Κεφάλαιο ΙΙ

Αλγεβρικές καμπύλες και κωδικοποίηση

Στόχος μας είναι η εισαγωγή στη θεωρία των κωδίκων Goppa. Πρόκειται για μια κλάση κωδίκων διόρθωσης λαθών με εντυπωσιακά καλές παραμέτρους.

Στην αρχή θα ασχοληθούμε με στοιχεία της θεωρίας αλγεβρικών καμπύλων. Η μελέτη θα γίνει με όσο το δυνατόν πιο εύκολο τρόπο.

1. Αλγεβρικές καμπύλες

Έστω K σώμα. Θεωρούμε τον δακτύλιο K[X, Y] των πολυωνύμων δύο μεταβλητών με συντελεστές από το σώμα K.

Έστω ένα πολυώνυμο $f(X, Y) \in K[X, Y]$. Το σύνολο

$$C_f(K) = \{(a, b) \in K \times K \text{ για τα οποία } f(a, b) = 0\}$$

θα λέγεται καμπύλη C_f και θα γράφουμε $C_f(X, Y) = 0$

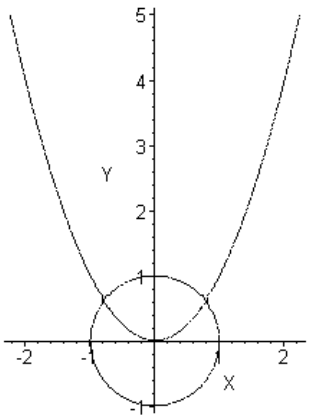
Παραδείγματα 2.1.1

(1) Η καμπύλη $C_f(\mathbf{R}) = \{(a, b) \in \mathbf{R} \times \mathbf{R}$ για τα οποία $f(a, b) = 0\}$ όπου $f(X,Y) = X^2 + Y^2 - 1$ είναι ένας κύκλος.

(2) Αν $f(X,Y) = X^2 + Y^2 + 1$. Τότε, $C_f(\mathbf{R}) = \varnothing$ ενώ $C_f(\mathbf{C}) \neq \varnothing$ αφού για παράδειγμα $(0, i) \in C_f(\mathbf{C})$.

(3) Αν $f(X,Y) = Y - X^2$ τότε η καμπύλη $C_f(\mathbf{R})$ είναι μία παραβολή.

(4) Αν $f(X,Y) = (X^2 + Y^2 - 1)(Y - X^2)$ τότε η καμπύλη $C_f(\mathbf{R})$ είναι



Ορισμός 2.1.2 Ένα μη σταθερό πολυώνυμο $f(X, Y) \in K[X, Y]$ θα λέγεται **ανάγωγο** όταν δεν επιδέχεται παραγοντοποίηση της μορφής $f = gh$ όπου g, h μη σταθερά πολυώνυμα με $\deg g < \deg f$ και $\deg h < \deg f$.

Παράδειγμα 2.1.3 Το πολυώνυμο $f(X, Y) = Y - X \in K[X, Y]$ είναι ανάγωγο. Ομοίως, το πολυώνυμο $f(X, Y) = X^3Y + Y^3 + X \in \mathbf{F}_2[X, Y]$

Θα αποδείξουμε ότι τα πολυώνυμα δύο μεταβλητών αναλύονται σε γινόμενο ανάγωγων παραγόντων. Η απόδειξη είναι πιο δύσκολη από την περίπτωση μίας μεταβλητής διοτί δεν ισχύει η Ευκλείδεια διαίρεση.

Ορισμός 2.1.4 Ένα πολυώνυμο $f(X, Y) \in K[X, Y]$ θα λέγεται **απόλυτα ανάγωγο** όταν παραμένει ανάγωγο σε κάθε δακτύλιο $L[X, Y]$ όπου L οποιαδήποτε πεπερασμένη επέκταση του K.

Σημείωση 2.1.5 Ένα πολυώνυμο $f(X) \in K[X]$ είναι απόλυτο ανάγωγο αν και μόνο αν $f(X) = aX + b$ για κάποια $a, b \in K$.

Πρόταση 2.1.6 Αν $f(X, Y) \in K[X, Y]$ μη-σταθερό πολυώνυμο τότε υπάρχει πεπερασμένη επέκταση L του K τέτοια ώστε το $f(X, Y)$ να έχει έναν τουλάχιστον ανάγωγο παράγοντα στον δακτύλιο $L[X, Y]$.

