

Με την χρήση αυτής της πρότασης, είμαστε πλέον έτοιμοι να περιγράψουμε μία διαδικασία με την οποία θα βρίσκουμε ακέραιους αλγεβρικούς. Αρχικά προφανώς αφού υπολογίσουμε την Δ_G και την βρούμε να είναι ελεύθερη τετραγώνων δεν θα υπάρχει τέτοιος αριθμός p οπότε $G = \mathfrak{D}$. Αλλιώς κάνουμε τα εξής βήματα.

1. Παίρνουμε την προφανή επιλογή για την G.
2. Υπολογίζουμε την Δ_G.
3. Για κάθε πρώτο αριθμό του οποίου το τετράγωνο διαιρεί την Δ_G, δοκιμάζουμε όλους τους αριθμούς της μορφής $\frac{1}{p}(l_1 a_1 + ... + l_n a_n)$, για να δούμε ποιοι είναι ακέραιοι αλγεβρικοί.
4. Αν προκύψει κάποιος ακέραιος αλγεβρικός, μεγαλώνουμε την G στην G', προσθέτοντας μέσα της τον νέο αριθμό.
5. Επαναλαμβάνουμε αυτήν την διαδικασία, μέχρι να μην μπορούμε πλέον να βρούμε νέους ακέραιους αλγεβρικούς αριθμούς.

Ας δούμε τώρα διεξοδικά ένα παράδειγμα, το οποίο θα είναι αρκετά διαφωτιστικό και θα αναδείξει όλα όσα έχουμε πει μέχρι τώρα.

Παράδειγμα 1.4 *Η δουλειά μας θα είναι να βρούμε όλους τους ακέραιους αλγεβρικούς του $\mathbb{Q}(\sqrt[3]{5})$. Έστω $u \in \mathbb{R}, u^3 = 5$. Η πρώτη και πολύ λογική επιλογή μας για την βάση ακεραιότητας του δακτυλίου ακεραίων, είναι η $\{1, u, u^2\}$. Έστω G*

η ομάδα που παράγεται από αυτήν τη βάση και $\omega = e^{2\pi i/3}$, *μία κυβική ρίζα της μονάδας. Οι μονομορφισμοί* $\sigma_i : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{C},\ i = 1, ..3$ *είναι οι:*

$$\sigma_1(u) = u, \sigma_2(u) = \omega u, \sigma_3(u) = \omega^2 u.$$

Επομένως με σκοπό να σχηματίσουμε και να υπολογίσουμε την ορίζουσα Δ_G, *θα έχουμε*

$$\sigma_1(1) = 1, \sigma_1(u) = u, \sigma_1(u^2) = u^2$$
$$\sigma_2(1) = 1, \sigma_2(u) = \omega u, \sigma_2(u^2) = \omega^2 u^2$$
$$\sigma_3(1) = 1, \sigma_3(u) = \omega^2 u, \sigma_3(u^2) = \omega u^2,$$

αφού ξέρουμε και ότι $\omega^3 = 1$. *Υπολογίζουμε τώρα την ορίζουσα.*

$$\Delta_G = \begin{vmatrix} 1 & u & u^2 \\ 1 & \omega u & \omega^2 u^2 \\ 1 & \omega^2 u & \omega u^2 \end{vmatrix}^2 =$$

$$= u^6 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}^2 =$$

$$= u^6(\omega^2 - \omega - \omega + \omega^2 + \omega^2 - \omega)^2 = u^6(3\omega^2 - 3\omega)^2$$
$$= u^6 3^2(\omega^2 - \omega)^2 = 5^3 3^2(-3) = -3^3 5^2.$$

Σύμφωνα λοιπόν με την πρόταση 1.2, αν υπάρχει κάποιος ακέραιος αλγεβρικός αριθμός θα πρέπει να έχει μία από τις δύο μορφές :

1. $a = \frac{1}{3}(l_1 + l_2 u + l_3 u^2), 0 \leq l_i \leq 2$
2. $a = \frac{1}{5}(l_1 + l_2 u + l_3 u^2), 0 \leq l_i \leq 4$

Θα δούμε μόνο την περίπτωση όπου $p = 5$, *όπου με τη βοήθεια του ίχνους θα καταφέρουμε να μειώσουμε αισθητά τις πράξεις, τις οποίες δε θα αποφύγουμε στην περίπτωση του* $p = 3$. *Αρχικά αυτό που θα κάνουμε, είναι να υπολογίζουμε το ίχνος του υποψήφιου ακέραιου αλγεβρικού και να ισχυριστούμε ότι ανήκει στο* $\mathbb{Z}$. *Ξεκινάμε τον υπολογισμό αυτόν με τη σημαντική, για τη μείωση των πράξεων παρατήρηση*

$$\omega^3 = 1 \Leftrightarrow \omega^3 - 1 = 0 \Leftrightarrow (\omega - 1)(\omega^2 + \omega + 1) = 0 \Leftrightarrow \omega^2 + \omega + 1 = 0.$$

Είναι:

$$T(a) = T(\frac{1}{5}(l_1 + l_2 u + l_3 u^2)) = \frac{1}{5}(l_1 + l_2 u + l_3 u^2) + \frac{1}{5}(l_1 + \omega l_2 u + \omega^2 l_3 u^2)$$

$$+\frac{1}{5}(l_1 + \omega^2 l_2 u + \omega l_3 u^2) = \frac{3l_1}{5} + \frac{1}{5}l_2 u(1 + \omega + \omega^2) + \frac{1}{5}l_3 u^2(1 + \omega + \omega^2) = \frac{3l_1}{5}.$$

Πρέπει λοιπόν το ίχνος αυτού του αριθμού, αν είναι ακέραιος αλγεβρικός, να είναι ακέραιος αριθμός. Επομένως θα πρέπει να έχουμε $l_1 \in 5\mathbb{Z}$. *Τότε ο αριθμός* $a' = \frac{1}{5}(l_2 u + l_3 u^2)$, *πρέπει να είναι επίσης ακέραιος αλγεβρικός. Επόμενο βήμα είναι να υπολογίσουμε την νόρμα του* a'. *Είναι:*

$$N(l_2 u + l_3 u^2) = (l_2 u + l_3 u^2)(\omega l_2 u + \omega^2 l_3 u^2)(\omega^2 l_2 u + \omega l_3 u^2)$$

$$= \omega^3(l_2u + l_3u^2)(l_2u + \omega l_3u^2)(l_2u + \omega^2 l_3u^2)$$

$$= (l_2u)^3 + (l_3u^2)^3 + l_3l_2^2u^4(\omega^2 + \omega + 1) + (l_2l_3^2)u^5(\omega^2 + \omega + 1) = (l_2u)^3 + (l_3u^2)^3.$$

Έτσι, έχουμε ότι για να είναι ο a' ακέραιος αλγεβρικός, θα πρέπει η νόρμα του να είναι ακέραιος. Επομένως θα πρέπει

$$(l_2u)^3 + (l_3u^2)^3 = (5l_2^3 + 25l_3^3)/125 = (l_2^3 + 5l_3^3)/25.$$

Ένας τρόπος να δούμε αν αυτό ισχύει, είναι η χρήση της ωμής βίας. Να τσεκάρουμε δηλαδή για τα $l_2, l_3,\ 0 \le l_2, l_3 \le 4$, ποια παράσταση θα διαιρεί το 25. Είναι

l_2	l_3	$l_2^3 + 5l_3^3$	*διαιρείται από 25*
0	1	5	*όχι*
0	2	40	*όχι*
0	3	135	*όχι*
0	4	320	*όχι*
1	0	1	*όχι*
1	1	6	*όχι*
1	2	41	*όχι*
1	3	136	*όχι*
1	4	321	*όχι*
2	0	8	*όχι*
2	1	13	*όχι*
2	2	48	*όχι*
2	3	143	*όχι*
2	4	328	*όχι*
3	0	27	*όχι*
3	1	32	*όχι*
3	2	67	*όχι*
3	3	162	*όχι*
3	4	347	*όχι*
4	0	64	*όχι*
4	1	69	*όχι*
4	2	104	*όχι*
4	3	199	*όχι*
4	4	384	*όχι*

Με χρήση της ωμής βίας, δείξαμε ότι δεν υπάρχουν άλλοι ακέραιοι αλγεβρικοί αριθμοί. Τις πράξεις που κάναμε, σε κάποιες περιπτώσεις μπορούμε να τις αποφύγουμε με τεχνικές όπως η παρακάτω. Έστω $l_2^3 + 5l_3^3 \equiv 0 \bmod 25$. Αν είχαμε $l_2 \equiv 0 \bmod 5$ τότε θα είχαμε και $l_3 \equiv 0 \bmod 5$. Αλλιώς είναι $5 \equiv (-\frac{l_2}{l_3})^3 \bmod 25$. Επομένως το 5 είναι κυβικό υπόλοιπο $\bmod 25$. Εξ αιτίας του παράγοντα 5, θα πρέπει να είναι $5 \equiv (5k)^3 \bmod 25$. Το οποίο όμως σημαίνει ότι $5 \equiv 0 \bmod 25$, που φυσικά είναι άτοπο.

Παράδειγμα 1.5 *Σε αυτό το παράδειγμα θα προσπαθήσουμε να βρούμε τον δακτύλιο ακεραίων, $\mathfrak{D}$, του $K = \mathbb{Q}(\sqrt[3]{175})$. Έστω $t = \sqrt[3]{175} = \sqrt[3]{25 \cdot 7} = \sqrt[3]{5^2 \cdot 7}$ και $u = \sqrt[3]{5 \cdot 7^2} = \sqrt[3]{245}$. Υπολογίζουμε κάποιες ποσότητες οι οποίες θα μας φανούν χρήσιμες στη συνέχεια. Είναι*

$$ut = \sqrt[3]{5^2 \cdot 7}\sqrt[3]{5 \cdot 7^2} = \sqrt[3]{5^3 \cdot 7^3} = 35$$

$$u^2 = \sqrt[3]{5^2 \cdot 7^4} = 7t$$
$$t^2 = \sqrt[3]{5^4 \cdot 7^2} = 5u.$$

Έχουμε $u = 35/t$ *δηλαδή* $u \in \mathbb{Q}(\sqrt[3]{175})$. *Επίσης* $u^3 - 245 = 0$, *δηλαδή το* u *ικανοποιεί πολυώνυμο με ακέραιους συντελεστές, που σημαίνει ότι είναι ακέραιος αλγεβρικός αριθμός. Δηλαδή* $u \in \mathbb{B} \cap K = \mathfrak{D}$. *Ο* u *λοιπόν ανήκει στον δακτύλιο ακεραίων και έτσι θα πάρουμε σαν αρχική μας υπόθεση για την ομάδα* G, *την αβελιανή ομάδα που παράγεται από* $\{1, t, u\}$. *Όπως κάναμε και στο προηγούμενο παράδειγμα, θα υπολογίσουμε την* Δ_G. *Πάμε λοιπόν να βρούμε τους μονομορφισμούς* $\sigma_i : K \to \mathbb{C}, i = 1, ...3.$ *με* $\sigma_1(t) = t, \sigma_2(t) = \omega t, \sigma_3(t) = \omega^2 t$ *με* $\omega^3 = 1$. *Ας δούμε τι κάνουν αυτοί οι μονομορφισμοί το στοιχείο* u. *Είναι:*

$$\sigma_1(u) = \sigma_1(35/t) = 35\sigma_1(1/t) = 35/t = u$$

$$\sigma_2(u) = \sigma_2(35/t) = 35\sigma_2(1/t) = 35/\omega t = \frac{35\omega^{-1}}{t} = \frac{35\omega^2}{t} = \omega^2 u$$

$$\sigma_3(u) = \sigma_3(35/t) = \frac{35}{\omega^2 t} = \frac{u}{\omega^2} = \omega u.$$

Είμαστε πλέον σε θέση να δημιουργήσουμε την

$$\Delta[1, t, u] = \begin{vmatrix} 1 & t & u \\ 1 & \omega t & \omega^2 u \\ 1 & \omega^2 t & \omega u \end{vmatrix}$$
$$= 3^2 t^2 u^2 (\omega^2 - \omega)^2$$

και με την βοήθεια των σχέσεων που αποδείξαμε προηγουμένως

$$\Delta[1, t, u] = 3^2 5^2 7^2 (-3) = -3^3 5^2 7^2.$$

Οπότε σύμφωνα με την πρόταση 1.2, οι πιθανοί ακέραιοι αλγεβρικοί θα έχουν μία από τις εξής μορφές

$$a = \frac{1}{3}(l_1 + l_2 t + l_3 u),\ 0 \le l_i \le 2,$$

$$a = \frac{1}{5}(l_1 + l_2 t + l_3 u),\ 0 \le l_i, \le 4,$$

$$a = \frac{1}{7}(l_1 + l_2 t + l_3 u),\ 0 \le l_i \le 6.$$

1.7 Τετραγωνικά σώματα

Ορισμός 1.10 *Ορίζουμε τετραγωνικό σώμα αριθμών, ένα σώμα αριθμών* K, *με βαθμό 2 πάνω από το* $\mathbb{Q}$. *Αυτής της μορφής σώματα αριθμών είναι που θα απασχολήσουν πιο πολύ. Έτσι πιο κάτω θα δείξουμε πως θα βρίσκουμε τους δακτύλιους ακεραίων τέτοιων σωμάτων.*

Θα έχουμε λοιπόν, $K = \mathbb{Q}(u)$, με u έναν ακέραιο αλγεβρικό αριθμό και φυσικά ο u θα είναι ρίζα του πολυωνύμου $t^2 + at + b, a, b \in \mathbb{Z}$. Τότε

$$u = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Από την ανάλυση σε πρώτους αριθμούς στο $\mathbb{Z}$ θα έχουμε ότι $a^2-4b = r^2 d, r, d \in \mathbb{Z}$ και ο d είναι αριθμός ελεύθερος τετραγώνων. Επομένως

$$u = \frac{-1 \pm r\sqrt{d}}{2}$$

και βλέπουμε ότι $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{d})$, όπου d είναι ένας ακέραιος αριθμός, ελεύθερος τετραγώνων. Αυτή είναι ουσιαστικά και η απόδειξη της παρακάτω πρότασης.

Πρόταση 1.3 *Τα τετραγωνικά σώματα είναι της μορφής $\mathbb{Q}(\sqrt{d})$, όπου d ακέραιος ελεύθερος τετραγώνων.*

Τώρα θα δούμε αυτό που υποσχεθήκαμε πριν, δηλαδή να βρούμε τον δακτύλιο ακεραίων ενός τετραγωνικού σώματος αριθμών.

Θεώρημα 1.13 *Έστω $d \in \mathbb{Z}$ ακέραιος ελεύθερος τετραγώνων. Τότε οι αλγεβρικοί ακέραιοι του $\mathbb{Q}(\sqrt{d})$ είναι της μορφής*

1. $\mathbb{Z}[\sqrt{d}]$, *αν* $d \not\equiv 1 \bmod 4$
2. $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ *αν* $d \equiv 1 \bmod 4$

Απόδειξη. Έχουμε το τετραγωνικό σώμα αριθμών $\mathbb{Q}(\sqrt{d})$. Τα στοιχεία αυτού του σώματος είναι της μορφής $x = r + s\sqrt{d},\ r, s \in \mathbb{Q}$. Επομένως μπορούμε να γράψουμε $x = \frac{a+b\sqrt{d}}{c},\ a, b, c \in \mathbb{Z}$ και να μην υπάρχει πρώτος αριθμός, ο οποίος να διαιρεί και τους τρεις αυτούς αριθμούς. Ο x θα είναι ακέραιος αλγεβρικός, αν και μόνο αν οι συντελεστές του ελάχιστου πολυωνύμου

$$(t - (\frac{a+b\sqrt{d}}{c}))(t - (\frac{a-b\sqrt{d}}{c})) = t^2 - \frac{2a}{c}t + \frac{a^2 - b^2 d}{c^2},$$

είναι ακέραιοι. Δηλαδή

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z} \text{ και } \frac{2a}{c} \in \mathbb{Z}.$$

Αν οι c, a έχουν έναν κοινό πρώτο παράγοντα p, και αφού ο d είναι ελεύθερος τετραγώνων, θα έχουμε ότι ο p πρέπει να διαιρεί και τον b. Αυτό όμως είναι άτοπο από την αρχική μας υπόθεση. Επομένως $\frac{2a}{c} \in \mathbb{Z}$ και οι a, c δεν έχουν κοινό παράγοντα. Αναγκαστικά , $c = 1$, ή $c = 2$. Αν $c = 1$ τότε φανερά ο x είναι ακέραιος αλγεβρικός σε κάθε περίπτωση. Πάμε λοιπόν για την περίπτωση όπου $c = 2$. Λόγω της επιλογής που έχουμε κάνει, θα πρέπει οι a, b να είναι περιττοί αριθμοί και $\frac{a^2-b^2 d}{4} \in \mathbb{Z}$. Άρα $a^2 - b^2 d \equiv 0 \bmod 4$. Έστω ένας περιττός αριθμός $2k+1$. Το τετράγωνό του είναι $4k^2 + 4k + 1 \equiv 1 \bmod 4$. Άρα, θα έχουμε ότι αφού a, b περιττοί $a^2 \equiv b^2 \equiv 1 \bmod 4 \to d \equiv 1 \bmod 4$. Επομένως καταλήγουμε στο ότι αν

$$d \not\equiv 1 \bmod 4 \text{ η βάση ακεραιότητας είναι } \mathbb{Z}[\sqrt{d}],$$

ενώ αν

$$d \equiv 1 \bmod 4 \text{ η βάση ακεραιότητας είναι } \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}].$$

Οι μονομορφισμοί τώρα από το K στο $\mathbb{C}$ είναι οι

$$\sigma_1(r + s\sqrt{d}) = r + s\sqrt{d}$$

$$\sigma_2(r+s\sqrt{d}) = r - s\sqrt{d}$$

Επομένως θα μπορούμε πλέον πολύ εύκολα να υπολογίζουμε τις διακρίνουσες των τετραγωνικών σωμάτων, με τη απόδειξη του επόμενου θεωρήματος.

Θεώρημα 1.14

1. *Αν* $d \not\equiv 1 \bmod 4$ *τότε το* $\mathbb{Q}(\sqrt{d})$ *έχει βάση ακεραιότητας την* $\left\{1, \sqrt{d}\right\}$ *και διακρίνουσα* $4d$.
2. *Αν* $d \equiv 1 \bmod 4$ *τότε το* $\mathbb{Q}(\sqrt{d})$ *έχει βάση ακεραιότητας την* $\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\right\}$ *και διακρίνουσα* d.

Απόδειξη. Η απόδειξη είναι τετριμμένη, αλλά ας την δώσουμε σαν υπενθύμιση για τον υπολογισμό διακρινουσών. Θα έχουμε λοιπόν για την πρώτη περίπτωση

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = (-2\sqrt{d})^2 = 4d,$$

ενώ για την δεύτερη όπου η βάση μας είναι $\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\right\}$

$$\begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix} = (-\sqrt{d})^2 = d.$$

Παράδειγμα 1.6 *Ας δούμε τώρα ένα παράδειγμα το οποίο αναδεικνύει την σημασία του παραπάνω θεωρήματος. Για ιστορικούς λόγους να σημειώσουμε ότι είναι το πρώτο σώμα αριθμών που μελετήθηκε ποτέ. Έχουμε λοιπόν το σώμα του Gauss,* $\mathbb{Q}(\sqrt{-1})$. *Είναι* $d \not\equiv 1 \bmod 4$ *άρα και σύμφωνα με το παραπάνω θεώρημα, η βάση ακεραιότητας είναι η* $\mathbb{Z}[\sqrt{-1}]$ *και η διακρίνουσα ισούται με* $\Delta = 4d = -4$. *Να σημειώσουμε ότι σε αυτό το παράδειγμα βλέπουμε ότι δεν δουλεύει πάντα η αντίστροφη φορά του θεωρήματος 1.10, αφού το -4 δεν είναι αριθμός ελεύθερος τετραγώνων, αλλά έχουμε περίπτωση βάσης ακεραιότητας.*

Για μελλοντική χρήση να δώσουμε και την νόρμα και το ίχνος ενός στοιχείου που ανήκει σε τετραγωνικό σώμα,

$$N(r+s\sqrt{d}) = r^2 - ds^2$$

$$T(r+s\sqrt{d}) = 2r.$$

Θα κλείσουμε την παράγραφο αυτή τον ορισμό του μιγαδικού τετραγωνικού σώματος, όπου και με τέτοια θα ασχοληθούμε.

Ορισμός 1.11 *Θα καλούμε μιγαδικό τετραγωνικό σώμα αριθμών, ένα τετραγωνικό σώμα αριθμών με* d *αρνητικό αριθμό. Ενώ αν* d *θετικός, πραγματικό τετραγωνικό σώμα αριθμών.*

Κεφάλαιο 2

Ανάλυση σε ανάγωγα

2.1 Τετριμμένη ανάλυση

Σε αυτό το κεφάλαιο θα γενικεύσουμε την ανάλυση σε πρώτα στοιχεία στο $\mathbb{Z}$, σε ανάλυση μέσα σε ακέραιες περιοχές και πιο συγκεκριμένα, μέσα σε δακτυλίους ακεραίων $\mathfrak{D}$ τετραγωνικών σωμάτων αριθμών. Σε αυτές τις περιπτώσεις, αντίθετα από το $\mathbb{Z}$, δεν έχουμε πάντα μοναδική ανάλυση των στοιχείων και αυτό είναι που προκαλεί κάποια σύγχυση, αλλά και ενδιαφέρον. Ξεκινάμε με μία υπενθύμιση της έννοιας της μονάδας.

Ορισμός 2.1 *Καλούμε μονάδες u, σε έναν δακτύλιο R, τα στοιχεία εκείνα που έχουν πολλαπλασιαστικό αντίστροφο, δηλαδή αν u μονάδα θα υπάρχει u^{-1} τέτοιο ώστε $uu^{-1} = 1$.*

Ορισμός 2.2 *Ένα στοιχείο y θα ονομάζεται συνεταιρικό με ένα στοιχείο x, αν $x = uy$ με u μονάδα.*

Επίσης, να υπενθυμίσουμε ότι μία παραγοντοποίηση $x = yz$ καλείται κανονική, αν κανένα εκ των y, z δεν είναι μονάδες. Ενώ μη κανονική, ή τετριμμένη, όταν ο ένας παράγοντας είναι μονάδα και ο άλλος είναι συνεταιρικό στοιχείο με το x.

Πρόταση 2.1 *Οι μονάδες $U(R)$, ενός δακτυλίου P, σχηματίζουν ομάδα με τον πολλαπλασιασμό.*

Ας δούμε μερικά παραδείγματα.

Παράδειγμα 2.1

1. *$R = \mathbb{Q}$. Οι μονάδες είναι όλοι οι ρητοί, εκτός από το 0. Δηλαδή το $U(\mathbb{Q})$ είναι άπειρη ομάδα.*
2. *$R = \mathbb{Z}$. Οι μονάδες εδώ είναι τα ± 1. Φτιάχνουν μία κυκλική ομάδα τάξης 2.*
3. *$R = \mathbb{Z}[i]$. Δηλαδή τα στοιχεία της μορφής $a + bi, a, b \in \mathbb{Z}$, οι ακέραιοι του Gauss. Ένα στοιχείο $a + bi$ είναι μονάδα αν και μόνο αν υπάρχει στοιχείο $c + di, c, d \in \mathbb{Z}$, τέτοιο ώστε*

$$(a + bi)(c + di) = 1.$$

Αυτό μας οδηγεί στο ότι $ac - bd = 1, ad + bc = 0$ *και θα είναι*

$$c = \frac{a^2 + b^2}{a},\ d = -\frac{b}{a^2 + b^2}.$$

Εδώ θα έχουμε ακέραιες λύσεις μόνο αν $a^2 + b^2 = 1$. *Επομένως* $a = \pm 1, b = 0$ *ή* $a = 0, b = \pm 1$. *Δηλαδή οι μονάδες θα είναι* $\{1, -1, i, -i\}$. *Το* $U(R)$ *λοιπόν είναι κυκλική ομάδα τάξης 4.*

Θα χρησιμοποιήσουμε τώρα την έννοια της νόρμας, για να επεκτείνουμε τα αποτελέσματα του παραπάνω παραδείγματος.

Πρόταση 2.2 *Η ομάδα των μονάδων των δακτυλίων ακεραίων, σε ένα μιγαδικό τετραγωνικό σώμα αριθμών, είναι*

1. *Για* $d = -1, U = \{\pm 1, \pm i\}$.
2. *Για* $d = -3, U = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}, \omega = e^{2\pi i/3}$.
3. *Για όλες τις άλλες τιμές του* d, *είναι* $U = \{\pm 1\}$.

Απόδειξη. Έστω a μια μονάδα στον δακτύλιο ακεραίων $\mathbb{Q}(\sqrt{d})$, με αντίστροφο το b. Τότε είναι $a^{-1} = b \Leftrightarrow ab = 1 \Leftrightarrow N(a)N(b) = 1 \Leftrightarrow N(a) = \pm 1$, αφού η νόρμα ενός στοιχείου είναι φυσικός αριθμός. Αν έχουμε $a = x + y\sqrt{d},\ x, y \in \mathbb{Q}$, τότε $N(a) = N(x + y\sqrt{d}) = x^2 - dy^2 = 1$. Αν $x, y \in \mathbb{Z}$, και $d = -1$ έχουμε $x^2 + y^2 = 1$, όπου οι λύσεις είναι $x = \pm 1, y = 0$ ή $x = 0, y = \pm 1$. Έτσι δείξαμε το 1. Για $d < -3$ υποχρεωτικά θα πρέπει $b = 0$. Άρα οι μόνες ακέραιες λύσεις είναι $a = \pm 1, b = 0$. Αν πάρουμε $d \equiv 1 \bmod 4$, τότε θα έχουμε και την περίπτωση όπου $a = A/2, b = B/2$, με A, B περιττοί ακέραιοι. Έτσι $A^2 - dB^2 = 4$. Για $d < -3$ παίρνουμε $B = 0$, άρα δεν θα έχουμε παραπάνω λύσεις. Έτσι δείξαμε το 3. Για $d = -3$ βρίσκουμε τις επιπλέον λύσεις $A = \pm 1, B = \pm 1$. Για $A = 1, B = 1$ είναι $a = \frac{1}{2}(-1 + \sqrt{-3}) = e^{2\pi i/3}$, λύση την οποία σημειώσαμε σαν ω. Οι άλλες περιπτώσεις είναι προφανώς τα $-\omega, \omega^2, -\omega^2$. Μαζί με τις λύσεις που βρήκαμε πριν, ολοκληρώνουμε και την απόδειξη του 2.

Πάμε να δείξουμε μερικές βασικές ιδιότητες των μονάδων, των συνεταιρικών στοιχείων και των αναγώγων.

Πρόταση 2.3 *Για μία ακέραια περιοχή* D, *έχουμε:*

1. *Το στοιχείο* x *είναι μονάδα αν και μόνο αν* $x|1$.
2. *Οποιαδήποτε δύο στοιχεία που είναι μονάδες, είναι συνεταιρικά και κάθε συνεταιρικό μονάδας είναι μονάδα και αυτό.*
3. *Δύο στοιχεία* x, y *είναι συνεταιρικά, αν και μόνο αν* $x|y$ *και* $y|x$.
4. *Ένα στοιχείο* x *είναι ανάγωγο, αν και μόνο αν κάθε διαιρέτης του είναι συνεταιρικό στοιχείο του* x *ή είναι μονάδα.*
5. *Ένα συνεταιρικό ενός ανάγωγου, είναι και αυτό ανάγωγο.*

Απόδειξη. Η απόδειξη των περισσοτέρων είναι τετριμμένη και έρχεται σχεδόν απ ευθείας από τους ορισμούς. Ας αποδείξουμε το 3 που απλά χρειάζεται νόμο διαγραφής. Έχουμε ότι $x|y$ και $y|x$. Υπάρχουν έτσι $a, b \in D$, τέτοια ώστε

$y = ax,\ x = by$. Με αντικατάσταση παίρνουμε $x = bax$. Τώρα ή $x = 0$ όπου θα είναι και $y = 0$, οπότε είναι συνεταιρικά στοιχεία, ή $x \neq 0$ και από τον νόμο διαγραφής έχουμε $1 = ba$. Τότε a, b είναι μονάδες. Άρα x, y συνεταιρικά στοιχεία.

Εκφράσουμε κάποιες από αυτές τις ιδιότητες με ιδεώδη και παίρνουμε την παρακάτω πρόταση.

Πρόταση 2.4 *Αν D μία ακέραια περιοχή και x, y είναι δύο μη μηδενικά στοιχεία της D, τότε:*

1. *$x|y$ αν και μόνο αν $\langle x \rangle \supseteq \langle y \rangle$.*
2. *Τα x και y είναι συνεταιρικά, αν και μόνο αν $\langle x \rangle = \langle y \rangle$.*
3. *Το στοιχείο x είναι μονάδα, αν και μόνο αν $\langle x \rangle = D$.*
4. *Το στοιχείο x είναι ανάγωγο, αν και μόνο αν το ιδεώδες $\langle x \rangle$ είναι μέγιστο μεταξύ όλων των κανονικών κύριων ιδεωδών της D.*

Απόδειξη. Για το 1 έχουμε: Αν $x|y \Rightarrow y = zx \in \langle x \rangle, z \in D$. Επομένως $\langle x \rangle \supseteq \langle y \rangle$. Αντίστροφα τώρα αν $\langle y \rangle \subseteq \langle x \rangle$, τότε $y \in \langle x \rangle \Rightarrow y = zx, z \in D$. Το 2 αποδεικνύεται άμεσα από το 1 και την πρόταση 2.3. Στο 3 αν x είναι μία μονάδα τότε $xv = 1, v \in D$. Έτσι για κάθε $y \in D$ είναι $y = xvy \in \langle x \rangle$ και άρα $\langle x \rangle = D$. Αντίστροφα αν $\langle x \rangle = D$, τότε αφού $1 \in D, 1 = zx$ και άρα προφανώς το x είναι μονάδα. Για την τελευταία ιδιότητα 4, έχουμε ότι το x είναι ένα ανάγωγο στοιχείο και υπάρχει στοιχείο y τέτοιο ώστε να ισχύει $\langle x \rangle \subset \langle y \rangle \subset D$. Τότε $y|x$ αλλά από την επιλογή του δεν είναι ούτε μονάδα, ούτε συνεταιρικό στοιχείο του x. Αυτό έρχεται σε αντίθεση με το αποτέλεσμα 4 της πρότασης 2.3. Το αντίστροφο, αν δεν υπάρχει τέτοιο y, τότε κάθε διαιρέτης του x είναι ή μονάδα, ή συνεταιρικό, επομένως το x είναι ανάγωγο.

2.2 Ανάλυση σε ανάγωγα στοιχεία

Έστω ότι δουλεύουμε μέσα σε μία ακέραια περιοχή D και έχουμε ένα μη μηδενικό και μη ανάγωγο στοιχείο x. Μπορούμε επομένως να το γράψουμε σαν $x = ab$. Έστω ότι και οι δύο αυτοί νέοι παράγοντες δεν είναι ανάγωγα στοιχεία. Τότε, συνεχίζουμε αυτήν τη διαδικασία μέχρι να καταλήξουμε να γράψουμε $x = p_1 p_2 ... p_m$, όπου τα p_i αυτά είναι ανάγωγα.

Ορισμός 2.3 *Θα λέμε ότι η ανάλυση σε ανάγωγα είναι δυνατή σε μία ακέραια περιοχή D, αν κάθε στοιχείο της x, γράφεται σαν πεπερασμένο γινόμενο ανάγωγων στοιχείων.*

Γενικά, μία τέτοια ανάλυση μπορεί να μην είναι δυνατή. Για παράδειγμα, σχετικό και με αυτά που έχουμε πει μέχρι τώρα, στο σύνολο των ακεραίων αλγεβρικών αριθμών $\mathbb{B}$, δεν είναι δυνατή η ανάλυση. Αυτό όμως δεν συμβαίνει και στον δακτύλιο ακεραίων ενός σώματος αριθμών, γεγονός που είναι ένας από τους λόγους για τους οποίους δουλεύουμε εκεί μέσα. Ξεκινάμε να αποδείξουμε ότι σε δακτύλιους ακεραίων είναι δυνατή η ανάλυση σε ανάγωγα στοιχεία, δίνοντας έναν ορισμό που έρχεται από την Emmy Noether(1882-1935).

