4. KŪNŲ PLĖTINIAI

UŽDAVINIAI.

1. Minimalaus polinomo radimas.

1.1. Raskite elemento $\beta = a\alpha^3 + b\alpha^2 + c\alpha + d \in Q(\alpha)$ minimalųjį polinomą , kai α yra ketvirtojo laipsnio neredukuojamo polinomo $m(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in Q[x]$ šaknis.

1.2. Raskite elemento $\beta = a\alpha^3 + b\alpha^2 + c\alpha + d \in GF(p)(\alpha)$ minimalųjį polinomą , kai α yra ketvirtojo laipsnio neredukuojamo polinomo $m(x) = x^4 + a_{p3}x^3 + a_{p2}x^2 + a_{p1}x + a_{p0} \in GF(p)[x]$ šaknis.

2. Atvirkštinio kūno elemento radimas.

2.1. Raskite elemento $\beta = a\alpha^3 + b\alpha^2 + c\alpha + d \in Q(\alpha)$ iš 1.1. atvirkštinį elementą $\beta^{-1} + \beta$.

2.2. Raskite elemento $\beta = a\alpha^3 + b\alpha^2 + c\alpha + d \in GF(p)(\alpha)$ iš 1.2. atvirkštinį elementą $\beta^{-1} + \beta$.

3. Neredukuojamo polinomo faktorizacija.

3.1. Faktorizuokite neredukuojamą polinomą $m(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in Q[x]$ iš 1.1 kūne $Q(\alpha)$. Ar $Q(\alpha)$ yra polinomo $m(x)$ skaidymo kūnas?

3.2. Faktorizuokite neredukuojamą polinomą $m(x) = x^4 + a_{p3}x^3 + a_{p2}x^2 + a_{p1}x + a_{p0} \in GF(p)[x]$ iš 1.2 kūne $GF(p)(\alpha)$. Ar $GF(p)(\alpha)$ yra polinomo $m(x)$ skaidymo kūnas?

PARAMETRAI.

Visoms grupėms: $a \neq 0, b \neq 0, c \neq 0, d \neq 0$; pirminis skaičius $p = 5$.

1 grupei: $a_3, a_{p3} \neq 0; a_2, a_{p2} \neq 0; a_1, a_{p1} \neq 0; a_0, a_{p0} \neq 0$.

2 grupei: $a_3, a_{p3} = 0; a_2, a_{p2} \neq 0; a_1, a_{p1} \neq 0; a_0, a_{p0} \neq 0$.

3 grupei: $a_3, a_{p3} \neq 0; a_2, a_{p2} = 0; a_1, a_{p1} \neq 0; a_0, a_{p0} \neq 0$.

4 grupei: $a_3, a_{p3} \neq 0; a_2, a_{p2} \neq 0; a_1, a_{p1} = 0; a_0, a_{p0} \neq 0$.