Πόρισμα 2.1.7 Αν $f(X, Y) \in K[X, Y]$ μη-σταθερό πολυώνυμο τότε υπάρχει πεπερασμένη επέκταση L του K τέτοια ώστε το $f(X, Y)$ να αναλύεται στον δακτύλιο $L[X, Y]$ σε γινόμενο απόλυτα ανάγωγων πολυωνύμων.

Το ακόλουθο κριτήριο μας δείχνει τον τρόπο να κατασκευάζουμε απόλυτα ανάγωγα πολυώνυμα.

Πρόταση 2.1.8 (Κριτήριο Eisenstein)

Αν το πολυώνυμο $f(X, Y) \in K[X, Y]$ το γράψουμε στη μορφή

$$f(X, Y) = f_0(X) + f_1(X)Y + \ldots + f_n(X)\, Y^n$$

και υποθέσουμε ότι $ΜΚΔ(f_0(X), f_1(X), \ldots, f_n(X)) = 1$ και επίσης ότι υπάρχει ένα στοιχείο $\alpha \in L$, σε κάποια πεπερασμένη επέκταση L του K, τέτοιο ώστε:

(1) Το α δεν είναι ρίζα του $f_n(X)$
(2) Το α είναι ρίζα του $f_i(X)$ για κάθε $i < n$
(3) Το α δεν είναι διπλή ρίζα του $f_0(X)$

Τότε το $f(X, Y)$ είναι απόλυτα ανάγωγο.

Σημείωση Το κριτήριο του Eisenstein είναι αναγκαία αλλά όχι και ικανή συνθήκη.

Πόρισμα 2.1.9 Για κάθε σώμα K υπάρχουν άπειρα απολύτως ανάγωγα πολυώνυμα $f(X, Y) \in K[X, Y]$.

Απόδειξη Θεωρούμε όλα τα πολυώνυμα της μορφής

$$f(X, Y) = Y^n - X \in K[X, Y]$$

είναι όλα τα τους, δηλαδή για κάθε φυσικό n, απολύτως ανάγωγα. Αυτό προκύπτει με εφαρμογή της πρότασης 2.1.8 για $\alpha = 0$.

Έστω $f(X, Y) \in K[X, Y]$ απόλυτα ανάγωγο πολυώνυμο. Για λόγους που θα φανούν παρακάτω αναγκαζόμαστε συχνά να θεωρήσουμε προβολικές αλγεβρικές καμπύλες.

Πρακτικός κανόνας Προσθέτουμε μια ακόμη μεταβλητή Z έτσι ώστε το πολυώνυμο $f(X, Y)$ να γίνει ομογενές.

Για παράδειγμα, αν $f(X, Y) = X^2 + Y^2 + 1$ τότε το αντίστοιχο ομογενές πολυώνυμο είναι το $g(X, Y, Z) = X^2 + Y^2 + Z^2$. Το $f(X, Y)$ προκύπτει από το $g(X, Y, Z)$ αν θέσουμε $Z = 1$. Για $Z = 0$ βρίσκουμε τα «επ' άπειρο» σημεία της καμπύλης.

Στη συνέχεια θα ασχοληθούμε με καμπύλες πάνω σε πεπερασμένα σώματα. Περίπτωση που ενδιαφέρει ιδιαίτερα τη θεωρία κωδίκων.

Υπενθυμίζουμε τον τρόπο κατασκευής πεπερασμένων σωμάτων. Για λόγους ευκολίας θα εξετάσουμε την περίπτωση $q = 2$.

Ξεκινάμε από το $\mathbf{F}_2 = \{0, 1\}$.

Το $X^2 + X + 1 \in \mathbf{F}_2[X]$ είναι ανάγωγο στο $\mathbf{F}_2[X]$ οπότε $\mathbf{F}_4 = \mathbf{F}_2[X] / \langle X^2 + X + 1 \rangle$. Αν α ρίζα του $X^2 + X + 1$ τότε ισχύει $\alpha^2 = \alpha + 1$ και $\mathbf{F}_4 = \{0, 1, \alpha, \alpha + 1\}$.

Ομοίως, κατασκευάζουμε τα πεπερασμένα σώματα $\mathbf{F}_8 = \mathbf{F}_2[X] / \langle X^3 + X^2 + 1 \rangle$ και $\mathbf{F}_{16} = \mathbf{F}_2[X] / \langle X^4 + X^3 + 1 \rangle$.

Ας θεωρήσουμε τώρα το πολυώνυμο $f(X, Y) = X^3 + Y^3 + 1 \in \mathbf{F}_2[X, Y]$. Αν εφαρμόσουμε το κριτήριο του Eisestein για $\alpha = 1$ βλέπουμε ότι είναι απόλυτα ανάγωγο.