Ορισμός 2.4 *Θα καλούμε μία ακέραια περιοχή Noetherian, αν κάθε ιδεώδες της είναι πεπερασμένα παραγόμενο.*

Έπειτα θα δώσουμε δύο συνθήκες οι οποίες μας είναι απαραίτητες για τη συνέχεια.

1. **Η συνθήκη της αύξουσας αλυσίδας.** Αν έχουμε μία αύξουσα αλυσίδα από ιδεώδη, $I_0 \subseteq I_1 \subseteq ... \subseteq I_n \subseteq ...$, τότε υπάρχει κάποιο N τέτοιο ώστε $I_n = I_N$ για κάθε $n \geq N$.

2. **Η συνθήκη μεγίστου.** Κάθε μη κενό σύνολο από ιδεώδη, περιέχει ένα μέγιστο στοιχείο.

Πρόταση 2.5 *Οι ακόλουθες συνθήκες είναι ισοδύναμες, για μία ακέραια περιοχή D.*

1. *Η D είναι Noetherian.*

2. *Η D ικανοποιεί της συνθήκη της αύξουσας αλυσίδας.*

3. *Η D ικανοποιεί την συνθήκη μέγιστου στοιχείου.*

Απόδειξη. Έστω αρχικά ότι ισχύει το 1. Έστω επίσης $I = \bigcup_{n=1}^{\infty} I_n$. Το I είναι προφανώς ιδεώδες και αφού η D είναι Noetherian, είναι και πεπερασμένα παραγόμενο δηλαδή $I = \langle x_1, ...x_m \rangle$. Κάθε x_i, θα ανήκει σε κάποιο $I_{n(i)}$. Έστω ότι $N = max_i n(i)$, τότε θα έχουμε $I = I_N$ και φυσικά $I_n = I_N$ για κάθε $n \geq N$. Ας υποθέσουμε ότι ισχύει το 2. Θεωρούμε ένα μη κενό σύνολο από ιδεώδη, S. Θα πάμε με άτοπο και θα υποθέσουμε ότι το S δεν έχει μέγιστο στοιχείο, για να αποδείξουμε το 3. Επιλέγουμε ένα $I_0 \in S$. Αφού το I_0 δεν είναι μέγιστο, θα υπάρχει ένα στοιχείο $I_1 \in S$, τέτοιο ώστε $I_0 \subset I_1$. Προχωρούμε επαγωγικά, έχοντας βρει το I_n, το οποίο με τη σειρά του δεν είναι μέγιστο, οπότε επιλέγουμε ένα $I_{n+1} \in S$ με $I_n \subset I_{n+1}$. Αλλά τώρα έχουμε μία αύξουσα αλυσίδα από ιδεώδη, η οποία δεν σταματάει ποτέ. Άρα καταλήγουμε σε άτοπο. Τέλος, έστω ότι ισχύει το 3. Παίρνουμε I ένα οποιοδήποτε ιδεώδες. Θέτουμε S το σύνολο όλων των πεπερασμένα παραγόμενων ιδεωδών, τα οποία περιέχονται στο I. Τότε το $\{0\} \in S$, δηλαδή το S δεν είναι το κενό σύνολο. Άρα θα έχει ένα μέγιστο στοιχείο J με $J \neq I$. Επιλέγουμε $x \in I/J$. Τότε $\langle J, x \rangle$ πεπερασμένα παραγόμενο ιδεώδες και αυστηρά μεγαλύτερο από το J. Άτοπο, επομένως $J = I$ και I πεπερασμένα παραγόμενο. Άρα η D είναι Noetherian. Δείξαμε λοιπόν και το 1.

Θεώρημα 2.1 *Αν μία ακέραια περιοχή D είναι Noetherian, τότε η ανάλυση σε ανάγωγα στοιχεία είναι δυνατή.*

Απόδειξη. Έστω D Noetherian ακέραια περιοχή και ότι υπάρχει κάποιο στοιχείο $x \in D$, το οποίο δεν είναι μηδέν, αλλά ούτε και μονάδα. Έστω ότι αυτό το x δεν μπορεί να γραφεί σαν γινόμενο πεπερασμένων ανάγωγων στοιχείων. Η επιλογή του x είναι τέτοια, ώστε το ιδεώδες $\langle x \rangle$ να είναι μέγιστο, όσων αφορά τις συγκεκριμένες συνθήκες για το x, πράγμα το οποίο μας επιτρέπει να το πούμε η συνθήκη του μεγίστου στοιχείου. Όπως ορίσαμε λοιπόν το x, ξέρουμε ότι δεν είναι ανάγωγο, επομένως $x = yz$, y, z δεν είναι μονάδες. Τότε $\langle x \rangle \subseteq \langle y \rangle$, από την πρόταση 2.4.1. Αν έχουμε $\langle x \rangle = \langle y \rangle$, τότε τα x, y είναι συνεταιρικά, που από την 2.4.2 σημαίνει ότι το z είναι μονάδα. Επομένως έχουμε $\langle x \rangle \subset \langle y \rangle$ και για τους ίδιους λόγους έχουμε επίσης ότι $\langle x \rangle \subset \langle z \rangle$. Από το γεγονός ότι το ιδεώδες $\langle x \rangle$ είναι μέγιστο, θα έχουμε

$$y = p_1...p_r$$

$$z = q_1...q_s,$$

όπου τα p_i, q_j είναι ανάγωγα στοιχεία. Πολλαπλασιάζοντας αυτές τις δύο σχέσεις μεταξύ τους, εκφράζουμε το x σαν πεπερασμένο γινόμενο ανάγωγων στοιχείων. Καταλήγουμε λοιπόν σε άτοπο. Επομένως η ανάλυση σε ανάγωγα στοιχεία είναι δυνατή.

Θεώρημα 2.2 *Ο δακτύλιος ακεραίων $\mathfrak{D}$ ενός σώματος αριθμών K, είναι Noetherian.*

Απόδειξη. Αυτό που πρέπει να δείξουμε είναι ότι κάθε ιδεώδες του $\mathfrak{D}$ είναι πεπερασμένα παραγόμενο. Έχουμε την $(\mathfrak{D}, +)$, η οποία είναι ελεύθερη αβελιανή τάξης n, όσος και ο βαθμός της επέκτασης του K. Επομένως και η $(I, +)$ είναι ελεύθερη αβελιανή , με τάξη έστω $s \leq n$. Έστω λοιπόν μία $\mathbb{Z}$-βάση της $(I, +)$, η $\{x_1, ...x_s\}$. Τότε προφανώς το ιδεώδες I θα παράγεται από αυτά τα στοιχεία. Δηλαδή $I = \langle x_1, ..., x_s \rangle$. Επομένως το I είναι πεπερασμένα παραγόμενο, που σημαίνει ότι δείξαμε αυτό που θέλαμε, ότι δηλαδή ο $\mathfrak{D}$ είναι Noetherian.

Συμμαζεύοντας ότι δείξαμε στα τελευταία θεωρήματα, έχουμε το εξής πόρισμα.

Πόρισμα 2.1 *Η ανάλυση σε ανάγωγα στοιχεία, είναι δυνατή μέσα στους δακτύλιους ακεραίων των σωμάτων αριθμών.*

Τώρα θα δούμε πως χρησιμοποιούμε την νόρμα, για να βρίσκουμε εύκολα μονάδες και ανάγωγα στοιχεία, μέσα στο $\mathfrak{D}$.

Πρόταση 2.6 *Έστω $x, y \in \mathfrak{D}$. Τότε είναι:*

1. *Το x είναι μονάδα, αν και μόνο αν $N(x) = \pm 1$.*
2. *Αν x, y συνεταιρικά στοιχεία, τότε $N(x) = \pm N(y)$.*
3. *Αν $N(x)$ είναι πρώτος αριθμός, τότε το x είναι ανάγωγο στον $\mathfrak{D}$.*

Απόδειξη.

1. Αν x μονάδα τότε $xu = 1$. Τότε $N(x)N(u) = 1, N(x), N(u) \in \mathbb{Z}$. Επομένως θα πρέπει $N(x) = \pm 1$. Αντίστροφα, έστω ότι $N(x) = \pm 1$. Τότε από τον ορισμό της νόρμας ενός στοιχείου έχουμε ότι

$$\sigma_1(x)...\sigma_n(x) = \pm 1,$$

όπου σ_i οι μονομορφισμοί από το $K \to \mathbb{C}$. Χωρίς να βλάψουμε τη γενικότητα, ένας από αυτούς τους παράγοντες, έστω ο σ_1, είναι ίσος με x. Θέτουμε $u = \pm\sigma_2(x)...\sigma_n(x)$ και συνεπώς θα έχουμε

$$xu = 1 \Leftrightarrow u = x^{-1} \in K.$$

Επομένως $u \in K \cap \mathbb{B} = \mathfrak{D}$, έτσι το x είναι μονάδα.

2. Αν έχουμε δύο συνεταιρικά στοιχεία x, y, θα είναι $x = uy, u \in U(\mathfrak{D})$.Είναι λοιπόν $N(x) = N(uy) = N(u)N(y) = \pm N(y)$.

3. Έστω $N(x)$ πρώτος αριθμός και x μη ανάγωγος, τέτοιος ώστε, $x = yz$ με τα y, z να μην είναι μονάδες. Τότε θα έχουμε $N(x) = N(y)N(z)$, όπου αφού $N(x)$ πρώτος, θα πρέπει ένα εκ των $N(y), N(z)$ να είναι $\pm N(x)$ και το άλλο ± 1. Αλλά το στοιχείο που η νόρμα του είναι ± 1 θα είναι μονάδα. Άτοπο.

Τα αντίστροφα των 2 και 3, γενικά δεν ισχύουν. Προχωρούμε τώρα στην επόμενη παράγραφο, όπου θα μιλήσουμε για μοναδική και μη μοναδική ανάλυση σε ανάγωγα, όπου θα φανούν ιδιαίτερα χρήσιμα τα αποτελέσματα των προηγούμενων θεωρημάτων.

2.3 Μη μοναδική ανάλυση σε ανάγωγα στοιχεία

Ορισμός 2.5 *Θα λέμε ότι η ανάλυση σε μία ακέραια περιοχή D είναι μοναδική, αν όταν έχουμε*

$$p_1...p_r = q_1...q_s$$

με p_i, q_j ανάγωγα στοιχεία στην D, ισχύει ότι $r = s$ και υπάρχει μία μετάθεση π του $\{1, ...r\}$ τέτοια ώστε τα $p_i, q_{\pi(i)}$ να είναι συνεταιρικά, για κάθε $i = 1, ..., r$.

Θα λέμε επίσης ότι έχουμε μοναδική ανάλυση σε ανάγωγα, όσων αφορά τη σειρά των παραγόντων και την ύπαρξη μονάδων. Στους δακτύλιους ακεραίων σωμάτων αριθμών, δεν έχουμε μοναδική ανάλυση. Αυτό γενικά δεν είναι και πολύ βολικό, αλλά στην κρυπτογραφία θα φανεί πολύ χρήσιμο. Ξεκινάμε δίνοντας το επόμενο θεώρημα.

Θεώρημα 2.3 *Η ανάλυση δεν είναι μοναδική στους δακτύλιους ακεραίων του $\mathbb{Q}(\sqrt{d})$ για τις (τουλάχιστον) παρακάτω τιμές του d:*

$$-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30.$$

Απόδειξη. Για τον $\mathbb{Q}(\sqrt{-5})$, και το στοιχείο 6, έχουμε τις εξής παραγοντοποιήσεις.

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

Θα δείξουμε λοιπόν ότι αυτοί οι παράγοντες δεν είναι ανάγωγα στοιχεία. Η νόρμα δίνεται από τον τύπο $N(a + b\sqrt{-5}) = a^2 + 5b^2$, οπότε θα έχουμε

$$N(2) = 4,\ N(3) = 9,\ N(1 + \sqrt{-5}) = 6 = N(1 - \sqrt{-5}).$$

Έστω ότι $2 = xy, x, y \in \mathfrak{D}$ και να μην είναι μονάδες. Τότε $4 = N(x)N(y) \Rightarrow N(x) = \pm 2, N(y) = \pm 2$. Όμοια οι μη τετριμμένοι παράγοντες του 3 πρέπει να έχουν νόρμα ± 3, ενώ των $1 \pm \sqrt{-5}$ να είναι ± 2 ή ± 3. Σύμφωνα με το θεώρημα 1.14, και αφού $-5 \equiv 3 \bmod 4 \neq 1 \bmod 4$ οι ακέραιοι αλγεβρικοί θα έχουν μορφή $a + b\sqrt{-5}, a, b \in \mathbb{Z}$. Έτσι έχουμε οδηγηθεί στις εξισώσεις

$$a^2 + 5b^2 = \pm 2 \text{ ή } \pm 3.$$

Έχουμε τώρα ότι $|b| \geq 1 \Rightarrow |a^2 + 5b^2| \geq 5$. Οπότε θα πρέπει $|b| = 0$. Θα έχουμε λοιπόν $a^2 = \pm 2$ ή ± 3, το οποίο είναι αδύνατο. Επομένως οι τέσσερις παράγοντες είναι ανάγωγα στοιχεία. Από την στιγμή τώρα που έχουμε, $N(2) = 4, N(1 \pm \sqrt{-5}) = 6$, από την πρόταση 2.6.2, παίρνουμε ότι τα στοιχεία αυτά δεν είναι ούτε συνεταιρικά μεταξύ τους. Επομένως η παραγοντοποίηση δεν είναι μοναδική. Για τις άλλες τιμές του d, δουλεύουμε με τον ίδιο ακριβώς τρόπο. Να προσέξουμε μόνο ότι σε κάποιες περιπτώσεις όπου $d \equiv 1 \bmod 4$ αλλάζει ο δακτύλιος ακεραίων.

Ακόμα δεν είμαστε σε θέση να αποδείξουμε ότι σε έναν δακτύλιο ακεραίων έχουμε μοναδική ανάλυση, αλλά ας σημειώσουμε ότι στις τιμές του d όπου εκεί θα δουλέψουμε, δηλαδή αρνητικές και ελεύθερες τετραγώνων, έχουμε μοναδική ανάλυση για

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

2.4 Παραγοντοποίηση σε πρώτα στοιχεία

Ορισμός 2.6 *Σε μία ακέραια περιοχή D ένα στοιχείο της x, θα καλείται πρώτο, αν $0 \neq x \notin U(D)$ και επιπλέον έχει την εξής ιδιότητα*

$$x \mid ab \Rightarrow x \mid a \text{ ή } x \mid b.$$

Πρόταση 2.7 *Ένα πρώτο στοιχείο σε μία ακέραια περιοχή, είναι και ανάγωγο.*

Απόδειξη. Έστω D ακέραια περιοχή και x ένα πρώτο στοιχείο της. Αν τότε $x = ab$, είναι $x \mid ab \Rightarrow x \mid a$ ή $x \mid b$. Αν $x \mid a$ τότε $a = xc,\ c \in D$ και άρα $x = xcb$. Διαγράφουμε το x και παίρνουμε ότι $cb = 1$, δηλαδή το στοιχείο b είναι μονάδα. Όμοια και όταν $x \mid b$ θα φτάσουμε στο συμπέρασμα ότι a είναι μονάδα, επομένως το πρώτο στοιχείο x, είναι και ανάγωγο.

Το αντίστροφο της προηγούμενης πρότασης δεν ισχύει. Υπάρχουν ακέραιες περιοχές, όπου ανάγωγα στοιχεία δεν είναι πρώτα. Για παράδειγμα, ας πάρουμε την παραγοντοποίηση που είδαμε λίγο πιο πριν στο $\mathbb{Z}[\sqrt{-5}]$, όπου είχαμε

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

Εδώ το 2 είναι ανάγωγο στοιχείο όπως είχαμε δείξει, αλλά δεν διαιρεί κανένα από τα $1 \pm \sqrt{-5}$, δηλαδή δεν είναι πρώτο.

Θεώρημα 2.4 *Σε μία ακέραια περιοχή όπου η ανάλυση σε πρώτα είναι δυνατή, θα είναι και μοναδική, αν και μόνο αν κάθε ανάγωγο στοιχείο είναι και πρώτο.*

Απόδειξη. Έχουμε D μία ακέραια περιοχή. Θα μας βοηθήσει να γράψουμε την ανάλυση ενός στοιχείου σε ανάγωγα ως εξής

$$x = up_1...p_r,$$

όπου u μονάδα. Έστω ότι η ανάλυση είναι μοναδική και και το στοιχείο p είναι ένα ανάγωγο στοιχείο. Εμείς πρέπει να δείξουμε ότι είναι και πρώτο. Αν έχουμε $p \mid ab$, τότε θα είναι $pc = ab, c \in D$. Παραγοντοποιούμε τα a, b, c, και έχουμε

$$a = u_1 p_1 ... p_n$$

$$b = u_2 q_1 ... q_m$$

$$c = u_3 r_1 ... r_s,$$

όπου u_i είναι μονάδες και τα στοιχεία p_i, q_i, r_i είναι ανάγωγα. Τότε με αντικατάσταση θα πάρουμε

$$pu_3 r_1 ... r_s = u_1 p_1 ... p_n u_2 q_1 ... q_m.$$

Το ότι έχουμε μοναδική ανάλυση, μας λέει ότι το p είναι συνεταιρικό στοιχείο με κάποιο από τα p_i ή q_i. Δηλαδή διαιρεί κάποιο από αυτά, οπότε διαιρεί ή το a ή το b. Επομένως είναι και πρώτο στοιχείο. Αντίστροφα τώρα, έστω ότι κάθε ανάγωγο στοιχείο είναι και πρώτο. Θα δείξουμε ότι αν

$$u_1 p_1 ... p_m = u_2 q_1 q_n, \tag{2.1}$$

όπου u_i μονάδες και p_i, q_i ανάγωγα στοιχεία, τότε $m = n$ και ότι υπάρχει μία μετάθεση π του $\{1, ..., m\}$, τέτοια ώστε $p_i, q_{\pi(i)}$ να είναι συνεταιρικά στοιχεία. Αυτό είναι προφανές για $m = 0$. Για $m \geq 1$, αν ισχύει η (1), τότε $p_m \mid u_2 q_1 ... q_n$. Το p_m είναι όμως πρώτοι στοιχείο, άρα $p_m \mid u_2$ ή $p_m \mid q_j$, για κάποιο j. Στην πρώτη περίπτωση έχουμε ότι p_m είναι μονάδα, άρα θα έχουμε ότι $p_m \mid q_j$. Κάνουμε τώρα μία ανακατάταξη στην αρίθμηση και λέμε ότι $n = j$ και θα έχουμε $p_m \mid q_n$ και $q_n = p_m u$, όπου το u είναι μονάδα. Άρα η σχέση 2.1 θα πάρει την μορφή

$$u_1 p_1 ... p_m = u_2 q_1 ... q_{n-1} q_n u p_m.$$

Διαγράφουμε το p_m και θα έχουμε

$$u_1 p_1 ... p_{m-1} = (u_2 u) q_1 ... q_{n-1}.$$

Συνεχίζουμε επαγωγικά και υποθέτουμε ότι $m - 1 = n - 1$ και υπάρχει μία μετάθεση των $\{1, ..., m-1\}$ τέτοια ώστε τα $p_i, q_{\pi(i)}$ να είναι συνεταιρικά στοιχεία. Επεκτείνουμε τώρα την μετάθεση στο $\{1, ...m\}$ και έχουμε το αποτέλεσμα που ζητούσαμε.

Ορισμός 2.7 *Μία ακέραια περιοχή καλείται περιοχή μοναδικής ανάλυσης, (εμείς από εδώ και πέρα θα αναφερόμαστε σε αυτές σαν ΠΜΑ), αν η ανάλυση σε ανάγωγα είναι δυνατή και μοναδική. Να μην ξεχνάμε ότι σε μία περιοχή μοναδικής ανάλυσης, τα ανάγωγα στοιχεία είναι και πρώτα, οπότε μπορούμε να κάνουμε λόγο και για ανάλυση σε πρώτα στοιχεία.*

2.5 Ευκλείδειες περιοχές

Ορισμός 2.8 *Έστω D μία ακέραια περιοχή. Μία ευκλείδεια συνάρτηση για την ακέραια περιοχή αυτή, είναι μία συνάρτηση $\phi : D - \{0\} \to \mathbb{N}$ τέτοια ώστε:*

1. *Αν $a, b \in D - \{0\}$ και $a|b$, τότε $\phi(a) \leq \phi(b)$.*
2. *Αν $a, b \in D - \{0\}$ τότε υπάρχουν $q, r \in D$, τέτοια ώστε $a = bq + r$, με $r = 0$, ή $\phi(r) < \phi(b)$.*

Ορισμός 2.9 *Μία ακέραια περιοχή η οποία έχει Ευκλείδεια συνάρτηση θα την ονομάζουμε, Ευκλείδεια περιοχή.*

Ο σκοπός μας είναι να δείξουμε ότι μία Ευκλείδεια περιοχή έχει μοναδική ανάλυση. Θα δείξουμε λοιπόν ότι κάθε ανάγωγο στοιχείο είναι και πρώτο. Αρχικά δείχνουμε ότι κάθε ιδεώδες σε μία τέτοια περιοχή είναι κύριο, (τέτοιες περιοχές καλούνται περιοχές κυρίων ιδεωδών και από εδώ και πέρα για συντομία, θα τις γράφουμε ΠΚΙ), και τέλος ότι αυτή η ιδιότητα είναι ισοδύναμη με το ότι όλα τα ανάγωγα είναι και πρώτα στοιχεία. Ξεκινάμε με μια υπενθύμιση του ορισμού του κυρίου ιδεώδους.

Ορισμός 2.10 *Αν έχουμε $a \in D$ τότε το ιδεώδες $\{ra, r \in D\}$, όλων των πολλαπλασίων του a, είναι το κύριο ιδεώδες που παράγεται από το a και το συμβολίζουμε $\langle a \rangle$.*

Θεώρημα 2.5 *Κάθε Ευκλείδεια περιοχή είναι ΠΚΙ.*

Απόδειξη. Έστω D Ευκλείδεια ακέραια περιοχή και I ένα ιδεώδες μέσα σε αυτήν. Αν είναι $I = 0$ τότε το I είναι κύριο. Έστω $x \neq 0 \in D$. Επιλέγουμε αυτό το x έτσι ώστε η τιμή του $\phi(x)$ να είναι η μικρότερη δυνατή. Έστω επίσης στοιχείο $y \in I$. Από την δεύτερη ιδιότητα της Ευκλείδειας συνάρτησης, θα έχουμε ότι $y = qx + r$ με $r = 0$ ή $\phi(r) < \phi(x)$. Η δεύτερη περίπτωση αποκλείεται λόγω της επιλογής που κάναμε για το x. Επομένως θα έχουμε $r = 0 \Rightarrow y = qx$. Άρα $I = \langle x \rangle$, δηλαδή το I είναι κύριο ιδεώδες και η D είναι περιοχή κύριων ιδεωδών.

Θεώρημα 2.6 *Κάθε περιοχή κύριων ιδεωδών (ΠΚΙ), είναι περιοχή μοναδικής ανάλυσης (ΠΜΑ).*

Απόδειξη. Έστω μία ακέραια περιοχή D, η οποία είναι ΠΚΙ. Αυτό φυσικά μας λέει ότι είναι και Noetherian. Επομένως από το θεώρημα 2.1, έχουμε ότι η ανάλυση σε ανάγωγα είναι δυνατή. Πρέπει να δείξουμε ότι είναι και μοναδική. Θα δείξουμε ότι κάθε ανάγωγο στοιχείο είναι και πρώτο. Έστω στοιχείο p ανάγωγο. Το ιδεώδες $\langle p \rangle$ θα είναι μέγιστο μεταξύ των άλλων κύριων ιδεωδών της D. Ας υποθέσουμε ότι το $p \mid ab$, αλλά να μην διαιρεί το a. Τότε αυτό σημαίνει ότι $\langle p \rangle \subset \langle p, a \rangle$. Και επειδή το $\langle p \rangle$ είναι μέγιστο, θα έχουμε $\langle p, a \rangle = D$. Έχουμε ότι $1 \in D \Rightarrow 1 = cp + da, c, d \in D$. Πολλαπλασιάζουμε με b και θα έχουμε,

$$b = cpb + dab,$$

και αφού $p \mid ab \Rightarrow p \mid cpb + dab \Rightarrow p \mid b$. Επομένως το p είναι πρώτο στοιχείο και άρα η D περιοχή μοναδικής ανάλυσης.

Συνδυάζοντας τα παραπάνω θεωρήματα παίρνουμε το εξής:

Θεώρημα 2.7 *Κάθε Ευκλείδεια περιοχή, είναι περιοχή μοναδικής ανάλυσης.*

Κεφάλαιο 3

Ιδεώδη

3.1 Ανάλυση ιδεωδών σε πρώτα ιδεώδη

Θα δώσουμε πρώτα τον ορισμό μέγιστου και πρώτου ιδεώδους, ενός δακτυλίου R.

Ορισμός 3.1 *Ένα ιδεώδες $\mathfrak{a}$ ενός δακτυλίου R λέγεται μέγιστο, αν δεν είναι το μηδενικό ιδεώδες και δεν υπάρχει άλλο ιδεώδες I του R, τέτοιο ώστε να ισχύει,*

$$\mathfrak{a} \subseteq I \subseteq R.$$

Ορισμός 3.2 *Ένα ιδεώδες $\mathfrak{a}$ ενός δακτυλίου R λέγεται πρώτο, αν για κάθε ιδεώδη $\mathfrak{b}, \mathfrak{c}$ του δακτυλίου R για τα οποία ισχύει ότι $\mathfrak{bc} \subseteq \mathfrak{a}$ να συνεπάγεται ότι $\mathfrak{b} \subseteq \mathfrak{a}$ ή $\mathfrak{c} \subseteq \mathfrak{a}$.*

Λήμμα 3.1 *Έστω R δακτύλιος και $\mathfrak{a}$ ιδεώδες αυτού του δακτυλίου. Τότε θα έχουμε τα εξής:*

1. *το $\mathfrak{a}$ είναι μέγιστο ιδεώδες αν και μόνο αν $R/\mathfrak{a}$ είναι σώμα.*
2. *το $\mathfrak{a}$ είναι πρώτο ιδεώδες αν και μόνο αν $R/\mathfrak{a}$ είναι ακέραια περιοχή.*

Απόδειξη. Τα ιδεώδη του $R/\mathfrak{a}$ είναι σε ένα προς ένα και επί αντιστοιχία με τα τα ιδεώδη του R, τα οποία βρίσκονται μεταξύ του R και του $\mathfrak{a}$. Άρα το $\mathfrak{a}$ είναι μέγιστο, αν και μόνο αν ο $R/\mathfrak{a}$ δεν έχει μη μηδενικά τετριμμένα ιδεώδη. Επίσης γνωρίζουμε ότι αν ένας δακτύλιος S, δεν έχει μη μηδενικά τετριμμένα ιδεώδη, είναι σώμα. Αποδείξαμε το 1. Έστω ότι $\mathfrak{a}$ πρώτο ιδεώδες. Θεωρούμε $x, y \in R$, τέτοια ώστε στον $R/\mathfrak{a}$ να έχουμε: $(\mathfrak{a} + x)(\mathfrak{a} + y) = 0$ και τότε $xy \in \mathfrak{a} \Rightarrow \langle x \rangle \subseteq \mathfrak{a}$ ή $\langle y \rangle \subseteq \mathfrak{a}$ δηλαδή ή $x \in \mathfrak{a}$ ή $y \in \mathfrak{a}$. Επομένως ένα από τα $\mathfrak{a} + x$ και $\mathfrak{a} + y$ είναι μηδέν στον $R/\mathfrak{a}$, δηλαδή ο $R/\mathfrak{a}$ δεν έχει διαιρέτες του μηδενός και είναι ακέραια περιοχή. Αντίστροφα, ας υποθέσουμε ότι ο $R/\mathfrak{a}$ είναι ακέραια περιοχή. Τότε η τάξη του $R/\mathfrak{a}$ θα είναι $|R/\mathfrak{a}| \neq 1$ έτσι $\mathfrak{a} \neq R$. Τώρα υποθέτουμε ότι $\mathfrak{bc} \subseteq \mathfrak{a}$ αλλά $\mathfrak{b} \subset \mathfrak{a}$ και $\mathfrak{c} \subset \mathfrak{a}$. Τότε μπορούμε να βρούμε στοιχεία $b \in \mathfrak{b}$ και $g \in \mathfrak{c}$ με $b, g \notin \mathfrak{a}$ αλλά $bg \in \mathfrak{a}$. Αυτό σημαίνει ότι $(\mathfrak{a} + b)$ και $(\mathfrak{a} + g)$ είναι διαιρέτες του μηδενός στον $R/\mathfrak{a}$. Άτοπο γιατί έχουμε υποθέσει ότι ο $R/\mathfrak{a}$ είναι ακέραια περιοχή.

Σημειώνουμε επίσης και το ακόλουθο πόρισμα, που προκύπτει εύκολα από το παραπάνω λήμμα.

Πόρισμα 3.1 *Κάθε μέγιστο ιδεώδες είναι πρώτο.*

Θεώρημα 3.1 *Ο δακτύλιος ακεραίων $\mathfrak{D}$ ενός σώματος αριθμών K έχει τις ακόλουθες ιδιότητες:*

1. *Είναι ακέραια περιοχή με σώμα κλασμάτων K.*
2. *Είναι Noetherian ακέραια περιοχή.*
3. *Αν ένα στοιχείο a το οποίο ανήκει στο K ικανοποιεί ένα μονικό πολυώνυμο στον $\mathfrak{D}$, τότε $a \in \mathfrak{D}$.*
4. *Κάθε μη μηδενικό πρώτο ιδεώδες του $\mathfrak{D}$ είναι μέγιστο.*

Απόδειξη.

1. Προφανές
2. Όπως ξέρουμε η ομάδα $(\mathfrak{D}, +)$ είναι ελεύθερη αβελιανή τάξης n. Επομένως αν $\mathfrak{a}$ ένα ιδεώδες του $\mathfrak{D}$ τότε και η $(\mathfrak{a}, +)$ θα είναι ελεύθερη αβελιανή με τάξη $|\mathfrak{a}| \leq n$. Κάθε βάση ακεραιότητας της $(\mathfrak{a}, +)$ παράγει το $\mathfrak{a}$ σαν ιδεώδες, επομένως το $\mathfrak{a}$ είναι πεπερασμένα παραγόμενο. Άρα είναι Noetherian.
3. Από το θεώρημα 1.8 έχουμε ότι αν ένα $\theta \in \mathbb{C}$ ικανοποιεί ένα μονικό πολυώνυμο το οποίο έχει συντελεστές ακέραιους αριθμούς, τότε και ο θ είναι ακέραιος αλγεβρικός. Άρα, αφού έχουμε ότι $\alpha \in K$ και ικανοποιεί μονικό πολυώνυμο στο $\mathfrak{D}$ θα είναι $\alpha \in \mathbb{B}$. Επομένως $\alpha \in \mathfrak{D}$.
4. Έστω $\mathfrak{p}$ ένα μη μηδενικό πρώτο ιδεώδες του $\mathfrak{D}$ και ένα στοιχείο του α, διάφορο του μηδενός. Είναι $N = N(\alpha) = \alpha_1 ... \alpha_n \in \mathfrak{p}$ (Αυτό γιατί τα α_i είναι τα συζυγή στοιχεία του α) και έστω ότι $\alpha = \alpha_1$. Τότε $\langle N \rangle \subseteq p$, και άρα ο δακτύλιος πηλίκο $\mathfrak{D}/\mathfrak{p}$ είναι ένας δακτύλιος πηλίκο του $\mathfrak{D}/N\mathfrak{D}$, ο οποίος αφού είναι πεπερασμένα παραγόμενη αβελιανή ομάδα με κάθε στοιχείο της να έχει πεπερασμένη τάξη, είναι πεπερασμένος. Οπότε αφού $\mathfrak{D}/\mathfrak{p}$ είναι ακέραια περιοχή και πεπερασμένη, είναι σώμα. Επομένως το ιδεώδες $\mathfrak{p}$ είναι μέγιστο.

