UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

3rd set

Exercise 1. For a finite field $\mathbb{F}_q$, with q odd, show that an element $a \in \mathbb{F}_q^*$ has a square root in $\mathbb{F}_q$ if and only if $a^{(q-1)/2} = 1$.

Exercise 2. Set $\mathbb{I}_q(n) := \{f \in \mathbb{F}_q[X] \mid f \text{ monic and irreducible of degree } n\}$ and $\pi_q(n) := |\mathbb{I}_q(n)|$.

1. Compute the numbers $\pi_3(1)$ and $\pi_3(2)$.
2. Find the sets $\mathbb{I}_3(1)$ and $\mathbb{I}_3(2)$.
3. Factor $X^9 - X$ over $\mathbb{F}_3$.

Exercise 3. How many elements does $\mathbb{F}_{5^6}$ have, that do not belong in any of its proper subfields? How many of them are non-primitive?

Exercise 4.
1. Find the set $D := \{d \in \mathbb{N} : d \mid 30 \text{ and } (d, 3) = 1\}$.
2. For every $d \in D$, write Ψ_d over $\mathbb{F}_3$ and describe its factorization, where Ψ_n stands for the n-th cyclotomic polynomial.
3. Factor $X^{30} - 1$ over $\mathbb{F}_3$.

Exercise 5.
1. Find the least prime p, such that $X^{22} + X^{21} + \cdots + X + 1$ is irreducible over $\mathbb{F}_p$.
2. Find the least prime $p > 7$ such that $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$ factors into linear factors. How does it factor over $\mathbb{F}_7$?

Exercise 6. Show that for $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$ the polynomial $x^{q^n} - x + na$ is divisible by $x^q - x + a$ over $\mathbb{F}_q$.

Exercise 7. Let $q = p^k$, for some k. Prove that $\mathrm{Tr}(a^{p^n}) = (\mathrm{Tr}(a))^{p^n}$ for all $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$.

Exercise 8. Let $q = p^m$. Prove that if $\{a_1, \ldots, a_m\}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, then $\mathrm{Tr}(a_i) \neq 0$ for at least one $1 \leq i \leq m$.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΕΦΑΡΜΟΣΜΕΝΗ ΑΛΓΕΒΡΑ - ΜΕΜ244 (ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2019-20)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

3ο σετ ασκήσεων

Άσκηση 1. Για ένα πεπερασμένο σώμα $\mathbb{F}_q$, με q περιττό, δείξτε ότι το $a \in \mathbb{F}_q^*$ έχει τετραγωνική ρίζα στο $\mathbb{F}_q$ αν και μόνο αν $a^{(q-1)/2} = 1$.

Άσκηση 2. Θέτουμε $\mathbb{I}_q(n) := \{f \in \mathbb{F}_q[X] \mid f \text{ μονικό και ανάγωγο βαθμού } n\}$ και $\pi_q(n) := |\mathbb{I}_q(n)|$.

1. Υπολογίστε τους αριθμούς $\pi_3(1)$ και $\pi_3(2)$.
2. Βρείτε τα σύνολα $\mathbb{I}_3(1)$ και $\mathbb{I}_3(2)$.
3. Αναλύστε σε ανάγωγους παράγοντες το $X^9 - X$ υπέρ του $\mathbb{F}_3$.

Άσκηση 3. Πόσα στοιχεία έχει το $\mathbb{F}_{5^6}$ που δεν ανήκουν σε κανένα γνήσιο υπόσωμά του; Πόσα από αυτά δεν είναι πρωταρχικά;

Άσκηση 4.
1. Βρείτε το σύνολο $D := \{d \in \mathbb{N} : d \mid 30 \text{ and } (d, 3) = 1\}$.
2. Για κάθε $d \in D$, γράψτε το Ψ_d υπέρ του $\mathbb{F}_3$ και περιγράψτε την παραγοντοποίησή του, όπου Ψ_n το n-στο κυκλοτομικό πολυώνυμο.
3. Παραγοντοποιείστε το $X^{30} - 1$ υπέρ του $\mathbb{F}_3$.

Άσκηση 5.
1. Βρείτε τον ελάχιστο πρώτο p, τέτοιο ώστε το $X^{22} + X^{21} + \cdots + X + 1$ να είναι ανάγωγο υπέρ του $\mathbb{F}_p$.
2. Βρείτε τον ελάχιστο πρώτο $p > 7$ τέτοιον ώστε το $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$ αναλύεται σε γραμμικούς (πρωτοβάθμιους) όρους. Πώς παραγοντοποιείται στο $\mathbb{F}_7$?

Άσκηση 6. Δείξτε ότι για $a \in \mathbb{F}_q$ και $n \in \mathbb{N}$ το πολυώνυμο $x^{q^n} - x + na$ διαιρείται από το $x^q - x + a$ στο $\mathbb{F}_q$.

Άσκηση 7. Έστω $q = p^k$, για κάποιο k. Δείξτε ότι $\mathrm{Tr}(a^{p^n}) = (\mathrm{Tr}(a))^{p^n}$ για κάθε $a \in \mathbb{F}_q$ και $n \in \mathbb{N}$.

Άσκηση 8. Έστω $q = p^m$. Δείξτε ότι αν $\{a_1, \ldots, a_m\}$ είναι μια $\mathbb{F}_p$-βάση του $\mathbb{F}_q$, τότε $\mathrm{Tr}(a_i) \neq 0$ για κάποιο $1 \leq i \leq m$.