Αλγεβρικές Δομές ΙΙ

Σύνολο ασκήσεων 5

Εβδομάδα 1.04.14-7.04.14

1. Έστω p πρώτος. Να δείξετε ότι στο σώμα $\mathbb{Z}_p$ τα στοιχεία $\overline{1}$ και $\overline{p-1}$ είναι τα μόνα στοιχεία που είναι αντίστροφα του εαυτού τους. Να αποφασίσετε αν ισχύει ότι $x^p + a = (x+a)^p$ στο $\mathbb{Z}_p[x]$.

Απάντηση Τα στοιχεία που είναι αντίστροφα του εαυτού τους είναι ρίζες του πολυωνύμου $x^2 - 1$. Ένα πολυώνυμο δευτέρου βαθμού έχει το πολύ δύο ρίζες σε ένα σώμα. Το $\overline{1}$ και $\overline{p-1} = \overline{-1}$ είναι ρίζες.

Είναι εύκολο να δει κανείς ότι p πρώτος διαιρεί $\binom{p}{k}$ για κάθε $k \neq 0, p$. Από το δυωνυμικό ανάπτυγμα προκύπτει ότι $(x+a)^p = x^p + a^p$. Αφού $a^p = a$ για κάθε a στο $\mathbb{Z}_p$ έπεται ότι $x^p + a = (x+a)^p$.

2. Να βρείτε το υπόλοιπο της διαίρεσης του πολυωνύμου $x^6 + 3x^5 + 4x^2 - 3x + 2$ με το $3x^2 + 2x - 3$ στο $\mathbb{Z}_7[x]$.

Απάντηση $x^6+3x^5+4x^2-3x+2 = (x^2+2x-3)(5x^4+5x^2-x)-6x+2$.

3. Έστω τα πολυώνυμα $x^5 - 1$, $x^6 - 1$, $x^7 - x$ στο $\mathbb{Z}_{14}[x]$. Να βρείτε τις ρίζες τους.

Απάντηση $\phi(14) = 6$. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{14}$ έχουν τάξη που διαιρεί το 6 και είναι ρίζες του $x^6 - 1$. Τα αντιστρέψιμα στοιχεία είναι τα $1, 3, 5, 9, 11, 13$. Η τάξη των στοιχείων που είναι ρίζες του $x^5 - 1$ πρέπει να διαιρεί το 5. Το μόνο στοιχείο που μπορεί να είναι ρίζα του $x^5 - 1$ είναι αυτό που έχει τάξη 1, δηλ. το 1. Είναι προφανές ότι όλα τα αντιστρέψιμα είναι ρίζες του $x(x^7 - 1)$. Επίσης 0 είναι ρίζα. Το ίδιο ισχύει για το 2: $2^4 = 2 \Rightarrow 2^7 = 2^4 2^3 = 2^4 = 2$. Αντίστοιχα για το 7. Έπεται ότι όλα τα στοιχεία του $\mathbb{Z}_{14}$ είναι ρίζες του $x^7 - x$: $((ab)^7 = a^7 b^7 = ab)$.

3. Έστω $I = (3, \sqrt{2})$, $J = (2, \sqrt{2})$ ιδεώδη στον $\mathbb{Z}[\sqrt{2}]$. Να βρείτε γεννήτορες για τα ιδεώδη $I + J$, IJ, $I \cap J$. Να αποδείξετε ότι αν $a + b\sqrt{2} \notin J$ τότε $J + (a + b\sqrt{2}) = \mathbb{Z}[\sqrt{2}]$.

Απάντηση $I = (1)$ αφού $2 = \sqrt{2}\sqrt{2} \in I$ και $3 - 2 \in I$. Επίσης $J = (\sqrt{2})$. Έπεται ότι $I + J = \mathbb{Z}[\sqrt{2}]$, $IJ = I \cap J = J$. Αν $a + b\sqrt{2} \notin J$ τότε αφού $b\sqrt{2} \in J$ έπεται ότι $a \notin J$. Επομένως $a \notin 2\mathbb{Z}$. Επομένως $a = 2k + 1$. Έπεται ότι $J + (a + b\sqrt{2}) = (\sqrt{2}, a) = (1)$ αφού $1 = (2k+1) - 2$.