Ένας δακτύλιος που ικανοποιεί τις παραπάνω ιδιότητες ονομάζεται δακτύλιος Dedekind. Ένα ιδεώδες, όπως γνωρίζουμε, μπορούμε να το δούμε σαν $\mathfrak{D}$-submodule του $\mathfrak{D}$, άρα μπορούμε να δουλεύουμε κοιτώντας τα $\mathfrak{D}$-submodules του σώματος K. Τα συγκεκριμένα submodules τα οποία θα μας χρειαστούν, θα έχουν την εξής ιδιότητα:

Ορισμός 3.3 *Ένα $\mathfrak{D}$-submodule $\mathfrak{a}$ του K θα καλείται κλασματικό ιδεώδες του $\mathfrak{D}$ αν υπάρχει κάποιο μη μηδενικό στοιχείο $c \in \mathfrak{D}$ τέτοιο ώστε να ισχύει: $c\mathfrak{a} \subseteq \mathfrak{D}$. Με άλλα λόγια το σύνολο $\mathfrak{b} = c\mathfrak{a}$, είναι ένα ιδεώδες του $\mathfrak{D}$ και $\mathfrak{a} = c^{-1}\mathfrak{b}$. Δηλαδή τα κλασματικά ιδεώδη του $\mathfrak{D}$ είναι υποσύνολα του K της μορφής $c^{-1}\mathfrak{b}$, όπου $\mathfrak{b}$ είναι ένα ιδεώδες του $\mathfrak{D}$ και c ένα μη μηδενικό στοιχείο του $\mathfrak{D}$.*

Θεώρημα 3.2 *Τα μη μηδενικά κλασματικά ιδεώδη του $\mathfrak{D}$ σχηματίζουν μία αβελιανή ομάδα με πράξη τον πολλαπλασιασμό.*

Απόδειξη. Βλέπε θεώρημα 5.5 [1].

Θεώρημα 3.3 *Όλα τα μη μηδενικά κλασματικά ιδεώδη ενός δακτυλίου ακεραίων $\mathfrak{D}$, μπορούν να γραφούν σα γινόμενο πρώτων ιδεωδών, με μοναδικό τρόπο, μέχρι τη σειρά των παραγόντων.*

Απόδειξη. Βλέπε θεώρημα 5.5 [1].

Πρόταση 3.1 *Για ιδεώδη* $\mathfrak{a}, \mathfrak{b}$ *του* $\mathfrak{D}$*, θα ισχύει:*

$$\mathfrak{a} \mid \mathfrak{b} \text{ } \textit{αν και μόνο αν} \text{ } \mathfrak{a} \supseteq \mathfrak{b}.$$

Αυτό μας λέει ότι οι παράγοντες ενός ιδεώδους του $\mathfrak{D}$, είναι ακριβώς τα ιδεώδη που το περιέχουν. Έτσι ο ορισμός του πρώτου ιδεώδους γίνεται ανάλογος με αυτόν του πρώτου στοιχείου.Έχουμε δηλαδή:

$$\mathfrak{p} \mid \mathfrak{ab} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ ή } \mathfrak{p} \mid \mathfrak{b}.$$

3.2 Νόρμα ιδεώδους

Θα ορίσουμε την έννοια της νόρμας ενός ιδεώδους $N(\mathfrak{a})$. Έχουμε δείξει ότι η τάξη του δακτύλιου πηλίκου $\mathfrak{D}/\mathfrak{a}$ είναι πεπερασμένη. Έτσι ορίζουμε τη νόρμα ως εξής

$$N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}|.$$

Ας δούμε την σχέση μεταξύ της νόρμας ενός ιδεώδους και ενός στοιχείου.

Θεώρημα 3.4

1. *Κάθε ιδεώδες* $\mathfrak{a} \neq 0$ *του* $\mathfrak{D}$*, σαν ένα* $\mathbb{Z}$*-module, έχει βάση* $\{\alpha_1, ..., \alpha_n\}$ *όπου* n*, όπως συνήθως, ο βαθμός της επέκτασης* K*.*

2. *Η νόρμα ενός ιδεώδους ισούται με*

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta} \right|^{1/2},$$

όπου Δ *η διακρίνουσα του* K*.*

Απόδειξη.

1. Γνωρίζουμε ότι η $(\mathfrak{D}, +)$ είναι ελεύθερη αβελιανή τάξης n. Επίσης αφού ο $\mathfrak{D}/\mathfrak{a}$ έχει πεπερασμένη τάξη θα έχουμε ότι και η $(\mathfrak{a}, +)$ θα είναι ελεύθερη αβελιανή τάξης n. Επομένως θα έχει βάση της μορφής $\{\alpha_1, ..., \alpha_n\}$.

2. Έστω $\{\omega_1, ..., \omega_n\}$ μία βάση ακεραιότητας για τον $\mathfrak{D}$, και υποθέτουμε ότι $\alpha_i = \sum c_{ij}\omega_{ij}$ Τότε έχουμε ότι

$$N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}| = |det(c_{ij})|$$

(βλέπε θεώρημα 1.13 [1]). Γνωρίζουμε λοιπόν ότι θα ισχύει

$$\Delta[\alpha_1, ..., \alpha_n] = (det(c_{ij}))^2 \Delta[\omega_1, ..., \omega_n] = (N(\mathfrak{a}))^2 \Delta \Leftrightarrow N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta} \right|^{1/2}$$

Παράδειγμα 3.1 *Ας δούμε μία εφαρμογή. Θα παραγοντοποιήσουμε το ιδεώδες* $\langle 18 \rangle$ *στον δακτύλιο ακεραίων* $\mathbb{Z}[\sqrt{-17}]$*. Γνωρίζουμε την παραγοντοποίηση του στοιχείου 18 στο* $\mathbb{Z}[\sqrt{-17}]$ *είναι:*

$$18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17}) \cdot (1 + \sqrt{-17})$$

Θεωρούμε το ιδεώδες $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-17}\rangle$, *του οποίου οι γεννήτορες είναι και οι δύο παράγοντες του* 18. *Προφανώς το* $18 \in \mathfrak{p}_1$, *άρα* $\langle 18\rangle \subseteq \mathfrak{p}_1$, *το οποίο σημαίνει ότι το ιδεώδες* $\mathfrak{p}_1$ *είναι παράγοντας του* $\langle 18\rangle$. *Τώρα επίσης έχουμε :*

$$1-\sqrt{-17} = 2-(1+\sqrt{-17}) \in \mathfrak{p}_1$$

επομένως: $18 = (1+\sqrt{-17})\cdot(1+\sqrt{-17}) \in \mathfrak{p}_1^2$ *το οποίο με τη σειρά του σημαίνει ότι* $\langle 18\rangle \subseteq \mathfrak{p}_1^2$ *και άρα* $\mathfrak{p}_1^2$ *είναι παράγοντας του* $\langle 18\rangle$. *Τα στοιχεία τώρα του* $\mathfrak{p}_1$ *έχουν την εξής μορφή:*

$$2x + (1+\sqrt{-17})y \text{ με } x, y \in \mathbb{Z}[\sqrt{-17}].$$

Δηλαδή έχουμε για $a, b, c, d \in \mathbb{Z}$*:*

$$2(a+b\sqrt{-17}) + (1+\sqrt{-17})(c+d\sqrt{-17})$$

$$= (2a+c-17d) + (2b+d+c)\sqrt{-17} = r + s\sqrt{-17}$$

με $r-s = 2a-2b-18d$, *δηλαδή το* $r-s$ *είναι άρτιος αριθμός. Αυτό μας οδηγεί στο συμπέρασμα ότι ο* r *και ο* s *πρέπει να είναι και οι δύο άρτιοι ή και οι δύο περιττοί. Επομένως το ιδεώδες* $\mathfrak{p}_1$ *δεν μπορεί να καλύπτει όλον τον δακτύλιο* $\mathbb{Z}[\sqrt{-17}]$. *Τώρα έχουμε ότι το ιδεώδες* $\mathfrak{p}_1$ *είναι μέγιστο. Αυτό γιατί αν πάρουμε ένα οποιοδήποτε στοιχείο της μορφής* $m+n\sqrt{-17}$ *το οποίο να μην ανήκει στο* $\mathfrak{p}_1$, *τότε θα είναι το ένα από τα* m, n *άρτιο και το άλλο περιττό. Δηλαδή θα είναι :* $\mathfrak{p}_1 = \langle m+n\sqrt{-17}\rangle = \mathbb{Z}[\sqrt{-17}]$.*Όμοια τώρα, παίρνουμε ιδεώδες* $\mathfrak{p}_2 = \langle 3, 1+\sqrt{-17}\rangle$. *Ένα στοιχείο του* $\mathfrak{p}_2$ *είναι της μορφής* $r+s\sqrt{-17} = (3a+c-17d) + (3b+c+d)\sqrt{-17}$, *όπου* $r-s = 3(a+b-6d)$. *Άρα τα* r, s *μπορούν να είναι οποιοιδήποτε ακέραιοι που ικανοποιούν την* $r = s \bmod 3$. *Όμοια με πριν το ιδεώδες* $\mathfrak{p}_2$ *είναι μέγιστο και* $18 = 2\cdot 3\cdot 3 \in \mathfrak{p}_2^2$, *επομένως το* $\mathfrak{p}_2^2$ *είναι παράγοντας του* $\langle 18\rangle$.
Τέλος, θα πάρουμε $\mathfrak{p}_3 = \langle 3, 1-\sqrt{-17}\rangle$, *και έτσι έχουμε ένα ακόμα πρώτο ιδεώδες, τέτοιο ώστε* $\mathfrak{p}_3^2$ *να είναι παράγοντας του* $\langle 18\rangle$. *Όμοιοι υπολογισμοί με πριν, θα μας δώσουν ότι* $r+s\sqrt{-17} \in \mathfrak{p}_3$ *αν και μόνο αν* $r+s = 0 \bmod 3$. *Επομένως σύμφωνα με το θεώρημα ανάλυσης θα έχουμε:*

$$\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2 \supseteq \langle 18\rangle .$$

Η νόρμα ενός ιδεώδους $\mathfrak{p}$, *όπως την ορίσαμε πριν* $N(\mathfrak{p})$, *είναι ίση με την τάξη του πηλίκου* $\mathfrak{D}/\mathfrak{p}$. *Μία ιδιότητά της που θα χρησιμοποιήσουμε είναι,*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Έχουμε τώρα ότι κάθε στοιχείο στο δακτύλιο ακεραίων $\mathbb{Z}[\sqrt{-17}]$ *θα είναι της μορφής* $1+x, x \in \mathfrak{p}_1$. *Επομένως θα είναι*

$$N(\mathfrak{p}_1) = \left|\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}_1\right| = 2.$$

Όμοια έχουμε για τα άλλα δύο ιδεώδη,

$$N(\mathfrak{p}_i) = \left|\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}_i\right| = 3, \text{ για } i = 2, 3.$$

Οπότε τώρα κάνοντας χρήση της παραπάνω ιδιότητας της νόρμας, έχουμε ότι :

$$N(\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2) = N(\mathfrak{p}_1)^2N(\mathfrak{p}_2)^2N(\mathfrak{p}_3)^2 = 2^2\cdot 3^2\cdot 3^2 = 18^2.$$

Τώρα ζητάμε τη νόρμα του ιδεώδους $\langle 18\rangle$. *Είναι*

$$N(\langle 18\rangle) = \left|\mathbb{Z}[\sqrt{-17}]/\langle 18\rangle\right|.$$

Κάθε στοιχείο του $\mathbb{Z}[\sqrt{-17}]$ *μπορούμε να το γράψουμε :*

$$a + b\sqrt{-17} + x \ \mu\epsilon\ a, b = 0...17 \ \kappa\alpha\iota\ x \in \langle 18\rangle$$

άρα έχουμε 18 επιλογές για το a *και 18 επιλογές για το* b. *Επομένως είναι*

$$N(\langle 18\rangle) = 18^2.$$

Έστω τώρα ότι το $\langle 18\rangle$ *αναλύεται σε πρώτα ιδεώδη ως εξής:*

$$\langle 18\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{a},$$

για κάποιο ιδεώδες $\mathfrak{a}$. *Τότε θα έπρεπε να είχαμε* $N(\mathfrak{a}) = 1$ *που σημαίνει ότι το* $\mathfrak{a}$ *είναι ολόκληρος ο δακτύλιος. Άρα καταλήγουμε ότι*

$$\langle 18\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$$

Είναι τώρα από την ανάλυση του στοιχείου $18, 2\cdot 3\cdot 3 = 18$, *επομένως*

$$\langle 2\rangle \langle 3\rangle^2 = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2.$$

Από τη μοναδικότητα της ανάλυσης των ιδεωδών θα έχουμε ότι και το $\langle 2\rangle$ *και το* $\langle 3\rangle$ *θα είναι γινόμενα των* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$. *Παρατηρούμε ότι* $2 \in \mathfrak{p}_1, 2 \notin \mathfrak{p}_2, 2 \notin \mathfrak{p}_3$. *Άρα θα είναι* $\mathfrak{p}_1 \mid \langle 2\rangle$ *και* $\mathfrak{p}_2 \nmid \langle 2\rangle, \mathfrak{p}_3 \nmid \langle 2\rangle$ *έτσι θα είναι*

$$\langle 2\rangle = \mathfrak{p}_1^q.$$

Ομοίως για το ιδεώδες $\langle 3\rangle$ *είναι*

$$\langle 3\rangle = \mathfrak{p}_2^r\mathfrak{p}_3^s.$$

Συνδυάζοντας τις τελευταίες σχέσεις παίρνουμε

$$\mathfrak{p}_1^q\mathfrak{p}_2^{2r}\mathfrak{p}_3^{2s} = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2.$$

και λόγω της μοναδικότητας της ανάλυσης πρέπει να είναι $q = 2, r = 1, s = 1 \Rightarrow \langle 2\rangle = \mathfrak{p}_1^2, \langle 3\rangle = \mathfrak{p}_2\mathfrak{p}_3$. *Ακριβώς ίδια δουλειά γίνεται και για την άλλη ανάλυση του στοιχείου 18 στον* $\mathbb{Z}[\sqrt{-17}]$

$$18 = (1+\sqrt{-17})(1-\sqrt{-17}).$$

Είναι λοιπόν

$$\langle 18\rangle = \left\langle 1+\sqrt{-17}\right\rangle \left\langle 1-\sqrt{-17}\right\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2.$$

επίσης

$$1+\sqrt{-17} \in \mathfrak{p}_1, 1+\sqrt{-17} \in \mathfrak{p}_2, 1+\sqrt{-17} \notin \mathfrak{p}_3$$
$$1-\sqrt{-17} \in \mathfrak{p}_1, 1-\sqrt{-17} \in \mathfrak{p}_3, 1-\sqrt{-17} \notin \mathfrak{p}_2.$$

Επομένως

$$\left\langle 1+\sqrt{-17}\right\rangle = \mathfrak{p}_1^m\mathfrak{p}_2^n$$

$$\left\langle 1-\sqrt{-17}\right\rangle = \mathfrak{p}_1^r\mathfrak{p}_3^s$$

Επομένως με τη βοήθεια της σχέσης

$$\langle 18\rangle = \left\langle 1+\sqrt{-17}\right\rangle \left\langle 1-\sqrt{-17}\right\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$$

θα έχουμε $m=1, r=1, n=2, s=2$*, άρα*

$$\left\langle 1+\sqrt{-17}\right\rangle = \mathfrak{p}_1\mathfrak{p}_2^2, \left\langle 1-\sqrt{-17}\right\rangle = \mathfrak{p}_1\mathfrak{p}_3^2$$

Έχουμε λοιπόν πλέον βρει δύο αναλύσεις του ιδεώδους $\langle 18\rangle$*. Είναι*

$$\langle 18\rangle = \langle 2\rangle \langle 3\rangle^2 = \mathfrak{p}_1^2(\mathfrak{p}_2\mathfrak{p}_3)^2 = (\mathfrak{p}_1\mathfrak{p}_2^2)(\mathfrak{p}_1\mathfrak{p}_3^2) = \left\langle 1+\sqrt{-17}\right\rangle \left\langle 1-\sqrt{-17}\right\rangle$$

Βλέπουμε λοιπόν ότι οι δύο αυτές διαφορετικές αναλύσεις προέρχονται από διαφορετικές ομαδοποιήσεις των ιδεωδών $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$*.*

Πόρισμα 3.2 *Αν* $\mathfrak{a}=\langle a\rangle$*, είναι ένα κύριο ιδεώδες, τότε* $N(\mathfrak{a}) = |N(a)|$*.*

Χάρη σε αυτό το πόρισμα μπορούμε να κάνουμε άμεσους υπολογισμούς για τη νόρμα κυρίων ιδεωδών.

Παράδειγμα 3.2 *Αν έχουμε έναν δακτύλιο ακεραίων* $\mathfrak{D}$ *ενός* $\mathbb{Q}(\sqrt{d})$*, για* d *ακέραιο αριθμό και ελεύθερο τετραγώνου, τότε είναι*

$$N(\left\langle a+b\sqrt{d}\right\rangle) = \left|a^2-b^2d\right|$$

και συγκεκριμένα για το προηγούμενο παράδειγμα που δουλέψαμε, δηλαδή $\mathfrak{D} = \mathbb{Z}[\sqrt{-17}]$ *και ιδεώδες το* $\langle 18\rangle$ *θα έχουμε*

$$N(\langle 18\rangle) = 18^2.$$

Θεώρημα 3.5 *Αν έχουμε δύο μη μηδενικά ιδεώδη* $\mathfrak{a},\mathfrak{b}$ *ενός* $\mathfrak{D}$ *τότε*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Απόδειξη. Λόγω μοναδικότητας της ανάλυσης και με επαγωγή στον αριθμό των παραγόντων, αρκεί να δείξουμε ότι

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p})$$

για $\mathfrak{p}$ πρώτο ιδεώδες. Ισχυριζόμαστε τώρα το εξής

$$|\mathfrak{D}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{a}|\,|\mathfrak{a}/\mathfrak{ap}|\,, \tag{3.1}$$

και

$$|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{p}|\,. \tag{3.2}$$

Από αυτές τις δύο σχέσεις και τον ορισμό της νόρμας, οδηγούμαστε στο αποτέλεσμα. Για την σχέση 3.1 θα δουλέψουμε ως εξής. Ορίζουμε τον ομομορφισμό δακτυλίων

$$\phi : \mathfrak{D}/\mathfrak{ap} \to \mathfrak{D}/\mathfrak{a}$$

με

$$\phi(\mathfrak{ap}+x) = \mathfrak{a}+x.$$

Τότε ο ϕ είναι ένας επί ομομορφισμός δακτυλίων με πυρήνα, $\mathfrak{a}/\mathfrak{ap}$. Εφαρμόζουμε λοιπόν το θεώρημα ισομορφισμού για δακτυλίους και θα έχουμε ότι υπάρχει ισομορφισμός

$$\phi' : \frac{\mathfrak{D}/\mathfrak{ap}}{\mathfrak{a}/\mathfrak{ap}} \longrightarrow \mathfrak{D}/\mathfrak{a}$$

Επομένως οι τάξεις αυτών των δακτυλίων θα είναι ίσες. Έτσι θα πάρουμε την σχέση 1.5.

$$\frac{|\mathfrak{D}/\mathfrak{ap}|}{|\mathfrak{a}/\mathfrak{ap}|} = |\mathfrak{D}/\mathfrak{a}| \Longleftrightarrow |\mathfrak{D}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$$

Για την σχέση 3.2, πρώτα παρατηρούμε ότι λόγω μοναδικής ανάλυσης θα έχουμε ότι $\mathfrak{a} \neq \mathfrak{ap}$ και έτσι θα είναι $\mathfrak{ap} \subset \mathfrak{a}$. Θα δείξουμε ότι δεν υπάρχει ιδεώδες $\mathfrak{b}$ μεταξύ των $\mathfrak{a}$ και $\mathfrak{ap}$. Αν υπήρχε τέτοιο ιδεώδες $\mathfrak{b}$ τότε θα ήταν

$$\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{ap}$$

και τότε σαν κλασματικά ιδεώδη

$$\mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{a}^{-1}\mathfrak{ap} \Longleftrightarrow \mathfrak{D} \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{p}.$$

Αφού λοιπόν έχουμε ότι $\mathfrak{D} \supseteq \mathfrak{a}^{-1}\mathfrak{b}$, είναι όντος ιδεώδες και επίσης αφού το $\mathfrak{p}$ είναι πρώτο στον δακτύλιο ακεραίων $\mathfrak{D}$ θα είναι και μέγιστο, θα είναι $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{D}$ ή $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$. Δηλαδή $\mathfrak{b} = \mathfrak{a}$ ή $\mathfrak{b} = \mathfrak{ap}$. Επομένως δεν υπάρχει ιδεώδες $\mathfrak{b}$ μεταξύ των $\mathfrak{a}$ και $\mathfrak{ap}$. Αυτό σημαίνει ότι για κάθε στοιχείο $\alpha \in \mathfrak{a}/\mathfrak{ap}$ θα έχουμε

$$\mathfrak{ap} + \langle \alpha \rangle = \mathfrak{a}. \tag{3.3}$$

Παίρνουμε ένα τέτοιο α και ορίζουμε την απεικόνιση

$$\theta : \mathfrak{D} \longrightarrow \mathfrak{a}/\mathfrak{ap}$$

με

$$\theta(x) = \mathfrak{ap} + \alpha x,$$

η οποία είναι ένας $\mathfrak{D} - module$ ομομορφισμός, και επί λόγω της σχέσης 3.3. Ο πυρήνας του θ είναι ένα ιδεώδες το οποίο ικανοποιεί την $\mathfrak{p} \subseteq ker\theta$. Θα δείξουμε ότι $\mathfrak{p} \neq ker\theta$. Αν ήταν $\mathfrak{p} = ker\theta$ τότε σύμφωνα με το θεώρημα ομομορφισμού θα είχαμε

$$0 = \mathfrak{D}/ker\theta \cong \mathfrak{a}/\mathfrak{ap},$$

και τότε θα είχαμε $\mathfrak{a} = \mathfrak{ap}$ άτοπο, αφού έχουμε υποθέσει από την αρχή ότι $\mathfrak{a} \neq \mathfrak{ap}$. Το ιδεώδες $\mathfrak{p}$ είναι μέγιστο, άρα $\mathfrak{p} = ker\theta$. Επομένως με χρήση πάλι του θεωρήματος ομομορφισμού θα πάρουμε ότι

$$\mathfrak{D}/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}.$$

Εξισώνουμε τις τάξεις και παίρνουμε την σχέση 3.2. Με συνδυασμό των σχέσεων 2.1 και 1.1

$$|\mathfrak{D}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{a}||\mathfrak{D}/\mathfrak{p}|$$

και τέλος

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p}).$$

Παράδειγμα 3.3 *Στο παράδειγμα που είχαμε δακτύλιο ακεραίων τον* $\mathbb{Z}[\sqrt{-17}]$, *είχαμε τα ιδεώδη* $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-17}\rangle, \mathfrak{p}_2 = \langle 3, 1+\sqrt{-17}\rangle, \mathfrak{p}_3 = \langle 3, 1-\sqrt{-17}\rangle$. *Επομένως θα έχουμε*

$$N(\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2) = 2^2 3^2 3^2 = 18^2$$

Θα περιγράψουμε άλλη μία χρήση που θα κάνουμε με τον όρο «διαίρεση». Αν έχουμε $\mathfrak{a}$ ιδεώδες ενός δακτυλίου ακεραίων $\mathfrak{D}$ και b ένα στοιχείο του $\mathfrak{D}$ τέτοιο ώστε $\mathfrak{a} | \langle b \rangle$ τότε θα μπορούμε να γράφουμε και $\mathfrak{a}|b$ και θα λέμε ότι το $\mathfrak{a}$ θα διαιρεί το b. Προφανώς $\mathfrak{a}|b$ αν και μόνο αν $b \in \mathfrak{a}$. Αυτός ο νέος συμβολισμός έχει κάποια επιπλέον πλεονεκτήματα, όπως για παράδειγμα ότι αν έχουμε $\mathfrak{p}$ πρώτο ιδεώδες και $\mathfrak{p} | \langle a \rangle \langle b \rangle$, τότε θα πρέπει να είναι $\mathfrak{p} | \langle a \rangle$ ή $\mathfrak{p} | \langle b \rangle$. Άρα για $\mathfrak{p}$ πρώτο ιδεώδες είναι $\mathfrak{p}|ab \Rightarrow \mathfrak{p}|a$ ή $\mathfrak{p}|b$.

Θεώρημα 3.6 *Έστω* $\mathfrak{a}$ *ιδεώδες ενός δακτυλίου ακεραίων* $\mathfrak{D}$, *με* $\mathfrak{a} \neq 0$

1. *Αν* $N(\mathfrak{a})$ *είναι πρώτος αριθμός τότε και το* $\mathfrak{a}$ *είναι πρώτο ιδεώδες.*
2. *Η νόρμα* $N(\mathfrak{a})$ *είναι στοιχείο του* $\mathfrak{a}$, *ή ισοδύναμα* $\mathfrak{a} \mid N(\mathfrak{a})$.
3. *Αν* $\mathfrak{a}$ *πρώτο ιδεώδες,διαιρεί ακριβώς έναν πρώτο αριθμό* p, *και είναι* $N(\mathfrak{a}) = p^m$, *με* $m \leq n$, *όπου* n *ο βαθμός του* K.

Απόδειξη. Βλέπε θεώρημα 5.12 [1].

Παράδειγμα 3.4 *Αν έχουμε δακτύλιο ακεραίων τον* $\mathbb{Z}[\sqrt{-17}]$ *και ιδεώδες το* $\mathfrak{p} = \langle 2, 1+\sqrt{-17}\rangle$, *επειδή ξέρουμε ότι η νόρμα του ισούται με* 2 *που είναι πρώτος αριθμός, αμέσως μπορούμε να συμπεράνουμε ότι και το ιδεώδες* $\mathfrak{p}$ *είναι πρώτο. Επίσης παρατηρούμε ότι όπως μας λέει το παραπάνω θεώρημα* $N(\mathfrak{p}) = 2 \in \mathfrak{p}$.

Παράδειγμα 3.5 *Πρέπει επίσης να σημειώσουμε, ότι υπάρχουν περιπτώσεις όπου ένα ιδεώδες είναι πρώτο αλλά η νόρμα του δεν είναι πρώτος αριθμός. Για παράδειγμα έστω ότι έχουμε* $\mathfrak{D} = \mathbb{Z}[i]$, *και ιδεώδες* $\mathfrak{a} = \langle 3 \rangle$. *Το* 3 *είναι ανάγωγο στοιχείο στο* $\mathbb{Z}[i]$ *και επειδή είμαστε σε περιοχή μοναδικής ανάλυσης, θα είναι και πρώτο στοιχείο. Γνωρίζουμε ότι ένα πρώτο στοιχείο παράγει και πρώτο ιδεώδες, επομένως το* $\mathfrak{a}$ *είναι πρώτο ιδεώδες. Επίσης έχουμε ότι* $N(\langle 3 \rangle) = 3^2$, *ο οποίος δεν είναι πρώτος αριθμός. Βέβαια, η νόρμα ενός πρώτου ιδεώδους, θα είναι πάντα δύναμη πρώτου αριθμού.*

Θεώρημα 3.7

1. *Κάθε μη μηδενικό ιδεώδες ενός* $\mathfrak{D}$ *έχει πεπερασμένους διαιρέτες,*
2. *Ένας μη μηδενικός ακέραιος αριθμός ανήκει μόνο σε πεπερασμένο αριθμό ιδεωδών του* $\mathfrak{D}$,
3. *Μόνο πεπερασμένα το πλήθος ιδεώδη ενός* $\mathfrak{D}$ *έχουν την ίδια νόρμα.*

Απόδειξη.

1. Είναι άμεση συνέπεια του θεωρήματος ανάλυσης σε πρώτα ιδεώδη.
2. Είναι μία ειδική περίπτωση του 1.
3. Είναι άμεση συνέπεια του 2.

Παράδειγμα 3.6 *Παίρνουμε το προηγούμενο αποτέλεσμα της ανάλυσης του ιδεώδους* $\langle 18\rangle$ *στον* $\mathfrak{D} = \mathbb{Z}[\sqrt{-17}]$,

$$\langle 18\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$$

με $\mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-17}\right\rangle, \mathfrak{p}_2 = \left\langle 3, 1+\sqrt{-17}\right\rangle, \mathfrak{p}_3 = \left\langle 3, 1-\sqrt{-17}\right\rangle$. *Έχουμε βρει λοιπόν ότι οι μόνοι διαιρέτες του* $\langle 18\rangle$ *είναι τα* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$.*(Για το θεώρημα 3.7.1). Έχουμε ότι αν το 18 ανήκει σε κάποιο ιδεώδες* $\mathfrak{a}$, *όπου θα είναι* $\mathfrak{a}/\langle 18\rangle$ *δηλαδή* $\mathfrak{a} \mid \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ *τότε θα είναι* $\mathfrak{a} = \mathfrak{p}_1^q\mathfrak{p}_2^r\mathfrak{p}_3^s$, *όπου* q, r, s *προφανώς θα είναι 0,1, ή 2. Άρα το 18 ανήκει μόνο σε πεπερασμένα το πλήθος ιδεώδη. Ας δούμε πόσα ιδεώδη έχουν νόρμα 18. Αυτό γίνεται μόνο όταν* $\mathfrak{a} \mid 18$, *άρα αν* $\mathfrak{a} = \mathfrak{p}_1^q\mathfrak{p}_2^r\mathfrak{p}_3^s$ *που σημαίνει ότι* $N(\mathfrak{a}) = 2^q3^r3^s$. *Η* $N(\mathfrak{a})$ *θα είναι 18 μόνο αν έχουμε* $q = 1, r+s = 2$, *που με τη σειρά του σημαίνει ότι το* $\mathfrak{a}$ *είναι* $\mathfrak{p}_1\mathfrak{p}_2^2$, *ή* $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, *ή* $\mathfrak{p}_1\mathfrak{p}_3^2$.

Λήμμα 3.2 *Αν* $\mathfrak{a}, \mathfrak{b}$ *δύο μη μηδενικά ιδεώδη ενός* $\mathfrak{D}$, *τότε υπάρχει στοιχείο* $a \in \mathfrak{a}$ *τέτοιο ώστε*

$$a\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{D}$$

Πριν προχωρήσουμε στην απόδειξη του λήμματος θα δώσουμε τους ορισμούς του μέγιστου κοινού διαιρέτη και του ελάχιστου κοινού πολλαπλάσιου, δύο ιδεωδών.

Ορισμός 3.4 *Δύο μη μηδενικά ιδεώδη* $\mathfrak{a}, \mathfrak{b}$ *έχουν μέγιστο κοινό διαιρέτη* $\mathfrak{g}$ *και ελάχιστο κοινό πολλαπλάσιο* $\mathfrak{l}$ *με τις ακόλουθες ιδιότητες.*

$$\mathfrak{g}/\mathfrak{a}, \mathfrak{g}/\mathfrak{b}$$

και αν για κάποιο $\mathfrak{g}'$ *έχουμε ότι* $\mathfrak{g}' \mid \mathfrak{a},\ \mathfrak{g}' \mid \mathfrak{b}$, *τότε είναι*

$$\mathfrak{g}'/\mathfrak{g}$$

και αν

$$\mathfrak{a}/\mathfrak{l}, \mathfrak{b}/\mathfrak{l}$$

και αν για κάποιο l' *έχουμε ότι* $\mathfrak{a} \mid l',\ \mathfrak{b} \mid l'$ *τότε είναι*

$$l \mid l'.$$

Λήμμα 3.3 *Αν* $\mathfrak{a}, \mathfrak{b}$ *δύο ιδεώδη ενός* $\mathfrak{D}$, *και* g, l *ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο αντίστοιχα, τότε θα έχουμε*

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b}, \mathfrak{l} = \mathfrak{a} \cap \mathfrak{b}$$

Απόδειξη. Γνωρίζουμε ότι για ένα ιδεώδες $\mathfrak{x}$ έχουμε $\mathfrak{x} \mid \mathfrak{a}$ αν και μόνο αν $\mathfrak{a} \subseteq \mathfrak{x}$. Επομένως το $\mathfrak{g}$ πρέπει να είναι το μικρότερο ιδεώδες που περιέχει τα $\mathfrak{a}, \mathfrak{b}$ και το $\mathfrak{l}$ το μεγαλύτερο ιδεώδες που περιέχεται στα $\mathfrak{a}, \mathfrak{b}$.

Τώρα μπορούμε να δώσουμε την απόδειξη του λήμματος 3.2. *Απόδειξη.* Πρώτα παρατηρούμε ότι αν $a \in \mathfrak{a}$ θα έχουμε $\mathfrak{a}/a$ επομένως το $a\mathfrak{a}^{-1}$ είναι ιδεώδες και όχι απλά κλασματικό ιδεώδες. Τώρα σύμφωνα με το προηγούμενο λήμμα που αποδείξαμε, ο μέγιστος κοινός διαιρέτης των $a\mathfrak{a}^{-1}$ και $\mathfrak{b}$ θα είναι το $a\mathfrak{a}^{-1} + \mathfrak{b}$, επομένως αρκεί να επιλέξουμε $a \in \mathfrak{a}$ τέτοιο ώστε

$$a\mathfrak{a}^{-1} + \mathfrak{p}_i = \mathfrak{D}, i = 1, ..., r$$

με τα $\mathfrak{p}_i$ να είναι τα διαφορετικά μεταξύ τους πρώτα ιδεώδη, τα οποία διαιρούν το $\mathfrak{b}$.

Θεώρημα 3.8 *Έστω $\mathfrak{a}$ ένα μη μηδενικό ιδεώδες ενός δακτυλίου ακεραίων $\mathfrak{D}$, και ένα στοιχείο $b \in \mathfrak{a}$. Τότε υπάρχει στοιχείο $a \in \mathfrak{a}$ τέτοιο ώστε $\mathfrak{a} = \langle a, b \rangle$.*

Απόδειξη. Έστω ιδεώδες $\mathfrak{b} = b\mathfrak{a}^{-1}$. Από το λήμμα 3.2, θα υπάρχει στοιχείο $a \in \mathfrak{a}$ τέτοιο ώστε

$$a\mathfrak{a}^{-1} + \mathfrak{b} = a\mathfrak{a}^{-1} + b\mathfrak{a}^{-1} = \mathfrak{D} \Leftrightarrow (\langle a \rangle + \langle b \rangle)\mathfrak{a}^{-1} = \mathfrak{D} \Leftrightarrow \mathfrak{a} = \langle a \rangle + \langle b \rangle \Leftrightarrow \mathfrak{a} = \langle a, b \rangle$$

Αυτό το θεώρημα μας λέει ότι κάθε ιδεώδες, σε έναν δακτύλιο ακεραίων ενός σώματος αριθμών, θα έχει το πολύ δύο γεννήτορες.

Θεώρημα 3.9 *Η ανάλυση σε ανάγωγα των στοιχείων ενός $\mathfrak{D}$ είναι μοναδική αν και μόνο αν είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Γνωρίζουμε ότι κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής ανάλυσης. Μένει λοιπόν να δείξουμε το αντίστροφο. Αρκεί να δείξουμε ότι μία περιοχή όπου η ανάλυση σε ανάγωγα στοιχεία είναι μοναδική, είναι και περιοχή κυρίων ιδεωδών. Δηλαδή ότι κάθε πρώτο ιδεώδες είναι κύριο, αφού κάθε ιδεώδες είναι γινόμενο πρώτων ιδεωδών. Έστω λοιπόν $\mathfrak{p} \in \mathfrak{D}$ πρώτο ιδεώδες, μη μηδενικό. Από το θεώρημα 3.6.2, υπάρχει ένας ακέραιος αριθμός $N = N(\mathfrak{p})$ τέτοιος ώστε $\mathfrak{p} \mid N$. Μπορούμε να παραγοντοποιήσουμε το N σαν γινόμενο αναγώγων στοιχείων του $\mathfrak{D}$, ως εξής:

$$N = v_1 ... v_s.$$

Αφού έχουμε ότι $\mathfrak{p} \mid N$ και το $\mathfrak{p}$ είναι πρώτο ιδεώδες, έχουμε ότι

$$\mathfrak{p} \mid v_i \text{ ή ισοδύναμα } \mathfrak{p} \mid \langle v_i \rangle .$$

Επειδή είμαστε σε περιοχή μοναδικής ανάλυσης, το ανάγωγο στοιχείο v_i είναι και πρώτο στοιχείο. Άρα και το κύριο ιδεώδες που παράγει το στοιχείο αυτό, είναι πρώτο. Επομένως έχουμε ότι $\mathfrak{p} \mid \langle v_i \rangle$ όπου και τα δύο αυτά ιδεώδη είναι πρώτα. Έτσι από μοναδικότητα ανάλυσης έχουμε ότι

$$\mathfrak{p} = \langle v_i \rangle ,$$

δηλαδή το $\mathfrak{p}$ είναι κύριο ιδεώδες.

Κεφάλαιο 4

Πλέγματα

Σε αυτό το σημείο θα αλλάξει λίγο το σκηνικό, αφού θα χρειαστεί να πάρουμε πληροφορίες από γεωμετρικές τεχνικές, οι οποίες θα βοηθήσουν τις αλγεβρικές μεθόδους μας. Θα αναπτύξουμε κάποιες ιδιότητες των πλεγμάτων, τα οποία είναι θεμελιώδη για την έννοια μιας ελλειπτικής καμπύλης. Θα μιλήσουμε και για την αντιστοιχία μιας θεμελιώδους περιοχής και ενός τόρου με ένα πλέγμα. Ξεκινάμε με τον ορισμό ενός πλέγματος (lattice).

Ορισμός 4.1 *Έστω $e_1, ..., e_m$ να είναι ένα σύνολο από γραμμικά ανεξάρτητα διανύσματα του $\mathbb{R}^n, m \leq n$. Η προσθετική υποομάδα του $(\mathbb{R}^n, +)$ η οποία παράγεται από αυτά τα διανύσματα, ονομάζεται πλέγμα διάστασης m, παραγόμενο από τα $e_1, ..., e_m$.*

Μπορούμε να δούμε ένα πλέγμα σαν μία ελεύθερη αβελιανή ομάδα, τάξης m. Άρα μπορούμε να εφαρμόσουμε την ορολογία των ομάδων αυτών, στα πλέγματα. Ας δώσουμε τώρα τοπολογικό χαρακτηρισμό στο πλέγμα. Έστω ο $\mathbb{R}^n$ εφοδιασμένος με τη συνήθη μετρική, όπου $||x - y||$ είναι η απόσταση μεταξύ του x και του y. Θα συμβολίζουμε επίσης με $B_r[x]$, την κλειστή μπάλα κέντρου x και ακτίνας r.

Ορισμός 4.2 *Θα λέμε ότι ένα σύνολο $X \subseteq \mathbb{R}^n$ είναι φραγμένο, αν $X \subseteq B_r[0]$, για κάποιο r.*

Ορισμός 4.3 *Θα λέμε ότι ένα σύνολο $X \subseteq \mathbb{R}^n$, το οποίο έχει δομή ομάδας είναι διακριτό, αν και μόνο αν το μηδέν δεν είναι σημείο συσσώρευσης, δηλαδή κάθε μπάλα $B_r[0]$ θα τέμνει το σύνολο X σε πεπερασμένα το πλήθος σημεία.*

Είμαστε έτοιμοι τώρα να δώσουμε το παρακάτω θεώρημα.

Θεώρημα 4.1 *Μία προσθετική υποομάδα του $\mathbb{R}^n$ θα είναι πλέγμα , αν και μόνο αν είναι διακριτή.*

Απόδειξη. Έστω L ένα πλέγμα διάστασης n, το οποίο παράγεται από τα $e_1, ..., e_n$. Αυτά τα διανύσματα τότε θα αποτελούν μία βάση για τον χώρο $\mathbb{R}^n$. Κάθε στοιχείο $v \in \mathbb{R}^n$, θα γράφεται σαν

$$v = \lambda_1 e_1 + ... + \lambda_n e_n, \lambda_i \in \mathbb{R}.$$

Ορίζουμε την $f : \mathbb{R}^n \to \mathbb{R}^n$ να είναι η

$$f(\lambda_1 e_1 + ... + \lambda_n e_n) = (\lambda_1, ..., \lambda_n).$$

Τότε το $f(B_r[0])$ είναι φραγμένο, έστω $||f(v)|| \leq k, v \in \mathbb{R}^n$. Αν τώρα έχουμε κάποιο $\sum a_i e_i \in B_r[0], a_i \in \mathbb{Z}$, τότε προφανώς θα είναι $||(a_1, ..., a_n)|| \leq k$. Αντίστροφα, έστω G μία διακριτή υποομάδα του $\mathbb{R}^n$. Θα δείξουμε με επαγωγή στο n, ότι η G είναι πλέγμα. Έστω $g_1, ..., g_m$ το μέγιστο γραμμικά ανεξάρτητο υποσύνολο του G. Έστω V ο υπόχωρος τώρα, που παράγεται από τα $g_1, ..., g_{m-1}$. Θέτουμε $G_0 = G \cap V$. Υπάρχουν λοιπόν γραμμικά ανεξάρτητα στοιχεία $h_1, ..., h_{m'}$ τα οποία παράγουν την G_0. Αφού τα στοιχεία $g_1, ..., g_m \in G_0$, τότε θα πρέπει να έχουμε $m' = m - 1$. Μπορούμε να αντικαταστήσουμε τα $g_1, ..., g_{m-1}$ με τα $h_1, ..., h_{m-1}$, ή ισοδύναμα να υποθέσουμε ότι κάθε στοιχείο που ανήκει στην G_0 μπορεί να γραφεί σαν ακέραιος γραμμικός συνδυασμός των $g_1, ..., g_{m-1}$. Έστω τώρα T, το υποσύνολο όλων των $x \in G$ της μορφής,

$$x = a_1 g_1 + ... + a_m g_m,$$

με $a_i \in \mathbb{R}$ τέτοια ώστε $0 \leq a_i < 1, i = 1, ..., m-1$ και $0 \leq a_m < 1$. Τότε το T θα είναι φραγμένο και άρα πεπερασμένο αφού το G είναι διακριτό σύνολο. Μπορούμε λοιπόν να επιλέξουμε $x' \in T$ με τον μικρότερο συντελεστή a_m, έστω

$$x' = b_1 g_1 + ... + b_m g_m.$$

Προφανώς τα $g_1, ..., g_{m-1}, x'$ είναι γραμμικά ανεξάρτητα. Ξεκινώντας με οποιοδήποτε διάνυσμα $v \in G$, μπορούμε να επιλέξουμε ακέραιους συντελεστές c_i, τέτοιους ώστε το στοιχείο

$$g' = g - c_m x' - c_1 g_1 - ... - c_{m-1} g_{m-1}$$

να ανήκει στο T και ο συντελεστής του g_m στο g' να είναι μικρότερος του b_m, αλλά φυσικά μη αρνητικός. Από την επιλογή του x' αυτός ο συντελεστής θα πρέπει να είναι μηδέν. Επομένως $g' \in G_0$. Τότε όμως τα $\{x', g_1, ..., g_{m-1}\}$ παράγουν την G, που σημαίνει ότι η G είναι πλέγμα.

Το υποσύνολο T που ορίσαμε στην προηγούμενη απόδειξη, είναι η λεγόμενη θεμελιώδης περιοχή και δίνουμε τον ακριβή ορισμό της αμέσως τώρα.

Ορισμός 4.4 *Αν έχουμε L ένα πλέγμα που παράγεται από τα $e_1, ..., e_n$, ορίζουμε τη θεμελιώδη περιοχή T να αποτελείται από όλα εκείνα τα στοιχεία της μορφής $\sum a_i e_i,\ a_i \in \mathbb{R}$, για τα οποία έχουμε $0 \leq a_i < 1$.*

Λήμμα 4.1 *Κάθε στοιχείο του $\mathbb{R}^n$ ανήκει σε ακριβώς ένα από τα σύνολα $T + l, l \in L$.*

4.1 Ο τόρος πηλίκο

Έστω L ένα πλέγμα στο $\mathbb{R}^n$ και διάστασης n. Αυτό που θα μας απασχολήσει είναι η μελέτη της ομάδας πηλίκο $\mathbb{R}^n/L$. Θα συμβολίζουμε με S το σύνολο των μιγαδικών αριθμών με μέτρο 1. Αυτό το σύνολο, εφοδιασμένο με τον πολλαπλασιασμό είναι ομάδα και ονομάζεται ομάδα των σημείων του κύκλου.

Λήμμα 4.2 *Η ομάδα πηλίκο $\mathbb{R}/\mathbb{Z}$ είναι ισόμορφη με την ομάδα S.*

Απόδειξη. Ορίζουμε την απεικόνιση $\phi : \mathbb{R} \to S$ με

$$\phi(x) = e^{2\pi i x}.$$

Αυτός ο ϕ είναι ένας επί ομομορφισμός και έχει προφανώς πυρήνα το $\mathbb{Z}$. Τέλος από το θεμελιώδες ομομορφισμού θα έχουμε ότι υπάρχει ένας ισομορφισμός από το $\mathbb{R}/\mathbb{Z}$ στο S.

Για να συνεχίσουμε πρέπει να ορίσουμε τον n-διάστατο τόρο T^n. Αυτό είναι το ευθύ γινόμενο της ομάδας του κύκλου S, n φορές. Για παράδειγμα έχουμε $T^2 = S \times S$, ο οποίος καλείται συνήθης τόρος.

Θεώρημα 4.2 *Έστω πλέγμα L του $\mathbb{R}^n$, διάστασης n. Τότε το $\mathbb{R}^n/L$ είναι ισόμορφο με τον n-διάστατο τόρο T^n.*

Απόδειξη. Έστω οι γεννήτορες του $L, \{e_1, ..., e_n\}$, οι οποίοι αποτελούν και μία βάση για το $\mathbb{R}^n$. Ορίζουμε τον $\phi : \mathbb{R}^n \to T^n$, με

$$\phi(a_1 e_1 + ... + a_n e_n) = (e^{2\pi i a_1}, ..., e^{2\pi i a_n}).$$

Ο ϕ είναι ένας επί ομομορφισμός και έχει πυρήνα το L, οπότε όπως και στην προηγούμενη απόδειξη και σύμφωνα με το θεμελιώδες θεώρημα του ισομορφισμού, θα έχουμε ότι $\mathbb{R}^n/L \cong T^n$.

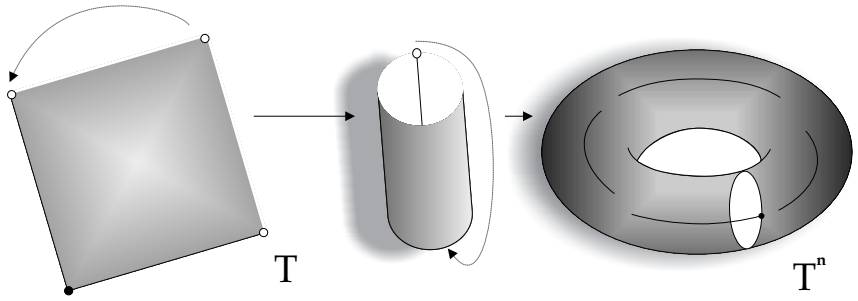
Ας δούμε τι συμβαίνει όταν το L έχει διάσταση $m \leq n$.

Θεώρημα 4.3 *Έστω L πλέγμα του $\mathbb{R}^n$, διάστασης $m \leq n$. Τότε το $\mathbb{R}^n/L$ είναι ισόμορφο με το $T^m \times \mathbb{R}^{n-m}$.*

Απόδειξη. Έστω V ο υπόχωρος που παράγεται από το L. Επιλέγουμε ένα συμπλήρωμά του W, τέτοιο ώστε $\mathbb{R}^n = V \oplus W$. Τότε θα έχουμε $L \subset V$, $V/L \cong T^m$ από το θεώρημα 4.2, θα είναι $W \cong \mathbb{R}^{n-m}$ και παίρνουμε το ζητούμενο.

Λήμμα 4.3 *Ο ομομορφισμός ϕ που ορίσαμε στο θεώρημα 4.2, αν περιοριστεί στη θεμελιώδη περιοχή T, επάγει μία ένα προς ένα και επί απεικόνιση*

$$\phi : T \to T^n.$$



Σχήμα 4.1:

Με τη βοήθεια του λήμματος 4.3 θα δώσουμε έναν ορισμό για τον όγκο $v(X)$, ενός υποσυνόλου X του T^n. Γενικά ο όγκος $v(X)$ ενός υποσυνόλου $X \subseteq \mathbb{R}^n$, ορίζεται όπως συνήθως, αρκεί δηλαδή να υπάρχει το πολλαπλό ολοκλήρωμα

$$v(X) = \int_X dx_1 ... dx_n.$$

Έστω πλέγμα $L \subseteq \mathbb{R}^n$, διάστασης n, τέτοιο ώστε $\mathbb{R}^n/L \cong T^n$. Έστω επίσης ότι η θεμελιώδης περιοχή του L, να είναι η T. Σύμφωνα με το λήμμα 4.3, υπάρχει υπάρχει μία ένα προς ένα και επί απεικόνιση $\phi : T \to T^n$. Για κάθε X υποσύνολο του T^n, ορίζουμε τον όγκο $v(X)$ να είναι

$$v(X) = v(\phi^{-1}(X)),$$

ο οποίος υπάρχει μόνο αν το $\phi^{-1}(X)$ έχει όγκο στο $\mathbb{R}^n$.

Θεώρημα 4.4 *Αν X ένα φραγμένο υποσύνολο του $\mathbb{R}^n$ και υπάρχει ο $v(X)$, και αν $v(\eta(X)) \neq v(X)$, όπου $\eta : \mathbb{R}^n \to T^n$ ο φυσικός ομομορφισμός, τότε ο $\eta|_X$ δεν είναι ένα προς ένα.*

Απόδειξη. Ας υποθέσουμε λοιπόν ότι ο $\eta|_X$ είναι ένα προς ένα. Αφού τώρα το σύνολο X είναι φραγμένο θα τέμνει πεπερασμένα το πλήθος σύνολα της μορφής $T+l$, όπου $l \in L$ και T θεμελιώδης περιοχή. Θέτουμε $X_l = X \cap (T+l)$. Τότε θα έχουμε $X = X_{l_1} \cup ... \cup X_{l_n}$. Για κάθε l_i ορίζουμε $Y_{l_i} = X_{l_i} - l_i$, έτσι ώστε $Y_{l_i} \subseteq T$. Εμείς ισχυριζόμαστε ότι τα Y_{l_i} είναι ξένα μεταξύ τους. Αφού $v(x - l_i) = v(x)$, για κάθε $x \in \mathbb{R}^n$ αυτό έπεται από το ότι έχουμε υποθέσει ότι ο η είναι ένα προς ένα. Είναι

$$v(X_{l_i}) = v(Y_{l_i}),$$
$$\eta(X_{l_i}) = \phi(Y_{l_i}),$$

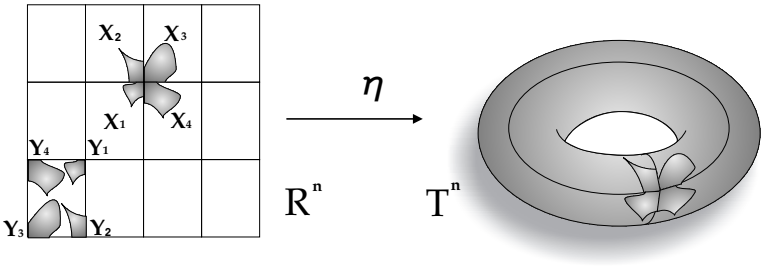
όπου ϕ η ένα προς ένα και επί συνάρτηση, $T \to T^n$. Και έχουμε

$$v(\eta(X)) = v(\eta(\cup X_{l_i})) = v(\cup Y_{l_i}) = \sum v(Y_{l_i})$$

αφού είναι ξένα. Συνεχίζοντας, είναι

$$v(Y_{l_i}) = \sum v(X_{l_i}) = v(X),$$

όπου ερχόμαστε σε αντίθεση με την αρχική μας υπόθεση.



Σχήμα 4.2:

4.2 Το θεώρημα του Minkowski

Ο σκοπός αυτής της παραγράφου είναι να αποδείξουμε το θεώρημα του Minkowski. Αυτό έχει να κάνει με την ύπαρξη ενός μη μηδενικού σημείου ενός πλέγματος, μέσα σε ένα κατάλληλο σύνολο X. Αρκεί ο όγκος του X να είναι αρκετά μεγάλος, σχετικά με αυτόν της θεμελιώδης περιοχής του πλέγματος. Δίνουμε δύο ορισμούς και έπειτα συνεχίζουμε με την απόδειξη του θεωρήματος του Minkowski.

Ορισμός 4.5 *Ένα υποσύνολο X του $\mathbb{R}^n$, ονομάζεται κυρτό, αν για $x, y \in X$, όλα τα σημεία που ανήκουν στην ευθεία που τα ενώνει, να ανήκουν και αυτά μέσα στο X. Δηλαδή, ένα σύνολο X ονομάζεται κυρτό, αν για $x, y \in X$, το σημείο $\lambda x + (1-\lambda)y, 0 \leq \lambda \leq 1$, να ανήκει στο X.*

Ορισμός 4.6 *Ένα $X \subseteq \mathbb{R}^n$ ονομάζεται συμμετρικό αν $x \in X$ έπεται ότι $-x \in X$.*

Θεώρημα 4.5 *(Το θεώρημα του Minkowski). Έστω L πλέγμα διάστασης n, του $\mathbb{R}^n$, με θεμελιώδη περιοχή T. Έστω επίσης X ένα φραγμένο, κυρτό και συμμετρικό υποσύνολο του $\mathbb{R}^n$. Αν $v(X) > 2^n v(T)$, τότε το X περιέχει ένα μη μηδενικό σημείο του L.*

Απόδειξη. Θα θεωρήσουμε το διπλάσιο πλέγμα $2L$ και $2T$ η θεμελιώδης περιοχή του, με όγκο $2^n v(T)$. Έστω ο τόρος $T^n = \mathbb{R}^n/2L$. Είναι λοιπόν

$$v(T^n) = v(2T) = 2^n v(T).$$

Ο φυσικός ομομορφισμός $\eta : \mathbb{R}^n \to T^n$ δεν είναι δυνατόν να διατηρεί τον όγκο του X, αφού από την υπόθεση είναι μεγαλύτερος από τον όγκο $v(T^n)$. Έχουμε επίσης ότι $\eta(X) \subseteq T^n$, άρα θα είναι

$$v(\eta(X)) \leq v(T^n) = 2^n v(T < v(X)).$$

Σύμφωνα με το θεώρημα 4.4, ο $\eta|_X$ δεν είναι ένα προς ένα. Επομένως υπάρχουν $x_1, x_2 \in X$ με $x_1 \neq x_2$, τέτοια ώστε

$$\eta(x_1) = \eta(x_2) \Leftrightarrow x_1 - x_2 \in 2L.$$

Έχουμε ότι αφού το X είναι συμμετρικό $x_2 \in X \Rightarrow -x_2 \in X$ και από κυρτότητα

$$\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X \Leftrightarrow \frac{1}{2}(x_1 - x_2) \in X.$$

Αλλά αφού όπως δείξαμε πριν $x_1 - x_2 \in 2L$ θα έχουμε ότι $\frac{1}{2}(x_1 - x_2) \in L$. Τέλος αφού $x_1 \neq x_2$ θα έχουμε ότι $\frac{1}{2}(x_1 - x_2) \neq 0$.

Ας δούμε μία εφαρμογή του θεωρήματος του Minkowski, στη θεωρία αριθμών.

Θεώρημα 4.6 *(Το θεώρημα των δύο τετραγώνων.) Αν έχουμε έναν πρώτο αριθμό $p = 4k + 1$, τότε αυτός ο πρώτος ισούται με το άθροισμα δύο τετραγώνων ακέραιων αριθμών.*

Απόδειξη. Γνωρίζουμε ότι η τάξη της $G = (\mathbb{Z}_p, \cdot)$, είναι $p - 1 = 4k$. Επομένως θα περιέχει σίγουρα ένα στοιχείο u τάξης 4 και σίγουρα το μόνο στοιχείο τάξης 2 είναι το -1. Επομένως $(-1)^2 \equiv 1 \bmod p$ και $u^4 \equiv 1 \bmod p$. Άρα $u^4 \equiv (-1)^2 \bmod p \Leftrightarrow u^2 \equiv (-1) \bmod p$. Έστω $L \subseteq \mathbb{Z}^2$ να είναι το πλέγμα του $\mathbb{R}^2$, το οποίο αποτελείται από όλα τα ζεύγη $(a, b), a, b \in \mathbb{Z}$, τέτοια ώστε $b \equiv ua \bmod p$. Αυτή είναι μια υποομάδα του $\mathbb{Z}^2$ με δείκτη p. Επομένως η θεμελιώδης ομάδα του L θα έχει όγκο p. Από το θεώρημα του Minkowski, αν πάρουμε οποιονδήποτε κύκλο με κέντρο την αρχή των αξόνων και ακτίνα r, ο οποίος έχει επιφάνεια $\pi r^2 > 4p$, θα περιέχει ένα μη μηδενικό σημείο του L. Η τιμή του r^2 για να ισχύει αυτό, θα πρέπει να είναι ίση με $\frac{3p}{2}$. Έχουμε λοιπόν, ότι θα υπάρχει ένα σημείο $(a, b) \in L$ για το οποίο

$$0 \neq a^2 + b^2 \leq r^2 = \frac{3p}{2} < 2p.$$

Παίρνουμε το $a^2 + b^2 \bmod p \equiv a^2 + u^2 a^2 \bmod p \equiv a^2 - a^2 \equiv 0 \bmod p$ που σημαίνει ότι το $a^2 + b^2$ είναι πολλαπλάσιο του p, αλλά σίγουρα μεγαλύτερο του μηδέν και μικρότερο, όπως δείξαμε πριν, του $2p$. Επομένως $a^2 + b^2 = p$, το οποίο ήταν και το ζητούμενο.

4.3 Ο χώρος L^{st}

Σε αυτήν την παράγραφο θα μιλήσουμε για γεωμετρικές απεικονίσεις αλγεβρικών αριθμών. Θα αναπτύξουμε μία μέθοδο όπου θα εμφυτεύσουμε ένα σώμα αριθμών K, σε έναν πραγματικό διανυσματικό χώρο, με διάσταση όσος ο βαθμός του K. Αυτό θα γίνει με τέτοιον τρόπο ώστε τα ιδεώδη του K να απεικονίζονται σε πλέγματα μέσα στον διανυσματικό χώρο. Θα χρειαστούμε τη βοήθεια των μονομορφισμών από το K στο $\mathbb{C}$, και θα πρέπει να διαχωρίσουμε αυτούς που στέλνουν το K στο $\mathbb{R}$, από τους υπόλοιπους. Έστω λοιπόν $K = \mathbb{Q}(\theta), \theta \in \mathbb{B}$, σώμα αριθμών βαθμού n και $\sigma_1, ..., \sigma_n$ οι μονομορφισμοί από το $K \to \mathbb{C}$. Αν έχουμε ότι $\sigma_i(K) \subseteq \mathbb{R}$, το οποίο συμβαίνει μόνο όταν το $\sigma_i(\theta) \in \mathbb{R}$ θα λέμε ότι ο σ_i είναι πραγματικός, αλλιώς ότι είναι μιγαδικός. Όπως πάντα το μιγαδικό συζυγές θα το συμβολίζουμε με μπάρα και ορίζουμε

$$\overline{\sigma_i}(a) = \overline{\sigma_i(a)}.$$

Αφού το μιγαδικό συζυγές είναι ένας αυτομορφισμός του $\mathbb{C}$, θα έχουμε ότι το $\overline{\sigma_i}$ θα είναι ένας μονομορφισμός από το K στο $\mathbb{C}$ και θα είναι ίσο με κάποιο σ_j. Οπότε οι μιγαδικοί μονομορφισμοί είναι σε συζυγή ζεύγη. Επομένως $n = s + 2t$, όπου s είναι το πλήθος των πραγματικών μονομορφισμών και $2t$ το πλήθος των μιγαδικών. Από εδώ και πέρα αυτός θα είναι ο τρόπος με τον οποίο θα αριθμούμε τους μονομορφισμούς από το K στο $\mathbb{C}$. Είναι

$$\sigma_1, ..., \sigma_s; \sigma_{s+1}, \overline{\sigma}_{s+1}, ..., \sigma_{s+t}, \overline{\sigma}_{s+t}.$$

Προφανώς τα $\sigma_1, ..., \sigma_s$ είναι πραγματικοί και οι υπόλοιποι είναι οι μιγαδικοί. Είμαστε τώρα σε θέση να ορίσουμε τον χώρο L^{st}.

Ορισμός 4.7 *Ορίζουμε*

$$L^{st} = \mathbb{R}^s \times \mathbb{C}^t,$$

το σύνολο όλων των $s+t$-άδων

$$x = (x_1, ..., x_s; x_{s+1}, ..., x_{s+t}),$$

όπου $x_1, ..., x_s \in \mathbb{R}$ και $x_{s+1}, ..., x_{s+t} \in \mathbb{C}$. Ο χώρος L^{st} λοιπόν είναι ένας διανυσματικός χώρος πάνω από το $\mathbb{R}$, διάστασης $s + 2t = n$.

Ορίζουμε την νόρμα ενός στοιχείου $x \in L^{st}$ να είναι η

$$N(x) = x_1...x_s|x_{s+1}|^2...|x_{s+t}|^2.$$

Έχουμε δύο προφανείς ιδιότητες αυτής της νόρμας.

1. $N(x) \in \mathbb{R}$ για κάθε x,
2. $N(xy) = N(x)N(y)$.

Ορίζουμε την απεικόνιση $\sigma : K \to L^{st}$ με

$$\sigma(a) = (\sigma_1(a), ..., \sigma_s(a); \sigma_{s+1}(a), ..., \sigma_{s+t}(a)), a \in K.$$

Προφανώς θα ισχύει

$$\sigma(a + b) = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = \sigma(a)\sigma(b),$$

για κάθε $a, b \in K$. Οπότε ο σ είναι ομομορφισμός δακτυλίου. Επιπλέον θα έχουμε $N(\sigma(a)) = N(a)$, αφού έχουμε ορίσει

$$N(a) = \sigma_1(a)...\sigma_s(a)\sigma_{s+1}(a)\overline{\sigma}_{s+1}(a)...\sigma_{s+t}(a)\overline{\sigma}_{s+t}(a).$$

Ας δούμε ένα παράδειγμα.

Παράδειγμα 4.1 *Έστω $K = \mathbb{Q}(\theta)$ με το θ να ικανοποιεί το $\theta^3 - 2 = 0$. Τα συζυγή στοιχεία του θ είναι $\theta, \omega\theta, \omega^2\theta$, με ω μία κυβική ρίζα της μονάδας. Οι μονομορφισμοί $\sigma_i : K \to \mathbb{C}$ είναι οι*

$$\sigma_1(\theta) = \theta, \sigma_2(\theta) = \omega\theta, \overline{\sigma}_2(\theta) = \omega^2\theta.$$

Επομένως σε αυτήν την περίπτωση θα είναι $s = 1, t = 1$. Ένα στοιχείο $x \in K$ με $x = q + r\theta + s\theta^2, q, r, s \in \mathbb{Q}$, θα απεικονίζεται στον $L^{1,1}$ σύμφωνα με

$$\sigma(x) = (q + r\theta + s\theta^2, q + r\omega\theta + s\omega^2\theta^2)$$

Θεώρημα 4.7 *Αν $a_1, ..., a_n$ είναι μία βάση για το K πάνω από το $\mathbb{Q}$, τότε τα $\sigma(a_1), ..., \sigma(a_n)$ είναι γραμμικά ανεξάρτητα πάνω από το $\mathbb{R}$.*

Απόδειξη. Έχουμε

$$\sigma_k(\alpha_l) = x_k^{(l)},$$
$$\sigma_{s+j}(\alpha_l) = y_j^{(l)} + iz_j^{(l)}$$

με $k = 1, ..., s,\ j = 1, ..., t$ και $x_k^{(l)},\ y_k^{(l)},\ z_k^{(l)} \in \mathbb{R}$. Τότε θα είναι

$$\sigma(\alpha_l) = (x_1^{(l)}, ..., x_s^{(l)}; y_1^{(l)} + iz_1^{(l)}, ..., y_t^{(l)} + z_t^{(l)}),$$

και αρκεί να δείξουμε ότι η διακρίνουσα

$$D = \begin{vmatrix} x_1^{(1)}...x_s^{(1)}y_1^{(1)}z_1^{(1)}...y_t^{(1)}z_t^{(1)} \\ .... \\ x_1^{(n)}...x_s^{(n)}y_1^{(n)}z_1^{(n)}...y_t^{(n)}z_t^{(n)} \end{vmatrix}$$

να είναι διάφορη του μηδενός. Θέτουμε :

$$E = \begin{vmatrix} x_1^{(1)}...x_s^1 & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & ... \\ ... & & & \\ x_1^{(n)}...x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & ... \end{vmatrix}$$
$$= \begin{vmatrix} \sigma_1(\alpha_1)... & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \bar{\sigma}_{s+1}(\alpha_1) & ... \\ & & ... & & \\ \sigma_1(\alpha_n) & ... & \sigma_s(\alpha_n)\sigma_{s+1}(\alpha_n) & \bar{\sigma}_{s+1}(\alpha_n) & ... \end{vmatrix}.$$

Τότε από τον ορισμό της διακρίνουσας και το θεώρημα 1.6, έχουμε $E \neq 0$. Τέλος από ιδιότητες διακρινουσών, θα πάρουμε ότι τελικά είναι

$$E = (-2i)^t D,$$

επομένως $D \neq 0$.

Πόρισμα 4.1 *$\mathbb{Q}$-γραμμικά ανεξάρτητα στοιχεία του K, απεικονίζονται μέσω του σ σε $\mathbb{R}$-γραμμικά ανεξάρτητα στοιχεία του L^{st}.*

Πόρισμα 4.2 *Αν G μία πεπερασμένα παραγόμενη υποομάδα του $(K, +)$ με βάση ακεραιότητας $\{a_1, ..., a_m\}$, τότε η εικόνα της G στο L^{st}, είναι ένα πλέγμα με γεννήτορες $\sigma(a_1), ..., \sigma(a)_m$.*

Κεφάλαιο 5

Ομάδα κλάσεων και αριθμός κλάσεων.

Σε αυτό το κεφάλαιο θα μελετήσουμε την class group ενός σώματος αριθμών. Αυτή είναι το πηλίκο της ομάδας των κλασματικών ιδεωδών προς την υποομάδα των κύριων κλασματικών ιδεωδών. Class number θα καλούμε την τάξη αυτής της ομάδας. Ουσιαστικά η ομάδα αυτή μετράει πόσα ιδεώδη μπορεί να μην είναι κύρια, δηλαδή σε ποιον βαθμό η παραγοντοποίηση είναι μοναδική. Πιο συγκεκριμένα, όπως θα δούμε και παρακάτω, η ανάλυση των στοιχείων ενός $\mathfrak{D}$ είναι μοναδική αν η class number είναι ίση με 1. Αλλά ας τα δούμε όλα αυτά πιο αναλυτικά.

5.1 Η ομάδα κλάσεων

Ορισμός 5.1 *Έστω K σώμα αριθμών και $\mathfrak{D}$ ο δακτύλιος των ακεραίων του. Θα συμβολίζουμε με $\mathcal{F}$ την ομάδα των κλασματικών ιδεωδών του, με πράξη τον πολλαπλασιασμό. Έστω επίσης $\mathcal{P}$ η ομάδα των κύριων κλασματικών ιδεωδών. Ορίζουμε σαν class group του $\mathfrak{D}$ να είναι η ομάδα πηλίκο*

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

Η τάξη αυτής της ομάδας θα συμβολίζεται με $h = h(\mathfrak{D})$.

Θα δώσουμε τον ορισμό της class group χρησιμοποιώντας λίγο διαφορετικούς όρους. Θα λέμε ότι δύο κλασματικά ιδεώδη είναι ισοδύναμα, αν και τα δύο στέλνουν την εικόνα τους στο ίδιο στοιχείο της $\mathcal{F}/\mathcal{P}$. Αν λοιπόν δύο κλασματικά ιδεώδη $\mathfrak{a}, \mathfrak{b}$ είναι ισοδύναμα θα έχουμε $\mathfrak{a} \sim \mathfrak{b}$ και θα συμβολίζουμε την κλάση ισοδυναμίας του $\mathfrak{a}$, με $[\mathfrak{a}]$. Η $\mathcal{H}$ είναι το σύνολο όλων αυτών των κλάσεων ισοδυναμίας. Αν έχουμε $\mathfrak{a}$ κλασματικό ιδεώδες θα είναι $\mathfrak{b} = c\mathfrak{a}, c \in \mathfrak{D}$ και $\mathfrak{b}$ ιδεώδες. Είναι $\mathfrak{b} = \langle c \rangle \mathfrak{a}$. Από την στιγμή τώρα που το $\langle c \rangle \in \mathcal{P}$, θα έχουμε ότι τα $\mathfrak{a}$ και $\mathfrak{b}$ είναι ισοδύναμα. Με λίγα λόγια, οποιαδήποτε κλάση ισοδυναμίας, θα περιέχει ένα ιδεώδες.

Έστω ότι έχουμε δύο ισοδύναμα ιδεώδη $\mathfrak{x}, \mathfrak{y}$. Τότε θα είναι $\mathfrak{x} = \mathfrak{c}\mathfrak{y}$ με $\mathfrak{c}$ ένα κύριο κλασματικό ιδεώδες, έστω $\mathfrak{c} = d^{-1}\mathfrak{e}, d \in \mathfrak{D}, \mathfrak{e}$ ένα κύριο ιδεώδες. Επομένως θα είναι $\mathfrak{x} \langle d \rangle = \mathfrak{y}\mathfrak{e}$. Αντίστροφα, αν υποθέσουμε ότι έχουμε $\mathfrak{x}\mathfrak{d} = \mathfrak{y}\mathfrak{e}$ με $\mathfrak{d}, \mathfrak{e}$ κύρια ιδεώδη, τότε προφανώς θα είναι $\mathfrak{x} \sim \mathfrak{y}$. Αυτό μας επιτρέπει να περιγράψουμε την $\mathcal{H}$ ως εξής: παίρνουμε όλα τα ιδεώδη $\mathcal{F}$ και ορίζουμε την σχέση $\sim$ με $\mathfrak{x} \sim \mathfrak{y}$, αν

και μόνο αν $\mathfrak{xd} = \mathfrak{ye}$. Τότε η $\mathcal{H}$ θα είναι το σύνολο των κλάσεων ισοδυναμίας $[\mathfrak{x}]$, με πράξη ομάδας η οποία ορίζεται από την $[\mathfrak{x}][\mathfrak{y}] = [\mathfrak{xy}]$. Αυτός είναι και ο λόγος που η $\mathcal{H}$ ονομάζεται class group.

Θεώρημα 5.1 *Η παραγοντοποίηση στον $\mathfrak{D}$ είναι μοναδική, αν και μόνο αν η τάξη της $\mathcal{H}$ είναι ίση με 1.*

Απόδειξη. Όπως έχουμε ήδη δείξει, η παραγοντοποίηση είναι μοναδική αν και μόνο αν κάθε ιδεώδες του $\mathfrak{D}$, είναι κύριο, δηλαδή αν κάθε κλασματικό ιδεώδες είναι κύριο. Δηλαδή $\mathcal{F} = \mathcal{P}$, που σημαίνει ότι $h = |\mathcal{H}| = 1$.

Από εδώ και πέρα θα αναλωθούμε στο να δείξουμε ότι η τάξη της ομάδας κλάσεων, είναι πεπερασμένη. Σε αυτό θα μας βοηθήσει το θεώρημα του Minkowski.

5.2 Ένα θεώρημα ύπαρξης

Λήμμα 5.1 *Αν M ένα πλέγμα στον L^{st}, με διάσταση $s+2t$, θεμελιώδη περιοχή όγκου V, και $c_1, ..., c_{s+t}$ να είναι θετικοί πραγματικοί αριθμοί με γινόμενο*

$$c_1 ... c_{s+t} > (\frac{4}{\pi})^t V,$$

τότε υπάρχει ένα μη μηδενικό στοιχείο μέσα στο M

$$x = (x_1, ..., x_{s+t}),$$

τέτοιο ώστε

$$|x_1| < c_1, ..., |x_s| < c_s;$$
$$|x_{s+1}|^2 < c_{s+1}, ..., |x_{s+t}|^2 < c_{s+t}.$$

Απόδειξη. Έστω X το σύνολο των σημείων του L^{st} για τα οποία ισχύει το συμπέρασμα του θεωρήματος. Έχουμε

$$v(X) = \int_{-c_1}^{c_1} dx_1 ... \int_{-c_s}^{c_s} dx_s \times \int_{y_1^2} + z_1^2 < c_{s+1} dy_1 dz_1$$

$$\times \int_{y_t^2} + z_t^2 < c_{s+t} dy_t dz_t$$

$$= 2c_1 \cdot 2c_2 ... 2c_s \pi c_{s+1} ... \pi c_{s+t} = 2^s \pi^t c_1 ... c_{s+t}.$$

Το X είναι ένα σύνολο από γραμμικά τμήματα και κυκλικούς δίσκους, δηλαδή θα είναι φραγμένο, συμμετρικό και κυρτό. Οπότε από το θεώρημα του Minkowski θα πάρουμε το αποτέλεσμα, αφού πρέπει να ισχύει

$$v(X) = 2^s \pi^t c_1 ... c_{s+t} > 2^{s+t} V \Leftrightarrow c_1 ... c_{s+t} > \left(\frac{4}{\pi}\right)^t V.$$

Λήμμα 5.2 *Έστω L ένα πλέγμα του $\mathbb{R}^n$, διάστασης n. Η βάση του είναι η $\{e_1, ..., e_n\}$. Υποθέτουμε ότι $e_i = (a_{1i}, ..., a_{ni})$. Τότε ο όγκος της θεμελιώδης περιοχής T του L, είναι*

$$v(T) = |det a_{ij}|.$$

Απόδειξη. Είναι $v(T) = \int_T dx_1...dx_n$. Ορίζουμε νέες μεταβλητές ως εξής: $x_i = \sum_j a_{ij}y_j$. Η Ιακωβιανή ορίζουσα της αλλαγής μεταβλητών στην περίπτωσή μας, είναι $deta_{ij}$ και ξέρουμε ότι το T είναι όλα τα σημεία $\sum b_i y_i$ με $0 \leq b_i < 1$. Άρα τώρα θα έχουμε

$$v(T) = \int_T |deta_{ij}| dy_1...dy_n$$

$$= |deta_{ij}| \int_0^1 dy_1... \int_0^1 dy_n = |deta_{ij}|.$$

Θεώρημα 5.2 *Έστω ένα σώμα αριθμών K, με βαθμό $n = s + 2t$ και δακτύλιο ακεραίων $\mathfrak{D}$. Έστω επίσης ένα μη μηδενικό ιδεώδες $\mathfrak{a}$ του $\mathfrak{D}$. Τότε ο όγκος μιας θεμελιώδους περιοχής του $\sigma(a)$ στον L^{st}, είναι*

$$v(T) = 2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|},$$

με Δ την διακρίνουσα του K.

Απόδειξη. Έστω μία ακέραια βάση του $\mathfrak{a}$ να είναι η $a_1, ..., a_n$. Ακολουθώντας τώρα τον συμβολισμό της απόδειξης του θεωρήματος 4.7, μία βάση ακεραιότητας για το $\sigma(\mathfrak{a})$ στο L^{st} είναι η

$$(x_1^{(1)}, ..., x_s^{(1)}, y_1^{(1)}, z_1^{(1)}, ..., y_t^{(1)}, z_t^{(1)})$$

$$.....$$

$$(x_1^{(n)}, ..., x_s^{(n)}, y_1^{(n)}, z_1^{(n)}, ..., y_t^{(n)}, z_t^{(n)}).$$

Επομένως από το λήμμα 5.2, θα έχουμε για T τη θεμελιώδη περιοχή του $\sigma(\mathfrak{a})$

$$v(T) = |D|,$$

όπου D η ορίζουσα του θεωρήματος 4.7. Συνεχίζουμε και έχουμε στο νου μας πάντα την απόδειξη του θεωρήματος 4.7, θα έχουμε $D = (-2i)^{-t}E \Leftrightarrow |D| = 2^{-t}|E|$. Αφού $E^2 = \Delta[a_1, ..., a_n]$ και $N(\mathfrak{a}) = |\frac{\Delta[a_1,...,a_n]}{\Delta}|^{1/2}$. Με συνδυασμό αυτών των σχέσεων θα έχουμε

$$|D| = v(T) = 2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Συνδυάζουμε το λήμμα 5.1 και το θεώρημα 5.2, για να αποδείξουμε το εξής θεώρημα :

Θεώρημα 5.3 *Αν έχουμε ένα μη μηδενικό ιδεώδες $\mathfrak{a}$, του $\mathfrak{D}$, τότε αυτό το ιδεώδες θα περιέχει έναν ακέραιο αριθμό α με*

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Απόδειξη. Έστω ένα τυχαίο $\epsilon > 0$, και επιλέγουμε πραγματικούς θετικούς αριθμούς $c_1, ..., c_{s+t}$ για τους οποίους θα έχουμε

$$c_1...c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|} + \epsilon.$$

Από το λήμμα 5.1 και το θεώρημα 5.2, υπάρχει ένα μη μηδενικό στοιχείο $\alpha \in \mathfrak{a}$ τέτοιο ώστε

$$|\sigma_1(\alpha)| < c_1, ..., |\sigma_s(\alpha)| < c_s, |\sigma_{s+1}(\alpha)|^2 < c_{s+1}, ..., |\sigma_{s+t}(\alpha)|^2 < c_{s+t}.$$

Πολλαπλασιάζουμε τώρα αυτές τις ανισώσεις και παίρνουμε

$$|N(\alpha)| < c_1...c_s c_{s+1}...c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} + \epsilon.$$

Ξέρουμε ότι ένα πλέγμα είναι διακριτό, οπότε το σύνολο A_ϵ αυτών των α, είναι πεπερασμένο. Επίσης $A_\epsilon \neq 0$ έτσι ώστε $A = \cap_\epsilon A_\epsilon \neq 0$. Αν διαλέξουμε $\alpha \in A$ θα είναι

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Πόρισμα 5.1 *Κάθε μη μηδενικό ιδεώδες $\mathfrak{a}$, του $\mathfrak{D}$ είναι ισοδύναμο με ένα ιδεώδες του οποίου η νόρμα είναι $\leq (2/\pi)^t\sqrt{|\Delta|}$.*

Απόδειξη. Η κλάση των κλασματικών ιδεωδών που είναι ισοδύναμα με το $\mathfrak{a}^{-1}$ θα περιέχει ένα ιδεώδες $\mathfrak{c}$, τέτοιο ώστε $\mathfrak{ac} \sim \mathfrak{D}$. Με χρήση του θεωρήματος 5.3, θα έχουμε ότι για έναν ακέραιο $\gamma \in \mathfrak{c}$ θα ισχύει ότι

$$|N(\gamma)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{c})\sqrt{|\Delta|}.$$

Από την στιγμή που έχουμε $\mathfrak{c}|\gamma$ θα είναι $\langle\gamma\rangle = \mathfrak{cb}$, για κάποιο ιδεώδες $\mathfrak{b}$. Παίρνοντας τις νόρμες θα έχουμε

$$N(\mathfrak{c})N(\mathfrak{b}) = N(\mathfrak{cb}) = N(\langle\gamma\rangle) = |N(\gamma)|.$$

Επομένως

$$N(\mathfrak{b})N(\mathfrak{c}) \leq (2/\pi)^t N(\mathfrak{c})\sqrt{|\Delta|} \Leftrightarrow N(\mathfrak{b}) \leq (2/\pi)^t\sqrt{|\Delta|}.$$

Ισχυριζόμαστε τέλος, ότι $\mathfrak{b} \sim \mathfrak{a}$. Αυτό είναι αληθές, γιατί $\mathfrak{a}^{-1} \sim \mathfrak{c}$ και $\mathfrak{b} \sim \mathfrak{c}^{-1}$.

Η επόμενη εφαρμογή υλολογίζει την class group του $\mathbb{Q}(\sqrt{-5})$.

Παράδειγμα 5.1 *Έστω $K = \mathbb{Q}(\sqrt{-5})$, με $\mathfrak{D} = \mathbb{Z}[\sqrt{-5}]$ ο οποίος δεν είναι ΠΜΑ, άρα $h > 1$. Οι μονομορφισμοί $\sigma_i : \mathbb{Q}(\sqrt{-5}) \to \mathbb{C}$, είναι οι σ_1, σ_2 με $\sigma_1 \neq \sigma_2$ και $\bar{\sigma_1} = \sigma_2$. Άρα $t = 1$. Ξέρουμε επίσης από προηγούμενη δουλειά μας, ότι $\Delta = -20$, άρα είναι*

$$\frac{2}{\pi}\sqrt{20} < 2.85.$$

Οπότε και σύμφωνα με το παραπάνω θεώρημα, θα έχουμε ότι κάθε ιδεώδες του $\mathfrak{D}$ θα είναι ισοδύναμο με ένα ιδεώδες νόρμας 1 ή 2. Τα ιδεώδη με νόρμα 1 είναι όλος ο δακτύλιος ακεραίων $\mathfrak{D}$. Ένα ιδεώδες τώρα $\mathfrak{a}$, το οποίο έχει νόρμα 2, ικανοποιεί την $\mathfrak{a}|2$, δηλαδή το $\mathfrak{a}$ είναι παράγοντας του $\langle 2\rangle$. Έχουμε δει όμως ότι

$$\langle 2\rangle = \left\langle 2, 1 + \sqrt{-5}\right\rangle^2,$$

όπου $\left\langle 2, 1 + \sqrt{-5}\right\rangle$ είναι ένα πρώτο ιδεώδες με νόρμα 2. Άρα όλα τα ιδεώδη του $\mathfrak{D}$ είναι ισοδύναμα με τον $\mathfrak{D}$ ή με το ιδεώδες $\left\langle 2, 1 + \sqrt{-5}\right\rangle$. Άρα $h = 2$.

5.3 Η class group έχει πεπερασμένη τάξη.

Θεώρημα 5.4 *Η ομάδα κλάσεων ενός σώματος αριθμών είναι πεπερασμένη αβελιανή ομάδα.*

Απόδειξη. Έστω K σώμα αριθμών με διακρίνουσα Δ και βαθμό $n = s + 2t$. Γνωρίζουμε ότι η $\mathcal{H}$ είναι αβελιανή, άρα μένει να δείξουμε ότι είναι πεπερασμένη. Αυτό θα ισχύει, αν και μόνο αν ο αριθμός των κλάσεων ισοδυναμίας των κλασματικών ιδεωδών, είναι πεπερασμένος. Έστω $[\mathfrak{c}]$ μία τέτοια κλάση ισοδυναμίας, η οποία θα περιέχει ένα ιδεώδες $\mathfrak{a}$. Από το πόρισμα 5.1, θα έχουμε ότι το $\mathfrak{a}$ είναι ισοδύναμο με ένα ιδεώδες $\mathfrak{b}$, το οποίο έχει νόρμα $N(\mathfrak{b}) \leq (2/\pi)^t \sqrt{|\Delta|}$. Ξέρουμε ότι μόνο πεπερασμένα το πλήθος ιδεώδη, μπορούν να έχουν συγκεκριμένη νόρμα, από το θεώρημα 3.7.3. Επομένως, υπάρχουν πεπερασμένες επιλογές για το ιδεώδες $\mathfrak{b}$. Τέλος, αφού είναι $[\mathfrak{c}] = [\mathfrak{a}] = [\mathfrak{b}]$, θα έχουμε και πεπερασμένες κλάσεις ισοδυναμίας $[\mathfrak{c}]$, που σημαίνει ότι η ομάδα κλάσεων $\mathcal{H}$ είναι πεπερασμένης τάξης.

Πρόταση 5.1 *Έστω K σώμα αριθμών, με class number h. Έστω επίσης ένα ιδεώδες $\mathfrak{a}$ του $\mathfrak{D}$. Τότε θα είναι:*

1. *$\mathfrak{a}^h$ είναι κύριο ιδεώδες.*
2. *Αν q πρώτος ως προς το h και $\mathfrak{a}^q$ είναι κύριο ιδεώδες, τότε και το $\mathfrak{a}$ θα είναι κύριο.*

Απόδειξη. Έχουμε $[\mathfrak{a}]^h = [\mathfrak{D}]$, για κάθε $[\mathfrak{a}] \in \mathcal{H}$, γιατί η $[\mathfrak{D}]$ είναι το ταυτοτικό στοιχείο της $\mathcal{H}$. Θα είναι $[\mathfrak{a}^h] = [\mathfrak{a}]^h = [\mathfrak{D}]$, δηλαδή τα $\mathfrak{a}^h$ και $\mathfrak{D}$, είναι ισοδύναμα, οπότε το $\mathfrak{a}^h$ είναι κύριο ιδεώδες. Αυτό δείχνει το 1. του θεωρήματος. Για το 2. έχουμε: έστω $v, u \in \mathbb{Z}$. Τότε αφού $(q, h) = 1$ θα είναι $uh + vq = 1$. Έχουμε και ότι $[\mathfrak{a}^h] = [\mathfrak{D}]$, επομένως θα είναι

$$[\mathfrak{a}] = [\mathfrak{a}]^{uh+vq} = ([\mathfrak{a}]^h)^u([\mathfrak{a}]^q)^v = [\mathfrak{D}]^u[\mathfrak{D}]^v = [\mathfrak{D}],$$

δηλαδή το ιδεώδες $\mathfrak{a}$ είναι κύριο.

Κεφάλαιο 6

Νόμος ανάλυσης

6.1 Ανάλυση ενός πρώτου στοιχείου

Αν έχουμε έναν p πρώτο στο $\mathbb{Z}$, δεν είναι απαραίτητο ότι και το ιδεώδες $\langle p\rangle$ θα είναι πρώτο στον δακτύλιο ακεραίων $\mathfrak{D}$ ενός σώματος αριθμών K. Είναι πολύ σημαντικό να μπορούμε να βρίσκουμε τους πρώτους παράγοντες του $\langle p\rangle$. Για την περίπτωση όπου ο $\mathfrak{D}$ παράγεται από ένα μόνο στοιχείο, δηλαδή για παράδειγμα τα τετραγωνικά σώματα, έχουμε το επόμενο θεώρημα που οφείλουμε στον Dedekind.

Θεώρημα 6.1 *Έστω K ένα σώμα αριθμών βαθμού n και $\mathfrak{D} = \mathbb{Z}[\theta]$, ο οποίος παράγεται από το $\theta \in \mathfrak{D}$. Έστω ότι έχουμε έναν ρητό πρώτο αριθμό p και το ελάχιστο πολυώνυμο f του θ στο $\mathbb{Q}$, έχει ανάλυση σε ανάγωγα πάνω από το $\mathbb{Z}_p$,*

$$f = f_1^{e_1}...f_r^{e_r}.$$

Τότε αν f_i ένα οποιοδήποτε από αυτά τα πολυώνυμα $\mathrm{mod} p$, το ιδεώδες $\mathfrak{p}_i = \langle p\rangle + \langle f_i(\theta)\rangle$ θα είναι πρώτο ιδεώδες και η ανάλυση του $\langle p\rangle$ σε πρώτα ιδεώδη στον $\mathfrak{D}$ είναι

$$\langle p\rangle = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}.$$

Απόδειξη. Έστω θ_i να είναι μία ρίζα του f_i στο $\mathbb{Z}_p[\theta_i] \cong \mathbb{Z}_p[t]/\langle f_i\rangle$. Υπάρχει φυσικός ομομορφισμός $v_i(p(\theta)) : \mathbb{Z}[\theta] \to \mathbb{Z}_p(\theta_i)$, όπου είναι

$$v_i(p(\theta)) = \bar{p}(\theta_i).$$

Η εικόνα του v_i είναι το $\mathbb{Z}_p(\theta_i)$, το οποίο είναι σώμα, επομένως ο πυρήνας $kerv_i$ είναι πρώτο ιδεώδες του $\mathbb{Z}[\theta] = \mathfrak{D}$. Προφανώς θα έχουμε

$$\langle p\rangle + \langle f_i(\theta)\rangle \subseteq kerv_i.$$

Αν $g(\theta) \in kerv_i$, τότε $\bar{g}(\theta_i) = 0$, άρα $\bar{g} = f_i\bar{h}, \bar{h} \in \mathbb{Z}_p[t]$. Το οποίο με τη σειρά του σημαίνει ότι το $g - f_ih \in \mathbb{Z}[t]$, έχει συντελεστές που διαιρούνται από το p. Επομένως θα έχουμε

$$g(\theta) = g(\theta) - f_i(\theta)h(\theta) + f_i(\theta)h(\theta)$$

$$\in \langle p\rangle + \langle f_i(\theta)\rangle .$$

Επομένως είναι

$$kerv_i = \langle p \rangle + \langle f_i(\theta) \rangle .$$

Έστω $\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle$, τότε για κάθε f_i το ιδεώδες $\mathfrak{p}_i$ είναι πρώτο και ικανοποιεί το $\langle p \rangle \subseteq \mathfrak{p}_i$ και $\mathfrak{p}_i | \langle p \rangle$. Για όλα τα ιδεώδη $\mathfrak{a}, \mathfrak{b}_1, \mathfrak{b}_2$, έχουμε $(\mathfrak{a} + \mathfrak{b}_1)(\mathfrak{a} + \mathfrak{b}_2) \subseteq \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2$. Επαγωγικά

$$\mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r} \subseteq \langle p \rangle + \langle f_1(\theta)^{e_1} ... f_r(\theta)^{e_r} \rangle$$

$$\subseteq \langle p \rangle + \langle f(\theta) \rangle = \langle p \rangle .$$

Άρα $\langle p \rangle | \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}$, και έτσι οι μόνοι πρώτοι παράγοντες του ιδεώδους $\langle p \rangle$ είναι τα $\mathfrak{p}_1, ..., \mathfrak{p}_r$. Έτσι θα έχουμε

$$\langle p \rangle = \mathfrak{p}_1^{k_1} ... \mathfrak{p}_r^{k_r}, 0 < k_i \leq e_i, 1 \leq i \leq r.$$

Παίρνουμε τώρα τη νόρμα του $\mathfrak{p}_i$ και είναι

$$N(\mathfrak{p}_i) = |\mathfrak{D}/\mathfrak{p}_i|$$

και είναι

$$\mathfrak{D}/\mathfrak{p}_i = \mathbb{Z}[\theta]/\mathfrak{p}_i \cong \mathbb{Z}_p[\theta_i] \Leftrightarrow N(\mathfrak{p}_i) = |\mathbb{Z}_p[\theta_i]| = p^{d_i},$$

όπου $d_i = \partial f_i$. Επίσης η νόρμα του $\langle p \rangle$ είναι

$$N(\langle p \rangle) = |\mathfrak{D}/\langle p \rangle| = p^n.$$

Εξισώνουμε τις δύο αυτές νόρμες και παίρνουμε

$$N(\langle p \rangle) = N(\mathfrak{p}_1^{k_1}) ... N(\mathfrak{p}_r^{k_r}) \Leftrightarrow p^n = p^{d_1 k_1 + ... + d_r k_r}$$

$$\Leftrightarrow n = d_1 k_1 + ... + d_r k_r,$$

και επειδή όπως είπαμε πιο πάνω $0 < k_i \leq e_i$, θέτουμε $k_i = e_i$ και παίρνουμε το ζητούμενο.

Παράδειγμα 6.1 *Έστω ότι έχουμε* $\mathbb{Q}(\sqrt{-1})$ *όπου είναι* $\mathfrak{D} = \mathbb{Z}[\theta]$ *με το* θ *να έχει ελάχιστο πολυώνυμο* $t^2 + 1$. *Ας πούμε ότι θέλουμε να παραγοντοποιήσουμε το ιδεώδες* $\langle 2 \rangle$. *Πρώτα παραγοντοποιούμε το ελάχιστο πολυώνυμο* mod2. *Είναι* $t^2 + 1 = (t + 1)(t + 1) = (t + 1)^2$. *Άρα το* $\langle 2 \rangle = \mathfrak{p}^2$ *με* $\mathfrak{p} = \langle 2 \rangle + \langle f_1(\theta_1) \rangle = \langle 2 \rangle + \langle \sqrt{-1} + 1 \rangle = \langle 1 + \sqrt{-1} \rangle$, *γιατί ξέρουμε ότι* $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$.

Γενικότερα τώρα ας θεωρήσουμε την περίπτωση όπου θέλουμε να παραγοντοποιήσουμε το $p \in \mathbb{Z}$, στον $\mathbb{Z}[\sqrt{-1}]$. Έχουμε τρεις περιπτώσεις:

1. $t^2 + 1$ να είναι ανάγωγο πολυώνυμο modulo p,
2. $t^2 + 1 = (t + l)(t - l) \bmod p$, με $l^2 \equiv -1 \bmod p,\ l \neq -l$,
3. $t^2 + 1 = (t + 1)^2 \bmod 2,\ p = 2$.

Στο 1 θα έχουμε το ιδεώδες $\mathfrak{p}$ να είναι πρώτο, ενώ στο 2 θα είναι $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2,\ \mathfrak{p}_1 \neq \mathfrak{p}_2$. Τέλος στο 3, $\langle p \rangle = \mathfrak{p}_1^2, \mathfrak{p}_1$ πρώτο ιδεώδες.

6.2 Ανάλυση σε επεκτάσεις Galois

Σε αυτήν την παράγραφο θα δούμε πως αναλύονται τα πρώτα ιδεώδη του K, σε επεκτάσεις Galois. Για να γίνει αυτό, θα πρέπει αρχικά να εισάγουμε τον όρο της διακλάδωσης. Έστω K ένα σώμα αριθμών και L μία πεπερασμένη επέκτασή του. Θα γράφουμε από εδώ και πέρα με $\mathfrak{D}_K$, $\mathfrak{D}_L$, τους δακτύλιους ακεραίων των K και L αντίστοιχα. Έστω ένα $\mathfrak{p}$, πρώτο ιδεώδες του $\mathfrak{D}_K$. Το $\mathfrak{p}\mathfrak{D}_L$ τότε, θα είναι ιδεώδες του $\mathfrak{D}_L$, οπότε θα αναλύεται σε πρώτα ιδεώδη

$$\mathfrak{p}\mathfrak{D}_L = \mathfrak{B}_1^{e_1}...\mathfrak{B}_g^{e_g}.$$

Τα $\mathfrak{B}_i$, είναι πρώτα ιδεώδη του $\mathfrak{D}_L$ και περιέχουν το $\mathfrak{p}$. Οι ακέραιοι αριθμοί e_i, τους οποίους τους συμβολίζουμε και $e_{\mathfrak{B}_i|\mathfrak{p}}$, ονομάζονται δείκτες διακλάδωσης του $\mathfrak{p}$ στο $\mathfrak{B}_i$. Κάθε $\mathfrak{B}_i$ δίνει μία επέκταση σώματος $\mathfrak{D}_K/\mathfrak{p} \subset \mathfrak{D}_L/\mathfrak{B}_i$, με βαθμό f_i ή $f_{\mathfrak{B}_i|\mathfrak{p}}$ που τον ονομάζουμε βαθμό αδράνειας του $\mathfrak{p}$ στο $\mathfrak{B}_\mathrm{i}$.

Θεώρημα 6.2 *Έστω $K \subset L$ και $\mathfrak{p}$ πρώτο στο K. Αν e_i, f_i όπως τα ορίσαμε πριν, τότε θα είναι*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Απόδειξη. Βλέπε θεώρημα 21 [3].

Θα λέμε ότι ένα ιδεώδες $\mathfrak{p}$ του K διακλαδίζεται, αν κάποιος από τους δείκτες διακλάδωσης e_i είναι μεγαλύτερος από 1. Οι περισσότερες επεκτάσεις που θα μας απασχολήσουν είναι Galois επεκτάσεις, οπότε και θα έχουμε τα ακόλουθα.

Θεώρημα 6.3 *Έστω $K \subset L$ Galois επέκταση και $\mathfrak{p}$ πρώτο ιδεώδες του K.*

1. *Η ομάδα Galois $Gal(L/K)$, έχει μεταβατική δράση στα πρώτα στοιχεία του L που περιέχουν το $\mathfrak{p}$, δηλαδή αν $\mathfrak{B}$, $\mathfrak{B}'$ πρώτα ιδεώδη του L που περιέχουν το $\mathfrak{p}$, τότε θα υπάρχει ένας $\sigma \in Gal(L/K)$, τέτοιος ώστε $\sigma(\mathfrak{B}) = \mathfrak{B}'$.*

2. *Τα πρώτα ιδεώδη $\mathfrak{B}_i$ του L που περιέχουν το $\mathfrak{p}$, έχουν όλα το ίδιο e και το ίδιο f, έτσι το θεώρημα 6.3 γίνεται*

$$efg = [L : K].$$

Απόδειξη. Το 2 είναι συνέπεια του 1. Για το 1 τώρα, έχουμε: έστω ότι $\sigma(\mathfrak{B}) \neq \mathfrak{B}'$, για όλους τους $\sigma \in Gal(L/K)$. Τότε σύμφωνα με το κινέζικο θεώρημα θα υπάρχει μία λύση για το σύστημα

$$x \equiv 0 \bmod \mathfrak{B}'$$

$$x \equiv 1 \bmod \sigma(\mathfrak{B}),$$

για όλους τους σ. Έστω $\alpha \in \mathfrak{D}_L$ η λύση του συστήματος. Θα είναι $N(\alpha) \in \mathfrak{D}_K \cap \mathfrak{B}'$, αφού από το σύστημα έχουμε ότι $\alpha \in \mathfrak{B}' = \mathfrak{p}$. Επίσης είναι $\alpha \notin \sigma(\mathfrak{B}) \Leftrightarrow \sigma^{-1}(\alpha) \notin \mathfrak{B}$. Μπορούμε τώρα να εκφράσουμε την νόρμα του α σαν γινόμενο όλων των $\sigma^{-1}(\alpha)$. Κανένα από αυτά τα στοιχεία δεν ανήκει στο $\mathfrak{B}$, άρα $N(\alpha) \notin \mathfrak{B}$. Αυτό όμως είναι άτοπο, αφού πριν δείξαμε ότι $N(\alpha) \in \mathfrak{p} \subset \mathfrak{B}$. Έτσι $\sigma(\mathfrak{B}) = \mathfrak{B}'$, για κάποιο σ.

Αν έχουμε επέκταση Galois L/K, θα λέμε ότι το ιδεώδες $\mathfrak{p}$ του K, διακλαδίζεται αν $e > 1$ και είναι αδιακλάδωτο αν $e = 1$. Αν $e = 1$ και επιπλέον έχουμε ότι

$f = 1$, τότε θα λέμε ότι το ιδεώδες $\mathfrak{p}$, διασπάται πλήρως στο L. Τότε το $\mathfrak{p}\mathfrak{D}_L$ θα είναι το γινόμενο $[L : K]$ πρώτων ιδεωδών.

Δίνουμε τους ορισμούς δύο ομάδων, της ομάδας διακλάδωσης (decomposition group) και της ομάδας αδράνειας (inertia group), ενός ιδεώδους $\mathfrak{B}$.

Ορισμός 6.1

1. *Ομάδα διακλάδωσης είναι η ομάδα* $D_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$.
2. *Ομάδα αδράνειας είναι η ομάδα* $I_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv a \bmod \mathfrak{B}, \ \text{για κάθε } \alpha \in \mathfrak{D}_L\}$.

Παρατηρούμε ότι ισχύει $I_{\mathfrak{B}} \subset D_{\mathfrak{B}}$. Αυτό γιατί το $\sigma(\mathfrak{B}) = \mathfrak{B}$ μπορεί να εκφραστεί σαν $\sigma(\alpha) \equiv 0 \bmod \mathfrak{B}$, αν και μόνο αν $\alpha \equiv 0 \bmod \mathfrak{B}$, που σημαίνει ότι $\alpha \in \mathfrak{B}$. Αν πάρουμε ένα στοιχείο $\sigma \in D_{\mathfrak{B}}$, αυτό θα επάγει αυτομορφισμό $\bar{\sigma}$ στο $\mathfrak{D}_L/\mathfrak{B}$, ο οποίος είναι ο ταυτοτικός στο $\mathfrak{D}_K/\mathfrak{p}$. Συμβολίζουμε με $\tilde{G}$ την ομάδα Galois της επέκτασης $\mathfrak{D}_K/\mathfrak{p} \subset \mathfrak{D}_L/\mathfrak{B}$. Άρα σύμφωνα με τα παραπάνω $\bar{\sigma} \in \tilde{G}$. Επομένως ο $\sigma \mapsto \bar{\sigma}$ επάγει ομομορφισμό $D_{\mathfrak{B}} \to \tilde{G}$. Ο πυρήνας αυτού του ομομορφισμού είναι ακριβώς η ομάδα αδράνειας $I_{\mathfrak{B}}$. Συνοψίζουμε στην ακόλουθη πρόταση.

Πρόταση 6.1 *Έστω* $D_{\mathfrak{B}}$, $I_{\mathfrak{B}}$, $\tilde{G}$, *όπως τα ορίσαμε πριν. Θα είναι*

1. *Ο ομομορφισμός* $D_{\mathfrak{B}} \to \tilde{G}$ *είναι επί. Επομένως* $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \tilde{G}$.
2. $|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}$, *και* $|D_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}} f_{\mathfrak{B}|\mathfrak{p}}$.

Απόδειξη. Βλέπε θεώρημα 28 [3].

Η επόμενη πρόταση θα μας βοηθήσει στο αν ένα πρώτο ιδεώδες είναι αδιακλάδωτο, ή διασπάται πλήρως σε μία επέκταση Galois.

Πρόταση 6.2 *Έστω επέκταση Galois* $K \subset L$, $\mu\epsilon\ L = K(\alpha)$, $\alpha \in \mathfrak{D}_L$ *και* $f(x)$ *το ελάχιστο πολυώνυμο του* α *πάνω από το* K, *τέτοιο ώστε* $f(x) \in \mathfrak{D}_K[x]$. *Αν το* $\mathfrak{p}$ *είναι πρώτο στο* $\mathfrak{D}_K$ *και το* $f(x)$ *αναλύεται πλήρως* $\bmod\mathfrak{p}$, *τότε έχουμε:*

1. *Το* $\mathfrak{p}$ *είναι αδιακλάδωτο στο* L.
2. *Αν* $f(x) \equiv f_1(x)...f_g(x) \bmod \mathfrak{p}$, *όπου τα* $f_i(x)$ *είναι ανάγωγα* $\bmod\mathfrak{p}$ *τότε το* $\mathfrak{B}_i = \mathfrak{p}\mathfrak{D}_L + f_i(\alpha)\mathfrak{D}_L$ *είναι πρώτο ιδεώδες του* $\mathfrak{D}_L$ $\mu\epsilon\ \mathfrak{B}_i \neq \mathfrak{B}_j$, $i \neq j$, *και* $\mathfrak{p}\mathfrak{D}_L = \mathfrak{B}_1...\mathfrak{B}_g$. *Επιπλέον όλα τα* $f_i(x)$, *έχουν τον ίδιο βαθμό, ο οποίος είναι ο βαθμός αδράνειας* f.
3. *Το* $\mathfrak{p}$ *διασπάται πλήρως στο* L, *αν και μόνο αν η* $f(x) \equiv 0 \bmod \mathfrak{p}$ *έχει λύση στο* $\mathfrak{D}_K$.

Απόδειξη. Βλέπε πρόταση 5.11 [4].

6.3 Το σώμα κλάσεων του Hilbert

.

Εισάγουμε μία πολύ σημαντική έννοια για την δουλειά μας, αυτή του σώματος κλάσεων του Hilbert. Ας δώσουμε δύο ορισμούς, οι οποίοι είναι απαραίτητοι για να το ορίσουμε.

Ορισμός 6.2 *Μία επέκταση $K \subset L$ είναι αβελιανή, αν είναι επέκταση Galois και η ομάδα $G = Gal(L/K)$ είναι αβελιανή.*

Ορισμός 6.3 *Μία επέκταση $K \subset L$ ονομάζεται αδιακλάδωτη (unrumified), αν κάθε πρώτο στοιχείο του K είναι αδιακλάδωτο στη L.*

Θεώρημα 6.4 *Αν έχουμε ένα σώμα αριθμών K, τότε υπάρχει μία πεπερασμένη επέκταση Galois L, για την οποία θα είναι:*

1. *Η L είναι αδιακλάδωτη αβελιανή επέκταση του K.*
2. *Κάθε αδιακλάδωτη αβελιανή επέκταση του K, βρίσκεται μέσα στην L.*

Ένα τέτοιο σώμα L, λέγεται σώμα κλάσεων του Hilbert, για το K. Είναι η μέγιστη αβελιανή επέκταση για το K και προφανώς είναι και μοναδική.

Απόδειξη. Βλέπε θεώρημα 5.7 [6].

Λήμμα 6.1 *Έστω επέκταση Galois $K \subset L$, και $\mathfrak{p}$ ένα πρώτο ιδεώδες του $\mathfrak{D}_K$, αδιακλάδωτο στο L. Αν το $\mathfrak{B}$ είναι πρώτο του $\mathfrak{D}_L$ και το οποίο να περιέχει το ιδεώδες $\mathfrak{p}$, τότε υπάρχει ένα μοναδικό στοιχείο $\sigma \in G$, τέτοιο ώστε για κάθε $\alpha \in \mathfrak{D}_L$ να είναι,*

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{B},$$

όπου $N(\mathfrak{p}) = |\mathfrak{D}_K/\mathfrak{p}|$, η νόρμα του ιδεώδους $\mathfrak{p}$.

Απόδειξη. Έστω $D_{\mathfrak{B}}$, $I_{\mathfrak{B}}$, $\tilde{G}$, όπως τα ορίσαμε στην προηγούμενη παράγραφο. Έχουμε λοιπόν δείξει ότι $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \tilde{G}$. Επίσης αφού το ιδεώδες $\mathfrak{p}$ είναι αδιακλάδωτο στο L, σύμφωνα με την πρόταση 6.1 θα έχουμε ότι $|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}} = 1$. Έτσι τελικά θα έχουμε ότι ο $\sigma \mapsto \bar{\sigma}$ ορίζει ισομορφισμό $D_{\mathfrak{B}} \cong \tilde{G}$. Η επέκταση Galois $\mathfrak{D}_K/\mathfrak{p} \subset \mathfrak{D}_L/\mathfrak{B}$, έχει ομάδα την $\tilde{G}$ η οποία σαν ομάδα Galois, έχει γεννήτορα τον αυτομορφισμό Frobenius $x \mapsto x^q$, όπου q είναι η $|\mathfrak{D}_K/\mathfrak{p}|$. Επομένως, θα υπάρχει ένας μοναδικός $\sigma \in D_{\mathfrak{B}}$, ο οποίος απεικονίζει στο στοιχείο του Frobenius. Έχουμε επίσης από τον ορισμό της νόρμας ενός ιδεώδους, ότι $|\mathfrak{D}_K/\mathfrak{p}| = N(\mathfrak{p}) = q$, άρα είναι

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{B},$$

για κάθε $\alpha \in \mathfrak{D}_L$.

Ορισμός 6.4 *Το μοναδικό στοιχείο σ του προηγούμενου λήμματος, καλείται σύμβολο του Artin και θα το συμβολίζουμε από εδώ και πέρα $\left(\frac{L/K}{\mathfrak{B}}\right)$. Έχει τις ακόλουθες ιδιότητες.*

Πόρισμα 6.1 *Έστω $K \subset L$ επέκταση Galois, $\mathfrak{p}$ ένα αδιακλάδωτο πρώτο ιδεώδες του K. Αν έχουμε ένα $\mathfrak{B}$, που να περιέχει το $\mathfrak{p}$, θα είναι:*

1. *Αν $\sigma \in G = Gal(L/K)$ τότε*

$$\left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \sigma \left(\frac{L/K}{\mathfrak{B}}\right) \sigma^{-1}$$

2. *Η τάξη του* $((L/K)/\mathfrak{B})$ *είναι ο βαθμός αδράνειας* $f = f_{\mathfrak{B}|\mathfrak{p}}$.

3. *Το* $\mathfrak{p}$ *διασπάται πλήρως στο* L, *αν και μόνο αν* $((L/K)/\mathfrak{B}) = 1$

Απόδειξη. Το 1 είναι προφανές και βγαίνει άμεσα από την μοναδικότητα του σύμβολου Artin, και το γεγονός ότι η G είναι αβελιανή. Το 2 τώρα. Έχουμε ότι το $\mathfrak{p}$ είναι αδιακλάδωτο, επομένως όπως έχουμε ξαναπεί, θα είναι $D_{\mathfrak{B}} \cong \tilde{G}$. Να θυμηθούμε ότι η $\tilde{G}$ είναι η ομάδα Galois της $\mathfrak{D}_K/\mathfrak{p} \subset \mathfrak{D}_L/\mathfrak{B}$, η οποία είναι επέκταση βαθμού f. Άρα και η τάξη της $\tilde{G}$ θα είναι f. Τέλος, το σύμβολο Artin, απεικονίζεται σε γεννήτορα, επομένως η τάξη του θα πρέπει να είναι f. Το 3 είναι τετριμμένο. Αφού το ιδεώδες $\mathfrak{p}$ διασπάται πλήρως όταν $e = f = 1$ και εδώ έχουμε υποθέσει ότι $e = 1$, σύμφωνα και με το 2, παίρνουμε το ζητούμενο.

Παρατήρηση: Το σύμβολο Artin είναι ίδιο για όλα τα πρώτα ιδεώδη $\mathfrak{p}$ μόνο αν η επέκταση είναι αβελιανή. Επομένως, θα εξαρτάται μόνο από το ιδεώδες $\mathfrak{p}$. Μπορούμε λοιπόν να το γράφουμε σαν $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Έστω η ομάδα των κλασματικών ιδεωδών $\mathcal{F}$ του $\mathfrak{D}_K$. Ξέρουμε ότι κάθε $\mathfrak{a} \in \mathcal{F}$ έχει ανάλυση σε πρώτα,

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i},\ r_i \in \mathbb{Z}.$$

Το σύμβολο Artin θα είναι :

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

Επομένως το σύμβολο Artin επάγει ομομορφισμό, τον οποίο ονομάζουμε Artin απεικόνιση:

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{F} \to Gal(L/K).$$

Να σημειώσουμε ότι αυτός ο ομομορφισμός έχει νόημα, μόνο για αδιακλάδωτες επεκτάσεις.

Θεώρημα 6.5 *Έστω* L *το σώμα κλάσεων του Hilbert ενός σώματος αριθμών,* K. *Τότε ο ομομορφισμός Artin*

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{F} \longrightarrow Gal(L/K),$$

είναι επί και έχει πυρήνα την ομάδα των κύριων κλασματικών ιδεωδών $\mathcal{P}$. *Επομένως, σύμφωνα με το θεμελιώδες θεώρημα των ισομορφισμών, θα έχουμε:*

$$\mathcal{H} \cong Gal(L/K).$$

Πόρισμα 6.2 *Αν έχουμε ένα σώμα αριθμών* K, *τότε υπάρχει μία ένα προς ένα αντιστοιχία μεταξύ των αδιακλάδωτων αβελιανών επεκτάσεων του* K, *και των υποομάδων* H *της ομάδας κλάσεων ιδεωδών* $\mathcal{H}$. *Δηλαδή αν μία επέκταση* M, *αντιστοιχεί σε μία υποομάδα* $H \subset \mathcal{H}$, *η Artin απεικόνιση θα επάγει ισομορφισμό*

$$\mathcal{H}/H \cong Gal(M/K).$$

Πόρισμα 6.3 *Έστω L το σώμα κλάσεων του Hilbert, ενός σώματος αριθμών K. Έστω επίσης ένα πρώτο ιδεώδες του K, $\mathfrak{p}$. Τότε το $\mathfrak{p}$ θα διασπάται πλήρως στο L, αν και μόνο αν είναι κύριο ιδεώδες.*

Απόδειξη. Ξέρουμε ήδη από το πόρισμα 6.1, ότι το $\mathfrak{p}$ διασπάται πλήρως, αν και μόνο αν $((L/K)/\mathfrak{p}) = 1$. Αφού ο Artin επάγει τον ισομορφισμό $\mathcal{H} \cong Gal(L/K)$ θα έχουμε $((L/K)/\mathfrak{p}) = 1$, αν και μόνο αν έχουμε την τετριμμένη κλάση ιδεωδών. Δηλαδή όλα τα κλασματικά ιδεώδη είναι κύρια, κάτι που φυσικά καθιστά και το $\mathfrak{p}$ κύριο ιδεώδες.

Κεφάλαιο 7

Ελλειπτικές Καμπύλες.

Η θεωρία των ελλειπτικών καμπύλων, είναι αυτή η οποία θα μας απασχολήσει από εδώ και πέρα. Αρχικά θα δώσουμε κάποια βασικά στοιχεία για τις ελλειπτικές καμπύλες και έπειτα θα δούμε κάποιες εφαρμογές τους στην κρυπτογραφία και τον τρόπο με τον οποίο συνδέεται με όλα τα προηγούμενα που έχουμε πει. Θα ξεκινήσουμε, χτίζοντας σιγά σιγά τον ορισμό μιας ελλειπτικής καμπύλης, χωρίς να είμαστε ιδιαίτερα αυστηροί.

7.1 Θεωρία των ελλειπτικών καμπύλων

Τις ελλειπτικές καμπύλες τις ορίζουμε πάνω από ένα σώμα K. Αυτό μπορεί για παράδειγμα να είναι το $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}$. Συνήθως τα $\mathbb{R}$, $\mathbb{C}$ χρησιμοποιούνται για γεωμετρικά προβλήματα, το $\mathbb{Q}$ για διοφαντικά προβλήματα, ενώ στην περίπτωση της κρυπτογραφίας βλέπουμε τις ελλειπτικές καμπύλες, πάνω από πεπερασμένα σώματα $\mathbb{F}_p$.

Ορισμός 7.1 *Θα ορίζουμε με $V(f)$ ενός πολυωνύμου $f(x,y) \in K[x,y]$, το σύνολο των σημείων μηδενισμού του. Θα το καλούμε αλγεβρικό σύνολο του f στο K. Είναι δηλαδή*

$$V(f) = \left\{(x,y) \in K^2 : f(x,y) = 0\right\}.$$

Ορισμός 7.2 *Ορίζουμε γένος g μιας επιφάνειας, τον αριθμό των «τρυπών» της.*

Στη συνέχεια, δίνουμε μία περιγραφή για τον προβολικό χώρο $\mathbb{P}^n(K)$ του K. Θα είναι το σύνολο

$$\left\{(x_0, ..., x_n) \in K^{n+1}\right\},$$

με τουλάχιστον κάποιο από τα $x_i \neq 0$ και εφοδιασμένο με την σχέση ισοδυναμίας $\sim$, σύμφωνα με την οποία

$$(x_0, ..., x_1) \sim (y_0, ..., y_n)k,$$

αν υπάρχει ένα $\lambda \in K^*$ τέτοιο ώστε $x_i = \lambda y_i$ για κάθε i. Δηλαδή για παράδειγμα, η προβολική ευθεία $\mathbb{P}^1(K)$ είναι

$$\mathbb{P}^1(K) = \left\{(x,y) \in K^2 \setminus (0,0)\right\} / \sim,$$

όπου έχουμε

$$(x, y) \sim (x', y') \text{ αν } (x, y) = \lambda(x', y').$$

Είναι δηλαδή το σύνολο των ευθειών του K^2 που περνάνε από το σημείο $(0, 0)$, εφοδιασμένες φυσικά με την σχέση ισοδυναμίας $\sim$. Η ευθεία όμως $x = 0$, δεν μπορεί να γραφτεί στη μορφή $y = \lambda x$. Ξέρουμε ότι καθώς το λ αυξάνει, τόσο η ευθεία αυτή θα πλησιάζει την $x = 0$. Επομένως θα έχουμε ότι $\mathbb{P}^1(K) = K \cup \{\infty\}$ με $\lambda \in K$ όταν έχω ευθεία $y = \lambda x$ και για την ευθεία $x = 0$ θα έχουμε $\lambda = \infty$. Επίσης θα έχουμε το προβολικό επίπεδο,

$$\mathbb{P}^2(K) = \{(x, y, z) \setminus (0, 0, 0)\} / \sim,$$

με $(x, y, z) \sim (x', y', z')$ αν $(x, y, z) = \lambda(x', y', z')$. Το $\mathbb{P}^2(K)$ θα είναι, το σύνολο των ευθειών που περνάνε από το σημείο $(0, 0, 0)$, με την σχέση ισοδυναμίας που έχουμε ορίσει προηγουμένως. Οι ευθείες που ανήκουν στο επίπεδο $z = 0$ αντιστοιχούν σε διανύσματα της μορφής $(x, y, 0)$, δηλαδή αποτελούν ένα $\mathbb{P}^1(K)$. Επομένως θα είναι

$$\mathbb{P}^2(K) = K^2 \cup \mathbb{P}^1(K) = K^2 \cup K \cup \{\infty\}.$$

Οι τριάδες που αποτελούν αυτά τα σημεία, ονομάζονται προβολικές συντεταγμένες και συμβολίζονται με $(x : y : z)$.

Ορισμός 7.3 *Θα καλούμε ομογενές πολυώνυμο, ένα πολυώνυμο f το οποίο είναι άθροισμα μονωνύμων του ίδιου βαθμού.*

Για παράδειγμα το $f(x, y, z) = xy^2z^3 + x^2y^4 + x^3yz^2$ είναι ένα ομογενές πολυώνυμο. Αν έχουμε ένα ομογενές πολυώνυμο f, και $(x : y : z) = (x' : y' : z') \Leftrightarrow (x : y : z) = \lambda(x', y', z')$, τότε $f(x, y, z) = 0 \Leftrightarrow f(x', y', z') = 0$ και $f(x, y, z) = \lambda^d f(x', y', z')$ με $d = \deg f,\ \lambda^d \neq 0$.

Πόρισμα 7.1 *Ομογενή πολυώνυμα σε προβολικό χώρο, ορίζουν αλγεβρικά σύνολα:*

$$V(f) = \left\{(x : y : z) \in \mathbb{P}^2 : f(x : y : z) = 0\right\}.$$

Ορισμός 7.4 *Έστω $f \in K[x, y, z]$ ομογενές πολυώνυμο. Το $V(f)$ θα καλείται ομαλό στο $(x_0 : y_0 : z_0)$ αν και μόνο αν $f(x_0, y_0z_0) = 0$ και $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}) \neq (0, 0, 0)$.*

Ορισμός 7.5 *Μία ελλειπτική καμπύλη ορισμένη στο K, είναι το σύνολο $V(f)$ ενός f ομογενούς πολυωνύμου βαθμού $\deg f = 3$, τέτοιο ώστε το $V(f)$ να είναι παντού ομαλό.*

Ορισμός 7.6 *Μία ελλειπτική καμπύλη θα καλείται μη ιδιόμορφη (non-singular), αν για κανένα σημείο της δεν ισχύει*

$$(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}) = (0, 0, 0).$$

Ορισμός 7.7 *Έστω K ένα σώμα και $\overline{K}$ η αλγεβρική κλειστότητά του. Μία ελλειπτική καμπύλη πάνω από το K ορίζεται να είναι το σύνολο των λύσεων στο προβολικό επίπεδο $\mathbb{P}^2(\overline{K})$, της ομογενούς εξίσωσης του Weierstrass,*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

με $a_1, a_2, a_3, a_4, a_6 \in K$. Η εξίσωση αυτή ονομάζεται μακρά εξίσωση του Weierstrass.

Ορισμός 7.8 *Έστω σώμα K για το οποίο να έχουμε $K \subseteq \tilde{K} \subseteq \overline{K}$. Ένα σημείο (X, Y, Z) της E θα καλείται $\tilde{K}$-ρητό σημείο της E, αν $(X, Y, Z) = \alpha(\tilde{X}, \tilde{Y}, \tilde{Z})$, $\alpha \in \tilde{K}$, $(\tilde{X}, \tilde{Y}, \tilde{Z}) \in \tilde{K}^3 \setminus (0, 0, 0)$. Τα K-ρητά σημεία της καμπύλης E θα τα συμβολίζουμε $E(K)$, για ευκολία και θα τα ονομάζουμε ρητά σημεία της καμπύλης.*

Η καμπύλη έχει ένα μόνο σημείο με την Z-συντεταγμένη του να είναι μηδέν. Είναι το $(0, 1, 0)$. Θα το ονομάζουμε σημείο στο άπειρο και θα το συμβολίζουμε με $\mathcal{O}$. Γενικά θα χρησιμοποιούμε την αφινική μορφή της εξίσωσης Weierstrass η οποία είναι

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Τα ρητά σημεία της καμπύλης στην αφινική περίπτωση είναι οι λύσεις της στο $\tilde{K}^2$ και το σημείο στο άπειρο $\mathcal{O}$. Θα δώσουμε τώρα κάποιες σταθερές, τις οποίες θα χρησιμοποιήσουμε στη συνέχεια. Έχουμε:

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Ορισμός 7.9 *Ορίζουμε διακρίνουσα Δ, μιας ελλειπτικής καμπύλης E, να είναι:*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Σε περιπτώσεις όπου η χαρακτηριστική του σώματος K είναι $char(K) \neq 2, 3$ τότε έχουμε

$$\Delta = (c_4^3 - c_6^2)/1728.$$

Μία κάμπύλη θα είναι μη ιδιόμορφη, αν και μόνο αν η διακρίνουσά της είναι διάφορη του μηδέν. Αν τώρα είναι $\Delta \neq 0$ ορίζουμε την j-αναλλοίωτη της καμπύλης να είναι

$$j(E) = \frac{c_4^3}{\Delta}$$

Η j-αναλλοίωτη έχει άμεση σχέση με την ισομορφία δύο ελλειπτικών καμπύλων. Πιο συγκεκριμένα, αν έχουμε ελλειπτικές καμπύλες E και E', ορισμένες πάνω από ένα αλγεβρικά κλειστό σώμα, τότε θα είναι ισόμορφες, αν και μόνο αν οι j-αναλλοίωτές τους είναι ίσες. Θα λέμε ότι οι E και E' ορισμένες με την εξίσωση του Weierstrass είναι ισόμορφες πάνω από το K, αν και μόνο αν υπάρχουν σταθερές $r, s, t \in K$ και $u \in K^*$ τέτοιες ώστε οι μεταβλητές

$$X = u^2X' + r,\ Y = u^3Y' + su^2X' + t$$

να μετατρέπουν την E στην E'. Είμαστε έτοιμοι πλέον, να ορίσουμε τον νόμο ομάδας σε μία ελλειπτική καμπύλη. Αν γίνει η αλλαγή μεταβλητών

$$X = X' - \frac{b_2}{12},\ Y = Y' - \frac{a_1}{2}(X' - \frac{b_2}{12}) - \frac{a_3}{2},$$

στην εξίσωση του Weierstrass, τότε θα πάρουμε την εξής ισόμορφη ελλειπτική καμπύλη:

$$E : Y^2 = X^3 + aX + b,\ a, b \in K. \tag{7.1}$$

Έστω επίσης P, Q δύο διαφορετικά ρητά σημεία της E. Η ευθεία που ενώνει αυτά τα δύο σημεία, αφού τέμνει μία κυβική καμπύλη, θα πρέπει να την τέμνει και σε άλλο ένα σημείο, έστω R. Παίρνουμε το συμμετρικό σημείο του R στον άξονα των x. Το σημείο που θα βρούμε είναι το άθροισμα των σημείων των P και Q. Αποδεικνύεται, ότι η πράξη αυτή, ορίζει προσθετική αβελιανή ομάδα με στοιχεία τα ρητά σημεία της E και ουδέτερο στοιχείο, το σημείο στο άπειρο $\mathcal{O}$. (Για λεπτομέρειες στη δομή ομάδας και στο νόμο ομάδας των ρητών σημείων μιας ελλειπτικής καμπύλης, βλέπε [8]). Το επόμενο λήμμα εφαρμόζεται για ελλειπτικές καμπύλες πάνω από σώματα με οποιαδήποτε χαρακτηριστική.

Λήμμα 7.1 *Έστω η ελλειπτική καμπύλη με εξίσωση*

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

και έστω $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ δύο σημεία της καμπύλης. Τότε

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3).$$

Θέτουμε

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},\ x_1 \neq x_2$$

και επίσης

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

αν $x_1 \neq x_2$ και $P_2 \neq -P_1$. Αν είναι $P_3 = (x_3, y_3) = P_1 + P_2 \neq \mathcal{O}$ τότε οι συντεταγμένες του P_3 θα δίνονται από

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3.$$

Άλλη μία έννοια που θα μας χρειαστεί είναι αυτή της απεικόνισης μέσω του m πολλαπλασιασμού. Αυτή παίρνει ένα σημείο P και το στέλνει στο σημείο $P+P+...+P$, m φορές. Αυτή η απεικόνιση είναι ουσιαστικά η βάση για την κρυπτογραφία με ελλειπτικές καμπύλες.

7.2 Ελλειπτικές καμπύλες πάνω από πεπερασμένα σώματα.

Από εδώ και στο εξής θα δουλεύουμε πάνω από πεπερασμένα σώματα $\mathbb{F}_q$, εκεί δηλαδή που έχουμε τις εφαρμογές στην κρυπτογραφία. Κάτι που θα μας απασχολήσει αρκετά, είναι η εύρεση της τάξης των ρητών σημείων της $E(\mathbb{F}_q)$. Έστω ελλειπτική καμπύλη E ορισμένη πάνω από ένα σώμα $\mathbb{F}_q$. Ορίζουμε τον ενδομορφισμό του Frobenius να είναι η εξής απεικόνιση

$$\phi : \begin{cases} E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_p) \\ (x, y) & \longmapsto & (x^q, y^q) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{cases}$$

Το επόμενο θεώρημα που αποδείχθηκε από τον Hasse, δίνει ένα φράγμα της τάξης της E.

Θεώρημα 7.1 *Έστω $E(\mathbb{F}_q)$. Τότε θα είναι*

$$|E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}.$$

Απόδειξη. Βλέπε [8] ή κεφάλαιο 5, θεώρημα 1.1 [2].

Έστω $E(\mathbb{F}_q)$ με q περιττό αριθμό. Η ελλειπτική καμπύλη τότε θα είναι

$$Y^2 = X^3 + aX + b.$$

Αυτό που θέλουμε για την $|E(\mathbb{F}_q)|$ ουσιαστικά είναι τα σημεία για τα οποία το $X^3 + aX + b$ είναι τετραγωνικό υπόλοιπο modulo q. Έστω το σύμβολο του Legendre, με

$$\left(\frac{X^3 + aX + b}{q}\right).$$

Για κάθε x που του δίνουμε θα μας δίνει ± 1, ανάλογα με το αν έχουμε ή όχι τετραγωνικό υπόλοιπο. Επομένως αν πάρουμε το άθροισμα

$$\sum_q \left(1 + \left(\frac{X^3 + aX + b}{q}\right)\right),$$

θα έχουμε ότι η $|E(\mathbb{F}_q)|$ αν λάβουμε υπόψη και το άπειρο σημείο, ισούται με

$$|E(\mathbb{F}_q)| = 1 + \sum_q \left(1 + \left(\frac{X^3 + aX + b}{q}\right)\right) = 1 + q + \sum_q \left(\frac{X^3 + aX + b}{q}\right).$$

Αν συνδυάσουμε το αποτέλεσμα αυτό και το θεώρημα 7.1, τότε θα πάρουμε το εξής πόρισμα:

Πόρισμα 7.2

$$\left|\sum_q \left(\frac{X^3 + aX + b}{q}\right)\right| \leq 2\sqrt{q}.$$

Η τάξη λοιπόν μιας ελλειπτικής καμπύλης θα είναι ίση με

$$|E(\mathbb{F}_q)| = 1 + q - t,$$

όπου το t αυτό, ονομάζεται ίχνος του Frobenius. Ο υπολογισμός του ίχνους του Frobenius είναι αρκετά δύσκολος. Είναι κάτι που θα μας απασχολήσει στη συνέχεια, αφού το να ξέρουμε στην κρυπτογραφία την τάξη της ομάδας των ρητών σημείων μίας καμπύλης, είναι εξαιρετικής σημασίας. Το t ικανοποιεί την επόμενη εξίσωση, η οποία είναι η βασική ιδέα για τον αλγόριθμο του Schoof, που θα δούμε αργότερα και ο οποίος υπολογίζει ακριβώς αυτό το t. Είναι λοιπόν για ένα σημείο $P(x, y)$ της καμπύλης

$$\phi^2(P) - [t]\phi(P) + [q]P = [0] \Longleftrightarrow$$

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \mathcal{O}.$$

Να σημειώσουμε επίσης ότι υπάρχουν κάποια είδη ελλειπτικών καμπύλων, όπου πρέπει να αποφεύγεται η κρυπτογράφηση αφού είναι ευάλωτες σε επιθέσεις, κάποιες από τις οποίες θα δούμε αργότερα. Αν έχουμε $t = 1$ θα λέμε ότι η E είναι

ανώμαλη, αφού θα είναι $|E(\mathbb{F}_q)| = q$. Ενώ, όταν έχουμε την περίπτωση όπου η χαρακτηριστική p διαιρεί το ίχνος t, τότε θα καλούμε την E supersingular. Αποδεικνύεται ότι ότι μία E θα είναι supersingular αν έχουμε $p = 2$ ή $p = 3$ και $j(E) = 0$ ή αν $p \geq 5$ και $t = 0$. Εμείς θα ασχοληθούμε με σώματα χαρακτηριστικής 2, ή μεγαλύτερης του 3.

Έστω λοιπόν $K = \mathbb{F}_q$ με $q = p^n$ και $p > 3$. Έχουμε την $E(K)$ με

$$E : Y^2 = X^3 + aX + b.$$

Θα έχουμε ότι $\Delta = -16(4a^3 + 27b^2)$, ενώ η j-αναλλοίωτη $j(E) = -1728\frac{4a^3}{\Delta}$. Οι τύποι για τον νόμο ομάδας θα είναι $-P_1 = (x_1, -y_1)$ και αν είναι $x_1 \neq x_2$ τότε

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Αν είναι $x_1 = x_2$ θα έχουμε

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Έτσι αν θέλουμε να βρούμε το σημείο $P_3 = P_1 + P_2$ θα πρέπει να κάνουμε χρήση των τύπων

$$P_3 = (x_3, y_3) = (\lambda^2 - x_1 - x_2,\ (x_1 - x_3)\lambda - y_1).$$

Αν τώρα έχουμε σώματα με χαρακτηριστική 2, δηλαδή $q = 2^n,\ n \geq 1$ θα είναι $j(E) = \frac{a_1^{12}}{\Delta}$. Η ελλειπτική καμπύλη τότε θα έχει εξίσωση

$$E : Y^2 + XY = X^3 + a_2X^2 + a_6.$$

Θα έχουμε τώρα

$$-P_1 = (x_1, x_1 + y_1)$$

και αν $x_1 \neq x_2$

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2},\ \mu = \frac{y_1x_2 + y_2x_1}{x_1 + x_2},$$

ενώ αν $x_1 = x_2$

$$\lambda = \frac{x_1^2 + y_1}{x_1},\ \mu = x_1^2.$$

Έτσι λοιπόν για το $(x_3, y_3) = P_3 = P_1 + P_2$ θα είναι

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2,$$

$$y_3 = (\lambda + 1)x_3 + \mu.$$

7.3 Πολυώνυμα διαίρεσης.

Τα πολυώνυμα διαίρεσης θα τα συναντήσουμε στον αλγόριθμο του Schoof, όπου θα βρούμε την τάξη μιας ελλειπτικής καμπύλης. Εδώ θα τα ορίσουμε και θα αναφέρουμε κάποιες βασικές τους ιδιότητες.

Λήμμα 7.2 *Έστω E ελλειπτική καμπύλη, ορισμένη πάνω από το σώμα K και $m \in \mathbb{Z}_+$. Υπάρχουν πολυώνυμα $\psi_m, \theta_m, \omega_m \in K[x, y]$ τέτοια ώστε για $P = (x, y)$ σημείο της καμπύλης με $[m]P \neq \mathcal{O}$, έχουμε*

$$[m]P = \left(\frac{\theta_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3}\right)$$

Το πολυώνυμο ψ_m ονομάζεται πολυώνυμο διαίρεσης της καμπύλης E. Δίνουμε τον αναδρομικό τύπο που θα χρησιμοποιούμε για την εύρεση του πολυωνύμου διαίρεσης.

$$\psi_0 = 0, \psi_1 = 1,$$

$$\psi_2 = 2y + a_1x + a_3,$$

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$

$$\psi_4 = (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\psi_2,$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2,$$

$$\psi_{2m} = \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{\psi_2},\ m > 2.$$

Οι υπολογισμοί του πολυωνύμου διαίρεσης θα γίνονται πάντα modulo την καμπύλη μας, αφού μιλάμε για σημεία πάνω σε αυτήν. Τα πολυώνυμα θ_m και ω_m, ορίζονται συναρτήσει του ψ_m. Είναι δηλαδή :

$$\theta_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1},$$

$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

Η απόδειξη του λήμματος 7.2, έρχεται από αυτούς τους ορισμούς, τον νόμο ομάδας και φυσικά αρκετές πράξεις.

Ορισμός 7.10 *Αν έχουμε K πεπερασμένο σώμα, τότε το $E(\overline{K})$ είναι ένα torsion group δηλαδή κάθε σημείο P της E έχει πεπερασμένη τάξη. Αν έχουμε αριθμό $m \in \mathbb{Z}_+$, τότε το σύνολο των m-torsion σημείων της E, το οποίο θα συμβολίζουμε με $E[m]$, είναι το*

$$E[m] = \{P \in E(K) :\ [m]P = \mathcal{O}\}.$$

Είναι το σύνολο των σημείων της E, τάξης m.

Θεώρημα 7.2 *Έστω ένα σημείο $P \in E(K) \setminus \{0\}$ και $m \geq 1$. Τότε $P \in E[m]$ αν και μόνο αν $\psi_m(P) = 0$.*

Ορίζουμε το πολυώνυμο

$$f_m = \begin{cases} \psi_m, & m \text{ περιττός}, \\ \frac{\psi_m}{\psi_2}, & m \text{ άρτιος} \end{cases}$$

Παρατηρούμε ότι αυτά τα πολυώνυμα, δεν έχουν καθόλου μέσα τους τον όρο y, δηλαδή εξαρτώνται μόνο από το x. Οι τύποι όπου θα χρησιμοποιούμε για να παίρνουμε τα f, είναι:

$$f_0 = 0,\ f_1 = 1,\ f_2 = 1,\ f_3 = \psi_3,\ f_4 = \frac{\psi_4}{\psi_2},$$

$$f_{2m+1} = \begin{cases} f_{m+2}f_m^3 - F^2 f_{m-1}f_{m+1}^3, & m \text{ περιττός} \\ F^2 f_{m+2}f_{m^3} - f_{m-1}f_{m+1}^3, & m \text{ άρτιος} \end{cases}$$

$$f_{2m} = (f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)f_m$$

όπου $Y^2 = F(X)$, η εξίσωση της ελλειπτικής καμπύλης. (Για πιο αναλυτικούς τύπους ξεχωριστά για σώματα χαρακτηριστικής δύο και μεγαλύτερης του τρία βλέπε κεφάλαιο 3 [5].)

7.4 Το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες

Έστω μία ελλειπτική καμπύλη E πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$, και P ένα σημείο της. Το πρόβλημα του διακριτού λογάριθμου για ελλειπτικές καμπύλες (ΠΔΛΕΚ), είναι ότι αν έχουμε ένα σημείο $Q \in \langle P \rangle$, να βρεθεί ακέραιος αριθμός m, τέτοιος ώστε

$$Q = [m]P.$$

Αυτό που οφείλει ένας κρυπτογράφος να κάνει, είναι να καταφέρει να βρει κατάλληλες ελλειπτικές καμπύλες, ώστε το ΠΔΛΕΚ, να είναι υπολογιστικά αδύνατο να λυθεί για αυτές. Μέχρι στιγμής, τρεις είναι οι συνθήκες που επιβάλλεται να πληρεί μία ελλειπτική καμπύλη για να είναι ανθεκτική σε επιθέσεις. Θα τις αναφέρουμε απλώς, χωρίς να τις αναλύσουμε και να δούμε τις μεθόδους επίθεσης που χρησιμοποιούνται. (Για λεπτομέρειες αναφορά κεφάλαιο 5 [5]).

1. Η πρώτη επίθεση οφείλεται στους Pohlig-Hellman, οι οποίοι παρατήρησαν ότι το ΠΔΛ σε μια ομάδα G, μπορεί να αναχθεί σε ΠΔΛ υποομάδων αυτής της G, οι οποίες έχουν τάξη δυνάμεις πρώτων αριθμών και η τελική λύση να έρθει με μία εφαρμογή στο κινέζικο θεώρημα. Η λύση για να αποφύγουμε αυτήν την επίθεση, είναι να επιλέξουμε τέτοια ελλειπτική καμπύλη, ώστε η τάξη της να έχει έναν μεγάλο πρώτο διαιρέτη. Ο όρος μεγάλος είναι βέβαια σχετικός, αφού έχει να κάνει με την υπολογιστική ισχύ των Η/Υ.

2. Μία καμπύλη θα πρέπει να μην είναι ανώμαλη, δηλαδή να μην έχει ίχνος ίσο με 1. Τότε θα έχουμε $t = 1$ και η τάξη της θα είναι ίση με την τάξη του σώματος $\mathbb{F}_q$. Αυτό κάνει τις καμπύλες ιδιαίτερες και έτσι πιο ευάλωτες σε επιθέσεις.

3. Τέλος, πρέπει να ικανοποιείται η συνθήκη MOV η οποία πήρε το όνομά της από τους Menezes, Okamoto, Vanstone. Εδώ απαιτούμε η μικρότερη τιμή του l για την οποία να ισχύει $q^l \equiv 1 \bmod n$, να είναι αρκετά μεγάλη. Με αυτόν τον τρόπο εξαιρούμε τις καμπύλες οι οποίες έχουν ίχνος μηδέν και δύο πάνω από το $\mathbb{F}_p$, καθώς και τις supersingular καμπύλες, όπου η χαρακτηριστική διαιρεί το ίχνος.

Να δούμε και πως εφαρμόζεται το ΠΔΛΕΚ, σε ένα κρυπτοσύστημα δημοσίου κλειδιού, για παράδειγμα στο El Gamal. Θα υποθέσουμε ότι ο Β θέλει να στείλει ένα μύνημα P στην Α. Δημοσιοποιούν ένα πρώτο p και μία ελλειπτική καμπύλη $E(\mathbb{F}_p)$. Επίσης επιλέγεται και ένα σημείο $Q \in E(\mathfrak{F}_p)$, το οποίο είναι και αυτό δημόσιο. Επιλέγουν αντίστοιχα ακέραιους n και m, που τα κρατούν μυστικά και υπολογίζουν τα nQ και mQ, τα οποία κοινοποιούνται. Ο Β επιλέγει έναν τυχαίο, μυστικό ακέραιο r και υπολογίζει το ζεύγος $(rQ,\ P + r(mQ))$. Η Α λαμβάνει αυτά και υπολογίζει το mrQ, το οποίο θα είναι ίσο με το rmQ. Τέλος κάνει απλά μία αφαίρεση και παίρνει το μύνημα P, στα χέρια της.

$$P + rmQ - rmQ = P.$$

7.5 Τάξη ομάδας ελλειπτικής καμπύλης

Θα μελετήσουμε κάποιες τεχνικές, που χρησιμοποιούνται για τον υπολογισμό της τάξης της ομάδας των ρητών σημείων μιας ελλειπτικής καμπύλης, πάνω από

ένα πεπερασμένο σώμα. Αυτή η διαδικασία είναι πολύ σημαντική στις εφαρμογές στην κρυπτογραφία.

Προκειμένου να παράγουμε ελλειπτικές καμπύλες με δεδομένη τάξη μπορούμε:

1. Παράγουμε τυχαίες καμπύλες και μετά υπολογίζουμε τις τάξεις ομάδων, μέχρι να βρούμε την καταλληλότερη.

2. Παράγουμε καμπύλες, με προκαθορισμένη τάξη ομάδας, και ένας αποδοτικός τρόπος είναι κάνοντας χρήση της θεωρίας του μιγαδικού πολλαπλασιασμού.

Ας υποθέσουμε πως έχουμε μία καμπύλη με μορφή

$$Y^2 = X^3 + aX + b,$$

και θέλουμε να υπολογίσουμε τα ρητά σημεία της, πάνω από σώματα χαρακτηριστικής p. Αυτό που έχουμε να κάνουμε, είναι να υπολογίσουμε το

$$p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right),$$

όπου $(\frac{\cdot}{p})$ είναι το σύμβολο του Legendre. Αυτός ο τρόπος είναι αρκετά γρήγορος για μικρές τιμές του p, συγκεκριμένα για $p < 10000$, αλλά για μεγάλες τιμές είναι αδύνατον να γίνουν οι υπολογισμοί που απαιτούνται.

Η μέθοδος αυτήν την στιγμή που θεωρείται πιο ανθεκτική σε επιθέσεις, είναι πρώτα να επιλέξουμε ένα μεγάλο πεπερασμένο σώμα και έπειτα να διαλέξουμε τυχαίες ελλειπτικές καμπύλες πάνω από αυτό, των οποίων οι ομάδες των ρητών σημείων να ικανοποιούν τις συνθήκες που ορίσαμε προηγουμένως για την τάξη ομάδας. Η διαδικασία φυσικά, προϋποθέτει να μπορούμε να βρούμε την τάξη της ελλειπτικής καμπύλης. Θα περιγράψουμε στην επόμενη παράγραφο τον αλγόριθμο του Schoof, ο οποίος κάνει ακριβώς αυτήν την δουλειά, δηλαδή υπολογίζει κατάλληλες τάξεις ομάδων.

Άλλη μέθοδο, την οποία θα δούμε με αρκετές λεπτομέρειες, είναι αυτή του μιγαδικού πολλαπλασιασμού. Εδώ κάνοντας χρήση αυτής της θεωρίας, των ελλειπτικών καμπύλων με μιγαδικό πολλαπλασιασμό, θα παράγουμε καμπύλες που θα διαθέτουν μία κυκλική υποομάδα με τάξη έναν μεγάλο πρώτο. Οι υπολογισμοί που απαιτούνται εδώ, είναι αρκετά λιγότεροι από τις υπόλοιπες μεθόδους.

7.6 Έλεγχος της τάξης ομάδας

Ένα κοινό χαρακτηριστικό για αρκετούς αλγόριθμους, είναι ότι εμφανίζουν σαν αποτέλεσμα αρκετές τιμές m, για την τάξη ομάδας. Σε αυτήν την παράγραφο, θα δούμε πως μπορούμε να κάνουμε την σωστή επιλογή της τάξης που ψάχνουμε. Από το θεώρημα 7.1 έχουμε ότι για μία ελλειπτική καμπύλη E, πάνω από ένα σώμα με q στοιχεία και τάξη ομάδας m, θα ικανοποιεί την

$$|q + 1 - m| \leq 2\sqrt{q}.$$

Αρχικά λοιπόν, παίρνουμε από τον αλγόριθμο την πιθανή τιμή της τάξης ομάδας, m. Η πρώτη και προφανής δοκιμασία που πρέπει να περάσει το m είναι και σύμφωνα με το θεώρημα 7.1,

$$q + 1 - 2\sqrt{q} \leq m \leq q + 1 + 2\sqrt{q}.$$

Αφού δούμε ότι ισχύει αυτό, έπειτα θα διαλέξουμε τυχαία ένα σημείο P πάνω στην ελλειπτική καμπύλη και θα ελέγξουμε την συνθήκη

$$[m]P = \mathcal{O}.$$

Φυσικά αν αυτή δεν ισχύει, το m που έχουμε βρει δεν είναι το σωστό. Κάνουμε αυτή την διαδικασία για αρκετά σημεία της καμπύλης και έτσι βρίσκουμε τελικά το m. Στις εφαρμογές της κρυπτογραφίας τώρα, τα πράγματα είναι λίγο πιο απλά. Οι τιμές οι οποίες μας ενδιαφέρουν για την ασφάλεια του κρυπτοσυστήματος, είναι οι $m = sr$, όπου s ένας μικρός ακέραιος αριθμός και r ένας πρώτος. Αυτό δεν έχει ιδιαίτερη υπολογιστική δυσκολία να ελεγχθεί, αφού μπορούμε γρήγορα να κάνουμε διαιρέσεις και τεστ πρώτου αριθμού, για να δούμε αν όντος το m έχει αυτήν τη μορφή. Αν στη συνέχεια δούμε ότι είναι $[m]P = \mathcal{O}$, τότε θα κάνουμε και τον έλεγχο $[s]P = \mathcal{O}$. Αν ισχύει, πετάμε το σημείο αυτό και επιλέγουμε ένα άλλο τυχαίο πάλι, αν και η πιθανότητα να συμβεί αυτό είναι πολύ μικρή.

Ας δώσουμε τώρα έναν αλγόριθμο που παράγει ελλειπτικές καμπύλες, κατάλληλες για κρυπτογραφία.
Input: Ένα μεγάλο πεπερασμένα σώμα $\mathbb{F}_q$ και έναν μικρό θετικό ακέραιο s.
Output: Μία ελλειπτική καμπύλη πάνω από το $\mathbb{F}_q$, με $|E(\mathbb{F}_q)| = rs$, με r έναν μεγάλο πρώτο.

1. Διάλεξε μία τυχαία Ε.
2. Βρες $m = |E(\mathbb{F})_q|$.
3. Έλεγξε τις συνθήκες MOV και ανωμαλίας.
4. Παραγοντοποίησε το m, μέσα σε λογικό χρόνο. Αν αποτύχεις πήγαινε στο βήμα 1.
5. Αν $m = rs$ δώσε την E, αλλιώς πήγαινε στο βήμα 1.

Όπως εύκολα καταλαβαίνει κανείς, η δυσκολία εδώ έγκειται στο να βρούμε την τάξη της ελλειπτικής καμπύλης. Ένας από τους πιο αποτελεσματικούς αλγόριθμους που υπάρχουν αυτή την στιγμή, είναι αυτός που θα περιγράψουμε αμέσως και τον οφείλουμε στον Schoof.

7.7 Ο αλγόριθμος του Schoof.

Υπενθυμίζουμε ότι για σώματα με χαρακτηριστική 2, ενδιαφερόμαστε μόνο για μη ιδιόμορφες καμπύλες με μορφή

$$Y^2 + XY = X^3 + a_2X^2 + a_6.$$

Για σώματα με χαρακτηριστική περιττό αριθμό οι καμπύλες που θα ασχοληθούμε είναι

$$Y^2 = X^3 + aX + b, a, b \in \mathbb{F}_q.$$

Η ιδέα του αλγόριθμου του Schoof, στηρίζεται στο θεώρημα του Hasse 7.1. Είναι να βρούμε τιμές $t \bmod l$, όπου l πρώτοι αριθμοί με $l \leq l_{max}$, με το l_{max} να είναι ο μικρότερος πρώτος για τον οποίο

$$\prod_{2 \leq l \leq l_{max}} l > 4\sqrt{q}.$$

Τέλος με ένα κινέζικο θεώρημα υπολογίζουμε την μοναδική τιμή του t και φυσικά την τάξη της ελλειπτικής καμπύλης. Ας δούμε λοιπόν λίγο πιο αναλυτικά τα παραπάνω. Αρχικά παρατηρούμε ότι η εύρεση του $t \bmod 2$ είναι εύκολη και για τις δύο περιπτώσεις σωμάτων με χαρακτηριστική περιττό ή δύο. Όταν έχουμε χαρακτηριστική περιττό, θα είναι $m \equiv q + 1 - t \bmod 2 \Leftrightarrow m \equiv t \bmod 2$ και αποδεικνύεται ότι $m = 1 \bmod 2$ αν και μόνο αν το $X^3 + aX + b$ είναι ανάγωγο πάνω από το $\mathbb{F}_q$. Για χαρακτηριστική 2 τώρα, από την στιγμή που η καμπύλη μας δεν είναι ιδιόμορφη, είναι $t \equiv 1 \bmod 2$. Οπότε ουσιαστικά, έχουμε να κάνουμε με πρώτους $l > 2$. Θα χρειαστούμε τον ενδομορφισμό ϕ του Frobenius, ο οποίος

$$\phi : \begin{cases} E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_p) \\ (x, y) & \longmapsto & (x^q, y^q) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{cases}$$

Αυτός θα ικανοποιεί την εξίσωση

$$\phi^2(P) - [t]\phi(P) + [q]P = \mathcal{O}.$$

Θεωρούμε τώρα την εξίσωση αυτή για σημεία που ανήκουν στο

$$E[l]^* = \{P \in E(\mathbb{F}_q),\ [l]P = \mathcal{O},\ P \neq \mathcal{O}\}.$$

Συμβολίζουμε επίσης $t_l \equiv t \bmod l,\ q_l \equiv q \bmod l$ να είναι οι μικρότεροι θετικοί αντιπρόσωποι της κλάσης ισοδυναμίας. Αυτό που κάνει ο Schoof είναι το εξής. Βρίσκει ένα σημείο $P(x, y) \in E(\mathbb{F}_q)$. Αυτό θα ικανοποιεί την

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau_l](x^q, y^q)].$$

Παίρνουμε όλα τα τ από το $\{0, ..., l-1\}$, τα βάζουμε στην εξίσωση και τσεκάρουμε ποιο θα την ικανοποιεί. Έπειτα επιλέγουμε άλλο τ και κάνουμε το ίδιο. Αυτά τα τ που θα βρούμε, θα αποτελέσουν το σύστημά μας, το οποίο όπως είπαμε θα λυθεί με κινέζικο θεώρημα και θα μας δώσει την λύση του t που ζητάμε και συνεπώς την τάξη της ομάδας. Ο αλγόριθμος βέβαια απαιτεί κάποιες πράξεις. Θα χρησιμοποιήσουμε τους τύπους για την πρόσθεση σημείων από την παράγραφο 7.2 και για τα $[\kappa]P$ από το λήμμα 7.2 της παραγράφου 7.3. Πρώτα υπολογίζουμε τις x συντεταγμένες και στα δύο μέλη. Αυτές θα θα είναι πολυωνυμικές εξισώσεις των x, y και θα περιέχουν και τα πολυώνυμα διαίρεσης. Επειδή δουλεύουμε modulo την καμπύλη μας, ο μεγαλύτερος βαθμός που θα έχουν οι όροι με y, θα είναι ένα. Φτάνουμε έτσι σε μία εξίσωση της μορφής $y = a(x)/b(x)$ και την αντικαθιστούμε στην εξίσωση της καμπύλης. Στο τέλος λοιπόν, θα είναι $h_X(x) = 0$. Μία παρατήρηση η οποία θα βοηθήσει αρκετά στις πράξεις, είναι ότι αφού τα σημεία $P \in E[l]$, μπορούμε να κάνουμε τις τις πολυωνυμικές πράξεις modulo f_l. Για την εύρεση τώρα μιας λύσης της $h_X(x) = 0$, πρέπει να βρούμε τον μέγιστο κοινό διαιρέτη των $h_X(x)$ και f_l. Αν $gcd(h_X(x),\ f_l) = 1$, τότε δεν υπάρχει λύση και δοκιμάζουμε την επόμενη τιμή του τ. Αν ο μέγιστος κοινός διαιρέτης είναι διάφορος του ένα, τότε θα υπάρχει ένα σημείο στο $E[l]^*$ τέτοιο ώστε

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = \pm[\tau](x^q, y^q).$$

Αφού η διαδικασία ελέγχει τις τιμές $\pm\tau$, αρκεί ο έλεγχος να γίνει μόνο για $\tau \in \{0, ..., (l-1)/2\}$. Το επόμενο βήμα είναι να κάνουμε την ίδια διαδικασία και για την y-συντεταγμένη, με τον ίδιο τρόπο. Τέλος, αυτή η δουλειά θα γίνει κι

άλλες φορές για να καταλήξουμε σε ένα σύστημα από ισοδυναμίες modulo πρώτοι αριθμοί, και λύνοντάς το με κινέζικο θεώρημα βρίσκουμε την τιμή του ίχνους του Frobenius t, που σημαίνει ότι έχουμε την τάξη της ελλειπτικής καμπύλης, $m = q + 1 - t$.

Στην επόμενη παράγραφο, θα περιγράψουμε μία άλλη μέθοδο παραγωγής καμπύλων, αυτήν του μιγαδικού πολλαπλασιασμού.

7.8 Η θεωρία του Μιγαδικού Πολλαπλασιασμού.

Ορισμός 7.11 *Έστω ότι έχουμε δύο ελλειπτικές καμπύλες E_1, E_2. Όλες οι απεικονίσεις*

$$\phi : E_1 \to E_2,$$

που στέλνουν το ταυτοτικό στοιχείο της E_1 στο ταυτοτικό της E_2, θα καλούνται ισογένειες. Η απεικόνιση που στέλνει κάθε στοιχείο της E_1 στο μηδενικό της E_2 είναι και αυτή μία ισογένεια και καλείται η ισογένεια του μηδενός.

Ορισμός 7.12 *Όλες οι ισογένειες από μία ελλειπτική καμπύλη E στον εαυτό της, μαζί με την ισογένεια του μηδενός, σχηματίζουν δακτύλιο. Αυτός είναι ο δακτύλιος των ενδομορφισμών της E, και θα τον συμβολίζουμε $End(E)$.*

Ορισμός 7.13 *Έστω K μία επέκταση του $\mathbb{Q}$. Μία order R του K, είναι ένας υποδακτύλιος του K, πεπερασμένα παραγόμενος σαν $\mathbb{Z}$-module και ο οποίος να ικανοποιεί*

$$R \otimes \mathbb{Q} = K.$$

Παράδειγμα 7.1 *Για παράδειγμα, αν έχουμε $K = \mathbb{Q}(\sqrt{-d})$, και $\mathfrak{D}$ ο δακτύλιος των ακεραίων του, τότε για κάθε $k \in \mathbb{Z}$ ο δακτύλιος $\mathbb{Z} + k\mathfrak{D}$ είναι μία order του $\mathbb{Q}(\sqrt{-d})$.*

Η δομή που μας ενδιαφέρει του $End(E)$, είναι αυτή της order ενός τετραγωνικού μιγαδικού σώματος αριθμών. Τότε ο $End(E)$ είναι αυστηρά μεγαλύτερος από το $\mathbb{Z}$ και σε αυτήν την περίπτωση θα λέμε ότι η ελλειπτική καμπύλη έχει μιγαδικό πολλαπλασιασμό.

Μία ελλειπτική καμπύλη E, είναι ισόμορφη με το $\mathbb{C}$ modulo L, όπου L ένα πλέγμα. Κάθε πλέγμα του $\mathbb{C}$ παράγεται από τα διανύσματα $\langle w_1, w_2 \rangle$. Δύο ομόθετα πλέγματα Λ_1, Λ_2, δηλαδή δύο πλέγματα για τα οποία υπάρχει μιγαδικός z τέτοιος ώστε $\Lambda_1 = z\Lambda_2$, δίνουν ισόμορφες ελλειπτικές καμπύλες και μπορούμε να θεωρήσουμε πλέγματα που να παράγονται από τα $\{1, \tau\}$, με $\tau \in \mathbb{H}$, όπου $\mathbb{H}$ συμβολίζει το υπερβολικό επίπεδο:

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

Παρατηρούμε ότι για να παράγουν δύο βάσεις $\{1, \tau_1\}$, $\{1, \tau_2\}$ το ίδιο πλέγμα, πρέπει και αρκεί να διαφέρουν κατά αντιστρέψιμο 2×2-πίνακα με στοιχεία από το $\mathbb{Z}$, δηλαδή με στοιχείο της $SL_2(\mathbb{Z})$. Δηλαδή το σύνολο των πλεγμάτων που δίνουν μη ισόμορφες ελλειπτικές καμπύλες ταυτίζεται με τον χώρο

$$Y := \mathbb{H}/SL_2(\mathbb{Z}).$$

Η συνάρτηση j είναι μία αναλοίωτος του χώρου των ελλειπτικών καμπύλων και μπορούμε να δούμε ότι ορίζει μερόμορφη συνάρτηση

$$Y \to \mathbb{C}$$

που να στέλνει την κλάση του $z \bmod SL_2(\mathbb{Z})$ στον $j(z)$. Αποδεικνύεται, ότι η j συνάρτηση επάγει μία μιγαδική αναλυτική συνάρτηση $j : \mathbb{H} \to \mathbb{C}$, η οποία είναι αναλλοίωτη κάτω από τα στοιχεία της $SL_2(\mathbb{Z})$, δηλαδή

$$j(\gamma z) = j(z), \text{ για κάθε } \gamma \in SL_2(\mathbb{Z}). \tag{7.2}$$

Παρατηρούμε ότι το στοιχείο $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ στέλνει το $\mathbb{H} \ni z \mapsto z+1 \in \mathbb{H}$, συνεπώς η εξίσωση (7.2) δίνει ότι η j-συνάρτηση είναι περιοδική και δέχεται μία ανάλυση Fourier

$$j(q) = \frac{1}{q} + \sum_{\nu=0}^{\infty} c(n) q^n,$$

όπου $q = e^{2\pi i z}$. Οι συντελεστές $c(n)$ μπορούν να υπολογιστούν και για παράδειγμα έχουμε ότι

$$j(q) = \frac{1}{q} + 744 + 19688q + 21493760q^2 + 864299970q^3 + 20245856256q^4 \tag{7.3}$$

$$+333202640600q^5 + 4252023300096q^6 + 44656994071935q^7 + 401490886656000q^8$$

$$+3176440229784420q^9 + 22567393309593600q^{10} + 146211911499519294q^{11}$$

$$+874313719685775360q^{12} + 4872010111798142520q^{13}$$

Έστω $End(E)$, ο δακτύλιος των ενδομορφισμών μιας ελλειπτικής καμπύλης E, μη ιδιόμορφης. Τότε ο δακτύλιος αυτός θα είναι ίσος με το $\mathbb{Z}$, ή με μία order ενός τετραγωνικού μιγαδικού σώματος αριθμών. Αν ισχύει το τελευταίο, όπου έχουμε περίπτωση μιγαδικού πολλαπλασιασμού, θα είναι $End(E) \cong \mathbb{Z} + \mathbb{Z}_\tau$.

Παράδειγμα 7.2 *Έστω σώμα K χαρακτηριστικής διαφορετικής του 2, και ας θεωρήσουμε την ελλειπτική καμπύλη ορισμένη στο K με εξίσωση*

$$E : y^2 = x^3 - x.$$

Σε κάθε ελλειπτική καμπύλη το $\mathbb{Z}$ είναι υποδακτύλιος του δακτυλίου των ενδομορφισμών αφού το τυχαίο $m \in \mathbb{Z}$, ορίζει τον ενδομορφισμό

$$[m] : E \to E,$$

$$P \mapsto mP = P + \ldots + P$$

Επιπλέον η E επιδέχεται και τον ενδομορφισμό

$$[i] : (x, y) \mapsto (-x, iy),$$

όπου i είναι μία πρωταρχική τέταρτη ρίζα της μονάδας. Είναι σαφές ότι $[i] \circ [i] = [-1]$, συνεπώς το $[i]$ δεν είναι ενδομορφισμός του $\mathbb{Z}$, και η μέγιστη τάξη $\mathbb{Z}[i] \subseteq End(E)$, άρα $End(E) = \mathbb{Z}[i]$.

Το βασικό θεώρημα των ελλειπτικών καμπύλων είναι

Θεώρημα 7.3 *Έστω $\tau \in \mathbb{H}$ να είναι ένας μιγαδικός αλγεβρικός αριθμός βαθμού 2. Τότε αν θέσουμε $E_\tau = \frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}}$, έχουμε ότι η ελλειπτική καμπύλη E_τ έχει μιγαδικό πολ/σμό, και ότι το $j(\tau)$ είναι ακέραιος αλγεβρικός. Επιπλέον το σώμα $K(j(\tau))$ είναι το Hilbert class field του σώματος K.*

Παράδειγμα 7.3 *Είναι γνωστό ότι υπάρχουν 9 μόνο μιγαδικά τετραγωνικά σώματα αριθμών με class number 1, τα*

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}),$$
$$\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}),$$
$$\mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163}).$$

Το παραπάνω ήταν μία εικασία του Gauss και αποδείχτηκε από τον Heegner. Το θεώρημα 7.3 μας εξασφαλίζει ότι

$$j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}.$$

Πράγματι αν αντικαταστήσουμε στον τύπο (7.3) την τιμή $\tau = \frac{1+\sqrt{-163}}{2}$ έχουμε [1]

```
?\p 100
%1 realprecision = 105 significant digits (100 digits displayed)
? t=(1+sqrt(-163))/2
%2 = 1/2 + 6.383572667401852330855476004890446173691181890150629425606301491924363086445119629779711741933765936*I
?x=2*Pi*I*t
%3 = -40.109169991132519755350083622904140053900534812458734406107015404701087892483085085878768851896494 3.141592653589793238462643383279502884197169399375105820974944592307816406286208998628034825342117068*I
?? y=exp(x)
%4 = -3.8089809370076523382262315164780054376196293193805973008790063609106204563666457118764923048099625 56 E-18 + 4.9823194709407332451152918416189002713812702505761935765504952944647966712954581762380783561872610 87 E-123*I
```

Δηλαδή η τιμή $q = e^{2*\pi*i*\tau} \cong -3.8089 * 10^{-18}$ Στην συνέχεια παρατηρούμε ότι για μικρές τιμές η συνεισφορά στο ανάπτυγμα Fourier στον τύπο (7.3) είναι από το $1/q$. Υπολογίζουμε και πάλι ότι

```
? 1/y
%5 = -262537412640768743.99999999999925007259719818568887935385633733699086270753741037821064791011860731293 -rare se fnm 3.434108189257855572773640382466514643819410392802921231010082353528515643600406171384239278930629331 E-88*I
```

[1] Οι παρακάτω πράξεις έγιναν στο πρόγραμμα gp-pari

Δηλαδή (και γνωρίζοντας ότι το $j(\tau)$ είναι ένας ακέραιος αλγεβρικός στο $\mathbb{Q}$, δηλαδή ένας ακέραιος) έχουμε ότι η πραγματική τιμή του $j(\tau)$ είναι

$$j(\tau) - 262537412640768744.$$

Παρατήρηση: Ο αριθμός $1/q$ που χρησιμοποιήσαμε για να υπολογίζουμε μία προσέγγιση του $j(\tau)$, είναι υπερβατικός αφού μπορούμε να υπολογίσουμε ότι

$$\frac{1}{q} = e^{\pi\sqrt{163}},$$

και το θεώρημα Gel'fond-Schneider λέει ότι $e^{\pi a}$ είναι υπερβατικός αν ο a αλγεβρικός βαθμού τουλάχιστον 2. Το $j(\tau)$ είναι ακέραιος, χάρη στην συνεισφορά των υπόλοιπων άπειρων προσθεταίων του αναπτύγματος Fourier.

Παρατήρηση: Ένα άλλο θέμα που πρέπει να μας απασχολήσει εδώ, είναι ότι για να κάνουμε αποτελεσματικά πράξεις με την συνάρτηση j, θα πρέπει να μπορούμε να κάνουμε πράξεις κινητής υποδιαστολής με μεγάλη ακρίβεια. Αυτό είναι ένα εμποδιο στην υλοποίηση των αλγορίθμων αυτής της μορφής σε συστήματα με μικρή υπολογιστική ισχύ, όπως hand held devices, smart cards κινητά τηλεφωνα.

Παράδειγμα 7.4 *Ας κάνουμε τώρα ένα παράδειγμα σε ένα τετραγωνικό μιγαδικό σώμα αριθμών που να έχει class number μεγαλύτερο της μονάδας. Το σώμα* $\mathbb{Q}(\sqrt{-15})$ *, το οποίο έχει δακτύλιο ακαιρέων* $\mathfrak{D} = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$*. Ο αριθμός κλάσεων είναι ίσος με 2, όπως μπορούμε να υπολογίσουμε με το χέρι ή με το gp-pari.*

```
? qfbclassno(-15)
%6 = 2
```

Κάνοντας χρήση του νόμου ανάλυσης, παρατηρούμε ότι το σώμα

$$H = \mathbb{Q}(\sqrt{5}, \sqrt{-3}),$$

δεν διακλαδίζεται πουθενά πάνω από το K*, άρα είναι το Hilbert class field του* K*. Το Hilbert class field είναι το* $K(j(\mathfrak{D}))$*, όποτε το* $\mathbb{Q}(j(\mathfrak{D}))$ *είναι μια τετραγωνική επέκταση του* $\mathbb{Q}$ *που περιέχεται στο* H*, αλλά δεν είναι το* K*. Συνεπώς, το* $\mathbb{Q}(j(\mathfrak{D}))$ *είναι το* $\mathbb{Q}(\sqrt{5})$*, ή το* $\mathbb{Q}(\sqrt{-3})$*.*

Θα χρειαστούμε το παρακάτω

Λήμμα 7.3 *Έστω* $\mathfrak{a}$ *ένα κλασματικό ιδεώδες του* $\mathfrak{D}$ *και έστω* E *μία ελλειπτική καμπύλη που να αντιστοιχεί στο* $\mathfrak{a}$*. Τότε ισχύει ότι*

$$\bar{\mathfrak{a}}^2 = 1 \text{ στην } Cl(\mathfrak{D}) \Leftrightarrow j(a) \in \mathbb{R}.$$

Απόδειξη. Βλέπε άσκηση 2.9 [10].

Με βάση το προηγούμενο λήμμα έχουμε ότι $\mathbb{Q}(j(\mathfrak{D})) = \mathbb{Q}(\sqrt{5})$. Ένα ιδεώδες που δεν είναι κύριο στον $\mathfrak{D}$ είναι το $\mathfrak{a} = 2\mathbb{Z} + a\mathbb{Z}$.

Ας υποθέσουμε ότι

$$j(\mathfrak{D}) = A + B\sqrt{5}$$

τότε

$$j(\mathfrak{a}) = A - B\sqrt{5},$$

οπότε έχουμε

$$A = \frac{j(\mathfrak{D}) + j(\mathfrak{a})}{2} \text{ και } B = \frac{j(\mathfrak{D}) - j(\mathfrak{a})}{2\sqrt{5}}.$$

Υπολογίζουμε ότι

$$j(\mathfrak{D}) = j(\mathbb{Z}+a\mathbb{Z}) = j(-e^{-\sqrt{15}\pi}) \cong j(-5.19748331238\cdot 10^{-6}) \cong -191657.832863.$$

Επίσης υπολογίζουμε ότι

$$j(\mathfrak{a}) = j(2\mathbb{Z} + a\mathbb{Z}) = j\left(\mathbb{Z} + \frac{1}{2}a\mathbb{Z}\right) = j(e^{-\sqrt{15}\pi/2}i)$$

$$\cong j(2.27979896315 \cdot 10^{-3}i) = 632.83286254$$

Κάνοντας χρήση των παραπάνω έχουμε

$$A = -95512.5000002 \text{ και } B = -42997.5000001,$$

συνεπώς

$$j(\mathfrak{D}) = -52512 - 85995\frac{1+\sqrt{5}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}.\right]$$

Ξέρουμε ότι δύο ελλειπτικές καμπύλες $E_1,\ E_2$ ορισμένες πάνω από ένα σώμα K που είναι ισόμορφες έχουν την ίδια j-αναλλοίωτο. Αντιστρόφως, αν δύο ελλειπτικές καμπύλες έχουν την ίδια j-αναλλοίωτο, τότε είναι ισόμορφες, αλλά ο ισομορφισμός ορίζεται πάνω από μία τετραγωνική εν γένει επέκταση του K. Δηλαδή αν το K είναι ένα μη αλγεβρικά κλειστό σώμα έχουμε δύο το πολύ ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο.

Έστω p ένας πρώτος του $\mathbb{Z}$, ο οποίος αναλύεται πλήρως στην επέκταση $K/\mathbb{Q}$, δηλαδή $p\mathfrak{D}_K = P_1P_2$. Θεωρούμε το πολυώνυμο Hilbert, $H_D(x) \in \mathbb{Z}[x]$. Σύμφωνα με τον νόμο ανάλυσης, το πολυώνυμο $H_D(x)$ αναλύεται πλήρως modulo p, αν και μόνο αν τα ιδεώδη P_i αναλύωνται πλήρως στην επέκταση H/K. Αυτό όμως σημαίνει ότι είναι κύρια αφού το H είναι το σώμα Hilbert. Άρα $P_i = a_i\mathfrak{D}_K$ και επίσης $a_1 = \bar{a}_2$. Άρα το ίχνος του Frobenious είναι ίσο με $a_1 + \bar{a_2} = tr(a_i)$ και η νόρμα είναι $a_1a_2 = p$.

Έχουμε δύο ιδιαίτερες τιμές του j, για $j = 0$ ή για $j = 1728$. Η μορφή που θα έχουν οι καμπύλες μας, για τις διάφορες τιμές του j, θα είναι:

1. Αν $j = 0$, τότε $Y^2 = X^3 - 1$
2. Αν $j = 1728$, τότε $Y^2 = X^3 - X$
3. Αν $j \neq 0, 1728$ τότε θέτουμε $c = \frac{j}{j-1728}$ και οι δύο ελλειπτικές καμπύλες μας είναι $Y^2 = X^3 - 3cX + 2c$ και $Y^2 = X^3 - 3ca^2X + 2ca^3$, όπου το a δεν είναι τετράγωνο στο K.

Θεώρημα 7.4 *Αν το K είναι το πεπερασμένο σώμα $\mathbb{F}_p$, και $j_0 \in \mathbb{F}_p$, $j \neq 0, 1728 \bmod p$, τότε οι δύο ελλειπτικές καμπύλες E_1, E_2 που έχουν j-ανναλοίωτο j_0 θα έχουν τάξεις*

$$|E_1| = p + 1 - t,\ |E_2| = p + 1 + t.$$

Απόδειξη: Βλέπε λήμμα $VIII.3$, [5].

Θεώρημα 7.5 *Έστω τ όπως ορίστηκε πριν και με διακρίνουσα $-D$. Δηλαδή $-D$ είναι η διακρίνουσα της πρωταρχικής τετραγωνικής μορφής $Q(x,y)$, η οποία έχει το τ σαν ρίζα της $Q(x,1)=0$. Έστω h_D ο αριθμός κλάσεων της order με διακρίνουσα $-D$. Τότε το $j(\tau)$ είναι ακέραιος αλγεβρικός και το ελάχιστο πολυώνυμό του δίνεται από*

$$H_D(x) = \prod (x - j(\alpha)),$$

όπου το α διατρέχει όλους τους μιγαδικούς αριθμούς τέτοιους ώστε, το $(\alpha,1)$ να είναι μία ρίζα μιας εκ των h_D το πλήθος ανηγμένων πρωταρχικών μορφών διακρίνουσας $-D$.

Παρατήρηση: Ο υπολογισμός του πολυώνυμου Hilbert με βάση το παραπάνω θεώρημα απαιτεί πράξεις κινητής υποδιαστολής με μεγάλη ακρίβεια και εν γένει οι συντελεστές του πολυωνύμου Hilbert είναι πάρα πολύ μεγάλοι.

7.9 Η μέθοδος κατασκευής ελλειπτικών καμπύλων

Παρατηρούμε ότι το θεώρημα του Hasse εξασφαλίζει ότι η ποσότητα $4p-(p+1-m)^2$ είναι θετική, άρα μπορούμε να γράψουμε

$$4p = u^2 + Dv^2, \tag{7.4}$$

για κάποιον ακέραιο u που ικανοποιεί

$$m = p + 1 \pm u.$$

Κάνοντας σύκριση με το θεώρημα 7.4, παρατηρούμε ότι αν κατασκευάσουμε μία ελλειπτική καμπύλη με μιγαδικό πολλαπλασιασμό όπου το πλέγμα κατασκευής να είναι ο δακτύλιος ακεραίων αλγεβρικών $\mathbb{Q}(\sqrt{-D})$, τότε η αναγωγή της modulo p θα δώσει δύο ελλειπτικές καμπύλες με τάξεις $m = p+1\pm u$. Επιπλέον η λύση της (7.4), κατασκευάζει τους γεννήτορες $a_i = \pm(u+\sqrt{-D}v)/2$ των ιδεωδών P_i του $\mathfrak{D}_K$ της προηγούμενης παραγάφου.

Η υλοποίηση του αλγορίθμου έχει ως εξής

1. Ξεκινάμε με ένα μεγάλο πρώτο.
2. Διαλέγουμε την μικρότερη διακρίνουσα και ακέραιους u, v ώστε να έχει λύση η (7.4).
3. Έλεγχουμε αν κάποια από τις $p+1\pm u$ είναι ικανοποιητική τάξη ελλειπτικής καμπύλης, αν όχι επαναλαμβάνουμε την διαδικασία από το στάδιο επιλογής πρώτου.
4. Αν ναι, υπολογίζουμε το πολυώνυμο Hilbert και μία ρίζα του modulo p, έστω j_0. Η ρίζα αυτή είναι η j-αναλλοίωτος που ψάχνουμε.
5. Κατασκευάζουμε τις δύο ελλειπτικές καμπύλες με j-αναλλοίωτο ίση με j_0 και διαλέγουμε αυτή που να έχει την επιθυμητή τάξη.

Ας δούμε μερικά παραδείγματα κατασκευής ελλειπτικών καμπύλων, με μιγαδικό πολλαπλασιασμό.

Παράδειγμα 7.5 *Εστω ότι έχουμε $D = 7$. Θέλουμε έναν αριθμό p, τέτοιον ώστε η $4p = u^2 + Dv^2$ να έχει μία λύση. Βρίσκουμε ότι για*

$$p = 781221660082682887337352611537,$$

έχουμε λύση $(u,\ v)$, οπότε θα προσπαθήσουμε να βρούμε μία ελλειπτική καμπύλη πάνω από το $\mathbb{F}_p$, με τάξη ομάδας ίση με

$$m = p - 1 \pm u = 781221660082681210712714541668$$

$$= s \cdot r = 4 \cdot 195305415020670302678178635417,$$

όπου r είναι ένας πρώτος αριθμός. Γνωρίζουμε ότι η class number του $\mathbb{Q}(\sqrt{-7})$ είναι ίση με ένα, επομένως ο βαθμός του πολυωνύμου Hilbert είναι και αυτός ίσος με ένα. Έπειτα υπολογίζουμε το πολυώνυμο Hilbert, το οποίο είναι

$$H_D(x) = x + 3375,$$

και προφανώς έχει μία ρίζα $\mathrm{mod} p$. Άρα ζητάμε μία ελλειπτική καμπύλη με j-αναλλοίωτο, ίση με

$$j(E) \equiv -3375 \equiv 781221660082682887337352608162 \bmod p.$$

Έχουμε δύο καμπύλες $E_1,\ E_2$ με την ίδια j, οι οποίες είναι

$$E_1 : Y^2 = X^3 + 384410658113592332551520525329 4X$$

$$+77708821214573747523503857655 4$$

και την

$$E_2 : Y^2 = X^3 + 586337137088968521507562977329X$$

$$+47061287768828409351193075021 3.$$

Η E_2 είναι αυτή η οποία έχει τάξη m.

Παράδειγμα 7.6 *Ας δούμε και ένα παράδειγμα όπου η class group είναι μεγαλύτερη του ένα. Έστω $D = 292$. Υπολογίζουμε την class group του $\mathbb{Q}(\sqrt{-292})$ και την βρίσκουμε ίση με 4. Όπως και στο προηγούμενο παράδειγμα, ψάχνουμε να βρούμε για ποιο p έχει λύση η $4p = u^2 + Dy^2$ και είναι για*

$$p = 47106401771464858174371611525 3.$$

Βρίσκουμε την τάξη ομάδας της ελλειπτικής καμπύλης ίση με

$$m = 4710640177146476307254985828 02.$$

Το πολυώνυμο Hilbert θα έχει βαθμό 4, και υπολογίζεται να είναι

$$H_D(x) = x^4 - 20628770986042830460800 0x^3$$

$$-93693622511929038759497066112000000x^2$$

$$+45521551386379385269629968384000000000x$$

$$-38025946104251240477999064268800000000000000,$$

το οποίο έχει 4 ρίζες $\bmod p$. *Αυτές οι ρίζες είναι οι 4* j*-αναλλοίωτες των ελλειπτικών καμπύλων με τάξη* m *πάνω από το* $\mathbb{F}_p$. *Μία τέτοια αναλοίωτος είναι η*

$$j = 952981631055855428990768234 35,$$

από την οποία παίρνουμε τις εξής ελλειπτικές καμπύλες:

$$E_1 : Y^2 = X^3 + 469268436428246725781035134277X$$

$$+155824285047281623272784717767$$

και

$$E_2 : Y^2 = X^3 + 354618739573347813123389093324X$$

$$+314551778593054362590879954574.$$

Η E_2 *είναι πάλι η καμπύλη που έχει τάξη* m, *επομένως είναι αυτή που θα χρησιμοποιήσουμε. Φυσικά και από τις υπόλοιπες ρίζες του* $H_D(x)$, *οι οποίες είναι οι* j*-αναλλοίωτες άλλων ελλειπτικών καμπυλών, μπορούμε να πάρουμε καμπύλες με τάξη* m.

Κεφάλαιο 8

Τετραγωνικές μορφές

Εμφανίζεται λοιπόν η ανάγκη για τη μελέτη των τετραγωνικών μορφών. Για την ακρίβεια θα μελετήσουμε τις ακέραιες τετραγωνικές μορφές δύο μεταβλητών

$$f(x,y) = ax^2 + bxy + cy^2,\ a,b,c \in \mathbb{Z}.$$

Αυτή η θεωρία πρώτα αναπτύχθηκε από τον Lagrange ο οποίος εισήγαγε τις έννοιες της διακρίνουσας, της ισοδυναμίας και της ανηγμένης μορφής (reduced form). Σε συνδυασμό με την έννοια του Gauss της γνήσιας ισοδυναμίας, ολοκληρώνονται τα βασικά στοιχεία που χρειαζόμαστε για την μελέτη της βασικής θεωρίας των τετραγωνικών μορφών. Ξεκινάμε δίνοντας μερικούς βασικούς ορισμούς.

Ορισμός 8.1 *Μία μορφή $ax^2+bxy+cy^2$, καλείται πρωταρχική, αν οι συντελεστές a,b,c είναι πρώτοι μεταξύ τους.*

Η μελέτη μας θα περιοριστεί μόνο στις πρωταρχικές μορφές. Να σημειώσουμε, ότι κάθε τετραγωνική μορφή είναι το ακέραιο πολλαπλάσιο κάποιας πρωταρχικής.

Ορισμός 8.2 *Θα λέμε ότι ένας ακέραιος αριθμός m απεικονίζεται από μία μορφή, αν η εξίσωση*

$$m = f(x,y)$$

έχει ακέραια λύση (x,y). Αν οι x και y είναι και αυτοί πρώτοι μεταξύ τους, τότε θα λέμε ότι ο m απεικονίζεται γνήσια από την $f(x,y)$.

Ορισμός 8.3 *Δύο μορφές $f(x,y)$ και $g(x,y)$ θα λέγονται ισοδύναμες αν υπάρχουν ακέραιοι p,q,r,s τέτοιοι ώστε*

$$f(x,y) = g(px+qy, rx+sy) \text{ και } ps - pr = \pm 1$$

Παρατηρούμε ότι η ορίζουσα

$$\begin{vmatrix} p & q \\ r & s \end{vmatrix} = \pm 1,$$

δηλαδή ο πίνακας $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ θα ανήκει στην ομάδα $GL(2,\mathbb{Z})$. Σύμφωνα λοιπόν με τους ορισμούς που έχει δώσει ο *Gauss*, θα έχουμε τα εξης

Ορισμός 8.4 *Μία ισοδυναμία θα καλείται γνήσια ισοδυναμία, αν* $ps - qr = 1$, *δηλαδή ο πίνακας* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL(2,\mathbb{Z})$. *Μία ισοδυναμία θα καλείται μη γνήσια ισοδυναμία αν* $ps - qr = -1$.

Λήμμα 8.1 *Μία μορφή* $f(x,y)$ *απεικονίζει γνήσια έναν ακέραιο αριθμό* m, *αν και μόνο αν η* $f(x,y)$ *είναι γνήσια ισοδύναμη με τη μορφή* $mx^2 + bxy + cy^2$ *για κάποιους ακέραιους* b, c.

Απόδειξη. Έχουμε ότι $f(x,y) = m$ με $(p,q) = 1$. Μπορούμε επομένως να βρούμε $r, s \in (Z)$, τέτοιους ώστε $ps - qr = 1$ και τότε θα είναι

$$f(px+ry, qx+sy) = f(p,q)x^2 + (f(p,s)+f(r,q))xy + f(r,s)y^2 = mx^2 + bxy + cy^2.$$

Για το αντίστροφο παρατηρούμε ότι η $mx^2 + bxy + cy^2$ απεικονίζει γνήσια το m παίρνοντας $(x,y) = (1,0)$.

Δίνουμε στην συνέχεια τον ορισμό της διακρίνουσας.

Ορισμός 8.5 *Διακρίνουσα λοιπόν* D *της μορφής* $ax^2 + bxy + cy^2$, *ορίζουμε την ποσότητα* $D = b^2 - 4ac$.

Για να δούμε πως αυτή η ποσότητα έχει να κάνει με την έννοια της ισοδυναμίας, ας υποθέσουμε ότι οι δύο τετραγωνικές μορφές $f(x,y), g(x,y)$ έχουν διακρίνουσες D, D' αντίστοιχα. Επίσης $f(x,y) = g(px+qy+rx+sy),\ p,q,r,s \in \mathbb{Z}$. Τότε θα είναι $D = (ps-qr)^2 D'$, επομένως οι δύο μορφές θα έχουν τις ίδιες διακρίνουσες μόνο αν $ps - qr = \pm 1$, δηλαδή πρέπει να είναι ισοδύναμες.

Το πρόσημο τώρα της διακρίνουσας μιας μορφής είναι πολύ σημαντικό για τη συμπεριφορά της μορφής. Αν έχουμε τη μορφή $f(x,y) = ax^2 + bxy + cy^2$, τότε ισοδύναμα θα έχουμε

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2 + b^2y^2 - b^2y^2 = (2ax+by)^2 - y^2(b^2 - 4ac)$$

$$\iff 4af(x,y) = (2ax+by)^2 - Dy^2.$$

Αν έχουμε $D > 0$, τότε η τετραγωνική μας μορφή απεικονίζει και θετικούς και αρνητικούς αριθμούς και την καλούμε απροσδιόριστη, ενώ αν $D < 0$ τότε θα έχουμε απεικόνιση ή μόνο θετικών, ή μόνο αρνητικών αριθμών, πράγμα το οποίο εξαρτάται από το πρόσημο του a. Σε αυτήν την περίπτωση η μορφή θα ονομάζεται θετικά ορισμένη, ή αρνητικά ορισμένη αντίστοιχα. Εμείς θα ασχοληθούμε μόνο με τις θετικά ορισμένες τετραγωνικές μορφές. Η διακρίνουσα έχει ακόμα ένα σημαντικό χαρακτηριστικό. Αφού έχουμε $D = b^2 - 4ac \iff D = b^2 mod 4$, συνεπώς ο συντελεστής b θα είναι άρτιος αν και μόνο αν $D = 0 \bmod 4$, ή θα είναι περιττός αν και μόνο αν $D = 1 \bmod 4$.

Λήμμα 8.2 *Έστω ότι έχουμε* $D = 0, 1 \bmod 4$ *και* m *ένας περιττός ακέραιος για τον οποίο ισχύει ότι* $(D,m) = 1$. *Τότε ο* m *θα απεικονίζεται γνήσια από μία πρωταρχική μορφή διακρίνουσας* D, *αν και μόνο αν η* D *είναι τετραγωνικό υπόλοιπο* $\bmod m$.

Απόδειξη. Για την ορθή φορά, ας υποθέσουμε ότι η $f(x,y)$ απεικονίζει γνήσια το m. Τότε, όπως γνωρίζουμε από τα προηγούμενα θα είναι $f(x,y) = mx^2 + bxy + cy^2$, οπότε $D = b^2 - 4mc$ δηλαδή $D \equiv b^2 \bmod m$. Για το αντίστροφο,

υποθέτουμε ότι $D \equiv b^2 \bmod m$. Αφού ο m είναι περιττός, τότε τα D και b είναι και οι δύο άρτιοι, ή και οι δύο περιττοί. Έτσι, και σύμφωνα με την προηγούμενη παρατήρηση είναι $D \equiv 0, 1 \bmod 4$, επομένως θα είναι $D \equiv b^2 \bmod 4m$. Αυτό προφανώς σημαίνει ότι για κάποιο c θα είναι $D = b^2 - 4mc$. Το οποίο με τη σειρά του, σημαίνει ότι η μορφή $mx^2+bxy+cy^2$ με διακρίνουσα D, θα απεικονίζει γνήσια το m. Για την ολοκλήρωση της απόδειξης να σημειώσουμε ότι οι συντελεστές είναι πρώτοι μεταξύ τους, από την στιγμή που οι m και D είναι σχετικά πρώτοι. Δηλαδή έχουμε να κάνουμε με πρωταρχική μορφή.

Προχωρούμε τώρα στη διατύπωση ενός πορίσματος, το οποίο είναι άμεσο συμπέρασμα του λήμματος που μόλις αποδείξαμε.

Πόρισμα 8.1 *Έστω $n \in \mathbb{Z}$ και p περιττός πρώτος, ο οποίος δε διαιρεί το n. Τότε θα είναι $(-n/p) = 1$, αν και μόνο αν ο p απεικονίζεται από μία πρωταρχική μορφή, διακρίνουσας $D = -4n$.*

Απόδειξη. Το πόρισμα είναι άμεσο συμπέρασμα από το προηγούμενο λήμμα αφού το $-4n$ είναι τετραγωνικό υπόλοιπο $\bmod p$ αν και μόνο αν $(-4n/p) = (-n/p) = 1$.

Το ερώτημα που θα μας απασχολήσει, θα είναι να βρούμε πρώτους διαιρέτες της μορφής x^2+ny^2 με $(x, y) = 1$. Με το παραπάνω πόρισμα, δώσαμε μία πρώτη απάντηση στο ερώτημα αυτό, αφού θέλουμε πρώτους που ικανοποιούν $(-n/p) = 1$, δηλαδή πρώτους που απεικονίζονται από πρωταρχικές μορφές διακρίνουσας $-4n$. Το πρόβλημα που παρουσιάζεται είναι ότι έχουμε πολλές μορφές με την ίδια διακρίνουσα. Επομένως θα προσπαθήσουμε να αποδείξουμε ότι κάθε μορφή ισοδυναμεί μα μία άλλη.

Μέχρι τώρα μιλούσαμε γενικά για τετραγωνικές μορφές, αλλά από εδώ και πέρα θα ασχοληθούμε μόνο με τις θετικά ορισμένες, οι οποίες έχουν και ιδιαίτερο ενδιαφέρον. Πιο συγκεκριμένα ας δούμε τις ανηγμένες μορφές (reduced forms).

Ορισμός 8.6 *Μία πρωταρχική, θετικά ορισμένη τετραγωνική μορφή $ax^2+bxy+cy^2$, θα καλείται ανηγμένη αν*

$$|b| \leq a < c, \text{ και } b \geq 0 \text{ ή αλλιώς } |b| = a \text{ ή } a = c.$$

Θεώρημα 8.1 *Κάθε πρωταρχική, θετικά ορισμένη μορφή, είναι γνήσια ισοδύναμη με μία ανηγμένη μορφή.*

Μετά την διατύπωση αυτού του θεωρήματος, μπορούμε να κάνουμε σαφή διαχωρισμό μεταξύ των εννοιών της ισοδυναμίας και της γνήσιας ισοδυναμίας. Για παράδειγμα ας δούμε την περίπτωση $3x^2 \pm 2xy + 5y^2$ όπου οι δύο μορφές είναι είναι ισοδύναμες, αλλά αφού είναι και οι δύο ανηγμένες, το προηγούμενο θεώρημα μας λέει ότι δεν είναι γνήσια ισοδύναμες. Ενώ αν έχουμε $2x^2 \pm 2xy + 3y^2$, βλέπουμε ότι μόνο η $2x^2+2xy+3y^2$ είναι ανηγμένη, αφού $a = |b|$. Άρα οι δύο αυτές μορφές είναι και γνήσια ισοδύναμες.

Προχωρούμε τώρα σε μία τελευταία παρατήρηση η οποία θα κλείσει το πέρασμά μας στην θεωρία των τετραγωνικών μορφών. Ας υποθέσουμε ότι έχουμε μία ανηγμένη μορφή $ax^2 + bxy + cy^2$ με διακρίνουσα $D < 0$. Τότε θα είναι $b^2 \leq a^2, a \leq c$, επομένως

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \Longleftrightarrow a \leq \sqrt{-D/3}.$$

Αν λοιπόν έχουμε φιξάρει το D τότε $|b| \leq a$ και η σχέση που μόλις καταλήξαμε μας λέει ότι έχουμε πεπερασμένες επιλογές για τα a, b. Επίσης αφού $D = b^2 - 4ac$ το ίδιο θα ισχύει και για το c. Έτσι έχουμε πεπερασμένο πλήθος ανηγμένων μορφών με δοθείσα διακρίνουσα D. Σύμφωνα με το θεώρημα 8.1, θα έχουμε και πεπερασμένο πλήθος κλάσεων γνήσιων ισοδυναμιών. Αυτόν τον αριθμό, των κλάσεων των πρωταρχικών θετικά ορισμένων μορφών, διακρίνουσας D θα τον συμβολίζουμε με $h(D)$. Ο οποίος σύμφωνα με το θεώρημα 8.1, είναι το πλήθος των ανηγμένων μορφών. Συνοψίζοντας, μπορούμε να διατυπώσουμε το παρακάτω θεώρημα.

Θεώρημα 8.2 *Έστω ότι έχουμε επιλέξει $D < 0$. Ο αριθμός $h(D)$ των κλάσεων ισοδυναμίας των πρωταρχικών, θετικά ορισμένων μορφών, διακρίνουσας D, είναι πεπερασμένος και ισούται με το πλήθος των ανηγμένων μορφών διακρίνουσας D.*

Βιβλιογραφία

[1] Ian Stewart David Tall, *Algebraic Number Theory*, Chapman and hall Math series.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics Springer-Verlag, (1991).

[3] Daniel Marcus, *Number Fields*, Springer, (1977).

[4] David Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley and Sons, (1989).

[5] F.Blake G.Seroussi N.P.Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, (1999).

[6] G.Shimura *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton, NJ: Princeton University Press, (1971).

[7] Serge Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, (1970).

[8] Ι.Αντωνιάδης, *Ελλειπτικές Καμπύλες (το θεώρημα του Mordell)*, (1999).

[9] Κ.Λάκκης - Γ.Τζιντζής, *Ασκήσεις Θεωρίας Αριθμών*, Εκδόσεις Ζήτη, (1989).

[10] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer.

[11] Κ.Λάκκης *Θεωρία Αριθμών*, Εκδόσεις Ζήτη, (1988).

[12] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag, (1989).

[13] J. Fraleigh, *Εισαγωγή στην Άλγεβρα*, Παν/κές Εκδόσεις Κρήτης, (1996).

[14] Χ.Γεωργαντάς, *Ελλειπτικές Καμπύλες και Εφαρμογές στην Κρυπτογραφία*, Πτυχιακή εργασία, (2003).